IBM InfoSphere Identity Insight

ユーザー・ガイド

バージョン ***9*** リリース ***0***

IBM InfoSphere Identity Insight

ユーザー・ガイド

バージョン ***9*** リリース ***0***

注記

本書および本書で紹介する製品をご使用になる前に、 461 ページの『特記事項』に記載されている情報をお読みください。

注意

本書は、IBM InfoSphere Identity Insight (製品番号 5724-L71) バージョン 9 リリース 0、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM InfoSphere Identity Insight
User Guide
Version 9 Release 0

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

前書き

IBM InfoSphere Identity Insight は、人物または事物の真のアイデンティティー (誰が誰であるのか) の認識に関連する業務上の問題、ならびに、顧客、従業員、取引先、およびその他の外部関係者間の関係 (誰が誰を知っているのか) の潜在的な価値または危険性の特定に関連する業務上の問題を解決できるよう組織を支援します。この分析は、既存のビジネス・アプリケーションのコンテキストでリアルタイムで行われます。IBM InfoSphere Identity Insight は、あらゆる業界において脅威、不正、悪用、および共謀の防止に役立つ、即時性があり実用的な情報を提供します。

本書について

IBM InfoSphere Identity Insight V8.1 は、脅威および不正に対抗するための、拡張が容易なエンティティー解決および分析のプラットフォームです。本書では、製品が提供するアイデンティティーおよび関係の曖昧性除去テクノロジーを使用し、そのテクノロジーをお客様の組織の機能に適用して、「誰が誰であるか?」、「誰が誰を知っているか?」、および「誰が何をするか?」を認識する方法に関する情報を記載します。長い期間をかけてアイデンティティー・コンテキストを蓄積することにより、InfoSphere Identity Insight V8.1 は、情報のさまざまなエンタープライズ・ソースを使用して、各個人が本当に本人が主張するとおりの人物であるかどうかを判定します。洗練されたエンティティー・アルゴリズムと特許を取得した多文化対応の名前分析とを適用することで、特定の個人が過去に身元識別されたことがあるかどうか、組織にとって新しい個人かどうか、または新しい事実に基づいて修正を必要とする以前の仮説があるかどうかを判断できます。

対象読者

本書は、システム・アドミニストレーター、アプリケーション・デベロッパー、データ・アナリスト、および IBM Professional Services 担当員がお客様の環境で本製品を有効に使用できるようにすることを意図しています。

前提条件および関連情報

このユーザー・ガイドは、オンラインのインフォメーション・センター (http://publib.boulder.ibm.com/infocenter/easii/v8r1m0/index.jsp) にある情報のサブセットです。これはユーザーの利便性を考えて提供されています。その他の製品情報のソースには以下が含まれます。

- IBM InfoSphere Identity Insight バージョン 8 リリース 1 リリース・ノート
- WebSphere Application Server の資料
- 使用するデータベース・ソフトウェアの資料
- IBM Cognos Business Intelligence ソフトウェア資料
- IBM ILOG Visualization ソフトウェア資料
- ご使用のデプロイメントに応じて、以下の情報のいずれかが含まれます。
  - メッセージ・キューイング・ソフトウェア資料

– 住所修正ソフトウェア資料
– ETL ツール・ソフトウェア資料

ご意見の送付方法

IBM にお客様のご意見をお寄せください。本書または他の IBM InfoSphere Identity Insight 資料についてコメントがある場合は、次のフォームを使用してコメントをお送りください。

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

また、インフォメーション・センターにアクセスし、そこに組み込まれているフィードバック・フォームと関連のフィードバック・オプションを使用することもできます。

IBM ソフトウェア・サポートへの連絡

IBM ソフトウェア・サポートは、製品の障害に関する支援を提供します。

始める前に

IBM ソフトウェア サポートに問い合わせるには、お客様の会社が有効な IBM ソフトウェア保守契約を結んでいること、およびお客様が IBM に問題を送信することを許可されていることが必要です。利用可能な保守契約の種類については、「*Software Support Handbook*」(techsupport.services.ibm.com/guides/services.html) の『Enhanced Support』を参照してください。

このタスクについて

問題について IBM ソフトウェア・サポートに連絡するには、以下の手順を実行します。

手順

1. 問題を明確にし、背景情報を収集し、問題の重大度を判断します。詳しくは、「*Software Support Handbook*」 (techsupport.services.ibm.com/guides/beforecontacting.html) の『Contacting IBM』を参照してください。
2. 診断情報を収集します。
3. IBM ソフトウェア・サポートを支援するために、問題レポートで以下の情報を提供できるように準備してください。
   - 製品の名前およびバージョン
   - データベースのタイプおよびバージョン
   - オペレーティング・システムの名前およびバージョン
4. 以下のいずれかの方法で問題を IBM ソフトウェア・サポートにお送りください。
   - オンライン: IBM ソフトウェア・サポート・サイト (http://www.ibm.com/software/support/probsub.html) の「**Submit and track problems**」をクリックします。

- 電話: お住まいの国でおかけになる電話番号については、「IBM Software Support Handbook」(techsupport.services.ibm.com/guides/contacts.html) の「Contacts」のページにアクセスしてください。

次のタスク

お送りいただいた問題がソフトウェアの欠陥、資料の不足、資料の不正確さに関するものの場合、IBM ソフトウェア・サポートではプログラム診断依頼書 (APAR) を作成します。この APAR には該当の問題が詳細に記載されます。IBM ソフトウェア・サポートでは、APAR が解決されてフィックスが配布されるまでの間実装できる回避策を可能な限り提供しています。IBM では、解決済みの APAR をソフトウェア・サポート Web サイトで毎日公開しています。これにより、同じ問題を抱える別のユーザーが同じ解決策を利用できるようになります。

第 1 章 IBM InfoSphere Identity Insight の概要

IBM® InfoSphere Identity Insight は、人物または事物の真のアイデンティティー (誰が誰であるのか) の認識に関連する業務上の問題、ならびに、顧客、従業員、取引先、およびその他の外部関係者間の関係 (誰が誰を知っているのか) の潜在的な価値または危険性の特定に関連する業務上の問題を解決できるよう組織を支援します。IBM InfoSphere Identity Insight は、あらゆる業界において脅威、不正、悪用、および共謀の防止に役立つ、即時性があり実用的な情報を提供します。

多くの組織では、アイデンティティーおよび関係を表す生データが既に存在します。大量のデータから最大限の洞察を導き出す必要がありますが、ほとんどのシステムで、それらの大量のデータを管理、分析、および解決する簡単な方法がないことが問題です。

IBM InfoSphere Identity Insight を使用すると、組織では、すべてのソース (顧客データベース、取引先リスト、従業員データベース、法規制遵守リスト、およびストリーミング・データ・フィードなど) からのデータをリアルタイムで管理、分析、および統合できます。IBM InfoSphere Identity Insight では、詳細な調査のために、アナリスト、セキュリティー担当者、またはその他の担当者に対してリアルタイム・アラートが送信されます。また、IBM InfoSphere Identity Insight の支援により、顧客に対する包括的な視点に基づき、顧客や顧客の市場区分のネットワークの価値を識別できます。

IBM InfoSphere Identity Insight を使用すると、組織では、すべてのナレッジベース・アプリケーションのプラットフォームとして使用できる集中動的エンティティー・データベースを作成できます。IBM InfoSphere Identity Insight は、多種多様なプロトコルおよびテクノロジーを通じて、他のエンタープライズ・システムと統合します。

アイデンティティーの認識

IBM InfoSphere Identity Insight は、エンティティー解決の中核処理を使用して、一致しない不明確なアイデンティティー・レコードを、それが意図的に虚偽表示されている場合でも、複数のデータ・セット間で包括的なエンティティーに解決します。

エンティティー解決中、IBM InfoSphere Identity Insight では以下が行われます。

- 異なるエンティティーのように見える複数のレコードが実際には単一のエンティティーである場合が特定されます。
- 解決されたエンティティーごとに、完全に異なるアイデンティティー・レコードがエンティティーの複合ビューに統合され、一方で各レコードのフル属性情報が維持されます。フル属性情報が保持されるため、データは損失せず、元のソースを常に探し出すことができます。
- 新しいデータがシステムにロードされると、IBM InfoSphere Identity Insight では、エンティティー・データベース内のエンティティーのコンテキストで情報が更新および管理されます。新規のデータまたは変更されたデータがロードされる

と、それらのデータの意味が完全に把握され、各トランザクションが最大限に活用され、エンティティー・データベース内の各エンティティーの包括的な視点が拡張されます。

関係の検出

複数のデータ・ソースからレコードがロードされ、処理されると、IBM InfoSphere Identity Insight では、エンティティー関係処理に基づいて、エンティティー・データベース内のエンティティー間の関係が検出されます。

エンティティー解決処理中、IBM InfoSphere Identity Insight では以下が行われます。

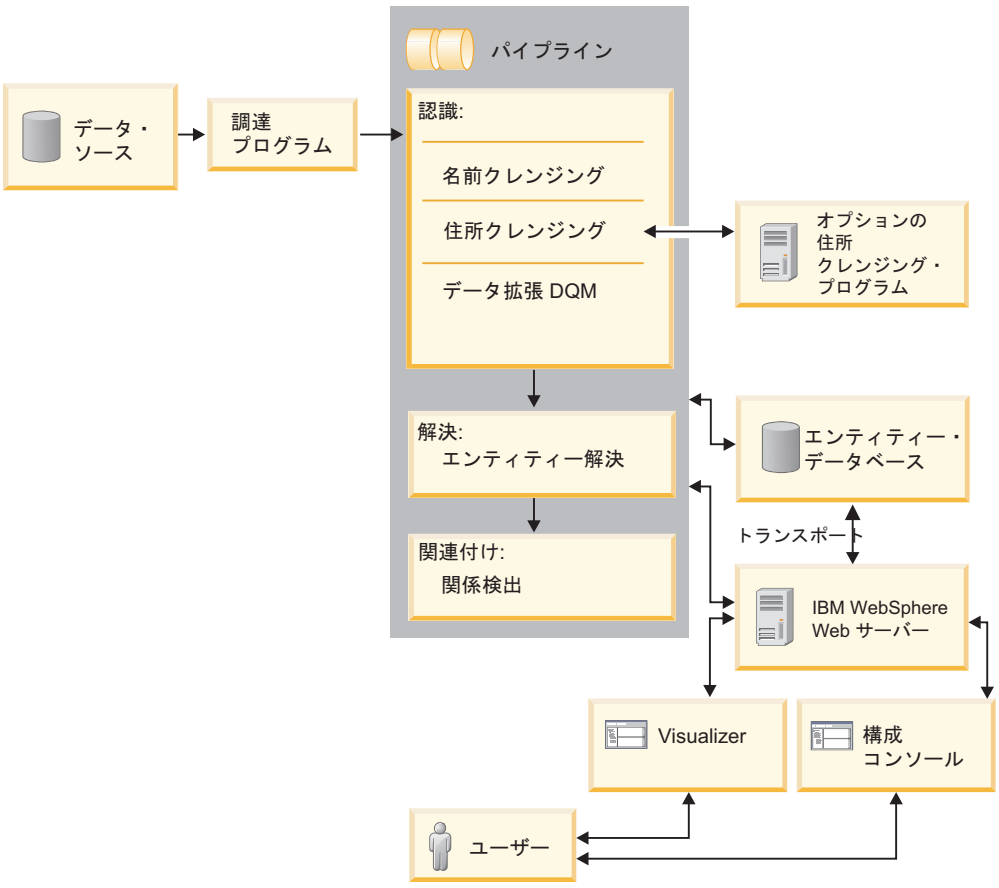
- 電話番号、住所など、アイデンティティー属性によりエンティティーがリンクされ、関連するが明らかではない関係が検出されます。
- 個々のデータ属性 (ID 番号、名前など)、ロケーション (IP アドレスなど)、施設 (倉庫、学校、空港、ホテルなど)、組織 (小集団、クラブ、団体、暴力団など)、お金 (現金、電信送金など)、および口座 (ロイヤルティー・クラブ、銀行、当座預金、クレジット、普通預金など) を使用して、関係者およびエンティティーのネットワークを整理します。
- 疑わしい関係または関心のある関係を特定し (それらの関係が隠蔽または偽装されていても)、一連のユーザー定義ルールに基づきリアルタイム・アラートを送信します。IBM InfoSphere Identity Insight を使用すると、アナリストおよび調査者は、エンティティー・データベースに対して高度な検索を実行して、関連する各エンティティーおよびすべてのエンティティー、またはそれらのエンティティーのリンク先の属性を詳細に調査できます。

IBM InfoSphere Identity Insight では、カスタマイズ可能なルール・ベースの例外報告もサポートされます。これにより、組織では、解決対象のどのエンティティーでアラートをトリガーするか、または検出対象のどの関係でアラートをトリガーするか指定できます。

製品体系

IBM InfoSphere Identity Insight は複数層のシステムであり、データ・ソースからのデータは調達プログラムを通じてシステムにロードされ、パイプライン・ノードでホストされるパイプラインにより処理されます。処理の結果はエンティティー・データベースに書き込まれます。この結果は他のシステムまたは他のデータベースにルーティングできます。

標準デプロイメントでは、複数データ・ソースからのエンタープライズ・データが調達プログラムに送信されます。調達プログラムで、データは Universal Messaging Format (UMF) に変換されます。各調達プログラムでは、トランスポートを使用してデータが 1 つ以上のパイプラインに送信されます。これらのトランスポートの多くは双方向トランスポートであり、調達プログラムに応答を提供するようにシステムを構成できます。



1 つ以上のパイプライン処理がパイプライン・ノードで実行されます。各パイプラインで、エンティティー・データベースへの専用接続が保持されます。パイプラインで 1 つ以上の調達プログラムから UMF データが受信されると、3 つの中核処理 (認識、解決、および関連付け) を通じてレコードごとにデータが処理されます。パイプラインで各レコードが処理されると、エンティティー・データベースに処理の結果が保管されます。

ユーザーは、次のインターフェースを使用してシステムと対話します。

- 構成コンソール。システムを構成およびモニターするために使用します。
- Analyst ツールキット・アプリケーション。アラートの分析および後処理、関係の探索、検索の実行、レポートの生成のために使用します。
- コマンド行インターフェース。パイプラインを実行するために使用します。
- Web サービス。パイプラインを実行するため、または製品を他のエンタープライズ・システム (カスタマイズ済みユーザー・インターフェースなど) に統合するために使用できます。

IBM InfoSphere Identity Insight は、IBM WebSphere Liberty を使用します。このアプリケーション・サーバーによって、構成コンソール、Analyst ツールキットのエレメント、および Web サービスがホストされます。

この堅固な体系により、デプロイメントの拡張容易性が実現します。パイプラインは、任意の数の小規模マシンまたは大規模マシンにデプロイできます。十分なデータベース容量がある場合、パイプラインのパフォーマンスを目的のレベルまで引き上げることができます。

調達プログラム

調達プログラムには、データを獲得して Universal Message Format (UMF) に変換し、変換したデータを処理用のパイプラインに送るためのツールとプログラムが含まれています。

製品に含まれている調達プログラム・ユーティリティーを使用して、データを UMF に変換できます。また、WebSphere® QualityStage などの抽出、変換、およびロード用のツール (ETL ツール) を調達プログラムとして使用することもできます。

Universal Message Format (UMF)

Universal Message Format (UMF) は、データ・ソース・ファイルの構造化に使用される拡張可能な XML の方言です。UMF には、アイデンティティー、関係、およびアクティビティーの主要な部分を表す標準タグが含まれています。データをパイプラインで処理する前に、データを UMF に変換して UMF 仕様に従う必要があります。

UMF は以下の階層コンポーネントで構成されています。

UMF 文書
: データを構成する UMF セグメントの集合であり、データ・ソース・レコードのタイプを示します。

UMF セグメント
: データ・ソースのデータを構成する UMF 文書の一部です。

UMF エレメント
: UMF 文書の UMF セグメント内のデータを定義する XML タグと値です。

UMF 仕様には、UMF 文書の具体的なタイプ、各 UMF 文書タイプ内の UMF セグメント、および各 UMF セグメント内の有効な UMF エレメントがリストされています。

パイプライン

パイプラインは、名前クレンジングと住所クレンジングおよびそれらの標準化、データ品質管理、およびエンティティー解決を実行するコンポーネントです。またパイプラインでは、システム構成に基づき、関係解決が実行され、アラートが生成されます。

パイプラインでは、次の 3 つの中核処理が実行されます。

- 認識。データの標準化、クレンジング、拡張、および品質チェックを実行することにより、入力データの最適化が行われます。
- 解決。エンティティーの解決が行われます。
- 関連付け。関係の検出とアラートの生成が行われます。

パイプラインは、パイプライン・ノードによりホストされます。

並列処理用のパイプラインを構成できます。これにより、1 つのパイプライン・コマンドで複数の並列パイプライン処理スレッドが生成され、システムで複数のデータ要求を同時に処理できます。この機能は、システム・パフォーマンスの改善、データ処理時間の削減、およびハードウェア・メモリー制約の緩和につながることがあります。

並列パイプライン処理機能は、次の 2 つの場所で構成します。

- グローバルな並行性設定は、構成コンソールの「システム構成」タブの「**パイプラインのデフォルトの並行性 (Pipeline default concurrency)**」パラメーターで制御します。この値により、パイプライン開始コマンドから開始される並列処理スレッドの数が決まります。このパラメーターのデフォルト値は 1 です。すなわち、このパラメーターを編集しない限り、1 つのパイプライン処理スレッドしか開始されません。
- ローカルの並行性設定 (パイプライン・ノード別) は、パイプライン構成ファイルで構成できます。パイプライン・ノード別のパイプライン構成ファイルで並行性パラメーターおよび値を指定すると、その値によりグローバル・システム・パラメーターがオーバーライドされます。そのパイプライン・ノードでパイプライン開始コマンドを発行すると、パイプライン構成ファイルに指定されている数と同じ数の並行パイプライン処理スレッドが開始されます。

パイプライン・ノード

パイプライン・ノードは、1 つ以上のパイプライン処理をホストする物理マシンです。

パイプライン・ノードは、パイプライン処理を実行するパイプライン実行可能ファイルをインストールし、開始する場所です。このマシンでホストされるすべてのパイプラインのパイプライン構成ファイルを構成および保持します。システムにより、パイプライン・ノードのログ・ファイルにパイプライン・メッセージが書き込まれます。

パイプライン・ノードにより、製品体系の次のコンポーネントにパイプライン処理が接続されます。

調達プログラム
: 抽出、変換、およびロード (ETL) 処理の一部として、調達プログラムはトランスポートを使用して UMF データを処理のためにパイプラインに送信します。調達プログラムのタイプに適したトランスポート方式を使用して、パイプラインに接続します。例えば、調達プログラムとして UMF ファイル・ユーティリティーを使用する場合、ファイル・トランスポートを使用します。

エンティティー・データベース
: エンティティー・データベースには、エンティティー情報が含まれます。パイプラインは、エンティティー解決および関係解決のために入力レコードを処理しながら、エンティティー情報にアクセスします。パイプラインでエンティティー・データベースにアクセスできるようにするために、パイプライン・ノードには適切なデータベース・クライアントがインストールされ、構成されている必要があります。

キュー
: データを処理のためにパイプラインに送信するトランスポート方式としてキューをシステムで使用する場合、各パイプライン・ノードに適切なメッセージ・キューイング・ソフトウェアをインストールし、構成する必要があります。

住所クレンジング・サーバー
: 住所の追加クレンジングのために、他社の住所クレンジング製品をシステムで使用する場合、その住所クレンジング・サーバーに接続するように各パイプライン・ノードを構成する必要があります。

Web サービス
: HTTP トランスポートを使用して、パイプライン・ノードでのパイプライン処理を Web サービスに接続する必要があります。

アプリケーション・モニター

構成コンソールにはアプリケーション・モニターがあり、これを使用して、パイプライン (の状況、統計、およびエラー) をモニターしたり、パイプラインと他のシステムまたはデータベースの間で結果をルーティングしたりします。

アプリケーション・モニターを使用するには、モニターするパイプライン、または結果をルーティングするパイプラインを、構成コンソールで登録する必要があります。

パイプラインのモニター

アプリケーション・モニターは SNMP エージェントと連携します。SNMP エージェントは、モニターするパイプラインをホストするパイプライン・ノードで実行されます。SNMP エージェントは、パイプライン・ノード上のすべての登録済みパイプラインに関する統計をアプリケーション・モニターに送信します。これらの統計は構成コンソールで公開されます。アプリケーション・モニターはパイプラインの状況と統計を 60 秒ごとに更新します。

パイプライン結果のルーティング

アプリケーション・モニターを使用すると、パイプラインで処理されたデータの結果を他のシステムまたはデータベースにルーティングできます。パイプライン処理の結果をルーティングするには、構成コンソールを使用してルーティング・ルールを構成します。ルーティング・ルールでは、ルーティング元のパイプライン、および結果のルーティング先を指定します。

例えば、一部の組織では、アナリストがエンティティー・データベースに対するレポート・クエリーを作成するのではなく (これは面倒な作業である場合がある)、結果のサブセットをレポート・データベースにルーティングする場合があります。アナリストは、レポート・データベースに対する調査レポート・クエリーを作成し、実行します。レポート・データベースには、アナリストにとって重要なエンティティー情報および関係情報のみ含まれます。

トランスポート

トランスポートにより、データが一方の場所から他方の場所 (調達プログラムとパイプライン間、パイプラインとエンティティー・データベース間、およびパイプラインと外部システム間) に移動します。

データをトランスポートするには、使用するトランスポート・モード・タイプ固有の構文フォーマットを使用する必要があります。これには、Universal Resource Identifier (URI) が含まれます。

IBM InfoSphere® Identity Insight は、次の複数のトランスポート方式をサポートしています。

- データベース
- ファイル
- HTTP
- メッセージ・キュー (IBM WebSphere MQ)

データ・ソース

データ・ソースには、エンティティー解決のために処理してエンティティー・データベースにロードする必要のある、アイデンティティーが含まれています。データ・ソースには、識別データ (アイデンティティーのユニークな個人 ID) と、非識別データ (アイデンティティーのその他の属性やデータ・ポイント) が含まれています。このデータ・ソース内のアイデンティティー・レコードをシステムで処理したり、エンティティー・データベースにロードしたりするためには、事前にそれらのレコードを Universal Message Format (UMF) としてエクスポートする必要があります。データ・ソースの例には、従業員リスト、監視リスト、顧客リスト、ベンダー・リストがあります (これらに限定されるわけではありません)。

データ・ソースには、元のソースに関する情報 (元のデータは UMF に変換済みであるため) や、データ・ソースの外部参照など、重要な情報が含まれています。これらの詳細によって、各データ・ソースがシステム内でユニークとなります。

エンティティー解決時に、2 つのエンティティーが未解決となった場合、システムはデータ・ソース情報を使用して、どの情報がどのエンティティーと結び付いているのかを判別します。

データ・ソースの場所とソース・システム

ソースの場所とソース・システムを作成し、それらをデータ・ソースに関連付けることで、入力データ・ソースを整理できます。ソースの場所とソース・システムを使用すると、同じようなタイプのデータ・ソースを区別することができます。

例えば、複数の場所からの予約データと人材データを処理する場合、次のようにデータ・ソースの場所を使用することで、どの場所から提供されたデータであるかを判別できます。

- プロパティー X 予約データ
- プロパティー X 人材データ
- プロパティー Y 予約データ
- プロパティー Y 人材データ

データ・ソース別の構成

エンティティー解決および関係検出の結果を最大化するには、以下の設定を使用して各データ・ソースを構成します。

ロール
: データ・ソースは同じタイプのデータをグループ化したものであるため、同じ入力データ・ソース内のすべてのアイデンティティー・レコードに自動的に同じロールを割り当てることができます。例えば、人材のデータ・ソースに「従業員 (Employee)」ロールを関連付けることで、従業員リストからのすべての入力レコードに自動的に「従業員 (Employee)」ロールが割り当てられます。

ロード・レベル
: 入力データ・ソース内のすべてのデータをロードするのか、1 つ以上のエンティティーに解決されるデータまたは 1 つ以上のエンティティーに関連するデータだけをロードするのかを決定できます。

関係解決の設定
: 関係検出レベルをデータ・ソース別に構成することができます。例えば、あるデータ・ソースについて関係解決をオフにしたり、その特定のデータ・ソース内での関係検出用の隔たり度合いを選択したりできます。

エンティティー・データベース

エンティティー・データベースは、アイデンティティー、エンティティーを保管するデータベースです。このデータベースには、関係、解決、およびアラートに使用されるデータも保管されます。

エンティティー・データベースには、すべての解決済みエンティティーおよびそれらの関係が永続的に保管されます。パイプラインで入力 UMF レコードが処理されるときに、新しいデータがエンティティー・データベース内の既存のデータと常に比較されます。したがって、エンティティー解決と関係検出は、以前のすべてのレコードのすべての属性が累積された複合エンティティーに対して実行されます。

ユーザー・インターフェース

IBM InfoSphere Identity Insight には、製品機能を操作するためのユーザー・インターフェースがいくつか備わっています。

構成コンソール

構成コンソールはタスク指向のインターフェースを提供し、Identity Insight を稼働させる上で最も不可欠なタスクの一部をより簡単に行えるよう支援します。

構成コンソールは、IBM WebSphere Liberty によってホストされます。

システム構成の管理

構成コンソールを使用して、ほとんどのシステム・パラメーターおよびオプションを、簡素化かつ能率化された一連のインターフェースで構成します。その後、コンソールによって変更内容が構成データベースに書き込まれます。構成データベースを直接変更することはサポートされていません。そのような変更を行うと、ほとんどの場合、製品が適切に機能しなくなります。

Visualizer

Visualizer は、アナリストや調査員がアラート、関係、エンティティー解決の結果を分析するために使用するグラフィカル・ユーザー・インターフェースです。

Visualizer は、組み込みバージョンの IBM WebSphere Application Server によってホストされます。Visualizer の構成は、構成コンソールから行うか、Visualizer の「ファイル **(File)**」メニューの「設定 **(Preferences)**」選択から行います。

Visualizer ユーザーは、以下のような各種の分析タスクを実行できます。

アラートの分析と後処理
: エンティティー解決処理によって生成されるアラートは、組織にとって関心のある関係やエンティティー解決を表します。通常はアナリストがアラートを確認し、アラート情報に基づいて、アクションが必要な場合には、実行するアクションを決定します。アラートには、ロール・アラート、属性アラート、およびイベント・アラートの 3 つのタイプがあります。

  Visualizer はアラートを表示し、アナリストに対し、アラートおよびアラートに含まれるエンティティーのテキスト・ビューとグラフィカル・ビューの両方を提供します。アナリストは詳細にドリルダウンしてから、アラートの後処理の状況を適切に設定できます。

属性アラート・ジェネレーターの作成と管理
: Visualizer を使用することで、アナリストは、属性アラート・ジェネレーター機能を介して永続検索を作成および管理でき、属性アラートを表示する方法と受け取る方法を管理できます。アナリストは、属性データに基づいて属性アラート・ジェネレーターを作成して、属性データに基づいてエンティティーに解決されたアイデンティティーを見つけることができます。また、アナリストは、属性アラート・ジェネレーターを作成して、エンティティー・データベースで特定のエンティティーを永続的に検索することもできます。

エンティティーの検索
: Visualizer ユーザーは、以下のようにいくつかの方法を使用して、さらに分析を行うためにエンティティーを検索することもできます。

  - 属性による検索
  - データ・ソース・アカウントによる検索
  - エンティティー ID による検索
  - 解決による検索 (最小解決スコアしきい値に基づいて、入力された基準がエンティティー・データベース内のアイデンティティーやエンティティーとどれくらい正確に一致しているか)

エンティティーおよび開示された関係の追加
: アナリストは、Visualizer を使用してエンティティー解決や関係検出のレコードを追加できます。単一アイデンティティー・レコードを追加することも、数千件のアイデンティティー・レコードを含んだ UMF ファイルをロードすることもできます。調達プログラムを通じてアイデンティティー・レコードが追加される場合と同様に、Visualizer から追加されたレコードも、エンティティー解決および関係検出のためにパイプラインによって処理されます。処理の結果はエンティティー・データベースに書き込まれ、アラートがある場合は Visualizer に公開されます。

アナリストは、アイデンティティー間にリンクがあることをわかっている場合、(アイデンティティーによって) エンティティー間の関係を開示することもできます。開示される関係の例として、求人の申込書にリストされている緊急時連絡先や身元保証人に基づいた関連エンティティーなどがあります。エンティティーにより、申込書にあるこれらの関係が開示されます。

レポートの生成と印刷
: Visualizer には、アナリストが Visualizer での作業を管理および追跡するのに役立てるために、アナリストが表示したり印刷したりできる複数のレポートも含まれています。

コマンド行インターフェース

この製品では、パイプラインを実行するためにコマンド行インターフェースを使用します。コマンド行でコマンドを発行することで、パイプラインを開始および停止します。

構成ユーティリティー

構成ユーティリティーを使用すると、インストール後にインストール設定の表示や変更を行ったり、パッチやホット・フィックスをインストールしたりすることができます。

以下のアプリケーションのパッチおよびホット・フィックスをインストールすることができます。

- 構成コンソール
- Visualizer
- Visualizer レポート
- Java™ Web Start
- Web サービス
- グラフ作成アプリケーション
- EntitySearcher アプリケーション
- 製品資料

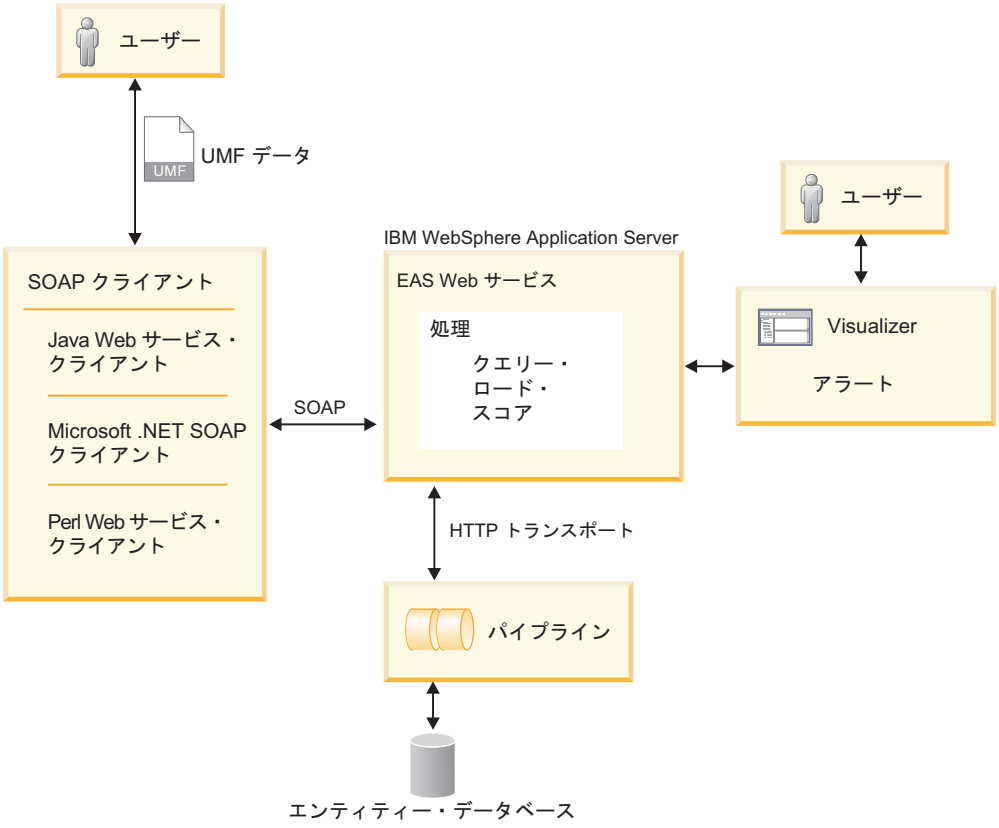
以下の設定を変更することもできます。

- 構成コンソール
- WebSphere 構成
- データベース接続
  - エンティティー・データベース接続の設定
  - アプリケーション・モニター・データベース接続の設定
  - 構成コンソール・データベース接続の設定
  - JDBC 設定

Web サービス

IBM InfoSphere Identity Insight は、外部アプリケーションを作成するために使用できる一連の Web サービスを提供しています。外部アプリケーションにより、パイプライン処理のため、またはエンティティー・データベース内のエンティティー

の検索のために Universal Message Format (UMF) データをロードできます。パイプラインの標準機能である双方向の HTTP (Hypertext Transfer Protocol) トランスポート・メソッドを使用します。



IBM InfoSphere Identity Insight の Web サービスでは、4 つの SOAP (Simple Object Access Protocol) メソッド (process、search、load、および score) が使用されます。本製品は SOAP バージョン 1.1 をサポートしています。

本製品には、Web サービスの初めての使用を支援する複数のコンポーネントが含まれます。

srd.wsdl

このファイルには、製品の Web サービスの Web サービス記述言語 (WSDL) 定義が含まれます。このファイルと任意の SOAP ツールキットまたはテクノロジーを使用することで Web サービスを開始できます。ファイルは、WebSphere Liberty を開始し、http://hostname:port/easws/resources/wsdl/srd.wsdl からファイルをロードすることで見つけることができます。

wsutil.jar

このファイルは、Web サービスのインストールおよび構成をテストするために提供されている Web サービス・テスト・クライアントです。このユーティリティーは、`ibm-home/easws` ディレクトリーにあります。

中核となる概念

IBM InfoSphere Identity を効果的に使用するには、エンティティー、アイデンティティー、属性などの主要概念を理解する必要があります。

エンティティー

エンティティーは、同じ個人、組織、場所、またはアイテムを表す 1 つ以上のアイデンティティーの集合です。エンティティーは、エンティティー・データベースに保管されます。

エンティティーは、人を表すものと考えられることが多いですが、企業や車両などを表す場合もあります。実際に、システムの拡張可能な構成を使用して、組織のデータをマップし、解決または関連付けが必要な任意のタイプのエンティティーを作成できます。

エンティティーは、多くの場合、いくつかの異なるソース・システムから取得されるアイデンティティーで構成されます。エンティティー解決は、どのアイデンティティーが実際には同じエンティティーであるかを判別し、複合エンティティーを作成します。複合エンティティーには、その複合エンティティーに関連付けられているすべてのアイデンティティーが含まれています。システムは、複合エンティティー内の各アイデンティティーに関連付けられたソースを識別して、レコードのフル属性情報を維持します。

組織の目標を満たすような方法で、エンティティーの解決と関連付けが行われるようにシステムを構成してください。

アイデンティティー

アイデンティティーは、個人、組織、場所、またはアイテムを表す、データ・ソースの属性の集合です。

エンティティー解決を通じて、アイデンティティーが解決され、個々のアイデンティティーから複合エンティティーが作成されます (アイデンティティーが複合エンティティーと一般的な属性を共有する場合)。

以前、アイデンティティーはアカウントと呼ばれる場合がありました。

属性

属性とは、個人、組織、場所、またはアイテムを説明する特性や特質です。一般的な属性としては、名前、住所、電話番号、クレジット・カード番号、納税者番号、免許証番号などの情報があります。

このシステムでは、次のような種類の属性がサポートされています。

名前　名前属性は、エンティティー・モデルと入力アイデンティティーによって定義されるとおりに、個人、組織、場所、またはアイテムの名前を定義します。通常、名前属性によって表すのは個人や企業ですが、用途を広げて、乗り物 (車、トラック、船、飛行機など) の名前や、グループの名前、あるいは企業がエンティティー・モデルの中で定義しているその他のどのようなタイプのエンティティーの名前でも表すことができます。

住所　住所属性は、アイデンティティーの場所を定義します。通常は、標準的な住所情報 (街区名や番地、ユニット番号や建物番号、市区町村、都道府県、国、郵便番号) を含んでいます。

番号　番号属性は、一般に番号で示されるデータ (クレジット・カード番号、電話番号、パスポート番号など) から成ります。ただし、番号といっても数字だけに限定されるわけではありません。これは、番号の多くに英数字が使用されるためです。

特性　特性属性は、他の種類の属性では表現されない、その他のアイデンティティーの特質や情報を定義します。特性属性を使用してシステムをカスタマイズすることで、エンティティー解決や関係検出で使用するアイデンティティーの特性を定義できます。一般的な特性のタイプとしては、生年月日や性別などがあります。

E メール

E メール属性は、インターネット E メール・アドレスを定義します。E メール・アドレスはユニークである傾向があります。ある研究によると、複数の名前を使用する人でも、1 つか 2 つの同じ E メール・アドレスを使用する傾向にあることが示されています。

Universal Message Format (UMF) では、さまざまな属性が UMF セグメントで表現されます。属性の種類 1 つ 1 つが、それぞれ独自の UMF セグメントです。

エンティティー解決

エンティティー解決とは、エンティティーを解決して関係を検出する処理です。認識、解決、関連付けという 3 つのフェーズの中で、パイプラインが入力アイデンティティー・レコードを処理しながら、エンティティー解決を実行します。

認識

エンティティー解決中、パイプラインで、入力アイデンティティー・データを検証、最適化、および拡張することでデータを認識する必要があります。パイプライン処理のこの認識フェーズ中、パイプラインで、データ値がクレンジングおよび標準化され、さらにエンティティー・データベースの整合性を保持するためにデータに対してデータ品質チェックが実行されます。

データ品質管理 (DQM)

データ品質管理 (DQM) は、必須値、有効なデータ・タイプ、および有効なコードがデータにあるかをチェックするパイプライン処理です。データを修正するように DQM を構成することもできます。このデータ修正では、デフォルト値を渡したり、数値および日付のフォーマットを設定したり、新しいコードを追加したりする処理が行われます。

データ品質管理は、名前クレンジングと名前標準化、住所クレンジングと住所標準化とともに、データ品質を最適化および向上させることを目的としています。データ品質準備により、結果として解決されたエンティティーおよび検出された関係の信頼性が向上するため、このデータ品質準備は、エンティティー解決の必要不可欠なステップです。

システムにロードされたデータにデータ品質管理を適用するには、データ品質管理ルール (DQM ルール) を構成します。DQM ルールにより、入力アイデンティティー・データ値に対して各種の修復機能、クリーンアップ機能、および標準化機能を実行できます (数値の適切なフォーマット設定、誤記エラーまたは文字の入れ替わりエラーの特定および修正、アイデンティティーを隠蔽しようとする意図で導入された意図的な誤りの特定および修正など)。

この製品には、UMF セグメントごとに、その UMF セグメントの最も一般的なデータ品質問題を処理するいくつかの DQM ルールが事前に構成されています。また、必要に応じて追加の DQM ルールを構成できます。ただし、追加ルールを構成するには、データの元の品質、およびアイデンティティー・データを UMF に変換するために使用された ETL (抽出、変換、およびロード) 処理について十分理解していることが前提となります。どの程度のデータ拡張が必要かを判断した後で、データ品質の最適化がさらに必要な各種アイデンティティー・データに適用する正しい DQM ルール、関数、および値を選択できます。

DQM ルールの使用例

例えば、システムの日付形式が DD/MM/YYYY であるとします。しかし、いくつかのデータ・ソースでは、日付値が MM-DD-YYYY という形式になっています。DQM ルール 204 を <NUMBER> UMF セグメントに追加して、MM-DD-YYYY という形式のすべての入力日付が DD/MM/YYYY という日付形式に修正されるよう構成できます。

名前クレンジングと名前標準化:

パイプライン処理中、最適なエンティティー解決処理に向けてアイデンティティー・レコードを準備するために、名前がクレンジングおよび標準化されます。

パイプライン処理では、現在の使用、将来の使用、および履歴目的の使用のために、エンティティーに関する最も正確な名前情報が提供されます。新しい、または変更されたアイデンティティーの名前データがシステムに入力されると、基本名と既知の派生名のリストが含まれている、製品の名前標準化ディクショナリーと比較され、基本名が特定されます。基本名が特定されると、システムで、入力アイデンティティー・レコードに対して基本名と元の名前の両方が保持されます。

次の表に、同じ基本名について有効な派生名の例を示します (名前の各種スペルを含む)。例は 2 つあります。右側が基本名で、左側はすべて、その基本名の派生名です。

表 1. 基本名 *Richard* および *Mohammad* の有効な派生名の例

派生名	基本名
Dick、Dickie、Ricardo Rich、Richie、Rick Rickey、Ricki、Rickie Ricky、Rikki、Ritchie	Richard
Mohamad、Mohammad Mohamed、Mohammed	Mohammad

名前クレンジングと名前標準化処理では、必要に応じて、ミススペルの修正も行われます。その場合も、本システムでは、元のスペルと修正したスペルの両方がレコードの一部として保持されます。他のほとんどのシステム (ETL ツール、データベース・マーケティング・ツールなど) では、これは行われません。

名前クレンジングと名前標準化は、エンティティー解決の信頼度を向上させる重要なステップです。平均的な人は、公的な目的および消費者としての用途に 5 種類もの名前を使用するため、この処理は特に重要です。

住所クレンジングと住所標準化:

住所クレンジングと住所標準化は、住所情報を正規化および標準化するパイプライン処理です。この処理では、起こりうるエラーおよび文字の入れ替わりを修正し、最適なエンティティー解決処理のためにアイデンティティー・レコードを準備します。

住所クレンジング処理の一部として、パイプラインで住所情報が解析および標準化されます。例えば、Street が St に、123-A Main St が 123 Main St Apt A に標準化されます。

また、このパイプライン処理では、IBM InfoSphere QualityStage 製品または別の住所クレンジング製品 (Group 1 Software CODE-1 製品など) で提供されているグローバル住所データベースおよび標準化ソフトウェアと照合して、新しい情報または変更された情報の確認も行います。選択した住所クレンジング製品により、住所情報の形式が正しいかどうか判別され、検出されたミススペル (番地名のミススペルなど) が修正され、さらに欠落している情報または正しくない情報が修正されます (郵便番号および住所に一致するように市名を更新するなど)。

次の表に、住所をクレンジングおよび標準化して、元の住所から修正および標準化された住所にする例を示します。

表 2. 元の住所と標準化された住所の 2 つを比較するための例

元の住所	標準化された住所
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

住所クレンジングと住所標準化のパイプライン処理では、後のエンティティー解決および関係検出の信頼度を向上させるために、元の住所と修正および拡張された住所の両方が保持されます。また、この情報を保持することで、より適切なヒストリカル情報が提供されます。

データ品質チェック:

アイデンティティー・データが処理のためにシステムに入力されると、エンティティー・データベースの整合性を維持するために、パイプラインでデータの品質がチ

ェックされます。各入力アイデンティティー・レコードについて、Universal Message Format (UMF) 構造が適切か、必須値があるか、データ・タイプは有効か、およびデータ・ソース・コードの構成が検査されます。

この処理でデータ品質がチェックされるときに、問題の修正が試行されます (問題の修正が可能で、修正を行うようにシステムが構成されている場合)。データ品質の問題を修正するかどうかをしsが判断するときに、構成済みのデータ品質管理 (DQM) ルールが使用されます。DQM ルールでは、入力アイデンティティー・レコードで、どのようなデータ品質不良であればシステムで修正できるか、また、どのようなデータ品質不良であれば (修正せずに) そのままにしてレコードを処理できるかを定義します。

特定のデータ・ソースのデータ品質を確認するために、ロード要約レポートを表示または印刷できます。「品質要約 (Quality summary)」セクションを使用すると、そのデータ・ソースの全体的なデータ品質、またはそのデータ・ソースからロードされたアイデンティティー・レコードの特定のセットの全体的なデータ品質を理解することができます。この情報を使用して、特定のデータ・ソースの ETL 処理を必要に応じて調整できます。

標準ロギングおよびエラー処理では、すべてのデータ品質エラーと修正、およびシステムが修正できなかった、または修正しなかったエラーが記録されます。パイプライン処理で修正されなかったデータ品質エラーを確認するために、システム・ログを頻繁にチェックしてください。ほとんどの場合、データ品質エラーを修正し、その後、修正したアイデンティティー・レコードを、エンティティー解決処理のためにパイプラインに再ロードする必要があります。

データ品質チェックの例

システムは、新しいコードとして認識されないコードを自動的に追加できます (この処理を構成している場合)。UMF_EXCEPT ログには、システムによって追加された新しいコードや、システムがコードを認識せず、それを新しいコードとして追加するように構成されていなかったために拒否されて処理されなかったレコードの結果が示されます。

次の表に、システムでまだ構成されていない、入力レコードのコードの例を 2 つ示します。

表 3. システムで構成されていない 2 つのコードとシステム処理の結果の例

コード	品質チェック	**UMF_EXCEPT** ログ
Addr_Type x	新しいコードは追加される	ログに書き込む
Num_Type xxx	新しいコードは拒否される	ログに書き込む

- 1 番目の例では、システムは、新しい住所タイプ・コードを自動的に追加するように構成されています。
- 2 番目の例では、システムは、新しいコードを自動的に追加するように構成されておらず、エンティティー解決のためにレコードを処理するようにも構成されていません。

どちらの場合も、システムは、適切なログ・ファイルにアクションを記録します。

解決

エンティティー解決中、パイプラインによりアイデンティティーがエンティティーに解決されます。アイデンティティー・レコードのデータ値がクレンジング、標準化、または拡張された後、パイプラインで高度な検索アルゴリズムを使用して、エンティティー・データベース内の既存エンティティーと入力アイデンティティー・レコードのデータ値が比較され、それらが同じエンティティーかどうか判別されます。

エンティティーの解決には、次のフェーズがあります。

候補リストの生成
: システムで、入力アイデンティティー・レコードの情報を使用して、エンティティー・データベースに既にあるエンティティーとの突き合わせが行われ、潜在的なエンティティー解決候補のリストが作成されます。各候補は十分な属性値を共有しており、エンティティー解決のために候補の評価が続行されます。候補リストを生成するためにシステムで使用される基準を構成できます。

エンティティー解決の実行
: 候補リストが生成された後、システムで、候補リストの各エンティティーに対して解決ルールが適用され、解決スコアを計算するスコアリング方式を使用して、入力アイデンティティーと既存のエンティティーを解決する必要があるかどうかが判別されます。解決ルールを構成し、解決スコアのしきい値を設定することで、入力アイデンティティーと候補エンティティーを 1 つのエンティティーに解決するために、属性値がどの程度近似する必要があるかを指定できます。

候補リスト

候補リストとは、入力アイデンティティー・レコードと一致する可能性のあるエンティティーのリストです。候補リストは、候補ビルダー構成に指定されている属性に基づいて、入力アイデンティティーと属性を共有しているエンティティーを取得することによって作成されます。

エンティティー解決処理では、エンティティー解決および関係解決用の候補リスト上にあるエンティティーのみが使用されます。

エンティティー解決および関係検出は属性に基づいて判別されるため、データ・ソース内の属性を慎重に検討して、最有力候補を作り出す属性がどれであるかを決定することが推奨されます。

候補リストが生成されると、エンティティー解決処理は、構成済みの解決ルールを使用し、候補リスト上の最初の候補と照らして入力アイデンティティーを比較します。システムは解決ルールを順番に使用して、入力アイデンティティーの属性が候補エンティティーの属性とどの程度正確に一致しているかを表す解決スコアを計算します。入力アイデンティティーの属性が当該ルールの解決スコアを満たしているか、または超えている場合、その入力アイデンティティー・レコードが候補エンティティーに解決されます。

解決スコアが当該解決ルールに設定されている解決スコアを満たしていない、または超えていない場合、システムは次の解決ルールに進みます。これが、入力アイデ

ンティティー・レコードが候補エンティティーに解決されるまで、またはすべての解決ルールが使い尽くされるまで行われます。

入力アイデンティティー・レコードが既存のエンティティーに解決されない場合、システムはこのレコードを新規エンティティーとして解決し、この新規エンティティーをエンティティー・データベースに保管します。

解決ルール

解決ルールとは、比較対象のエンティティー (同じエンティティーでも同じエンティティーでなくても) をどのように解決して、どのように関連付けるか (それらのエンティティーが同じエンティティーに解決されない場合、属性をいくつ共有するか) を定義するためにシステムが使用する基準のセットです。

解決ルールを定義するときは、次のように、合計解決スコアを導くしきい値を指定する必要があります。合計解決スコアによって、入力アイデンティティーが既存のエンティティーに解決されるかどうかが決まります。

- 候補しきい値により、アイデンティティーやエンティティーが 1 つの複合エンティティーに解決されるかどうかを判別するための、比較対象とする属性データ値を指定します。このしきい値は、解決ルールを満たすために入力アイデンティティーと既存のエンティティーの間で特定の属性値が一致する必要がある最小スコアです。
- 確定/否定しきい値には、否定の使用を有効にした場合に、一致する属性や競合する属性のデータ値に対してどの程度のスコアリングの重みづけ (正または負) を与えるかを指定します。

また、同じ属性の競合する値が、どのように解決スコアに影響するかを指定することもできます。これらの競合する値は否定と呼ばれます。属性値に何らかの競合 (否定) がある場合はルールを満たしていない、ということを指定する解決ルールを構成できます。また、指定したしきい値スコアを 1 つ以上満たしていない比較スコアに基づいて、自動否定が作成されるように、解決ルールのしきい値を調整することもできます。設定したしきい値スコアが高くなるほど、解決ルールを満たすためにはより正確に一致していなければならないことになります。

再解決

2 つのエンティティーが同じエンティティーとして解決され、複合エンティティー・レコードが作成される場合、エンティティー解決処理中に再解決処理が実行されます。エンティティー解決で、新しい複合エンティティー・レコードを使用して処理がもう一度最初から開始され、新しい複合エンティティーをエンティティー・データベース内の他のいずれかのエンティティーに解決できるかどうか確認されます。

新しい入力エンティティーと同様に、エンティティー解決処理で、エンティティー・データベースからエンティティーの候補リストの生成が試行されます。候補リストを生成できる場合、エンティティー解決処理でエンティティー解決が開始され、リストの各候補と新しい複合エンティティーが比較されます。候補リストを生成できない場合、エンティティー解決処理に続いて関係検出処理が実行されます。

未解決

未解決処理は、エンティティー解決処理の一部として実行されます。入力アイデンティティーの属性値によって、ある複合エンティティーが実際には 2 つのエンティティーから構成されていることを示す新しい情報が提供された場合、その複合エンティティー・レコードを 2 つのエンティティーに分割するというものです。各レコードに関連付けられているデータ・ソースにより、システムはどのレコードがどのエンティティーに属しているか認識します。未解決処理が完了すると、システムで再解決処理が開始されます。

未解決の例

以前に、このシステムでは、住所が 1234 Main Street、Anytown、USA、電話番号が (201) 555-2244、E メール・アドレスが jrsmith@internetprovider.com の Will Smith の入力アイデンティティー・レコードを、その同じ住所に住み、同じ電話番号を使用する William Smith, Sr. に解決したことがありました。

ここで、E メール・アドレスが jrsmith@internetprovider.com で、クレジット・カード番号が 123-54-9999 の Will Smith, Jr. の新しい入力アイデンティティー・レコードを処理します。

新しい情報である Jr. およびクレジット・カード番号に基づき、システムで、William Smith, Sr. の複合エンティティー・レコードを、William Smith, Sr. と William Smith, Jr. とで、未解決とする必要があることを決定できます。1 つのエンティティーが 2 つのエンティティーに分割された後、システムでは再解決処理が開始されて、新しい情報に基づき、データベース内の他のエンティティーが William Smith, Jr に解決されるかどうかがチェックされます。

関連付け

エンティティー解決中、パイプラインにより関係検出処理も実行され、これにより、アイデンティティーとエンティティーの間の関係が検出され、関心のある関係に関するアラートが生成されます。

システムで、ロールを使用してエンティティー間の関係が検出され、確立されます。ロールとは、アイデンティティーの分類であり、そのアイデンティティーの重要点または目的を定義します。システムで、ロールを定義し、データ・ソースごとにアイデンティティーにロールを割り当てるか、元のデータ・ソース・データを Universal Message Format (UMF) に変換する一部としてアイデンティティーにロールを割り当てます。

パイプラインで、エンティティー解決のために入力アイデンティティーが処理され、アイデンティティーが既存のエンティティーに解決されると、2 つのレコードが 0 次の関係 (入力アイデンティティーとエンティティーが同じ) を持つことになります。ただし、エンティティー解決処理は、システムの構成方法によっては、0 次の関係以上に進む場合があります。

パイプラインにより、エンティティー解決の解決フェーズですべての可能性が検証された後、関係検出処理で、候補リストに残るエンティティー、または入力アイデンティティーに解決されなかったエンティティーが評価され、それらのエンティティーの間に関係が存在するかどうか確認されます。通常、少なくとも 1 つの属性に

ついて、候補リストにあるエンティティーが 1 次の隔たり度合いで入力アイデンティティーにリンクされます。つまり、両方のエンティティーが、少なくとも 1 つの属性について同じ属性データ値を共有します。これが、エンティティーが候補リストにある理由です。

処理により関係が検出された後、システムで、アイデンティティーとエンティティーの間の割り当て済みロールと構成済みのロール・アラート・ルールが比較されます。アイデンティティーおよびエンティティーに割り当てられているロールがルールの基準を満たすことが判明した場合、関心のある関係が検出されたことを示すアラートがシステムで生成されます。関係は、システムおよびロール・アラート・ルールの構成方法に基づき、0 次、1 次、またはそれ以上の次数になる場合があります。

関係

関係は、2 つ以上のエンティティー間のつながりです。関係は、エンティティー解決処理の最後に、2 つのエンティティーがいくつかのデータ属性値を共有している場合に検出されます。

関係は、システムによってディスカバーされたリンク、アナリストによって開示されたリンク、またはその両方に基づくことが可能です。ただし、すべての関係が、さらに詳細な分析または調査を促すためにアラートの生成を必要とするほど、価値のあるものとは限りません。エンティティーに割り当てられたロールのどの組み合わせでアラートを生成する必要があるかを指定するロール・アラート・ルールを構成することで、関心のある関係を定義します。

関係の例

エンティティー解決中に検出できる関係の例を以下に示します。

- 顧客が取引先でもある。組織の方針および手順に基づき、これを関心のある関係と見なす場合があります。
- 従業員が顧客を知っている。組織の方針および手順でこのような関係性を禁止している場合は例外であり、また、従業員と顧客が共有するデータにもよりますが、これは関心のある関係とは見なされない可能性があります。
- 顧客が別の顧客を知っている。いずれかの顧客が会社にとって高い価値がある場合、その顧客が知っている人物を知ることは、顧客ネットワークを使用してそのネットワーク内で販売を行うための効果的な方法となる可能性があります。

隔たり度合いの概要**:**

隔たり度合い機能により、IBM Relationship Resolution の関係マッチング能力が拡張されます。

IBM InfoSphere Identity Insight のデフォルトの動作では、関心の高い関係が特定され、エンティティーに解決されたインバウンド・アイデンティティーから 1 次の隔たりにあるエンティティーが照合されます。隔たり度合い機能を有効化すると、これらの機能が、エンティティーに解決されたインバウンド・アイデンティティーからほぼ無限の範囲のユーザー定義隔たり度合いに拡張されます。

隔たり度合い機能では、隔たり構成、ロール、ロール・アラート・ルール、および関係スコアを使用して、非常に大きいデータ・セットに対してリアルタイムのリンク分析を行います。

インバウンド・アイデンティティーがエンティティーに解決されると、IBM InfoSphere Identity Insight が検出した 1 次の関係を使用してエンティティー・グラフが作成されます。エンティティー・グラフでは、この 1 次の関係を使用して、インバウンド・アイデンティティーの解決先となったエンティティーから派生する複数次の関係チェーンが作成されます。これで、インバウンド・アイデンティティーが解決された先のエンティティーから派生した 2 つの複数次の関係チェーンをリンクすることで、ロール・アラート・チェーンを作成できます。その後、このロール・アラート・チェーンを使用して、複数次の関係の各チェーンの末端まで包括的にエンティティー間の関係を見つけることができます。

隔たり度合いにより、2 つのエンティティーを結ぶすべてのパスを評価し、関係報告において最も強いパスの強度を使用することにより、作業が軽減されます。隔たり度合いは、インバウンド・アイデンティティーの解決先となったエンティティーごとに、構成済みロール・アラート・ルール 1 つにつきロール・アラートを 1 つ報告するように構成できます。

隔たり度合いの構成は、コンソールの「システム構成」タブで「隔たり度合い (Degrees of Separation)」の値を使用して設定できます。

インパーソナル認識**:**

インパーソナル認識は、従来の関係解決処理を拡張してインパーソナル関係を検出および分析する製品機能です。関係検出処理では、エンティティーに関連付けられた属性値に基づいて、エンティティー間の関係を見つけます。ときには、アクティビティーまたはその他のインパーソナル ID に基づいてエンティティー間の関係を見つけることが重要な場合があります。こうした、アクティビティーまたはその他のインパーソナル ID に基づいたエンティティー間の関係を、インパーソナル 関係と呼び、人を関連付けるアクティビティーやインパーソナル ID を、関連事実 と呼びます。

インパーソナル関係は常に 2 次以上の隔たりに存在します。これは、関連事実が、それ自体で 1 つのエンティティーであるからです。そのため、インパーソナル認識を有効にしてインパーソナル関係を検出するには、隔たり度合い機能を使用するようにデータ・ソースを構成します。これで、エンティティー解決および関係解決が拡張され、2 次より大きな隔たりにある関係が検出されます。

例えば、電話トランザクションには電話番号に関するデータ (発信者の電話番号と受信者の電話番号の両方) が含まれています。ある個人が別の個人に電話をかけたとしても、その電話トランザクションだけでは、それらの個人の属性として共通のデータを関連付けることはできません。多くの場合、関連事実 (電話呼び出し) のほうが、関連エンティティー (電話で話していたその 2 人の人) に関する他のどのような情報よりも前に把握されます。これらの関連事実を 1 人の個人の属性として関連付けることはできないため、人ではないが人に関連する、別個のエンティティーとして表す必要があります。しかしながらインパーソナル認識では、電話の結果として、2 人の個人の間に関係が存在することを認識します。

UMF にはエンティティー・タイプ機能が組み込まれているため、これを使用して、関連事実をエンティティー・タイプとして定義することができます。この機能を使用すると、関連事実はエンティティー・データベース内で別個のエンティティーとなり、Person エンティティー間の関係検出に使用できるようになります。新規エンティティー・タイプを構成し、UMF 内で適切なエンティティー・タイプを指定し、新規解決構成を作成することで、これらの関連事実を使用してエンティティー間のインパーソナル関係および競合を自動的に検出することができます。

たとえ解決ルールで許可されている場合であっても、あるいはデータが解決をサポートしていても、異なるエンティティー・タイプのエンティティーが相互解決されることは決してありません。つまり、エンティティー・タイプ Phone call がエンティティー・タイプ Person に解決されることはありません。

Analyst ツールキットは、インパーソナル関係および関連付けられたあらゆるアラートを、パーソナル関係および関連付けられたアラートの場合とまったく同様に、グラフ化し、レポート化します。

インパーソナル認識の例

例えば、通話によってインパーソナル関係を見つける場合、「通話 (Phone call)」という新規エンティティー・タイプを作成し、調達ノードを調整して、エンティティー・タイプが「通話 *(Phone call)*」 である各通話レコードに正しくタグを付けます。

通話レコードがシステムに取り込まれると、標準のエンティティー解決および関係解決が Phone call エンティティーと発呼側エンティティー (Person) 間の 1 次の関係を検出します。電話を受けた個人と Phone call エンティティー間の 1 次の関係も検出されます。ただ、それだけではシステムは個人間の関係は検出しません。

しかし、隔たり度合いが構成されていると、引き続き分析されて、発信者と着信者の 2 次のインパーソナル関係が検出されます。インパーソナル関係は、Phone call エンティティー・タイプの属性である電話番号に基づいて存在します。その後、隔たり度合いによってインパーソナル関係が分析され、競合が見つかった場合はアラートが生成されます。

ロール

ロールとは、アイデンティティーの分類であり、そのアイデンティティーの重要点または目的を定義します。アイデンティティーには、1 つ以上のロールを関連付けることができます。アイデンティティーはエンティティーに解決されるため、エンティティーは、関連付けられたロールをすべて継承します。

ロールを使用してロール・アラート・ルールを構成します。このルールでは、関心のある関係を定義し、アラートを生成します。

次の 2 つの方法のいずれかで、すべてのアイデンティティーにロールを割り当てます。

入力データ・ソースによって
: 新規データ・ソースを構成するときに、そのデータ・ソースにロールを関連付けます。これにより、そのデータ・ソース・コードを含んでいるすべてのアイデンティティーに、そのロールが割り当てられます。

UMF によって
: データ・ソースを Universal Message Format (UMF) に変換するとき、<SEP_ROLES> UMF セグメントと <ROLE_CODE> UMF タグを使用して、UMF レコードの一部として、ロールを直接割り当てることができます。UMF によって構成した場合は、DQM ルールと参照表を追加する必要があります。

有益なロールの例としては、従業員、ベンダー、顧客、監視リストなどがあります。

UMF を使用したロール割り当ての例

UMF を使用して Employee (従業員) のロールをアイデンティティー・レコードに割り当てるには、アイデンティティー・レコードに対して、以下のように <SEP_ROLES> UMF セグメントおよび <ROLE_CODE> UMF タグを入力します。

```
<SEP_ROLES>
  <ROLE_CODE>Employee</ROLE_CODE>
</SEP_ROLES>
```

アラート

アラートは、イベントが発生したことを示す、メッセージまたはその他の通知です。

アラートは、次の 2 つの方法のいずれかで生成されます。

- 属性アラート: エンティティーが指定の属性集合に一致したときに、生成されます。
- ロール・アラート: 1 つのエンティティー、または関係を通じてリンクされた複数のエンティティーが、ユーザーが関心のある または競合 として定義したロールを共有しているときに、生成されます。

どのようなアラートが組織の目標を満たすのかを明確にすることが重要です。最初に、エンティティー間のどの関係が、組織にとって関心があるのかを明確にしてください。関係は、ユーザーが構成したロールに基づきます。ロールは、ソース・システムにより入力データ・レコードに割り当てられます。2 つのエンティティーが多くの属性データ値を共有していながらも、同じエンティティーとして解決されない場合、それらのエンティティーは関係を築いています。組織用に構成するロール・アラート・ルールでは、どのエンティティー・ロールが、アナリストによる詳細調査が必要になる関係を形成しているかを明確に定義する必要があります。

アラートの例

組織でのアラート生成の対象となるような、関心のある関係の例を以下に示します。

- 組織で雇用した人員のいずれかが、組織に支払対象の商品またはサービスを提供する取引先でもある。
- いずれかの顧客の住所および名前が、政府の監視リストにリストされている個人の住所および名前と類似している。

- 組織で転倒レポートを提出した 2 人の人物の名前と住所が類似しており、電話番号も共通である。

属性アラート:

属性アラートは、属性アラート・ジェネレーターによって生成されるアラートです。属性アラート・ジェネレーターは、エンティティー・データベース内で特定の属性またはアイデンティティーを検索する永続システム・クエリーを作成します。エンティティーの属性が属性アラート・ジェネレーターの基準に一致するたびに、システムによって属性アラートが作成されます。

Visualizer ユーザーは、ユーザー個人用の属性アラート・ジェネレーターを独自に作成します。特定の属性のセットに一致する特定のアイデンティティーまたは任意のアイデンティティーかエンティティーを探している場合、指定された有効期限まで一致を検索する、ユーザー個人用の属性アラート・ジェネレーターを独自に作成できます。

通知が必要になる可能性があるエンティティー属性の例を以下に示します。

- 名前とユニーク番号 (クレジット・カード番号など)
- 名前と電話番号
- 住所
- 名前と非ユニーク番号

属性アラート・ジェネレーターの構成と表示には、Visualizer を使用します。作成した属性アラート・ジェネレーターは、作成した本人のみが使用できます。

住所属性アラートの例

「675 Hickory Street Las Vegas, NV」という住所を監視しているとします。エンティティー・データベースに追加される入力アイデンティティー・レコードにその住所が関連づけられている場合に属性アラートを作成するように、属性アラート・ジェネレーターを構成できます。

ロール・アラート:

ロール・アラートは、関係を通してリンクされている 1 つのエンティティーまたは 2 つのエンティティーが、構成されているロール・アラート・ルールを満たすか上回ったことを識別します。ロール・アラートは、構成されているロールとロール・アラート・ルールに基づいています。それらは、警告または問題 (「顧客が問題人物を知っている」など) を示していることもあれば、単純に関心のある関係 (「顧客が従業員を知っている」など) を示していることもあります。

単一エンティティー内に存在すべきでないロールまたは 1 つ以上のエンティティー間でリンクされてはならないロールを識別するロール・アラート・ルールを構成することで、関心のある 関係または 競合 とする関係を定義します。構成コンソールを使用して、ロール・アラートのフィルターを構成します。このフィルターで、新しい情報 (新規アイデンティティーまたは新規データ・ソース・コードなど) がある場合に、システムが再度アラートを発行するかどうかを決定します。

エンティティー解決時、パイプラインによって、入力アイデンティティーと候補リストにあるエンティティーの間の関係が評価されます。システムは、入力アイデンティティーと候補エンティティーの間に関係が存在するかどうかを判別してから、割り当てられているロールが構成済みのロール・アラート・ルールを満たしているかどうかを評価します。満たしている場合、システムはロール・アラートを生成します。

ロール・アラートが識別するエンティティー・データはロール・アラート作成時のものです。ロール・アラートの詳細画面には、ロール・アラートが作成されたときのエンティティー・データが当時のまま示されます。エンティティー・データは時間とともに変化するため、エンティティー・レジュメには最新のエンティティー・データが含まれます。特定のエンティティーの現在のデータを表示する必要がある場合は、エンティティー・レジュメを表示してください。

ロール・アラートは Analyst ツールキットのコンポーネント (Cognos Report、i2 用の Identity Insight プラグイン、および Identity Insight エクスプローラー) で表示および処理できます。

ロール・アラート・ルール:

ロール・アラート・ルールは、単一のエンティティーには存在できないような、または複数のエンティティー間ではリンクできないような 1 つ以上のロールを識別する、ユーザーが定義するルールです。エンティティー解決中、ロール・アラート・ルールの基準が満たされると、システムによりロール・アラートが生成されます。

ほとんどのロール・アラート・ルールでは、ロールが競合する場合を指定しますが、ロールを割り当てられたエンティティーが、同じロールを割り当てられた別のエンティティーを知っている場合のロール・アラート・ルールも定義できます。例えば、顧客同士がお互いに知っていることを把握することが役立つ可能性があります。この場合、エンティティー・データベースで一方の顧客エンティティーが他方の顧客エンティティーに関連する場合に常にロール・アラートを生成するロール・アラート・ルール (顧客が顧客を知っている) を定義します。

エンティティーは複数のレコード (通常、各種データ・ソースからのレコード) で構成されており、ロールは、通常、データ・ソースにより割り当てられるため、1 つのエンティティーに複数のロールが割り当てられる場合があります。したがって、入力データに基づき、1 つのエンティティーに顧客ロールと問題人物ロールの両方が割り当てられた場合に常にロール・アラートを生成するロール・アラート・ルールを定義することもできます。

注: システムが多数のロールを使用するように構成されている場合、ロール・アラート・ルールの数も飛躍的に増えますので注意してください。

システムで、ロール・アラート・ルールに違反する各関係が検出されても、デフォルトでは、エンティティーごとに 1 つのロール・アラートのみ報告されます。例えば、システムで、従業員ロールが割り当てられているエンティティーが 2 種類の取引先エンティティーに関連することが検出され、従業員が取引先を知っている場合にロール・アラートを生成するようにロール・アラート・ルールが構成されている場合、両方の競合が検出され、データベースに書き込まれますが、デフォルトでは 1 つのロール・アラートのみ報告されます。

ロール・アラート・ルールを構成する場合、新しいアイデンティティーまたは新しいデータ・ソース・コードが、以前生成されたアラートに関連する既存のエンティティーに導入された場合にシステムで再アラート (新しいアラート) を生成するかどうか制御するアラート・フィルターも指定できます。

ロール・アラートの無効化:

エンティティーおよび関係の解決を通じてデータが処理されると、時間の経過とともにエンティティーおよびエンティティー間の関係が変化します。これらの変化が原因で、新しいデータおよび既存のデータの永続的な分析に基づき、ロール・アラートが無効になる場合があります。InfoSphere Identity Insight のロール・アラート無効化機能によって最新のコンテキストがアナリストに提供されるため、アナリストは無効になった競合の調査に時間を費やすことはありません。

ロール・アラートの無効化により、保留状態のままになっている関係ベースのロール・アラートが削除されます。通常、保留状態のアラートは、アナリストによってまだ表示および処理されていません。ロール・アラートが別の状態 (完了済み、割り当て済みなど) の場合、データでそのロール・アラートの無効化がサポートされていても、アラートは無効化されません。アラートには 1 つの状況しか割り当てることができないため、アラートが既に「割り当て済み」または「完了済み」状態の場合、そのアラートは無効化されません。

アイデンティティーがエンティティーから削除された場合、または未解決の場合、0 次で発生するロール・アラートも無効化されます。

ロール・アラート無効化の動作方法

関係ベースのロール・アラートは、次のいくつかの理由により無効になる場合があります。

- エンティティーで、再解決処理または未解決処理の一部としてそのエンティティー ID が変更された場合、関係が取り除かれたり、新しいエンティティー ID に移行したりする場合があります。
- 新しいデータに基づき、単一のエンティティーが 2 つの別個のエンティティーになる場合、新しいエンティティーそれぞれに新しいエンティティー ID が割り当てられます。フル属性情報を通じて、新しいエンティティーに属するすべてのデータが古いエンティティーから削除され、その新しいエンティティーに追加されます (関係ベースのロール・アラートを作成するロールを含む)。
- エンティティー・データベースからデータが削除されると、エンティティー全体または関係の主要コンポーネントが削除される場合があり、それが原因でロール・アラートが無効になります。
- データが汎用としてマークされると、関係の検出で使用されるそのデータの有効性は減少するか、またはなくなります。関係が削除されると、その関係に基づくすべてのロール・アラートは無効になります。

代替ロール・アラート

ロール・アラートが無効化されると、常にパイプラインで関係パスに沿って各競合が自動的に再評価され、代わりの関係ベースの競合をサポートするデータが検索されます。

関係パス とは、あるエンティティーを別のエンティティーにリンクする、エンティティーと属性のチェーンです。隔たり度合いの構成により、関係パスの長さが決まります。隔たり構成は、構成コンソールで設定します。

スコアリング

エンティティー解決中、システムにより、入力アイデンティティーの属性が既存エンティティーの属性にどの程度近似しているか計算されます。この計算分析の結果は、システムがアイデンティティーをエンティティーに解決するため、およびエンティティー間の関係を検出するために使用するスコアです。

解決スコア

解決スコアとは、エンティティー解決中に確定および否定処理の結果として割り当てられる値であり、比較対象のアイデンティティーが同じエンティティーを表す可能性を定義します。このスコアは、ユーザー定義であり、新しいアイデンティティーを既存のエンティティーに解決するために使用されます。

パイプラインで、エンティティー解決のために入力アイデンティティーが処理されるとき、入力アイデンティティーの属性と、候補リストの各エンティティーの属性の共有属性値が比較されます。比較の一部として、属性値がどの程度近似しているかを表すスコアの計算が行われます。その後、これらのスコアは、各解決ルールの構成済みしきい値および解決スコアと比較されます。エンティティー解決処理で、確定および否定処理を使用して誤検出が回避された後、システムで、入力アイデンティティーと、候補リストのエンティティーの両方に対して基本解決スコアが作成されます。

詳細な確定/否定のために 1 つ以上の属性が使用されるように構成されている場合、処理によりそれらの属性が評価されます。この結果は、入力アイデンティティーおよび候補エンティティーの基本解決スコアに影響します。属性値が一致する場合、構成済みのポイント数を加算することで、解決スコアに正の影響を与えることができます。属性値が一致しない場合、構成済みのポイント数を減算することで、関係スコアに負の影響を与えることができます。確定または否定のために属性を使用するように構成する場合、ポイント数の増減を指定することで、基本解決スコアを調整します。

次に、システムで、各解決ルールに対して入力アイデンティティーと候補エンティティーの結果の解決スコアが比較されます。解決スコアが、解決ルールの構成済みの解決信頼度スコアを満たすか、超過する場合、システムで入力アイデンティティーが候補エンティティーに解決され、エンティティー・データベースに 1 つの複合エンティティーが作成されます。

関係スコア

関係スコアは、解決ルール適用の結果としてエンティティー解決中に割り当てられる値であり、比較対象の 2 つのアイデンティティーがどの程度近い関係にあるかを定義します。このスコアは、ユーザー定義であり、エンティティーを関連付けるために使用されます。

エンティティー解決中、パイプラインで、候補リストの残りのリストと入力アイデンティティー (エンティティーに解決されない場合がある) が比較されます。これら

の候補エンティティーが入力アイデンティティーに解決されない間は、関係について候補エンティティーが引き続き評価されます。

関係検出処理中、パイプラインで、入力アイデンティティーと候補リストのエンティティーの間で共有される属性データ値ごとに関係スコアが計算され (最初のエンティティーから開始される)、関係が特定されます。

- 関係スコアが、(隔たり度合いにより) 関係に対して構成されている基準を満たす場合、システムは 2 つのエンティティーが関連していると見なします。この関係は、両方の複合エンティティー・レコードに書き込まれます。システムで、構成済みのロール・アラート・ルールがチェックされ、その関係が関心のある関係かどうかが判別されます。関心のある関係である場合、システムによりアラートが生成されます。関心のある関係ではない場合、候補リストの次のエンティティーに処理が移動します。
- 関係スコアが、関係に対して構成されている基準を満たさない場合、候補リストの次のエンティティーに処理が移動します。この処理は、関係についてすべてのエンティティーが評価されるまで行われます。

Event Manager

Event Manager は、アイデンティティーおよび関係の解決にほぼリアルタイムのイベント分析とイベント・モニターを組み合わせることで、IBM InfoSphere Identity Insight の機能を拡張します。組織で Event Manager が有効になっている場合、ビジネス・イベントを追跡したり、疑わしいイベントまたは関心のあるイベントに関してアラートを生成したりすることができます。これにより、適切なビジネス・アクションをタイムリーに実行することが可能になり、脅威および不正への対応において組織を支援できます。

脅威および不正のシナリオは絶えず変化しています。このため、Event Manager では、追跡するイベントのタイプの定義や、イベント処理およびイベント・アラート生成のためのビジネス・ルールの構成を柔軟に行えるようになっています。ビジネス・ルールは、イベントの処理方法、および何がイベント・アラートのトリガーとなるかを決定するために Event Manager で使用される一連の基準です。ビジネス・ルールは、ビジネス・ニーズおよびシナリオに基づいて構成します。

イベント・アラートの構成要素についても決定します。イベント・アラートは、通常、単一のイベントではトリガーされません。異なるコンテキスト内で、それぞれ異なる時刻に発生した一連の複合イベントによりトリガーされます。例えば、所定の期間内に顧客が行った送金を集計し、合計金額が法的制限を超過した場合にアラートを生成するビジネス・ルールを定義する場合があります。あるいは、1 時間以内に、200 マイル以上離れた場所で同じクレジット・カード番号を使用して 2 つのクレジット・カード購入が行われた場合にアラートを生成するビジネス・ルールを定義する場合があります。

イベント処理の仕組み

IBM InfoSphere Identity Insight の Event Manager 機能は、IBM Active Middleware Technology[tm] の複合イベント・プロセッサーと連携します。このプロセッサーは、2 つの部分 (CEP エンジンと Eclipse[TM] ベースのルール作成ツール) で構成されます。ルール作成ツールでイベントおよびイベント・アラートのビジネ

ス・ルールを構成し、その構成を CEP.XML ファイルとしてエクスポートします。Event Manager を有効にすると、EVENT データ・セグメントを使用してフォーマット設定された入力 UMF ファイルがパイプラインで検出されるごとに、アイデンティティー解決のためにパイプラインによりデータが処理され、処理されたデータが CEP エンジンに渡されます。CEP エンジンでは、CEP.XML ファイルで構成されているイベント・ビジネス・ルールと照合してイベント・データが処理され、決定情報が IBM InfoSphere Identity Insight のパイプラインに返され、そこで、イベント情報がエンティティー・データベースに保管されます。イベントまたはイベントの組み合わせに関連するイベント・アラートがある場合、より詳細な分析および処理のために、Visualizer または別の可視化ツールにそれらのイベント・アラートが表示されるように Event Manager を構成できます。

また、クライアント・アプリケーションを構成して、CEP エンジンでクライアント・アプリケーションに決定を直ちに返すことができます。これにより、組織の担当者にリアルタイムの情報が提供されます。例えば、CEP エンジンで、取引 (電信送金で 24 時間以内に顧客が送金できる法的金額制限を超過した場合など) を停止するためのアラートを顧客サービス担当者に直ちに送信できます。

イベント

イベントは、ビジネス・ドメインで発生した事象 （「顧客が口座を開設する」、「顧客が電信送金する」など） についての情報を表します。Event Manager では、イベントには複数の属性があり、それらの属性は対応するイベント・タイプに基づいています。

イベント・アラート

イベント・アラートは、1 つ以上の複合イベントが、指定の存続期間にわたって設定基準を満たす場合に発生します。イベント・アラートは、イベント・ルール・ファイル (cep.xml) に含まれている複合イベントのビジネス・ルールやその他の構成に基づいています。アラートは、例えば、「過去 1 時間以内に相互に 200 マイル離れた場所で 10,000 米ドルを超える購入トランザクションが複数発生した」という、関心のある状態を示している場合があります。

イベント・タイプ

イベント・タイプによって、イベントをカテゴリー化し、Event Manager でイベントに関連付けられた値の計測単位を定義します。イベント・タイプの例には、電信送金、口座開設、クレジット・カード取引などがあります。

イベント・プロセッサーで使用されるユーザー定義のビジネス・ルールは特定のイベント・タイプを呼び出すため、イベント処理にはイベント・タイプが必要です。イベント・タイプが存在しないと、イベント・プロセッサーはイベントを処理できません。

イベント・ルール

イベント・ルールは、複合イベント処理 (CEP) エンジンで入力イベント・レコードをどのように処理するかを決定し、さらにどのタイプのイベント応答 (イベント・アラートなど) をパイプラインおよびクライアント・アプリケーションに返すかを決定する一連のビジネス・ルールです。イベント・ルールの構成は、Eclipse ™ ベ

ースの複合イベント処理用のルール作成ツールで行います。イベント・ルールは CEP プロジェクトでグループ化され、cep.xml という名前のイベント・ルール・ファイルにエクスポートされます。

組織またはアナリストが関心のある項目に基づいて、情報およびアラートが返されるようにイベント・ルールを構成します。単一の入力イベント・レコードのデータに対してアラートが返されるようにイベント・ルールを構成できます。ただし、ほとんどのイベント・ルールでは、複合イベント・データの集合をグループ化し、特定のしきい値または条件が満たされるとアラートがトリガーされるようにします。

ルール作成ツールでは、イベント・ビジネス・ルールをシチュエーション と呼びます。詳しくは、35 ページの『CEP の用語』を参照してください。

一般的なイベント・ルールには、合計関数とカウント関数が含まれます。例えば、エンティティーが 24 時間で 15,000 U.S. ドルを上回る金額を電信送金した場合にイベント・アラートを生成するイベント・ルールを構成できます。

Event Manager 入門

次のステップをチェックリストとして使用して、Event Manager を構成および使用します。

手順

1. 必須: Eclipse ベースの CEP (複合イベント・プロセッサー) ルール作成ツールをインストールします。 本製品では、Eclipse™ ベースのルール作成ツールは自動的にインストールされません。(Event Manager 機能および CEP エンジンは自動的にインストールされます。) ルール作成ツールは、製品ダウンロード内の ZIP ファイルに含まれています。
2. 必須: ルール作成ツールを使用して、Event Manager のすべてのイベント・ルールおよび構成をグループ化するための CEP プロジェクトを作成します。
3. 必須: ルール作成ツールで、CEP プロジェクトに cep.xml イベント・ルール・ファイルをインポートし、ビジネス・イベント処理およびアラート使用のシナリオを満たすイベント・ルールを作成することで、このファイルをカスタマイズします。 元の初期ファイルを変更する前に、念のためにそのファイルを別のディレクトリーにバックアップまたはコピーしてください。

   重要: イベント・ルール・ファイルの名前での大/小文字の使用は、特に Unix 環境では非常に重要です。ファイル名は小文字のみにする必要があります。
4. 必須: cep.xml イベント・ルール・ファイルをエクスポートします。CEP エンジンおよび Event Manager では、このイベント・ルール XML ファイルを使用してイベントが処理され、アラートをいつ生成するかが決定されます。エクスポートした XML ファイルは cep.xml という名前にする必要があり、また次のディレクトリーに配置する必要があります: *product_installation_home*/ibm-home/gem/。
5. 必須: 構成コンソールで、Event Manager システム・パラメーターを構成します。

   要確認: システム構成の変更を有効にするには、実行中のすべてのパイプラインを停止し、再始動する必要があります。Event Manager のシステム・パラメ

ーターおよびイベント・タイプを構成する前に、実行中のすべてのパイプラインを停止することも、あるいは、Event Manager のシステム・パラメーターおよびイベント・タイプを構成した後で、実行中のすべてのパイプラインを停止して再始動することもできます。

6. 必須: 構成コンソールで、イベント・タイプを構成します。

   要確認**:** システム構成の変更を有効にするには、実行中のすべてのパイプラインを停止し、再始動する必要があります。Event Manager のシステム・パラメーターおよびイベント・タイプを構成する前に、実行中のすべてのパイプラインを停止することも、あるいは、Event Manager のシステム・パラメーターおよびイベント・タイプを構成した後で、実行中のすべてのパイプラインを停止して再始動することもできます。

7. Analyst ツールキット・アプリケーションでイベント・アラートを表示するには、以下を実行します。
   a. オプション: Identity Insight には、イベント・アラート (保留中、割り当て済み、およびクローズ済み) を処理するためのデフォルト・アクティビティー・コードがあらかじめ含まれています。ただし、必要に応じて、構成コンソールでイベント・アラートの追加アクティビティー・コードを作成できます。アクティビティー・コードを作成する前に、実行中のすべてのパイプラインを停止します。次に、アクティビティー・コードが作成された後、パイプラインを再始動します。
   b. オプション: イベント・アラートの確認、イベント・アラートの状況の変更、自分へのイベント・アラートの割り当て、他のアナリスト・アラート・グループへのイベント・アラートの割り当てを実行できます。
   c. オプション: 特定のイベント・アラートに関する全詳細を確認するために、「イベント・アラート詳細 (Event Alert Detail)」レポートを生成できます。
   d. オプション: エンティティー・レジュメで、エンティティーに関するイベント・アラート・ヒストリーを確認できます。
   e. オプション: エンティティー・レジュメから、「イベントの表示 **(Show Events)**」をクリックすることで、エンティティーに関連するすべてのイベント (イベント・アラートを生成しなかったイベントを含む) を表示できます。また、「レポート **(Report)**」をクリックすることで、同様にエンティティーに関連するすべてのイベントを示す「すべてのイベント (All Events)」レポートを出力できます。
8. 必須: EVENT データ・セグメント定義を使用して、パイプラインに送信する変換対象の UMF データにイベント処理情報を含めます。
9. オプション: システム・メッセージ (Event Manager のメッセージなど) をクライアント・アプリケーションに送信する場合、HTTP パイプラインを使用する必要があり、またクライアント・アプリケーションが標準 SYSTEM_MESSAGE 戻り文書からのメッセージを受信できるようにする必要があります。
10. オプション: Event Manager でイベントが処理された後、Event Manager のログ・ファイルおよび関連する構成コンソールのログ・ファイルを確認できます。

構成コンソールでの Event Manager の有効化

Event Manager を使用してイベントを処理するには、事前に構成コンソールで Event Manager を有効にし、構成する必要があります。

このタスクについて

手順

1. 構成コンソールで、「システム構成」タブをクリックします。
2. イベント処理を有効にする場合、「イベント処理を有効にする **(Enable Event Processing)**」の値を変更します。
3. CEP の Universal Resource Indicator (URI) を構成する場合、「イベント・プロセッサー **URI (Event Processor URI)**」の値を変更します。デフォルトは、http://localhost:13510/gem です。
4. イベント処理の合計時間の設定値を増やす場合、「イベント・プロセッサーのタイムアウト **(Event Processor Timeout)**」の値を変更します。 この設定は、エラーでタイムアウトになる前に、パイプラインが外部イベント・プロセッサー (CEP) からの応答を待機する時間 (秒単位) を指定します。
5. 新規インバウンド・イベントの評価用にパイプラインへ送信するイベント・ヒストリーの日数を変更する場合、「イベント・ヒストリー期間 **(Event History Window)**」の値を変更します。
6. 「保存 **(Save)**」をクリックします。

Event Manager CEP モジュールの構成

IBM InfoSphere Identity Insight では、*CEP* は、製品にパッケージされている複合イベント処理ツールを表します。このツールは、Event Manager 内のコンポーネントであり、イベント・トランザクションを処理するため、およびイベント・アラートを生成するために、アイデンティティーおよび関係の解決を拡張します。このセクションでは、CEP ツールを構成する方法、具体的には、Event Manager と連携して動作するように構成する方法について説明します。

体系

Event Manager の CEP コンポーネントは、次の 2 つのツールで構成されます。

Eclipse™ ベースのルール作成ツール

Eclipse ベースの複合イベント処理のルール作成ツールは、`cep.xml` ファイルのイベント・ルールを構成およびエクスポートするために使用するコンポーネントです。イベント・ルール・ファイルにより、イベントをどのように処理するか、および何によりイベント・アラートをトリガーするかが決まります。

IBM InfoSphere Identity Insight をインストールするとき、ルール作成ツールとそのユーザーズ・ガイドを含む圧縮ファイルもインストールします。ただし、イベント・ルールの構成を開始する前に、ツールのファイルを解凍する必要があります。

複合イベント処理エンジン **(CEP** エンジン**)**

複合イベント処理エンジン (CEP エンジン) は、入力イベント・データを、cep.xml ファイルに構成されているイベント・ルールと照合して処理するコンポーネントです。

パイプラインで、入力 UMF 文書の EVENT データ・セグメントを使用してフォーマット設定されたデータが受信されると、そのデータはイベント処理のために CEP エンジンに送信されます。CEP エンジンにより、構成済みの cep.xml ファイルと照合してイベント・データが評価された後、その結果がパイプラインに送信されます。また、イベント・データが構成済みのイベント・ルールを満たすか、上回る場合、CEP エンジンにより、イベント・アラートを生成するためのシグナルがパイプラインに送信されます。イベント・アラートが生成されるかどうかに関係なく、パイプラインで受信された最終的なイベント・データは、エンティティー・データベースに書き込まれます。

CEP エンジンは、IBM InfoSphere Identity Insight とともにデフォルトでインストールされます。

これらの複合イベント処理コンポーネントは、特定のバージョンの IBM Active Middleware[tm] Technology の一部であり、Event Manager に含まれます。これらの複合イベント処理コンポーネントは、お買い上げの製品に含まれています。

cep.xml ファイル

cep.xml ファイルには、イベント・データを処理するため、およびイベント・アラートを生成するために必要なイベント・ルールおよびその他の設定が含まれます。パイプラインおよび CEP エンジンの Event Manager 機能では、cep.xml という名前のイベント・ルール・ファイルと照合したイベントのみを処理できます。このファイルは **E**xtensible **M**arkup **L**anguage (XML) 形式です。これは、パイプラインに入力されるデータが、XML に基づいた形式である **U**niversal **M**essaging **F**ormat (UMF) であるためです。

製品インストールには、初期 cep.xml ファイルが含まれています。この初期ファイルには、Event Manager が CEP エンジンと連携して動作するために必要な必須構成設定が多数含まれています。初期 cep.xml を CEP プロジェクトにインポートし、その後、イベント・ビジネス・ルールを構成できます。

注**:** cep.xml イベント・ルール・ファイルをインポートし、そのファイルを変更またはエクスポートする前に、元のファイルのバックアップ・コピーを作成し、その元のファイルを別のディレクトリーに保管してください。イベント・ルール・ファイルを変更する場合は必ず、バージョン管理システムまたはソース管理システムを使用することを検討してください。

CEP の追加リソース

Eclipse ベースのルール作成ツールの詳しい使用方法については、ツールのユーザーズ・ガイドを参照してください。AMT3.0.UserGuide.PDF という名前のガイドが、*install_path*/cep/ にあります。

Eclipse ベースの複合イベント・プロセッサーのルール作成ツールのインストール

以下の手順を実行して、Eclipse™ ベースのルール作成ツールをワークステーションにインストールします。製品インストール・プログラムにより、Event Manager と CEP エンジンの両方がインストールされます。ただし、ルール作成ツールは、インストールに含まれる ZIP ファイルからユーザーがインストールする必要があります。

始める前に

ルール作成ツールは、Microsoft Windows オペレーティング・システムでのみ動作し、Java バージョン 1.5 以上を必要とします。

このタスクについて

ルール作成ツールを使用して、ビジネスをモニターするために使用するルールおよびしきい値を構成し、その情報をイベント・ルール・ファイル (cep.xml) にエクスポートします。Event Manager および複合イベント・プロセッサー (CEP) エンジンは、イベント・ルール・ファイルを使用してイベントを処理し、イベント・アラートを検出します。単一のイベントまたはイベントの組み合わせにイベント・アラートを関連付けることができます。より詳細な分析のために、Event Manager を構成して、それらのイベント・アラートを Analyst ツールキットまたは別の視覚化ツールで表示できます。

ZIP ファイルから Eclipse ベースのルール作成ツールをインストールするには、以下のようにします。

手順

1. 製品インストール・ディレクトリーを参照します。
2. /cep サブディレクトリーを参照します。
3. CEP_3.0.1.1.03.zip ファイルを Microsoft Windows クライアント・マシンにコピーします。
4. CEP_3.0.1.1.03 ファイルを、ドライブ名:/CEP/ に解凍します。

次のタスク

ルール作成ツールの詳しい使用法については、ユーザーズ・ガイド (cep/AMT3.0_UserGuide.PDF ファイル) を参照してください。

ルール作成ツールの開始:

Eclipse™ ベースのルール作成ツールを使用するには、最初にツールを開始する必要があります。ルール作成ツールは、IBM InfoSphere Identity Insight コンポーネントとは別にインストールして開始します。

このタスクについて

ルール作成ツールは、Microsoft Windows オペレーティング・システムのクライアントでのみ動作し、Java バージョン 1.5 以上を必要とします。

手順

1. Microsoft Windows エクスプローラーを開き、Eclipse ベースのルール作成ツールがインストールされているディレクトリーに移動します。
2. AmitIDE.cmd という名前のバッチ・スクリプトをダブルクリックします。 バッチ・スクリプトにより、ルール作成ツールの実行可能ファイルが開きます。

CEP の用語

Eclipse[tm] ベースのルール作成ツールで使用される一部の用語は、IBM InfoSphere Identity Insight およびそのコンポーネントで使用される用語とわずかに異なる場合があります。この用語集を使用すると、複合イベント処理の用語を理解することができます。また、それらの用語が Event Manager やその他のコンポーネントとどのように関係するかを理解することもできます。

cep.xml ファイル (cep.xml file)

cep.xml ファイルには、Event Manager および CEP エンジンが入力イベント・レコードを処理するために必要な、すべてのイベント・ビジネス・ルール、および必須の複合イベント処理の構成設定が含まれます。この名前のイベント・ルール・ファイルは、ロケーション *product_installation_directory*¥ibm-home¥gem¥ にエクスポートする必要があります。

重要**:** ファイル名はすべて小文字にする必要があります (特に Unix 環境)。

ルール作成ツールを使用して、イベント・ルール・ファイルを維持およびエクスポートします。

IBM InfoSphere Identity Insight の製品インストールに、初期 cep.xml イベント・ルール・ファイルが含まれます。この初期ファイルには、Event Manager を使用するために必要な必須の設定および構成の多くが既に含まれています。元の初期 cep.xml イベント・ルール・ファイルのバックアップ・コピーを最初に作成してから、初期 cep.xml イベント・ルール・ファイルをルール作成ツールにインポートして、イベント・ビジネス・ルールを追加したり、このファイルを必須ロケーションにエクスポートしたりすることができます。このファイルを変更する前後に、バージョン管理システムまたはソース管理システムを使用して、ファイルを保管することを検討してください。

CEP エンジン (CEP engine)

複合イベント処理エンジン (または CEP エンジン) は、パイプラインからの入力イベント・データを処理し、CEP プロジェクトで定義されているルールと照合してデータを評価するメカニズムです。CEP プロジェクトは cep.xml ファイルで定義します。このファイルは、ルール作成ツールで構成およびエクスポートします。

Event Manager で現在使用されている CEP エンジンは、IBM Active Middleware[tm] Technology 製品の一部です。Event Manager で必要な CEP エンジンのバージョンが IBM InfoSphere Identity Insight の一部として含まれており、インストールされます。ただし、CEP エンジンでイベントを正常に処理できるようにするために、事前に構成コンソールで Event Manager を構成し、ルール作成ツールでイベント・ルールを構成する必要があります。

CEP プロジェクト (CEP projects)
プロジェクトは、複合イベント・プロセッサーがイベント、存続期間、およびルールのグループを格納するために使用する最上位グループです。Event Manager を使用するには、モニターするイベントのすべてのイベント情報 (ビジネス・イベント・ルールを含む) を格納する CEP プロジェクトを 1 つ作成します。Event Manager では一度に 1 つの CEP プロジェクトのみ使用されますが、単一のプロジェクトで複数のイベント・タイプをテストすること、およびイベント・タイプごとに複数のルールをテストすることができます。

ルール作成ツール内で CEP プロジェクトを作成および維持します。

ルール作成ツール (Eclipse ベースのルール作成ツール)(Rule Author tool (Eclipse-based Rule Author tool))
このツールを使用すると、cep.xml イベント・ルール・ファイルの構成要素として CEP プロジェクト、イベント、およびその他の構成を定義できます。CEP エンジンは、このファイルを使用して、イベントを処理し、イベント・アラートを生成します。

イベント・クラス (Event classes)
Event Manager を使用するには、CEP プロジェクトに次のイベント・クラスを含める必要があります。これらのイベント・クラスは、初期 cep.xml ファイルで事前構成されています。

- EAS_START.event: Event Manager の存続期間イニシエーターを示すために使用されます。
- EAS_STOP.event: Event Manager の存続期間ターミネーターを示すために使用されます。
- EVENT.event: 入力イベント・データを処理し、イベント・アラートを生成するために使用される、Event Manager のビジネス・ルール (またはシチュエーション) を定義するために使用されます。

EVENT.event
この CEP イベント・クラスでは、処理のためにパイプラインから CEP エンジンに渡される入力データがマップされます。このマッピングは、エンティティー・データベース内の GEM_EVENT 表に直接対応します。ルール作成ツールを使用して、EAS_EVENT に関連する属性が GEM_EVENT 表内のデータ・マッピングに一致することを確認します。

存続期間 (Lifespans)
CEP では、存続期間は、シチュエーション (イベント・ルール) が関連する時間間隔です。存続期間は、常にイニシエーターで開始し、常にターミネーターで終了します。存続期間はイベント・クラスに関連付けられています。

Event Manager では、イベント・クラス EVENT に、存続期間イニシエーター EAS_START および存続期間ターミネーター EAS_STOP を含める必要があります。

シチュエーション (Situations)
ルール作成のシチュエーションは、イベント・ルール と同等です。ルール作成ツールを使用してシチュエーションを構成します。このシチュエーショ

ンで、どのイベントまたはどのイベントの組み合わせを組織で対象とするか、および何によりイベント・アラートをトリガーするか決定するビジネス・ルールを定義します。

シチュエーションは、CEP プロジェクトおよびイベント・クラスに関連付けられていて、cep.xml イベント・ルール・ファイルに含まれています。

UMF データがパイプラインに入力されると、EVENT データ・セグメント定義を含むレコード (つまり UMF_ENTITY 入力文書) が CEP エンジンに送信されます。CEP エンジンで、cep.xml イベント・ルール・ファイル内の構成済みシチュエーションと照合して、この入力イベント・データが評価されます。イベントが定義済みのシチュエーションを満たす場合、または上回る場合、CEP エンジンはイベント・アラートをパイプラインに送り返します。このアラートは、Analyst ツールキット・アプリケーションまたは任意の視覚化ツールで表示できます。

しきい値条件 **(Threshold condition)**

イベント・ルール (シチュエーション) の一部としてしきい値条件を定義します。しきい値条件は、データ・フィルターまたはクイック・データ・チェックと見なすことができます。処理中、CEP エンジンは入力イベント・データをチェックして、そのデータが指定のしきい値条件を満たすどうか確認し、その後、データをルールと照合して処理します。データがしきい値条件を満たす場合、CEP エンジンはイベント・データをルールと照合して処理します。データがしきい値条件を満たさない場合、CEP エンジンは次のイベント・ルールに移行します。

例えば、ブランチ 102 で発生したイベントのみ処理するには、EVENT_LOC='102' を指定するしきい値条件を作成します。

UMF_LOG_ID キー (UMF_LOG_ID key)

UMF_LOG_ID は、レコードの処理時に各レコードに割り当てられるユニーク・シーケンス番号です。CEP プロジェクトでは、UMF_LOG_ID は、Event Manager の必要なすべてのイベント・クラスおよび存続期間インディケーターに関連付けられるグループ化キーです。このグループ化キーにより、同じ UMF_LOG_ID を持つすべての入力レコードが必ず一緒に処理されます。

製品に含まれる初期 cep.xml ファイルを CEP プロジェクトにインポートした場合、UMF_LOG_ID キーは既に構成されており、Event Manager のイベント・クラスおよび存続期間インディケーターに割り当てられています。

cep.xml イベント・ルール・ファイルの構成

cep.xml イベント・ルール・ファイルに構成されている情報により、Event Manager および CEP エンジンで入力イベント・データがどのように処理されるか、およびどのような応答がクライアント・アプリケーション、パイプライン、エンティティー・データベース、およびアプリケーションに返されるかが決まります。イベント・ルールは、cep.xml ファイルに含まれる情報の大部分を占めますが、イベント・ルールが唯一の必須情報というわけではありません。Event Manager を通じてイベントを適切に処理するためには、含める必要がある要素や設定が他にもあります。

本製品には、必要な要素および設定を含む初期 cep.xml イベント・ルール・ファイルが含まれており、このファイルは既に構成されています。初期 cep.xml ファイル

をインポートする場合、ユーザーはこれらの要素や設定を構成および変更する必要はなく、イベント・ビジネス・ルールの構成、および cep.xml ファイルへのルールの追加に集中できます。イベント・ルールは組織ごとにユニークであるため、初期 cep.xml ファイルには、事前構成済みのイベント・ルール (およびシチュエーション・タイプ) は含まれていません。

cep.xml ファイルで必須の要素および設定

この情報は参照用です。提供されている初期 cep.xml ファイルをインポートせずに、最初から独自のファイルを作成することを選択した場合、この情報を使用して、ファイルに必要なすべての要素および設定を含めてください。Event Manager で使用するためにエクスポートする cep.xml イベント・ルール・ファイルが不完全な場合 (この情報が含まれていない場合)、Event Manager は入力イベント・データを処理できません。

イベント・クラス

イベント・クラスは、CEP エンジンに認識させる必要がある各種イベント構造を表します。イベントを処理するには、次のイベント・クラスを cep.xml イベント・ルール・ファイルに含める必要があります。

EAS_START.event

このイベント・クラスは、Event Manager の存続期間イニシエーター、または CEP エンジンがイベントの処理を開始するためのシグナルになります。

EAS_STOP.event

このイベント・クラスは、Event Manager の存続期間ターミネーター、または CEP エンジンがイベントの処理を停止するためのシグナルになります。

EVENT.event

このイベント・クラスは、ユーザーが作成するすべてのイベント・ビジネス・ルールの基礎となるものです。Event Manager 表 (GEM_EVENT) および EVENT データ・セグメントに入力イベント・レコード・データをマップする情報が含まれます。

存続期間

CEP では、存続期間は、特定のイベント・ルールが関連付けられる時間間隔です。パイプラインでは、ほぼリアルタイムのデータが処理されるため、存続期間の実際の目的は、イベント・レコードの開始と終了をシグナル通知することのみです。

Event Manager 処理に必要な存続期間情報として、次の要素があります。

EAS_START

この要素は、必須の存続期間イニシエーターであり、イベントの開始をシグナル通知します。この存続期間要素の設定は、「存続期間: イニシエーター **(Lifespan: Initiators)**」タブの「イベント・イニシエーター **(Event Initiators)**」表で行います。

EAS_STOP

この要素は、必須の存続期間ターミネーターであり、イベントの終了をシグナル通知します。「存続期間: ターミネーターおよびキー

(Lifespan: Terminators & Keys)」タブの「イベントにより終了 **(Terminate By Event)**」でターミネーターを選択します。

UMF_LOG_ID グループ化キー
A UMF_LOG_ID は、レコード処理時に各レコードに割り当てられるユニーク・シーケンス番号です。CEP プロジェクトでは、UMF_LOG_ID グループ化キーにより、同じ UMF_LOG_ID を持つすべての入力レコードが同時に処理されます。このグループ化キーは、すべてのイベント・クラスおよび存続期間インディケーターに割り当てられます。

EVENT.event 属性
このイベント・クラスの必須属性は、EVENT データ・セグメントに直接マップされます。これらの必須属性は、エンティティー・データベース内の GEM_EVENT 表のフィールドです。これらの必須属性が EVENT.event から欠落している場合、イベント処理は失敗します。場合により、「無効または誤った形式の XML」または「CEP 構成 XML ファイルでの情報の欠落」を示すエラーなど、1 つ以上のエラー・メッセージが表示されます。

これらの属性は、各イベント・ルールの「シチュエーション **(Situation)**」:「一般およびイベント **(General & Event)**」タブで指定します。

CEP プロジェクトの作成**:**

CEP プロジェクトは、Event Manager および CEP エンジンで使用されるイベント・ルール、存続期間、およびその他のイベント情報のグループです。CEP プロジェクトは、cep.xml イベント・ルール・ファイルの一部であり、Eclipse ™ ベースの CEP ルール作成ツールで作成および保持されます。Event Manager 用のイベント・ビジネス・ルールを構成するには、あらかじめ CEP プロジェクトを定義しておく必要があります。

始める前に

- CEP ルール作成ツールが既にインストールされており、そのファイルが圧縮解除されている必要があります。
- CEP ルール作成ツールは、Microsoft Windows オペレーティング・システムでのみ動作し、Java バージョン 1.5 以上を必要とします。

手順

1. CEP ルール作成ツールで、「ファイル **(File)**」 > 「新規 **(New)**」 > 「プロジェクト **(Project)**」を選択します。
2. 「イベント処理プロジェクト **(Event Processing Project)**」を選択し、「次へ **(Next)**」をクリックします。
3. 「完了 **(Finish)**」をクリックします。 左ナビゲーション・ペインに CEP プロジェクトが表示されます。

次のタスク

製品インストールに含まれる初期の ibm-home¥gem¥cep.xml イベント・ルール・ファイルをインポートします。このファイルには、Event Manager を扱うために必要なエレメントおよび設定が既に含まれています。これらの必須オブジェクトを CEP プロジェクトにインポートした後、イベント・ビジネス・ルールを構成し、Event

Manager を通じてイベントの処理を開始するための最終的な cep.xml イベント・ルール・ファイルをエクスポートできます。

cep.xml イベント・ルール・ファイルのインポート:

cep.xml イベント・ルール・ファイルには、CEP エンジンおよび Event Manager がイベントを処理し、イベント・アラートを生成するために使用する情報が含まれます。Event Manager を扱うために必要なエレメントおよび設定が既に含まれている初期 cep.xml ファイルが、製品インストールに組み込まれています。既存の cep.xml ファイルを CEP プロジェクトにインポートすることにより、ファイルを最初から作成する必要がなくなります。

始める前に

- 元の cep.xml イベント・ルール・ファイルのバックアップ・コピーを作成し、必要に応じて元のファイルに戻すことができるようにします。バージョン管理システムまたはソース管理システムでファイルを保持することを検討します。
- Eclipse tm ベースのルール作成ツールをインストールし、そのファイルを解凍する必要があります。
- ルール作成ツールは、Microsoft Windows オペレーティング・システムのクライアントでのみ動作し、Java バージョン 1.5 以上を必要とします。
- ルール作成ツールで CEP プロジェクトを事前に作成しておく必要があります。

手順

1. ルール作成ツールで、「ファイル **(File)**」 > 「インポート **(Import)**」を選択します。
2. 「イベント処理定義 **(Event Processing Definition)**」を選択し、「次へ **(Next)**」をクリックします。
3. cep.xml ファイルを参照して選択します。 必ずデフォルトのファイル・タイプを DEF から XML に変更してください。通常、このファイルは、*product_installation_directory*¥ibm-home¥gem ディレクトリーにあります。
4. 次の項目を確認します。
   - ファイルのすべての内容が選択されていることを確認します。(必要に応じて、最上位フォルダーを展開して、ファイルの内容を調べます。)
   - 正しい CEP プロジェクト名が表示されていることを確認します。(必要に応じて、プロジェクトを参照して選択します。)
5. 「完了 **(Finish)**」をクリックします。 既存のファイルを上書きするかどうか尋ねるメッセージを受け取った場合、「**OK**」をクリックして既存のファイルを上書きします。 ファイルが正常にインポートされると、ルール作成ツールの左ナビゲーション・ペインに正符号がいくつか表示されます。

次のタスク

ビジネス・イベント・ルールを追加し、cep.xml イベント・ルール・ファイルを *product_install_directory*¥ibm-home¥gem¥ ディレクトリーにエクスポートします。

cep.xml イベント・ルール・ファイルのエクスポート**:**

Event Manager で複合イベント処理ルールを実行するために、Eclipse [tm] ベースのルール作成ツールで構成した cep.xml イベント・ルール・ファイルをエクスポートする必要があります。

始める前に

ルール作成ツールは、Microsoft Windows オペレーティング・システムのクライアントでのみ動作し、Java バージョン 1.5 以上を必要とします。

このタスクについて

- イベント・ルール・ファイルのエクスポート時に CEP エンジンが既に稼働している場合、エクスポートした新しい cep.xml イベント・ルール・ファイルの変更を有効にするために、IBM WebSphere サーバーでファイルを再ロードする必要があります。

手順

1. ルール作成ツールで、「ファイル **(File)**」 > 「エクスポート **(Export)**」を選択します。
2. 「イベント処理定義 **(Event Processing Definition)**」を選択し、「次へ **(Next)**」をクリックします。
3. CEP プロジェクトを選択します。
4. イベント処理定義ファイルを新しい cep.xml イベント・ルール・ファイルとして設定します。 このファイルは、通常、*product_installation_directory*¥ibm-home¥gem¥cep.xml にあります。
5. 「完了 **(Finish)**」をクリックします。 既存の cep.xml ファイルの上書きについてシステムから警告が出された場合、「**OK**」をクリックします。
6. オプション: IBM WebSphere サーバーが現在実行中の場合、CEP ルールを再ロードします。 製品アプリケーション・サーバーで CEP エンジンが始動すると、CEP により現行の cep.xml イベント・ルール・ファイルがロードされます。ファイルのエクスポート時に WebSphere サーバーが実行中である場合、新しい cep.xml ファイルを再ロードするまで変更は有効になりません。
   a. Web ブラウザー・ウィンドウを開き、WebSphere サーバーにナビゲートします。 例えば、http://localhost:13510/gem です。
   b. 「ルールの再ロード **(Reload Rules)**」をクリックします。

      注**:** WebSphere サーバーでは、ルールが再ロードされたことを示す情報は表示されません。

イベント・ルール結果の構成に関するガイドライン

イベント・ルールでは、イベントをどのように処理するか、およびどのようなシチュエーションでイベント・アラートを生成するかを定義します。イベント・ルール (Eclipse[tm] ベースの CEP ルール作成ツールでは、シチュエーション・タイプ と呼ばれる) は、cep.xml イベント・ルール・ファイルに含まれています。Event Manager および CEP エンジンは、このファイルを使用して入力イベント・データを処理します。定義する複合イベント・ルールは組織にユニークなものです。

ルールが Event Manager で機能するようにするために、イベント・ルールの定義を開始する前に、次の考慮事項に注意してください。

- イベント・ルールでは、エンティティー、およびエンティティーが実行できるトランザクションに焦点を当てる必要があります。エンティティーは、通常、個人ですが、エンティティーが場所または物事を表す場合もあります。例えば、エンティティーが船の場合があります。
- イベント・ルールは、宣言ステートメント (「Location=Texas」など) として表すか、一定時間における個数 （合計、カウント、平均） の数式として表す必要があります。

各イベント・ビジネス・ルールの必須シチュエーション属性

複合イベント・プロセッサーからエンティティー・データベースにイベント・データを戻すために、作成する各イベント・ビジネス・ルールに必須シチュエーション属性を手動で追加する必要があります。これらの属性は初期 `cep.xml` イベント・ルール・ファイルには含まれていません。したがって、この初期ファイルをインポートしても、イベント・ビジネス・ルール (シチュエーション) が自動的に作成されることも、これらの属性が新規または既存のルールに自動的に追加されることもありません。

これらのシチュエーション属性により、イベント・データが Event Manager の `GEM_EVENT` 表に直接マップされます (各入力イベント・レコードの UMF に一致します)。これらの必須属性がない場合、CEP エンジンで処理されたデータは、パイプラインを通じて Event Manager に戻されません。

表 4. 複合イベント・ビジネス・ルールの必須シチュエーション属性

属性名	属性タイプ	属性式	属性の説明
EVENT_SIT_STATUS	ストリング	"PENDING"	イベント・アラートのイベント・アラート状況を示します。 i2 プラグイン、エクスプローラー、および Cognos アラート要約レポートでは、イベント・アラート状況は「アラート要約 (Alert Summary)」の一部として表示されます。新しく生成されたアラートは、通常、すべて保留状況となります。保留状況は、アナリストがそのアラートを分析および処理する必要があることを示します。 イベント・アラート状況は、組織にとって意味があるものであればどのようなものでも構わないこと、構成コンソールでイベント状況として構成されることを覚えておいてください。 イベントを Analyst ツールキット・コンポーネントのユーザー・インターフェースに表示しないようにするには、「CLOSED」イベント・アラート状況を使用します。

表 4. 複合イベント・ビジネス・ルールの必須シチュエーション属性 (続き)

属性名	属性タイプ	属性式	属性の説明
REASON_DESC	ストリング	"<イベント・ルールまたはアラートの説明>"	イベント・アラートをトリガーしたイベント・ルールについての説明を示します。この説明は、アナリストにとってできるだけ意味のあるものにします。 例えば、エンティティーが 24 時間以内に $1500 を上回る取引を行った場合にイベント・ルールでアラートを生成する場合、REASON_DESC として「SumOver1500」などと入力します。
ALERT_GROUP	ストリング	"<*alert group*>"	どのアラート・グループに、このイベント・ルールから生成されるイベント・アラートを割り当てるかを示します。 通常、この値は「DEFAULT」ですが、構成コンソールで構成されている任意のアラート・グループを入力できます。

イベント・アラートの詳細の表示

通常、イベント・アラートは複数の複合イベントからトリガーされます。Analyst ツールキット・アプリケーションまたはクライアント・アプリケーションでイベント・アラートを表示できますが、デフォルトでは、そのアラートを生成したイベントの詳細は含まれません。

イベント・アラートを生成したイベントの詳細を含める場合、次のシチュエーション属性を含める必要があります。

表 5. イベント・ルールで *EVENTS* シチュエーション属性を作成するために必要な設定

名前	タイプ	式	ディメンション (「詳細の表示 **(Show Advanced)**」ボタン)
EVENTS	整数	Event.EventID	[] (EventID が配列であることを示します。) この列の設定を表示および定義するには、このシチュエーション属性を編集し、「詳細の表示 (Show Advanced)」ボタンをクリックしてください。

ベスト・プラクティス

Analyst ツールキット・アプリケーションでイベント・アラートを表示する場合、イベントの値をメッセージに追加するのではなく、REASON_DESC シチュエーション属性がシンプルなテキスト・ストリングになるようにしてください。Analyst ツールキットでは、共通のアラートは 1 つのアラート要約にグループ化されます。アラート要約には、その要約に組み込まれたアラートの数が含まれます。アナリストは、アラート要約をクリックすることで、その要約に含まれるすべてのアラートを処理できます。

REASON_DESC にイベントの値を定義すると、各イベント・アラートが、カウント 1 の個別アラート要約として表示されます。これにより、アナリストは、アラート要約と「アラート要約 (Alert Summary)」ウィンドウのアラート詳細領域の両方で各イベント・アラートを確認できます。

複合イベントを合計するイベント・ルールの作成

イベントの合計数を計算し、それらのイベントの合計が設定しきい値を超過した場合にイベント・アラートを作成する基本 SUM イベント・ルールを作成します。例えば、ある個人が 24 時間以内に送金した全金額を合計し、それらの送金金額 (イベント) の合計が $15,000 を超過した場合にイベント・アラートを送信するイベント・ルールを作成できます。

始める前に

イベント・ルールおよびすべてのルール構成をグループ化する既存の CEP プロジェクトが必要です。

このタスクについて

以下に、任意の値を合計する簡単なビジネス・ルールを作成するための基本的な手順を示します。一部の手順では、同じ最終結果を達成するための方法が複数あります。その他のオプションについては、製品に同梱されている「IBM Advanced

Middleware™ Technology ユーザーズ・ガイド」(Eclipse™ ベースの CEP ルール作成ツールのガイド) の『シチュエーション *(Situations)*』 セクションを参照してください。

手順

1. 左側のナビゲーション・ペインで、「シチュエーション **(Situation)**」を右クリックし、「新規 **(New)**」 > 「シチュエーション **(Situation)**」を選択します。「イベント処理プロジェクト **(Event Processing Project)**」に、正しいプロジェクト名が表示されていることを確認します。
2. 「シチュエーション名 **(Situation name)**」に、ユニーク・ルール名を入力します。 シチュエーション名は、エンティティー・データベースおよび Visualizer コンポーネントに表示されるイベント・ルール名です (そこにイベント・アラートが表示されるように選択した場合)。この名前は、イベント・アラートを分析する担当者にとって分かりやすいものにします。例えば、すべてのイベントの値を合計し、イベントの合計が $15,000 という制限値を超過した場合にアラートを送信するルールを作成する場合、そのルールに `SumOver15K` という名前を付けます。
3. 「ソースの選択 **(Select source)**」で「空タイプ **(Empty of Type)**」を選択し、ドロップダウン・リストから「以上 **(atleast)**」を選択します。 「以上 **(atleast)**」シチュエーションでは、イベント値を合計でき、さらにイベント・ルールを満たす各イベントの情報を保存できます。シチュエーション・タイプについて詳しくは、ユーザーズ・ガイドの『シチュエーション・プロパティー *(Situation Properties)*』 を参照してください。
4. 「完了 **(Finish)**」をクリックします。 メイン・シチュエーション画面が表示されると、「問題 **(Problems)**」セクションにいくつかのエラーがある場合があります。これらのエラーは、欠落する値を示していますが、現時点ではこれらのエラーは無視してかまいません。この手順を完了すると、エラーは解消されます。
5. 「イベント **(Events)**」セクションで、このルールの基本イベントとして「`EVENT`」を選択します。 「`EVENT`」は、常にすべてのイベント・ビジネス・ルールの基本イベントです。これには、エンティティー・データベース `GEM_TABLE` および `EVENT` データ・セグメントへの必須マッピングが含まれます。
6. オプション: しきい値条件 を作成すると、イベントをこのルールと照合して評価する前にそれらのイベントをフィルター処理できます。これにより、イベントは、適用されるよう指定されているしきい値条件を満たす必要があります。
7. 合計式を作成するために、「詳細の表示 **(Show Advanced)**」をクリックし、「編集 **(Edit)**」をクリックします。
8. 「数量詞 **(Quantifier)**」で、「**それぞれ** (`each`)」を選択します。 この選択により、このイベント・ルールの条件を満たす各入力イベント・レコードが合計に組み込まれます。
9. 「ウェイト **(Weight)**」で、「**...**」をクリックしてフィールドを編集します。「式ビルダー **(Expression Builder)**」を使用して、合計するイベント・フィールドを選択します。式が「式ビルダー・テキスト **(Expression Builder Text)**」領域に表示されていることを確認し、「**OK**」をクリックします。 デフォルトでは、各イベントのウェイトは 1 と同等です。イベント・ルールが評価

されるとき、すべてのウェイトの合計が「条件および結果 **(Condition & Results)**」タブの「数量 **(Quantity)**」属性と比較されます。合計が、指定されている数量以上である場合、イベント・アラートが生成されます。例えば、イベント・ルールを満たす各イベントの値を合計するために、EVENT.EVENT_VALUE を選択します。

10. オプション: ウェイトとして選択されているフィールドに小数桁数 (double 型) が含まれる場合、式ビルダーを使用して、以下を実行する式を作成します。
    a. 計算結果に 100 を乗算して、小数桁数がドルからセントに変換されるようにします。
    b. double 型を integer 型に変換します。 関数を使用して、これを実行できます。

    例えば、イベントの値 (EVENT.EVENT_VALUE) を合計する場合、「式ビルダー・テキスト **(Expression Builder Text)**」領域に EVENT.EVENT_VALUE*100 と入力します。次に、「関数 **(Functions)**」 > 「演算 **(Math)**」 > 「丸め **(Round)**」を選択して、結果を最も近い整数値に丸めます。 最終的な式は Round(EVENT.EVENT_VALUE*100) となります。
11. 「合計式 **(Sum Expression)**」で、「**...**」をクリックしてフィールドを編集し、合計するイベント・フィールドを選択します。 例えば、イベント・ルールを満たす、または上回る各イベントの値を合計するには、EVENT_VALUE を選択します。
12. オプション: 特定の条件を満たすイベントのみ合計するには、「しきい値条件 **(Threshold Condition)**」に条件を入力するか、補助となる式ビルダーを使用します。 例えば、ブランチ 102 で発生したイベントの値のみを合計するには、EVENT.EVENT_LOC="102" と入力します。このフィールドはフィルターとして機能し、条件を満たさない、または超過しないイベントは自動的にスキップされます。

    ヒント**:** 表示を簡素化して「しきい値条件 **(Threshold Condition)**」を見やすくするには、「詳細の非表示 **(Hide Advanced)**」をクリックします。
13. 「条件および結果 **(Condition & Results)**」タブの「存続期間 **(Lifespan)**」で、「EASLifeSpan」を選択します。 選択を行うまで、このフィールドは赤色で表示されます。この赤色は、このフィールドが必須であり、「問題 **(Problems)**」セクションにリストされているいずれかのエラーがあることを示します。 存続期間の選択を行うと、エラーは「問題 **(Problems)**」セクションからなくなります。
14. 「数量 **(Quantity)**」に数量を入力します。イベント・ルールで合計がこの数量「以上 (atleast)」になったらイベント・アラートが生成されます。 ドル金額には必ず 100 を乗算してください。例えば、合計が $15,000 以上に達した場合にイベント・アラートを生成するには、1500000 を入力します。
15. 「検出モード **(Detection Mode)**」で、「即時 (immediate)」が選択されていることを確認します。この選択はこのままにします。 検出モードにより、イベントの結果をいつ計算し、報告するかが決まります。「即時 (immediate)」を選択すると、合計が数量に達した場合に即座にアラートが生成されます。
16. 「シチュエーション属性 (Situation Attributes)」で、次のシチュエーション属性に対して必須シチュエーション値を入力します。
    - EVENT_SIT_STATUS

- REASON_DESC
- ALERT_GROUP

17. オプション: 合計を構成するすべてのイベントの詳細を保存するために、次の情報を使用して EVENTS シチュエーション属性を追加します。
    a. 「名前 **(Name)**」に EVENTS と入力します。
    b. 「タイプ **(Type)**」に、integer と入力します。
    c. 「式 **(Expression)**」に EVENT_ID と入力します (または、「式ビルダー **(Expression Builder)**」でこれを選択します)。
    d. 「詳細の表示 **(Show Advanced)**」をクリックして「ディメンション **(Dimensions)**」列を表示し、この列に [] を入力して、タイプがイベントの配列であることを示します。

    これらの値により、CEP は、合計に含まれる各イベントの内部 EVENT_ID を、イベント・アラートと共にパイプラインに送り返します。パイプラインによって、各 EVENT_ID がエンティティー・データベースに書き込まれ、イベント・アラートの表示に使用される Visualizer またはクライアント・アプリケーションに情報が送信されます。EVENT_ID は、パイプラインによりイベント・データが CEP エンジンに送信されるときに作成される内部シーケンス番号 (ID) です。
18. イベント・ルールを保存します。

複合イベントをカウントするイベント・ルールの作成

イベントをカウントし、合計カウントがしきい値設定を超過した場合にイベント・アラートを作成する基本 COUNT イベント・ルールを作成します。例えば、24 時間以内のすべての電信送金取引をカウントし、取引カウントが 500 を超えた場合にイベント・アラートを送信するイベント・ルールを作成できます。

始める前に

イベント・ルールおよびすべてのルール構成をグループ化する既存の CEP プロジェクトが必要です。

このタスクについて

以下に、任意の値をカウントする簡単なビジネス・ルールを作成するための基本的な手順を示します。一部の手順では、同じ最終結果を達成するための方法が複数あります。その他のオプションについては、製品に同梱されている「IBM Advanced Middleware™ Technology ユーザーズ・ガイド」(Eclipse™ ベースの CEP ルール作成ツールのガイド) の『シチュエーション *(Situations)*』 セクションを参照してください。

手順

1. 左側のナビゲーション・ペインで、「シチュエーション **(Situation)**」を右クリックし、「新規 **(New)**」 > 「シチュエーション **(Situation)**」を選択します。「イベント処理プロジェクト **(Event Processing Project)**」に、正しいプロジェクト名が表示されていることを確認します。
2. 「シチュエーション名 **(Situation name)**」に、ユニーク・ルール名を入力します。 シチュエーション名は、エンティティー・データベースおよび Visualizer

コンポーネントに表示されるイベント・ルール名です (そこにイベント・アラートが表示されるように選択した場合)。この名前は、イベント・アラートを分析する担当者にとって分かりやすいものにします。例えば、特定のブランチ・ロケーションで発生したすべてのイベントをカウントするルールを作成する場合、このルールに CountBranch102Transactions という名前を付けます。

3. 「ソースの選択 **(Select source)**」で、「空タイプ **(Empty of Type)**」を選択し、ドロップダウン・リストから次のいずれかの値を選択します。
   - 「以上 **(atleast)**」: 存続期間中に *n* 件以上のイベントが発生したことを示します。
   - 「以下 **(atmost)**」: 存続期間の終わりまでに、*n* 件以下のイベントが発生したことを示します。

   どちらのシチュエーション・タイプでもイベント値をカウントでき、さらにイベント・ルールを満たす各イベントの情報を保存できます。シチュエーション・タイプについて詳しくは、ユーザーズ・ガイドの『シチュエーション・プロパティー *(Situation Properties)*』 を参照してください。
4. 「完了 **(Finish)**」をクリックします。 メイン・シチュエーション画面が表示されると、「問題 **(Problems)**」セクションにいくつかのエラーがある場合があります。これらのエラーは、欠落する値を示していますが、現時点ではこれらのエラーは無視してかまいません。この手順を完了すると、エラーは解消されます。
5. 「イベント **(Events)**」セクションで、このルールの基本イベントとして「EVENT」を選択します。 「EVENT」は、常にすべてのイベント・ビジネス・ルールの基本イベントです。これには、エンティティー・データベース GEM_TABLE および EVENT データ・セグメントへの必須マッピングが含まれます。
6. オプション: しきい値条件 を作成すると、イベントをこのルールと照合して評価する前にそれらのイベントをフィルター処理できます。これにより、イベントは、適用されるよう指定されているしきい値条件を満たす必要があります。
7. 「条件および結果 **(Condition & Results)**」タブの「存続期間 **(Lifespan)**」で、「EASLifeSpan」を選択します。 選択を行うまで、このフィールドは赤色で表示されます。この赤色は、このフィールドが必須であり、「問題 **(Problems)**」セクションにリストされているいずれかのエラーがあることを示します。 存続期間の選択を行うと、エラーは「問題 **(Problems)**」セクションからなくなります。
8. 「数量 **(Quantity)**」に数量を入力します。イベント・ルールでのカウントが、この数量「以上 (atleast)」または「以下 (atmost)」のとき、イベント・アラートが生成されます。
9. 「検出モード **(Detection Mode)**」で、「即時 (immediate)」が選択されていることを確認します。この選択はこのままにします。 検出モードにより、イベントの結果をいつ計算し、報告するかが決まります。「即時 (immediate)」を選択すると、カウントが数量に達した場合に即座にアラートが生成されます。
10. 「シチュエーション属性 (Situation Attributes)」で、必須のシチュエーション属性の名前、タイプ、および式を入力します。
    - EVENT_SIT_STATUS
    - REASON_DESC

- ALERT_GROUP

11. カウントを構成するすべてのイベントの詳細を保存するために、次の情報を使用して EVENTS シチュエーション属性を追加します。
    a. 「名前 **(Name)**」に EVENTS と入力します。
    b. 「タイプ **(Type)**」に、integer と入力します。
    c. 「式 **(Expression)**」に EVENT_ID と入力します (または、「式ビルダー **(Expression Builder)**」でこれを選択します)。
    d. 「詳細の表示 **(Show Advanced)**」をクリックして「ディメンション **(Dimensions)**」列を表示し、この列に [] を入力して、タイプがイベントの配列であることを示します。

    これらの値により、CEP は、合計に含まれる各イベントの内部 EVENT_ID を、イベント・アラートと共にパイプラインに送り返します。パイプラインによって、各 EVENT_ID がエンティティー・データベースに書き込まれ、イベント・アラートの表示に使用される Visualizer またはクライアント・アプリケーションに情報が送信されます。EVENT_ID は、パイプラインによりイベント・データが CEP エンジンに送信されるときに作成される内部シーケンス番号 (ID) です。
12. イベント・ルールを保存します。

アクセシビリティー

アクセシビリティー機能は、運動障がいまたは視覚障がいなど身体に障がいを持つユーザーがソフトウェア・プロダクトを快適に使用できるようにサポートします。

主なアクセシビリティー機能は、以下のとおりです。

- 推奨されている Internet Explorer ブラウザーを使用している場合、ナビゲーションにマウスの代わりにキーボードを使用して、すべてのユーザー・インターフェース機能を利用できます。
- 本製品は支援技術と互換性があります。
- IBM InfoSphere Identity Insight の資料は、アクセシビリティー対応の形式で提供されています。

キーボード・アクセス

IBM InfoSphere Identity Insight の構成コンソールおよび Visualizer は、Internet Explorer ブラウザーを使用して表示した場合、アクセシビリティーに完全に対応しています。

キーボードのみを使用して、構成コンソールまたは Visualizer を操作できます。マウスを使用して実行できる操作を、複数のキーまたはキーの組み合わせを使用して実行することもできます。標準的なオペレーティング・システムの操作には、標準的なオペレーティング・システムのキー・ストロークが使用されます。

サポートされているすべてのオペレーティング・システムおよびブラウザーで、キー・ストロークが有効なアクティブ・ウィンドウの領域が強調表示されます。テキスト・ボックスおよびテキスト領域には、明滅する挿入ポイント・カーソルが表示されます。その他のフィールドは、破線の境界線で強調表示されます。

注**:** 構成コンソールは Mozilla Firefox ブラウザー使用時にキーボードで操作できますが、このブラウザーで **Alt** + 数字 キーを使用したキーボード・アクセラレーターおよびショートカットがサポートされないという既知の問題があります。

アクセシビリティー対応の表示

構成コンソールおよび Visualizer には、視力の弱いユーザーやその他の視力障がいがあるユーザーのためにアクセシビリティーを向上させる機能が備わっています。これらのアクセシビリティーの強化には、カスタマイズ可能なフォント・プロパティーのサポートが含まれます。

ユーザー・インターフェースごとに、メニューおよびダイアログ・ウィンドウで使用されるテキストの色、サイズ、およびフォントを選択できます。

- 構成コンソール: ブラウザー設定を通じて
- Visualizer: 「画面設定の構成 **(Configure Screen Preferences)**」設定を通じて

本製品のすべての機能を使用するために、ユーザーは必ずしも色を識別する必要はありません。

支援技術との互換性

Visualizer のユーザー・インターフェースは、Java Accessibility API をサポートしています。この API により、スクリーン・リーダーおよびその他の支援技術を使用できます。構成コンソールでは、サポートされているブラウザーでスクリーン・リーダーを有効にすることができます。

アクセシビリティー対応の資料

IBM InfoSphere Identity Insight の資料は、ほとんどの Web ブラウザーで表示可能な XHTML 1.0 形式で提供されています。XHTML により、ご使用のブラウザーに設定されている表示設定に従って資料を表示できます。また、スクリーン・リーダーやその他の支援技術も使用できます。

構成コンソールのキーボード・ショートカットおよびアクセラレーター

構成コンソールは、サポートされているブラウザーを使用して表示した場合、アクセシビリティーに完全に対応しています。つまり、マウスを使用して実行できる操作を、複数のキーまたはキーの組み合わせを使用して実行することもできます。

注**:** 構成コンソールは、Mozilla Firefox ブラウザーを使用した、キーボードによるナビゲーションが可能ですが、このブラウザーでは、リストされている **Alt** + 数字 キーが正しく動作しません。

表 *6.* 一般的なキーボード・ショートカットおよびアクセラレーター

アクション	ショートカット
次の画面要素 (入力フィールド、ボタン、リンク) にフォーカスを移動する (読み取り専用フィールドはスキップされます)。	**Tab**
前の画面要素 (入力フィールド、ボタン、またはリンク) にフォーカスを移動する (読み取り専用フィールドはスキップされます)。	**Shift** + **Tab**

表 *6.* 一般的なキーボード・ショートカットおよびアクセラレーター *(*続き*)*

アクション	ショートカット
アクション (リンクまたはボタン) を実行する。	**Enter**

表 *7.* フィールド・ナビゲーション

アクション	キーまたはショートカット
ドロップダウン・リスト内で上または下に移動する。 テキスト域フィールドの複数行で上または下に移動する。	上矢印または下矢印
テキスト入力フィールド内で左または右に移動する。	左矢印または右矢印
テキスト入力フィールドの先頭に移動する。 大きいテキスト域フィールドの現在行の先頭に移動する。	**Home**
入力フィールドの末尾に移動する。 大きいテキスト域フィールドの現在行の末尾に移動する。	**End**
テキスト入力フィールドの末尾に移動する。 テキスト域フィールドの次のページに移動する。	**Page Down**
テキスト入力フィールドの先頭に移動する。 テキスト域フィールドの前のページに移動する。	**Page Up**
ドロップダウン・リストを展開または縮小する。	**Alt** + 上矢印または下矢印
テキスト域の先頭に移動する。	**Ctrl + Page Up**
テキスト域の末尾に移動する。	**Ctrl + Page Down**

表 *8.* 画面ナビゲーション

アクション	ショートカット
(スクリーン・リーダー使用時) ページ・ヘッダー内のすべてのナビゲーション・リンクおよびアクション・リンクをスキップする。	**Alt + 0**
ロケーション域および右上隅のアクションにフォーカスを移動する。	**Alt + 1**
メニューまたはサブメニューにフォーカスを移動する。	**Alt + 2**
最上位タブにフォーカスを移動する。	**Alt + 3**
最上位リンクにフォーカスを移動する。	**Alt + 4**
(詳細画面のみ) 左ナビゲーション・ペインの項目にフォーカスを移動する。	**Alt + 5**

表 *8.* 画面ナビゲーション *(*続き*)*

アクション	ショートカット
(詳細画面のみ) サブタブおよび詳細アクション・ボタンにフォーカスを移動する。	**Alt + 6**
メイン・コンテンツ領域のフォーム・フィールドにフォーカスを移動する。	**Alt + 7**
(スクリーン・リーダー使用時) ディレクトリーをスキップして詳細画面のフィールドに移動する。	**Alt + 8**
(スクリーン・リーダー使用時) 画面下部にあるヘルプ・フッターにスキップする。	**Alt + 9**

表 *9.* 編集アクション *(*入力フィールド内*)*

アクション	ショートカット
コピー	**Ctrl + C**
切り取り	**Ctrl + X**
貼り付け	**Ctrl + V**
すべて選択	**Ctrl + A**
取り消し	**Ctrl + Z**
カーソルの左にある文字を削除する。	**Backspace**
カーソルの右にある文字を削除する。	**Delete**

Visualizer のキーボード・ショートカットおよびアクセラレーター

Visualizer は、アクセシビリティーに完全に対応しています。つまり、マウスを使用して実行できる操作を、複数のキーまたはキーの組み合わせを使用して実行することもできます。

表 *10.* 一般的なキーボード・ショートカットおよびアクセラレーター

アクション	ショートカット
次の画面要素 (入力フィールド、ボタン、リンク) にフォーカスを移動する。	**Tab**
前の画面要素 (入力フィールド、ボタン、またはリンク) にフォーカスを移動する。	**Shift + Tab**
アクション (リンクまたはボタン) を実行する。	**Enter** またはスペース・バーを押す
「レポート基準 (reports criteria)」画面を表示し、デフォルトとして属性アラート・ジェネレーター・レポートを設定する。	**Ctrl + A**
「UMF ファイル・ロード (UMF File Load)」画面を表示する。	**Ctrl + B**
「パスワードの変更 (Change password)」ダイアログを表示する。	**Ctrl + H**
アプリケーションをロックする。現行ユーザーの Visualizer セッションは続行されますが、画面はロックされます。	**Ctrl + L**

表 *10.* 一般的なキーボード・ショートカットおよびアクセラレーター *(*続き*)*

アクション	ショートカット
情報またはレポート (エンティティー・レジュメなど) を印刷できるウィンドウまたはタブから「印刷 (Print)」ダイアログを表示する。	**Ctrl + P**
現行ユーザーを Visualizer セッションからログアウトし、アプリケーションを終了する。	**Ctrl + Q**
「画面設定の構成 (Configure Screen Preferences)」ダイアログを表示する。	**Ctrl + R**
製品のインフォメーション・センターを表示する。	**F1**
製品のバージョン番号を含む「バージョン情報 (About)」ウィンドウを表示する。	**Shift + F1**

表 *11.* フィールド・ナビゲーション

アクション	キーまたはショートカット
上または下のフィールドに移動する。 ドロップダウン・リスト内で上または下に移動する。 入力フィールドの複数のテキスト行で上または下に移動する。	上矢印または下矢印
入力フィールド内で左または右に移動する。	左矢印または右矢印
入力フィールドの先頭に移動する。 大きいテキスト・フィールドの現在行の先頭に移動する。	**Home**
入力フィールドの末尾に移動する。 大きいテキスト・フィールドの現在行の末尾に移動する。	**End**
入力フィールドの末尾に移動する。	**Page Down**
入力フィールドの先頭に移動する。	**Page Up**
ドロップダウン・リストを展開または縮小する。	**Alt** + 上矢印または下矢印
三角アイコンを展開または縮小する (三角アイコンが選択されている場合)。	スペース・バー
表の外部にある次のコントロールに移動する。	**Ctrl + Tab**

表 *12.* 編集アクション

アクション	ショートカット
コピー	**Ctrl + C**
切り取り	**Ctrl + X**
貼り付け	**Ctrl + V**

表 *12.* 編集アクション *(*続き*)*

アクション	ショートカット
テキスト・ボックス内のすべてのテキストを選択する。	**Ctrl + A**
取り消し	**Ctrl + Z**
カーソルの左にある文字を削除する。	**Backspace**
カーソルの右にある文字を削除する。	**Delete**

第 2 章 システム要件と計画立案

この参照セクションには、サポートされるプラットフォーム、システム要件、およびシステム体系に関する情報が含まれています。

システム要件の詳細

以下に、IBM サポート・チームに問題報告をオープンする前に、インストールして使用する必要のあるハードウェア製品およびソフトウェア製品の要件を示します。

IBM AIX で実行する場合のシステム要件

以下に、AIX® オペレーティング・システム上で IBM InfoSphere Identity Insight を実行するときにサポートされる製品をリストします。

表 *13. IBM AIX* で実行する場合のシステム要件

オペレーティング・システム	• IBM AIX 7.1L
ハードウェア要件	• POWER7® (64 ビット) • POWER6® • POWER5
Java	以下のものが、この製品とともにインストールされます。 • IBM 64 ビット Java ランタイム環境、バージョン 8
データベース	• IBM DB2® Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g リリース 2 (11.2.0.1、11.2.0.2、またはそれ以降)
データベース・クライアント	• DB2 クライアント v11.1 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c クライアント (接続先が Oracle 12c の場合) • Oracle 11g リリース 2 クライアント (接続先が Oracle 11g リリース 2 の場合)

表 *13. IBM AIX* で実行する場合のシステム要件 *(*続き*)*

Java Database Connectivity (JDBC) クライアント	• DB2 クライアント v11.1 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c JDBC ドライバー (接続先が Oracle 12c の場合) • Oracle 11g JDBC ドライバー (接続先が Oracle 11g の場合)
Web ブラウザー	• Mozilla Firefox
メッセージ・キューイング・ソフトウェア	• IBM WebSphere MQ
その他	• IBM C++ Runtime Environment Components for AIX。この要件について詳しくは、サポート情報: http://www-01.ibm.com/support/docview.wss?uid=swg24025181 を参照してください。

HP-UX で実行する場合のシステム要件

以下に、HP-UX オペレーティング・システム上で IBM InfoSphere Identity Insight を実行するときにサポートされる製品をリストします。

表 *14. HP-UX* で実行する場合のシステム要件

オペレーティング・システム	• HPUX 11i v3
ハードウェア要件	• Intel Itanium 2 (IA64)
Java	以下のものが、この製品とともにインストールされます。 • IBM 64 ビット Java Runtime Environment for HPUX、Java Technology Edition バージョン 6
クライアント **Java** 要件	HPUX は、サポートされるクライアント・プラットフォームではありません。構成コンソールまたは Visualizer に接続されている、サポートされるプラットフォームのそれぞれのクライアント・マシンには、SUN Java SE Runtime Environment (JRE) バージョン 6 がインストールされている必要があります。

表 *14. HP-UX* で実行する場合のシステム要件 (続き)

データベース	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g リリース 2 (11.2.0.1、11.2.0.2、またはそれ以降)
データベース・クライアント	• DB2 クライアント v11.1 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c クライアント (接続先が Oracle 12c の場合) • Oracle 11g リリース 2 クライアント (接続先が Oracle 11g リリース 2 の場合)
Java Database Connectivity (JDBC) Clients (構成コンソールおよび **Visualizer** 用**)**	• DB2 クライアント v11.1 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c JDBC ドライバー (接続先が Oracle 12c の場合) • Oracle 11g JDBC ドライバー (接続先が Oracle 11g の場合)
Web ブラウザー	• Mozilla Firefox
サポートされるメッセージ・キューイング・ソフトウェア	• IBM WebSphere MQ

Linux x86 で実行する場合のシステム要件

以下に、Linux x86 オペレーティング・システム上で IBM InfoSphere Identity Insight を実行するときにサポートされる製品をリストします。

表 *15. Linux x86* で実行する場合のシステム要件

オペレーティング・システム	• Red Hat Enterprise Linux AS バージョン 6.0 • Red Hat Enterprise Linux AS バージョン 5.0 • Novell SUSE Linux Enterprise Server バージョン 10

表 *15. Linux x86* で実行する場合のシステム要件 (続き)

ハードウェア要件	• Intel x86 (IA32)
Java	以下のものが、この製品とともにインストールされます。 • IBM 32 ビット Runtime Environment for Linux on Intel architecture、Java Technology Edition バージョン 6
クライアント **Java** 要件	構成コンソールまたは Visualizer に接続されている、サポートされるプラットフォームのそれぞれのクライアント・マシンには、SUN Java SE Runtime Environment (JRE) バージョン 6 がインストールされている必要があります。
データベース	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g リリース 2 (11.2.0.1、11.2.0.2、またはそれ以降)
データベース・クライアント	• DB2 クライアント v11.1 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c クライアント (接続先が Oracle 12c の場合) • Oracle 11g リリース 2 クライアント (接続先が Oracle 11g リリース 2 の場合)
Java Database Connectivity (JDBC) Clients (構成コンソールおよび **Visualizer** 用**)**	• DB2 クライアント v11.1 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c JDBC ドライバー (接続先が Oracle 12c の場合) • Oracle 11g JDBC ドライバー (接続先が Oracle 11g の場合)
Web ブラウザー	• Mozilla Firefox
サポートされるメッセージ・キューイング・ソフトウェア	• IBM WebSphere MQ

Linux for System x 上で実行する場合のシステム要件

以下に、Linux for System x オペレーティング・システム上で IBM InfoSphere Identity Insight を実行するときにサポートされる製品をリストします。

表 16. *Linux for System x* 上で実行する場合のシステム要件

オペレーティング・システム	• Red Hat Enterprise Linux AS バージョン 7.0 • Red Hat Enterprise Linux AS バージョン 6.0
ハードウェア要件	• Intel x86_64
Java	以下のものが、この製品とともにインストールされます。 • IBM 64 ビット Java ランタイム環境、バージョン 8
データベース	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g リリース 2 (11.2.0.1、11.2.0.2、またはそれ以降)
データベース・クライアント	• DB2 クライアント v11.1 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c クライアント (接続先が Oracle 12c の場合) • Oracle 11g リリース 2 クライアント (接続先が Oracle 11g リリース 2 の場合)
Java Database Connectivity (JDBC) クライアント	• DB2 クライアント v11.1 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c JDBC ドライバー (接続先が Oracle 12c の場合) • Oracle 11g JDBC ドライバー (接続先が Oracle 11g の場合)
Web ブラウザー	• Mozilla Firefox

表 16. *Linux for System x* 上で実行する場合のシステム要件 (続き)

サポートされるメッセージ・キューイング・ソフトウェア	• IBM WebSphere MQ

Linux for System z 上で実行する場合のシステム要件

以下に、64 ビットの Linux for System z® オペレーティング・システム上で IBM InfoSphere Identity Insight を実行するときにサポートされる製品をリストします。

表 17. *System z* 上で *64* ビット *Linux* を実行する場合のシステム要件

オペレーティング・システム	• Red Hat Enterprise Linux AS バージョン 7.0
ハードウェア要件	• IBM System z
Java	以下のものが、この製品とともにインストールされます。 • IBM 64 ビット Java ランタイム環境、バージョン 8
データベース	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g リリース 2 (11.2.0.1、11.2.0.2、またはそれ以降)
データベース・クライアント	• DB2 クライアント v11.1 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracale 10g リリース 2 (10.2.0.2.0) クライアント (Oracle 11g リリース 1 (11.2.0.1) または 11g リリース 2 (11.2.0.2) に接続されている場合)

表 17. *System z* 上で *64* ビット *Linux* を実行する場合のシステム要件 (続き)

Java Database Connectivity (JDBC) クライアント	• DB2 クライアント v11.1 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracale 10g リリース 2 (10.2.0.2.0) クライアント (Oracle 11g リリース 1 (11.2.0.1) または 11g リリース 2 (11.2.0.2) に接続されている場合)
Web ブラウザー	• Mozilla Firefox
サポートされるメッセージ・キューイング・ソフトウェア	• IBM WebSphere MQ

Sun Solaris で実行する場合のシステム要件

以下に、Sun Solaris オペレーティング・システム上で IBM InfoSphere Identity Insight を実行するときにサポートされる製品をリストします。

表 18. *Sun Solaris* で実行する場合のシステム要件

オペレーティング・システム	• Sun Solaris 10.0
ハードウェア要件	• UltraSPARC T2 • UltraSPARC IV 以降
Java	以下のものが、この製品とともにインストールされます。 • IBM 64 ビット Java Runtime Environment for Solaris、Java Technology Edition バージョン 6
クライアント **Java** 要件	構成コンソールまたは Visualizer に接続されている、サポートされるプラットフォームのそれぞれのクライアント・マシンには、SUN Java SE Runtime Environment (JRE) バージョン 6 がインストールされている必要があります。
データベース	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g リリース 2 (11.2.0.1、11.2.0.2、またはそれ以降)

表 *18. Sun Solaris* で実行する場合のシステム要件 (続き)

データベース・クライアント	• DB2 クライアント v11.1 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c クライアント (接続先が Oracle 12c の場合) • Oracle 11g リリース 2 クライアント (接続先が Oracle 11g リリース 2 の場合)
Java Database Connectivity (JDBC) Clients (構成コンソールおよび **Visualizer** 用**)**	• DB2 クライアント v11.1 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c JDBC ドライバー (接続先が Oracle 12c の場合) • Oracle 11g JDBC ドライバー (接続先が Oracle 11g の場合)
Web ブラウザー	• Mozilla Firefox
サポートされるメッセージ・キューイング・ソフトウェア	• IBM WebSphere MQ
その他のソフトウェア	• GNU Compiler Collection、gcc (または gcc_small) バージョン 3.3.2 パッケージ。

Microsoft Windows Server で実行する場合のシステム要件

以下に、Microsoft Windows Server (64 ビット) オペレーティング・システム上で IBM InfoSphere Identity Insight を実行するときにサポートされる製品をリストします。

表 *19. Microsoft Windows Server* で実行する場合のシステム要件

オペレーティング・システム	• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 R2
ハードウェア要件	• Intel x86_64
Java	以下のものが、この製品とともにインストールされます。 • IBM 64 ビット Java ランタイム環境、バージョン 8

表 19. *Microsoft Windows Server* で実行する場合のシステム要件 (続き)

データベース	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g リリース 2 (11.2.0.1、11.2.0.2、またはそれ以降)
データベース・クライアント	• DB2 クライアント v11.1 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c クライアント (接続先が Oracle 12c の場合) • Oracle 11g リリース 2 クライアント (接続先が Oracle 11g リリース 2 の場合)
Java Database Connectivity (JDBC) クライアント	• DB2 クライアント v11.1 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 11.1 の場合) • DB2 クライアント v10.5 JDBC ドライバー (接続先が IBM DB2 Database for Linux, UNIX, and Windows 10.5 の場合) • Oracle 12c JDBC ドライバー (接続先が Oracle 12c の場合) • Oracle 11g JDBC ドライバー (接続先が Oracle 11g の場合)
Web ブラウザー	• Windows Internet Explorer 10 以上 • Mozilla Firefox
サポートされるメッセージ・キューイング・ソフトウェア	• IBM WebSphere MQ

システム体系の定義

製品のインストールでは、データベース構成とサーバー構成の計画を練る必要があります。

製品データベース構成

IBM InfoSphere Identity Insight のインストール済み環境には、製品構成用およびエンティティー・データ・ストレージ用に、最大 3 個の別個のデータベースを含めることができます。

データベースは以下のとおりです。

エンティティー・データベース
: アイデンティティーおよび エンティティーに加え、関係、解決、およびアラートに使用されるデータを格納するデータベース。

構成コンソール・データベース
: 構成コンソールのリソースを格納するデータベース

アプリケーション・モニター・データベース
: パイプラインのルーティングおよびモニタリング情報を格納するデータベース。

新規のインストールでは、インストールするフィーチャー次第で、複数のデータベースを単一のデータベースに統合できます。データベース統合のオプションは、インストール・プログラムのそれぞれのデータベース構成画面にあります。単一のデータベースが推奨される構成です。

パイプライン・デプロイメント

パイプラインは、システム要件およびサーバー・リソースに応じて、単一のサーバーや複数のサーバーにインストールできます。

パイプラインをデプロイする場合、以下のパフォーマンス要因を検討してください。

- パイプラインは、単一形式で実行できます。または、同時並列処理スレッドを実行するように構成できます。
- 各 CPU は、1.5 から 2 のパイプラインを処理することも、並列処理パイプライン・スレッドを処理することもできます。
- 並列処理パイプラインは、一度に複数のデータ・ソースからデータを受信できます。したがって、単一パイプラインの数と同じになるようにファイルを手動で分割する必要はありません。

パイプラインをデプロイする場合、以下の要因も検討してください。

- パイプラインは、サポートされているすべてのハードウェアおよびオペレーティング・システム構成で実行できます。
- 可能ではありますが、データベースが存在するマシン上でパイプラインを実行しないでください。
- 並列処理パイプラインの構成は、複数のパイプラインの場合よりも少ない作業で済みます。
- 複数サーバー構成では、管理のためにより多くの作業と保守が必要です。
- 単一サーバー構成では、CPU 数に伴って指数関数的に増加する高価なハードウェアが必要です。

Windows 以外のインストール済み環境での保護ユーザーの作成

すべての Windows 以外のプラットフォームの場合、製品のインストール・プログラムを実行する保護ユーザーを作成します。

このタスクについて

root ユーザーとして、製品のインストール・プログラムを実行しないでください。

ユーザー・ロールと責任

ユーザー・ロールは、IBM InfoSphere Identity Insight を効率的にデプロイして使用するために完了する必要のある一般的なタスクを分類するのに役立ちます。さまざまなタイプのユーザーが IBM InfoSphere Identity Insight をさまざまな目的で使用する可能性があります。すなわち、ユーザーは、製品の使用において、1 つ以上のロールの責任を引き受けます。

さまざまなユーザー・ロールと責任に基づいて、ユーザーのグループを定義できます。

最も一般的なユーザー・ロールを以下に示します。

アナリスト
: データを分析し、エンティティー、関係、およびアラートをレビューします。アナリストは、何が最も重要な結果であるかを定義し、システムがそのような結果を返すようにします。アナリストはオペレーターおよびアプリケーション・アドミニストレーターと密接に連携します。

オペレーター
: 必要に応じてロード品質レポートを提供しながら、システムにデータをロードし、パイプラインを実行し、システムが許容できる状態で稼働していることを確認します。オペレーターはまた、結果、例外、およびイベントをレビューします。オペレーターは、アナリスト、データ・ソース・アドミニストレーター、およびアプリケーション・アドミニストレーターと密接に連携します。

データ・ソース・アドミニストレーター
: データをシステムにロードできるよう、データの準備をします。これには、データの UMF ファイルへの変換とそのファイルの検証が含まれます。データ・ソース・アドミニストレーターは、オペレーター、アプリケーション・アドミニストレーター、およびデータベース・アドミニストレーターと密接に連携します。

アプリケーション・アドミニストレーター
: アプリケーションを構成します。これには、データ、エンティティー・モデル、およびルールの構成が含まれます。アプリケーション・アドミニストレーターは、データ・ソース・アドミニストレーターおよびオペレーターと密接に連携してエンティティー・モデルを定義するとともに、データベース・アドミニストレーター、データ・ソース・アドミニストレーター、およびオペレーターと構成変更について調整します。また、アプリケーション・アドミニストレーターは、総合的なシステム・アドミニストレーター (存在する場合) との調整および協議も行います。

データベース・アドミニストレーター
: データベースを適切に構成および調整して、アプリケーションで使用できる

ようにします。データベース・アドミニストレーターは、オペレーター、データ・ソース・アドミニストレーター、およびアプリケーション・アドミニストレーターと密接に連携します。

システム・アーキテクト
: アプリケーションのデプロイメント計画において、ハードウェア要件およびソフトウェア要件の規模を判定し、工数を見積もります。システム・アーキテクトは、インストール担当者、データベース・アドミニストレーター、データ・ソース・アドミニストレーター、およびアプリケーション・アドミニストレーターと密接に連携して、デプロイメントにより構想、戦略、および目標が達成され、期待どおりの結果を提供しながらデプロイメントがビジネス・プロセスに確実に統合されるようにします。

インストール担当者
: アプリケーションのインストールおよび初期構成を管理します。システムの初期ユーザーをセットアップするのも、インストール担当者です。多くの場合、IBM プロフェッショナル・サービスがシステム・アーキテクトと協力して、これらの責任を果たします。

プログラマー
: アプリケーションのデプロイメントがシームレスに環境に統合されるように、グラフィカル・インターフェースの設計および開発や、さまざまな機能に合わせたグラフィカル・インターフェースのカスタマイズを行います。プログラマーは、システム・アーキテクトおよびアプリケーション・アドミニストレーターと密接に連携します。また、適切な関係者に対して、その環境において最も効果的な方法でアラートの周知に努めることもよくあります。

セキュリティー・アーキテクト
: プロジェクト・チームがセキュアなシステムを計画し、実装するようにします。セキュリティー・アーキテクトは、システム・アーキテクト、インストール担当者、およびデータベース・アドミニストレーターと密接に連携します。

第 3 章 データベースのセットアップ

製品をインストールする前に、必要なデータベースをセットアップする必要があります。

環境変数の設定

DB2 データベースまたは Oracle データベースの場合は、環境変数を設定する必要があります。

DB2 環境変数

ターゲット・マシン上で、ご使用のオペレーティング・システムに必要な以下のすべての環境変数を設定してください。

AIX 環境変数

注**:** これらの環境変数値は、同じ環境変数の既存のエントリーがあれば、必ずその前に付加する必要があります。

すべての環境変数を大文字にする必要があります。

表 *20. DB2* データベースに関する *AIX* 環境変数

環境変数	値	条件
DB2DIR	DB2 ソフトウェア・インストール・パス	*DB2DIR* は DB2 クライアント/サーバー・ソフトウェアのインストール場所です。
DB2INSTANCE	DB2 データベース・インスタンス名	*DB2INSTANCE* は作成済みの DB2 データベース・インスタンスの名前です。
LIBPATH	$*DB2DIR*/lib64: *INSTALLDIRECTORY*/lib	*DB2DIR* は DB2 クライアント/サーバー・ソフトウェアのインストール場所、*INSTALLDIRECTORY* は製品がインストールされる予定の場所です。

Linux 環境変数

表 *21. DB2* データベースに関する *Linux* 環境変数

環境変数	値	条件
DB2DIR	DB2 ソフトウェア・インストール・パス	*DB2DIR* は DB2 クライアント/サーバー・ソフトウェアのインストール場所です。
DB2INSTANCE	DB2 データベース・インスタンス名	*DB2INSTANCE* は作成済みの DB2 データベース・インスタンスの名前です。

表 21. DB2 データベースに関する Linux 環境変数 (続き)

環境変数	値	条件
LD_LIBRARY_PATH	$*DB2DIR*/lib64: *INSTALLDIRECTORY*/lib	*DB2DIR* は DB2 クライアント/サーバー・ソフトウェアのインストール場所、*INSTALLDIRECTORY* は製品がインストールされる予定の場所です。

Microsoft Windows 環境変数

Microsoft Windows 環境で環境変数をセットアップするときには、Microsoft Windows の 8.3 命名規則を使用する必要があります。環境変数にはスペースを含めないでください。

表 22. DB2 データベースに関する Microsoft Windows 環境変数

環境変数	値	条件
DB2DIR	DB2 ソフトウェア・インストール・パス	ここで *DB2DIR* は、DB2 インスタンスが作成された場所です。DB2 の一部のバージョンでは、*DB2_HOME* または *DB2PATH* と設定されることがあります。*DB2DIR* が見つからない場合、インストーラーはそれらを探します。
DB2INSTANCE	DB2 データベース・インスタンス名	*DB2INSTANCE* は作成済みの DB2 データベース・インスタンスの名前です。
DB2CODEPAGE	DB2 データベースの CODEPAGE 値と同じに設定します。	一致しない場合、データ・ロード時に Latin-1/UTF-8 データに関してエンコードの問題が生じる可能性があります。

Oracle 環境変数

ターゲット・マシン上で、ご使用のオペレーティング・システムに必要な以下のすべての環境変数を設定してください。

注: これらの環境変数値は、同じ環境変数の既存のエントリーがあれば、必ずその前に付加する必要があります。

すべての環境変数を大文字にする必要があります。

AIX 環境変数

表 23. *Oracle* データベースに関する *AIX* 環境変数

環境変数	値	条件
ORACLE_HOME	Oracle クライアント・ソフトウェアのインストール・ディレクトリー	*ORACLE_HOME* は Oracle クライアント・ソフトウェアがインストールされている場所です。
LIBPATH	$*ORACLE_HOME*/lib:<*product install directory*>/lib	*ORACLE_HOME* は Oracle クライアント・ソフトウェアのインストール・ディレクトリー、<*product_install_directory*> は製品がインストールされる予定の場所です。

Linux 64 ビット環境変数

表 24. *Oracle* データベースに関する *Linux 64* ビット環境変数

環境変数	値	条件
ORACLE_HOME	Oracle クライアント・ソフトウェアのインストール・ディレクトリー	*ORACLE_HOME* は Oracle クライアント・ソフトウェアがインストールされている場所です。
LD_LIBRARY_PATH	$*ORACLE_HOME*/lib:<*product install directory*>/lib	*ORACLE_HOME* は Oracle クライアント・ソフトウェアのインストール・ディレクトリー、<*product_install_directory*> は製品がインストールされる予定の場所です。

Microsoft Windows 環境変数

Microsoft Windows 環境で環境変数をセットアップするときには、Microsoft Windows の 8.3 命名規則を使用する必要があります。環境変数にはスペースを含めないでください。

表 25. *Oracle* データベースに関する *Microsoft Windows* 環境変数

環境変数	値	条件
ORACLE_HOME	Oracle クライアント・ソフトウェアのインストール・ディレクトリー	*ORACLE_HOME* は Oracle クライアント・ソフトウェアがインストールされている場所です。

Microsoft SQL Server 環境変数

ターゲット・マシン上で、ご使用のオペレーティング・システムに必要な以下のすべての環境変数を設定してください。

Microsoft Windows 環境変数

Microsoft Windows 環境で環境変数をセットアップするときには、Microsoft Windows の 8.3 命名規則を使用する必要があります。環境変数にはスペースを含めないでください。

表 *26. Microsoft SQL Server* データベースに関する *Microsoft Windows* 環境変数

環境変数	値	条件
MSSQL_JDBC	Microsoft JDBC ドライバーの場所。	ここで、*MSSQL_JDBC* は Microsoft JDBC ドライバーと `.jar` ファイルが置かれているサーバー上の場所です。このパスは、製品インストーラーによって使用されます。

Microsoft SQL Server での ODBC DSN の設定

Microsoft SQL Server ODBC DSN (データ・ソース名) は、Microsoft SQL Server データベース名と正確に一致する値に設定する必要があります。

このタスクについて

DSN の接続タイプは、Microsoft SQL Server に構成されている認証メカニズム (OS ユーザー認証または SQL Server 認証) に応じてセットアップする必要があります。

Microsoft SQL Server での XA トランザクションの有効化

構成コンソールと Visualizer を正しく実行するためには、XA トランザクションを有効にする必要があります。

手順

1. Windows のコンポーネント・サービス管理ツールを使用して、XA トランザクションを有効にします。
2. Microsoft SQL Server デスクトップを使用して、分散トランザクション・コーディネーター・サービスを実行します。
3. Java Transaction API (JTA) ストアード・プロシージャーを、該当する Microsoft SQL Server の資料に記載されているようにインストールします。
4. Microsoft SQL Server Enterprise Manager を使用して、ユーザーが Java Transaction API (JTA) ストアード・プロシージャーを実行するためのアクセス権を設定します。

Oracle ユーザーへの CREATE VIEW 特権の付与

製品が正しく実行されるようにするには、Oracle データベース・ユーザーに CREATE VIEW 特権を付与する必要があります。

このタスクについて

CREATE VIEW 特権は、ロールに基づいて割り当てるのではなく、ユーザーに対して直接割り当てる必要があります。

データベースの作成および構成

製品のすべてのコンポーネントが使用する、エンティティー・データベースとも呼ばれる単一のデータベースを作成します。

エンティティー・データベースの作成

アイデンティティー、エンティティー、関係、およびアラートを保管するだけでなく、構成コンソール構成情報とアプリケーション・モニター情報も保管するパイプライン用のデータベースを作成する必要があります。

このタスクについて

新規データベースを作成する手順については、ご使用のデータベースの資料を参照してください。

データベース名には大文字を使用してください。

クライアント認証の構成

クライアント認証を使用すると、パイプラインの `.ini` ファイルで追加のユーザー名やパスワードの資格情報を提供しなくとも、ユーザーはエンティティー・データベースに接続できます。

このタスクについて

クライアント認証は、トラステッド OS データベース認証とも呼ばれます。クライアント認証を使用すると、現在ログインしているユーザー名を使用して接続を作成できます。この認証スキームは、オペレーティング・システムが既にそのユーザーを正しく認証していることを信頼するものです。クライアント認証は、DB2 および Oracle の各データベース・プラットフォームで使用できます。パイプラインおよび IBM WebSphere 処理は、エンティティー・データベースにトラステッド・モードでアクセスできる OS ユーザーが実行する必要があります。複数のユーザーがそれらの処理を実行する必要がある場合は、詳細について IBM サポートにお問い合わせください。

DB2 データベースでのクライアント認証の構成

クライアント認証を使用するよう、DB2 をセットアップします。

手順

1. 以下のグローバル・データベース・サーバー構成オプションを設定します。
   a. **`authentication`** の値を `client` に設定します。
   b. **`trust_allclnts`** の値を `yes` に設定します。
   c. **`trust-clntauth`** の値を `server` に設定します。

2. **db2 catalog database** コマンドの **authentication client** パラメーターを使用して、製品データベースをカタログします。
3. オペレーティング・システムと DB2 データベースのユーザー名を同期化します。
4. 標準 DB2 JDBC Type 4 ドライバーのほかに、DB2 JDBC Type 2 ドライバーもあることを確認します。 これは、db2java.zip ファイルに含まれています。
5. 製品をインストールする際に、トラステッド認証を有効にします。

Oracle データベースでのクライアント認証の構成

クライアント認証を使用するよう、Oracle をセットアップします。

手順

1. 以下のグローバル・データベース・サーバー構成オプションを設定します。
   a. **os_authent_prefix** の値を OPS$ に設定します。
   b. **remote_os_authent** の値を TRUE に設定します。
2. Oracle データベース・ユーザーを、そのユーザーが外部認証方式とデータベース認証方式の両方を使用できるように作成します。 構文例:

```
CREATE USER OPS$<user> IDENTIFIED BY <dbpassword> DEFAULT
TABLESPACE <tablespace> TEMPORARY TABLESPACE <temp-tablespace>
QUOTA UNLIMITED ON <tablespace>;
GRANT CONNECT, RESOURCE TO OPS$<user>;
```

3. 標準 Oracle JDBC Type 4 ドライバーのほかに、Oracle JDBC Type 2 ドライバーもあることを確認します。 Oracle の場合、これは ojdbc16.zip ファイルに含まれています。
4. 製品をインストールする際に、トラステッド認証を有効にします。 製品インストーラーでデータベース資格情報を要求されたときは、OPS$ プレフィックスを付けたユーザー名を指定します。

Microsoft SQL Server データベースでのクライアント認証の構成

クライアント認証を使用するよう、Microsoft SQL Server をセットアップします。

手順

1. システム DSN が、SQL Server 認証でなく、必ず Windows NT 認証を使用するようにします。または、Windows NT 認証を使用して、新規のシステム DSN を作成します。
2. データベース・アドミニストレーター・ユーザーが Microsoft SQL Server Enterprise Manager に存在することを確認します。 各製品データベースのアドミニストレーターに、少なくとも public および db_owner のデータベース・アクセス権を付与します。デフォルトのデータベースをエンティティー・データベースに設定します。
3. Type 1 の ODBC ブリッジ JDBC ドライバーがあることを確認します。
4. エンティティー・データベースにアクセスできるデータベース・ユーザー (非オペレーティング・システム) を作成します。
5. 製品をインストールする際に、トラステッド認証を有効にします。 製品インストーラーでデータベース資格情報を要求されたときは、データベース・ユーザー (非オペレーティング・システム) を使用します。

Oracle ステートメント・キャッシュのサイズ変更

Oracle データベース・アドミニストレーターは、ステートメント・キャッシュを適切にサイズ変更する必要があります。

このタスクについて

本製品はステートメントを集中的に使用する可能性があります。このため、Oracle ステートメント・キャッシュが急速に増大し、デフォルトの Oracle データベース設定を超える場合があります。それらのパラメーターのサイズ変更とチューニングについて詳しくは、ご使用の Oracle の資料を参照してください。

手順

Oracle の **ALTER SYSTEM SET** コマンドを使用して、以下のパラメーターをサーバー・レベルで構成します。

SESSION_CACHED_CURSORS
このパラメーターに適した値は、パイプライン・スレッド当たり、または並列処理パイプライン・スレッド当たり約 20 個の同時カーソルです。

OPEN_CURSORS
このパラメーターに適した値は、パイプライン・スレッド当たり、または並列処理パイプライン・スレッド当たり約 20 個の同時カーソルです。

CURSOR_SHARING
このパラメーターは、パフォーマンスに大きく影響します。このパラメーターは、製品がバインド変数を幅広く使用し、アプリケーションはカーソル共有から大きな恩恵を受けるという事実に基づいて構成してください。

第 4 章 管理

管理タスクには、ユーザー・インターフェースに関するシステム設定の構成と保守、グローバル構成設定の更新などがあります。アドミニストレーターは、構成コンソールを使用して管理用タスクを実行します。

コンソールの管理

コンソールを効果的に使用するためには、ブラウザーの構成、該当ユーザーのアカウントのセットアップ、およびコンソールへのアクセスの管理を行う必要があります。

構成コンソール

構成コンソールはタスク指向のインターフェースを提供し、Identity Insight を稼働させる上で最も不可欠なタスクの一部をより簡単に行えるよう支援します。

構成コンソールは、IBM WebSphere Liberty によってホストされます。

システム構成の管理

構成コンソールを使用して、ほとんどのシステム・パラメーターおよびオプションを、簡素化かつ能率化された一連のインターフェースで構成します。その後、コンソールによって変更内容が構成データベースに書き込まれます。構成データベースを直接変更することはサポートされていません。そのような変更を行うと、ほとんどの場合、製品が適切に機能しなくなります。

ユーザー・ロールと責任

ユーザー・ロールは、IBM InfoSphere Identity Insight を効率的にデプロイして使用するために完了する必要のある一般的なタスクを分類するのに役立ちます。さまざまなタイプのユーザーが IBM InfoSphere Identity Insight をさまざまな目的で使用する可能性があります。すなわち、ユーザーは、製品の使用において、1 つ以上のロールの責任を引き受けます。

さまざまなユーザー・ロールと責任に基づいて、ユーザーのグループを定義できます。

最も一般的なユーザー・ロールを以下に示します。

アナリスト
: データを分析し、エンティティー、関係、およびアラートをレビューします。アナリストは、何が最も重要な結果であるかを定義し、システムがそのような結果を返すようにします。アナリストはオペレーターおよびアプリケーション・アドミニストレーターと密接に連携します。

オペレーター
: 必要に応じてロード品質レポートを提供しながら、システムにデータをロードし、パイプラインを実行し、システムが許容できる状態で稼働しているこ

とを確認します。オペレーターはまた、結果、例外、およびイベントをレビューします。オペレーターは、アナリスト、データ・ソース・アドミニストレーター、およびアプリケーション・アドミニストレーターと密接に連携します。

データ・ソース・アドミニストレーター
: データをシステムにロードできるよう、データの準備をします。これには、データの UMF ファイルへの変換とそのファイルの検証が含まれます。データ・ソース・アドミニストレーターは、オペレーター、アプリケーション・アドミニストレーター、およびデータベース・アドミニストレーターと密接に連携します。

アプリケーション・アドミニストレーター
: アプリケーションを構成します。これには、データ、エンティティー・モデル、およびルールの構成が含まれます。アプリケーション・アドミニストレーターは、データ・ソース・アドミニストレーターおよびオペレーターと密接に連携してエンティティー・モデルを定義するとともに、データベース・アドミニストレーター、データ・ソース・アドミニストレーター、およびオペレーターと構成変更について調整します。また、アプリケーション・アドミニストレーターは、総合的なシステム・アドミニストレーター (存在する場合) との調整および協議も行います。

データベース・アドミニストレーター
: データベースを適切に構成および調整して、アプリケーションで使用できるようにします。データベース・アドミニストレーターは、オペレーター、データ・ソース・アドミニストレーター、およびアプリケーション・アドミニストレーターと密接に連携します。

システム・アーキテクト
: アプリケーションのデプロイメント計画において、ハードウェア要件およびソフトウェア要件の規模を判定し、工数を見積もります。システム・アーキテクトは、インストール担当者、データベース・アドミニストレーター、データ・ソース・アドミニストレーター、およびアプリケーション・アドミニストレーターと密接に連携して、デプロイメントにより構想、戦略、および目標が達成され、期待どおりの結果を提供しながらデプロイメントがビジネス・プロセスに確実に統合されるようにします。

インストール担当者
: アプリケーションのインストールおよび初期構成を管理します。システムの初期ユーザーをセットアップするのも、インストール担当者です。多くの場合、IBM プロフェッショナル・サービスがシステム・アーキテクトと協力して、これらの責任を果たします。

プログラマー
: アプリケーションのデプロイメントがシームレスに環境に統合されるように、グラフィカル・インターフェースの設計および開発や、さまざまな機能に合わせたグラフィカル・インターフェースのカスタマイズを行います。プログラマーは、システム・アーキテクトおよびアプリケーション・アドミニストレーターと密接に連携します。また、適切な関係者に対して、その環境において最も効果的な方法でアラートの周知に努めることもよくあります。

セキュリティー・アーキテクト
: プロジェクト・チームがセキュアなシステムを計画し、実装するようにしま

す。セキュリティー・アーキテクトは、システム・アーキテクト、インストール担当者、およびデータベース・アドミニストレーターと密接に連携します。

構成コンソールを使用するための最適なブラウザー設定

構成コンソールは Web ベース・アプリケーションです。構成コンソールへのアクセスに使用するブラウザーは、特定の設定になっている必要があります。

構成コンソールの表示を最適にするには、以下のブラウザー設定を使用します。

表 27. 最適なブラウザー設定

設定	値	説明
解像度	最小 800 x 600、1024 x 768 以上を推奨	
文字サイズ	中	
JavaScript	オン	
Cookie	オン	少なくとも、ファースト・パーティーのセッション Cookie を有効にする必要があります。
セキュリティー: 信頼できる Web サイト	構成コンソールの HTTP アドレス	構成コンソールの HTTP アドレスが、信頼されたインターネット Web サイトのリストに含まれていることを確認します。
セキュリティー: ダウンロード・オプション	「有効 (Enabled)」	信頼されたインターネット Web サイト向けのダウンロード・オプションはすべて有効になっていることを確認します。
ポップアップ・ブロッカー	構成コンソールの HTTP アドレスからのポップアップを許可	構成コンソールの HTTP アドレスが、ポップアップが許可された Web サイトのリストに含まれていることを確認します。

構成コンソールへのログイン

構成コンソールにログインすることで、システム構成設定を表示したり変更したりできます。

始める前に

ログインに使用するユーザー・アカウントが、既にシステム・アドミニストレーターによって作成されていることが必要です。

手順

1. 次の手順で、構成コンソールを開きます。
   a. 構成コンソールを実行するブラウザーを開きます。

b. 次の構文を使用して、構成コンソールの URL を入力します。
`http://<servername>/console/`
c. **Enter** キーを押します。

2. 「ログイン **(Login)**」ウィンドウで、ユーザー名とパスワードを入力します。
3. オプション: システム・アドミニストレーターであり、かつ現在のシステム構成を編集する必要がある場合は、「構成の編集 **(Edit Configuration)**」オプションを選択します。 現在のシステム構成を編集する場合、通常、構成変更が完了するまで新規データが処理されないようにするため、すべてのパイプラインを停止する必要があります。
4. 「ログイン **(Login)**」ボタンをクリックします。

次のタスク

ユーザー名とパスワードが、構成コンソール用にセットアップされたものと一致すると、構成コンソールが開きます。一致しないと、エラーが発生します。この場合、適切なユーザー名とパスワードを判別後、再度ログインする必要があります。

構成コンソールからのログアウト

アプリケーションを終了せずに、現在の構成コンソール・セッションからログアウトできます。60 分間アクティビティーがないと、現行ユーザーは自動的に構成コンソールからログアウトされます。

手順

構成コンソール・ウィンドウの右上隅にある「サインオフ **(Sign off)**」をクリックします。

次のタスク

構成コンソール・セッションからログアウトされました。引き続き構成コンソールを使用するには、再度ログインする必要があります。

構成コンソール用のユーザー・アカウント

構成コンソールにログインするには、システム・アドミニストレーターが作成したユーザー・アカウントを受け取ります。ユーザー・アカウントに含まれているユーザー名とパスワードは、ユーザーが変更できます。

同じユーザー・アカウントを使用して複数回ログインすることはできません。ユーザー・アカウントを別のユーザーと共有している場合、そのユーザーと同時に構成コンソールにログインすることはできません。別のユーザーが現在使用しているユーザー・アカウントを使用してログインを試行すると、その別のユーザーのセッションが強制終了して、自分のセッションが開始されることになります。

システム・アドミニストレーターは、いつでも追加のユーザー・アカウントを作成することができます。さらにシステム・アドミニストレーターは、構成コンソールを再始動して、強制的にタイムアウトにすることができます。

構成コンソールへのアクセスの管理

構成コンソールのユーザー各人に、構成コンソールへのアクセス権限が与えられ、ユーザー各人がユーザー名とパスワードを使用して構成コンソールにログインする必要があります。構成コンソールに用意されているアプリケーション固有のファイルを使用して、ユーザー名とパスワードを管理することができます。または、エンティティー・データベースへのアクセスが許可された RDBMS ユーザー・アカウントをユーザーが持っている場合は、それらのユーザー・アカウントとデータベース管理ツールを使用して、構成コンソールへのユーザーのアクセスを管理することができます。これらのユーザー名およびパスワードは、Visualizer へのアクセス用に構成されるユーザー名およびパスワードとは区別され、必ずしも Visualizer 用のユーザー名およびパスワードと同じである必要はありません。

データベース・ログイン情報を使用した構成コンソールへのアクセスの管理

エンティティー・データベースと同じユーザー ID とパスワードを使用して、構成コンソールへのアクセスを管理することができます。

始める前に

構成の競合を防ぐため、構成コンソールに誰もログインしていないことを確認します。

手順

1. `<install location>/installer/util/` ディレクトリーに移動し、次のいずれかのコマンドを入力して、構成ユーティリティーを起動します。
   a. Windows の場合は、`eacfg.bat –i –l ../logs/` と入力します。
   b. UNIX の場合は、`eacfg –i –l ../logs/` と入力します。
2. ナビゲーション・ペインで、「構成コンソールの設定 **(Configuration Console Settings)**」をクリックします。
3. 「構成コンソール認証の変更 **(Modify Configuration Console Authentication)**」チェック・ボックスをクリックします。
4. 「**SQL 認証 (SQL authentication)**」ラジオ・ボタンをクリックします。
5. 「**OK**」をクリックします。
6. データベース管理ツールを使用して、構成コンソール (およびエンティティーデータベース) のログイン情報を指定します。

パスワード・マネージャー・ユーティリティーを使用した構成コンソールへのアクセスの管理

パスワード・マネージャー・ユーティリティーを使用して、構成コンソールへのアクセスを管理することができます。

始める前に

構成コンソールに誰もログインしていないことを確認します。

手順

1. <install location>/installer/util/ ディレクトリーに移動し、次のいずれかのコマンドを入力して、構成ユーティリティーを起動します。
   a. Windows の場合は、eacfg.bat –i –l ../logs/ と入力します。
   b. UNIX の場合は、eacfg –i –l ../logs/ と入力します。
2. ナビゲーション・ペインで、「構成コンソールの設定 **(Configuration Console Settings)**」をクリックします。
3. 「構成コンソール認証の変更 **(Modify Configuration Console Authentication)**」チェック・ボックスをクリックします。
4. 「ファイル認証 **(File Authentication)**」ラジオ・ボタンをクリックします。
5. 「**OK**」をクリックします。

タスクの結果

srd-home/console ディレクトリーに配置されているパスワード・マネージャー・ユーティリティー (pwdmgr.jar) を使用して、ユーザーの追加または削除や、console_password.properities ファイル内のユーザーのパスワードの再設定を行えるようになりました。

ユーザーとその状況のリストの表示**:**

パスワード・マネージャー・コマンドを使用して、ユーザーとその状況のリストを表示することができます。

手順

1. コマンド・ウィンドウで、¥srd-home¥console ディレクトリーに移動します。
2. 次のコマンドを入力します。 pwdmgr console-passwords.properties console-principals.properties -l

例

例えば、 pwdmgr console-passwords.properties console-principals.properties -l コマンドを入力した場合、次のような出力が表示されます。

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

最近パスワードを再設定した場合は、そのユーザーがまだ一度も新規パスワードで構成コンソールにログインしていないことを示すメッセージが表示されます。

新規ユーザーの追加**:**

構成コンソールへのアクセスを管理している場合は、パスワード・マネージャー・コマンドを使用して、 console-passwords.properties ファイルに新規ユーザーを追加できます。

手順

1. コマンド・ウィンドウで、¥srd-home¥console ディレクトリーに移動します。

2. コマンド `pwdmgr console-passwords.properties console-principals.properties -a username` を入力します。ここで、*username* は、追加するユーザー名です。

次のタスク

指定したユーザー名をデフォルト・パスワードとして持つユーザーが追加されます。この新規ユーザーは、構成コンソールにログインできるようになりました。

既存ユーザーの削除:

構成コンソールへのアクセスを管理している場合は、パスワード・マネージャー・コマンドを使用して、 console-passwords.properties ファイルから既存ユーザーを削除できます。

始める前に

`¥srd-home¥console¥` ディレクトリーからコマンドを実行できることを確認します。また、削除するユーザーが存在することを確認します。存在しないユーザーを削除しようとすると、エラーメッセージが返されます。

手順

1. コマンド・ウィンドウで、¥srd-home¥console ディレクトリーに移動します。
2. コマンド `pwdmgr console-passwords.properties console-principals.properties -d username` を入力します。ここで、*username* は、削除するユーザー名です。

次のタスク

ユーザー名が削除されたユーザーは、構成コンソールにログインできなくなります。

パスワードの再設定:

ユーザーが構成コンソール・アカウント用のパスワードを忘れた場合、あるいはセキュリティー上の目的からパスワードを変更する必要がある場合、システム・アドミニストレーターはパスワード・マネージャー・コマンドを使用してパスワードを再設定できます。

始める前に

`¥srd-home¥console¥` ディレクトリーからコマンドを実行できることを確認します。

手順

1. コマンド・ウィンドウで、`¥srd-home¥console` ディレクトリーに移動します。
2. コマンド `pwdmgr console-passwords.properties console-principals.properties -r username` を入力します。ここで、*username* は、パスワードの再設定の対象となるユーザーのユーザー名です。

次のタスク

指定したユーザー名のパスワードが、ユーザー名とマッチングするように再設定されました。パスワードが再設定された後、次回このユーザーが構成コンソールにログインしたときに、パスワードの再設定を求めるプロンプトが出されます。したがって、パスワードを再設定した後は、できるだけ迅速にログインとパスワードの変更を行ってセキュリティー上の懸念や問題を最小限にするよう、そのユーザーに推奨するとよいでしょう。

パスワード・マネージャー・コマンド:

パスワード・マネージャーコマンドを使用すると、プロパティー・ファイルを使用して構成コンソールへのアクセスを管理できます。ユーザーの追加、削除、およびリストと、ユーザーのパスワードの再設定を行うことができます。

パスワード・マネージャー・コマンドの構文は、次のとおりです。

```
pwdmgr -option parameter
```

パスワード・マネージャー・コマンドを使用するには、コマンドを ¥srd-home¥console¥ ディレクトリーから実行します。

オプションとパラメーター

パスワード・マネージャーのコマンドは、オプションおよびパラメーターごとに、それぞれ別々のコマンドとして指定する必要があります。オプションを指定しないと、コマンド・ヘルプが表示されます。

-a *username*
一度に 1 ユーザーを追加します。

指定した名前は、ユーザーの初期パスワードのデフォルト値になります。ユーザーは、構成コンソールへの最初のログイン時に、このパスワードを変更するよう、プロンプトが出されます。

既に存在するユーザーを追加すると、エラー・メッセージが表示されます。

-d *username*
一度に 1 ユーザーを削除します。

存在しないユーザーを削除しようとすると、エラーメッセージが表示されます。list オプションを使用してユーザーのリストを表示することで、当該ユーザーが正常に削除されたことを確認できます。

-l
すべてのユーザーとその状況のリストを表示します。

-r *username*
指定したユーザーのパスワードを、そのユーザーのユーザー ID に再設定します。例えば、judy/sunflower であれば judy/judy に再設定されます。

パスワード・マネージャー・コマンドで正常動作するファイルは、次の 2 つです。

- console-passwords.properties。このファイルには、すべてのユーザー名と、パスワードのメッセージ・ダイジェストが記録されます。

- console-principals.properties。このファイルは、将来的に異なるレベルのユーザーを作成する場合のために予約されています。現在、構成コンソールのユーザーはすべて、スーパーユーザーであると見なされ、構成コンソールのすべての領域にアクセスできます。

これらのファイルは、srd-home ディレクトリーに配置されています。ただし、これらのファイルを手動で変更しないでください。これらのファイルは、製品によるユーザー・ログインの追跡に使用されます。また、他の一部のコマンドで使用される必須パラメーターでもあります。

パスワード・マネージャー・コマンドの例

ログイン名およびデフォルト・パスワードがどちらも「judy」である新規ユーザーを追加するには、次のコマンドを入力します。 `pwdmgr -a judy`

judy という名前の既存ユーザー、および対応するパスワードを削除するには、次のコマンドを入力します。 `pwdmgr -d judy`

現行ユーザーとそれぞれの状況のリストを表示するには、次のコマンドを入力します。 `pwdmgr -l`

例えば、 `pwdmgr -l` コマンドを入力した場合、次のような出力が表示されます。

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

最近パスワードを再設定した場合は、そのユーザーがまだ一度も新規パスワードで構成コンソールにログインしていないことを示すメッセージが表示されます。

ユーザーのパスワードをそのユーザーのユーザー ID に再設定するには、次のコマンドを入力します。 `pwdmgr -r` *`username`*

例えば、 `pwdmgr -r judy` コマンドを入力した場合、judy という名前の既存ユーザーのパスワードが、デフォルト・パスワード「judy」に再設定されます。元のログイン/パスワードが judy/sunflower であったとすると、現在は judy/judy に再設定されています。

ヘルプ・トピック

構成コンソール・ログイン・ウィンドウ

このウィンドウを使用して、構成コンソールにログインします。

「ユーザー **ID (User ID)**」
　構成コンソール・ユーザー ID を入力します。

「パスワード **(Password)**」
　構成コンソール・パスワードを入力します。

「構成の編集 **(Edit Configuration)**」
　編集モードを使用するときに、このチェック・ボックスを選択します。

「ログイン **(Login)**」
ユーザー IDとパスワードを送信して構成コンソールにアクセスするときに、クリックします。

「クリア **(Clear)**」
ユーザー IDとパスワードの入力を削除し、「構成の編集 (Edit Configuration)」チェック・ボックスを選択解除するときに、クリックします。

構成コンソールからのレポートの実行

構成コンソールでは、データ・ソース別のパイプライン統計の集計を示すレポートや、現行のシステム構成設定 (エンティティー解決構成など) がリストされたレポートを生成できます。結果として得られるレポートは、Web ベースの BIRT (Business Intelligence Reporting Tool) レポート・ビューアーに表示されます。ポップアップ・ブロッカーがオンになっていると、ビューアーへのレポートの表示を妨げる可能性があります。そのため、ポップアップ・ブロッカーはすべてオフにしておいてください。

統計レポートの表示

データの処理と並行して、この製品は、ロードされた入力データ・ソース・ファイルのパフォーマンスとデータに関する統計情報を追跡します。この情報は、データ・ソース要約レポートおよびロード要約レポートという 2 つのレポートに要約されます。

このタスクについて

これらのレポートの統計によりユーザーは、製品がすべての入力データ・レコードを処理していることの確認、製品のパフォーマンスに関する運用上の意思決定、入力データの品質評価、データ・ファイルを処理した結果として生成された新規アイデンティティーの数、新規エンティティーの数、新規関係の数、および新規アラートの数の表示といったことを素早く行うことができます。

手順

1. 構成コンソールで、「状況 **(Status)**」 > 「レポート **(Reports)**」を選択します。
2. 必須: 「レポート **(Report)**」リストから、統計レポートを選択します。
   - 「データ・ソース要約レポート **(Data Source Summary Report)**」。このレポートには、統計の即時要約が、ロードされて処理されたレコードのデータ・ソース別に示されます。このレポートを使用して、ロードされたレコードのデータ・ソース・ファイル別の総数、処理された新規アイデンティティー・レコードのデータ・ソース・ファイル別の総数、およびこのデータ・ソース・ファイル内のデータに基づく新規エンティティーの総数を確認します。データ・ソース要約レポート (Data Source Summary Report) は、ロード日、ロード ID、データ・ソース、およびデータ・ソース・ファイルでソートされます。
   - 「ロード要約レポート **(Load Summary Report)**」。このレポートには、1 つ以上のデータ・ソースの統計および品質特性の要約が示されます。このレ

ポートを使用して、ロード・パフォーマンスの情報、データ・ソース・ファイルの品質、およびエンティティー解決に使用されたデータ値の要約についての確認、ならびに関係の検出およびアラートの生成を行います。このレポートは、特定のデータ・ソースからロードされているデータの品質の判別に役立ちます。データ品質が低い場合、このデータ・ソースのデータに対して追加のクレンジングが必要であることを示している可能性があります。追加のクレンジングは、製品に読み込まれる前に、あるいは特定の DQM (データ品質管理) ルールをデータに適用することによりエンティティー解決中に行います。ロード要約レポートはロード ID でソートされます。

3. 「開始日 **(From Date)**」フィールドに、mm/dd/yyyy 形式を使用して、レポートの開始日を入力します。 デフォルトでは、このフィールドには現在の日付が入力されています。

   このフィールドはブランクのままでもかまいません。ブランクにすると、製品は、製品が運用可能になった日付で始まる、指定された他のすべての基準の範囲内にあるデータをすべて報告します。

4. 「終了日 **(Thru Date)**」フィールドに、mm/dd/yyyy 形式を使用して、レポートの終了日を入力します。 デフォルトでは、このフィールドには現在の日付が入力されています。

   このフィールドはブランクのままでもかまいません。ブランクにすると、製品は、指定された他のすべての基準の範囲内にある、現在の日付までのデータをすべて報告します。

5. オプション: 「データ・ソース・コード **(Data Source Code)**」に、レポートの対象とする、特定のデータ・ソース・コードを入力します。 入力するデータ・ソース・コードは、構成済みデータ・ソース・コードと正確に一致している必要があります。

   このフィールドはブランクのままでもかまいません。ブランクにすると、製品は、指定された他のすべての基準の範囲内にある全データ・ソースの統計を報告します。

6. 必須: 「レポートの実行 **(Run Report)**」をクリックして、選択したレポートを生成します。

タスクの結果

選択した統計レポートが、指定したすべての基準に基づいて生成されます。生成されたレポートは、「**BIRT** レポート・ビューアー **(BIRT Report Viewer)**」という名前の、別の Web ブラウザー・ウィンドウに表示されます。選択した基準に基づき、報告するデータがない場合は、「**BIRT** レポート・ビューアー **(BIRT Report Viewer)**」ウィンドウの上部にレポート名、レポートの生成日時、および「ページ **1/1 (Page 1/1)**」が表示されます。データ・セクションはブランクです。

次のタスク

このレポートの統計情報を使用して、製品やデータ・ファイルの調整に役立てます。

「データ・ソース要約レポート (Data Source Summary Report)」

「データ・ソース要約レポート (Data Source Summary Report)」は、処理のためにシステムにロードされたレコードの簡潔な統計的要約をデータ・ソース別に提供します。このレポートから、処理されたレコードの合計数をロード ID 別に確認できます。レポートでは、ロードされた合計レコード数のうち、新規アイデンティティーまたは新規エンティティーを表していたレコード数が表示されるほか、新規アイデンティティーに該当したレコードのパーセンテージと、新しく作成されたエンティティーに該当したレコードのパーセンテージが計算されます。

データ・ソース内のロード別統計

「ロードされた日付 **(Date Loaded)**」
: このデータ・ソース・ファイルがロードされた日付が表示されます。

ロード **ID**
: システムによって割り当てられたロード ID 番号が表示されます。

データ・ソース
: ロードされたデータ・ソース・ファイルのデータ・ソース・コードと説明 (ダッシュで区切られています) が表示されます。

「ロードされた **UMF** レコード数 **(UMF Records Loaded)**」
: ロードされたこのデータ・ソース・ファイル内のアイデンティティー・レコードの総数を示します。

「新規アイデンティティー数 **(New Identities)**」
: ロードされたデータ・ファイルで発見された新しいアイデンティティーの総数を示します。(この数値は、以前にシステムによって処理されたことがないアイデンティティーの数を示します。)

「新規アイデンティティー **% (New Identity %)**」
: 新規アイデンティティーを表す、ロードされた合計レコード数のパーセンテージ (「新規アイデンティティー数 (New Identities)」を「ロードされた UMF レコード数 (UMF Records Loaded)」で除算した値) を示します。

「新規エンティティー数 **(New Entities)**」
: このデータ・ロードによって作成された新規エンティティーの総数を示します。

「新規エンティティー **% (New Entities %)**」
: 新規エンティティーを表す、ロードされた合計レコード数のパーセンテージ (「新規エンティティー数 (New Entities)」を「ロードされた UMF レコード数 (UMF Records Loaded)」で除算した値) を示します。

データ・ソース別の統計グラフ

「データ・ソース別のロードされたレコード数 **(Records Loaded by Data Source)**」
: 指定されたその他のレポート基準に基づいて、各データ・ソースからシステムにロードされたレコードの数をグラフィカルに示した棒グラフが表示されます。最も多くのレコードまたは最も少ないレコードを提供したデータ・ソースを確認し、予想していたロード数と比較できます。
  - 縦軸は、データ・ソース・コード別のデータ・ソース数を示します。
  - 横軸は、ロードされたレコードの数を示します。

特定のデータ・ソースでロードされたレコード数が予想より少ない場合、このデータ・ソースのデータ・ファイルを調べることができます。 (データ品質はロードされるレコード数に直接的に影響するため、「ロード要約レポート (Load Summary Report)」を実行して、このデータ・ソースでロードされたファイルのデータ品質を確認することも検討してください。)

「データ・ソース別の新規エンティティー数 **(New Entities by Data Source)**」
指定されたその他のレポート基準に基づいて、どのデータ・ソースが最も多い数の新規エンティティーを生成したかをグラフィカルに示した棒グラフが表示されます。

- 縦軸は、データ・ソース・コード別のデータ・ソース数を示します。
- 横軸は、作成された新規エンティティーの数を示します。

「ロード要約レポート (Load Summary Report)」

「ロード要約レポート (Load Summary Report)」には、データ・ソース別の統計および品質特性の要約が示されます。そこには、データ・ソース・ファイルに関する情報が含まれています。このレポートを使用して、ロード・パフォーマンスの統計、ロードによって作成されたエンティティーおよびアラートの数、ロードされたデータのデータ品質に関する一般情報、UMF レコードに関するアクションのロード別の要約、およびロードによって生成された UMF 例外を判定します。レポートはロード ID ごとにグループ化されます。

レポートでは、ロードごとに統計が以下のセクションに分割されます。

- 「ロード要約 (Load Summary)」
- 「ロール・アラート要約 (Role Alert Summary)」
- 「関係要約 (Relationship Summary)」
- 「品質要約 (Quality Summary)」
- 「UMF 文書要約 (UMF Document Summary)」
- 「例外要約 (Exception Summary)」

「ロード要約 (Load Summary)」

このセクションを使用して、特定のファイルの処理にかかった時間を判定できるほか、このデータ・ソース・ファイルがエンティティー解決および関係検出の全体にとって、どれくらい有効であったかを総合的に判断します。

「開始日時 **(Date and Time Started)**」
データ・ロードが開始された日時を示します。

「完了日時 **(Date and Time Completed)**」
データ・ソース・ファイルのロードが終了した日時を示します。

「**UMF** レコード・カウント **(UMF Record Count)**」
「開始日時 **(Date and Time Started)**」から「完了日時 **(Date and Time Completed)**」の範囲内にこのデータ・ソース・ファイルからロードされたレコードの総数を示します。

「完了日時 **(Date and Time Completed)**」の数値から「開始日時 **(Date and Time Started)**」の数値を引くと、この特定のデータ・ソース・ファイルをロードするのにかかった分数がわかります。この分数を見るとシステ

ム・パフォーマンスを推定できます。また、処理時間を短縮するために、大きいデータ・ソース・ファイルを小さいファイルに分割する必要があることを示唆している場合もあります。

「新規アイデンティティー数 **(New Identities)**」
「開始日時 **(Date and Time Started)**」から「完了日時 **(Date and Time Completed)**」の時間フレーム内でロードされた新規アイデンティティーの総数を示します。

「新規アイデンティティー **% (New Identity %)**」
このデータ・ロード内で、新規アイデンティティー (エンティティー・データベースにとって新しいアイデンティティー) であったアイデンティティー数合計のパーセンテージを示します。

「新規エンティティー数 **(New Entities)**」
「開始日時 **(Date and Time Started)**」から「完了日時 **(Date and Time Completed)**」の時間フレーム内で新しく作成されたエンティティーの総数を示します。

「新規エンティティー **% (New Entity %)**」
このデータ・ソース・ロードの結果として新しく作成されたエンティティーに該当するエンティティー数合計のパーセンテージを示します。

新規アイデンティティーおよび新規エンティティーの数から、このデータ・ソースがエンティティー解決および関係検出の全体にとって、どれくらい価値のあるものであったかという概要を把握できます。これらの数値が低く、かつ長期的に低いままであれば、このデータ・ソースは、ユーザーの会社のエンティティー解決の目標を達成するうえであまり有益でない可能性があります。

「ロール・アラート要約 (Role Alert Summary)」

このセクションを使用して、ロール・アラートの生成につながった、検出された関係に共通する解決ルールと解決スコアを確認します。各行に、リストされている基準に基づいて生成されたロール・アラートの数が提示されます。

「解決ルール **(Resolution Rule)**」
エンティティー解決および関係検出の中で、アイデンティティーとエンティティーを評価するために使用された解決ルールの名前が表示されます。

「アラート説明 **(Alert Description)**」
ロール・アラートをトリガーしたロール・アラート・ルールの名前が表示されます。

「重大度 **(Severity)**」
このロール・アラートの優先度または重要度を測るユーザー定義のインディケーターが表示されます。

「解決スコア **(Resolution Score)**」
ロール・アラートに含まれるアイデンティティーとエンティティーに対して判定された、解決ルールの解決スコア (0 から 100) が表示されます。このスコアは、アイデンティティーとエンティティー間の相似の度合いを示します。スコアが 100 の場合、そのアイデンティティー・レコードがそのエンティティーに解決されたことを意味します。

「アラート・カウント **(Alert Count)**」
ロール・アラート・ルールの説明、解決ルール、および解決スコアに基づいて生成されたロール・アラートの総数を示します。

「関係要約 (Relationship Summary)」

このセクションを使用して、ロール・アラートを生成しなかった、検出された関係に共通する属性を確認します。各行に、リストされている基準に基づいて検出された関係の数が提示されます。

「解決ルール **(Resolution Rule)**」
エンティティー解決および関係検出の中で、入力アイデンティティー・レコードと既存のエンティティーを評価するために使用された解決ルールの名前が表示されます。

「解決スコア **(Resolution Score)**」
エンティティー解決時にアイデンティティーとエンティティーに対して判定された、解決ルールの解決スコア (0 から 100) が表示されます。このスコアは、アイデンティティーとエンティティー間の相似の度合いを示します。スコアが 100 の場合、そのアイデンティティー・レコードがそのエンティティーに解決されたことを意味します。

「関係スコア **(Relationship Score)**」
関係解決時にアイデンティティーとエンティティーに対して判定された、解決ルールの関係スコア (0 から 100) が表示されます。このスコアは、アイデンティティーとエンティティー間の関係の度合いを示します。

マッチング属性に基づいて、関係スコアが高いほど、アイデンティティーとエンティティーがより密接に関連していることになります。

「関係カウント **(Relationship Count)**」
解決ルール、解決スコア、および関係スコアに基づいて検出された関係の総数を示します。

「品質要約 (Quality Summary)」

このセクションの情報を使用して、各データ・ソース・ファイル内のデータの品質を評価します。このセクションでは、UMF セグメントおよび UMF 文書タイプ内の属性タイプ別の品質を示します。品質要約と UMF 例外要約を一緒に確認することで、対応が必要な、品質の問題を含むデータ・ソース・ファイルや誤った形式の UMF を含むデータ・ソース・ファイルがわかります。通常は、データ・ソース・ファイルを処理する前に、ETL や DQM/データ・ソース構成によってこれらの問題を解決できます。

場合によって、このセクションから、特定のデータ・ソースの品質が低すぎるためにエンティティー解決にそのデータ・ソースを使用すべきでないと判断できます。

「文書タイプ **(Document Type)**」
「データ・タイプ (Data Type)」にリストされているデータ・タイプを含んでいる UMF 文書タイプの名前が表示されます。通常、この値は UMF_ENTITY です。

「表名 **(Table Name)**」
類似した名前の UMF セグメントからのデータを保管するデータベース表の名前が表示されます。例えば、NUMBER セグメントからのデータは NUMS 表に保管されます。

「データ・タイプ **(Data Type)**」
入力レコード属性タイプ UMF タグにリストされているデータ・タイプを示します。このタイプは、「表名 (Table Name)」にリストされる UMF セグメントに対応します。例えば、「表名 (Table Name)」が *ADDRESS* で、「データ・タイプ (Data Type)」に *H* とリストされる場合、品質情報の評価対象は住所タイプ *Home* (自宅) です。

データ・タイプに見覚えがない場合、データ・ソース・ファイルが、UMF 文書、UMF セグメント、および UMF タグの適切な組み合わせに正しくマップされていない可能性があります。「例外要約 (Exception Summary)」セクションで、同じ UMF セグメントおよび UMF タグによって 1 つ以上のセグメント例外が発生していないかどうか確認してください。無効な UMF が問題である場合、たいていは「品質要約 (Quality Summary)」セクションの「低品質カウント (Low Quality Count)」の数値と「UMF 例外 (UMF Exception section)」セクションの「セグメント例外カウント (Segment Exception Count)」の数値が一致します。

「レコード・カウント **(Record Count)**」
特定の「文書タイプ (Document Type)」、「表名 (Table Name)」、および「データ・タイプ (Data Type)」の入力アイデンティティー・レコードの総数を示します。

「汎用カウント **(Generic Count)**」
汎用値と見なされる値を含んでいる、特定の「文書タイプ (Document Type)」、「表名 (Table Name)」、および「データ・タイプ (Data Type)」を持つ入力アイデンティティー・レコードの総数を示します。

「低品質カウント **(Low Quality Count)**」
品質が低いと見なされる、特定の「文書タイプ (Document Type)」、「表名 (Table Name)」、および「データ・タイプ (Data Type)」を持つ入力アイデンティティー・レコードの総数を示します。この数値は、データ・ソース・ファイルのデータ入力または ETL 変換に問題があることを示している場合があります。

「使用可能パーセント **(Usable Percent)**」
特定の「文書タイプ (Document Type)」、「表名 (Table Name)」(この UMF セグメントの) 、および「データ・タイプ (Data Type)」を持ち、エンティティー解決および関係検出に使用可能な、入力アイデンティティー・レコードのパーセンテージを示します。 (「レコード・カウント (Record Count)」 - 「汎用カウント (Generic Count)」 - 「低品質カウント (Low Quality Count)」) ÷「レコード・カウント (Record Count)」= 「使用可能パーセント (Usable Percent)」です。

「アイデンティティー・パーセント **(Identity Percent)**」
特定の「文書タイプ (Document Type)」、「表名 (Table Name)」、および「データ・タイプ (Data Type)」を含んでいた入力アイデンティティー・レコードのパーセンテージを示します。

「属性要約 (Attribute Summary)」

このセクションを使用して、関係の検出やロール・アラートの生成に役立った、データ・ソース・ファイル内の属性を確認します。各属性は特定の UMF セグメントにマップされ、このセクションには、入力 UMF セグメント内のデータに基づいて検出された関係の数と生成されたロール・アラートの数が表示されます。

「セグメント名 **(Segment Name)**」
: 特定の属性に直接マップされる UMF セグメントの名前が表示されます。

「データ・タイプ **(Data Type)**」
: 「精度の説明 (Precision Description)」に対応している UMF セグメント内の属性タイプ (またはデータ・タイプ) がリストされます。レポートには特定の属性タイプがリストされる場合と、*ALL* がリストされる場合があります。後者は、UMF セグメントのすべての属性タイプを示しています。

「精度の説明 **(Precision Description)**」
: インバウンド・アイデンティティーの属性と既存のエンティティーの属性間のマッチングしきい値を記述します。

ロール・アラート
: この UMF セグメント、データ・タイプ、および精度の説明に基づいて生成されたロール・アラートの総数を示します。

関係
: この UMF セグメント、データ・タイプ、および精度の説明に基づいて検出された関係の総数を示します。

「UMF 文書要約 (UMF Document Summary)」

このセクションを使用して、レコードに対して実行されるアクションに基づいて、データ・ソース・ファイル内の入力レコードの総数を検証できます。これらの数値を「ロード要約 (Load Summary)」セクションの「レコード・カウント (Record Count)」と照合できます。

「文書タイプ **(Document Type)**」
: UMF 文書タイプの名前が表示されます。通常、この値は UMF_ENTITY です。

アクション
: 入力アイデンティティー・レコードに対するアクションのタイプを示します。以下に、最もよく使用されるアクションのリストを示します。

  - *A* - 追加
  - *C* - 変更
  - *D* - 削除

  システム処理時に各入力レコードに対してどのようなアクションを取るべきか指示するために、通常、ETL 処理の一環としてアイデンティティー・レコードには UMF によってタグが付けられます。

「**UMF** レコード・カウント **(UMF Record Count)**」
: 文書タイプ内でアクション・タイプごとの処理されたレコードの総数を示します。

「パーセント **(Percent)**」
「レコード・カウント (Record Count)」が表す、ロードされた合計レコード数のパーセンテージを示します。(合計は 100% を超えてはなりません。)

「例外要約 (Exception Summary)」

この情報を使用して、誤った形式の UMF など、問題のあるアイデンティティー・レコードを特定します。例外にはどのような問題かが記述され、表名とエレメントは、問題のあるセグメントとレコードを示しています。カウントには、ファイル内でそのような誤った UMF を含んでいたレコードの数が示されます。

「文書タイプ **(Document Type)**」
UMF 文書タイプの名前が表示されます。通常、この値は UMF_ENTITY です。

アクション
入力アイデンティティー・レコードに対するアクションのタイプを示します。

- *A* - 追加
- *C* - 変更
- *D* - 削除

システム処理時に各入力レコードに対してどのようなアクションを取るべきか指示するために、通常、ETL 処理の一環としてアイデンティティー・レコードには UMF によってタグが付けられます。

セグメント
例外が発生した UMF セグメントの名前が表示されます。

「**UMF** タグ **(UMF Tag)**」
UMF 例外の原因となった UMF タグの値が表示されます。

例外　発生した UMF 例外のタイプを示すメッセージ ID またはその他の例外コードが表示されるほか、例外を解決する方法についての情報が与えられます。この情報は、UMF_EXCEPT 表にも提供されます。

「セグメント例外カウント **(Segment Exception Count)**」
このタイプの UMF 例外の総数を示します。

「品質要約 (Quality Summary)」セクションの「低品質カウント (Low Quality Count)」で、一致するデータ・タイプが低品質または使用に耐えない品質として報告されていないかどうか確認してください。正しくない UMF が問題である場合、同じ UMF セグメントおよび UMF タグを対象に、たいていは「品質要約 (Quality Summary)」セクションの「低品質カウント (Low Quality Count)」の数値と「UMF 例外 (UMF Exception section)」セクションの「セグメント例外カウント (Segment Exception Count)」の数値が一致します。

構成レポートの実行

構成レポートは、構成コンソールを使用して構成できる全システム設定の総合的な概要を提供します。現在の製品構成を変更する前や、構成の問題をトラブルシューティングするとき、あるいは異なる構成設定を比較するときには、このレポートを表示して、現行システム構成の設定を確認してください。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「レポート **(Reports)**」をクリックします。
2. 「レポート **(Report)**」から、「構成レポート **(Configuration Report)**」を選択します。
3. 「レポートの実行 **(Run Report)**」をクリックします。

タスクの結果

選択した統計レポートが、指定したすべての基準に基づいて生成されます。生成されたレポートは、「**BIRT** レポート・ビューアー **(BIRT Report Viewer)**」という名前の、別の Web ブラウザー・ウィンドウに表示されます。選択した基準に基づき、報告するデータがない場合は、「**BIRT** レポート・ビューアー **(BIRT Report Viewer)**」ウィンドウの上部にレポート名、レポートの生成日時、および「ページ **1/1 (Page 1/1)**」が表示されます。データ・セクションはブランクです。

構成レポート

構成レポートは、構成コンソールを使用して構成したシステム設定の総合的なビューを提供します。構成の問題をトラブルシューティングするときや、異なる構成設定を比較する必要がある場合には、システム構成を変更する前に、このレポートを使用して、現行システムの構成を表示または印刷してください。

このレポートには、現在の構成設定がカテゴリー別にリストされます。

「データ・ソース **(Data Sources)**」
: データ・ソースの構成設定が表示されます。例えば、データ・ソース ID、データ・ソース・コード、データ・ソースに関連付けられたロール・コード、データ・ソースに関連付けられたエンティティー解決構成、およびデータ・ソース・コードの現在の状況 (アクティブまたは非アクティブ) が表示されます。

  データ・ソースを構成するには、「セットアップ **(Setup)**」 > 「ソース **(Sources)**」 > 「データ・ソース **(Data Sources)**」を選択します。

「番号タイプ **(Number Types)**」
: 番号タイプの構成設定が表示されます。例えば、番号タイプ ID、番号タイプ、番号タイプの最小長と最大長、番号タイプの関連マスク (ある場合)、エンティティー解決において番号タイプがどのように使用されるかの情報、および番号タイプがアクティブであるか非アクティブであるかが表示されます。

  番号タイプを構成するには、「セットアップ **(Setup)**」 > 「ソース **(Sources)**」 > 「番号 **(Numbers)**」を選択します。

「特性タイプ **(Characteristic Types)**」
: 特性タイプの構成設定が表示されます。例えば、特性タイプ ID、特性タイプの名前、特性の関連データ・タイプ (文字または日付など)、エンティティー解決において特性タイプがどのように使用されるかの情報、および特性タイプがアクティブであるか非アクティブであるかが表示されます。

  特性タイプを構成するには、「セットアップ **(Setup)**」 > 「ソース **(Sources)**」 > 「特性 **(Characteristics)**」を選択します。

「プラグイン **(Plugin)**」
属性およびスコアリングのカスタマイズに関する構成設定が表示されます。例えば、プラグイン ID、名前、タイプ、バージョン、およびライブラリー短縮名が表示されます。

属性およびスコアリングのカスタマイズ用プラグインを構成するには、「セットアップ **(Setup)**」 > 「一般 **(General)**」 > 「プラグイン **(Plugins)**」を選択します。

「イベント・タイプ **(Event Types)**」
イベント・タイプの構成設定が表示されます。例えば、このイベントの値に関連付けられた計測単位が表示されます。イベント・タイプは、Event Manager の一部です。

イベント・タイプを構成するには、「セットアップ **(Setup)**」 > 「ソース **(Sources)**」 > 「イベント・タイプ **(Event Types)**」を選択します。

「データ品質管理ルール **(Data Quality Management Rules)**」
データ品質管理ルール (DQM ルール) のリストと、UMF セグメント内の特定の UMF タグ用に構成された、それぞれのルールの関連パラメーターのリストが表示されます。例えば、どの UMF セグメントおよび UMF タグの名前に DQM ルールが関連付けられているか、その UMF セグメントおよび UMF タグ上で DQM ルールが使用されるときの順序、その UMF セグメントおよび UMF タグ上での DQM ルール用の関連パラメーター、DQM ルールがその UMF セグメントおよび UMF タグに対して入力データを修正するかどうか、および DQM ルールが現在その UMF セグメントおよび UMF タグ上で有効になっているかどうかが表示されます。

DQM ルールが使用されるように UMF セグメントおよび UMF タグを構成するには、「セットアップ **(Setup)**」 > 「**UMF**」 > 「**DQM** ルール **(DQM Rules)**」を選択します。

「マッピングのロード **(Load Mapping)**」
エンティティー・データベース内の対応する表および表列に UMF データがどのようにマップされるかについての構成情報が表示されます。例えば、UMF セグメント名、UMF データ・パス、エンティティー・データベース表の名前、そのエンティティー・データベース表内のフィールド名とフィールド・タイプ、そのフィールドのデータ・タイプ、およびマッピングが有効になっているかどうかが表示されます。

UMF セグメントからエンティティー・データベース内の表にデータをマップするには、「セットアップ **(Setup)**」 > 「**UMF**」 > 「データ・マップ **(Data Map)**」を選択します。

「エンティティー解決ルール **(Entity Resolution Rules)**」
各エンティティー解決ルールの構成設定が表示されます。例えば、エンティティー解決ルール ID、ルールの順序、ルールの解決および関係の最小スコア、およびルールに否定が組み込まれているかどうかが表示されます。

エンティティー解決ルールを構成するには、「セットアップ **(Setup)**」 > 「解決 **(Resolution)**」 > 「解決ルール **(Resolution Rules)**」を選択します。

「エンティティー解決の確定/否定 **(Entity Resolution Confirm/Deny)**」
エンティティー解決の確定と否定の処理を導くスコアの設定が表示されます。例えば、関連付けられたエンティティー解決 ID および構成 ID、各スコアの優先度、各スコアの説明と属性名、およびスコアの数値が表示されます。

エンティティー解決の確定と否定の設定を構成するには、「セットアップ **(Setup)**」 > 「解決 **(Resolution)**」 > 「確定と否定 **(Confirms & Denials)**」を選択します。

「エンティティー解決特性 **(Entity Resolution Characteristics)**」
エンティティー解決中に使用される確定と否定の重みづけで構成される特性タイプに関する設定が表示されます。例えば、優先度、確定の重みづけ、および否定の重みづけが表示されます。

特性タイプに関する確定と否定の重みづけを構成するには、「セットアップ **(Setup)**」 > 「解決 **(Resolution)**」 > 「特性 **(Characteristics)**」を選択します。

「ロール・コード **(Role Codes)**」
構成済みロール・コードおよびその関連設定のリストが表示されます。例えば、ロール・コードの ID と説明、ロール・コードのクラス、およびロール・コードの現在の状況 (アクティブか非アクティブか) が表示されます。

ロール・コードを構成するには、「セットアップ **(Setup)**」 > 「関係 **(Relationships)**」 > 「ロール **(Roles)**」を選択します。

「ロール・アラート・ルール **(Role Alert Rules)**」
構成済みロール・アラート・ルールおよびその関連設定のリストが表示されます。例えば、ロール・アラート・ルールの ID と説明、重大度、アラートの最小しきい値、およびこのロール・アラート・ルールをトリガーする 2 つのロールのロール・コード ID が表示されます。

ロール・アラート・ルールを構成するには、「セットアップ **(Setup)**」 > 「関係 **(Relationships)**」 > 「ロール・アラート・ルール **(Role Alert Rules)**」を選択します。

「**Name Manager** 構成 **(Name Manager Configuration)**」
エンティティー解決中に名前の精度を拡張する Name Manager 機能に関する構成済み設定が表示されます。

Name Manager の設定を構成するには、「セットアップ **(Setup)**」 > 「解決 **(Resolution)**」 > 「**Name Manager** のマッチング構成 **(Name Manager Match Config)**」を選択します。

「隔たり構成 **(Separation Configuration)**」
1 次の隔たり、2 次の隔たり、またはそれより大きな隔たり度合いの関係を検出できる、パイプラインの隔たり度合い機能に関する構成済み設定が表示されます。

隔たり度合いの設定を構成するには、「セットアップ **(Setup)**」 > 「関係 **(Relationships)**」 > 「隔たり構成 **(Separation Config)**」を選択します。

「システム・シーケンス **(System Sequences)**」
システムがどのようにデータをロードして処理するかを示す、シーケンス番号の構成設定が表示されます。システム・シーケンス番号は、システムのロ

ード・パフォーマンスを 2 つの面から支援します。まず、システム・シーケンス番号によって、各パイプラインが連続する番号セットをグラブするクエリーを 1 つ発行し、それらの番号がすべて使用されるまで、それらの番号をキャッシュに保持できるようになります。さらに、シーケンス番号があることで、システム生成 ID を生成する複数のパイプラインが、複数のレコードに対して同じ ID 番号を使用することが防止されます。

例えば、エンティティー解決処理中、パイプラインが新規エンティティーを作成するたびに、システムはユニーク・エンティティー ID を生成します。システム・シーケンスを使用することで、パイプラインは次に使用可能な 1000 件のエンティティー ID 番号を要求するクエリーを 1 つ送信することができます。そのため、新規作成される次の 1000 件のエンティティーに対し、パイプラインはそれ自体のメモリーに格納されている使用可能なエンティティー ID 番号を使用できます。代わりの (より低速な) 方法は、各パイプラインが、作成される新規エンティティーごとに、新規エンティティー ID を要求するクエリーを 1 つ、エンティティー・データベースに送信するようにすることです。

システム・シーケンスを構成するには、「セットアップ **(Setup)**」 > 「**UMF**」 > 「ロード・シーケンス **(Load Sequence)**」を選択します。

「汎用しきい値 **(Generic Thresholds)**」
属性別に構成済みの汎用しきい値の設定が表示されます。例えば、属性名、属性タイプ、およびその属性の特定の値が汎用になるタイミングを決定するしきい値が表示されます。

属性タイプ別の汎用しきい値を構成するには、「セットアップ **(Setup)**」 > 「**UMF**」 > 「汎用しきい値 **(Generic Threshold)**」を選択します。

「表ディクショナリー **(Table Dictionary)**」
エンティティー・データベース表別のディクショナリーの設定が表示されます。例えば、表名、説明、および表タイプが表示されます。

表ディクショナリーを構成するには、「セットアップ **(Setup)**」 > 「**UMF**」 > 「ディクショナリー **(Dictionary)**」を選択します。

「ルックアップ表 **(Look Up Tables)**」
システムが処理中に参照表として使用する表のリストについて、設定が表示されます。例えば、表名、キー・フィールド名、ID フィールド名、および処理中に表をメモリーにロードするかどうかが表示されます。

システムがどの表を参照表として使用するかを構成するには、「セットアップ **(Setup)**」 > 「**UMF**」 > 「ルックアップ **(Lookup)**」を選択します。

「マッチング構成 **(Matching Configuration)**」
システム上に構成されている、解決構成ごとの設定が表示されます。例えば、構成の名前と ID、マッチング・タイプ、および UMF セグメント名が表示されます。

マッチング構成を構成するには、「セットアップ **(Setup)**」 > 「解決 **(Resolution)**」 > 「候補ビルダー **(Candidate Builder)**」を選択します。

「文書タイプ **(Document Types)**」
UMF 入力文書についての設定が表示されます。例えば、文書タイプ、この文書タイプに対してデータ品質管理を実行するかどうか、この文書タイプに

よって処理されたデータをエンティティー解決データベースにロードするかどうか、およびこの入力 UMF 文書タイプに対して実行するエンティティー解決のレベルが表示されます。

UMF 入力文書を構成するには、「セットアップ **(Setup)**」 > 「**UMF**」 > 「入力文書 **(Input Documents)**」を選択します。

「**UMF** 出力フォーマット **(UMF Output Format)**」
UMF 出力文書のフォーマット設定が表示されます。例えば、フォーマット ID とコード、経路の方向、および出力フォーマット設定が有効になっているかどうかが表示されます。

UMF 出力文書のフォーマットを構成するには、「セットアップ **(Setup)**」 > 「**UMF**」 > 「出力文書 **(Output Documents)**」を選択します。

「**GEM** イベント・タイプ **(GEM Event Types)**」
Event Manager のイベントについてのフォーマット設定が表示されます。例えば、イベントの ID、タイプ、説明、カテゴリー、計測単位、および作成日時が表示されます。

イベント・タイプを構成するには、「セットアップ **(Setup)**」 > 「ソース **(Sources)**」 > 「イベント・タイプ **(Event Type)**」を選択します。

「システム・パラメーター **(System Parameters)**」
システム・パラメーター設定のリストが、パラメーター・グループ別に表示されます。例えば、システム・パラメーターの値とデフォルト値、およびパラメーターの検証タイプと値が表示されます。

システム・パラメーターを構成するには、「セットアップ **(Setup)**」 > 「一般 **(General)**」 > 「システム・パラメーター **(System Parameters)**」を選択します。

「アプリケーション・アクティビティー・コード **(Application Activity Codes)**」
Visualizer 用に構成されたアクティビティー・コードのリストが、アクティビティー・タイプ (ロール・アラート、属性アラート、イベント・アラート) 別に表示されます。例えば、アクティビティー・コード、アクティビティー・コードの有効な状況、およびアクティビティー・コードがアクティブであるか非アクティブであるかが表示されます。

Visualizer で使用されるアクティビティー・コードを構成するには、「セットアップ **(Setup)**」 > 「**Visualizer**」 > 「アクティビティー・コード **(Activity Codes)**」を選択します。

「ユーザー・グループ **(User Groups)**」
Visualizer 用に構成されたユーザー・グループの設定が表示されます。例えば、関連の Visualizer ユーザー名、ユーザー・グループの作成日時、およびユーザー・グループがアクティブであるか非アクティブであるかが表示されます。

Visualizer で使用されるユーザー・グループを構成するには、「セットアップ **(Setup)**」 > 「**Visualizer**」 > 「コード **(Codes)**」を選択した後、「アナリスト・グループ **(ANALYZER_GROUP)**」を選択します。

「ロール・アラート・グループ **(Role Alert Groups)**」
構成済みのロール・アラート・グループの設定が表示されます。例えば、割り当てられたアプリケーション・グループ、関連付けられたロール・アラー

ト・ルール ID と説明、ロール・アラート・グループの作成日時、およびロール・アラート・グループがアクティブであるか非アクティブであるかが表示されます。

Visualizer で使用されるロール・アラート・グループを構成するには、「セットアップ **(Setup)**」 > 「関係 **(Relationships)**」 > 「ロール・アラート・ルール **(Role Alert Rules)**」を選択した後、「アラート・グループ **(Alert Group)**」フィールドを編集します。

「ユーザー **(Users)**」

Visualizer にログインできるように構成されているユーザーに関する設定が表示されます。例えば、ユーザーのログイン名、エンティティー・データベースの資格情報を使用して Visualizer ユーザーを認証するかどうか、および Visualizer ユーザーがアクティブであるか非アクティブであるかが表示されます。

ユーザーを構成するには、「セットアップ **(Setup)**」 > 「**Visualizer**」 > 「**Visualizer** ユーザー **(Visualizer Users)**」を選択します。

レポートのエクスポート

BIRT レポート・ビューアーには、構成コンソールのレポート・データを他のアプリケーション (Microsoft Excel、Microsoft PowerPoint、Microsoft Word、または Adobe Acrobat など) にエクスポートするオプションがあります。レポート全体をエクスポートすることも、レポートの特定のデータをエクスポートすることもできます。

構成コンソール・レポートのエクスポート

レポート全体 (データとフォーマット設定の両方) を、別のアプリケーション (Microsoft PowerPoint など) や、別のフォーマット (Adobe Acrobat PDF など) にエクスポートする場合は、BIRT レポート・ビューアーの「レポートのエクスポート**(Export reports)**」オプションを使用します。フル・レポートのエクスポートは、複数ページにわたるレポートの場合に、またレポートをエクスポートした後でデータを操作する必要がない場合に適しています。

このタスクについて

Microsoft Word *.doc ファイルにエクスポートした構成コンソール・レポートを開くためには、Microsoft Word バージョン 2003 以降を使用する必要があります。

エクスポートされたレポートに小さな変更や追加を行う場合は、Microsoft Word または Microsoft Excel のいずれかにレポートをエクスポートしてください。これらのアプリケーションでは、レポートのフォーマット設定が維持されますが、通常は列や表でデータが表示されます。そのため、多少のデータ操作が可能です。エクスポートされたレポートは読み取り専用ファイルであるため、新規名でファイルを保存して変更内容を保存してください。

手順

1. レポート生成後、「**BIRT** レポート・ビューアー **(BIRT Report Viewer)**」ウィンドウで「レポートのエクスポート **(Export report)**」をクリックします。 「レポートのエクスポート (Export report」アイコンは、BIRT レポート・ビューアーのアイコン・ツールバーにある、左から 4 番目のアイコンです。

2. 「レポートのエクスポート **(Export Report)**」で、データをエクスポートするフォーマットまたはアプリケーションを選択します。
   - 「**PDF**」
   - 「**PowerPoint**」
   - 「**Word**」
   - 「**PostScript**」
   - 「**Excel**」
3. エクスポートするページまたはページ範囲を選択します。
4. オプション: 結果として得られるレポートのサイズを選択します。 このオプションは、PDF、PowerPoint、または PostScript のいずれかのオプションを選択した場合にのみ使用できます。
   - 「自動 **(Auto)**」: レポートの各ページが別々のページになります。
   - 「実際のサイズ **(Actual size)**」: レポートのどのページも 1 つの長いページに収められます。
   - 「ページ全体に合わせる **(Fit to whole page)**」: レポートのどのページも、1 ページのおよそ 3 分の 1 に収まるように縮小されます。「PowerPoint」オプションを選択した場合、レポートは画像としてページに挿入されますので、この画像をサイズ変更することができます。
5. 「**OK**」をクリックします。

タスクの結果

レポートを PDF 形式または PostScript 形式でエクスポートした場合、結果として得られるファイルは、通常、クライアントにダウンロードしたファイルが配置されるフォルダー・ロケーションに配置されます。例えば、C:¥Documents and Settings¥Administrator¥My Documents¥Downloads です。

PowerPoint、Word、または Excel にエクスポートした場合、データは、通常 *reportname.selected_application_extension* という名前の読み取り専用ファイルにエクスポートされます。

- *reportname* は、エクスポートした構成コンソール・レポートの名前です。
- *selected_application_extension* は、選択したアプリケーションに応じた適切なファイル・フォーマットの拡張子です。

例えばロード要約レポートを Word にエクスポートした場合、ファイル名は通常、LoadSummary.doc となります。表示されたダイアログで、選択したアプリケーションでファイルを開くのか、ファイルに保管するのかを選択します。

構成コンソール・レポートからのデータのエクスポート

レポートのデータを CSV ファイル (コンマ区切り値ファイル) にエクスポートして、データを別のアプリケーション (Microsoft Excel など) で表示したり処理したりする必要がある場合、BIRT レポート・ビューアーの「データのエクスポート **(Export data)**」オプションを使用します。レポート内の 1 つのセクション、エクスポート対象のフィールド、およびエクスポート・データ・フォーマットを選択できます。

このタスクについて

BIRT レポート・ビューアーは、一度に 1 つのデータ・セクションをレポートからエクスポートします。つまり、このビューアーは、レポート内のセクションごとに別の結果セットを作成します。エクスポートされるデータは、フォーマット設定のない、生データです。

レポート全体をエクスポートする場合は、代わりに「レポートのエクスポート **(Export report)**」オプションを使用します。ただし、そのエクスポート・オプションでエクスポートされるのは、データとレポート・フォーマットの両方です。そのため、エクスポート後にデータを操作することはできません。

手順

1. レポート生成後、BIRT レポート・ビューアーで「データのエクスポート **(Export data)**」アイコンをクリックします。 「データのエクスポート **(Export data)**」アイコンは、BIRT レポート・ビューアーのアイコン・ツールバーにある、左から 3 番目のアイコンです。
2. 必須: 「データのエクスポート **(Export Data)**」の「使用可能な結果セット **(Available results sets)**」で、エクスポートするレポート・セクションを 1 つ選択します。 レポート・セクションの名前は、ELEMENT_2041 のように、エレメントで表示されます。通常、「使用可能な列 **(Available Columns)**」にリストされている列名を参照することで、選択しているセクションを見分けることができます。
3. 必須: 「使用可能な列 **(Available Columns)**」で、エクスポートする列を選択します。 「使用可能な結果セット **(Available results sets)**」で選択したレポート・セクションに該当する列名が、「選択された列 **(Selected Columns)**」に表示されます。そのレポート・セクションで使用可能なすべての列のデータを表示する必要はありません。
4. オプション: 「選択された列 **(Selected Columns)**」で、列の順序を設定します。 このオプションを使用すると、データをエクスポートする前に、データを列で並べ替えることができます。
5. オプション: デフォルトで選択されている「コンマ **(Comma)**」ではなく、次の区切り記号を使用する場合は、「区切り記号 **(Separator)**」でその区切り記号を選択します。
   - 「セミコロン **(Semi-colon)**」
   - 「コロン **(Colon)**」
   - 「縦線 **(Vertical line)**」
   - **Tab**
6. 「**OK**」をクリックします。 表示されたダイアログで、エクスポートされたデータを開くのか、ファイルに保管するのかを選択します。ファイルを開く場合のデフォルトのアプリケーションは Microsoft Excel ですが、CSV ファイルをエクスポートできるアプリケーションであればどれでも参照して選択できます。

タスクの結果

データは通常、*reportname*.csv という名前のファイルにエクスポートされます。ここで、*reportname* は、エクスポートしたデータが含まれていた構成コンソール・レポートの名前です。

Visualizer の管理

Visualizer を効果的に使用するためには、ブラウザーの構成、適切なユーザーのアカウントのセットアップ、および Visualizer へのアクセスの管理を行う必要があります。

Visualizer

Visualizer は、アナリストや調査員がアラート、関係、エンティティー解決の結果を分析するために使用するグラフィカル・ユーザー・インターフェースです。

Visualizer は、組み込みバージョンの IBM WebSphere Application Server によってホストされます。Visualizer の構成は、構成コンソールから行うか、Visualizer の「ファイル **(File)**」メニューの「設定 **(Preferences)**」選択から行います。

Visualizer ユーザーは、以下のような各種の分析タスクを実行できます。

アラートの分析と後処理
: エンティティー解決処理によって生成されるアラートは、組織にとって関心のある関係やエンティティー解決を表します。通常はアナリストがアラートを確認し、アラート情報に基づいて、アクションが必要な場合には、実行するアクションを決定します。アラートには、ロール・アラート、属性アラート、およびイベント・アラートの 3 つのタイプがあります。

  Visualizer はアラートを表示し、アナリストに対し、アラートおよびアラートに含まれるエンティティーのテキスト・ビューとグラフィカル・ビューの両方を提供します。アナリストは詳細にドリルダウンしてから、アラートの後処理の状況を適切に設定できます。

属性アラート・ジェネレーターの作成と管理
: Visualizer を使用することで、アナリストは、属性アラート・ジェネレーター機能を介して永続検索を作成および管理でき、属性アラートを表示する方法と受け取る方法を管理できます。アナリストは、属性データに基づいて属性アラート・ジェネレーターを作成して、属性データに基づいてエンティティーに解決されたアイデンティティーを見つけることができます。また、アナリストは、属性アラート・ジェネレーターを作成して、エンティティー・データベースで特定のエンティティーを永続的に検索することもできます。

エンティティーの検索
: Visualizer ユーザーは、以下のようにいくつかの方法を使用して、さらに分析を行うためにエンティティーを検索することもできます。

  - 属性による検索
  - データ・ソース・アカウントによる検索
  - エンティティー ID による検索

- 解決による検索 (最小解決スコアしきい値に基づいて、入力された基準がエンティティー・データベース内のアイデンティティーやエンティティーとどれくらい正確に一致しているか)

エンティティーおよび開示された関係の追加
: アナリストは、Visualizer を使用してエンティティー解決や関係検出のレコードを追加できます。単一アイデンティティー・レコードを追加することも、数千件のアイデンティティー・レコードを含んだ UMF ファイルをロードすることもできます。調達プログラムを通じてアイデンティティー・レコードが追加される場合と同様に、Visualizer から追加されたレコードも、エンティティー解決および関係検出のためにパイプラインによって処理されます。処理の結果はエンティティー・データベースに書き込まれ、アラートがある場合は Visualizer に公開されます。

  アナリストは、アイデンティティー間にリンクがあることをわかっている場合、(アイデンティティーによって) エンティティー間の関係を開示することもできます。開示される関係の例として、求人の申込書にリストされている緊急時連絡先や身元保証人に基づいた関連エンティティーなどがあります。エンティティーにより、申込書にあるこれらの関係が開示されます。

レポートの生成と印刷
: Visualizer には、アナリストが Visualizer での作業を管理および追跡するのに役立てるために、アナリストが表示したり印刷したりできる複数のレポートも含まれています。

ユーザー・ロールと責任

ユーザー・ロールは、IBM InfoSphere Identity Insight を効率的にデプロイして使用するために完了する必要のある一般的なタスクを分類するのに役立ちます。さまざまなタイプのユーザーが IBM InfoSphere Identity Insight をさまざまな目的で使用する可能性があります。すなわち、ユーザーは、製品の使用において、1 つ以上のロールの責任を引き受けます。

さまざまなユーザー・ロールと責任に基づいて、ユーザーのグループを定義できます。

最も一般的なユーザー・ロールを以下に示します。

アナリスト
: データを分析し、エンティティー、関係、およびアラートをレビューします。アナリストは、何が最も重要な結果であるかを定義し、システムがそのような結果を返すようにします。アナリストはオペレーターおよびアプリケーション・アドミニストレーターと密接に連携します。

オペレーター
: 必要に応じてロード品質レポートを提供しながら、システムにデータをロードし、パイプラインを実行し、システムが許容できる状態で稼働していることを確認します。オペレーターはまた、結果、例外、およびイベントをレビューします。オペレーターは、アナリスト、データ・ソース・アドミニストレーター、およびアプリケーション・アドミニストレーターと密接に連携します。

データ・ソース・アドミニストレーター
: データをシステムにロードできるよう、データの準備をします。これには、データの UMF ファイルへの変換とそのファイルの検証が含まれます。データ・ソース・アドミニストレーターは、オペレーター、アプリケーション・アドミニストレーター、およびデータベース・アドミニストレーターと密接に連携します。

アプリケーション・アドミニストレーター
: アプリケーションを構成します。これには、データ、エンティティー・モデル、およびルールの構成が含まれます。アプリケーション・アドミニストレーターは、データ・ソース・アドミニストレーターおよびオペレーターと密接に連携してエンティティー・モデルを定義するとともに、データベース・アドミニストレーター、データ・ソース・アドミニストレーター、およびオペレーターと構成変更について調整します。また、アプリケーション・アドミニストレーターは、総合的なシステム・アドミニストレーター (存在する場合) との調整および協議も行います。

データベース・アドミニストレーター
: データベースを適切に構成および調整して、アプリケーションで使用できるようにします。データベース・アドミニストレーターは、オペレーター、データ・ソース・アドミニストレーター、およびアプリケーション・アドミニストレーターと密接に連携します。

システム・アーキテクト
: アプリケーションのデプロイメント計画において、ハードウェア要件およびソフトウェア要件の規模を判定し、工数を見積もります。システム・アーキテクトは、インストール担当者、データベース・アドミニストレーター、データ・ソース・アドミニストレーター、およびアプリケーション・アドミニストレーターと密接に連携して、デプロイメントにより構想、戦略、および目標が達成され、期待どおりの結果を提供しながらデプロイメントがビジネス・プロセスに確実に統合されるようにします。

インストール担当者
: アプリケーションのインストールおよび初期構成を管理します。システムの初期ユーザーをセットアップするのも、インストール担当者です。多くの場合、IBM プロフェッショナル・サービスがシステム・アーキテクトと協力して、これらの責任を果たします。

プログラマー
: アプリケーションのデプロイメントがシームレスに環境に統合されるように、グラフィカル・インターフェースの設計および開発や、さまざまな機能に合わせたグラフィカル・インターフェースのカスタマイズを行います。プログラマーは、システム・アーキテクトおよびアプリケーション・アドミニストレーターと密接に連携します。また、適切な関係者に対して、その環境において最も効果的な方法でアラートの周知に努めることもよくあります。

セキュリティー・アーキテクト
: プロジェクト・チームがセキュアなシステムを計画し、実装するようにします。セキュリティー・アーキテクトは、システム・アーキテクト、インストール担当者、およびデータベース・アドミニストレーターと密接に連携します。

Visualizer を使用するための最適なブラウザー設定

Visualizer は、Web でアクセスする、Java ベースのアプリケーションです。Visualizer へのアクセスに使用するブラウザーが特定の設定になっている場合に、最適なパフォーマンスを発揮します。

Visualizer の表示を最適にするには、以下のブラウザー設定を使用します。

表 *28. Visualizer* 用の最適なブラウザー設定

設定	値	説明
文字サイズ	中	
JavaScript	オン	
Cookie	オン	少なくとも、ファースト・パーティーのセッション Cookie を有効にする必要があります。
セキュリティー: 信頼できる Web サイト	Visualizer の HTTP アドレス	Visualizer の HTTP アドレスが、信頼されたインターネット Web サイトのリストに含まれていることを確認します。
セキュリティー: ダウンロード・オプション	「有効 (Enabled)」	信頼されたインターネット Web サイト向けのダウンロード・オプションはすべて有効になっていることを確認します。
ポップアップ・ブロッカー	Visualizer の HTTP アドレスからのポップアップを許可	Visualizer の HTTP アドレスが、ポップアップが許可された Web サイトのリストに含まれていることを確認します。

Visualizer へのログイン

Visualizer にログインするためには、Visualizer ユーザー・アカウント (ユーザー名とパスワード) が必要です。Visualizer ユーザー・アカウント情報はシステム・アドミニストレーターから入手できます。

手順

1. 以下のいずれかのステップを実行します。
   - デスクトップ上にある Visualizer アイコンをダブルクリックします。
   - インターネット・ブラウザーを開き、アドレス行に Visualizer の Uniform Resource Locator (URL) を入力します。

   Visualizer を起動するための URL は以下のとおりです。

   `http://server:install_port`

例えば、http://localhost:13510 です。Visualizer のインストール時、デフォルトの *install_port* は 13510 ですが、ポート番号は変更可能です。正しいサーバー名またはポート番号が不明な場合は、システム・アドミニストレーターに問い合わせてください。

2. ユーザー名とパスワードを入力してログインします。

   注**:** ユーザー名およびパスワードの両方のフィールドが大/小文字を区別します。最初にログインするときは、システム・アドミニストレーターから割り当てられたパスワードを使用してください。最初のログインが成功した後、通常は、Visualizer アカウントのセキュリティーを保護するために Visualizer パスワードを変更します。

3. 「ログイン **(Login)**」をクリックします。

Visualizer の終了

Visualizer の使用が終了したら、アプリケーションを閉じます。 Visualizer を閉じることによって、ユーザーはログアウトされます。休憩を取る際など、数分間のみワークステーションを保護する必要がある場合は、代わりに Visualizer をロックできます。

手順

Visualizer を終了し、ログアウトするには、以下のようにします。

- 「ファイル **(File)**」 > 「終了 **(Exit)**」を選択します。
- または、**Ctrl** + **Q** を押します。

Visualizer へのアクセスの管理

Visualizer ユーザーは、Visualizer にログインするためには、登録済みのアカウントを持っている必要があります。これらのユーザー・アカウントは、構成コンソール用のユーザー・アカウントと同じではなく、Visualizer の使用を許可された専用ユーザー・アカウントです。

新規 Visualizer ユーザーの作成

ユーザーが Visualizer にアクセスし、これを使用するためには、システム・アドミニストレーターがそのユーザー用の Visualizer ユーザー・アカウントを構成コンソールで作成する必要があります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**Visualizer**」ボタンをクリックします。
3. 「**Visualizer** ユーザー **(Visualizer Users)**」タブをクリックします。
4. 「新規 **(New)**」ボタンをクリックします。
5. 「データベース・ログイン **(Database Login)**」ドロップダウン・リストから、以下の値のいずれかを選択します。
   - このユーザーがエンティティー・データベースへのアクセス権限が付与されたユーザー・アカウントを持っていて、かつ、そのデータベース・ログイン情報を使用する場合は、「はい **(Yes)**」を選択します。

- デフォルトのファイル・ログイン情報を使用する場合は、「いいえ **(No)**」を選択します。これを選択することはつまり、ユーザーが Visualizer へのログインに使用する初回パスワードをシステム・アドミニストレーターが選択すること、および、システム・アドミニストレーターは要求時に Visualizer ユーザーのパスワードを再設定できることを意味します。

6. 「ユーザー名 **(User Name)**」フィールドに、追加するユーザー名を入力します。「データベース・ログイン **(Database Login)**」 ドロップダウンで「はい **(Yes)**」を選択した場合は、このユーザー名が、このユーザーのエンティティー・データベース用のユーザー名と一致している必要があります。
7. 「パスワード **(Password)**」フィールドで、次の操作を行います。
   a. 「データベース・ログイン **(Database Login)**」 ドロップダウン・リストで「はい **(Yes)**」を選択した場合は、この値が、データベース・ログイン情報に保管されているパスワードと一致している必要があります。
   b. 「データベース・ログイン **(Database Login)**」 ドロップダウン・リストで「いいえ **(No)**」を選択した場合は、このユーザーの初期パスワードを入力します。

   注**:** セキュリティー上の理由から、初回ログイン成功後に初期パスワードを変更するよう Visualizer ユーザーに働きかけてください。
8. オプション: 「グループ **(Group)**」フィールドで、この個人が所属するアナライザー・グループを、ドロップダウン・リストから選択します。
9. 「保存 **(Save)**」ボタンをクリックします。

次のタスク

ユーザーは、このユーザー名とパスワードを即時に使用して Visualizer にログインできるようになりました。

Visualizer ユーザーの非アクティブ化

Visualizer へのアクセスが不要になったユーザーの Visualizer ユーザー・アカウントを非アクティブ化することができます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**Visualizer**」ボタンをクリックします。
3. 「**Visualizer** ユーザー **(Visualizer Users)**」タブをクリックします。
4. 非アクティブ化するユーザー・アカウントのユーザー名をクリックします。
5. 「状況 **(Status)**」ドロップダウン・リストから、「非アクティブ化 **(Inactive)**」を選択します。
6. 「保存 **(Save)**」ボタンをクリックします。

タスクの結果

非アクティブ化したユーザーは、Visualizer にログインできなくなります。

Visualizer パスワードの再設定

Visualizer ユーザーがパスワードを忘れた場合、そのユーザーのログイン情報が、基礎となるデータベース・ログイン・オプションを通じてではなく、構成コンソールを通じて構成されたものであれば、構成コンソールを使用してパスワードを再設定することができます。そうでない場合は、基礎となるデータベース・ログイン構成を使用して、そのユーザーのパスワードを再設定する必要があります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**Visualizer**」ボタンをクリックします。
3. 「**Visualizer** ユーザー **(Visualizer Users)**」タブをクリックします。
4. パスワード編集の対象となるユーザーのユーザー名をクリックします。
5. 「パスワード **(Password)**」フィールドに、ユーザーの新規パスワードを入力します。

   注**:** セキュリティー上の理由から、パスワードを知っているのがユーザー自身だけであるようにするため、初回ログイン成功後にパスワードを変更するようユーザーに働きかけてください。
6. 「保存 **(Save)**」ボタンをクリックします。

次のタスク

ユーザーは、即時にこの新規パスワードを使用して、Visualizer にログインできます。パスワードを再設定した後は、セキュリティー上の理由から、ログイン成功後にパスワードを変更するようユーザーに働きかけてください。

Visualizer ユーザー・グループの作成

アラートは、Visualizer 内でアナリストのグループに割り当てられます。アナリストの新規グループをプロジェクトに追加する場合は、構成コンソールを使用して新規アナリスト・グループを作成できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. 「コード **(Codes)**」タブをクリックします。
4. 「タイプ **(Type)**」ドロップダウン・リストから、「アナリスト・グループ **(ANALYZER_GROUP)**」 をクリックします。
5. 「新規 **(New)**」ボタンをクリックします。
6. 「コード **(Code)**」フィールドに、アナリスト・グループの名前を入力します。
7. 「状況 **(Status)**」ドロップダウン・リストから、「アクティブ **(Active)**」を選択します。
8. 「保存 **(Save)**」ボタンをクリックします。

ヘルプ・トピック

Visualizer の「ユーザー一般 **(Users General)**」タブ**:**

新規 Visualizer ユーザーの追加や、既存のユーザー・パスワードの変更を行うには、このタブを使用します。

「データベース・ログイン **(Database Login)**」
Visualizer へのアクセス用として、基礎となるエンティティー・データベースへのログイン情報 (ユーザー名とパスワード) を使用するかどうかを決定するためのオプションを選択します。

- 「はい (Yes)」: この Visualizer ユーザーが既に、エンティティー・データベースへのユーザー・アクセス権限が付与されたユーザー・アカウントを持っている場合のみ、この設定を使用します。このオプションを選択した場合は、エンティティー・データベースへのログイン用のユーザー名およびパスワードを、Visualizer 用のユーザー名およびパスワードとして使用します。(この 2 つが一致していないと、この Visualizer ユーザーはログインできないことになります。)
- 「いいえ (No)」: このタブで入力したログイン情報を使用します。

「ユーザー名 **(User Name)**」
この Visualizer ユーザーのユーザー名を入力します。このユーザーがデータベース・ログインを使用する場合、このユーザー名は、対応するエンティティー・データベース用のユーザー名と一致する必要があります。

「パスワード **(Password)**」
この Visualizer ユーザーの新規パスワードを入力します。このユーザーがデータベース・ログインを使用する場合、このパスワードは、対応するデータベース・パスワードと正確に一致する必要があります。

「グループ **(Group)**」
このユーザーが属する Visualizer グループを選択します。属する Visualizer グループによって、どのアラートおよび通知が Visualizer の「アラート要約 **(Alert Summary)**」ウィンドウに表示されるかが決まります。(例えば、組織に「セキュリティー Visualizer」グループと「予約グループ」がある場合、Visualizer には各グループのユーザーに対して異なるタイプのアラートが表示される可能性があります。)

状況　この Visualizer ユーザーが現在アクティブである (Visualizer にログインできる) かどうかを示す状況を選択します。

Visualizer 用のアクティビティー・コードの構成

Visualizer には、アラート処理用のデフォルトのアクティビティー・コードがいくつか用意されています。構成コンソールを通じて、新規アクティビティー・コードを追加したり、既存のアクティビティー・コードを削除したりできます。

検索用のアクティビティー・コードの作成

Visualizer には、検索結果アラート用のアクティビティー・コードが用意されています。アラート処理に関連した追加のアクティビティーを追跡する必要がある場合は、構成コンソールを使用して、新規アクティビティー・コードを追加できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**Visualizer**」ボタンをクリックします。
3. 「アクティビティー・コード **(Activity Codes)**」タブをクリックします。
4. 「アクティビティー・タイプ **(Activity Type)**」ドロップダウン・リストから、「検索 **(SEARCH)**」を選択します。
5. 「新規 **(New)**」ボタンをクリックします。
6. 「アクティビティー・コード **(Activity Code)**」フィールドに、このアクティビティー・コードの名前を入力します。
7. 「アクティビティー状況コード **(Activity Status Code)**」ドロップダウン・リストから、新規アクティビティー・コードが相当する、内部で認識されるアクティビティー状況コードを選択します。
8. 「状況 **(Status)**」ドロップダウン・リストから、「アクティブ **(Active)**」を選択します。
9. 「保存 **(Save)**」ボタンをクリックします。

検索用のアクティビティー・コードの削除

Visualizer には、検索結果アラート用のアクティビティー・コードが用意されています。アラート処理に関連したアクティビティー・コードを削除する必要がある場合は、構成コンソールを使用して、既存のアクティビティー・コードを削除できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**Visualizer**」ボタンをクリックします。
3. 「アクティビティー・コード **(Activity Codes)**」タブをクリックします。
4. 「アクティビティー・タイプ **(Activity Type)**」ドロップダウン・リストから、「検索 **(SEARCH)**」を選択します。
5. 削除するアクティビティー・コードの横にあるチェック・ボックスを選択します。
6. 「削除 **(Delete)**」ボタンをクリックします。 確認ウィンドウが表示されます。
7. 「**OK**」をクリックします。

ロール・アラート用のアクティビティー・コードの作成

Visualizer には、ロール・アラート用のアクティビティー・コードが用意されています。アラート処理に関連した追加のアクティビティーを追跡する必要がある場合は、構成コンソールを使用して、新規アクティビティー・コードを追加できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**Visualizer**」ボタンをクリックします。
3. 「アクティビティー・コード **(Activity Codes)**」タブをクリックします。
4. 「アクティビティー・タイプ **(Activity Type)**」ドロップダウン・リストから、「競合 **(CONFLICT)**」を選択します。

5. 「新規 **(New)**」ボタンをクリックします。
6. 「アクティビティー・コード **(Activity Code)**」フィールドに、このアクティビティー・コードの名前を入力します。
7. 「アクティビティー状況コード **(Activity Status Code)**」ドロップダウン・リストから、新規アクティビティー・コードが相当する、内部で認識されるアクティビティー状況コードを選択します。
8. 「状況 **(Status)**」ドロップダウン・リストから、「アクティブ **(Active)**」を選択します。
9. 「保存 **(Save)**」ボタンをクリックします。

ロール・アラート用のアクティビティー・コードの削除

Visualizer には、ロール・アラート用のアクティビティー・コードが用意されています。アラート処理に関連したアクティビティー・コードを削除する必要がある場合は、構成コンソールを使用して、既存のアクティビティー・コードを削除できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**Visualizer**」ボタンをクリックします。
3. 「アクティビティー・コード **(Activity Codes)**」タブをクリックします。
4. 「アクティビティー・タイプ **(Activity Type)**」ドロップダウン・リストから、「競合 **(CONFLICT)**」を選択します。
5. 削除するアクティビティー・コードの横にあるチェック・ボックスを選択します。
6. 「削除 **(Delete)**」ボタンをクリックします。 確認ウィンドウが表示されます。
7. 「**OK**」をクリックします。

イベント・アラート用のアクティビティー・コードの作成

Visualizer には、イベント処理を通じて生成されるイベント・アラート用のアクティビティー・コードが用意されています (ご使用のシステムで Event Manager が有効になっている場合)。イベント・アクティビティー・コードを使用すると、イベント・アラートの処理に関連した追加のアクティビティーを追跡できます。システムには、事前定義されたイベント・アクティビティー・コードが 3 つ用意されていますが、構成コンソールを使用して、イベント・アラート用の新規アクティビティー・コードを追加できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**Visualizer**」ボタンをクリックします。
3. 「アクティビティー・コード **(Activity Codes)**」タブをクリックします。
4. 「アクティビティー・タイプ **(Activity Type)**」ドロップダウン・リストから、「**EVENT**」を選択します。
5. 「新規 **(New)**」ボタンをクリックします。
6. 「アクティビティー・コード **(Activity Code)**」フィールドに、新規アクティビティー・コードのユニーク名を入力します。

7. 「アクティビティー状況コード **(Activity Status Code)**」ドロップダウン・リストから、新規アクティビティー・コードが相当する、内部で認識されるアクティビティー状況コードを選択します。
8. 「状況 **(Status)**」ドロップダウン・リストから「アクティブ **(Active)**」を選択して、このアクティビティー・コードが Visualizer で使用可能になるようにします。
9. 「保存 **(Save)**」ボタンをクリックします。

イベント・アラート用に事前定義されているアクティビティー・コード**:**

イベント・アクティビティー・コードは、アナリストが Visualizer でイベント・アラートの後処理を行うときに使用します。インストール後の v4.2 フィックスパック 1 SQL スクリプトを実行すると、システムには、イベント用の事前定義アクティビティー・コードが 3 つ含まれています。

事前定義セットのイベント・アラート・アクティビティー・コードには、以下のイベント・アラート用アクティビティー・コードが含まれています。

ASSIGNED (割り当て済み**)**
アナリストがイベント・アラートを自身または別のアナリスト・グループに割り当てると、システムはデフォルトで ASSIGNED アクティビティー・コードを割り当てます。

CLOSED (クローズ**)**
アナリストがイベント・アラートをクローズすると、システムはデフォルトで CLOSED アクティビティー・コードを割り当てます。

PENDING (保留中**)**
アナリストがイベント・アラートを後処理するよりも前に、システムは自動的にそれらのイベント・アラートに PENDING アクティビティーを割り当てます。つまり、そのイベント・アラートはオープンになり、割り当てられたグループ内のどのアナリストでもレビューや後処理を行うことができます。

イベント・アラート用のアクティビティー・コードの編集

Visualizer でのイベント・アラートの後処理に使用される既存のアクティビティー・コードを編集できます。既存のアクティビティー・コードを名前変更することはできませんが、関連付けられた説明、アクティビティー状況コード、および状況を変更することができます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**Visualizer**」ボタンをクリックします。
3. 「アクティビティー・コード **(Activity Codes)**」タブをクリックします。
4. 「アクティビティー・タイプ **(Activity Type)**」ドロップダウン・リストから、「**EVENT**」を選択します。
5. 編集するアクティビティー・コードをクリックします。
6. 「アクティビティー・コード一般 **(Activity Codes General)**」タブで、変更を行います。 例えば、アクティビティー・コードを構成したいが、そのアクティ

ビティー・コードを Visualizer には選択肢として表示したくない場合、「非アクティブ **(Inactive)**」状況を選択します。そうすることで、後でアクティブ化しようと考えているアクティビティー・コードを削除する必要がありません。

7. 「**OK**」ボタンをクリックします。

イベント・アラート用のアクティビティー・コードの削除

Visualizer には、イベント・アラートを後処理するためのアクティビティー・コードが用意されています。イベント・アラート処理に関連したアクティビティー・コードを削除する必要がある場合は、構成コンソールを使用して、既存のアクティビティー・コードを削除できます (事前定義されているイベント・アラート・アクティビティー・コードも削除できます)。アクティビティー・コードを削除すると、イベント・アラートの処理時に、そのアクティビティー・コードを Visualizer で使用できなくなります。

このタスクについて

アクティビティー・コードの情報を変更するだけであれば、アクティビティー・コードを削除および再作成せずに、アクティビティー・コードを編集することができます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**Visualizer**」ボタンをクリックします。
3. 「アクティビティー・コード **(Activity Codes)**」タブをクリックします。
4. 「アクティビティー・タイプ **(Activity Type)**」ドロップダウン・リストから、「**EVENT**」を選択します。
5. 削除するアクティビティー・コードの横にあるチェック・ボックスを選択します。
6. 「削除 **(Delete)**」ボタンをクリックします。 確認ウィンドウが表示されます。
7. 「**OK**」ボタンをクリックします。

Visualizer の「アクティビティー・コード一般 (Activity Codes General)」タブ

アクティビティー・コードは、アナリストが Visualizer でロール・アラート、イベント・アラート、および検索の後処理を行うときに使用します。

「アクティビティー・タイプ **(Activity Type)**」
: システムによって取り込まれます。アクティビティー・タイプを選択して、アクティビティー・コードを表示、追加、または削除します。
  - 「競合 **(CONFLICT)**」: ロール・アラートの場合に使用
  - 「**EVENT**」: イベント・アラートの場合に使用
  - 「検索 **(SEARCH)**」: Visualizer 検索の場合に使用

「アクティビティー・コード **(Activity Code)**」
: このアクティビティー・コードのユニーク名を入力します。

説明
: このアクティビティー・コードの説明を入力します。

「アクティビティー状況コード **(Activity Status Code)**」
このユーザー・アクティビティー・コードが相当する内部状況コードを選択します。

- 「オープン **(Open)**」
- 「割り当て済み **(Assigned)**」
- 「クローズ **(Closed)**」
- 「フィルタリング済み **(Filtered)**」

状況　このアクティビティー・コードが現在アクティブかどうかを示します。例えば、構成したアクティビティー・コードを非アクティブにしておくことで、アクティビティー・コードを Visualizer に実装する前に、アクティビティー・コードを構成することができます。その後、実装の時期がきたら、そのアクティビティー・コードを編集してアクティブにします。

システム構成設定の管理

システム構成の変更は、以下のプロセスに従って実行できます。

第 5 章 データ用のシステムの構成

IBM InfoSphere Identity Insight を効果的に使用するためには、エンティティー・データベース、エンティティー解決、およびシステム・パラメーターを構成する必要があります。

システム内のデータの構成

IBM InfoSphere Identity Insight を使用する前に、まず、ソース・データと連携するようにエンティティー・データベースを構成する必要があります。

特性タイプの構成

名前、番号、住所、E メール・アドレスのいずれのタイプにも分類できないデータ用に、特性タイプを構成できます。新規データがデータ・ソースに追加され、そのデータを、システム内にまだ構成されていない特性タイプとして分類する場合は、その新規データ用に新規特性タイプを作成する必要があります。

特性

特性とは、一般的には名前、番号、住所、または E メール・アドレスで表されないアイデンティティーに関連付けられる、ユーザー定義の特質や性質です。

この属性によりユーザーは、自分のデータ・ソースにとって意味のある、カスタマイズ可能なエンティティー属性を定義することによって、製品を拡張することができます。

特性タイプ**:**

特性タイプによって、エンティティー・データベースに保管されているデータが編成され識別されます。エンティティー・データベース内に既に構成されているデフォルトの特性タイプの例には、生年月日や性別があります。

デフォルトの特性タイプのいずれでも定義されないデータがある場合は、そのデータ用の新しい特性タイプを作成する必要があります。

例

第 2 世界銀行の信託部門では最近、顧客のタイプに関して新しい種類のデータを追加しました。このデータは、次のような UMF タグを使用して調達ノードに到着します。

```
<attribute>
 <attr_type>cust_type</attr_type>
 <attr_value>merchant</attr_value>
</attribute>
```

この例では、cust_type という名前の新しい特性タイプをセットアップする必要があります。

システムが作成する特性タイプ:

処理される UMF メッセージに未構成の特性タイプが含まれていると、システムが自動的に新しい特性タイプを作成します。

この UMF メッセージの値は、新規作成された特性タイプを使用してデータベースに記録され、UMF 例外が書き込まれます。

システムが自動的に新規特性を作成すると、結果として、次の情報のみが含まれた不完全なデータベース・レコードになります。

- UMF メッセージに基づいた新規 **Type** 情報
- System Created という **Status** 値

特性タイプの表示

特性タイプは、名前、番号、住所、E メール・アドレスのいずれのタイプにも分類できないデータ用です。新規特性タイプの追加を検討している場合に、既存の特性タイプの確認が必要になることがあります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「特性 **(Characteristics)**」タブをクリックします。
4. 表示する特性タイプを選択します。

特性タイプの作成

エンティティーの特性は、システム内でタイプ別に編成されます。

始める前に

新規特性タイプを作成する前に、入力特性データを検討して、既存のいずれかの特性タイプを使用して正確にそのデータを記述できるかどうか確認してください。

このタスクについて

新規特性データを効果的に使用するには、構成コンソールを使用して新規特性タイプを構成する必要があります。データ・タイプ値として DATE を指定して新規特性タイプを作成した場合、新規特性タイプを検証する新規 DQM ルールを作成するための選択項目が示されます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「特性 **(Characteristics)**」タブをクリックします。
4. 「新規 **(New)**」ボタンをクリックします。
5. **「一般 (General)」**タブで、この特性タイプのタイプ、説明、データ・タイプ、クラス、解決での用途、状況、ヒストリー保持、および表示レベルを指定します。

6. 「保存 **(Save)**」ボタンをクリックします。 データ・タイプ値として DATE を指定して新規特性タイプを作成する場合に、新規特性タイプを検証するための新規 DQM ルールを作成することを選択すると、新規特性タイプに基づいて値が事前入力された DQM ルール作成ページにリダイレクトされます。

タスクの結果

UMF ファイル内の、<CHARACTERISTIC_TYPE> として指定されたデータが、システムで処理されるようになりました。

特性タイプの削除

エンティティー・データベースで使用されなくなった既存の特性タイプは、削除してかまいません。

このタスクについて

特性タイプに付随する DQM ルールを作成した場合、それに伴い、対応する DQM ルールを削除したい場合があります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「特性 **(Characteristics)**」タブをクリックします。
4. 削除する特性タイプの横にあるチェック・ボックスを選択します。
5. 「削除 **(Delete)**」ボタンをクリックします。

ヘルプ・トピック

「特性 **(Characteristics)**」 **-** 「一般 **(General)**」タブ**:**

「一般 **(General)**」タブを使用して、特性タイプの詳細を指定します。

タイプ
: 作成する特性タイプの名前を入力します。

説明
: 作成する特性タイプの説明を入力します。

「データ・タイプ **(Data Type)**」
: ドロップダウン・リストから、作成する特性タイプのデータ・タイプを選択します。

  「**CHAR**」
  : 特性タイプのデータ・タイプとして文字を指定するには、このフィールド・タイプを選択します。

  「**CLOB**」
  : 特性タイプのデータ・タイプとして CLOB を指定するには、このフィールド・タイプを選択します。

    CLOB は、大量のデータから成る特性タイプに対して使用する必要があります。

注**:** データ・タイプを CLOB に設定すると、パフォーマンスに悪影響を与える可能性があります。潜在的なパフォーマンスへの影響を軽減するため、可能であれば VARCHAR (Informix の場合は LVARCHAR) を使用してください。

「**DATE**」
特性タイプのデータ・タイプとして日付を指定するには、このフィールド・タイプを選択します。

「**DQM ルールの作成 (Create DQM rule)**」
データ・タイプ値として DATE を指定して新規特性タイプを作成した場合、新規特性タイプを検証する新規 DQM ルールを作成するための選択項目が示されます。新規特性タイプに基づいて値が事前入力された DQM ルール作成ページにリダイレクトされます。

「**VARCHAR**」
特性タイプのデータ・タイプとして可変文字を指定するには、このフィールド・タイプを選択します。

「クラス **(Class)**」
ドロップダウン・リストから、作成する特性タイプのクラスを選択します。

LC 特性タイプのデータ・タイプとして生活特性を指定するには、このフィールド・タイプを選択します。

例えば、身長や体重です。

SC 特性タイプのデータ・タイプとしてシステム特性を指定するには、このフィールド・タイプを選択します。

例えば、航空機の座席の好みや、頻繁な顧客ポイント交換などです。

「解決での用途 **(Resolution Usage)**」
ドロップダウン・リストから、この特性をエンティティー解決に使用するかどうかを選択します。

「なし **(None)**」
特性値がエンティティー解決に使用されないことを指定するには、このフィールド・タイプを選択します。

「確定**/**否定 **(Confirm/Deny)**」
特性値がエンティティー解決に使用されることを指定するには、このフィールド・タイプを選択します。

「候補 **(Candidates)**」
特性値が、候補リストを作成したり候補のスコアを上げたりするために使用されることを指定するには、このフィールド・タイプを選択します。

「候補**/**スコアリングなし **(Candidates/No Scoring)**」
特性値が候補リストの作成に使用されるが、それによって候補のスコアが上がることはないことを指定するには、このフィールド・タイプを選択します。

状況　この特性がアクティブであることを指定するには、ドロップダウン・リストから「アクティブ **(Active)**」を選択します。または、「非アクティブ **(Inactive)**」を選択します。

「ヒストリー保持 **(Keep History)**」
特性タイプ値のヒストリカル状況を記録するには、ドロップダウン・リストから「はい **(Yes)**」を選択します。値が頻繁には変わらない特性タイプに対してのみ使用してください。または、「いいえ **(No)**」を選択します。

「表示レベル **(Display Level)**」
ドロップダウン・リストから、この特性をグラフとレポートに使用するかどうかを選択します。

「なし **(None)**」
この特性タイプの値をグラフやレポートから除外するには、このフィールド・タイプを選択します。

「すべて **(All)**」
この特性タイプの値をすべてのグラフおよびレポートに含めるには、このフィールド・タイプを選択します。

番号タイプの構成

番号として分類できるデータに対しては、番号タイプを構成できます。新規データがデータ・ソースに追加され、そのデータを、システム内にまだ構成されていない番号として分類する場合は、その新規データ用に新規番号タイプを作成する必要があります。

番号

番号とは、番号として分類できるアイデンティティーに関連付けられた、ユーザー定義の特質や性質です。

番号タイプ

番号タイプによって、エンティティー・データベースに保管されている番号データが編成され識別されます。エンティティー・データベース内に既に構成されているデフォルトの番号タイプの例には、電話番号や社会保障番号があります。

デフォルトの番号タイプのいずれでも定義されない番号データがある場合は、そのデータ用の新しい番号タイプを作成する必要があります。

例

第 2 世界銀行の信託部門に、顧客の当座預金口座番号を含む番号データがあるとします。この部門では、この新規データをエンティティー・データベースに追加する必要があります。このデータは、次のような UMF タグを使用して調達ノードに到着します。

```
<number>
 <num_type>ca</num_type>
 <num_value>41510155060</num_value>
</number>
```

この例では、ca という名前の新規番号タイプをセットアップする必要があります。

番号タイプの表示

番号タイプは、番号として分類できるデータ用です。新規番号タイプの追加を計画している場合に、既存の番号タイプの確認が必要になることがあります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「番号 **(Numbers)**」タブをクリックします。
4. 表示する番号タイプを選択します。

番号タイプの作成

新規データがソース・システムに追加され、そのデータを、まだ構成されていない番号タイプとして分類する場合は、新規番号タイプを作成する必要があります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「番号 **(Numbers)**」タブをクリックします。
4. 以下のいずれかのステップを実行します。
   - 新規番号タイプを作成するには、「新規 **(New)**」ボタンをクリックします。
   - 既存の番号タイプに基づいて番号タイプを作成するには、リストから番号タイプを選択した後、「複製 **(Clone)**」ボタンをクリックします。
5. 「一般 **(General)**」タブで、この番号タイプのタイプ、説明、クラス、ユニーク性、解決での用途、状況、ヒストリー保持、場所の確定の重みづけ、場所の否定の重みづけ、およびその他の構成情報を指定します。
6. 「フォーマット **(Format)**」タブで、この番号タイプの最小長、最大長、マスク、マスク充てんの有無、充てん文字、ハッシュ長、およびその他の構成情報を指定します。
7. 「保存 **(Save)**」ボタンをクリックします。

番号タイプの削除

システムで使用されなくなった既存の番号タイプを削除できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「番号 **(Numbers)**」タブをクリックします。
4. リストから番号タイプを選択した後、「削除 **(Delete)**」ボタンをクリックします。

ヘルプ・トピック

「番号 **(Numbers)**」 **-** 「一般 **(General)**」タブ**:**

「一般 **(General)**」タブを使用して、番号タイプの詳細を指定します。

タイプ
作成する番号タイプの名前を入力します。

説明　作成する番号タイプの説明を入力します。

「クラス **(Class)**」
ドロップダウン・リストから、作成する番号タイプのクラスを選択します。

CC　番号タイプとして、クレジット・カードを指定するには、このフィールド・タイプを選択します。

「**MISC**」
番号タイプとして、各種を指定するには、このフィールド・タイプを選択します。

例えば、マイレージ会員番号など。

「**OTHER**」
番号タイプとして、その他を指定するには、このフィールド・タイプを選択します。

例えば、データ・ソース内の不明な番号など。

「**PHONE**」
番号タイプとして電話番号を指定するには、このフィールド・タイプを選択します。

「**PID**」
番号タイプとして個人識別番号を指定するには、このフィールド・タイプを選択します。

例えば、運転免許証番号や社会保障番号など。

「**SYSID**」
番号タイプとしてシステム ID 番号を指定するには、このフィールド・タイプを選択します。

例えば、IP アドレスなど。

「解決での用途 **(Resolution Usage)**」
ドロップダウン・リストから、この番号タイプをエンティティー解決に使用するかどうかを選択します。

「なし **(None)**」
番号値がエンティティー解決に使用されないことを指定するには、このフィールド・タイプを選択します。

「候補 **(Candidates)**」
番号値が、候補リストを作成したり候補のスコアを上げたりするために使用されることを指定するには、このフィールド・タイプを選択します。

状況　この番号がアクティブであることを指定するには、ドロップダウン・リストから「アクティブ **(Active)**」を選択します。または、「非アクティブ **(Inactive)**」を選択します。

「ヒストリー保持 **(Keep History)**」
番号タイプ値のヒストリカル状況を記録するには、ドロップダウン・リスト

から「はい **(Yes)**」を選択します。値が頻繁には変わらない番号タイプに対してのみ使用してください。または、「いいえ **(No)**」を選択します。

「表示レベル **(Display Level)**」
ドロップダウン・リストから、この番号をグラフとレポートに使用するかどうかを選択します。

「なし **(None)**」
この番号タイプの値をグラフやレポートから除外するには、このフィールド・タイプを選択します。

「すべて **(All)**」
この番号タイプの値をすべてのグラフおよびレポートに含めるには、このフィールド・タイプを選択します。

名前データの構成

名前データとは、あらゆる入力 UMF 文書の <NAME> セグメントに含まれるデータのことです。エンティティー解決処理の実行中、名前データが分析され、エンティティー・データベース内の既存エンティティーの名前データに対して比較され、その名前データがどの程度正確に一致しているかに基づいてスコアが与えられます。

IBM Global Name Recognition Name Hasher を使用した拡張名前ハッシュ法

Name Hasher は IBM Global Name Recognition テクノロジーを使用し、入力された名前ごとにバリアント・ハッシュを作成することによって、名前ハッシュ法を強化します。バリアント名前ハッシュがあることで、エンティティー解決は名前の分析およびスコアリング時にファジー名前マッチングを使用できます。

次のシナリオは、Name Hasher を利用した場合の利点を示しています。

- <NAME> セグメントのみでデータの多くを突き合わせることができる
- <NAME> セグメントのみでデータの多くを突き合わせることができるが、データの大半は英語圏という国/地域別環境におけるファーストネーム、ミドルネーム、およびラストネームの表記に準拠していない。

Name Manager の名前スコアリング・アルゴリズムにおいて Name Hasher を使用すると、国/地域別環境の名前を分類し、国/地域別環境のコンテキストの中で候補リスト上の名前を正確に比較してスコアリングすることが可能になります。

Name Hasher はデフォルトでは有効になっていません。構成コンソールを使用して Name Hasher とその関連 DQM 関数を有効にします。

重要**:** 製品バージョン 8.0 または 4.2 から Name Hasher をアップグレードする場合、または Name Hasher を初めて有効にする既存のお客様は、IBM サービスまたは IBM サポートまでお問い合わせください。どちらの場合も、IBM サービスまたは IBM サポートの支援なしには、新規データをエンティティー・データベース内の既存データに対して比較した際に、新規データのエンティティー解決が失敗します。

IBM Global Name Recognition Name Hasher 機能の有効化:

UMF の <NAME> セグメント・データ品質処理のための IBM Global Name Recognition Name Hasher 機能を有効にすることで、名前解析、国/地域別情報分類、および名前ハッシュ生成が強化されます。

始める前に

既存のインストール済み環境において初めて Name Hasher を有効にする場合は、IBM サービス または IBM サポートに連絡し、支援を依頼してください。エンティティー・データベース内の既存データに対する新規データのエンティティー解決が失敗しないようにするため、あらゆるデータ・ソースからのすべての既存データを再ロードする必要があります。

このタスクについて

以下の説明は、Name Hasher を有効にするために完了しなければならないタスクの要約です。どのステップも、構成コンソールを使用して完了します。各タスクのステップバイステップの説明を見るには、当該リンクをクリックしてください。

手順

1. 名前ハッシュを作成するため、DQM 関数 282 を有効にします。この関数は、パイプライン内の Name Hasher 機能をオンにします。 製品バージョン 8.0 フィックスパック 2 よりも前の Name Hasher を使用していた場合は、アップグレード済みの Name Hasher へのマイグレーションの説明を参照してください。DQM 282 で使用されるいくつかのパラメーターの再利用が必要になることがあります。
2. Name Hasher が 複合名前ハッシュ属性を作成できるように、DQM 関数 610 を有効にします。
3. 拡張名前ハッシュ法のための 「デフォルトおよび名前のみ (Default w/ Name Only)」候補ビルダーの構成を行います。
4. 拡張名前ハッシュ法のための各データ・ソースの構成を行います。
5. DQM 関数 252 のフルネーム解析を無効化します。 Name Hasher は、単にフルネームだけではなく、名前のすべての部分について、名前ハッシュ・バリアントを作成します。
6. 拡張名前ハッシュ法のためのDQM ルール 255 の構成を行います。 このステップを完了することで、DQM 255 の名前標準化機能は保持しながら、標準の名前ハッシュ法を無効にして、Name Hasher の拡張名前ハッシュ法を使用します。また、DQM 255 が有効になっていることを確認するパイプライン妥当性検査が失敗してパイプラインがシャットダウンされることがないようにします。
7. UMF <NAME> セグメントのための DQM 関数 260 を有効にします。 この DQM 関数は、名前の国/地域別情報を入力名前データに割り当てます。 Name Hasher は、多国/地域別情報の専門知識を拡張名前ハッシュ法に適用するため、名前の国/地域別情報を必要とします。 Name Manager が有効になっていることを確認してください。 (通常、Name Manager はオンになっています。) DQM ルール 260 を有効にした場合、Name Manager がオンになっていないと、DQM 260 ルールは失敗し、パイプラインがシャットダウンします。

8. Name Hasher のシステム・パラメーターを設定します。 このステップを完了することで、拡張名前ハッシュ法の実行中に使用される、パイプラインに必要なシステム・パラメーターを構成します。

拡張名前ハッシュ法のシステム・パラメーターの構成*:*

エンティティー解決中に Name Hasher を正常に機能させるためには、MM システム・パラメーター HASHLESS_NAMES_ARE_GENERIC のデフォルト値がオフになっている必要があります。この値をオフにすると、Name Hasher の機能がすべての入力名前データに適用されます。

拡張名前ハッシュ法のためのフルネーム解析の無効化*:*

Name Hasher を正常に機能させるためには、<NAME> セグメントの既存の DQM 252 ルールを無効にする必要があります。

IBM Global Name Recognition Name Hasher 機能用の ***DQM 255*** ルールの構成*:*

Name Hasher を正常に機能させるためには、DQM 関数 255 の「**UMF 除外 (UMF Exclude)**」パラメーターの値を構成する必要があります。

このタスクについて

- Name Hasher によって提供される拡張構文解析および拡張ハッシュ法を優先するため、DQM 255 ルールの標準の名前構文解析と名前ハッシュ機能を無効化します。
- DQM 255 ルールが有効であり、DQM 255 ルールが有効であることを必要とするパイプライン妥当性検査の要件が満たされるようにします。

拡張名前ハッシュ法のための候補ビルダーの構成*:*

Name Hasher を正常に機能させるためには、「**デフォルトおよび名前のみ (Default w/ Name Only)**」という候補ビルダー構成に「**特性 (Characteristic)**」というマッチング・タイプが含まれているようにします。

拡張名前ハッシュ法のためのデータ・ソースの構成*:*

拡張名前ハッシュ法を使用する場合は、名前属性の候補リスト生成を許可するように、各データ・ソースを構成する必要があります。これを行うには、候補ビルダー構成を「デフォルトおよび名前のみ **(Default w/ Name Only)**」候補ビルダーに設定します。

複合名前ハッシュ属性の作成*:*

DQM 610 関数は、入力 UMF 文書に含まれている各種の小さい値から新規属性を構築します。 Name Hasher は、DQM 610 を使用して複合名前ハッシュを作成し、それらのハッシュを属性として <NAME> および <ATTRIBUTE> の両 UMF セグメントに格納します。

このタスクについて

結果として得られる複合名前ハッシュ属性には常に、<ATTR_TYPE> として GNR_HASH が含まれます。これらの名前ハッシュ属性を作成することによって、エンティティー解決は名前の分析およびスコアリング時にファジー名前マッチングを使用できます。ファジー名前マッチングの機能があると、アイデンティティーおよびエンティティーの名前データに関する一致の可能性の範囲が広がります。

アップグレード済みの **IBM Global Name Recognition Name Hasher** へのマイグレーション**:**

ご使用の製品で使用していた Name Hasher が製品バージョン 8.0 フィックスパック 2 よりも前のものであった場合は、最新の Name Hasher 機能にアップグレードするのに必要な標準タスクに加えて、以下のタスクを完了してください。

手順

1. 製品インストール・プログラムを使用して、標準の製品アップグレードを実行します。
2. 構成コンソールで、UMF <NAME> セグメントの DQM 関数 660 を無効にします。HTTP URL パラメーターに含まれている **maxVariants** パラメーターおよび **variantScoreThreshold** パラメーターの現行値をコピーするか、または書き留めます。 製品バージョン 8.0 フィックスパック 2 よりも前は、拡張名前ハッシュ機能に使用されていたのは、Web アプリケーション・サーバーで実行される Name Hasher サーブレットでした。製品バージョン 8.0 フィックスパック 2 以降では、Name Hasher 機能はパイプラインに組み込まれています。<NAME> セグメントの DQM 関数 660 を無効にすることで、既存の Name Hasher サーブレットを無効にします。
3. 構成コンソールで、UMF <NAME> セグメントの DQM ルール 282 (名前ハッシュ・バリアント) を有効にし、以下の関数パラメーター値を貼り付けるか、または手動で構成します。

   maxVariants
   この値を、以前に DQM 関数 660 の **maxVariants** パラメーターで使用していたのと同じ値に設定します。

   variantScoreThreshold
   この値を、以前に DQM 関数 660 の **variantScoreThreshold** パラメーターで使用していたのと同じ値に設定します。

   注**:** DQM 関数 660 の URL にこれらのパラメーターの値が含まれていない場合、DQM 関数 282 のデフォルト値を使用してください。
   このステップを完了することで、パイプライン内での Name Hasher 機能をアクティブにします。
4. 構成コンソールで、Name Hasher の システム・パラメーターを構成します。このステップを完了することで、Name Hasher 機能の一部としてパイプラインが使用する必須パラメーターをグローバルに構成します。

代替名解析

入力フルネームを対象とする代替名解析を作成すると、エンティティー解決における名前のスコアリングおよびマッチングの能力が強化されます。

名前を解析して名前の各部分に分割することは、名前マッチングにおける最初のステップの 1 つです。代替名解析とは、名前の変形の候補です。入力名前データを対象とする代替名解析を生成することで、入力された名前が正しく分析およびスコアリングされる可能性を高めることができます。

代替名解析を生成するには、DQM 関数 289 を使用します。デフォルトでは、この関数は有効になっていません。代替名解析を生成するには、構成コンソールで <NAME> セグメント上に DQM 関数 289 を構成する必要があります。

すべての名前に対して代替解析が存在しない場合があります。名前に対して代替名解析が存在し、かつ、その代替解析が 1 次名前解析とは異なる場合にのみ、DQM 関数は、代替解析を含んだ第 2 の <NAME> セグメントを生成します。

例えば、次のような入力名前データがあるとします。

```
<UMF_ENTITY>
 <NAME>
  <NAME_TYPE>M</NAME_TYPE>
  <FULL_NAME>ALLEN CRAIG</FULL_NAME>
 </NAME>
....
</UMF_ENTITY>
```

この例では、このフルネームには、少なくとも 2 つの異なる解析が存在する可能性あります。「Allen」と「Craig」はどちらも、名である可能性もあり、姓である可能性もあります。この名前の代替解析を生成することによって、エンティティー解決処理は、エンティティー・データベース内にあるより多くのエンティティーに対して名前を分析しスコアリングできるようになります。

<NAME> セグメントの <FULL_NAME> UMF タグに DQM 関数 289 が構成されていると、名前処理時に、代替名解析が作成されて UMF レコードに追加されます。結果として得られるレコードは、次のようになります。

```
<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>
```

1 番目の <NAME> セグメントには、1 次名前解析と、元の <NAME_TYPE> 値が含まれています。2 番目の <NAME> セグメントには、生成された代替解析が含まれていて、<NAME_TYPE> 値には ALT と示されています。(この例では、代替解析名タイプの値がデフォルト値であると仮定しています。)

代替名解析を作成するための名前の構成:

代替名解析が作成されるように名前を構成できます。代替名解析を使用することで、複数の名前ハッシュの生成をサポートできます。IBM Global Name

Recognition Name Hasher 機能を使用する場合、代替名解析を作成することで、名前のファジー・マッチング能力を強化して、名前データに関するエンティティー解決を向上させることができます。

始める前に

- Name Manager がオンになっていることと、Name Manager サポート・ファイルのパスがシステム・パラメーターで設定されていることを確認します。 Name Manager サポート・ファイルの有効なパスを設定せずにこの DQM 関数を有効にすると、パイプラインはログにエラーを記録してシャットダウンします。
- 代替名解析機能の DQM 関数を有効にするということは、システム構成を変更するということです。いずれの構成変更の場合も、アクティブなパイプラインを確実に停止してから構成を変更してください。その後、パイプラインを再始動することで、構成変更を使用してパイプラインを再初期化します。

このタスクについて

- V8.0 フィックスパック 2 以降を新規インストールした製品の場合、この DQM 関数は既に構成され、アクティブになっています。
- V8.0 フィックスパック 2 以降にアップグレードした製品の場合、この DQM 関数は構成されていますが、非アクティブになっています。代替名解析を生成するには、既存の DQM 関数の状況を「アクティブ **(Active)**」に変更します。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「**UMF**」 > 「**DQM** ルール **(DQM Rules)**」をクリックします。
2. 「セグメント **(Segment)**」リストから「NAME」 を選択します。
3. 「関数 **(Function)**」に「**289 -** 代替名解析 **(289 - Alternate Name Parsing)**」とリストされている UMF タグ名を選択します。
4. 「状況 **(Status)**」で、「アクティブ (Active)」が選択されていることを確認します。
5. 「パラメーター **(Parameters)**」タブで、以下のパラメーター値を確認または設定します。
   - 「解析スコアしきい値 **(Parse Score Threshold)**」: この値を 0 から 100 までの数値に設定します。スコアが高いほど、作成される代替解析は少なくなります。この値は、入力された名前の代替解析を作成すべきかどうかを判別するために名前パーサーが使用する、最小信頼度スコアのしきい値を設定します。そのしきい値よりも高い信頼度スコアを持つ代替解析が見つからないか、または元々提供されたインバウンド解析のスコアが既にそのしきい値を上回っていると、代替解析は作成されません。
   - 「代替名タイプ **(Alternate Name Type)**」: この名前が代替解析であることを指示する NAME_TYPE の値を入力します。この値は、作成された代替名解析ごとに <NAME> セグメントに追加される UMF タグです。デフォルトでは、この値は ALT に設定されています。エンティティー解決のフル属性情報を保証するため、この値を、構成コンソールで構成した既存のインバウンド NAME_TYPE には設定しないでください。特に、この値は **M** または **A** のいずれにも設定しないでください。
6. 「保存 **(Save)**」をクリックします。

性別判定

入力名前データの処理時に、ときには個人名の性別が要因となって、2 つのエンティティーが一致しているかどうかが判定されることがあります。性別により、確定と否定の重みがエンティティー解決のスコアリングに加算され、2 つのアイデンティティーが同一エンティティーであるかどうかが判別されます。

DQM 関数 258 は、動的に入力 UMF レコード内の <NAME> セグメントの性別を識別し、性別特性を作成し、性別特性を入力 UMF レコードに追加します。性別特性は <ATTRIBUTE> セグメントを使用して追加されます。

- 入力 UMF レコードのデータに既に性別特性が含まれている場合、DQM 関数 258 は別の性別特性を生成することはありません。
- 入力 UMF レコードに複数の <NAME> セグメントが含まれている場合、 DQM 関数 258 は、その入力レコード全体に対して性別特性を 1 つだけ作成します。この場合、複数の性別属性が生成されると、重複または競合する可能性があります。

名前の性別を動的に判別するには、<NAME> セグメント内の UMF タグが少なくとも 1 つ、DQM 関数 258 を使用するように構成されているようにします。

- V8.0 フィックスパック 2 以降を新規インストールした製品の場合、この DQM 関数は既に構成され、アクティブになっています。
- V8.0 フィックスパック 2 以降にアップグレードした製品の場合、この DQM 関数は構成されていますが、非アクティブになっています。この強化された性別機能を使用する場合は、状況を 「アクティブ **(Active)**」 に変更する必要があります。以前に DQM 関数 255 の「性別特性タイプ **(Gender Characteristic Type)**」パラメーターを使用して性別を割り当てていた場合、そのパラメーターの値を NONE にリセットしてください。DQM 255 は引き続きどの UMF <NAME> タグに対しても、名前を標準化するために使用できます。

構成コンソールで次の構成を確認することも推奨されます。

- データ・ソース別に、エンティティー解決における確定または否定として性別特性が構成されていることを確認します。この設定は、「セットアップ **(Setup)**」 > 「ソース **(Sources)**」 > 「特性 **(Characteristics)**」を選択すると見つかる「解決での用途 **(Resolution Usage)**」フィールドで表示または構成します。
- エンティティー解決のための正しい調整値によって性別特性が構成されていることを確認します。この設定は、「セットアップ **(Setup)**」 > 「解決 **(Resolution)**」 > 「特性 **(Characteristics)**」を選択して表示または構成します。性別特性に割り当てられた確定と否定の重みづけの値を調べて、ビジネス・ニーズに適合していることを確認してください。

.

この入力 UMF レコードの以下の <NAME> セグメントの例を検討します。

```
<UMF_ENTITY>
 <NAME>
  <NAME_TYPE>M</NAME_TYPE>
  <LAST_NAME>RASUL</LAST_NAME>
  <FIRST_NAME>KARIM</FIRST_NAME>
 </NAME>
.....
</UMF_ENTITY>
```

<NAME> セグメントの <FIRST_NAME> UMF タグで DQM 258 がアクティブにされると、性別が分析されて作成された後に、入力 UMF レコードは次のレコードのようになります。

```
<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>
```

性別を割り当てるための名前の構成**:**

名前に基づいて性別を割り当てることで、エンティティー解決を強化できます。比較対象のエンティティーの性別が同じであるかどうかに基づいた確定と否定のスコアを設定できます。動的に性別を割り当て、その Gender 特性を入力 UMF レコードに追加するように、名前を構成できます。

始める前に

- Name Manager がオンになっていること、および Name Manager サポート・ファイルのパスがシステム・パラメーターで設定されていることを確認します。Name Manager サポート・ファイルの有効なパスを設定せずにこの DQM 関数を有効にすると、パイプラインはログにエラーを記録してシャットダウンします。
- この DQM 関数の性別機能を有効にするということは、システム構成を変更するということです。いずれの構成変更の場合も、アクティブなパイプラインを確実に停止してから構成を変更してください。その後、パイプラインを再始動することで、構成変更を使用してパイプラインを再初期化します。

このタスクについて

- V8.0 フィックスパック 2 以降を新規インストールした製品の場合、この DQM 関数は既に構成され、アクティブになっています。
- V8.0 フィックスパック 2 以降にアップグレードした製品の場合、この DQM 関数は構成されていますが、非アクティブになっています。この強化された性別機能を使用するには、既存の DQM 関数の状況を 「アクティブ **(Active)**」 に変更します。以前に DQM 関数 255 の「性別特性タイプ **(Gender Characteristic Type)**」パラメーターを使用して性別を割り当てていた場合、そのパラメーターの値を NONE にリセットしてください。DQM 255 は引き続きどの UMF <NAME> タグに対しても、名前を標準化するために使用できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「**UMF**」 > 「**DQM** ルール **(DQM Rules)**」をクリックします。
2. 「セグメント **(Segment)**」リストから「**NAME**」 を選択します。
3. 「関数 **(Function)**」として「**258 - Name Genderizer**」もリストされる、UMF タグ名 **FIRST_NAME** を選択します。 この構成は、個人名に相当する入力レ

コード内のファーストネームのみを評価します。 Name Manager の名前カテゴリー化機能がオンになっている場合、NAME セグメントの LAST_NAME UMF タグに名前全体を指定する必要があります。

4. 「状況 **(Status)**」で、「アクティブ **(Active)**」が選択されていることを確認します。
5. 「ルール・フィルター **(Rule Filter)**」で、フィールド値が NAME_TYPE=M になっていることを確認します。この値により、各入力レコードのメインの名前だけが評価されて性別が割り当てられるようになります。
6. 「パラメーター **(Parameters)**」タブで、「性別の最小信頼度スコア **(Minimum Gender Confidence Score)**」が 0 から 100 までの数値に設定されていることを確認します。 デフォルト・スコアは 90 に設定されています。これは、性別割り当てにおいて 90% の信頼度がなければ性別が割り当てられないことを意味します。最小スコアを 90 未満にすると、エンティティー解決における性別の確定時または否定時に影響します。そのため、このスコアを下げることは慎重に行ってください。
7. 「保存 **(Save)**」をクリックします。

名前のカテゴリー化

Name Manager のシステム・パラメーター **NAMESIFTER** が有効になっていると、この製品は名前をタイプ別にカテゴリー化します。名前をタイプ別にカテゴリー化することで、名前分析、スコアリング、およびマッチング時にエンティティー解決が適切な言語データ・リソースおよび参照データ・リソースを適用することができます。

名前は、個人名または組織名のいずれかのタイプにカテゴリー化されます。

個人名
: 個人名には、他のどのようなカテゴリーに属していることも示唆するインディケーターは含まれていません。 (例えば、「Linda K. Smith」です。) 個人名としてカテゴリー化される名前は、解析されて名前の各部分に分割されます。次に名前の各部分は、国/地域別情報でカテゴリー化され、分析およびスコアリングの処理に精度が加えられます。

組織名
: ビジネス名や組織名には、何らかの形式の非個人のインディケーターが含まれています。 (例えば、「Smith & Company」です。) 組織名としてカテゴリー化される名前には、自動的に「会社 (Company)」という国/地域別情報が割り当てられます。

不明な名前
: 「不明」としてカテゴリー化される名前には、つづりの誤りと考えられる、または、通常は個人名にもビジネス名にも現れない他の構成体であると考えられる、何らかのエレメントが含まれています。 (例えば、「SMI」です。)

名前のタイプ別カテゴリー化**:**

Name Manager システム・パラメーターの 1 つ (**NAMESIFTER**) に、名前をタイプ別にカテゴリー化する機能が組み込まれています。名前の最も一般的なタイプは、

個人およびビジネスです。名前をカテゴリー化することで、エンティティー解決処理における名前の分析およびスコアリングの部分をより正確なものにすることができます。

国/地域別情報ごとの個人名のカテゴリー化:

DQM 関数 260 は、名前の国/地域別情報を判別し、その値を UMF <NAME> セグメントに付加するために作成されました。デフォルトでは、<NAME> セグメント構成の <LAST_NAME> UMF タグに DQM 260 ルールが組み込まれています。DQM 260 ルールを <NAME> セグメント内の別の UMF タグに追加するか、または <LAST_NAME>UMF タグの既存のルールを更新するには、以下の手順を使用します。

Name Manager の概要

Name Manager

Name Manager は、複数の名前文字変換、国/地域内でのつづりの誤り、国/地域内でのスペルの変形、国/地域が異なることによるスペルの変形、父称や敬称の指定を使用する名前など、名前確定に関する高度な問題への対応として、名前の精度を向上させます。 Name Manager は、1,000,000,000 を超える多文化の名前やユニークな言語情報から成る知識ベースが含まれた IBM InfoSphere Global Name Recognition コンポーネント・ライブラリーを使用することで、国/地域にユニークな名前マッチング能力を追加します。

Name Manager は、次の処理を使用して名前のスコアを算出します。

- 名前を名前タイプ (個人またはビジネス) でカテゴリー化する
- 個人名を解析して名前の各部分に分割する
- 名前を国/地域別情報ごとに分類する (アフガニスタン語、アラビア語、ペルシア語、ハン語、日本語、韓国語、タイ語、ベトナム語、ヨルバ語など 20 を超える国/地域別情報をサポート)
- 個人名を正規化する (名前が英語、アラビア語、中国語、フランス語、ドイツ語、スペイン語、インド語、韓国語、ロシア語、またはタイ語のいずれかに分類される場合)

Name Manager の構成

デフォルトでは、 IBM InfoSphere Identity Insight をインストールした時点で既に Name Manager による名前スコアリングは有効化され、構成されています。ただし、構成コンソールを使用すると、次のような Name Manager の構成設定を確認、変更することができます。

- Name Manager コンポーネント・ライブラリーのサポート・パスなどの Name Manager システム・パラメーター (エンティティー解決を実行するためにパイプラインが使用するグローバル・パラメーター)
- 名前マッチング時に使用される Name Manager 名前スコアリングしきい値 (確定と否定)

Name Manager のシステム・パラメーターの構成:

デフォルトでは、製品のインストール時に、Name Manager による名前スコアリングのシステム・パラメーターが構成されます。しかし、必要に応じて、デフォルト

のシステム・パラメーターを更新できます。例えば、Name Manager サポート・ライブラリーの場所の変更が必要になることがあります。

このタスクについて

Name Manager のシステム・パラメーターを通じて、Name Manager サポート・ライブラリーのパスを設定し、タイプ別の名前のカテゴリー化を有効にします。また、**CROSSCHECKCULTURE** システム・パラメーターを設定して、各種国/地域別情報間での名前処理を構成します。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「一般 **(General)**」 > 「システム・パラメーター **(System Parameters)**」を選択します。
2. 「**パラメーター・グループ (Parameter Group)**」 リストから、「**NAMEMANAGER**」パラメーター・グループを選択します。
3. 左側のペインから、構成する Name Manager システム・パラメーターを選択します。

Name Manager システム・パラメーター	説明
「**SUPPORTPATH**」	Name Manager サポート・ファイルの場所を指示します。デフォルト値は ./data で、これは最上位製品ディレクトリーからの相対パスです。インストール時にサポート・ファイルを別の場所に移動した場合は、この値を新しい場所の絶対パスに変更します。
「**NAMESIFTER**」	名前タイプ別 (個人名か組織名か) の名前カテゴリー化機能をオンにするどうかを指示します。 名前のタイプ別カテゴリー化 (名前フィルター機能) を有効にするには、「現行値 **(Current Value)**」に 1 (インストール時の新しいデフォルト) を入力します。 名前のタイプ別カテゴリー化 (名前フィルター機能) を無効にするには、「現行値 **(Current Value)**」に 0 (アップグレード時のデフォルト) を入力します。

Name Manager システム・パラメーター	説明
「**CROSSCHECKCULTURE**」	名前の国/地域別情報が異なる場合に、名前の国/地域別情報間で Name Manager による名前スコアリングを実行するかどうかを指示します。 インバウンド側の名前の国/地域別情報のみを検査してから、両者の名前をスコアリングするには、「現行値 **(Current Value)**」に `0` を入力します。 名前の国/地域別情報の値を検査してから、両者の名前をスコアリングする (インストール時の新しいデフォルト) には、「現行値 **(Current Value)**」に `1` を入力します。

重要: **CROSSCHECKCULTURE** システム・パラメーターは、パイプラインにおいてエンティティー解決がどのように名前スコアリングを国/地域別情報ごとに処理するかに影響します。システム・パラメーターを現行値から変更する場合は、事前に IBM サービス または IBM サポートにご相談ください。

4. 「保存 **(Save)**」をクリックします。

Name Manager での確定と否定のしきい値の構成:

エンティティー解決中に Name Manager が使用する名前スコアしきい値を、解決ルール別に設定できます。候補リストが作成されると、エンティティー解決は、名前の部分および名前の各部分ごとに判別される国/地域別情報に基づいて、これらのしきい値に対して Name Manager の名前スコアを比較します。 Name Manager のスコアが、その名前の部分についての構成済みしきい値スコアを満たしているか、または超えている場合、それらの名前は一致していると見なされます。

このタスクについて

重要: デフォルトでは、Name Manager の名前部分スコアリングしきい値は、Name Manager の最適なスコアリングとパフォーマンスが得られるように構成されています。デフォルト値を変更すると、名前スコアリングが組み込まれたルールのエンティティー解決に悪影響を及ぼす可能性があるため、デフォルト値の変更は高度な構成タスクです。デフォルト値を変更する場合は、事前に IBM サービス または IBM サポートにご相談ください。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「解決 **(Resolution)**」 > 「解決ルール **(Resolution Rules)**」を選択します。
2. 「解決構成 **(Resolution Config)**」リストから解決構成を選択します。
3. 解決ルールを選択します。
4. 「確定/否定しきい値 **(Confirm/Deny Thresholds)**」をクリックします。
5. 「**Name Manager**」の下に、0.0 から 1.0 までのスコアに基づいて、各名前部分のしきい値の最小スコアを入力します。スコアを高くするほど、名前の各部分

がより正確に一致しなければならないことになります。通常、0.7 未満のスコアは名前の各部分のマッチングに適しません。

***Name Manager* による名前スコアリング:**

Name Manager アルゴリズムは、名前を各部分にグループ化した後、名前の各部分の国/地域別情報を判別し、それに基づいて入力名前データのスコアを算出します。次に、このアルゴリズムは名前の各部分のスコアを算出し、結果として得られたスコアがエンティティー解決中に使用されます。

Name Manager アルゴリズムは Name Comparator アルゴリズム (NC1 および NC2) とは別個のものですが、それでもやはり NC1 または NC2 のいずれかを選択する必要があります。エンティティー解決処理の実行中に、まず、選択された Name Comparator アルゴリズムに基づいて名前のスコアが算出されます。名前のスコアが完全一致である場合、完全名前一致は解決ルールの名前スコア部分を満たしているため、エンティティー解決は Name Manager によるスコアリングをスキップします。一方、入力された名前のスコアが完全一致に満たない場合、エンティティー解決処理は Name Manager アルゴリズムを使用して名前のスコアを算出します。

まず、アルゴリズムが名前を解析して名前の各部分 (名、姓、およびフルネーム) に分割した後、アルゴリズムが名前の各部分の国/地域別情報を判別します。最後に、アルゴリズムが名前の各部分にスコアを割り当て、構成済みの Name Manager スコアしきい値に対してスコアを比較し、それらの名前がどの程度正確に一致しているかを判別します。スコアしきい値の設定が高くなるほど、入力名前データの名前の各部分が、エンティティー・データベース内の既存エンティティーの名前の各部分とより正確に一致している必要があります。

Name Manager による名前スコアリングのための国/地域別情報の選択:

エンティティー解決の名前スコアリング処理において、どの名前スコアリング方式が国/地域別情報によって使用されるのかを構成できます。Name Manager ができることは、名前の国/地域別情報を判別し、Name Manager による名前マッチングを使用するように構成されている国/地域別情報に該当する名前をスコアリングすることだけです。

このタスクについて

デフォルトでは、標準的な名前スコアリングのための最新のベスト・プラクティスに基づいて、サポートされている個々の国/地域別情報が既に構成されています。デフォルト値の変更は、名前スコアリングが組み込まれたルールのエンティティー解決に悪影響を及ぼす可能性のある、高度なタスクです。デフォルト構成の値を変更する場合は、事前に IBM サービス または IBM サポートにご相談ください。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「解決 **(Resolution)**」 > 「**Name Manager** のマッチング構成 **(Name Manager Match Config)**」を選択します。
2. Name Manager の国/地域別情報を選択します。

3. 「**Name Manager** の名前マッチングを使用する **(Use Name Manager Name Matching)**」で、「はい (Yes)」を選択します。
4. 「保存 **(Save)**」をクリックします。

DQM ルールの構成

最低データ品質基準を満たさないデータを修復またはクリーンアップするための DQM ルールを構成できます。 DQM ルールは、特定の UMF セグメント内にある特定の UMF タグに適用されます。

このタスクについて

DQM ルールは、コンソールを使用して「**DQM** ルール **(DQM Rules)**」タブで表示および変更できます。

DQM ルール

DQM ルールは、修復、クリーンアップ、および標準化を行う構成済みのシステム定義の関数で、入力アイデンティティーのデータ値に特定の順序で適用されます。

DQM ルールは、システムが入力データをどのように処理するかを定義するもので、数値を適切にフォーマットし、誤記や文字の入れ替わりエラーを識別して修正し、アイデンティティーを隠ぺいしようとする意思によってもたらされた意図的な間違いを識別して修正するように設計されています。DQM ルールは、入力アイデンティティーのデータ値に対して、修復、クリーンアップ、および標準化のためのさまざまな関数を実行できます。

DQM ルールを構成するには、特定の UMF セグメント (NAME など) および UMF タグ (NAME_TYPE など) を選択した後、入力データに適用するシステム定義 DQM 関数を選択し、最後に、その関数の関連パラメーター (システムが適用しなければならないデフォルト値など) を指定します。また、この製品は、UMF セグメントごとに複数の DQM ルールをサポートしているため、選択した UMF セグメントに対してこの DQM ルールを適用するときの順序も選択してください。

DQM ルールの表示

DQM ルールは、最低データ品質基準を満たさないデータを修復またはクリーンアップします。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「**DQM** ルール **(DQM Rules)**」タブをクリックします。
4. 「セグメント **(Segment)**」ドロップダウン・リストから、表示する DQM ルールが含まれている UMF セグメントを選択します。

DQM ルールの作成

最低データ品質基準を満たさないデータを修復またはクリーンアップするための DQM ルールを作成します。

このタスクについて

DQM ルールは、特定の UMF セグメント内にある特定の UMF タグに適用されます。DQM ルールを複製することで新規ルールの基盤を作成することもできます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「**DQM ルール (DQM Rules)**」タブをクリックします。
4. 「セグメント **(Segment)**」ドロップダウン・リストから、DQM ルールの作成の対象となる UMF セグメントを選択します。
5. 以下のいずれかのステップを実行します。
   - 新規 DQM ルールを作成するには、「新規 **(New)**」ボタンを作成します。
   - 既存の DQM ルールに基づいて DQM ルールを作成するには、リストから DQM ルールを選択した後、「複製 **(Clone)**」ボタンをクリックします。
6. 「**一般 (General)**」タブで、この DQM ルールの順序、UMF タグ名、関数、ルール・フィルター、UMF 除外、訂正可否、状況、およびその他の構成情報を指定します。
7. 「**パラメーター (Parameters)**」タブで、DQM ルールのパラメーターを指定します。
8. 「保存 **(Save)**」ボタンをクリックします。
9. DQM ルールを検証します。

DQM ルールの削除

必要なくなった DQM ルールは削除する必要があります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「**DQM ルール (DQM Rules)**」タブをクリックします。
4. 「セグメント **(Segment)**」ドロップダウン・リストから、DQM ルールの削除の対象となる UMF セグメントを選択します。
5. 削除する DQM ルール (複数可) の横にあるチェック・ボックスを選択します。
6. 「削除 **(Delete)**」ボタンをクリックします。

DQM ルールの検証

DQM ルールを追加または編集した場合、ソース・データに適用する前に、その DQM ルールを検証する必要があります。

このタスクについて

検証機能を使用して、すべてのルールを、セグメント全体での相互の関連で検証します。単一ルールを対象に実行できる検証は、ルールの保存時に自動的に実行されます。

構成コンソールへのログイン時に、自動妥当性検査が実行され、DQM ルールが有効であるかどうかが確認されます。エラーが見つかると、構成コンソール画面の最上部にヘッダー・メッセージが表示されます。「エラーの確認 **(Review the errors)**」リンクをクリックすると、別のウィンドウが開いて、エラーの説明が示されます。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「**DQM** ルール **(DQM Rules)**」タブをクリックします。
4. 「セグメント **(Segment)**」ドロップダウン・リストから、DQM ルールの検証の対象となる UMF セグメントを選択します。 セグメントが選択されていない場合、すべてのセグメントに対して検証が実行されます。
5. 「検証 **(Validate)**」ボタンをクリックします。

DQM ルールをオフにする

不要になった DQM ルールをオフにすることができます。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「**DQM** ルール **(DQM Rules)**」タブをクリックします。
4. 「セグメント **(Segment)**」ドロップダウン・リストから、オフにする DQM ルールが含まれている目的の UMF セグメントを選択します。
5. オフにする DQM ルールをクリックします。
6. 「**一般 (General)**」タブで、状況フィールドを「非アクティブ **(Inactive)**」に設定します。
7. 「保存 **(Save)**」ボタンをクリックします。

ヘルプ・トピック

「**DQM** ルール **(DQM Rules)**」 **-** 「一般 **(General)**」タブ**:**

「一般 **(General)**」タブを使用して、DQM ルールの詳細を指定します。

セグメント
: DQM ルールの適用先の UMF セグメント名を入力します。このフィールドは通常は読み取り専用です。このフィールドを編集できるのは、DQM ルールの作成時に「セグメント **(Segment)**」ドロップダウン・リストを空白のままにした場合だけです。このセグメント名は大文字で入力する必要があります。

「順序 **(Order)**」
: この DQM ルールが適用される順序番号を入力します。

「**UMF** タグ名 **(UMF Tag Name)**」
: DQM ルールの適用先の UMF タグ名を入力します。この UMF タグ名は大文字で入力する必要があります。

「関数 **(Function)**」
ドロップダウン・リストから、DQM ルールのベースにする DQM 関数を選択します。

「関数の説明 **(Function Description)**」
この関数の説明フィールドは、何を行う DQM ルールかを説明する読み取り専用フィールドです。

「ルール・フィルター **(Rule Filter)**」
UMF タグに特定の値が含まれている場合にのみ、この DQM ルールが適用されるようにする場合は、UMF タグ名と、DQM ルールの実行に必要な値を含めた式を入力します。

例: `NAME_TYPE=m`
この設定例の場合は、UMF タグ `NAME_TYPE` の値が `m` の場合にのみ DQM ルールが適用されます。

「**UMF** 除外 **(UMF Exclude)**」
この DQM ルールが特定の UMF 入力文書に適用されないようにする場合は、このルールの実行対象としない UMF 入力文書のコンマ区切りリストを入力します。

例: `UMF_QUERY, UMF_DISCLOSED RELATION`
この設定例の場合は、`UMF_QUERY` UMF 入力文書および `UMF_DISCLOSED_RELATION` UMF 入力文書のみが、DQM ルールの適用対象外となります。

「訂正可能 **(Correctable)**」
無効値や不良値を調整するには、ドロップダウン・リストから「はい **(Yes)**」を選択します。または、「いいえ **(No)**」を選択します。

各 DQM ルールのパラメーターによって、どの程度不良なデータ値が調整されるかが決まります。

状況　この DQM ルールがアクティブであることを指定するには、ドロップダウン・リストから「アクティブ **(Active)**」を選択します。または、「非アクティブ **(Inactive)**」を選択します。

ルックアップ・コードの構成

ルックアップ・コードは、アプリケーションの各種機能が使用するデフォルト値です。

ルックアップ・コードは、コード・タイプにより分類されます。DQM ルール 190 を使用すると、入力ルックアップ・コードが定義済みのコード・タイプの一部であることを検証でき、そのコードがない場合は、任意でそのコード・タイプに追加することができます。

ルックアップ・コードの表示

ルックアップ・コードは、アプリケーションの各種機能が使用するデフォルト値です。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. 「コード **(Codes)**」タブをクリックします。
4. 「タイプ **(Type)**」ドロップダウンから、表示するルックアップ・コード値のタイプを選択します。

ルックアップ・コードの作成

ルックアップ・コードは、アプリケーションの各種機能が使用するデフォルト値です。

このタスクについて

新規ルックアップ・コードを作成することも、既存のルックアップ・コードに基づいたルックアップ・コードを作成することもできます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. 「コード **(Codes)**」タブをクリックします。
4. 「タイプ **(Type)**」ドロップダウンから、作成するルックアップ・コード値のタイプを選択します。 完全に新規のコード・タイプを作成するには、値をそのままにします。
5. 以下のいずれかのステップを実行します。
   - 新規ルックアップ・コードを作成するには、「新規 **(New)**」ボタンをクリックします。
   - 既存のルックアップ・コードに基づいてルックアップ・コードを作成するには、リストからルックアップ・コードを選択した後、「複製 **(Clone)**」ボタンをクリックします。
6. 「一般 **(General)**」タブで、このルックアップ・コードのタイプ (「タイプ **(Type)**」 ドロップダウンで既に指定済みの場合は読み取り専用フィールドになります)、コード、説明、状況、およびその他の構成情報を指定します。

ルックアップ・コードの削除

使用しなくなったユーザー作成のルックアップ・コードは削除できます。

このタスクについて

システムのデフォルトのルックアップ・コードは、製品のさまざまなコンポーネントにとって必要ですので、削除しないでください。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. 「コード **(Codes)**」タブをクリックします。

4. 「タイプ **(Type)**」ドロップダウンから、削除するルックアップ・コード値のタイプを選択します。
5. リストからルックアップ・コードを選択した後、「削除 **(Delete)**」ボタンをクリックします。

ルックアップ・コードをオフにする

不要になったルックアップ・コードをオフにすることができます。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. 「コード **(Codes)**」タブをクリックします。
4. 「タイプ **(Type)**」ドロップダウンから、オフにするルックアップ・コード値のタイプを選択します。
5. リストからルックアップ・コードを選択します。
6. **「一般 (General)」**タブで、状況フィールドを「非アクティブ **(Inactive)**」に設定します。
7. 「保存 **(Save)**」ボタンをクリックします。

ヘルプ・トピック

「ルックアップ・コード **(Lookup Codes)**」 **-** 「一般 **(General)**」タブ**:**

「一般 **(General)**」タブを使用して、ルックアップ・コードの詳細を指定します。

タイプ
: どのルックアップ・コード・タイプとしてルックアップ・コードをグループ化するのかを入力します。いったん指定すると、このフィールドは読み取り専用になります。これは、新規ルックアップ・コードの作成時に「タイプ **(Type)**」ドロップダウンを未指定のままにした場合にのみ、編集できます。

コード
: ルックアップ・コードのデフォルト値として選択可能にする値を入力します。これは通常、実際に UMF タグで使用され、データベース表に保管されている値です。既存のルックアップ・コードを編集する場合、このフィールドは読み取り専用になります。

説明　ルックアップ・コードの説明を入力します。

状況　このルックアップ・コードがアクティブであることを指定するには、ドロップダウン・リストから「アクティブ **(Active)**」を選択します。または、「非アクティブ **(Inactive)**」を選択します。

「ルックアップ・コード **(Lookup Codes)**」 **-** 「タイプ **(Type)**」フィールド**:**

「タイプ **(Type)**」フィールドを使用して、どのタイプとしてルックアップ・コードをグループ化するのかを指定します。

「**ADDR_STAT**」
このルックアップ・コード・タイプは、住所の状況値用に使用されます。これらの値は、配送可能な住所であるかどうかといった情報で特定の住所にマークを付けるために使用できます。

「**ADDR_TYPE**」
住所についてのユーザー定義が可能な分類。これらは、ADDR_TYPE UMF タグの有効な値です。

「**ANALYZER_GROUP**」
このルックアップ・コード・タイプは、ロール・アラート・ルールおよび Visualizer によって使用されます。 ANALYZER_GROUP タイプの新規ルックアップ・コードはすべて、「セットアップ **(Setup)**」 > 「関係 **(Relationships)**」 > 「ロール・アラート・ルール **(Role Alert Rules)**」 > 「一般 **(General)**」タブにある「アラート・グループ **(Alert Group)**」ドロップダウン、および「セットアップ **(Setup)**」 > 「**Visualizer**」 > 「**Visualizer** ユーザー **(Visualizer Users)**」 > 「一般 **(General)**」タブにある「グループ **(Group)**」ドロップダウンで選択可能なオプションです。

「**ATTR_CLASS**」
特性タイプについてのユーザー定義が可能な分類。ここで入力した値は、「セットアップ **(Setup)**」 > 「ソース **(Sources)**」 > 「特性 **(Characteristics)**」 > 「一般 **(General)**」タブにある「クラス **(Class)**」ドロップダウンに、オプションとして表示されます。属性クラスとして LINK ルックアップ・コードを使用する特性は、その特性の値が次の形式に従っている場合は、Visualizer 内に HTML リンクとして表示することができます。

Link Display Text=URL

「**ATTR_MATCH_LEVEL**」
このルックアップ・コード・タイプは推奨されません。

「**CONF_LEVEL**」
このルックアップ・コード・タイプは推奨されません。

「**DENSITY_LOG_LEVEL**」
このルックアップ・コード・タイプは推奨されません。

「**DOC_TYPE**」
このルックアップ・コード・タイプは推奨されません。

「**DSRC_ACTION**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**EX_CLASS**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**EX_SEVERITY**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**LOG_LEVEL**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**ER_LEVEL**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**ER_LOG_LEVEL**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**LDR_MESSAGE_TYPE**」
このルックアップ・コード・タイプは推奨されません。

「**MM_STAT**」
このルックアップ・コード・タイプは推奨されません。

「**NAME_TYPE**」
このルックアップ・コード・タイプは、名前のユーザー定義可能分類を保管するために使用されます。これらは、NAME_TYPE UMF タグの有効な値です。

「**NS-FGEN**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**NS-LGEN**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**NS-PREFIX**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**NS-SUFFIX**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**NUM_CLASS**」
このルックアップ・コード・タイプは、番号タイプのユーザー定義可能分類を保管するために使用されます。ここで入力した値は、「セットアップ **(Setup)**」 > 「ソース **(Sources)**」 > 「番号 **(Numbers)**」 > 「一般 **(General)**」タブにある「クラス **(Class)**」ドロップダウンに、オプションとして表示されます。

「**REC_STAT**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**SEARCH_REASON**」
このルックアップ・コード・タイプは、属性アラート検索の理由フィールドに表示されるドロップダウン・オプションのリスト用として、Visualizer によって使用されます。ユーザーは、その有効な属性アラート理由の独自のリストを、ここで追加できます。

「**SYS_DELETE_STAT**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

「**UNIQUE_FLAG**」
このルックアップ・コード・タイプは推奨されません。

「**USABILITY_LOG_LEVEL**」
このルックアップ・コード・タイプはシステムで使用されます。変更しないでください。

汎用データ値の構成

エンティティー・データベース内でのデータ値の出現回数が構成済みの回数を超えた場合に、それらのデータ値が汎用となるように構成できます。

汎用値

エンティティー・データベース内に繰り返し発生し、その結果、システムがエンティティー解決に使用しなくなったデータ値を記述したものが、汎用値です。

データ値は、特定のしきい値を超えると、汎用であると見なされます。このしきい値とは、データ値を共有できるエンティティー・データベースでの、エンティティーの最大発生回数を構成したものです。

汎用値は、属性別および属性タイプ別に編成されて構成されます。ある特定の属性タイプの汎用データ値は、その親属性の汎用データ値をオーバーライドします。値が汎用であると見なされる可能性のある標準データ・エレメントは、次のとおりです。

- 住所
- 特性
- E メール
- 名前
- 番号

例

電話番号の汎用しきい値が 25 に設定されている場合、ある電話番号値 (例えば 555-555-5555 など) が 25 件を上回るエンティティーの電話番号値であることが検出された時点で、それ以降その特定値はエンティティー解決に使用されなくなります。

注**:** 汎用しきい値をどの程度高い値に設定するか検討する際は、汎用しきい値の設定を高くしすぎると、汎用であるべきデータが大量になることで、最終的にはシステム・パフォーマンスに悪影響が及ぶ可能性があることを考慮してください。逆に、汎用しきい値の設定を低くしすぎると、キーとなる基準も汎用と見なされるため、重要なアラートが生成されない場合があります。

汎用データ値の表示

汎用データ値は、汎用と見なす各データ・エレメントの汎用しきい値です。新規のデータ・ソースを追加する場合に、既存の汎用値の確認が必要になることがあります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「汎用しきい値 **(Generic Threshold)**」タブをクリックします。

汎用データ値の構成

汎用値がエンティティー解決中に無視されるようにするには、そのデータ・エレメントの汎用しきい値を構成する必要があります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「汎用しきい値 **(Generic Threshold)**」タブをクリックします。
4. 以下のいずれかのステップを実行します。
   - 新規汎用データ値を作成するには、「新規 **(New)**」ボタンをクリックします。
   - 既存の汎用データ値に基づいて汎用データ値を作成するには、リストから汎用データ値を選択した後、「複製 **(Clone)**」ボタンをクリックします。
5. 「一般 **(General)**」タブで、汎用値の属性、属性タイプ、およびしきい値を指定します。
6. 「保存 **(Save)**」ボタンをクリックします。

汎用データ値の削除

汎用データ値は、汎用と見なす各データ・エレメントの汎用しきい値です。入力データとの関連がなくなった既存の汎用データ値は、削除してかまいません。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「汎用しきい値 **(Generic Threshold)**」タブをクリックします。
4. 削除する既存のエレメント名の横にあるチェック・ボックスを選択します。
5. 「削除 **(Delete)**」ボタンをクリックします。

ヘルプ・トピック

「汎用しきい値 **(Generic Threshold)**」 **-** 「一般 **(General)**」タブ**:**

「一般 **(General)**」タブを使用して、汎用データ値の詳細を指定します。

「属性名 **(Attribute Name)**」
ドロップダウン・リストから、汎用データ値の適用対象とする属性を選択します。

属性タイプ
: ドロップダウン・リストから、汎用データ値の適用対象とする属性タイプを選択します。

  このドロップダウン・リストに複数のオプションが表示されるのは、「属性名 **(Attribute Name)**」フィールドが Name または Characteristic に設定されている場合のみです。

「しきい値 **(Threshold)**」
: 構成されたタイプの UMF 値 1 つが汎用と見なされるまで、その UMF 値を共有できるエンティティーの数を入力します。

ロールの構成

エンティティー・データベース内のエンティティーを分類するためのロールを構成できます。ロールは、データ・ソースまたはエンティティーに割り当てることができます。ロールが競合しているとアラートが生成されます。

このタスクについて

ロールは、コンソールを使用して「データ・ソース」タブで表示および変更できます。

ロール

ロールとは、アイデンティティーの分類であり、そのアイデンティティーの重要点または目的を定義します。アイデンティティーには、1 つ以上のロールを関連付けることができます。アイデンティティーはエンティティーに解決されるため、エンティティーは、関連付けられたロールをすべて継承します。

ロールを使用してロール・アラート・ルールを構成します。このルールでは、関心のある関係を定義し、アラートを生成します。

次の 2 つの方法のいずれかで、すべてのアイデンティティーにロールを割り当てます。

入力データ・ソースによって
: 新規データ・ソースを構成するときに、そのデータ・ソースにロールを関連付けます。これにより、そのデータ・ソース・コードを含んでいるすべてのアイデンティティーに、そのロールが割り当てられます。

UMF によって
: データ・ソースを Universal Message Format (UMF) に変換するとき、<SEP_ROLES> UMF セグメントと <ROLE_CODE> UMF タグを使用して、UMF レコードの一部として、ロールを直接割り当てることができます。UMF によって構成した場合は、DQM ルールと参照表を追加する必要があります。

有益なロールの例としては、従業員、ベンダー、顧客、監視リストなどがあります。

UMF を使用したロール割り当ての例

UMF を使用して Employee (従業員) のロールをアイデンティティー・レコードに割り当てるには、アイデンティティー・レコードに対して、以下のように <SEP_ROLES> UMF セグメントおよび <ROLE_CODE> UMF タグを入力します。

```
<SEP_ROLES>

  <ROLE_CODE>Employee</ROLE_CODE>

</SEP_ROLES>
```

ロールの表示

ロールは、システム内でエンティティーがどのように分類されるか、またはどのように認識されるかを定義します。新規ロールの追加を計画している場合に、既存のロールの確認が必要になることがあります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「関係 **(Relationships)**」ボタンをクリックします。
3. 「ロール・コード **(Role Codes)**」タブをクリックします。
4. 表示するロールを選択します。

ロールの作成

エンティティーが他のエンティティーとどのように関連するかを定義するには、システム内にロールを作成します。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「関係 **(Relationships)**」ボタンをクリックします。
3. 「ロール・コード **(Role Codes)**」タブをクリックします。
4. 以下のいずれかのステップを実行します。
   - 新規ロールを作成するには、「新規 **(New)**」ボタンをクリックします。
   - 既存のロールに基づいてロールを作成するには、リストからロールを選択した後、「複製 **(Clone)**」ボタンをクリックします。
5. 「一般 **(General)**」タブで、この新規ロールのロール・コード、説明、クラス、状況、およびその他の構成情報を指定します。
6. 「保存 **(Save)**」ボタンをクリックします。

次のタスク

ロール・アラート・ルールを定義するときに、このロールを使用できます。

ロールの削除

ロールは、システム内でエンティティーがどのように分類されるか、またはどのように認識されるかを定義します。もはや有効でなくなった既存のロールは、削除してかまいません。

このタスクについて

ロール・アラート・ルールやデータ・ソースで使用されているロールは削除できません。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「関係 **(Relationships)**」ボタンをクリックします。
3. 「ロール・コード **(Role Codes)**」タブをクリックします。
4. 削除する既存のロールの横にあるチェック・ボックスを選択します。
5. 「削除 **(Delete)**」ボタンをクリックします。

ヘルプ・トピック

「ロール **(Roles)**」 **-** 「一般 **(General)**」タブ**:**

「一般 **(General)**」タブを使用して、ロールの詳細を指定します。

「**ID**」
ロール ID を識別するユニークな整数を入力します。

ID 値には、使用されていない次の連番が自動的に取り込まれます。

「ロール・コード **(Role Code)**」
このロールを識別するユニーク値を入力します。

説明　このロールの説明を入力します。

「ロール・クラス **(Role Class)**」
このロールのロール・クラスを入力します。

状況　このロールがアクティブであることを指定するには、ドロップダウン・リストから「アクティブ **(Active)**」を選択します。または、「非アクティブ **(Inactive)**」を選択します。

ロール・アラート・ルールの構成

ロール・アラート・ルールを構成することで、ロールの組み合わせを定義できます。このロールの組み合わせが検出されると、アラートが生成されます。

このタスクについて

ロール・アラート・ルールは、コンソールを使用して「ロール・アラート・ルール **(Role Alert Rules)**」タブで表示および変更できます。

ロール・アラート

ロール・アラートは、アラートの生成に使用される関係を表したロール・アラート・ルールによって、システム内に定義されます。

ロール・アラート・ルールとは、関係またはエンティティー内に検出された場合に何らかの形式の競合を表す、ロールの組み合わせを定義したものです。例えば、「従業員 (Employee)」ロールを持つエンティティーが「ベンダー (Vendor)」ロールを持つエンティティーを知っている場合には常にロール・アラートが存在することを、ロール・アラート・ルールで示す場合があります。このロール・アラート・

ルールは、「従業員はベンダーを知っている (Employee knows Vendor)」と記述することができます。システムがエンティティーまたは関係にロール・アラートを見つけると、アラート (エンタープライズへの公開および Analyst ツールキット・アプリケーションでの確認が可能) が作成されます。

ほとんどのロール・アラート・ルールは、競合を示唆する 2 つの異なるロールの組み合わせを指定するものですが、あるロールのエンティティーが同じロールの別のエンティティーを知っていることを示すロール・アラート・ルールを設定することも妥当です。例えば、自分の顧客間のあらゆる関係を把握し、ある顧客エンティティーが別の顧客エンティティーと関連する場合にはいつでもロール・アラートを生成するようなロール・アラート・ルールを作成したいと考える場合があります。このロール・アラート・ルールは、「顧客は顧客を知っている (customer knows customer)」と記述することができます。

ロール・アラート・ルールは、既存のロール・コードに基づきます。ロールに関連した競合ルールを作成するためには、事前にそのロールを定義する必要があります。

ロール・アラート・ルールの表示

ロール・アラート・ルールは、2 つの定義済みロール間の関係が検出された場合にアラートを生成するために使用します。新規ロール・アラート・ルールの追加を計画している場合に、既存のロール・アラート・ルールの確認が必要になることがあります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「関係 **(Relationships)**」ボタンをクリックします。
3. 「ロール・アラート・ルール **(Role Alert Rules)**」タブをクリックします。
4. 表示するロール・アラート・ルールを選択します。

ロール・アラート・ルールの構成

2 つのロール間つまりアイデンティティー間のロール・アラートや関係を生成するロール・アラート・ルールを構成します。

始める前に

ロール・アラート・ルールを定義する前に、まずロール・アラート・ルールで使用するロールを構成する必要があります。例えば、従業員がベンダーであってはならない、というロール・アラート・ルールを構成する場合、「従業員 (Employee)」および「ベンダー (Vendor)」というロールがシステムに含まれている必要があります。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「関係 **(Relationships)**」ボタンをクリックします。
3. 「ロール・アラート・ルール **(Role Alert Rules)**」タブをクリックします。
4. 以下のいずれかのステップを実行します。

- 新規ロール・アラート・ルールを作成するには、「新規 **(New)**」ボタンをクリックします。
- 既存のロール・アラート・ルールに基づいてロール・アラート・ルールを作成するには、リストからロール・アラート・ルールを選択した後、「複製 **(Clone)**」ボタンをクリックします。

「ロール・アラート・ルール **ID (Role Alert Rule ID)**」フィールドには、自動的に次のユニーク ID が入力されます。これは任意のユニーク ID 番号に変更できます。

5. 「新規 **(New)**」ボタンをクリックします。
6. 「一般 **(General)**」タブで、このロール・アラート・ルールの ID、説明、重大度、ロール・コード、アラート・グループ、およびアラートの最小しきい値を指定します。
7. 「フィルター **(Filters)**」タブでは、オプションとして、アイデンティティー・フィルター、データ変更フィルター、およびパスの強度調整 (「データ変更フィルター (data change filter)」フィールドが 「パスの強度調整 (Path Strength Adjustment)」に設定されている場合のみ表示される) を指定します。 両方のフィルターが設定されている場合、一方のフィルターが満たされているだけでロール・アラートは生成されます。
8. 「保存 **(Save)**」ボタンをクリックします。

ロール・アラート・ルールの削除

ロール・アラート・ルール内の定義済みロールが削除されることになった場合や、ロール・アラート・ルール内のそのロールの組み合わせにはもはや関心がない場合、そのようなロール・アラート・ルールは削除する必要があります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「関係 **(Relationships)**」ボタンをクリックします。
3. 「ロール・アラート・ルール **(Role Alert Rules)**」タブをクリックします。
4. 削除する既存のロール・アラート・ルールの横にあるチェック・ボックスを選択します。
5. 「削除 **(Delete)**」ボタンをクリックします。

ヘルプ・トピック

「ロール・アラート・ルール **(Role Alert Rules)**」 **-** 「一般 **(General)**」タブ**:**

ロール・アラート・ルールの詳細を構成するには、「ロール・アラート・ルール **(Role Alert Rules)**」ウィンドウの「一般 **(General)**」タブを使用します。ロールはデータ・ソースに関連付けられます。データ・ソースからシステムに入力された個々のアイデンティティーには、そのデータ・ソースがどのように構成されているかに基づいて、ロールが割り当てられます。ロール・アラート・ルールにより、入力アイデンティティーに割り当てられたロールと、エンティティー・データベース内のエンティティーに関連付けられたアイデンティティーに割り当てられたロールとの間の競合に基づいて、ロール・アラートを生成するタイミングを定義します。

「ロール・アラート・ルール **ID (Role Alert Rule ID)**」
ID 値には、使用されていない次の連番が自動的に取り込まれます。

説明　このロール・アラート・ルールの説明を入力します。このロール・アラート・ルールに基づいてロール・アラートが生成された場合は常に、このテキストが Visualizer に表示されます。

「重大度 **(Severity)**」
このルールによって生成されるアラートの重要度をカテゴリー化するのに使用される、ユーザー定義の 1 文字のコード。

ロール・アラートの重大度をその重要度と一致させます。このコードは、このロール・アラート・ルールによって生成されたロール・アラートとともに Visualizer に表示されます。アナリストはこれを使用して、どのアラートを最初に検討すべきか、優先順位を付けます。したがって、この 1 文字のコードは Visualizer ユーザーにとって有意義なはずです。例えば、ある乗客が搭乗拒否リストに載っている誰かと一致した場合には常にアラートを生成するロール・アラート・ルールは、ある従業員がある顧客を知っている場合にアラートを生成するように設計されたロール・アラート・ルールと比べて、より検討が不可欠である可能性があります。

例えば、重大度コードの例として、重大を表す C (critical)、中程度を表す N (neutral)、対象であることを表す I (interesting)、高を表す H (high)、低を表す L (low) などがあります。

「ロール **1 (Role 1)**」
ドロップダウン・リストから、このロール・アラート・ルールで比較する最初のロールを選択します。

表示されるロール・オプションは、既存の、構成済みのロールです。選択する必要のあるロールが表示されていない場合は、「ロール **(Roles)**」タブでロールを構成してください。

「ロール **2 (Role 2)**」
ドロップダウン・リストから、このロール・アラート・ルールで比較する 2 番目のロールを選択します。

表示されるロール・オプションは、既存の、構成済みのロールです。選択する必要のあるロールが表示されていない場合は、「ロール **(Roles)**」タブでロールを構成してください。

「アラート・グループ **(Alert Group)**」
ドロップダウン・リストから、このロール・アラート・ルールによって生成されるロール・アラートを分析する Visualizer アナライザー・グループを選択します。例えば、「搭乗拒否リストに載っている乗客がいる」というロール・アラートはすべてセキュリティー・デスクに送信し、「従業員がベンダーを知っている」というロール・アラートはすべて人事部門に送信する、といったことが可能です。

表示されるグループ・オプションは、アクティブであり、構成済みであり、コード・タイプが `ANALYZER_GROUP` である Visualizer アナライザー・グループです。選択する必要のあるグループが表示されていない場合は、最初に、「セットアップ **(Setup)**」 **-** 「一般 **(General)**」 **-** 「コード **(Codes)**」タブで新規 ANALYZER_GROUP コードを構成してください。

これは必須フィールドです。したがって、たとえ組織で Visualizer を使用していない場合であっても、アラート・グループ・コードを構成して選択する必要があります。

「ロール・アラート・ルール **(Role Alert Rules)**」タブ**:**

両方のフィルターが設定されている場合、一方のフィルターが満たされているだけでロール・アラートは生成されます。

「アイデンティティー・フィルター **(Identity Filter)**」
ロール・アラートに関与するエンティティーに新規アイデンティティーが追加された場合に、ロール・アラート生成を制限するには、ドロップダウン・リストからこのフィルターを選択します。

このフィルターが影響するのは、再アラート動作のみです。特定のエンティティー・セットについて初めてロール・アラート・ルールが満たされたときには、常にロール・アラートが生成されます。このフィルターを使用すると、関与するエンティティーに変更が加えられた場合に同じロール・アラートがさらに生成されるのを防ぐことができます。

「オフ **(Off)**」
ロール・アラートに関与するエンティティーに新規アイデンティティーが追加された場合のロール・アラート制限をオフにするには、このフィールド・タイプを選択します。

「新規アイデンティティー **(New Identity)**」
ロール・アラートに関与するエンティティー内のアイデンティティー間に新規データ・ソース・コードが取り込まれたときにのみアラートを再生成するには、このフィールド・タイプを選択します。

「新規データ・ソース・コード **(New Data Source Code)**」
アイデンティティー間に新規データ・ソース・コードが取り込まれたときにアラートを生成するには、このフィールド・タイプを選択します。

「データ変更フィルター **(Data Change Filter)**」
ロール・アラートに関与するエンティティーに新規属性データが追加された場合に、ロール・アラート生成を制限するには、ドロップダウン・リストからこのフィルターを選択します。

このフィルターが影響するのは、再アラート動作のみです。特定のエンティティー・セットについて初めてロール・アラート・ルールが満たされたときには、常にロール・アラートが生成されます。このフィルターを使用すると、関与するエンティティーに変更が加えられた場合に同じロール・アラートがさらに生成されるのを防ぐことができます。

「オフ **(Off)**」
ロール・アラートに関与するエンティティーに新規属性データが追加された場合のロール・アラート制限をオフにするには、このフィールド・タイプを選択します。

「新規属性データ **(New Attribute Data)**」
ロール・アラートに関与するエンティティーに新規属性データが追加されたときにのみアラートを再生成するには、このフィールド・タイプを選択します。

「パスの強度調整 **(Path Strength Adjustment)**」
新規属性データが追加された結果として「パスの強度調整 **(Path Strength Adjustment)**」値以上にパスの強度が変わることになる場合にのみアラートを再生成するには、このフィールド・タイプを選択します。

「パスの強度調整 **(Path Strength Adjustment)**」
このフィールドは、「データ変更フィルター **(Data Change Filter)**」ドロップダウンが「パスの強度調整 (Path Strength Adjustment)」に設定されている場合にのみ表示されます。「データ変更フィルター **(Data Change Filter)**」を「パスの強度調整 (Path Strength Adjustment)」に設定した場合に使用する調整値 (-100 から 100) を入力します。これにより、新規属性データが追加された結果として、「パスの強度調整 (Path Strength Adjustment)」値以上にパスの強度が変わることになる場合にのみロール・アラートが再生成されるようになります。ゼロを指定した場合は、フィルターをオフにしたのと同じです。

エンティティー・タイプの構成

エンティティーの正確な性質を識別するためのエンティティー・タイプを構成できます。

このタスクについて

新規アイデンティティー・データがデータ・ソースに追加され、そのデータを、システム内にまだ構成されていないエンティティー・タイプとして分類する場合は、その新規データ用に新規エンティティー・タイプを作成する必要があります。

エンティティー・タイプは、コンソールを使用して「エンティティー・タイプ **(Entity Types)**」タブで表示および変更できます。

エンティティー・タイプ

エンティティー・タイプは、エンティティーの正確な性質を識別するためにエンティティーに関連付けられる、ユーザー定義の特質や性質です。

インパーソナル認識では、本来 1 次関係を持つことがないであろうエンティティーを、エンティティー・タイプを使用してリンクします。

例えば、通話によってインパーソナル関係を見つける場合、「通話 *(Phone call)*」という新規エンティティー・タイプを作成し、調達ノードを調整して、エンティティー・タイプが「通話 *(Phone call)*」 である各通話レコードに正しくタグを付けます。

通話レコードがパイプラインに取り込まれると、エンティティー解決および関係解決の処理が「通話 *(Phone call)*」 エンティティーと発呼側エンティティー (個人) 間

の 1 次関係を見つけます。これはまた、電話を受けた個人と「通話 *(Phone call)*」エンティティー間の 1 次関係も見つけます。何もしないと、こうした個人間の 1 次関係は検出されません。

```
<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>
```

インパーソナル認識

インパーソナル認識は、従来の関係解決処理を拡張してインパーソナル関係を検出および分析する製品機能です。関係検出処理では、エンティティーに関連付けられた属性値に基づいて、エンティティー間の関係を見つけます。ときには、アクティビティーまたはその他のインパーソナル ID に基づいてエンティティー間の関係を見つけることが重要な場合があります。こうした、アクティビティーまたはその他のインパーソナル ID に基づいたエンティティー間の関係を、インパーソナル 関係と呼び、人を関連付けるアクティビティーやインパーソナル ID を、関連事実 と呼びます。

インパーソナル関係は常に 2 次以上の隔たりに存在します。これは、関連事実が、それ自体で 1 つのエンティティーであるからです。そのため、インパーソナル認識を有効にしてインパーソナル関係を検出するには、隔たり度合い機能を使用するようにデータ・ソースを構成します。これで、エンティティー解決および関係解決が拡張され、2 次より大きな隔たりにある関係が検出されます。

例えば、電話トランザクションには電話番号に関するデータ (発信者の電話番号と受信者の電話番号の両方) が含まれています。ある個人が別の個人に電話をかけたとしても、その電話トランザクションだけでは、それらの個人の属性として共通のデータを関連付けることはできません。多くの場合、関連事実 (電話呼び出し) のほうが、関連エンティティー (電話で話していたその 2 人の人) に関する他のどのような情報よりも前に把握されます。これらの関連事実を 1 人の個人の属性として関連付けることはできないため、人ではないが人に関連する、別個のエンティティーとして表す必要があります。しかしながらインパーソナル認識では、電話の結果として、2 人の個人の間に関係が存在することを認識します。

UMF にはエンティティー・タイプ機能が組み込まれているため、これを使用して、関連事実をエンティティー・タイプとして定義することができます。この機能を使用すると、関連事実はエンティティー・データベース内で別個のエンティティーとなり、Person エンティティー間の関係検出に使用できるようになります。新規エンティティー・タイプを構成し、UMF 内で適切なエンティティー・タイプを指定し、新規解決構成を作成することで、これらの関連事実を使用してエンティティー間のインパーソナル関係および競合を自動的に検出することができます。

たとえ解決ルールで許可されている場合であっても、あるいはデータが解決をサポートしていても、異なるエンティティー・タイプのエンティティーが相互解決されることは決してありません。つまり、エンティティー・タイプ Phone call がエンティティー・タイプ Person に解決されることはありません。

Analyst ツールキットは、インパーソナル関係および関連付けられたあらゆるアラートを、パーソナル関係および関連付けられたアラートの場合とまったく同様に、グラフ化し、レポート化します。

インパーソナル認識の例

例えば、通話によってインパーソナル関係を見つける場合、「通話 (Phone call)」という新規エンティティー・タイプを作成し、調達ノードを調整して、エンティティー・タイプが「通話 *(Phone call)*」 である各通話レコードに正しくタグを付けます。

通話レコードがシステムに取り込まれると、標準のエンティティー解決および関係解決が Phone call エンティティーと発呼側エンティティー (Person) 間の 1 次の関係を検出します。電話を受けた個人と Phone call エンティティー間の 1 次の関係も検出されます。ただ、それだけではシステムは個人間の関係は検出しません。

しかし、隔たり度合いが構成されていると、引き続き分析されて、発信者と着信者の 2 次のインパーソナル関係が検出されます。インパーソナル関係は、Phone call エンティティー・タイプの属性である電話番号に基づいて存在します。その後、隔たり度合いによってインパーソナル関係が分析され、競合が見つかった場合はアラートが生成されます。

エンティティー・タイプの表示

エンティティー・タイプは、エンティティーの正確な性質を識別するためにエンティティーに関連付けられる、ユーザー定義の特質や性質です。新規エンティティー・タイプの追加を検討している場合に、既存のエンティティー・タイプの確認が必要になることがあります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「エンティティー・タイプ **(Entity Types)**」タブをクリックします。
4. 表示するエンティティー・タイプを選択します。

エンティティー・タイプの作成

エンティティー・タイプは、エンティティーの正確な性質を識別するためにエンティティーに関連付けられる、ユーザー定義の特質や性質です。システムに新規タイプのデータを追加する予定がある場合に、システムへの新規エンティティー・タイプの追加が必要になることがあります。

始める前に

新規エンティティー・タイプを作成する前に、入力アイデンティティー・データを検討して、既存のいずれかのエンティティー・タイプを使用して正確にそのデータを記述できるかどうか確認してください。

このタスクについて

インパーソナル認識では、本来 1 次関係を持つことがないであろうエンティティーを、エンティティー・タイプを使用してリンクします。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「エンティティー・タイプ **(Entity Types)**」タブをクリックします。
4. 「新規 **(New)**」ボタンをクリックします。
5. **「一般 (General)」**タブで、ID 、タイプ、説明、エンティティー解決構成、汎用コントリビューター、ロール・アラート・コントリビューター、検索タイプを指定するとともに、このエンティティー・タイプの解決を許可します。
6. 「保存 **(Save)**」ボタンをクリックします。

タスクの結果

システムがデータにエンティティー・タイプを割り当て、インパーソナル認識を使用して、本来 1 次関係を持つことがないであろうエンティティーをリンクできるようになりました。

エンティティー・タイプの削除

エンティティー・データベースで使用されなくなった既存のエンティティー・タイプは、削除してかまいません。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「エンティティー・タイプ **(Entity Types)**」タブをクリックします。
4. 削除する特性タイプの横にあるチェック・ボックスを選択します。
5. 「削除 **(Delete)**」ボタンをクリックします。

ヘルプ・トピック

エンティティー・タイプ **-** 「一般 **(General)**」タブ**:**

「エンティティー・タイプ **(Entity Types)**」タブを使用して、エンティティー・タイプの詳細を指定します。

「**ID**」
: 作成するエンティティー・タイプの ID 番号を入力します。

  ID は、自動的に 1 つずつ増加する数字コードです。使用可能な次の番号が順番に割り当てられますが、「ID」フィールドに任意のユニーク数値を入力して、コードをその数値に設定することもできます。

タイプ
: 作成するエンティティー・タイプの名前を入力します。

  例えば、Phone call というエンティティー・タイプを使用して、2 つのアイデンティティー間の実際の通話記録であるエンティティーを記述することができます。

説明　作成するエンティティー・タイプの説明を入力します。

「エンティティー解決構成 **(Entity Resolution Configuration)**」
ドロップダウン・リストから、ロード時にこのエンティティー・タイプが使用する解決構成を選択します。

解決構成は、「セットアップ **(Setup)**」 > 「解決 **(Resolution)**」 > 「解決構成 **(Resolution Configs)**」画面で設定します。

「汎用コントリビューター **(Generic Contributor)**」
このエンティティー・タイプのデータが汎用になることを許可するには、ドロップダウン・リストから「はい **(Yes)**」を選択します。または、「いいえ **(No)**」を選択します。

「ロール・アラート・コントリビューター **(Role Alert Contributor)**」
このエンティティー・タイプのデータがロール・アラートを生成することを許可するには、ドロップダウン・リストから「はい **(Yes)**」を選択します。または、「いいえ **(No)**」を選択します。

「検索タイプ **(Search Type)**」
このエンティティー・タイプのデータが検索に使用されることを許可するには、ドロップダウン・リストから「はい **(Yes)**」を選択します。または、「いいえ **(No)**」を選択します。

「解決を許可 **(Allow Resolve)**」
このエンティティー・タイプのデータがエンティティーの解決に使用されることを許可するには、ドロップダウン・リストから 「はい **(Yes)**」を選択します。または、「いいえ **(No)**」を選択します。

隔たり度合いの概要

隔たり度合い機能により、IBM Relationship Resolution の関係マッチング能力が拡張されます。

IBM InfoSphere Identity Insight のデフォルトの動作では、関心の高い関係が特定され、エンティティーに解決されたインバウンド・アイデンティティーから 1 次の隔たりにあるエンティティーが照合されます。隔たり度合い機能を有効化すると、これらの機能が、エンティティーに解決されたインバウンド・アイデンティティーからほぼ無限の範囲のユーザー定義隔たり度合いに拡張されます。

隔たり度合い機能では、隔たり構成、ロール、ロール・アラート・ルール、および関係スコアを使用して、非常に大きいデータ・セットに対してリアルタイムのリンク分析を行います。

インバウンド・アイデンティティーがエンティティーに解決されると、IBM InfoSphere Identity Insight が検出した 1 次の関係を使用してエンティティー・グラフが作成されます。エンティティー・グラフでは、この 1 次の関係を使用して、インバウンド・アイデンティティーの解決先となったエンティティーから派生する複数次の関係チェーンが作成されます。これで、インバウンド・アイデンティティーが解決された先のエンティティーから派生した 2 つの複数次の関係チェーンをリンクすることで、ロール・アラート・チェーンを作成できます。その後、このロール・アラート・チェーンを使用して、複数次の関係の各チェーンの末端まで包括的にエンティティー間の関係を見つけることができます。

隔たり度合いにより、2 つのエンティティーを結ぶすべてのパスを評価し、関係報告において最も強いパスの強度を使用することにより、作業が軽減されます。隔たり度合いは、インバウンド・アイデンティティーの解決先となったエンティティーごとに、構成済みロール・アラート・ルール 1 つにつきロール・アラートを 1 つ報告するように構成できます。

隔たり度合いの構成は、コンソールの「システム構成」タブで「隔たり度合い (Degrees of Separation)」の値を使用して設定できます。

隔たり度合いの例

この例では、1 つの関係パスを通じて、隔たり度合い構成がロール・アラートの判別にどのように織り込まれるかを示します。

隔たり度合いの例

入力データを処理した後、Identity Insight は次のような関係パスを報告したとします。

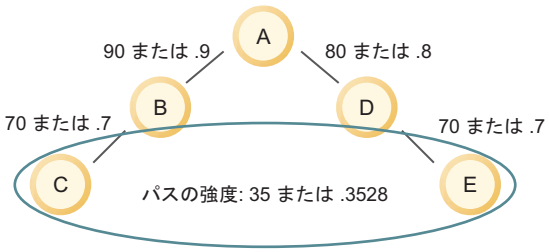
- エンティティー A はエンティティー B を知っている。
- エンティティー B はエンティティー C を知っている。
- エンティティー A はエンティティー D を知っている。
- エンティティー D はエンティティー E を知っている。

関係パス とは、あるエンティティーを別のエンティティーにリンクする、エンティティーと属性のチェーンです。

関係およびロール・アラートの処理の一部として、Identity Insight は関係パスの強度を判別します。パスの強度とは、チェーン内のすべてのエンティティーの関係スコアを小数に変換したものの積を、整数に変換したものです。

この例では、製品は次のように関係スコアを計算し、それらのスコアを小数に変換します。

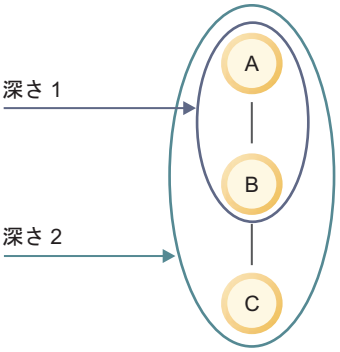
- エンティティー A がエンティティー B を知っている関係スコアは 90。90 が小数 0.9 に変換される。
- エンティティー B がエンティティー C を知っている関係スコアは 70。70 が小数 0.7 に変換される。
- エンティティー A がエンティティー D を知っている関係スコアは 80。80 が小数 0.8 に変換される。
- エンティティー D がエンティティー E を知っている関係スコアは 70。70 が小数 0.7 に変換される。



関係パスの関係スコアが乗算されます。計算結果は .3528 という関係パスの強度で、これが整数 35 に変換されます。

その後、製品は計算されたパス強度を、構成済みの隔たり度合いパラメーター **path strength threshold** に対して比較します。関係パスの強度が構成済みのパスしきい値を満たしているか、または超えている場合、製品はロール・アラートを生成します。関係パスの強度が構成済みのパス強度しきい値に満たない場合、製品はロール・アラートを生成しません。

その後、製品は構成済みの隔たり度合いパラメーター **max depth** を使用して、関係チェーン内のエンティティー間の隔たり度合いを計算します。この max depth の設定により、ロール・アラート検出の一部と見なすことのできる、複数次の関係パス内の最大隔たり度合いが決まります。



通常、**max depth** パラメーターは 2 に設定されています。

この例では、**max depth** パラメーターは 6 に設定されています。エンティティー C とエンティティー E はロールが競合していて 6 次隔たっているため、ロール・アラートが生成されます。

隔たり構成の表示

この製品では複数の隔たり構成が許可されるため、特定の隔たり構成の設定を表示するには、以下の手順を使用します。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「関係 **(Relationships)**」 > 「隔たり構成 **(Separation Configuration)**」をクリックします。
2. 隔たり構成を選択します。

新規隔たり構成の作成

関係解決が検出するエンティティー間の隔たりが 1 次なのか、2 次なのか、複数次なのかを決定する隔たり構成を定義します。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「関係 **(Relationships)**」 > 「隔たり構成 **(Separation Configuration)**」をクリックします。
2. 「新規 **(New)**」をクリックします。
3. 「一般 **(General)**」タブで、この隔たり構成の設定を指定します。

4. 「保存 **(Save)**」をクリックします。

隔たり構成の編集

2 つのエンティティーが何次隔たっていても関係が考慮されるかを決定する設定を変更するには、隔たり構成を編集します。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「関係 **(Relationships)**」 > 「隔たり構成 **(Separation Configuration)**」をクリックします。
2. 編集する「隔たり構成 **(separation configuration)**」を選択して変更を加えます。
3. 「保存 **(Save)**」をクリックします。

ヘルプ・トピック

「隔たり構成 **(Separation Configuration)**」 **-** 「一般 **(General)**」タブ**:**

「一般 **(General)**」タブを使用して、隔たり構成の詳細を指定します。

「**ID**」
: 隔たり構成を識別するユニークな整数を入力します。

  ID 値には、使用されていない次の連番が自動的に取り込まれます。

コード
: このロールを識別するユニーク値を入力します。

説明　この隔たり構成の説明を入力します。

「最大深さ **(Max depth)**」
: ロール・アラート検出が考慮されるエンティティー・グラフ内の 1 つの複数次の関係チェーンにおける、隔たり度合いの最大数。

「パスの強度しきい値 **(Path strength threshold)**」
: ロール・アラート・チェーンの算出済みの **path strength threshold**。パスの強度がこのしきい値を下回るロール・アラート・チェーンは、ロール・アラートを生成しません。

  パスの強度は、ロール・アラート・チェーン内のすべてのエンティティーの関係スコアを小数に変換したものの積を、整数に変換したものです。このパラメーターのデフォルト設定は 15 です。

  隔たり度合いは、2 つのエンティティーを結ぶすべてのパスを評価し、関係報告において最も強いパスの強度を使用します。

UMF 文書の構成

Unified Messaging Format (UMF) 文書を正常に使用するには、それらの文書がシステムにとって既知であり、構成されていることが必要です。

デフォルトの UMF 入力文書の表示

UMF 入力文書は、エンティティー・データベースを対象としてデータをロードしたり変更したりクエリーしたりするための、入力データを構造化する UMF セグメントの集合です。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「入力文書 **(Input Documents)**」タブをクリックします。

出力文書の構成

出力文書フォーマット・コードを使用する場合は、その有効化状況を構成する必要があります。

このタスクについて

UMF 出力文書は UMF 結果データをフォーマットします。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「出力文書 **(Output Documents)**」タブをクリックします。
4. 編集する UMF 出力文書フォーマット・コードが含まれている行内の任意のリンクをクリックします。
5. 「有効 **(Enabled)**」ドロップダウン・リストから、UMF 出力文書フォーマット・コードの適切な状況を選択します。
6. 「保存 **(Save)**」ボタンをクリックします。

データ・ソースの構成

エンティティー・データベースにロードする新しいデータ・ソースがある場合、そのデータ・ソースを構成する必要があります。

始める前に

データ・ソースを構成するには、まずロールをセットアップする必要があります。

このタスクについて

データ・ソースは、コンソールを使用して「データ・ソース」タブで表示および変更できます。

データ・ソース

データ・ソースには、エンティティー解決のために処理してエンティティー・データベースにロードする必要のある、アイデンティティーが含まれています。データ・ソースには、識別データ (アイデンティティーのユニークな個人 ID) と、非識別データ (アイデンティティーのその他の属性やデータ・ポイント) が含まれています。このデータ・ソース内のアイデンティティー・レコードをシステムで処理したり、エンティティー・データベースにロードしたりするためには、事前にそれらのレコードを Universal Message Format (UMF) としてエクスポートする必要があります。データ・ソースの例には、従業員リスト、監視リスト、顧客リスト、ベンダー・リストがあります (これらに限定されるわけではありません)。

データ・ソースには、元のソースに関する情報 (元のデータは UMF に変換済みであるため) や、データ・ソースの外部参照など、重要な情報が含まれています。これらの詳細によって、各データ・ソースがシステム内でユニークとなります。

エンティティー解決時に、2 つのエンティティーが未解決となった場合、システムはデータ・ソース情報を使用して、どの情報がどのエンティティーと結び付いているのかを判別します。

データ・ソースの場所とソース・システム

ソースの場所とソース・システムを作成し、それらをデータ・ソースに関連付けることで、入力データ・ソースを整理できます。ソースの場所とソース・システムを使用すると、同じようなタイプのデータ・ソースを区別することができます。

例えば、複数の場所からの予約データと人材データを処理する場合、次のようにデータ・ソースの場所を使用することで、どの場所から提供されたデータであるかを判別できます。

- プロパティー X 予約データ
- プロパティー X 人材データ
- プロパティー Y 予約データ
- プロパティー Y 人材データ

データ・ソース別の構成

エンティティー解決および関係検出の結果を最大化するには、以下の設定を使用して各データ・ソースを構成します。

ロール
: データ・ソースは同じタイプのデータをグループ化したものであるため、同じ入力データ・ソース内のすべてのアイデンティティー・レコードに自動的に同じロールを割り当てることができます。例えば、人材のデータ・ソースに「従業員 (Employee)」ロールを関連付けることで、従業員リストからのすべての入力レコードに自動的に「従業員 (Employee)」ロールが割り当てられます。

ロード・レベル
: 入力データ・ソース内のすべてのデータをロードするのか、1 つ以上のエンティティーに解決されるデータまたは 1 つ以上のエンティティーに関連するデータだけをロードするのかを決定できます。

関係解決の設定
: 関係検出レベルをデータ・ソース別に構成することができます。例えば、あるデータ・ソースについて関係解決をオフにしたり、その特定のデータ・ソース内での関係検出用の隔たり度合いを選択したりできます。

データ・ソースの表示

データ・ソースには、エンティティー・データベースにロードされるデータが含まれています。新規データ・ソースの追加を計画している場合に、既存のデータ・ソースの確認が必要になることがあります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「データ・ソース **(Data Sources)**」タブをクリックします。
4. 表示するデータ・ソースを選択します。

データ・ソースの構成

データをエンティティー・データベースに正常にロードするには、各データ・ソースを認識するようにシステムを構成する必要があります。

始める前に

データをシステムにロードするためには、データ・ソースに UMF 標準が使用されている必要があります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「データ・ソース **(Data Sources)**」タブをクリックします。
4. 「新規 **(New)**」ボタンをクリックします。
5. 「一般 **(General)**」タブで、このデータ・ソースの ID、説明、およびその他の構成情報を指定します。
6. **「エンティティー解決 (Entity Resolution)」**タブをクリックします。
7. **「エンティティー解決 (Entity Resolution)」**タブで、データ・ソースの解決構成情報を指定します。
8. **「関係 (Relationships)」**タブをクリックします。
9. **「関係 (Relationships)」**タブで、データ・ソースの関係構成情報を指定します。
10. 「保存 **(Save)**」ボタンをクリックします。

Name Manager の名前マッチング・レベルの構成

名前データはソースごとに異なる可能性があるため、Name Manager のマッチング・レベルは、データ・ソース別に構成します。選択したマッチング・レベルは、このデータ・ソースから入力された名前とどの程度厳格に突き合わせるかを決める、比較パラメーターです。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「ソース **(Sources)**」 > 「データ・ソース **(Data Sources)**」をクリックします。
2. データ・ソースを選択します。
3. 「エンティティー解決 **(Entity Resolution)**」をクリックします。
4. 「**Name Manager** のマッチング・レベル **(Name Manager Match Level)**」で、突き合わせのレベルを選択します。ほとんどの場合は、「デフォルト **(Default)**」値を使用してください。これは十分厳格であり、良好な名前一致が得られます。

拡張名前ハッシュ法のためのデータ・ソースの構成

拡張名前ハッシュ法を使用する場合は、名前属性の候補リスト生成を許可するように、各データ・ソースを構成する必要があります。これを行うには、候補ビルダー構成を「デフォルトおよび名前のみ **(Default w/ Name Only)**」候補ビルダーに設定します。

データ・ソースの削除

データ・ソースには、エンティティー・データベースにロードされるデータが含まれています。もはや存在しないデータ・ソースや、エンティティー・データベースとの関連がなくなった既存のデータ・ソースは、削除してかまいません。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「データ・ソース **(Data Sources)**」タブをクリックします。
4. 削除するデータ・ソースの横にあるチェック・ボックスを選択します。
5. 「削除 **(Delete)**」ボタンをクリックします。

データ・ソースの場所の作成

データ・ソースを分類するための場所を選択するには、システム上でその場所が構成されている必要があります。

このタスクについて

データ・ソースの場所を、構成コンソールを使用して作成します。これは、データ・ソースが物理的な複数の場所からデータを収集する場合に主に使用されるオプションです。例えば、データを複数の物理的なホテルの場所から収集するホテル・システムのデータベースです。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. 「ロケーション **(Locations)**」タブをクリックします。
4. 「新規 **(New)**」ボタンをクリックします。
5. 「一般 **(General)**」タブで、このデータ・ソースの場所の場所コード、場所名、地区、会社、緯度、経度、状況、およびその他の構成情報を指定します。
6. 「保存 **(Save)**」ボタンをクリックします。

次のタスク

新たに構成した場所を、システム内のデータ・ソースに適用できるようになりました。

ヘルプ・トピック

「データ・ソース **(Data Sources)**」 **-** 「エンティティー解決 **(Entity Resolution)**」タブ**:**

「エンティティー解決 **(Entity Resolution)**」タブを使用して、データ・ソースのエンティティー解決の詳細を指定します。

「エンティティー解決構成 **(Entity Resolution Configuration)**」
リストから、データのロード時にこのデータ・ソースが使用する解決構成を選択します。

「候補ビルダー構成 **(Candidate Builder Configuration)**」
リストから、このデータ・ソースからのデータのロード時に、エンティティー解決の処理中に使用される適切な候補ビルダー構成を選択します。

デフォルト **(Default)**
デフォルトの候補ビルダー構成を使用するには、この設定を選択します。

「デフォルトおよび名前のみ **(Default w/ Name Only)**」
デフォルトの候補ビルダー構成に加えて、名前のみのマッチングを使用するには、この設定を選択します。

このデータ・ソースに関して、Name Hasher を使用して名前データを処理するには、この候補ビルダー構成を選択します。 (Name Hasher のシステム・パラメーターが設定されていることを確認してください。)

「特性確定 **(Characteristic Confirmation)**」
このデータ・ソースからのデータのロード時に、特性確定を処理することを指定するには、リストから「はい **(Yes)**」 を選択します。または、「いいえ **(No)**」を選択します。

「切り離しの実行 **(Perform Detach)**」
この設定は通常、ホテル・システムのみに使用されます。

データ・ソース・アカウントを持たないデータの突き合わせをパイプラインが行えることを指定するには、リストから 「はい **(Yes)**」 を選択します。突き合わせが成功しなかった場合、事前データに対して削除日が設定されます。または、「いいえ **(No)**」を選択します。

「**Name Manager** のマッチング・レベル **(Name Manager Match Level)**」
このデータ・ソースからの入力名前データのスコアリング時に使用する比較レベルの値を、リストから選択します。

デフォルト **(Default)**
最も一般的な名前一致比較レベルを使用するには、この値を選択します。

「緩い **(Loose)**」
このデータ・ソースからより多くの名前一致を生成したい場合、この値を選択します。この値を選択すると、デフォルト値ほど比較の基準が厳しくならないように、名前一致比較レベルが緩和されます。

「緊密 **(Tight)**」
このデータ・ソースからより少ない名前一致を生成したい場合、この値を選択します。この値を選択すると、デフォルト値よりも比較の基準が厳しくなるように、名前一致比較レベルが厳格になります。

「未解決を許可 **(Allow Unresolve)**」
未解決機能とは、入力データからの新規情報に基づいて、解決済みのアイデンティティーを 2 つの別個のエンティティーに分離する処理です。リストから、このデータ・ソースについて適切な選択を行います。

- このデータ・ソース用のアカウントのロード時に、正当であるなら、アイデンティティーを別個のエンティティーに分離するエンティティー解決を許可するには、「はい **(Yes)**」を選択します。
- このデータ・ソース用のアカウントのロード時に、エンティティー解決によってアイデンティティーが別個のエンティティーに分離されるのを防止するには、「いいえ **(No)**」を選択します。

データ・ソース **-** 「一般 **(General)**」タブ**:**

「一般 **(General)**」タブを使用して、データ・ソースの詳細を指定します。

「**ID**」
作成するデータ・ソースの ID 番号を入力します。

ID は、自動的に 1 つずつ増加する数字コードです。使用可能な次の番号が順番に割り当てられますが、「ID」フィールドに任意のユニーク数値を入力して、コードをその数値に設定することもできます。

コード
作成するデータ・ソースのコードを入力します。

これは、DSRC_CODE UMF タグの値です。データ・ソース・コード値は英数字で、データ・ソースをさらに識別するために使用されます。この値はユニークでなければならず、いったんレコードを保存した後は変更できません。

説明　作成するデータ・ソースの説明を入力します。

「ロケーション **(Location)**」
ドロップダウン・リストから、作成するデータ・ソースのロケーション・コードを選択します。

このフィールドは参照専用です。

「ソース・システム **(Source System)**」
ドロップダウン・リストから、作成するデータ・ソースのソース・システム・コードを選択します。

このフィールドは参照専用です。

状況　このデータ・ソースがアクティブであることを指定するには、ドロップダウン・リストから「アクティブ **(Active)**」を選択します。または、「非アクティブ **(Inactive)**」を選択します。

「アクションを信頼 **(Trust Action)**」
データ・ソースからの ACTION UMF タグの正確度に頼れることを指定するには、ドロップダウン・リストから「はい **(Yes)**」を選択します。または、

「いいえ **(No)**」を選択して、エンティティー・データベースを調べてアクションを決定します。「いいえ **(No)**」を選択すると、パフォーマンスの低下を招きます。

「検索用 **(For Searching)**」
このデータ・ソースを使用して検索をロードすることを指定するには、ドロップダウン・リストから「はい **(Yes)**」を選択します。または、「いいえ **(No)**」を選択します。

「文字変換 **(Transliterate)**」
このデータ・ソースを対象に文字変換が行われる必要があることを指定するには、ドロップダウン・リストから「はい **(Yes)**」を選択します。これにより、Latin 1 文字セットがサポートされるようになります。または、「いいえ **(No)**」を選択します。

注**:** どのデータ・ソースについても、文字変換の設定を有効にする場合は、データ・ソース ID 1589 (検索) 用の文字変換構成設定も有効にしてください。1589 データ・ソースは、この製品がパイプラインに検索を入力するために使用され、デフォルトでは ASCII 文字入力が想定されます。この構成を有効にすると、検索の一部である名前も適切に文字変換されるようになるため、最も正確な検索結果が得られます。

「データ・ソース **(Data Sources)**」 **-** 「関係 **(Relationships)**」タブ**:**

「関係 **(Relationships)**」タブを使用して、データ・ソースの関係の詳細を指定します。

「ロール **(Role)**」
このデータ・ソースに割り当てるロール・コードを選択します。

「データ・ソース・クラス **(Data Source Class)**」
このデータ・ソース用の適切なデータ・ソース・クラスを選択します。

「フル・ロード **(Full Load)**」
データをデータベースにロードするには、このフィールド・タイプを選択します。

この設定にすると、解決可能なアイデンティティーがすべて解決され、エンティティーが更新され、可能性のある関係がすべて検出され、ユーザー定義のロール・アラートが生成されます。

「完全にパッシブ **(Fully Passive)**」
データをデータベースにロードしないためには、このフィールド・タイプを選択します。

完全にパッシブにロードした場合、データは保管されません。Visualizer はアラートを表示できません。

「解決される**/**関連する場合にロード **(Load if Resolve/Relate)**」
データがエンティティー・データベース内の既存のレコードに解決されるか、または関連している場合に、データをデータベースにロードするには、このフィールド・タイプを選択します。

この設定にすると、解決可能なアイデンティティーがすべて解決され、エンティティーが更新され、可能性のある関係がすべて検出され、ユーザー定義のロール・アラートが生成されます。

「選択的に解決される/関連する場合にロード **(Load if Selective Resolve/Relate)**」
データがエンティティー・データベース内の既存のレコードに解決されるか、または関連している場合で、かつこのデータ・ソースが SELECTIVE_PASSIVE_CONFIG 表で構成されている場合にのみ、データをデータベースにロードするには、このフィールド・タイプを選択します。

この設定にすると、解決可能なアイデンティティーがすべて解決され、エンティティーが更新され、可能性のある関係がすべて検出され、ユーザー定義のロール・アラートが生成されます。

「選択的に関連する場合にロード **(Load if Selective Resolve)**」
データがエンティティー・データベース内の既存のレコードに関連している場合で、かつこのデータ・ソースが SELECTIVE_PASSIVE_CONFIG 表で構成されている場合にのみ、データをデータベースにロードするには、このフィールド・タイプを選択します。

また、この設定にすると、解決可能なアイデンティティーがすべて解決され、エンティティーが更新され、可能性のある関係がすべて検出され、ユーザー定義のロール・アラートが生成されます。

「隔たりレベル **(Separation Level)**」
ドロップダウン・リストから、このデータ・ソース用の適切な隔たりレベルを選択します。

「データをロード **(Load Data)**」
常にこのフィールド・タイプを選択してください。現在、これが唯一のオプションです。

「**DoS** 構成 **(DoS Configuration)**」
ドロップダウン・リストから、このデータ・ソース用の適切な隔たり度合い構成を選択します。

隔たり構成は、「セットアップ **(Setup)**」 > 「関係 **(Relationships)**」 > 「隔たり構成 **(Separation Config)**」画面で設定します。

「場所 **(Locations)**」 **-** 「一般 **(General)**」タブ**:**

「場所 **(Locations)**」タブを使用して、データ・ソースの場所の詳細を指定します。

「場所コード **(Location Code)**」
このデータ・ソースの場所に割り当てる場所コードを入力します。

英数字の値で、いったんレコードを保存した後は変更できません。

この値は必須です。

「場所名 **(Location Name)**」
このデータ・ソースの場所に割り当てる場所名を入力します。

「地区 **(District)**」
このデータ・ソースの場所に割り当てる地区を入力します。

この値は必須です。

「会社名 **(Company)**」
このデータ・ソースの場所に割り当てる会社名を入力します。

「緯度 **(Latitude)**」
このデータ・ソースの場所の緯度を次の形式で入力します。

DD:MM:SS

「経度 **(Longitude)**」
このデータ・ソースの場所の経度を次の形式で入力します。

DD:MM:SS

状況　このデータ・ソースの場所がアクティブであることを指定するには、ドロップダウン・リストから「アクティブ **(Active)**」を選択します。または、「非アクティブ **(Inactive)**」を選択します。

関係検出をオフにする

ビジネス要件として求められるものが、誰が誰であるかを判別することだけであり、誰が誰を知っているかを判別する必要がないのであれば、エンティティー間の関係検出は行わずに、エンティティー解決だけを実行するように関係解決を構成することによって、新規レコードごとに必要になる処理時間を短縮し、システム全体のパフォーマンスを上げることができます。

始める前に

構成コンソールの現行セッションにログインするときに「構成の編集 **(Edit Configuration)**」を選択したことを確認してください。

手順

1. 各データ・ソースのロール割り当てをオフにします。
   a. 「セットアップ **(Setup)**」をクリックします。
   b. 「ソース **(Sources)**」をクリックします。
   c. 「データ・ソース **(Data Sources)**」タブで、編集するデータ・ソースをクリックします。
   d. 「関係 **(Relationships)**」タブをクリックします。
   e. 「ロール **(Role)**」ドロップダウン・リストから、「**— 1** つ選択してください **— (— Select One —)**」を選択します。
   f. 「隔たりレベル **(Separation Level)**」ドロップダウン・リストから、「アラートのみ **(Alerts Only)**」を選択します。
   g. 「保存 **(Save)**」をクリックします。
2. 「デフォルトのロール割り当て (Default Role Assignments)」データ品質管理ルールを無効にします。
   a. 「セットアップ **(Setup)**」をクリックします。
   b. 「**UMF**」をクリックします。

c. 「**DQM ルール (DQM Rules)**」タブで、「セグメント **(Segment)**」ドロップダウン・リストから「ルート **(ROOT)**」を選択します。

d. DQM 551、つまり「デフォルトのロール割り当て (Default Role Assignment)」関数が含まれている行の、任意のリンクをクリックします。

e. 「一般 **(General)**」タブで、「状況 **(Status)**」ドロップダウン・リストから「非アクティブ **(Inactive)**」を選択します。

f. 「保存 **(Save)**」をクリックします。

3. エンティティーを解決するように設定されていない解決ルールをすべて削除します。

a. 「セットアップ **(Setup)**」をクリックします。

b. 「解決 **(Resolution)**」をクリックします。

c. 「解決ルール **(Resolution Rules)**」タブをクリックします。

d. 「解決構成 **(Resolution Config)**」ドロップダウン・リストから、「デフォルト **(DEFAULT)**」を選択します。

e. 「解決をトリガーする **(Triggers Resolve)**」列に「いいえ **(No)**」という値が表示されている解決ルールの横にあるチェック・ボックスをクリックします。

f. 「削除 **(Delete)**」をクリックします。

g. 選択した解決ルールの削除を確認するには、「**OK**」をクリックします。

4. 最後に、すべての競合ルールを削除します。

a. 「セットアップ **(Setup)**」をクリックします。

b. 「関係 **(Relationships)**」をクリックします。

c. 「競合ルール **(Conflict Rules)**」タブをクリックします。

d. 競合する各ルールの横にあるチェック・ボックスをクリックします。

e. 「削除 **(Delete)**」をクリックします。

f. 選択した競合ルールの削除を確認するには、「**OK**」をクリックします。

次のタスク

関係検出はせずに、エンティティーを解決するように、システムが構成されました。

イベント・タイプの構成

Event Manager で処理されるイベントを定義およびカテゴリー化するには、イベント・タイプを構成します。ただし、イベント・タイプが含まれている入力データをシステムが処理する前に、ユーザーが、Event Manager のシステム・パラメーターでイベント処理を有効にし、Eclipse ベースの複合イベント・プロセッサー・ツールでビジネス・ルールを構成し、UMF EVENT データ・セグメント定義を使用して入力イベント・データをフォーマット設定する必要があります。

イベント・タイプは、コンソールを使用して「イベント・タイプ **(Event Types)**」タブで表示および変更できます。

イベント・タイプ

イベント・タイプによって、イベントをカテゴリー化し、Event Manager でイベントに関連付けられた値の計測単位を定義します。イベント・タイプの例には、電信送金、口座開設、クレジット・カード取引などがあります。

イベント・プロセッサーで使用されるユーザー定義のビジネス・ルールは特定のイベント・タイプを呼び出すため、イベント処理にはイベント・タイプが必要です。イベント・タイプが存在しないと、イベント・プロセッサーはイベントを処理できません。

イベント・タイプの作成

イベント処理のための新規イベント・シナリオを追加するときに、新規イベント・タイプを作成して、そのイベント・シナリオに組み込まれたトランザクションやアクティビティーのタイプはもちろん、このイベント・カテゴリーに関連付ける計測単位の定義を行うことが必要になる場合があります。

始める前に

IBM InfoSphere Identity Insight システムで Event Manager が有効になっている必要があります。

このタスクについて

イベント・タイプは複合イベント処理プログラムによって呼び出されますが、この複合イベント処理プログラムは、ユーザー定義のビジネス・ルールに従ってイベントを処理します。イベント・タイプを使用するためには、その前に、そのイベント・タイプを使用するビジネス・ルールを少なくとも 1 つ作成する必要もあります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「イベント・タイプ **(Event Type)**」ボタンをクリックします。
4. 「新規 **(New)**」ボタンをクリックします。
5. 必須: 「一般 **(General)**」タブで、イベント・タイプの名前と説明、このイベント・タイプに関連付ける計測単位、およびこのイベント・タイプの状況 (アクティブまたは非アクティブ) を指定します。
6. オプション: カテゴリー、サブカテゴリー、このイベント・タイプに関する注記など、追加情報を指定することもできます。
7. 「保存 **(Save)**」ボタンをクリックします。

イベント・タイプの編集

イベント・タイプに関連付けられた説明、計測単位、または追加情報を変更する必要がある場合は、イベント・タイプを編集します。また、イベント・タイプが使用されないようにするため、イベント・タイプを編集して非アクティブにすることもできます。イベント・タイプ名は編集できません。

このタスクについて

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「イベント・タイプ **(Event Type)**」ボタンをクリックします。
4. 編集するイベント・タイプを選択します。
5. 「一般 **(General)**」タブで変更を加えます。
6. 「保存 **(Save)**」ボタンをクリックします。

次のタスク

イベント・タイプの削除

イベント処理で使用されなくなったイベント・タイプは、削除してかまいません。イベント・タイプそのものは保持し、単に非アクティブにするだけであれば、削除する代わりに、イベント・タイプの状況を編集できます。

始める前に

このタスクについて

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「ソース **(Sources)**」ボタンをクリックします。
3. 「イベント・タイプ **(Event Type)**」ボタンをクリックします。
4. 削除するイベント・タイプの横にあるチェック・ボックスを選択します。
5. 「削除 **(Delete)**」ボタンをクリックします。

次のタスク

ヘルプ・トピック

「イベント・タイプ **(Event Types)**」 **-** 「一般 **(General)**」タブ**:**

このタブを使用してイベント・タイプを定義、編集します。イベント・タイプによってイベントを定義したりカテゴリー化したりします。イベント・タイプは、システムで Event Manager が有効になっている場合に、イベント処理時に使用されます。

タイプ
: イベント・タイプのユニーク名を入力します。例えば、**電信送金** という名前のイベント・タイプを作成できます。

説明
: イベント・タイプの説明を入力します。

「計測単位 **(Unit of Measure)**」
: イベント・タイプに関連付けられる値の計測単位の略語を入力します。例えば、米ドルの場合は USD と入力します。

状況
: ドロップダウン・リストから、イベント・タイプの状況として「アクティブ **(Active)**」または「非アクティブ **(Inactive)**」のいずれかを入力します。

(「非アクティブ **(Inactive)**」状況を使用することで、このイベント・タイプをイベント処理から除外しつつも、このイベント・タイプの構成を保持することができます。)

「カテゴリー **(Category)**」
イベント・タイプのオプションのカテゴリー名を入力します。

「サブカテゴリー **(Sub-Category)**」
イベント・タイプのオプションのサブカテゴリー名を入力します。

「メモの見出し **1 (Memo Heading 1)**」
イベント・タイプのオプションのメモ 1 の見出しを入力します。

「メモの見出し **2 (Memo Heading 2)**」
イベント・タイプのオプションのメモ 2 の見出しを入力します。

エンティティー解決の構成

エンティティー解決とは、データ内の関係を見つける処理です。エンティティー解決の構成設定は、解決構成と呼ばれるグループ分けによって編成されます。解決構成は、解決ルール、確定と否定、属性、Name Manager のマッチング構成、候補ビルダーという 5 つのコンポーネントから成ります。

エンティティー解決

エンティティー解決とは、エンティティーを解決して関係を検出する処理です。認識、解決、関連付けという 3 つのフェーズの中で、パイプラインが入力アイデンティティー・レコードを処理しながら、エンティティー解決を実行します。

解決構成の構成

エンティティー解決の設定はすべて、解決構成内に維持されます。2 つの解決構成がデフォルトで用意されています。

解決構成

エンティティー解決の設定は、構成コンソールの「システム構成 **(System Configuration)**」タブの「システム・ロード解決ルール (System Load Resolution Rule)」値を使用して定義した解決構成のグループ別に編成されます。

関係解決のデフォルトのインストール済み環境には、次の 2 つの解決構成が組み込まれています。

- 「デフォルト **(DEFAULT)**」 - 定義済みデータ・ソースから新規データがシステムに入ったときに常に使用されるデフォルトの解決設定。
- 「検索 **(SEARCH)**」 - 完全に解決される検索要求をユーザーが送信した場合に常に、解決される検索処理によって使用される解決設定。

独自の解決設定のセットを作成し、新規作成した解決構成を使用してそれらの設定を識別することができます。この処理を行う場合は、必ず「デフォルト **(DEFAULT)**」解決構成の複製を作成し、その複製を開始点として使用することで、新規解決構成を作成してください。

特定のデータ・ソースにさまざまな解決構成を割り当てることができます。複数のデータ・ソース間で複数の解決構成を適用することにした場合、エンティティー解決は、アラート生成時に常に、入力アイデンティティーに割り当てられた解決構成を使用することを考慮してください。このことは、比較対象のアイデンティティーのどれが入力アイデンティティーなのかによって、またどのアイデンティティーがエンティティー・データベース内に既に存在するのかによって、異なるアラート結果を招くことがあります。例えば、Customer データ・ソースのアイデンティティー #123 に割り当てられている DEFAULT 解決構成には、名前と住所用の解決ルール (名前しきい値は 80、住所しきい値は 5 に設定されている) が含まれているとします。Vendor データ・ソースのアイデンティティー #456 が使用する NEW 解決構成にも同じ解決ルールが含まれているとします (ただし、名前しきい値は 95、住所しきい値は 7 に設定されている)。Customer 123 が入力アイデンティティーで、既存の Vendor 456 と比較した場合、両者間の名前スコアが 85、住所スコアが 5 と算出され、アラートが生成されることになります。処理の順序が逆の場合、つまり Customer 123 が既にシステム内にあり、Vendor 456 がシステムに入ってきた場合であっても、やはり生成されるのは同じ解決スコア (名前スコア 85、住所スコア 5) です。ただし、この場合アラートは生成されません。それは、解決スコアが NEW 解決構成の解決しきい値 (名前スコアが 95、住所スコアが 7 に設定されている) に満たないためです。

注**:**

デフォルトのエンティティー解決構成以外の解決構成を使用する場合は、計画立案の上、注意して行ってください。解決ルールやスコアリング設定などのデフォルトのエンティティー解決設定は、何百人もの人間が現実の世界のデータに基づき何年にもわたって分析および研究を重ねた結果です。通常、これらのデフォルトを変更する必要があるのは、データやビジネス・ルールの要件により、特定の、標準的ではないシステム動作が必要になる場合のみです。

解決構成の表示

解決構成は、エンティティー解決設定の集合を指定するために使用します。エンティティー解決設定に変更を加えることを計画している場合や、エンティティー解決設定の新規セットを作成しようとする場合に、既存の解決構成の確認が必要になることがあります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。

デフォルトの解決構成の複製およびカスタマイズ

新規のエンティティー解決構成を作成する場合の理想的な方法は、デフォルトの解決構成の複製 (コピー) を作成し、その複製を開始点として使用することで、新規解決構成を作成することです。未変更状態のデフォルト構成を保持することで、必要なときには常に、製品を再インストールすることなく、デフォルト構成に戻すことができます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。
3. 「解決構成 **(Resolution Configs)**」タブで、DEFAULT 解決構成の横にあるチェック・ボックスを選択します。
4. 「複製 **(Clone)**」ボタンをクリックします。
5. 「一般 **(General)**」タブの「コード **(Code)**」フィールドに、解決構成の新規名を入力します。
6. 「説明 **(Description)**」フィールドに、複製した解決構成の新しい説明を入力します。
7. 「保存 **(Save)**」ボタンをクリックします。

次のタスク

エンティティー解決設定に変更を加えるとき、例えば解決ルールや、確定と否定、候補ビルダーなどを構成するときには、この新しい解決構成を選択できます。

カスタマイズした解決構成の削除

使用しなくなったカスタマイズ済みの解決構成は削除できます。 DEFAULT 解決構成は削除しないでください。未変更状態のデフォルト構成を保持することで、必要なときには常に、製品を再インストールすることなく、デフォルト構成に戻すことができます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。
3. 「解決構成 **(Resolution Configs)**」タブで、削除する解決構成の横にあるチェック・ボックスを選択します。
4. 「削除 **(Delete)**」ボタンをクリックします。
5. 確認ウィンドウで「**OK**」をクリックして、その解決構成を削除します。

次のタスク

エンティティー解決設定に変更を加える際、この解決構成を選択できなくなりました。また、この解決構成に関連したエンティティー解決設定をエンティティー解決処理に適用できなくなりました。

ヘルプ・トピック

「解決構成 **(Resolution Configs)**」ウィンドウ**:**

使用可能なエンティティー解決構成のリストを表示するには、このウィンドウを使用します。エンティティー解決設定は、解決構成と呼ばれるグループに編成されています。個々のデータ・ソースにさまざまな解決構成を割り当てることができます。各データ・ソースに一度に適用できる解決構成は 1 つだけです。

コード
: 解決構成の名前。

説明　解決構成の説明。

解決ルールの構成

比較対象のエンティティーをどのように解決し、関連付けるかを定義するためには、候補しきい値や、確定/否定しきい値など、解決ルールを構成する必要があります。

このタスクについて

解決ルールは、コンソールを使用して「解決ルール **(Resolution Rules)**」タブで表示および変更できます。

解決ルール

解決ルールとは、比較対象のエンティティー (同じエンティティーでも同じエンティティーでなくても) をどのように解決して、どのように関連付けるか (それらのエンティティーが同じエンティティーに解決されない場合、属性をいくつ共有するか) を定義するためにシステムが使用する基準のセットです。

解決ルールを定義するときは、次のように、合計解決スコアを導くしきい値を指定する必要があります。合計解決スコアによって、入力アイデンティティーが既存のエンティティーに解決されるかどうかが決まります。

- 候補しきい値により、アイデンティティーやエンティティーが 1 つの複合エンティティーに解決されるかどうかを判別するための、比較対象とする属性データ値を指定します。このしきい値は、解決ルールを満たすために入力アイデンティティーと既存のエンティティーの間で特定の属性値が一致する必要がある最小スコアです。
- 確定/否定しきい値には、否定の使用を有効にした場合に、一致する属性や競合する属性のデータ値に対してどの程度のスコアリングの重みづけ (正または負) を与えるかを指定します。

また、同じ属性の競合する値が、どのように解決スコアに影響するかを指定することもできます。これらの競合する値は否定と呼ばれます。属性値に何らかの競合 (否定) がある場合はルールを満たしていない、ということを指定する解決ルールを構成できます。また、指定したしきい値スコアを 1 つ以上満たしていない比較スコアに基づいて、自動否定が作成されるように、解決ルールのしきい値を調整することもできます。設定したしきい値スコアが高くなるほど、解決ルールを満たすためにはより正確に一致していなければならないことになります。

候補しきい値

候補しきい値は、実際に入力アイデンティティーが既存のエンティティーを表しているのか、まったく新規のエンティティーを表しているのかを判別するために使用される、解決ルールの最初の部分です。

候補しきい値は、コンソールを使用して構成され、解決ルールの不可欠な部分です。例えば、解決ルールにユニーク番号の候補しきい値が含まれている場合、その解決ルールでは、一致するユニーク番号が要求されるものと説明できます。

候補しきい値は、エンティティー解決処理の一部として既存のエンティティーを候補リストに配置するために、既存のエンティティーにのみ適用されます。実際のし

きい値は、既存のエンティティーを候補リストに追加するエンティティー解決処理のために、入力アイデンティティーと既存エンティティーとの間で特定のデータ・タイプが一致しなければならない最小レベルです。

住所精度**:**

住所精度とは、比較対象の 2 つの住所が同じ住所を表しているかどうかを判別するために、エンティティー解決によって使用されるスコアリング処理です。

住所精度は 9 つの異なるレベル (1 から 9) に分割されています。ほとんどの住所には、街区 (番地を含む)、市、州、郵便番号、郵便番号下 4 桁のような、比較可能な基本要素が含まれています。これらの構成要素を比較する際に、住所精度は一致する街区要素を開始点とし、精度レベル 5 を割り当てます。次に、それ以外の構成要素が一致しているか異なっているかに基づいて、精度レベルが上位方向または下位方向に調整されます。構成要素が一致するごとに精度レベルが 1 ずつ増加し、構成要素が異なるごとに精度レベルが 1 ずつ減少します。ある構成要素の値が一方の住所には存在するが、他方の住所の同じ構成要素には値が存在しない場合、精度調整は発生しません。

エンティティー解決において、デフォルトでは、比較された住所のうち住所精度レベルが 5 以上の住所がすべて、住所一致の候補と見なされます。

表 *29.* 住所精度レベル

レベル	説明
1	街区とすべての部分が一致しているが、郵便番号下 4 桁が異なる。これは、すべての部分が一致するが郵便番号下 4 桁が異なる住所が存在するに違いないことを意味します。例えば、123 N Water St. Las Vegas, NV 89123-1234 と 123 S Water St. Las Vegas, NV 89123-5433 です。
2	街区が一致しているが、すべての部分が異なる。これは、街区のみが一致し、市、州、郵便番号、国がすべて異なるか、または欠落していることを意味します。例えば、123 Main St. Orlando, FL 32555 と 123 Main St. Las Vegas, NV です。
3	街区が一致し、誤差因子が -2。これは、街区が一致するが、計算は -2 になることを意味します。例えば、123 Main St. Las Vegas, NV 89111 と 123 Main St. Las Cruces, NM です。
4	街区が一致し、誤差因子が -1。これは、街区が一致するが、計算は -1 になることを意味します。例えば、123 Main St. Las Vegas, NV 89111 と 123 Main St. Las Vegas, NM 54633 です。
5	街区が一致し、誤差因子が 0 (基準)。これは、街区が一致するが、計算は 0 になることを意味します。例えば、123 Main St. Las Vegas, NV 89111 と 123 Main St です。
6	街区が一致し、一致因子が +1。これは、街区が一致するが、計算は +1 になることを意味します。例えば、123 Main St. Las Vegas, NV 89111 と 123 Main St. Las Vegas です。
7	街区が一致し、一致因子が +2。これは、街区が一致するが、計算は +2 になることを意味します。例えば、123 Main St. Las Vegas, NV 89111 と 123 Main St. Las Vegas, NV です。

表 29. 住所精度レベル (続き)

8	街区およびすべての部分が一致しているが、郵便番号下 4 桁が欠落している。これは、郵便番号下 4 桁が存在しないことを除いて、住所のすべての部分が一致していることを意味します。例えば、123 Main St. Las Vegas, NV 89111 と 123 Main St. Las Vegas, NV 89111 です。
9	完全一致 (街区およびすべての部分)。これが選択された場合、郵便番号下 4 桁を含め、住所のすべての部分が一致していることを意味します。例えば、123 Main St. Las Vegas, NV 89111-1234 と 123 Main St. Las Vegas, NV 89111-1234 です。 **注:** これは、郵便番号下 4 桁が使用されない国際郵便コードでは機能しません。

精度レベル **1**

1 から 9 までの各精度レベルは、精度レベルの増加を表していますが、レベル 1 は例外です。レベル 1 は、住所情報が北と南あるいは西と東の街区の指定を除いて同じである可能性がある、特殊なケースを表しています。例えば、456 North Main Street Sometown, Nevada と 456 South Main Street Sometown, Nevada などです。このケースでは、住所は同じである可能性がありますが、郵便番号下 4 桁が明確に異なっています。一見、これらの住所は、解決が必要であるように見える可能性があります。しかし、実際には異なる住所であるため、相互に解決されるべきではありません。この、一見したところ絶対に住所解決が必要なケースは、実際には、絶対に相互に住所解決すべきでないケースです。そのため、住所が解決されるのを防止するために、このシナリオの精度レベルに割り当てられる値は、レベル階層の最下位 (レベル 1) となります。

また、レベル 1 は、意図的な誤住所を示唆している可能性もあります。意図的な誤住所パターンに興味を持つ顧客、つまり、欺くために故意に住所を改ざんする人々もいます。そのような理由から、レベル 1 のような低い住所精度レベルを考慮できるように、解決ルールの順序を構成することができます。

注**:** エンティティーを解決する上でレベル 1 に関心がある場合、例えば、誰かが郵便番号下 4 桁に矛盾する住所情報を指定していないか調べる必要がある場合は、別の解決ルールを作成する必要があります。このようなルールは、5 以上のすべての精度レベルを考慮するデフォルトの解決ルールの前に配置する必要があります。新規解決ルールを適切に作成するためには複雑さが伴うため、十分な専門知識を得てから、あるいは IBM の支援を得て、作成するようにしてください。

住所精度の詳細な例*:*

以下の例は、比較対象のデータと、比較結果として得られる住所精度スコアを表しています。

1 番目の住所は、エンティティー・データベース内の既存の住所を表しています。2 番目の住所は入力住所です。

精度レベル **1 -** 街区とすべての部分が一致しているが、郵便番号下 **4** 桁が異なる。

この例では、類似した街区にあるが、明確に異なる住所である、2 つの住所を示しています。一方は街区の北端にあり、もう一方は南端にあります。これら 2 つの住所の唯一の違いは、郵便番号下 4 桁です。

街区	市	州	郵便番号
123 N Main St	Fairmount	IN	46928-1655
123 S Main St	Fairmount	IN	46928-1924

注**:** 精度レベル 1 は、北と南あるいは西と東の街区指定の差こそあれ、住所情報は同じである可能性がある、特殊なケースを表しています。一見、これらの住所は、解決が必要であるように見える可能性があります。しかし、実際は異なる住所であるため、相互に解決されるべきではありません。この、一見したところ絶対に住所解決が必要なケースは、実際には、絶対に相互に住所解決すべきでないケースでもあるため、住所が解決されるのを防止するため、このシナリオの値は、レベル階層の最下位 (1) となっています。

精度レベル **2 -** 街区が一致しているが、すべての部分が異なる

この例では、街区情報は類似しているが、市、州、および郵便番号の情報が異なる 2 つの住所を示しています。ネバダの郵便番号はすべて 89 で始まるため、この 2 番目の住所は (おそらくは意図的な) 明らかな間違いです。

街区	市	州	郵便番号
123 E Main St	Fairmount	IN	46928
123 S Main St	Las Vegas	NV	46999

精度レベル **3 -** 街区が一致しているが **-2** の誤差因子を伴う。

この例では、街区情報のみが一致しています。入力住所に州情報が提供されておらず、市情報と郵便番号情報は競合しています。

街区	市	州	郵便番号
123 E Main St	Delphi	IN	46923-1522
123 E Main St	Fairmount		46928

精度レベル **4 -** 街区が一致しているが **-1** の誤差因子を伴う。

この例では、街区情報と州情報は同じであるが、市情報と郵便番号情報が競合している 2 つの住所を示しています。

街区	市	州	郵便番号
123 E Main St	Delphi	IN	46923-1522
123 E Main St	Fairmount	IN	46928-1924

精度レベル **5 -** 街区が一致し、誤差因子が **0 (**基準**)**。

この例では、入力住所に街区情報だけが提供されています。市、州、および郵便番号が含まれていないにもかかわらず、この一致には住所精度スコアの基準である (5) が与えられています。精度スコアには、欠落部分が反映されます (競合部分がある場合は欠落部分がスコアリングされないため、これとは混同しないでください)。

街区	市	州	郵便番号
220 JEFFERSON	BUFFALO	IA	
220 Jefferson St.			

精度レベル **6 -** 街区が一致し、一致因子が **+1**。

この例では、州情報も郵便番号情報もないが、同じ街区情報および市情報である入力街区住所を示しています。この入力住所は、正しい住所であるが、データが欠落している可能性があります。

街区	市	州	郵便番号
220 Washington	Syracuse	NY	
220 Washington Sq.	Syracuse		

精度レベル **7 -** 街区が一致し、一致因子が **+2**。

この例では、街区、市、および簡易郵便番号が一致しているが、州情報が提供されていない入力住所を示しています。

街区	市	州	郵便番号
220 JEFFERSON	BUFFALO	IA	52728
220 Jefferson St.	Buffalo		52728

精度レベル **8 -** 街区およびすべての部分が一致しているが、郵便番号下 **4** 桁が欠落している。

この 2 つの住所は同じですが、郵便番号下 4 桁を受け取らなかったため、住所クレンジングがこれらの住所を検証できませんでした。

街区	市	州	郵便番号
220 JEFFERSON	BUFFALO	IA	52728
220 Jefferson St.	Buffalo	IA	52728

精度レベル **9 -** 完全一致 **(**街区およびすべての部分**)**。これが選択された場合、郵便番号下 **4** 桁を含め、住所のすべての部分が一致していることを意味します。

この例では、2 つの住所が同じ街区住所、市、州、および郵便番号下 4 桁を共有しています。結果として、比較されたこれらの住所は最高の住所精度スコアを受け取ります。

注**:** これは、郵便番号下 4 桁が使用されない国際郵便コードでは機能しません。

街区	市	州	郵便番号
123 W Main St	Camden	IN	46917-9997
123 W Main	Camden	IN	46917-9997

名前精度**:**

名前精度とは、比較対象の 2 つの名前が同じ名前を表しているかどうかを判別するため、エンティティー解決によって使用されるスコアリング処理です。

名前精度スコアリングは、2 種類あるアルゴリズムの内、どちらかの使用に基づいています。

- Name Comparator 1.0
- Name Comparator 2.0

各アルゴリズムには、解決ルールを構成する際に構成の一部として使用できる、名前マッチング基準の独自のセットがあります。

これらのアルゴリズムのどちらも Name Manager 機能で動作します。 Name Manager は、国/地域にユニークな考慮事項に基づいた追加のマッチング能力を組み込むために名前マッチングを拡張する、個別に構成することが可能な機能です。

比較の考慮事項

Name Comparator 1.0 は、バージョン 3.9.0 以前からアップグレード・インストールした場合のデフォルト設定です。Name Comparator 2.0 は、バージョン 3.9.1 以降からアップグレード・インストールした場合と、新規インストールの場合の、デフォルト設定です。

どちらのアルゴリズムが自分のニーズに最適であるかを考慮する際には、それぞれのアルゴリズムが提供する利点を考慮してください。

Name Comparator 1.0:

- 必要な CPU 使用率が少ないため、パフォーマンスが高速化する
- 名前が一致した理由をより正確に理解できる

Name Comparator 2.0:

- 3 語を超える語から成る名前の処理がより優れている
- 語の順序が異なる場合のマッチングがより優れている
- ファジー・マッチングがより優れている
- 組織名のマッチングがより優れている
- イニシャルの処理がより優れている

Name Comparator 1.0:

この名前マッチング・アルゴリズムは、主に 2、3 語から成る名前で機能するように設計されています。これは、バージョン 3.9.0 以前からアップグレードした場合のデフォルトの名前マッチング設定です。

Name Comparator 1.0 は、2 つの名前を比較した後、異なる 15 の類似レベルに従って、それらの名前の相似性をランク付けします。

表 *30. Name Comparator 1.0* - 精度レベル

レベル	説明
1	ファーストネームまたはラストネームのみが部分一致 例: John Jacob Smith = Joe Smithson
2	ファーストネームまたはラストネームのみが完全一致 例: John Jacob Smith = Jonathan Henry Smith
3	ハッシュ法による近似一致 例: Joe Smith = Joe Snith
4	ラストネームのみが異なり、順序が異なる 例: Bob Jacob Smith = Jacob Bob Jones
5	ラストネームのみが異なる 例: Bob Jacob Smith = Bob Jacob Jones
6	標準化された名前の一致だが、多少の差異がある 例: John Jacob Smith = Jonathan Henry Smith
7	標準化された名前の一致 例: Joe W Anderson = Joseph Andersen
8	標準化された名前の一致で、ラストネームとミドルネームのイニシャルが正確に一致するが、順序が異なる : J Bob Smith = Robert J Smith
9	標準化された名前の一致で、ラストネームおよびミドルネームのイニシャルが正確に一致する 例: Joe W Anderson = Joseph W Anderson
10	標準化された名前の一致で、ラストネームが正確に一致するが、順序が異なる 例: Bob Smith = Robert Smith
11	標準化された名前の一致で、ラストネームが正確に一致する 例: John Jacob Smith = Johnny Jake Smith
12	未加工の名前の一致で、ミドルネームのイニシャルが一致するが、順序が異なる 例: Joe W. Brown = Will Joe Brown
13	未加工の名前の一致で、ミドルネームのイニシャルが一致する 例: Joe W Anderson = Joe W Anderson
14	未加工の名前の一致だが、順序が異なる 例: John Bob Smith = Bob John Smith

表 30. *Name Comparator 1.0* - 精度レベル (続き)

15	未加工の名前の一致 例: Joe William Anderson = Joe William Anderson

Name Comparator 2.0:

この名前マッチング・アルゴリズムは、比較対象の名前をトークン化 (名前文字列の語の集まりを個々の名前つまりトークンに分割) するように設計されています。その後、このアルゴリズムはトークンを比較し、各トークンのスコアを作成します。これは、バージョン 3.9.1 以降からアップグレード・インストールした場合と、新規インストールの場合の、デフォルトの名前マッチング設定です。

Name Comparator 2.0 は、名前を以下の 3 つのカテゴリーにグループ化した後、それらのカテゴリー内で比較して、カテゴリーをスコアリングします。

- 名 (ファーストネームおよびミドルネーム – またはラストネーム以外のすべての語)
- 姓 (ラストネーム)
- フルネーム (すべての語)

これらの 3 つのスコアリング・カテゴリーにより、名前マッチングの要件に合わせて、特定の解決ルール用の名前マッチングを調整することができます。スコアは、0 から 100 までの整数ベースで、0 が最低スコア、100 が最高スコアです。あるカテゴリーのスコアが高くなるほど、そのカテゴリーの名前はより正確に一致しています。

構成に関する考慮事項**:** スコアリング・ガイドライン

Name Comparator 2.0 の名前マッチング設定を編集または変更する場合は常に、以下のスコアリング・ガイドラインを使用して、解決ルールの名前しきい値をセットアップするのに役立ててください。また、これらのガイドラインは、このアルゴリズムが持つスコアリング・カテゴリーのスコアリング結果を解釈する際にも役立ちます。

「フルネーム・スコア **(Full Name Score)**」

0 から 100 までのスコアに基づいて、フルネーム・スコアのマッチング・レベルを判別するのに役立つガイドラインを以下に示します。

- 100 = 完全一致
- 90 = 非常に良好な一致 (名前と DOB の解決に適している)
- 80 = 良好な一致 (ほとんどの解決ルールに適している)
- 70 = 平均的な一致 (ユニーク番号も存在する場合に適している)
- 70 未満 = マッチングに適さない

「名スコア **(Given Name Score)**」

0 から 100 までのスコアに基づいて、名スコアのマッチング・レベルを判別するのに役立つガイドラインを以下に示します。

- 100 = 完全一致

- 90 = 非常に良好な一致 (名と姓が逆であることを示唆している可能性がある)
- 85 = 許容される最低一致
- 85 未満 = マッチングに適さない。姓またはフルネームと結合して、何らかの類似性を保証する場合に役立つことがある

「姓スコア **(Surname Score)**」

0 から 100 までのスコアに基づき、姓スコアのマッチング・レベルを判別するのに役立つガイドラインを以下に示します。

- 100 = 完全一致
- 90 = 非常に良好な一致 (名と姓が逆であることを示唆している可能性がある)
- 85 = 許容される最低一致
- 85 未満 = マッチングに適さない。名またはフルネームと結合して、何らかの類似性を保証する場合に役立つことがある

Name Manager による名前スコアリング**:**

Name Manager アルゴリズムは、名前を各部分にグループ化した後、名前の各部分の国/地域別情報を判別し、それに基づいて入力名前データのスコアを算出します。次に、このアルゴリズムは名前の各部分のスコアを算出し、結果として得られたスコアがエンティティー解決中に使用されます。

Name Manager アルゴリズムは Name Comparator アルゴリズム (NC1 および NC2) とは別個のものですが、それでもやはり NC1 または NC2 のいずれかを選択する必要があります。エンティティー解決処理の実行中に、まず、選択された Name Comparator アルゴリズムに基づいて名前のスコアが算出されます。名前のスコアが完全一致である場合、完全名前一致は解決ルールの名前スコア部分を満たしているため、エンティティー解決は Name Manager によるスコアリングをスキップします。一方、入力された名前のスコアが完全一致に満たない場合、エンティティー解決処理は Name Manager アルゴリズムを使用して名前のスコアを算出します。

まず、アルゴリズムが名前を解析して名前の各部分 (名、姓、およびフルネーム) に分割した後、アルゴリズムが名前の各部分の国/地域別情報を判別します。最後に、アルゴリズムが名前の各部分にスコアを割り当て、構成済みの Name Manager スコアしきい値に対してスコアを比較し、それらの名前がどの程度正確に一致しているかを判別します。スコアしきい値の設定が高くなるほど、入力名前データの名前の各部分が、エンティティー・データベース内の既存エンティティーの名前の各部分とより正確に一致している必要があります。

生年月日精度**:**

生年月日精度は、エンティティー解決で使用される、比較対象の 2 つの生年月日が同じ日を表しているかどうかを判別するためのスコアリング処理です。

この比較では、生年月日の文字列について、整数の位置、文字の入れ替わり、日数差、月数差、年数差など、さまざまな類似指標が考慮されます。これらの指標が分析され、2 から 100 の範囲で相似スコアが決定されます。次の 4 つの類似カテゴリーに基づいて、生年月日精度の設定を構成できます。

- 「完全一致 (Exact)」: 100 ポイント一致
- 「緊密 (Tight)」: 90 ポイント以上一致
- 「中間 (Medium)」: 85 ポイント以上一致
- 「緩い (Loose)」: 80 ポイント以上一致

構成に関する考慮事項

システムには、解決ルールが比較対象の 2 つの生年月日を同一であると判定するための最小相似レベルとして、「緊密」という事前構成設定が用意されています。この設定を変更すると、一致数に影響するとともに、システムが実行するエンティティー解決の数に影響が及ぶ可能性があります。この設定の変更は慎重に検討してください。変更した場合は、必ずテストしてから実稼働環境に実装してください。

生年月日精度の詳細例*:*
以下の例は、比較対象のデータと、比較結果として得られる生年月日精度スコアを表しています。1 番目の生年月日は、エンティティー・データベース内のエンティティーの既存の生年月日を表しています。2 番目の生年月日は、入力生年月日アイデンティティーのものです。

精度レベル**:** 完全一致 **(100** ポイント**)**

この例は、正確に一致する 2 つの日付を示しています。アルゴリズムは、100 ポイント一致を生成します。

生年月日	状況
1963/12/01	既存
1963/12/01	入力

精度レベル**:** 緊密 **(90** ポイント**)**

この例は、精度スコアが 90 ポイント以上の 2 つの日付を示しています。この例に示す 2 つの生年月日値は、年と日にちの値は同じですが、月の値が 1 カ月異なります。

生年月日	状況
1963/12/01	既存
1963/11/01	入力

精度レベル**:** 中間 **(85** ポイント**)**

この例は、精度スコアが 85 ポイント以上の 2 つの日付を示しています。この例に示す 2 つの生年月日値は、月と日にちの値は同じですが、年の値の最後の 2 桁が逆です。

生年月日	状況
1963/12/01	既存
1936/12/01	入力

精度レベル**:** 緩い **(80** ポイント**)**

この例は、精度スコアが 80 ポイント以上の 2 つの日付を示しています。この例に示す 2 つの生年月日値は、月と日にちの値は同じですが、年の値の 3 桁目が間違っています (それでも生年月日としては適切な値です)。

生年月日	状況
1963/12/01	既存
1933/12/01	入力

解決ルールの表示

解決ルールを追加したり削除したりする前に、解決ルールの現在のセットを表示できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。
3. 「解決ルール **(Resolution Rules)**」タブをクリックします。
4. 「解決構成 **(Resolution Config)**」ドロップダウン・リストから、解決構成を選択します。
5. 特定の解決ルールの詳細を表示するには、表示する解決ルールが含まれている行内のリンクをクリックします。

解決ルールの作成

ビジネス要件を慎重に検討し、既存の解決ルールをよく確認した結果、データ用の新規解決ルールを作成する必要があると決定した場合は、この手順に従ってください。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。
3. 「解決ルール **(Resolution Rules)**」タブをクリックします。
4. 「解決構成 **(Resolution Config)**」ドロップダウン・リストから、解決構成を選択します。
5. 「新規 **(New)**」ボタンをクリックします。
6. 「一般 **(General)**」タブで、2 つのエンティティーのデータの比較時に使用する値を指定します。
7. 「候補しきい値 **(Candidate Thresholds)**」タブをクリックします。
8. 「候補しきい値 **(Candidate Thresholds)**」タブで、データのしきい値を指定します。
9. 「確定**/**否定しきい値 **(Confirm/Deny Thresholds)**」タブをクリックします。
10. 「確定**/**否定しきい値 **(Confirm/Deny Thresholds)**」タブで、データのしきい値を指定します。
11. 「保存 **(Save)**」ボタンをクリックします。

解決ルールの削除

エンティティー解決処理における考慮事項から解決ルールを削除するには、そのルールを削除します。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。
3. 「解決ルール **(Resolution Rules)**」タブをクリックします。
4. 「解決構成 **(Resolution Config)**」ドロップダウン・リストから、解決構成を選択します。
5. 削除する解決ルールの横にあるチェック・ボックスを選択します。
6. 「削除 **(Delete)**」ボタンをクリックします。
7. 確認ウィンドウで「**OK**」をクリックして、その解決構成を削除します。

ヘルプ・トピック

「解決ルール **(Resolution Rules)**」ウィンドウ**:**

解決構成に含まれている解決ルールを表示するには、この画面を使用します。解決ルールはリストされた順序で処理されます。解決ルールが満たされて、割り当てられた解決スコアが適用された後、解決をトリガーするようにルールが構成されている場合は、入力アイデンティティーが既存エンティティーに解決されます。その他のエンティティー解決ルールは、その特定の比較において考慮されません。

「順序 **(Order)**」
: 比較対象の入力アイデンティティーおよび既存エンティティーに解決ルールが適用される順序

説明
: 解決ルールの説明

「解決の信頼度 **(Resolution Confidence)**」
: ルールが満たされた場合に比較に適用される解決スコア

「関係の信頼度 **(Relation Confidence)**」
: ルールが満たされた場合に比較に適用される関係スコア

「解決をトリガーする **(Triggers resolve)**」
: ルールが満たされた場合に、ルールが自動的に入力アイデンティティーを既存エンティティーに解決するかどうか

「解決ルール **(Resolution Rules)**」 **-** 「一般 **(General)**」タブ**:**

新しい解決ルールを構成する場合や、既存の解決ルールの詳細を表示する場合に、このタブを使用します。

「順序 **(Order)**」
: ルールの処理順を指定するユニーク番号を入力します。

説明
: ルールの説明を入力します。

「解決の信頼度 **(Resolution Confidence)**」
: このルールが成功した場合の相似の信頼度をパーセンテージで入力します。100% のみが解決と見なされます。

「関係の信頼度 **(Relation Confidence)**」
このルールが成功した場合の関係の信頼度をパーセンテージで入力します。100% のみが解決と見なされます。

「解決をトリガーする **(Triggers Resolve)**」
解決および関係の信頼度が 100% である場合に入力アイデンティティーと既存エンティティーを解決するには、「はい (Yes)」を選択します。

「否定を有効化 **(Denials Enabled)**」
確定/否定の処理を有効にするには、「はい (Yes)」を選択します。それ以外の場合、否定の処理は行われません。

「特性の否定を有効化 **(Characteristic Denials Enabled)**」
特性の確定/否定の処理を有効にするには、「はい (Yes)」を選択します。それ以外の場合、特性の否定の処理は行われません。

「解決ルール **(Resolution Rules)**」 **-** 「候補しきい値 **(Candidate Thresholds)**」タブ**:**

新規解決ルールの候補しきい値の設定を指定する場合や、既存の解決ルールの候補しきい値の詳細を表示する場合に、このタブを使用します。これらの設定により、解決の「一般 **(General)**」タブに入力される、解決ルールの「説明 **(description)**」が定義されます。

「住所精度しきい値 **(Address Precision Threshold)**」
ルールが満たされたと見なされるのに必要な、最低住所ランキングを選択します。

「近似住所しきい値 **(Approximate Address Threshold)**」
ルールが満たされたと見なされるのに必要な、近似一致した住所値の最小数を選択します。

「隣接性しきい値 **(Proximity Threshold)**」
ルールが満たされたと見なされるのに必要な、品質ルールで定義された領域内にある住所の最小数を選択します。

「ユニーク番号しきい値 **(Unique Number Threshold)**」
ルールが満たされたと見なされるのに必要な、一致したユニーク番号の最小数を選択します。

「非ユニーク番号しきい値 **(Non-Unique Number Threshold)**」
ルールが満たされたと見なされるのに必要な、一致した非ユニーク番号の最小数を選択します。

「特性しきい値 **(Characteristic Threshold)**」
ルールが満たされたと見なされるのに必要な、一致した特性の最小数を選択します。

「**E** メールしきい値 **(Email Threshold)**」
ルールが満たされたと見なされるのに必要な、一致した E メールの最小数を選択します。

「要約データしきい値 **(Summary Data Threshold)**」
ルールが満たされたと見なされるのに必要な、一致した「ユニーク番号

(Unique Number)」、「その他の番号 (Other Number)」、「住所 (Address)」、「特性 (Characteristic)」、および「E メール (Email)」の最小合計数を選択します。

「要約しきい値 **(Summary Threshold)**」
ルールが満たされたと見なされるのに必要な、一致した「住所隣接性 (Address Proximity)」、「近似住所 (Approximate Address)」、「近似番号 (Close Number)」、および「DOB」の最小合計数を選択します。

「解決ルール **(Resolution Rules)**」 **-** 「確定/否定しきい値 **(Confirm/Deny Thresholds)**」タブ**:**

新規解決ルールの確定および否定のしきい値の設定を指定する場合や、既存の解決ルールの確定および否定のしきい値の詳細を表示する場合に、このタブを使用します。

「近似番号しきい値 **(Close Number Threshold)**」
ルールが満たされたと見なされるのに必要な、一致した近似番号の最小数を選択します。

「生年月日しきい値 **(Date of Birth Threshold)**」
ルールが満たされたと見なされるのに必要な、生年月日の最小一致スコアを選択します。

「**Name Comparator** 設定 **(Name Comparator settings)**」
これらの設定により、エンティティー解決の名前精度要件が決まります。これらの設定は、単体の設定としても、あるいは Name Manager 設定との連動によっても機能します。

「名スコアしきい値 **(Given Name Score Threshold)**」
名のスコアしきい値を 0 から 100 の範囲で入力します。

「姓スコアしきい値 **(Surname Score Threshold)**」
姓のスコアしきい値を 0 から 100 の範囲で入力します。

「フルネーム・スコアしきい値 **(Full Name Score Threshold)**」
フルネームのスコアしきい値を 0 から 100 の範囲で入力します。

「**Name Manager** 設定 **(Name Manager settings)**」
Name Manager は、国/地域の重要な考慮事項が組み込まれるように、標準の名前精度を拡張します。これらの設定は、Name Manager が構成されている場合にのみ適用されます。

「名スコアしきい値 **(Given Name Score Threshold)**」
ルールが満たされたと見なされるのに必要な、名の最小スコアを入力します。

しきい値は 0 から 100 の間の整数値にする必要があります。スコアが高くなるほど、より正確に一致します。通常、70 未満のスコアはマッチングに適しませんが、姓またはフルネームと結合された場合に何らかの類似性を保証するのに役立つ可能性があります。

「姓スコアしきい値 **(Surname Score Threshold)**」
ルールが満たされたと見なされるのに必要な、姓の最小スコアを入力します。

しきい値は 0 から 100 の間の整数値にする必要があります。スコアが高くなるほど、より正確に一致します。通常、70 未満のスコアはマッチングに適しませんが、名またはフルネームと結合された場合に何らかの類似性を保証するのに役立つ可能性があります。

「フルネーム・スコアしきい値 **(Full Name Score Threshold)**」
ルールが満たされたと見なされるのに必要な、フルネームの最小スコアを入力します。

しきい値は 0 から 100 の間の整数値にする必要があります。スコアが高くなるほど、より正確に一致します。通常、70 未満のスコアはマッチングに適しません。

候補ビルダーのカスタマイズ

候補ビルダー構成を使用することによって、候補ビルダーの設定を変更できます。候補ビルダー機能に対する変更は、構成コンソールを使用して行います。

候補ビルダー

候補ビルダー機能により、システムがエンティティー解決処理の一部として、既存のエンティティーを候補リストに追加するときに使用する基準を定義します。

通常の候補ビルダーの設定に組み込まれているのは、住所、ユニーク番号、およびその他の番号です。これらは、入力アイデンティティーに対してどの既存のエンティティーが解決される可能性があるかを判別するために、システムが比較するデータ・タイプです。新規アイデンティティー・レコードがシステムに入ってきたときに、候補ビルダーによって識別されたデータ・タイプのいずれかについて一致する値を持っている既存のエンティティーがあれば、そのエンティティーが候補リストに追加されます。

候補ビルダー構成

候補ビルダーの設定は、候補ビルダー構成と呼ばれるグループ別に編成されます。1 つの解決構成内で使用できる候補ビルダー構成は 1 つだけです。

この製品に組み込まれている候補ビルダー構成は、次のとおりです。

- 「デフォルト **(Default)**」 - この設定には、エンティティーを候補リストに入れる際の基準として、住所、ユニーク番号、およびその他の番号が組み込まれています。
- 「デフォルトおよび名前のみ **(Default with name only)**」 - この設定には、エンティティーを候補リストに入れる際の基準として、名前が組み込まれています。この設定は、エンティティー・データに含まれるものが名前だけ、あるいは名前と他のわずかなデータ・タイプだけの可能性がある場合に使用されるように設計されています。

構成に関する考慮事項

汎用値の設定は、値が候補ビルダー処理の一部と見なされるかどうかに直接影響します。汎用値と見なされた値は、その後、候補リストの生成に使用されることはなくなります。

候補ビルダーの設定は、システム・パフォーマンスに直接影響します。索引ルックアップを使用してエンティティー・データベース内のありとあらゆるエンティティーに対して入力アイデンティティーを比較しているシステムでは、候補ビルダー機能で構成されているデータ・タイプのみが比較されています。これにより、候補リストが非常に迅速に生成されるようになります。エンティティー・データベースの規模が増大し、含まれるエンティティーの数が増大するにつれ、候補ビルダーが比較する対象も増大します。例えば、エンティティー・データベースに 100,000 件のエンティティーが含まれていて、候補ビルダーが候補リスト作成時に 3 つのデータ・タイプを比較するように設定されている場合、このシステムは、新規アイデンティティーがシステムに入ってくるたびに、候補リストを作成するためだけに最大 300,000 回の比較を行う可能性があります。エンティティー・データベースに 1,000,000 件のエンティティーが含まれていて、候補ビルダーが候補リスト作成時に 3 つのデータ・タイプを比較するように設定されている場合、このシステムは、新規アイデンティティーがシステムに入ってくるたびに、候補リストを作成するためだけに最大 3,000,000 回の比較を行う可能性があります。候補ビルダーの基準を 1 つ追加すると、このシステムはさらに、候補リストを作成するためだけに最大 1,000,000 回の比較を行う可能性があります。つまり、システムにロードされるアイデンティティー・レコード 1 件につき、追加で最大 1,000,000 回の比較が行われることになります。考慮するデータ・タイプが増えたために候補リストの規模が大きくなりすぎると、効果的な候補リストの作成に必要なデータ・タイプのみが候補ビルダーの設定に含まれている場合に比べて、エンティティー解決処理の実行速度ははるかに遅くなります。

構成設定として「デフォルト **(Default)**」を使用するか「デフォルトおよび名前のみ **(Default with name only)**」を使用するかを検討する際、「デフォルトおよび名前のみ **(Default with name only)**」を選択すると、「デフォルト **(Default)**」構成の場合よりも、必要となる比較の回数が 1 桁増えることを忘れないでください。

候補リスト

候補リストとは、入力アイデンティティー・レコードと一致する可能性のあるエンティティーのリストです。候補リストは、候補ビルダー構成に指定されている属性に基づいて、入力アイデンティティーと属性を共有しているエンティティーを取得することによって作成されます。

エンティティー解決処理では、エンティティー解決および関係解決用の候補リスト上にあるエンティティーのみが使用されます。

エンティティー解決および関係検出は属性に基づいて判別されるため、データ・ソース内の属性を慎重に検討して、最有力候補を作り出す属性がどれであるかを決定することが推奨されます。

候補リストが生成されると、エンティティー解決処理は、構成済みの解決ルールを使用し、候補リスト上の最初の候補と照らして入力アイデンティティーを比較します。システムは解決ルールを順番に使用して、入力アイデンティティーの属性が候補エンティティーの属性とどの程度正確に一致しているかを表す解決スコアを計算します。入力アイデンティティーの属性が当該ルールの解決スコアを満たしているか、または超えている場合、その入力アイデンティティー・レコードが候補エンティティーに解決されます。

解決スコアが当該解決ルールに設定されている解決スコアを満たしていない、または超えていない場合、システムは次の解決ルールに進みます。これが、入力アイデンティティー・レコードが候補エンティティーに解決されるまで、またはすべての解決ルールが使い尽くされるまで行われます。

入力アイデンティティー・レコードが既存のエンティティーに解決されない場合、システムはこのレコードを新規エンティティーとして解決し、この新規エンティティーをエンティティー・データベースに保管します。

候補ビルダー構成の作成

構成コンソールを使用して、候補ビルダー設定の新規グループを作成できます。これらの候補ビルダー構成は、設定を 1 つだけ変更することによって構成済みのさまざまな候補ビルダー設定を適用するための簡単な方法として役立ちます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。
3. 「候補ビルダー **(Candidate Builder)**」タブをクリックします。
4. 「候補ビルダー構成 **(Candidate Builder Config)**」ドロップダウン・リストに「**- - - 1** つ選択してください **- - - (- - - Select One - - -)**」が表示されていることを確認した後、「新規 **(New)**」ボタンをクリックします。
5. 「候補ビルダー構成 **(Candidate Builder Config)**」フィールドに、新規候補ビルダー構成の名前を入力します。
6. 「マッチング・タイプ **(Match Type)**」フィールドで、解決の候補基準として使用する最初のデータ・タイプを選択します。
7. 「セグメント名 **(Segment Name)**」フィールドに、マッチング・タイプのデータがある UMF セグメントの名前を入力します。
8. 「保存 **(Save)**」ボタンをクリックします。

次のタスク

ここで作成した候補ビルダー構成が「候補ビルダー構成 **(Candidate Builder Config)**」ドロップダウン・リストに表示されます。これで、この新規構成に基準を追加できるようになりました。

候補ビルダー構成への基準の追加

構成コンソールを使用して、既存の候補ビルダー構成にデータ・タイプを追加できます。候補ビルダー構成によって、エンティティー解決処理の一部として既存のエンティティーを候補リストに追加するための基準として、特定のデータ・タイプを指定します。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。
3. 「候補ビルダー **(Candidate Builder)**」タブをクリックします。
4. 「候補ビルダー構成 **(Candidate Builder Config)**」ドロップダウン・リストから構成を選択します。

5. 「新規 **(New)**」ボタンをクリックします。
6. 「マッチング・タイプ **(Match Type)**」ドロップダウン・リストからデータ・タイプを選択します。
7. 「セグメント名 **(Segment Name)**」フィールドに、マッチング・タイプのデータがある UMF セグメントの名前を入力します。
8. 「保存 **(Save)**」ボタンをクリックします。

次のタスク

エンティティー解決処理の一部として候補リストが作成されるときに、指定したデータ・タイプをシステムが考慮するようになりました。

候補ビルダー構成の削除

構成コンソールを使用して、候補ビルダー構成を削除できます。作成した候補ビルダー構成のうち、使用しないと決めたものは削除できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。
3. 「候補ビルダー **(Candidate Builder)**」タブをクリックします。
4. 「候補ビルダー構成 **(Candidate Builder Config)**」ドロップダウン・リストから構成を選択します。
5. 削除するマッチング・タイプの横にあるチェック・ボックスを選択します。
6. 「削除 **(Delete)**」ボタンをクリックします。 確認ボックスが表示され、「選択したレコードが削除されます。 (The selected records will be deleted.)」と示されます。
7. 候補ビルダー構成の削除を確認するには、「**OK**」をクリックします。

次のタスク

ここで削除した候補ビルダー設定の集合は、エンティティー解決処理の一部として候補リストを生成する際に使用できなくなります。

ヘルプ・トピック

「候補ビルダー **(Candidate Builder)**」ウィンドウ**:**

候補ビルダー設定のリストを表示するには、このウィンドウを使用します。候補ビルダーの設定は、候補ビルダー構成別にグループ化されています。

「候補ビルダー構成**: (Candidate Builder Config:)**」フィールド
: 設定を表示したい候補ビルダー構成を選択します。

マッチング・タイプ
: 入力アイデンティティーと既存のエンティティーの間で一致していなければならないデータのタイプです。このタイプのデータが一致している場合、その既存のエンティティーがエンティティー解決用の候補リストに追加されます。

「セグメント名 **(Segment Name)**」
マッチング・タイプのデータがある UMF セグメントの名前です。

一致シーケンス
候補リストの基準が比較されるときの順序のグループ番号です。

「候補ビルダー **(Candidate Builder)**」 **-** 「一般 **(General)**」タブ**:**

新しい候補ビルダー基準を構成する場合や、既存の候補ビルダー基準の詳細を表示する場合に、このタブを使用します。

「候補ビルダー構成 **(Candidate Builder Config)**」
この基準が属する候補ビルダー構成です。

マッチング・タイプ
解決の候補と見なされる既存のエンティティーと突き合わせるデータのタイプを選択します。

「セグメント名 **(Segment Name)**」
マッチング・タイプのデータがある UMF セグメントの名前を、次のように入力します。「ユニーク番号およびその他の番号 (Unique & Other Number)」= NUMBER。「住所 (Address)」= ADDRESS。「特性 (Characteristic)」= ATTRIBUTE。「名前 (Name)」= NAME。「E メール (Email)」= EMAIL_ADDR

確定と否定の構成

確定と否定の設定を調整することで、比較されたエンティティーの解決スコアを変更できます。

このタスクについて

確定と否定は、コンソールを使用して「解決ルール **(Resolution Rules)**」タブで表示および変更できます。

確定と否定

候補リストが作成され、基本的な解決基準の比較が済むと、エンティティー解決は追加基準の比較を行い、解決スコアを増減します。こうした追加基準が確定と否定です。

確定と否定は、次のようなデータ・タイプを比較します。

- 生年月日
- ユニーク番号
- 世代
- 特性
  - 任意の特性を指定して、確定と否定の一部として使用することができます。

確定の重みづけは、比較された 2 つのエンティティーの基準解決スコアに、より大きな重みを適用するために使用される値です。否定の重みづけは、比較された 2 つのエンティティーの基準解決スコアに、より小さな重みを適用するために使用される値 (通常は負の値) です。

例

ある解決構成に、生年月日について +10 の確定値と -20 の否定値が設定されているとします。インバウンド・レコードが候補エンティティーと共通の生年月日を共有している場合、解決スコアに値 10 が追加されます。両者の生年月日が異なる場合は、解決スコアから値 20 が減算されます。

注**:** 生年月日の確定と否定の重みづけは、特定の解決ルールによって割り当てられた解決スコアに対して適用されます。これらの重みづけは、パイプライン構成ファイルで構成されている **DOBConfThreshold** パラメーターと同じではありません。

特性の確定と否定の表示

新しい確定と否定を作成する前に、エンティティー解決中に使用される特性タイプの現在のリストを検討できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。
3. 「特性 **(Characteristics)**」タブをクリックします。
4. 「解決構成 **(Resolution Config)**」ドロップダウン・リストから、解決構成を選択します。

特性の確定と否定の作成

どの特性タイプもエンティティー解決の基準として指定できます。これを行うには、特性の確定と否定のリストにその特性タイプを追加します。

始める前に

特性タイプの解決での用途を、特定タイプの解決設定の構成時に、既に確定/否定に構成してあることが必要です。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。
3. 「特性 **(Characteristics)**」タブをクリックします。
4. 「解決構成 **(Resolution Config)**」ドロップダウン・リストから、解決構成を選択します。
5. 「新規 **(New)**」ボタンをクリックします。
6. 「一般 **(General)**」タブの「グループ番号 **(Group Number)**」フィールドで、この特性に適用するグループの番号を入力します。
7. 「説明 **(Description)**」フィールドで、構成している特性タイプの説明を入力します。
8. 「特性タイプ **(Characteristic Type)**」ドロップダウン・リストから、構成する特性タイプを選択します。
9. 「確定の重みづけ **(Confirm Weight)**」フィールドに、(比較されたエンティティーが確定要件を満たした場合に) 相似スコアに加算する値を (1 から 100 の段階で) 入力します。

10. 「否定の重みづけ **(Denial Weight)**」フィールドに、(比較されたエンティティーが否定要件を満たした場合に) 相似スコアから減算する負の値を、負符号 (-) を使用して (1 から 100 の段階で) 入力します。
11. 「保存 **(Save)**」ボタンをクリックします。

特性の確定と否定の削除

エンティティー解決の基準となる考慮事項から特性タイプを削除するには、特性の確定と否定のリストからその特性タイプを削除します。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「解決 **(Resolution)**」ボタンをクリックします。
3. 「特性 **(Characteristics)**」タブをクリックします。
4. 「解決構成 **(Resolution Config)**」ドロップダウン・リストから、解決構成を選択します。
5. 削除する特性タイプの横にあるチェック・ボックスを選択します。
6. 「削除 **(Delete)**」ボタンをクリックします。
7. 確認ウィンドウで「**OK**」をクリックして、その解決構成を削除します。

ヘルプ・トピック

「確定と否定 **(Confirms & Denials)**」ウィンドウ**:**

エンティティー解決の確定と否定の処理を構成するには、このウィンドウを使用します。解決スコアに追加される確定および否定のスコアに加えて、確定および否定が処理される順序を指定できます。いずれかの確定または否定が満たされれば、対応するスコアが適用され、残りの確定と否定は処理されません。確定の場合は正のスコアが適用され、否定の場合は負のスコアが適用されます。

「順序 **(Order)**」
: 現行の処理順

説明
: 確定または否定の説明

「スコア **(Score)**」
: 指定の確定/否定用の正または負のスコア因子を入力します。

「並べ替え **(Reorder)**」
: 矢印 (上向きまたは下向き) をクリックして、確定または否定を 1 段階、該当する方向に移動します。最初の確定または否定が満たされれば処理は停止しますので、正しい順序を選択することが重要です。正しい順序を選択することは、エンティティー解決処理の結果に重大な影響を及ぼす可能性があります。

「特性 **(Characteristics)**」ウィンドウ**:**

このウィンドウは、比較結果がエンティティー解決のスコアリングに影響を与えるように構成されているエンティティー特性のリストを表示する際に使用します。エンティティー解決のスコアリングに影響するのは、「解決ルール一般 **(Resolution Rules General)**」タブの「特性の否定を有効化 **(Characteristic Denials Enabled)**」値が「はい (Yes)」に設定されている場合のみです。

説明　比較される特性の名前

「特性タイプ **(Characteristic Type)**」
比較される特性タイプのシステム名

「確定の重みづけ **(Confirm Weight)**」
比較された特性値が同一であった場合にエンティティー解決のスコアリング処理に追加される値

「否定の重みづけ **(Denial Weight)**」
比較された特性値が異なるものであった場合にエンティティー解決のスコアリング処理に追加される値

「解決 **(Resolution)**」 **-** 「特性 **(Characteristics)**」 **-** 「一般 **(General)**」タブ**:**

新しい特性確定/否定を構成する場合や、既存の特性確定/否定の詳細を表示する場合に、このタブを使用します。

「グループ **(Group)**」
特性確定/否定の処理順を指定する番号を入力します。

説明　確定/否定の説明を入力します。

「特性タイプ **(Characteristic Type)**」
確定/否定の特性タイプを選択します。

「確定の重みづけ **(Confirm Weight)**」
比較された特性値が同一であった場合にエンティティー解決スコアに追加されるスコアを入力します。

「否定の重みづけ **(Denial Weight)**」
比較された特性値が異なるものであった場合にエンティティー解決スコアに追加される負のスコアを入力します。

システム・パラメーターの構成

Identity Insight システムの特定の機能を構成できます。

名前スコアリングのシステム・パラメーターの構成

エンティティー解決処理の一部として候補リストが生成されるときに使用する、名前スコアリング・アルゴリズムを構成できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「一般 **(General)**」 > 「システム・パラメーター **(System Parameters)**」を選択します。
2. 「**パラメーター・グループ (Parameter Group)**」 リストから、「**NAME_MATCHING**」パラメーター・グループを選択します。
3. 「**ALGORITHM**」システム・パラメーターを選択します。
4. 「現行値 **(Current Value)**」で、使用する Name Comparator アルゴリズムを示す整数値を指定します。 このシステム・パラメーターをデフォルト値に戻すには、「デフォルト値 **(Default Value)**」に表示されている値を、「現行値 **(Current Value)**」フィールドに入力します。

注**:** Name Comparator 2 が、製品バージョン 3.9.1 以降のデフォルトの名前スコアリング・アルゴリズムです。

5. 「保存 **(Save)**」をクリックします。

Name Manager のシステム・パラメーターの構成

デフォルトでは、製品のインストール時に、Name Manager による名前スコアリングのシステム・パラメーターが構成されます。しかし、必要に応じて、デフォルトのシステム・パラメーターを更新できます。例えば、Name Manager サポート・ライブラリーの場所の変更が必要になることがあります。

このタスクについて

Name Manager のシステム・パラメーターを通じて、Name Manager サポート・ライブラリーのパスを設定し、タイプ別の名前のカテゴリー化を有効にします。また、**CROSSCHECKCULTURE** システム・パラメーターを設定して、各種国/地域別情報間での名前処理を構成します。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」 > 「一般 **(General)**」 > 「システム・パラメーター **(System Parameters)**」を選択します。
2. 「**パラメーター・グループ (Parameter Group)**」 リストから、「**NAMEMANAGER**」パラメーター・グループを選択します。
3. 左側のペインから、構成する Name Manager システム・パラメーターを選択します。

Name Manager システム・パラメーター	説明
「**SUPPORTPATH**」	Name Manager サポート・ファイルの場所を指示します。デフォルト値は ./data で、これは最上位製品ディレクトリーからの相対パスです。インストール時にサポート・ファイルを別の場所に移動した場合は、この値を新しい場所の絶対パスに変更します。
「**NAMESIFTER**」	名前タイプ別 (個人名か組織名か) の名前カテゴリー化機能をオンにするどうかを指示します。 名前のタイプ別カテゴリー化 (名前フィルター機能) を有効にするには、「現行値 **(Current Value)**」に 1 (インストール時の新しいデフォルト) を入力します。 名前のタイプ別カテゴリー化 (名前フィルター機能) を無効にするには、「現行値 **(Current Value)**」に 0 (アップグレード時のデフォルト) を入力します。

Name Manager システム・パラメーター	説明
「**CROSSCHECKCULTURE**」	名前の国/地域別情報が異なる場合に、名前の国/地域別情報間で Name Manager による名前スコアリングを実行するかどうかを指示します。 インバウンド側の名前の国/地域別情報のみを検査してから、両者の名前をスコアリングするには、「現行値 **(Current Value)**」に 0 を入力します。 名前の国/地域別情報の値を検査してから、両者の名前をスコアリングする (インストール時の新しいデフォルト) には、「現行値 **(Current Value)**」に 1 を入力します。

重要: **CROSSCHECKCULTURE** システム・パラメーターは、パイプラインにおいてエンティティー解決がどのように名前スコアリングを国/地域別情報ごとに処理するかに影響します。システム・パラメーターを現行値から変更する場合は、事前に IBM サービス または IBM サポートにご相談ください。

4. 「保存 **(Save)**」をクリックします。

データベースのシステム・パラメーターの構成

エンティティー解決中にパイプラインによって作成されるすべての候補リストの IN 節の最大サイズを構成できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. システム・パラメーター **(System Parameters)**」タブをクリックします。
4. 「**パラメーター・グループ (Parameter Group)**」 ドロップダウン・リストから、「**DB_CONFIG**」パラメーター・グループを選択します。
5. 「**MAX_IN_CLAUSE**」システム・パラメーターをクリックします。
6. 「現行値 **(Current Value)**」フィールドに、エンティティー解決処理の一部として候補リストが生成されるときに IN 節に含める最大文字数を入力します。 有効な値は、0 から 1000 までの任意の整数です。 このシステム・パラメーターをそのデフォルト値に戻すには、このフィールドで、「デフォルト値」**(Default Value)**」フィールドに表示されている値を入力してください。

   注: この値は、データベースのパフォーマンスに影響します。データベースのサイズおよびシステム・ハードウェアの性能に基づいて、このパラメーターに指定する値は慎重に検討してください。
7. 「保存 **(Save)**」をクリックします。

ログのシステム・パラメーターの構成

データベース内の特定のエンティティー解決表に使用するロギング・レベルを構成できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. システム・パラメーター **(System Parameters)**」タブをクリックします。
4. 「**パラメーター・グループ (Parameter Group)**」ドロップダウン・メニューから、「**LOG_LEVEL**」システム・パラメーターを選択します。
5. 構成するパラメーターの名前をクリックします。
6. 「現行値 **(Current Value)**」フィールドに、このパラメーター・コードに適用するログ・レベルを入力します。「パラメーターの説明 **(Parameter Description)**」 フィールドに、有効な値のリストと説明があります。 このシステム・パラメーターをそのデフォルト値に戻すには、このフィールドで、「デフォルト値 **(Default Value)**」フィールドに表示されている値を入力してください。

   注**:** この値は、データベースおよび Visualizer などのコンポーネントのパフォーマンスに影響します。データベースのサイズおよびシステム・ハードウェアの性能に基づいて、このパラメーターに指定する値は慎重に検討してください。例えば、次のような表に対して LOG_LEVEL を 4 未満に設定すると、Visualizer が動作を停止する原因となります。

   - ER_DETAIL
   - ER_ENTITY_SCORE
   - ER_ENTITY_STATE
   - ER_RELOCATION
7. 「保存 **(Save)**」をクリックします。

確定と否定のシステム・パラメーターの構成

構成済みの確定と否定のための比較をすべて実行するかどうかを指定できます。または、構成されている順序で、いずれかの確定または否定が満たされるまで比較を行うことを指定できます。 2 番目のオプションを使用すると、処理時間が高速になります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. システム・パラメーター **(System Parameters)**」タブをクリックします。
4. 「**パラメーター・グループ (Parameter Group)**」ドロップダウン・メニューから、「**MM**」パラメーター・グループを選択します。
5. 「**MULTICONFIRMATION**」システム・パラメーターをクリックします。
6. すべての確定と否定が処理され、条件が満たされた確定/否定すべてについて、スコアの変更の合計が現在処理中の解決ルールに適用されるようにするには、「現行値 **(Current Value)**」フィールドに 1 を入力します。または、確定と否定が指定の順序で処理され、最初に条件が満たされた確定/否定で処理を停止し、そのスコアの変更が現在処理中の解決ルールに適用されるようにするには、

0 を入力します。 このシステム・パラメーターをそのデフォルト値に戻すには、このフィールドで、「デフォルト値」**(Default Value)**」フィールドに表示されている値を入力してください。

7. 「保存 **(Save)**」をクリックします。

ロール・アラートのシステム・パラメーターの構成

インバウンド・エンティティーに対してエンティティー解決ルールによって生成されたすべてのロール・アラートが報告されるようにするのか、インバウンド・エンティティーに対してエンティティー解決ルールによって生成された最も強いロール・アラートのみが報告されるようにするのかを構成できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. システム・パラメーター **(System Parameters)**」タブをクリックします。
4. 「**パラメーター・グループ (Parameter Group)**」ドロップダウン・メニューから、「**MM**」パラメーター・グループを選択します。
5. 「**REPORT_SAME_CONFLICTS**」システム・パラメーターをクリックします。
6. インバウンド・エンティティーに対して各解決ルールによって生成されたすべてのロール・アラートが報告されるようにするには、「現行値 **(Current Value)**」フィールドに 1 を入力します。または、インバウンド・エンティティーに対して各解決ルールによって生成された最も強いロール・アラートのみが報告されるようにするには、0 を入力します。 このシステム・パラメーターをそのデフォルト値に戻すには、このフィールドで、「デフォルト値」**(Default Value)**」フィールドに表示されている値を入力してください。
7. 「保存 **(Save)**」をクリックします。

属性アラート・ジェネレーターのシステム・パラメーターの構成

新規属性アラート・ジェネレーターの期限切れになるまでのアクティブ期間のデフォルト日数を構成できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. システム・パラメーター **(System Parameters)**」タブをクリックします。
4. 「**パラメーター・グループ (Parameter Group)**」ドロップダウン・メニューから、「**PERSISTENT_SEARCH**」を選択します。
5. 「**SEARCH_EXPIRATION_TIME**」システム・パラメーターをクリックします。
6. 「現行値 **(Current Value)**」フィールドに、新規属性アラート・ジェネレーターの期限切れになるまでのアクティブ期間のデフォルト日数を入力します。Visualizer ユーザーは別の有効期限を指定できますが、この値が、新規属性アラート・ジェネレーターのアクティブ期間のデフォルトの日数になります。
7. 「保存 **(Save)**」をクリックします。

並行性のシステム・パラメーターの構成

パイプラインが並列パイプライン処理用に構成されている場合は、パイプラインが開始されたときに開始されるデフォルトの並列パイプライン・スレッド数を設定できます。

始める前に

構成コンソールへのログイン時に「構成の編集 **(Edit Configuration)**」チェック・ボックスを選択したことを確認します。この選択により、システム・パラメーターを含めて、システム構成を追加、変更、削除できるようになります。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. システム・パラメーター **(System Parameters)**」タブをクリックします。
4. 「**パラメーター・グループ (Parameter Group)**」ドロップダウン・メニューから、「**CONCURRENCY**」パラメーター・グループを選択します。
5. 「**DEFAULT_CONCURRENCY**」システム・パラメーターを選択します。
6. 「現行値 (Current Value)」に、パイプラインが開始されたときに常に開始されるデフォルトのパイプライン処理スレッド数を示す数を入力します。

データ品質管理のシステム・パラメーターの構成

日付をフォーマットする際に構成コンソールが使用するデフォルトの日付区切り文字を構成できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. システム・パラメーター **(System Parameters)**」タブをクリックします。
4. 「**パラメーター・グループ (Parameter Group)**」ドロップダウン・メニューから、「**DQM**」パラメーター・グループを選択します。
5. 「**SYSTEM_DATE_DELIMITER**」システム・パラメーターをクリックします。
6. 「現行値 **(Current Value)**」フィールドに、**/** または **-** を入力して、システムが日付をフォーマットする際にどちらの区切り文字が使用されるようにするかを指定します。 このシステム・パラメーターをそのデフォルト値に戻すには、このフィールドで、「デフォルト値」**(Default Value)**」フィールドに表示されている値を入力してください。
7. 「保存 **(Save)**」をクリックします。

製品オプションのシステム・パラメーターの構成

追加でどの製品オプションを有効にするかを構成できます。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。

3. システム・パラメーター **(System Parameters)**」タブをクリックします。
4. 「**パラメーター・グループ (Parameter Group)**」ドロップダウン・メニューから、「**CONSOLE_CONFIG**」パラメーター・グループを選択します。
5. 「**PRODUCT_OPTIONS**」システム・パラメーターをクリックします。
6. 「現行値 **(Current Value)**」フィールドに、IBM によって提供された、有効にする製品機能に対応するコードを入力します。 すべて大文字を使用する必要があります。システムで有効にする全機能をスペース区切りのリストとして入力できます。このシステム・パラメーターをそのデフォルト値に戻すには、このフィールドで、「デフォルト値」**(Default Value)**」フィールドに表示されている値を入力してください。
7. 「保存 **(Save)**」をクリックします。

Event Manager のシステム・パラメーターの構成

Event Manager によるイベント処理を有効化し、イベント処理のシステム・パラメーター (イベント・プロセッサーの Universal Resource Indicator (URI) など) を構成することができます。

手順

1. 構成コンソールで、「システム構成」タブをクリックします。
2. 左側のペインから、構成する Event Manager システム・パラメーターを選択します。
   a. 「イベント処理を有効にする **(Enable Event Processing)**」は、Event Manager を通じたイベント処理が有効であるか無効であるかを示します。
   b. 「イベント・プロセッサーのタイムアウト **(Event Processor Timeout)**」は、パイプラインが外部イベント・プロセッサーからの応答を待機する、タイムアウト・エラーが発生するまでの秒数を示します。デフォルト値は 60 秒です。
   c. 「イベント・プロセッサー **URI (Event Processor URI)**」は、外部イベント・プロセッサーに接続するための Universal Resource Indicator (URI) を示します。 「現行値 **(Current Value)**」に URI を入力します。デフォルトのポート番号である場合でも、ポート番号を含めてください。例えば、`http://localhost:13510/gem` です。
   d. 「イベント・ヒストリー期間 **(Event History Window)**」は、新規インバウンド・イベントの評価時にパイプラインが外部イベント・プロセッサーに送信するイベント・ヒストリーの日数を示します。(デフォルトの日数は 180 です。)
3. 「保存 **(Save)**」ボタンをクリックします。

Visualizer のシステム・パラメーターの構成

Visualizer のシステム・パラメーターには、各ロール・アラート・ルールに定義されている「最小アラートしきい値 **(Minimum Alert Threshold)**」の設定を下回るアラートも含め、すべてのアラートを個々の Visualizer ユーザーが表示できるようにする機能が備わっています。Visualizer ユーザーがより柔軟にアラートを表示できるように、この設定を変更することが可能です。

手順

1. 構成コンソールで、「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. システム・パラメーター **(System Parameters)**」タブをクリックします。
4. 「**パラメーター・グループ (Parameter Group)**」 ドロップダウン・リストから、「**VISUALIZER**」パラメーター・グループを選択します。
5. 「**ALLOW_ALERT_THRESHOLD_OVERRIDE**」システム・パラメーターをクリックします。
6. 次のオプションのいずれかを選択してください。
   - Visualizer ユーザーが構成コンソールの「ロール・アラート・ルール - フィルター **(Role Alert Rules - Filters)**」 タブで定義済みのアラートしきい値をオーバーライドできるようにするには、「現行値 **(Current Value)**」フィールドに 1 を入力します。
   - Visualizer ユーザーが構成コンソールの「ロール・アラート・ルール - フィルター **(Role Alert Rules - Filters)**」 タブでシステム定義のアラートしきい値をオーバーライドする機能を無効化する (つまり非許可にする) には、0 を入力します。
   - このシステム・パラメーターをデフォルト値に戻すには、「デフォルト値 **(Default Value)**」フィールドに表示されている値を、「現行値 **(Current Value)**」フィールドに入力します。
7. 「保存 **(Save)**」ボタンをクリックします。

Centrifuge のデフォルト・パスの設定

オプションである Centrifuge Systems の Centrifuge Desktop を使用してエンティティー・グラフを視覚化および表示する場合、Visualizer 設定に Centrifuge Desktop ファイル・パスを指定する必要があります。

このタスクについて

デフォルト・パス設定は、Visualizer クライアントごとに構成されます。このタスクに従ってデフォルト・パスを指定することでパスが設定される対象は、現在ログインしている Visualizer のみです。

手順

1. Visualizer で、「ファイル **(File)**」 > 「設定 **(Preferences)**」 > 「システム設定 **(System Preferences)**」をクリックします。
2. 「**Centrifuge** パス **(Centrifuge path)**」の「ファイル・パス **(File Paths)**」セクションの下で、以下を実行します。
   - Centrifuge Desktop アプリケーションのファイル・パスまたは URL (Uniform Resource Locator) をフィールドに入力します。
   - または、Centrifuge Desktop アプリケーションを参照し、開きます。
3. 「送信 **(Submit)**」をクリックします。 確認メッセージによって、変更を有効にするには Visualizer の再始動が必要なことが通知されます。
4. 確認メッセージで「**OK**」をクリックします。
5. Visualizer を閉じて、Visualizer を再オープンし、再度ログインします。

タスクの結果

パスが構成されると、「調査 **(Research)**」ウィンドウの「ロール・アラート詳細 **(Role Alert Detail)**」画面および「エンティティー・レジュメ **(Entity Resume)**」画面に「**Centrifuge**」ボタンが表示されます。そのボタンをクリックすると、Visualizer から直接、Centrifuge Desktop アプリケーションが起動されます。

UMF ファイルのデフォルト・パスの設定

Visualizer による処理のためにアイデンティティー・レコードを UMF データ・ファイルで定期的にロードする場合、デフォルト・パスを設定することで手順を 1 つ省略できます。

このタスクについて

デフォルト・パス設定は、Visualizer クライアントごとに構成されます。このタスクに従ってデフォルト・パスを指定することでパスが設定される対象は、現在ログインしている Visualizer のみです。

手順

1. Visualizer で、「ファイル **(File)**」 > 「設定 **(Preferences)**」 > 「システム設定 **(System Preferences)**」を選択します。
2. 「ファイル・ロードのデフォルト・パス **(Default path for File Load)**」で、以下のいずれかを実行します。
   - 使用するディレクトリーの絶対パスを入力します。
   - または、ディレクトリーを参照して選択します。
3. 「送信 **(Submit)**」をクリックします。 確認メッセージによって、変更を有効にするには Visualizer の再始動が必要なことが通知されます。
4. 確認メッセージで「**OK**」をクリックします。
5. Visualizer を閉じて、Visualizer を再始動し、再度ログインします。

タスクの結果

UMF ファイルをロードするとき、ここで指定したディレクトリーが、毎回デフォルト・パスになります。

属性とスコアリングのカスタマイズ

IBM InfoSphere Identity Insight には、属性データの構成、およびスコアリング・アルゴリズムの統合を行うための機能拡張が用意されています。これらの変更により、比較およびスコアリングすることができるアイデンティティー・データの規模やタイプが拡張され、エンティティー解決処理において新規スコアリング・アルゴリズムの追加が可能になります。これらの機能を総称して、属性とスコアリングのカスタマイズと呼んでいます。

エンティティー解決テクノロジーでは、アイデンティティー・マッチング・アルゴリズムおよびスコアリング・アルゴリズムを使用して、一般的なアイデンティティー・データ (名前、住所、電話番号、クレジット・カード番号、納税者番号、免許証番号など) を比較して解決し、一致の可能性を示すことができます。このシステ

ムでは、アカウントやエンティティーを説明するデータ・エレメントのことを、属性と呼んでいます。属性には、個人、組織、場所、またはアイテムを説明する特性や特質などが含まれます。属性とスコアリングのカスタマイズを追加することで、新しいタイプの識別データを追加することや、製品スコアリング・プラグインとして開発されたスコアリング・アルゴリズムを関連付けることができます。例えば、指紋、網膜スキャン、または DNA 鑑定から得られたアイデンティティー・データを追加し、適切な比較アルゴリズムが組み込まれたスコアリング・プラグインを使用してそれらのデータを比較してスコアリングすることができます。

これらの属性およびスコアリングの機能拡張により、次のようなことが可能になるため、エンティティー解決処理が強化されます。

- ATTR_VALUE (8 KB に拡張) と、さらに大きいサイズのデータを保管するための ATTR_LARGE_DATA を使用して、より大きいサイズの属性データを保管および比較する。
- 提供されたスコアリング・アルゴリズムを広範な属性タイプに適用し、それらの属性をより簡単に構成して、詳細に制御する。
- 属性比較とスコアリングのカスタマイズによって得られた結果を、Visualizer のレポート機能およびアラート機能を使用して統合する。
- ユーザーが作成したスコアリング・アルゴリズムを追加するためのプラグイン・モデルを適用する。
- 構成コンソールを使用してカスタム・スコアリング・プラグインを統合する。

大きい属性データの保管

システムがスコアリング・プラグインを使用して、より大きい属性データを保管および処理できるようにするには、メタデータを Universal Message Format (UMF) に変換して、適切な列に保管する必要があります。

このタスクについて

手順

1. システム用に作成したエンティティー・モデルを使用して、入力データを分析し、入力データがどの程度 UMF 標準に適合しているかを確認します。 次のステップに進む前に、既存の UMF セグメントおよび UMF タグについて明確に理解しておく必要があります。
2. エンティティー・モデルと一致する UMF レコードを生成する ETL ツールを構成します。
3. ETL ツールを実行します。

次のタスク

データを UMF に変換した後は、それらの UMF レコードをパイプラインに送信して処理することができます。

大きい属性データの保管パラメーター

システムでスコアリング用の大きい属性データを保管および処理するためには、メタデータを Universal Message Format (UMF) に変換して、適切な列に保管する必要があります。

カスタム属性アプリケーションおよびカスタム・スコアリング・アプリケーション用の大きい属性データまたは構造化されていない属性データを保管するには、ATTR_VALUE 列と ATTR_LARGE_DATA 列を使用します。

列と **UMF** タグ名	データのタイプとサイズ	必須	説明
ATTR_VALUE	varchar(255) (デフォルト) 最大 8k までサイズ変更可能	はい	基本スコアリング・プラグインによる ETL 処理において属性の 1 つとして使用されるデータ。 データが 8k を超えていて、バイナリー形式の場合は、データを ATTR_LARGE_DATA 列に保管し、そのデータ用のユニーク ID を ATTR_VALUE 列に作成します。その ATTR_VALUE ID が比較とスコアリングで使用されます。例えば、比較や Visualizer およびレポートへの表示が可能な MD5 (メッセージ・ダイジェスト・アルゴリズム 5) 片方向ハッシュを作成します。 最大列サイズはデータベースに依存します。255/3 よりも大きいバイナリー・データを ATTR_VALUE に保管するためには、列をサイズ変更する必要があります。そうすると、キャッシュに収まる行数はかなり少なくなるため、パフォーマンス上の理由から、データベース・キャッシュを再チューニングすることを検討してください。

ATTR_LARGE_DATA	文字ラージ・オブジェクト (CLOB)。8k を超えるデータに使用します。	いいえ	文字データとして保管します。例えば、バイナリー・データの Base64 エンコードを使用します。 この列を使用して、ATTR_VALUE 列には大きすぎて収まらない属性データを保管します。 ATTR_LARGE_DATA は、CLOB (文字ラージ・オブジェクト) タイプの列で、処理できるデータのサイズは無制限です。 このデータはエンティティー解決に使用できます。カスタマイズされた比較プラグインの作成者は、このデータの構造を分かっている必要があります。このデータは、フォーマットが非標準であり各種システムごとに異なるため、Visualizer には表示されません。 CLOB をキャッシュすることはできず、ディスク読み取りが必要になるため、CLOB は varchar 列ほどの役割は果たしません。ATTR_VALUE のほうが望ましい理由は、そこにあります。 ATTR_VALUE のサイズを増やすことで、キャッシュされる属性データの数が非常に少なくなってしまう場合は、ATTR_LARGE_DATA を 8k 未満のデータのみに使用するようにして、他の、大きくない属性 (性別や DOB など) 用にキャッシュを確保したほうが良い場合もあります。これはアーキテクトの裁量に委ねられます。データベース・アドミニストレーターに相談することを検討してください。 ATTR_LARGE_DATA を使用する場合は、ATTR_VALUE にも何らかの値を入力してください。ATTR_VALUE に収まるデータから、意味のある検索キーを作る方法がある場合は、これを作成して ATTR_VALUE に配置すべきです。意味のある検索キーを作成する方法がない場合は、何か別の、値としてユニークな検索キーを ATTR_VALUE に配置してください。そうしないと、パイプラインが正常に機能せず、おそらくは DQM エラーが出て失敗します。 ユニーク・キーは、DQM ルールをセットアップして、データの MD5 ハッシュを作成するか (600 ルール)、構成済みのルールに基づいてカスタム・ハッシュを作成することによって (615 ルール)、自動的に生成できます。ATTR_VALUE は汎用値の判別に使用されるため、永続検索用として属性タイプをセットアップする場合は特に、この値が極めてユニークであることが重要です。 **注:** 組み込みの「binaryAttributeScoring」プラグインは、ATTR_VALUE の比較を一切行いません。これは、ATTR_LARGE_DATA セグメントを調べてスコアを算出するのみです。

例

以下に、大きいバイナリー・データの MD5 ハッシュ出力の例を示します。

```
<ATTRIBUTE><ATTR_TYPE>BIOMETRIC-1</ATTR_TYPE>
<ATTR_VALUE>214b21fc3e040f844a07710b1bb451a0
</ATTR_VALUE><ATTR_LARGE_DATA>
<![H4sICBRTqkgAA2Zvby50eHQAK0ktLuHlAgDkTqoPBgAAAA==]>
</ATTR_LARGE_DATA></ATTRIBUTE>
```

実際の ATTR_LARGE_DATA 値は、この例よりはるかに大きくなる可能性があります。

大きい属性データのソース特性の構成

構成コンソールを使用して、大きい属性データのソース特性を構成します。

このタスクについて

構成コンソールを使用することで、基本プラグイン用のデータを構成する場合と同じように、カスタマイズされたスコアリング・プラグイン用の属性データの新規タイプを構成できます。

手順

1. 構成コンソールの「プラグイン (Plugins)」タブで、カスタマイズされたプラグインの選択ボックスをクリックします。
2. 「特性 (Characteristics)」タブをクリックします。
3. 「一般 (General)」タブをクリックして、必要に応じて各フィールドに入力します。
4. 適切な「データ・タイプ (Data Type)」を選択します。 「データ・タイプ (Data Type)」は、CHAR、DATE、CLOB のいずれかです。「データ・タイプ (Data Type)」の要件は、 207 ページの『大きい属性データの保管パラメーター』に記載されています。
5. 適切な「クラス (Class)」を選択します。
6. 「解決での用途 (Resolution Usage)」の値を選択します。
7. 構成しているスコアリング・プラグインの名前を選択します。
8. 「表示レベル (Display Level)」フィールドで適切な値を選択します。 ATTRIBUTE.ATTR_VALUE 列や ATTRIBUTE.ATTR_LARGE_DATA 列の内容が Visualizer に表示されないようにするには、「タイプのみ、値なし (Type only without value)」を選択します。通常、ラージ・オブジェクト列 (CLOB) を使用する場合は ATTR_VALUE 列は使用しません。また、ATTR_LARGE_DATA (CLOB) 列には通常、Base64 エンコードのデータが含まれますが、このデータは Visualizer での表示にとって関連性も有益性もありません。
9. 「保存 (Save)」をクリックします。

タスクの結果

「ソース (Sources)」の下の「特性 (Characteristics)」タブに、新規タイプと関連情報が表示されました。

大きいデータの解決特性の構成

構成コンソールを使用して、大きい属性データおよびカスタム・スコアリング・プラグインの解決特性を構成します。

このタスクについて

最後に、新規特性タイプの確定と否定の情報を構成します。

手順

1. 構成コンソールで、「セットアップ (Setup)」ボタンをクリックします。
2. 「解決 (Resolution)」ボタンをクリックします。
3. 「特性 (Characteristics)」タブをクリックします。
4. ドロップダウン・メニューから「デフォルト (DEFAULT)」などの適切な「解決構成 (Resolution Configuration)」を選択した後、「新規 (New)」ボタンをクリックします。
5. 「一般 (General)」タブを選択し、表示されたフィールドに値を入力します。フィールド・オプションと推奨事項の説明については、『解決特性と解決オプション』を参照してください。
6. 「保存 (Save)」をクリックします。

タスクの結果

解決構成用に作成した値が含まれた要約表が、概要画面に表示されます。

解決特性と解決オプション

解決特性の「一般 (general)」タブ表示を使用して、大きいデータのデータ・タイプおよびカスタム・スコアリング・プラグイン用のアクションとオプションを構成します。

「解決での用途 (Resolution Usage)」フィールドと「確定/否定 (Confirm/Deny)」値による選択のある特性タイプを構成している場合、追加フィールドが動的に表示されます。

フィールド	必須	フィールドの選択肢および説明
「グループ (Group)」	はい	この特性の識別に使用するグループの番号を入力します。
説明	はい	このデフォルト解決構成の簡略説明を入力します。このフィールドをブランクのままにすると、エラーになります。
「特性タイプ (Characteristic Type)」	はい	作業対象のタイプを選択します。このリストには、ソースに対して既に構成済みのタイプがすべて含まれています。
「確定の重みづけ (Confirm Weight)」	はい	0 - 100 の任意の値。相似スコアに影響します。

「プラグインでの確定しきい値 (Plugin Confirm Threshold)」	いいえ	フリー・フォームのテキスト・フィールド。このフィールドは、「解決での用途 (Resolution Usage)」フィールドが「確定/否定 (Confirm/Deny)」に設定された特性タイプを指定した場合、例えばこのタイプがカスタム・プラグイン用である場合などに表示されます。 この特性タイプが、エンティティー解決処理の一部である確定と否定においてスコアリング・プラグインによってスコアリングされる場合は、確定しきい値を指定します。プラグインによって割り当てられたスコアがこの値以上であった場合、その一致は確定と見なされ、「確定の重みづけ (Confirm Weight)」フィールドの値が「解決の信頼度 (Resolution Confidence)」スコアに追加されます。
「否定の重みづけ (Denial Weight)」	はい	0 - 100 の任意の値。相似スコアに影響します。
「プラグインでの否定しきい値 (Plugin Denial Threshold)」	いいえ	フリー・フォームのテキスト・フィールド。このフィールドは、「解決での用途 (Resolution Usage)」フィールドが「確定/否定 (Confirm/Deny)」に設定された特性タイプを指定した場合にのみ、例えばこのタイプがカスタム・プラグイン用である場合などに表示されます。 この特性タイプが、エンティティー解決処理の一部である確定と否定においてスコアリング・プラグインによってスコアリングされる場合は、ここに (プラグインによって解釈される) 否定しきい値を指定します。プラグインによって割り当てられたスコアがこの値以下であった場合、その一致は否定と見なされ、「否定の重みづけ (Denial Weight)」フィールドの値が「解決の信頼度 (Resolution Confidence)」スコアに追加されます。

属性およびスコアリングのカスタマイズ用構成レポート

構成コンソール上の構成レポートには、属性およびスコアリングのカスタマイズ用のエレメントも含まれています。

構成レポートには、次のようなエレメントが追加されています。

- レポートの「特性タイプ (Characteristics Types)」セクションには、「スコアリング・プラグイン (Scoring Plugin)」という新しい列があります。この列には、それぞれのプラグイン特性タイプの値が表示されます。
- 新しい「プラグイン・レポート (Plugin report)」セクションには、構成済みのレコードが表示されます。「ID」、「名前 (Name)」、「タイプ (Type)」、「バージョン (Version)」、および「ライブラリー短縮名 (Library Short Name)」という列ヘッダー・ラベルが含まれています。
- 「エンティティー解決特性 (Entity Resolution Characteristics)」セクションに 2 つの新しい列が追加され、「プラグインでの確定しきい値 (Plugin Confirm Threshold)」と「プラグインでの否定しきい値 (Plugin Denial Threshold)」の両方の値が示されています。

カスタム・スコアリング・プラグインの構成

構成コンソールを使用して、カスタム・スコアリング・プラグインを構成します。

始める前に

新規のプラグインでは、それが正しく IBM InfoSphere Identity Insight に適合していることを確認します。IBM InfoSphere Identity Insight 用のカスタム・スコアリング・プラグインの開発を参照してください。

このタスクについて

構成コンソールを使用すると、システムに追加したスコアリング・プラグインを構成することができます。

手順

1. 構成コンソールで、「セットアップ (Setup)」ボタンをクリックします。
2. 「一般 (General)」ボタンをクリックします。
3. 「プラグイン (Plugins)」タブをクリックします。
4. 新規プラグインを構成するには、「新規 (New)」ボタンをクリックします。
5. 既存のプラグインを編集するには、「プラグイン (Plugins)」列のリストから、構成するプラグインをクリックして選択します。編集できるのは、お客様のプラグインのみです。
6. 「一般 (General)」タブで、必要に応じて各フィールドに入力します。

フィールド名	必須	説明
「プラグイン (Plugin)」	はい	「スコアリング・プラグイン (Scoring Plugin)」メニュー・オプションに表示されるプラグイン名。
「ライブラリーの短縮名 (Short Library Name)」	はい	このフィールドのこの名前は、プラグイン表の LIBRARY_NAME 列に使用されます。「ライブラリーの短縮名 (Library Short Name)」フィールドは、パイプライン・コードが呼び出すソフトウェア・ライブラリー・ファイルの名前の作成に使用されます。 パイプラインが呼び出す実際のライブラリー・ファイルに使用されている大/小文字と一致させることをお勧めします。これは、一部のシステムが大/小文字を区別するためです。この名前には、OS により接頭部または接尾部またはその両方に EAS が付きます。
「バージョン (Version)」	はい	このフィールドは、ソフトウェア・ライブラリーのバージョン番号の追跡に使用されます。

7. 「保存 (Save)」をクリックします。

タスクの結果

「プラグイン (Plugin)」タブに、更新されたプラグイン名と関連情報が表示されます。

IBM InfoSphere Identity Insight 用のカスタム・スコアリング・プラグインの開発

IBM InfoSphere Identity Insight では、カスタム・スコアリング・プラグインを作成して、さらに多くのタイプの属性データをエンティティー解決処理に組み込むことができます。

IBM InfoSphere Identity Insight 用のスコアリング・プラグインを作成するには、いくつかの基本エレメントを組み込んで、共有ライブラリーを作成する必要があります。カスタム・プラグインは、ライブラリー・ロード・パスに指定されているディレクトリーにインストールする必要があります。

スコアリング・プラグイン開発インターフェース

カスタム・スコアリング・プラグインには、標準インターフェースが必要です。

プリミティブ・オブジェクトを使用して、ライブラリーのバージョンやコンパイラーのオプションへの依存を排除します。これにより、パイプライン側でライブラリーやコンパイラーのバージョンあるいはその他のオプションが変更になった場合でも、プラグインを再ビルドすることなく、プラグインを複数のパイプライン・バージョンで使用できるようになります。以下の、C または C++ のインターフェース・プロトタイプを組み込む必要があります。

```
#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

カスタム・スコアリング・プラグインには、getVersion 関数が必要です。

例

次のコードを含める必要があります。

```
const char *getVersion();
```

return char * には、プラグインのバージョンを記述するヌル終了ストリングが含まれます。

プラグインのバージョン番号を静的ストリングに保管することによってこの関数を実装し、ポインターをストリングのベースポインターに返します。

myPlugin.h には次のコードが含まれます。

```
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

カスタム・スコアリング・プラグインには、initPlugin 関数が必要です。

例

initPlugin は、スコアリング用に必要となる構成情報をプラグインがロードおよび保存できるようにします。データベース接続ストリングと .ini ファイル名は、**configInfo** ストリングに含めます。initPlugin は、プラグインを使用する属性タイプごとに一度呼び出されます。これらは共有オブジェクトです。複数の属性タイプに対してプラグインの使用をサポートするには、属性タイプごとに構成情報を保存する必要があります。このようにすることで、スコアが呼び出されたときに、スコアが適切な属性タイプの構成情報をルックアップできるようになります。

```
const int initPlugin(const char *configInfo,
                     const uint configSize,
                     char *errorStr,
                     const uint maxStrSize);
```

configSize

configInfo に含まれているストリングの長さです。エラーは次のような形式になります。

errorStr

ヌル終了ストリングをコピーするための、事前割り振りされたメモリー・バッファーです。このストリングには、初期化エラーがある場合にそのエラーを記述する XML が含まれます。エラーは次のような形式になります。

```
<ERROR>error text</ERROR>
```

maxStrSize

errorStr がポイントする事前割り振りされたメモリー・バッファーのサイズです。エラー・ストリングのサイズは、この値を超えることはできません。

以下に、スコア関数の疑似コードの例を示します。

```
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.
}
```

エラーが発生した場合、initPlugin は -1 を返すはずです。

スコア

カスタム・スコアリング・プラグインには、score 関数が必要です。

score には次のパラメーターがあります。

```
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
確定と否定のしきい値が含まれます。これらのしきい値は必須ではありません。

thresholdSize
thresholdStr に含まれるストリングのサイズです。

inboundStr
スコアリング対象のインバウンド・エンティティーからの属性が含まれます。

inboundSize
inboundStr に含まれるストリングのサイズです。

candidateStr
スコアリング対象の候補エンティティーからの属性が含まれているストリングへのポインターです。

candidateSize
candidateStr に含まれるストリングのサイズです。

result スコアリング結果を記述する XML が含まれているヌル終了ストリングをコピーするための、事前割り振りされたメモリー・バッファーです。エラーの場合、結果はエラーの説明になります。この戻りストリングの形式は、次のように定義されます。

```
<SCORE_RESULT>
  <MATCH_SCORE>integer 0-100</MATCH_SCORE>
  <CONFIRMATION>TRUE/FALSE</CONFIRMATION>
</SCORE_RESULT>
```

エラーの場合、結果の形式は以下のとおりです。

```
<ERROR>error text</ERROR>
```

resultSize

result がポイントする事前割り振りされたメモリー・バッファーのサイズです。 result ストリングは、このサイズを超えることはできません。result 文書は極めて小さいものです。したがって、きわめて長いエラー・メッセージになることを除いては、サイズは問題にならないはずです。

以下に、スコア関数の疑似コードの例を示します。

```
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.
}
```

エラーが発生した場合、このスコア関数は -1 を返すはずです。

データ・フォーマット

カスタム・スコアリング・プラグインには、指定のデータ・フォーマットを使用する必要があります。

例

しきい値のデータ・フォーマット

```
<THRESHOLDS>
  <CONFIRMATION_THRESHOLD>string</CONFIRMATION_THRESHOLD>
  <DENY_THRESHOLD>string</DENY_THRESHOLD>
</THRESHOLDS>
```

しきい値は、フリー・フォーム・ストリングです。これらは MATCH_MERGE_ATTR 表からロードされ、プラグインが予期しているフォーマットに準拠している必要があります。フォーマットは、そのプラグインの作成者が定義するもので、プラグインごとに異なっていてもかまいません。

属性のデータ・フォーマット

```
<ATTRIBUTE>
  <ATTR_TYPE_ID>unsigned int</ATTR_TYPE_ID>
  <ATTR_VALUE>string</ATTR_VALUE>
  <ATTR_LARGE_DATA>string</ATTR_LARGE_DATA>
</ATTRIBUTE>
```

ATTR_LARGE_DATA は、属性タイプや ETL 処理によっては、空ストリングにすることができます。ATTR_LARGE_DATA はオプションであり、属性のデータが大きすぎて ATTR_VALUE 列に収まらない場合にのみ使用してください。これについては、UMF が正しく作成され、正しいフィールドが使用されるようにプラグインへの書き込みが可能になるようにするため、システム構成時に判別してください。

ATTR_LARGE_DATA は、XML の有効文字セットに準拠するようにエンコードできます。 Base64 エンコードが推奨されますが、これは ETL プロセスで行われます。プラグインが ATTR_LARGE_DATA 内のデータのエンコード解除を必要とすることがあります。また、ストリングは UTF-8 エンコードになっている必要があります。ストリングが ETL において Base64 エンコードであった場合、この UTF-8 ストリングは ASCII7 ストリングと同一になります。

以下に、スコア関数の疑似コードの例を示します。

```
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.
}
```

エラーが発生した場合、このスコア関数は -1 を返すはずです。

プラグイン・オブジェクトの作成

プラグイン・オブジェクトは共有ライブラリー内に構築する必要があります。

このタスクについて

オブジェクトを共有ライブラリー (Windows では .dll、Linux/UNIX では .so) 内に構築します。すべてのライブラリーを静的にリンクする必要があります。これにより、ライブラリーのバージョンの不一致や未解決記号が発生する可能性を防止できます。

第 6 章 パイプラインの管理

パイプラインは、システムの中核部分です。そこで処理が行われ、エンティティーが解決され、関係が検出され、アラートが生成されます。パイプラインは、データをエンティティー・データベースにロードする基本手段です。パイプラインの管理は継続的な運用タスクであり、このタスクにはパイプラインの構成、パイプラインの開始と停止、パイプラインのモニター、およびパイプラインから他のパイプライン、ノード、または外部システムへのメッセージのルーティングが含まれます。

パイプライン

パイプラインは、名前クレンジングと住所クレンジングおよびそれらの標準化、データ品質管理、およびエンティティー解決を実行するコンポーネントです。またパイプラインでは、システム構成に基づき、関係解決が実行され、アラートが生成されます。

パイプラインでは、次の 3 つの中核処理が実行されます。

- 認識。データの標準化、クレンジング、拡張、および品質チェックを実行することにより、入力データの最適化が行われます。
- 解決。エンティティーの解決が行われます。
- 関連付け。関係の検出とアラートの生成が行われます。

パイプラインは、パイプライン・ノードによりホストされます。

並列処理用のパイプラインを構成できます。これにより、1 つのパイプライン・コマンドで複数の並列パイプライン処理スレッドが生成され、システムで複数のデータ要求を同時に処理できます。この機能は、システム・パフォーマンスの改善、データ処理時間の削減、およびハードウェア・メモリー制約の緩和につながることがあります。

並列パイプライン処理機能は、次の 2 つの場所で構成します。

- グローバルな並行性設定は、構成コンソールの「システム構成」タブの「**パイプラインのデフォルトの並行性 (Pipeline default concurrency)**」パラメーターで制御します。この値により、パイプライン開始コマンドから開始される並列処理スレッドの数が決まります。このパラメーターのデフォルト値は 1 です。すなわち、このパラメーターを編集しない限り、1 つのパイプライン処理スレッドしか開始されません。
- ローカルの並行性設定 (パイプライン・ノード別) は、パイプライン構成ファイルで構成できます。パイプライン・ノード別のパイプライン構成ファイルで並行性パラメーターおよび値を指定すると、その値によりグローバル・システム・パラメーターがオーバーライドされます。そのパイプライン・ノードでパイプライン開始コマンドを発行すると、パイプライン構成ファイルに指定されている数と同じ数の並行パイプライン処理スレッドが開始されます。

パイプライン構成チェック

システムは、パイプラインの構成が有効であることを確認するために、新しいパイプライン処理を開始する前や、実行中の各パイプラインを対象に短い間隔でパイプライン構成チェックを実行します。

パイプライン構成チェック時、システムはパイプラインの構成が有効かどうか判定するために以下のチェックを実行します。

- このパイプラインの構成は、構成コンソールでの構成と同じか？
- パイプラインが使用する各構成テーブルのレコード数は妥当か?
- 特定の構成テーブル内に標準的な値が存在しているか？
- 特定の構成テーブル内に構成 ID と値が設定されているか？

これらの構成チェックに合格しない場合、矛盾の重大度に応じて、システムは、警告をログ・ファイルに記録するか、またはパイプラインを自動的にシャットダウンして (あるいはパイプラインを開始しないで)、エラーをログに記録します。

パイプライン・ノード

パイプライン・ノードは、1 つ以上のパイプライン処理をホストする物理マシンです。

パイプライン・ノードは、パイプライン処理を実行するパイプライン実行可能ファイルをインストールし、開始する場所です。このマシンでホストされるすべてのパイプラインのパイプライン構成ファイルを構成および保持します。システムにより、パイプライン・ノードのログ・ファイルにパイプライン・メッセージが書き込まれます。

パイプライン・ノードにより、製品体系の次のコンポーネントにパイプライン処理が接続されます。

調達プログラム
: 抽出、変換、およびロード (ETL) 処理の一部として、調達プログラムはトランスポートを使用して UMF データを処理のためにパイプラインに送信します。調達プログラムのタイプに適したトランスポート方式を使用して、パイプラインに接続します。例えば、調達プログラムとして UMF ファイル・ユーティリティーを使用する場合、ファイル・トランスポートを使用します。

エンティティー・データベース
: エンティティー・データベースには、エンティティー情報が含まれます。パイプラインは、エンティティー解決および関係解決のために入力レコードを処理しながら、エンティティー情報にアクセスします。パイプラインでエンティティー・データベースにアクセスできるようにするために、パイプライン・ノードには適切なデータベース・クライアントがインストールされ、構成されている必要があります。

キュー
: データを処理のためにパイプラインに送信するトランスポート方式としてキ

ューをシステムで使用する場合、各パイプライン・ノードに適切なメッセージ・キューイング・ソフトウェアをインストールし、構成する必要があります。

住所クレンジング・サーバー
: 住所の追加クレンジングのために、他社の住所クレンジング製品をシステムで使用する場合、その住所クレンジング・サーバーに接続するように各パイプライン・ノードを構成する必要があります。

Web サービス
: HTTP トランスポートを使用して、パイプライン・ノードでのパイプライン処理を Web サービスに接続する必要があります。

パイプラインの開始

パイプラインでデータを受け取って処理するには、前もってパイプラインを開始しておく必要があります。データ・スループットを高めたり、さまざまなタイプのソース・データを処理したりするために、複数のパイプラインを実行するのが一般的です。以下の手順を使用して、パイプラインを開始するか、ダウンしているパイプラインを再始動します。

始める前に

- パイプラインをホストするパイプライン・ノードに、パイプライン実行可能ファイルがインストールされている必要があります。
- 開始するパイプラインに使用するパイプライン構成ファイルが、少なくとも 1 つ構成されている必要があります。使用するパイプライン構成ファイルをパイプライン開始コマンドの一部として指定できます。パイプライン・コマンドの一部として構成ファイルの名前を指定しない場合は、パイプライン構成ファイルがパイプライン・ノード上に置かれている必要があり、そのファイルは、実行可能ファイル (パイプライン名が指定されている) の名前に一致する必要があります。例えば、pipeline.ini です。
- データベース環境変数が設定されている必要があります。環境変数の設定を参照してください。
- スクリプトを使用してパイプラインを開始する場合は、必ず、開始するパイプラインと同じディレクトリーにスクリプトを配置してください。
- *DEFAULT_CONCURRENCY* システム・パラメーターが 1 より大きい値に設定されている場合、またはパイプライン・ノードのパイプライン構成ファイルに *concurrency* パラメーターを構成してある場合は、単一のパイプライン開始コマンドを使用して複数の並列パイプライン処理スレッドを開始することができます。

このタスクについて

パイプラインを開始するには、3 つのステップがあります。

手順

1. 各パイプラインは、そのパイプライン・ノードに対してユニーク名を持っている必要があります。このため、開始するパイプラインと同じ名前で稼働しているパイプラインが他に存在しないようにしてください。(デフォルトのパイプライン

名は pipeline です。) これを確認するために、以下のコマンドをコマンド・プロンプトに入力します。 pipeline -n *pipelinename* -l

ここで、*pipelinename* は新規パイプラインを開始するために使用する名前です。この名前が、構成コンソールに登録されているこのパイプラインの名前に一致することを確認してください。

2. コマンド・プロンプトで、次の形式で適切なパイプライン・コマンドのオプションとパラメーターを指定して、1 つ以上のパイプラインを開始します。

   pipeline -*option parameter*

3. コマンドが機能し、パイプラインが開始され、アクティブであることを確認します。
   a. システムが Microsoft Windows プラットフォームで稼働しており、サービス・パイプライン・オプションを使用している場合は、パイプラインの状況を Microsoft Windows サービスのコントロール・パネルで見ることができます。
   b. システムが UNIX プラットフォームで稼働しており、デーモン・パイプライン・オプションを使用している場合は、次のコマンドを入力して、実行中の処理を確認できます。

      ps -fu *userid*

      ここで、*userid* はパイプラインを開始しているユーザーの ID です。
   c. または、コマンド・プロンプトで、次のコマンドを入力します。

   pipeline -n *pipelinename* -l

   ここで、*pipelinename* は、開始したばかりのパイプラインの名前です。 パイプラインがアクティブである場合、コマンド・プロンプトは Running を返します。

パイプラインの停止

パイプラインを停止することは、パイプラインをアクティブかつデータ処理に対してオープンな状況から、非アクティブかつ入力データに対してクローズされた状況に変更することを意味します。一度に 1 つのパイプラインを手動で停止できます。ホット・フィックスまたはアップグレード・リリースをインストールする場合、またパイプラインをホストするパイプライン・ノードに対して構成変更を加える場合は、システム構成に変更を加えた後に、以下の手順に従ってパイプラインを停止します (その後、構成変更を有効にするためには、パイプラインを再始動します)。

手順

1. 停止しようとしているパイプラインが現在実行中であることを確認します。 これを確認するには、次のように入力します: pipeline -n *pipelinename* -l ここで、*pipelinename* は、停止するパイプラインの名前です。パイプラインがアクティブであれば、コマンド・プロンプトに Running と返されます。
2. コマンド行で、以下のようにパイプライン停止コマンドを入力します。
   pipeline -e -n *pipelinename* ここで、*pipelinename* は、停止するパイプラインの名前です。

注**:** パイプラインのデバッグ・コマンド・オプションを使用してパイプラインを開始していた場合、コマンド行で **Ctrl** + **C** を押してパイプラインを停止できます。

3. コマンドが機能し、パイプラインが停止されたことを確認します。 `pipeline -n pipelinename -l` ここで、*pipelinename* は、停止したばかりのパイプラインの名前です。パイプラインが停止されていれば、コマンド・プロンプトに `Stopped` と返されます。

パイプラインの構成

パイプラインは開始時、パイプライン構成ファイルをチェックして、初期開始変数を入手するほか、入力データを処理するために必要な構成情報も入手します。デフォルトで、パイプラインがパイプライン・ノードにインストールされるとき、システムはデフォルトのパイプライン構成ファイルもインストールします。この構成ファイルは、pipeline.ini という名前で、そのパイプライン・ノード上のすべてのパイプラインがこのファイルを使用できます。ただし、パイプラインがエンティティー・データベースに適切に接続およびアクセスできるように、このデフォルト・ファイルの一部のセクションは、パイプライン・ノード上で実行されるパイプラインにあわせて具体的に構成する必要があります。以下の手順を使用して、パイプライン構成ファイルを構成します。

始める前に

- エンティティー・データベースの正確な名前と、エンティティー・データベースにアクセスするために必要なログイン資格情報がわかっている必要があります。
- システムが外部の住所修正ソフトウェアに接続する場合、住所修正ソフトウェアのホスト・マシンの名前がわかっている必要があるとともに、このソフトウェアに関する適切な設定を選択できなければなりません。
- 構成ファイルの変更を有効にするには、このパイプライン・ノード上の実行中のパイプラインをすべて停止してから、変更を完了した後にパイプラインを再始動してください。

このタスクについて

pipeline.ini 構成ファイルは、標準の ASCII テキスト・ファイルです。任意の ASCII テキスト・エディターを使用してファイルを編集できます。

手順

1. デフォルトの pipeline.ini 構成ファイルのコピーを作成し、元のファイルを安全な場所に保管します。 元のファイルのコピーを保存しておくと、必要な場合、そのファイルに戻すことができます。
2. pipeline.ini 構成ファイルのコピーを任意のテキスト・エディターで開きます。
3. このパイプライン・ノード上で実行されるパイプライン用の適切な構成を反映するように、ファイルを更新します。 通常は、デフォルトのパイプライン構成ファイル内のデフォルト値で適切に対応できます。一般に、入力または更新が必要なのは、[SQL] という見出しの下のデータベース接続情報と、[OAC] セクションの下の住所修正情報 (システムが外部の住所修正ソフトウェアを使用する場合) のみです。

4. 更新したパイプライン構成ファイルを保存します。 このファイルは、パイプラインの実行可能コマンドが置かれているディレクトリーに保存する必要があります。 (そうしない場合には、このパイプライン・ノード上のパイプラインを開始するとき、パイプライン構成ファイルの名前と絶対パス・ロケーションを毎回指定しなければなりません。)

次のタスク

変更を行う前に、このパイプライン・ノード上の実行中のパイプラインをすべて停止した場合は、パイプラインを再始動できます。これらの変更を行う前に、実行中のすべてのパイプラインを停止しなかった場合は、今すぐ停止して再始動する必要があります。実行中のパイプラインは、再始動が完了するまで、パイプライン構成ファイルの変更内容が適用されません。パイプラインを停止せずにパイプライン構成情報を変更すると、パイプライン構成ファイルの正しくない値が原因で、パイプラインのシャットダウンなどパイプライン・エラーが発生するおそれがあります。

パイプラインの登録

パイプラインの状況をモニターしたり、パイプラインの結果をルーティングしたりするには、まず、構成コンソールでパイプラインを登録する必要があります。パイプラインの登録は、パイプラインのインストールまたは構成とは異なります。登録とは、構成コンソールで「パイプライン **(Pipelines)**」タブにパイプラインを追加することを指します。

システムは、「パイプライン **(Pipelines)**」タブに登録されている情報を使用して、パイプラインを一意的に識別します。アプリケーション・モニターはこの情報を使用して、モニター対象のパイプラインの状況と統計を報告したり、パイプラインとその他のシステム間の通信や結果をルーティングしたりします。パイプラインを開始するときは、パイプラインの名前として登録した名前と正確に一致する名前 (大/小文字も含めて) を使用しなければなりません。別の名前を使用した場合、または登録済みパイプラインの大/小文字と一致しない場合、アプリケーション・モニターはパイプラインを認識せず、ルーティングもモニターも行いません。

「パイプライン **(Pipelines)**」タブでパイプラインを登録した後は、「ルーティング **(Routing)**」タブでパイプラインのルーティング・ルールを構成したり、「パイプラインの状況 **(Pipeline Status)**」タブからパイプラインの状況や統計をモニターしたりできます。パイプラインの状況や統計をモニターするためには、パイプラインの登録時に、システムを使用してそのパイプラインをモニターする必要があることを指示しなければなりません。

パイプラインの登録後に、登録済みの名前を編集することはできません。ただし、パイプラインに関するその他の情報は更新できます。例えば、パイプライン・ノードの名前を変更する場合や、パイプラインの状況や統計のモニターを開始する必要が生じた場合、それらの情報を編集できます。

パイプラインの登録

パイプラインを登録する理由は 3 つあります。アプリケーション・モニターを使用してパイプラインの状況と統計をモニターする、パイプラインのルーティング・ル

ールを構成する、またはその両方の 3 つです。まったく新しいパイプラインを追加で登録することも、既存の登録済みパイプラインをベースに登録することもできます。

始める前に

パイプラインのユニーク名と、パイプラインをホストしているパイプライン・ノードの名前がわかっている必要があります。登録するパイプラインは、必ずしも事前にパイプライン・ノード上にインストールおよび構成されている必要はありません。(ただし、システムがそのパイプラインをモニターしたり、パイプラインにルーティングするためには、インストールと構成が完了している必要があります。)

このタスクについて

ヒント: すべて同じパイプライン・ノード上で実行される複数のパイプラインを追加する場合、最初のパイプラインを登録し、その後、追加した最初のパイプラインからその他のパイプラインを複製するようにできます。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. 「パイプライン **(Pipelines)**」タブをクリックします。
4. 以下のいずれかのステップを実行します。
   - 新しいパイプラインを登録する場合は、「新規 **(New)**」ボタンをクリックします。
   - 既存のパイプラインをベースにした新しいパイプラインを登録する場合は、「複製 **(Clone)**」ボタンをクリックします。
5. 「一般 **(General)**」タブで、パイプラインのユニーク名、説明、パイプライン・ノード名、およびパイプラインの状況と統計をモニターするかどうかを指定します。

   注**:**
   - ここで入力するパイプライン名と同じ名前を、このパイプラインの開始時に使用しなければなりません。この名前には大/小文字の区別があります。したがって、パイプラインを開始するときは、この登録済みパイプライン名と完全に一致する名前を入力する必要があります。入力内容が完全に一致しない (または大/小文字が一致しない) 場合、このパイプラインに構成されているルーティング・ルールとこのパイプラインのアプリケーション・モニターはいずれも機能しません。
   - 構成コンソールの「パイプラインの状況 **(Pipeline Status)**」タブでこのパイプラインの状況と統計をモニターする必要がある場合、「モニター対象 **(Monitored)**」フィールドで「はい **(Yes)**」を選択してください。
6. 「保存 **(Save)**」ボタンをクリックします。

次のタスク

パイプラインが正常に追加された場合は、画面の左側にあるリストに表示されます。これで、このパイプラインのルーティング・ルールをセットアップしたり、シ

ステムを使用してパイプラインをモニターしたりできます。ただし、パイプラインへのルーティングやパイプラインのモニターを正常に行うには、「パイプライン名 **(Pipeline Name)**」フィールドに登録された名前と大/小文字も含めて完全に同じ名前を使用してパイプラインを開始する必要がある点に留意してください。

登録済みパイプラインの詳細の表示

構成コンソールに登録されているパイプラインの詳細を表示して、登録情報が最新であることを確認できます。システムがパイプラインのパフォーマンスと統計をモニターしたり、パイプラインにルーティングしたり、あるいはその両方をできるようにするために、パイプラインを登録します。

始める前に

- パイプラインが、構成コンソールに登録されている必要があります。

手順

1. 「状況 **(Status)**」ボタンをクリックします。
2.
3. 「概要 **(Overview)**」タブをクリックします。
4. パイプラインの登録名をクリックします。

タスクの結果

「詳細」ウィンドウで、選択したパイプラインの詳細を確認します。

パイプライン登録の編集

パイプライン・ノードの名前など、パイプライン登録のキー・コンポーネントに変更があるときは、登録済みパイプラインに関する情報を編集します。変更することができない情報は、パイプラインの登録名のみです。パイプラインの登録済みの名前を変更する必要がある場合は、パイプライン登録を削除してから正しい情報を使用して追加しなおすか、別のパイプライン登録を追加してください。

このタスクについて

編集対象のパイプラインがアクティブ (現在実行中) の場合、登録内容を編集する前に、パイプラインを停止することをお勧めします。モニター状況を変更する場合は特にそうです。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. 「パイプライン **(Pipelines)**」タブをクリックします。
4. 編集するパイプラインを選択してから、「編集」ボタンをクリックします。
5. 情報を変更します。

   注**:** パイプラインの状況と統計を「パイプラインの状況 **(Pipeline Status)**」タブでモニターするには、「モニター対象 **(Monitored)**」フィールドを「はい **(Yes)**」に設定する必要がある点に注意してください。

6. 「保存 **(Save)**」ボタンをクリックします。

タスクの結果

「パイプライン **(Pipelines)**」タブで変更を表示できます。

次のタスク

パイプラインを停止していた場合、再始動します。

パイプライン登録の削除

構成コンソールでパイプライン登録を削除しても、システムからパイプラインが物理的に削除されるわけではありません。ここでは、「パイプライン **(Pipelines)**」タブ、「ルーティング・ルール **(Routing Rules)**」タブ、および「パイプラインの状況 **(Pipeline Status)**」タブからパイプラインを削除します。登録が削除されると、ルーティング・ルールを使用して情報をルーティングしたり、状況や統計のモニター情報を提供したりすることはできなくなります。登録済みパイプライン名を編集することはできません。登録済みパイプラインの名前を変更する必要がある場合は、パイプライン登録を削除してから正しい情報を使用して追加しなおすか、別のパイプライン登録を追加してください。

このタスクについて

削除対象のパイプラインがアクティブ (現在実行中) であり、「パイプラインの状況 **(Pipeline Status)**」タブでシステムによってモニターされている場合、削除する前にパイプラインを停止することをお勧めします。また、「ルーティング・ルール **(Routing Rules)**」タブを確認して、このパイプラインに関連付けられているルーティング・ルールが存在するかどうかを調べることもお勧めします。存在する場合は、このパイプラインを削除する前に、それらのルーティング・ルールを別のパイプラインにルーティングしなおすか、それらのルーティング・ルールを使用する新しいパイプラインを追加してください。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「一般 **(General)**」ボタンをクリックします。
3. 「ノード **(Nodes)**」タブをクリックします。
4. 削除するパイプライン (複数可) を選択してから、「削除 **(Delete)**」ボタンをクリックします。

次のタスク

削除したパイプラインは、「ノード **(Nodes)**」タブにも「ルーティング・ルール **(Routing Rules)**」タブにも表示されなくなります。削除されたパイプラインからは、「パイプラインの状況 **(Pipeline Status)**」タブに状況は報告されません。システムは、削除されたパイプラインに「ルーティング・ルール **(Routing Rules)**」タブで割り当てられていたいずれのルーティング・ルールのルーティングも行わなくなります。

ヘルプ・トピック

「パイプライン (Pipelines)」タブ

「パイプライン **(Pipelines)**」タブを使用して、パイプラインを登録したり、登録済みパイプラインを編集、削除、または表示したりします。このタブでパイプラインが登録され、登録済みパイプラインを実行するパイプライン・ノード上に SNMP エージェントがインストールされ、構成されていると、「状況 **(Status)**」タブでパイプラインの状況、統計、およびパフォーマンスを確認できます。また、「ルーティング・ルール **(Routing Rules)**」タブを使用して、登録済みパイプラインからその他のデータベースや外部システム宛ての結果を構成し、ルーティングできます。

「パイプライン名 **(Pipeline Name)**」
: 構成コンソールでアプリケーション・モニターの対象として登録されている各ノードの名前がアルファベット順でリストされます。

説明
: このノードをさらに詳しく記述し、他のシステム・ノードと区別するのに役立つ追加テキストを指定します。

ホスト名
: このパイプラインをホストするパイプライン・ノードの名前が表示されます。(このパイプラインをモニターする計画がある場合、これは SNMP エージェントをインストールして実行する必要があるサーバーでもあります。)

「モニター対象 **(Monitored)**」
: このパイプラインの状況と統計がモニターされていて、「状況 **(Status)**」タブにそれが報告されるかどうかが表示されます。(これは、パイプラインの現在の状況を示しているわけではありません。この列は、このパイプラインが現在どのように登録されているかを示しています。)

  - 「はい (Yes)」は、この登録済みパイプラインがアプリケーション・モニターによってモニターされていることを示します。
  - 「いいえ (No)」は、このパイプラインがアプリケーション・モニターの対象として構成されていないことを示します。ただし、ルーティングは構成されている場合があります。

「パイプライン - 詳細 (Pipelines - detail)」タブ

このタブを使用して、パイプラインを登録したり、既存の登録済みパイプラインの詳細を表示したりします。「ルーティング **(Routing)**」タブでパイプラインのルーティング・ルールを構成したり、「状況 **(Status)**」タブでパイプラインの統計や状況をモニターしたりするためには、まずパイプラインを登録する必要があります。

パイプラインを正常に登録するためには、このタブ上のすべてのフィールドが必要です。パイプラインの登録後、パイプラインの名前を除いてすべてを変更することができます。例えば、パイプライン・ノードの名前 (「ホスト名」フィールド) を変更する必要があれば、その名前を編集します。ただし、パイプラインの名前を変更する必要がある場合は、まず、ここで登録済みの正しくないパイプライン名を削除し、次に正しい情報を使用してパイプラインを追加しなおしてください。

「パイプライン名 **(Pipeline name)**」
: パイプラインのユニーク名を 15 文字以内で入力します。パイプラインをモニターする場合、またはそのパイプラインをルーティング先またはルーティ

ング元にする場合、パイプラインの開始時に指定する名前は、この登録済みパイプライン名と大/小文字も含めて正確に一致しなければなりません。

左側のリストには、既に登録されているすべてのパイプラインの名前が表示されます。

説明　他のパイプラインと区別するためのパイプラインの説明を 50 文字以内で入力します。例えば、説明を使用して、システムの用途、またはシステムが処理するデータ・ソースのタイプを示します。

ホスト名
このパイプラインを実行するパイプライン・ノードの名前を入力します。

「モニター対象 **(Monitored)**」
アプリケーション・モニターでこのパイプラインの状況を報告するかどうかを選択します。

- 「はい **(Yes)**」は、このパイプラインの状況および統計をモニターする必要があることを示します。このパイプラインが構成コンソールで適切に登録されていて、パイプライン・ノード上で SNMP エージェントが実行されていれば、このパイプラインの状況と統計が「状況 **(Status)**」タブに表示されます。
- 「いいえ **(No)**」は、このパイプラインをルーティングのために登録する必要があり、モニター対象にはしないことを示します。「状況 **(Status)**」タブには、このパイプラインの状況も統計も表示されません。ただし、登録済みパイプラインのルーティング・ルールは構成できます。

ルーティング・ルールの構成

ルーティング・ルールを使用すると、パイプライン処理または調達プログラムの結果をデータベース、パイプライン、または外部システムにルーティングできます。ルーティング・ルールの構成は構成コンソールの「ルーティング・ルール **(Routing Rules)**」タブで行います。ただし、ルーティング元は、アプリケーション・モニターに登録が完了しているパイプラインまたは調達プログラムでなければなりません。新規ルーティング・ルールを最初から構成することも、既存のルーティング・ルールをベースに構成することもできます。

始める前に

- ルーティング元になるパイプラインまたは調達プログラムがアプリケーション・モニターに登録されている必要があります。
- パイプラインまたは調達プログラムを登録するときに使用された正確なユニーク名がわかっている必要があります。
- 宛先にルーティングするために使用するトランスポート方式と、使用する必要がある特定のトランスポート URI 構文がわかっている必要があります。

手順

1. 「セットアップ **(Setup)**」タブをクリックします。
2. 「一般 **(General)**」タブをクリックします。
3. 「ルーティング・ルール **(Routing Rules)**」タブをクリックします。

4. 以下のいずれかを実行します。
   - 新規ルーティング・ルールを構成する場合は、「新規 **(New)**」ボタンをクリックします。
   - 既存のルーティング・ルールをベースにした新しいルーティング・ルールを構成する場合は、新しいルールのベースとなるルーティング・ルールの横のチェック・ボックスを選択し、「複製 **(Clone)**」ボタンをクリックします。
5. 必須: 「元のパイプライン **(From Pipeline)**」フィールドで、ルーティング元のパイプラインまたはアプリケーション・プログラムの登録名を入力します。入力する名前は、「パイプライン **(Pipelines)**」タブで登録した名前と完全に一致しなければなりません。
6. 必須: 「順序 **(Order)**」フィールドで、システムがこのルーティング・ルールを使用する順序を表す 0 から 999 までの数値を入力します。 システムはこのフィールドをデフォルトで 0 に設定します。これは、いずれのパイプラインまたは調達プログラムに対しても、処理される最初のルーティング・ルールになります。このフィールドの数値は、このパイプラインまたは調達プログラムに対してユニークでなければなりません。パイプラインまたは調達プログラムに対して既に構成されているルーティング・ルールが複数ある場合は、特に注意が必要です。

   注**:** このタブの左側のペインで、既存のルーティング・ルールが構成されているパイプラインまたは調達プログラムのリストを参照してください。このパイプラインまたはノードがリストに表示されている場合、パイプラインまたは調達プログラムの名前の後のコロンに続く一番大きい数字を探し、その数字の次に大きい数字を入力してください。例えば、PIPE08 用の新しいルーティング・ルールを構成している場合に、左側のペインのリストに PIPE08:0 と表示されていれば、「順序 (Order)」フィールドに 1 以上の数値を入力する必要があります。
7. 必須: 「宛先 **(Destination)**」フィールドに、ルーティングされる情報の宛先のトランスポート URI を入力します。これで、意図したパイプライン、データベース、または外部システムの宛先にルーティングする方法をシステムに通知します。

   注**:** ルーティングが成功するには、指定されたものと同じトランスポート URI を使用して、宛先のプロセスにアクセスできなければなりません。例えば、宛先がパイプラインの場合は、同じトランスポート URI を使用してパイプラインが開始される必要があります。
8. 必須: 「文書 **(Document)**」ドロップダウン・リストで、宛先にルーティングするメッセージ・タイプを表す UMF 文書タイプを選択します。
9. オプション: 「ルート・フィルター **(Route Filter)**」フィールドに、ルーティングされる情報に適用するフィルターを入力し、システムが特定の情報のみを宛先にルーティングできるようにします。 フィルターは、ルーティング・ルールの拡張機能です。フィルター演算式 `MODDIST(`*`UMF_tag_name`* を入力します。ここで、(*`UMF_tag_name`* は、システムがレコードを配布するために使用する UMF タグの名前を示します。
10. 必須: 「有効 **(Enabled)**」ドロップダウン・リストで、「はい **(Yes)**」を選択して、このルーティング・ルールを有効にします。
11. 必須: 「保存 **(Save)**」ボタンをクリックします。

例

次のタスク

パイプラインまたは調達プログラムの名前が、ここで構成したルーティング・ルールの詳細とともに「ルーティング・ルール **(Routing Rules)**」タブに表示されます。システムは、構成されたルーティング・ルールを使用して、パイプラインまたは調達プログラムから宛先への情報のルーティングを開始します。

ルーティング・ルール

ルーティング・ルールにより、アプリケーション・モニターに対して、調達プログラムからパイプラインへのメッセージ送信、またはパイプラインからデータベースや外部システムへのメッセージ送信を指示します。ルーティング・ルールは、アプリケーション・モニターに登録されているパイプラインのみに構成できます。ただし、結果は、適切なトランスポートの Universal Resource Indicator (URI) 構文を使用して任意の宛先にルーティングできます。

ルーティング・ルールには、以下のような一般的な使用法を含め、多くの用途があります。

- データ処理のために行われる調達プログラム (UMF データベース・ユーティリティーなど) から複数のパイプラインへのデータ・ロードのバランスを取る。
- 追加調査またはレポート作成の目的で、外部システムまたはレポート・データベースにパイプライン処理の結果 (アラートなど) を送信する。

UMF 文書とルーティング・ルール

ルーティング・ルールは、1 つ以上の UMF 文書タイプを使用してメッセージをルーティングするために構成されます。何を選択するかは、ルーティング元のパイプラインまたはシステム・ノードから結果として生成される情報に応じて変わります。例えば、UMF_ALERT は、パイプライン経由でアイデンティティー・レコードやエンティティー・レコードを処理することで生成されるアラートを表す UMF 文書タイプです。特定のパイプラインから生成されるアラートを、例えば、システムによって生成されたアラートを調査するアナリストが使用するユーザー・インターフェースなど、外部システムにすべてルーティングするようにできます。

システムに構成されている任意のカスタム UMF 文書タイプを含め、すべての UMF 文書タイプまたは特定の UMF 文書タイプをルーティングするルーティング・ルールを構成できます。

フィルター

ルーティング・ルールの構成時にフィルター演算式を指定することで、宛先にルーティングされる情報をフィルタリングできます。フィルターによって、特定の情報のみを宛先にルーティングすることを指定します。

ルーティング・フィルターを構成するときは MODDIST(*UMF_tag_name*) 式を使用します。ここで、各指定項目は次のとおりです。

MODDIST
: モジュラス式配布を示す式です。

(*UMF_tag_name***)**
レコードの配布方法をシステムに指示する UMF タグを識別します。システムは識別された UMF タグを使用して、そのタグに含まれるすべての文字の ASCII 値を合計してデータ処理の負荷のバランスを取るために必要なルートの数を判定します。

データ・ソース・コード「datasource5」からのすべてのレコードを別のレポート・データベースにルーティングする必要があるとします。この場合、フィルター演算式 `MODDIST(datasource5)` を使用してルーティング・ルールを構成できます。ここで、`datasource5` はデータ・ソース・コードです。

ルーティング処理

パイプラインまたは調達プログラムにルーティング・ルールが構成されている場合に、アプリケーション・モニターによってルーティング処理がどのように実行されるかを以下に説明します。

1. パイプラインまたは調達プログラムが開始されると、それらは UMF メッセージを使用してアプリケーション・モニターに要求を送信します。
2. アプリケーション・モニターは要求を受け取ると、すべてのアクティブなルーティング・ルールの中から、要求側パイプラインまたは調達プログラムに関連したものを探します。
3. アプリケーション・モニターは、要求側パイプラインまたは調達プログラムに対応するアクティブなルーティング・ルールを見つけると、ルーティング指示を含んだ UMF 文書を作成し、その UMF 文書を要求側パイプラインまたは調達プログラムに返信します。
4. 要求側パイプラインまたは調達プログラムは UMF 文書メッセージを解釈し、ファイル拡張子 *.RTE (* は要求側パイプラインまたは調達プログラムの名前) を持つルーティング・ファイルを作成します。パイプラインまたは調達プログラムは、開始時にアプリケーション・モニターと通信できない場合、ルーティング・ファイルでルーティング指示を探します。
5. 要求側パイプラインまたは調達プログラムは、ルーティング・ルールに構成されている宛先と通信するために必要なトランスポートを開きます。
   - パイプラインまたは調達プログラムは、正常にトランスポートを開いて、宛先を見つけることができた場合、宛先が開始済みでアクティブにデータを処理していれば、適切な UMF 文書メッセージを宛先にルーティングします。
   - パイプラインまたは調達プログラムがトランスポートを開くことができない場合、または宛先が見つからない場合、パイプラインまたは調達プログラムはエラーで停止します。

ヘルプ・トピック

「ルーティング・ルール (Routing Rules)」タブ

このタブを使用して、「パイプライン **(Pipelines)**」タブで登録完了しているパイプラインの既存のルーティング・ルールを表示または削除したり、新規ルーティング・ルールを構成したりします。いったん構成されたルーティング・ルールは、削除のみが可能で、編集することはできません。

「元のパイプライン **(From Pipeline)**」
ルーティング・ルールが構成されるパイプラインの名前が表示されます。

「順序 **(Order)**」
「元のパイプライン **(From Pipeline)**」列のパイプラインでこのルーティング・ルールが処理される順序が表示されます。ルーティング・ルールが複数ある場合、順序は便利です。多くの場合、順序は 0 に設定されます。

「宛先 **(Destination)**」
受信側パイプライン、データベース、または外部システムのトランスポート URI が表示されます。

「文書タイプ **(Document type)**」
このルーティング・ルールが送信する UMF 文書タイプが表示されます。これは、「元のパイプライン **(From Pipeline)**」列のパイプラインによって処理される結果の文書タイプです。この選択項目は、特定の UMF 文書タイプか * (アスタリスク) にすることができます。アスタリスクは、このルーティング・ルールがすべての UMF 文書タイプをルーティングすることを示します。

「有効 **(Enabled)**」
このルーティング・ルールがアクティブかそうでないかを示します。

- 「はい **(Yes)**」は、ルーティング・ルールが有効なことを示します。「元のパイプライン **(From Pipeline)**」列に表示されるパイプラインまたはノードが、指定された文書タイプの結果を処理するとき、システムは、その UMF 文書タイプに関連付けられたデータを「宛先 **(Destination)**」列に示されている宛先に必ずルーティングします。
- 「いいえ **(No)**」は、ルーティング・ルールが有効でないことを示します。

「ルーティング・ルール - 詳細 (Routing Rules - detail)」タブ

このタブを使用して、新しいルーティング・ルールを構成したり、既存のルーティング・ルールの詳細を表示したりします。ルーティング・ルールは、一般に、処理された特定タイプの結果をパイプラインから他のデータベースや外部システムに公開するために構成されます。「パイプライン **(Pipelines)**」タブで登録済みのパイプラインに対してのみルーティング・ルールを構成できます。

新規ルーティング・ルールを正常に構成するために、「ルート・フィルター **(Route Filter)**」フィールドを除くすべてのフィールドが必須です。いったん構成されたルーティング・ルールは、編集できません。ルーティング・ルールを変更する必要がある場合は、削除してから、正しい情報を使用して追加しなおしてください。

「元のパイプライン **(From Pipeline)**」
結果をルーティングする元のパイプラインのユニーク名を入力します。このパイプラインの名前は、「パイプライン **(Pipelines)**」タブで登録された名前と正確に一致しなければならず、名前には大/小文字の区別があります。名前が一致しない場合、システムによって、指定されたパイプラインが存在しないことを示すエラー・メッセージが表示されます。

「順序 **(Order)**」
システムが、「元のパイプライン **(From Pipeline)**」フィールドに含まれる登録済みパイプラインにこのルーティング・ルールを適用する順序を示す 0

から 999 までの数値を入力します。このフィールドのデフォルトは 0 であり、システムがこのルーティング・ルールを最初に処理することを示します。このパイプラインに 1 つ以上のルーティング・ルールが既に構成されている場合、最大順序番号より大きい数値を入力します。

左側のペインで、このパイプラインに既に構成されている既存のルーティング・ルールの順序設定を確認します。この順序は、パイプライン名の後のコロンに続くシーケンス番号によって示されます。(例えば、PIPE08:0 は、パイプライン PIPE08 にルーティング・ルールが 1 つ既に構成されており、それは現在最初に処理されるように設定されていることを示しています。PIPE08 に新しいルーティング・ルールを構成する場合、順序を 1 に設定します。)

「宛先 **(Destination)**」
処理された結果をルーティングする宛先のパイプライン、データベース、または外部システムのトランスポート URI を入力します。使用するトランスポートのタイプに応じた適切な構文を使用してください。

「文書タイプ **(Document Type)**」ドロップダウン・リスト
ドロップダウン・リストから、登録済みパイプラインから宛先にルーティングする UMF 文書タイプを選択します。処理されたすべての結果を宛先にルーティングする場合は、アスタリスク文字 * を選択してください。

「ルート・フィルター **(Route Filter)**」
特定の情報のみを宛先にルーティングするように指定する必要がある場合、このルーティング・ルールでルーティングする UMF 値をフィルタリングするためにシステムが使用する式を入力します。(例えば、特定のデータ・ソースからのアイデンティティー・レコードまたはエンティティー・レコードのみをルーティングする場合、DSRC_CODE=x というフィルターを入力できます。ここで、*x* は、フィルタリングするデータ・ソースのユニーク・データ・ソース・コードです。)

フィルターは、ルーティング・ルールの拡張機能です。

「有効 **(Enabled)**」ドロップダウン・リスト
ドロップダウン・リストからオプションを選択します。

- 「はい **(Yes)**」は、アプリケーション・モニターがこのルーティング・ルールに従って、パイプラインから宛先に情報をルーティングすることを意味します。
- 「いいえ **(No)**」は、アプリケーション・モニターがパイプラインから情報をルーティングするにあたって、このルーティング・ルールに従わないことを意味します。

ルーティング・ルールの削除

いったん構成されたルーティング・ルールは、編集できません。情報を訂正または更新する必要がある場合、古いルーティング・ルールを削除し、新しいものを構成する必要があります。また、不要になったルーティング・ルールや使用されなくなったルーティング・ルールも削除する必要があります。構成コンソールの「ルーティング・ルール **(Routing Rules)**」タブで、1 つ以上の構成済みルーティング・ルールを削除できます。

手順

1. 「セットアップ **(Setup)**」タブをクリックします。
2. 「一般 **(General)**」タブをクリックします。
3. 「ルーティング・ルール **(Routing Rules)**」タブをクリックします。
4. 削除する各構成済みルーティング・ルールの横にあるチェック・ボックスを選択します。
5. 「削除 **(Delete)**」ボタンをクリックします。

次のタスク

システムによって、選択済みルーティング・ルールが削除され、削除されたルーティング・ルールは情報のルーティングに使用されなくなります。

パイプラインの状況および統計

状況、統計、およびパフォーマンスをモニターすることは、パイプラインを継続的に実行し、パイプラインのデータ・ロードのバランスを取り、問題が発生する前の潜在的なパイプラインの問題を見つけるうえで重要になります。

パイプラインに関する状況や統計を表示するには、まず以下が正常に完了している必要があります。

1. パイプラインがパイプライン・ノードにインストールされ、構成されている。

注**:** (Windows プラットフォームのみ) パイプラインをサービスとして開始している場合、他の場所には表示されない追加の状況情報を Windows の「イベント ビューア」で表示できます。

状況および統計の情報

パイプラインがデータの処理を開始すると、以下のように、構成コンソールで UMF 例外情報を確認できます。

- UMF 例外 (「**UMF 例外 (UMF Exceptions)**」タブ)

SNMP エージェント

Simple Network Management Protocol (SNMP) は、システムおよびネットワーク・デバイスのモニターに使用される標準プロトコルです。SNMP エージェントは、システム内の各登録済みパイプラインに状況と統計を定期的に要求します。SNMP エージェントが各登録済みパイプラインに関して収集した情報は、「パイプラインの状況 **(Pipeline Status)**」タブに表示されます。

SNMP エージェントがパイプラインをモニターするためには、以下の前提条件があります。

- SNMP エージェントが、モニター対象のパイプラインを実行しているパイプライン・ノード上にインストールされ、構成されている必要があります。
- モニターする必要がある各パイプラインが、構成コンソールで登録済みであり、モニター対象として構成されている必要があります。
- SNMP エージェントが、パイプライン・インストール時に構成されたポート番号と同じポート番号を使用して、パイプライン・ノード上で開始され、実行されて

いる必要があります。この SNMP エージェント・ポート番号は、パイプライン・ノードごとではなく、システム全体での番号です。デフォルトの SNMP ポート番号は 13516 ですが、各パイプライン・ノード上にある server.xml ファイル内で、構成されている SNMP エージェント・ポート番号を見つけることができます。

SNMP エージェントはサービスであり、必要に応じて停止したり開始したりできます。

SNMP エージェントの使用例

ABC 社は、アプリケーション・モニターを使用して同社のすべてのパイプラインをモニターしています。ここに、Pipeline300、Pipeline310、および Pipeline320 の 3 つの新しいパイプラインをホストする別のパイプライン・ノード (EAS-2) を追加します。これらのパイプラインをモニターするために、ABC 社のオペレーターは、以下のタスクを実行する必要があります。

- パイプライン・ノード EAS-2 上に 1 つの SNMP エージェントをインストールして構成します。
- 構成コンソールの「パイプライン **(Pipelines)**」タブで、新しい各パイプライン (Pipeline300、Pipeline310、および Pipeline320) を登録します。
- パイプライン・ノード EAS-2 上の SNMP エージェントを開始します。SNMP エージェントが使用するポート番号は、このパイプライン・ノードにパイプラインをインストールするときに構成した、システム全体向けのポート番号にしてください。
- 登録済みの各パイプラインを処理のために開始します。登録済みのパイプライン名には大/小文字の区別があるため、パイプラインに登録された正確な名前を入力してください。

これで新しいパイプラインが実行中になると、ABC 社のオペレーターは、構成コンソールを使用してパイプラインの状況と統計をモニターできます。

SNMP エージェントの開始

構成コンソールで、1 つ以上のパイプラインの状況および統計をモニターするには、それらのパイプラインが稼働しているパイプライン・ノード上で SNMP エージェントを開始する必要があります。

始める前に

- SNMP エージェントが、パイプラインを実行しているパイプライン・ノード上にインストールされ、構成されている必要があります。
- パイプラインが、構成コンソールの「パイプライン **(Pipelines)**」タブに登録されており、モニター対象として構成されている必要があります。

手順

1. パイプライン・ノードのコマンド行から **Change directory** コマンドを使用してホーム・ディレクトリーに移動します。

2. 次のコマンドを入力します: **java -jar SNMPAgent**-p *port number* ここで、*port number* は、SNMP エージェントに必要な、パイプライン・インストール時に構成されたシステム全体向けのポート番号です。デフォルトのポート番号の値は 13516 です。

   注**:** パイプライン・ノード上の server.xml ファイル内で、構成されている SNMP エージェント・ポート番号を見つけることができます。

タスクの結果

SNMP エージェントが開始されます。

次のタスク

構成コンソールで、「パイプラインの状況 **(Pipeline Status)**」タブを選択して、SNMP エージェントが稼働していることを確認します。稼働している場合、SNMP エージェントによって、このパイプライン・ノード上で実行中のすべてのパイプラインに関する状況と統計が報告されます。.SHM ファイルが同じディレクトリー内にある限り (通常、これは SNMP エージェントが開始されるディレクトリーです)、さらにパイプラインを追加した場合でも SNMP エージェントを再始動する必要はありません。

SNMP エージェントの停止

構成の更新など、パイプライン・ノードに変更を加える必要がある場合、必ずパイプライン・ノード上の SNMP エージェントを停止します。

始める前に

現時点で、SNMP エージェントがパイプライン・ノード上で実行されている必要があります。また、このパイプライン・ノード上に、アプリケーション・モニターによってモニターされている実行中のパイプラインがある場合、それらを停止することをお勧めします。

手順

SNMP エージェントを実行しているウィンドウで、**Ctrl** + **C** キーを押します。

次のタスク

- SNMP エージェントが停止します。
- 構成コンソールの「パイプラインの状況 **(Pipeline Status)**」タブで、このパイプライン・ノード上のすべてのパイプラインに対して STOPPED 状況が表示されます。

構成コンソールでのパイプライン状況の確認

パイプラインがダウンすることは、システムの一部がダウンしていることになるため、パイプラインの現在の状況を把握しておくことが重要になります。構成コンソールの「パイプラインの状況 **(Pipeline Status)**」タブで、最新のパイプラインの状況やパフォーマンスの統計をすぐに確認できます。アプリケーション・モニター

は、SNMP エージェントをポーリングして、アクティブな SNMP エージェントから情報を受け取り、「パイプラインの状況 **(Pipeline Status)**」タブを 60 秒ごとに最新表示します。

始める前に

- SNMP エージェントが、モニター対象のパイプラインを実行しているパイプライン・ノード上にインストールされ、構成されている必要があります。
- SNMP エージェントが、パイプライン・インストール時に構成されたシステム全体向けのポート番号を使用して、開始されている必要があります。(この構成済みポート番号は、server.xml ファイル内で確認できます。)
- パイプラインが、構成コンソールの「パイプライン **(Pipelines)**」タブで登録済みで、モニター対象として構成されている必要があります。
- 「パイプライン **(Pipelines)**」タブで登録されたパイプライン名と完全に同じ名前および同じ大/小文字を使用して、パイプラインが開始されている必要があります。

このタスクについて

構成コンソールから状況を表示できない場合は、コマンド行を使用してパイプラインの状況を確認できます。

手順

1. 「状況 **(Status)**」ボタンをクリックします。
2. 「パイプラインの状況 **(Pipeline Status)**」ボタンをクリックします。
3. 「パイプライン名 **(Pipeline Name)**」列を調べて、確認する必要があるパイプラインの名前を見つけます。(パイプラインは名前の英数字順にリストされています。) 次に、そのパイプライン名と同じ行にある状況列やトランザクション統計列の情報を参照してください。

次のタスク

その他のいずれかのボタンをクリックして、このパイプラインに関するその他の情報を表示することもできます。例えば、このパイプラインが最後に開始された時刻を確認するには、「イベント」タブをクリックします。

コマンド行を使用したパイプライン状況の確認

パイプラインがダウンすることは、システムの一部がダウンしていることになるため、パイプラインの現在の状況を把握しておくことが重要になります。構成コンソールの「パイプラインの状況 **(Pipeline Status)**」タブには、60 秒ごとに、システムによる自動ポーリングに基づいた最新のパイプラインの状況と統計が表示されるので、組織の多くはこのタブを使用してパイプラインをチェックします。しかし、ユーザーはコマンド行を使用して、特定のパイプラインまたは特定のパイプライン・ノード上のすべてのパイプラインの状況を確認することもできます。(コマンド行でのチェックには、パイプラインの状況のみが提供されます。パイプラインのパフォーマンス統計は提供されません。)

始める前に

- SNMP エージェントが、パイプラインを実行しているパイプライン・ノード上にインストールされ、構成されている必要があります。
- SNMP エージェントが、パイプライン・インストール時に構成されたポート番号と同じポート番号を使用して、パイプライン・ノード上で開始され、実行されている必要があります。この SNMP エージェント・ポート番号は、パイプライン・ノードごとではなく、システム全体での番号です。デフォルトの SNMP ポート番号は 13516 ですが、各パイプライン・ノード上にある server.xml ファイル内で、構成されている SNMP エージェント・ポート番号を見つけることができます。

手順

1. パイプライン・ノードのコマンド行から、以下のいずれかのステップを実行します。
   - このパイプライン・ノード上のすべてのパイプラインの状況を確認するには、次のコマンド **pipeline -l** を入力します。
   - このパイプライン・ノード上の特定のパイプラインの状況を確認するには、次のコマンド **pipeline -n pipelinename -l** を入力します。

   ここで、*pipelinename* は、確認するパイプラインのユニーク名です。

   注**:** 入力する名前は、パイプラインを開始するときに使用した名前と一致しなければなりません。
2. **Enter** キーを押します。

タスクの結果

システムによって、パイプラインごとに以下のいずれかの状況が返されます。

- Running - 現在アクティブな各パイプラインが対象。
- Stopped - 現在非アクティブな各パイプラインが対象。

例

例えば、pipeline08 の状況を確認するには、次のコマンド **pipeline -n pipeline08 -l** を入力します。

次のタスク

パイプラインの状況が予期せず Stopped とリストされた場合、トラブルシューティングのトピックを使用して理由を判別してください。

アプリケーション・モニター・イベントの表示

アプリケーション・モニターと、構成コンソールの「パイプライン **(Pipelines)**」タブに登録済みのパイプラインの間でメッセージが交換されると、必ずアプリケーション・モニター・イベントが発生します。これらのメッセージには、パイプラインの開始または停止から、システムがエラーまたは警告をログに記録したことまで (ただし、Universal Message Format (UMF) 例外は除きます) 幅広い情報が含まれます。このような情報は、特定のパイプラインで発生したエラーをトラブルシューティングするのに役立ちます。

始める前に

- パイプラインが、構成コンソールの「パイプライン **(Pipelines)**」タブに登録されている必要があります。
- 「パイプライン **(Pipelines)**」タブに表示される登録済みパイプライン名と同じ名前を使用して、「パイプライン **(Pipelines)**」タブに登録されているパイプライン・ノード上でパイプラインが開始されている必要があります。

このタスクについて

パイプラインが構成コンソールの「パイプライン **(Pipelines)**」タブに登録されている場合、構成コンソールの「イベント」タブで現在または過去のイベントを表示できます。

手順

1. 「状況 **(Status)**」ボタンをクリックします。
2. 「イベント」ボタンをクリックします。
3. オプション: 「開始日 **(From Date)**」フィールドに、表示するアプリケーション・モニター・イベントの開始日を mm/dd/yyyy 形式で入力します。 このフィールドをブランクのままにした場合、システムは、指定されたその他の基準を満たす、システムが作動可能になった最初の日からのアプリケーション・モニター・イベントをすべて表示します。このフィールドに日付を入力する場合でも、「終了日 **(Thru Date)**」フィールドには必ずしも日付を入力する必要はありません。
4. オプション: 「終了日 **(Thru Date)**」 フィールドに、表示するアプリケーション・モニター・イベントの終了日を mm/dd/yyyy 形式で入力します。 このフィールドをブランクのままにした場合、システムは、指定されたその他の基準を満たす、今日の日付までのアプリケーション・モニター・イベントをすべて表示します。このフィールドに日付を入力する場合でも、「開始日 **(From Date)**」フィールドには必ずしも日付を入力する必要はありません。
5. オプション: 「元のパイプライン **(From Pipeline)**」フィールドに、アプリケーション・モニター・イベントを表示する特定のパイプラインの登録済みの名前を入力します。 このフィールドをブランクのままにした場合、システムは、指定されたその他の基準を満たす、すべてのパイプラインのアプリケーション・モニター・イベントを登録済みの名前別にすべて表示します。
6. オプション: 「最大カウント **(Max Count)**」ドロップダウン・リストから、表示するアプリケーション・モニター・イベントの最大数を選択します。 システムは、指定されたその他の基準をすべて満たすアプリケーション・モニター・イベントをその最大数までの件数、表示します。指定された数よりも多いアプリケーション・モニター・イベントが存在する場合でも、システムはそれらを表示しません。指定されたその他の基準をすべて満たすアプリケーション・モニター・イベントの数が指定された数より少ない場合、すべてのアプリケーション・モニター・イベントが表示されます。
7. 必須: 「検索 **(Search)**」ボタンをクリックします。

例

例えば、pipeline08 で今日発生したアプリケーション・モニター・イベントの最後の 500 件を表示するには、以下のような基準を指定します。

- 「開始日 **(From Date)**」フィールドに、今日の日付を入力します。
- 「終了日 **(Thru Date)**」フィールドに、今日の日付を入力します。
- 「元のパイプライン **(From Pipeline)**」フィールドに、「pipeline08」と入力します。
- 「最大カウント **(Max Count)**」ドロップダウン・リストから「**500**」を選択します。

次のタスク

特定のアプリケーション・モニター・イベントをクリックすると、その詳細を詳しく調べることができます。表示される情報は、イベント発生時にそのイベントに関して報告されたものです。

UMF 例外の表示

UMF 例外は、パイプラインによって処理されている入力データに関する問題を示しています。これは、入力データの構造を解析できない場合に発生します。一般的に、UMF 例外はパイプラインのエラー限界カウントに影響しないため、UMF 例外はシステムによってログに記録され、パイプラインは通常、処理を続行します。この情報は、特定のパイプラインの入力データをトラブルシューティングするのに役立ちます。

始める前に

- パイプラインが、構成コンソールの「パイプライン **(Pipelines)**」タブに登録されている必要があります。
- 「パイプライン **(Pipelines)**」タブに表示される登録済みパイプライン名を使用して、「パイプライン **(Pipelines)**」タブに登録されているパイプライン・ノード上でパイプラインが開始されている必要があります。

このタスクについて

パイプラインが構成コンソールの「パイプライン **(Pipelines)**」タブに登録されている場合、構成コンソールの「**UMF** 例外 **(UMF Exceptions)**」タブで現在または過去の UMF 例外を表示できます。

手順

1. 「状況 **(Status)**」ボタンをクリックします。
2. 「**UMF** 例外 **(UMF Exceptions)**」ボタンをクリックします。
3. オプション: 「開始日 **(From Date)**」フィールドに、表示する UMF 例外の開始日を mm/dd/yyyy 形式で入力します。 このフィールドをブランクのままにした場合、システムは、指定されたその他の基準を満たす、システムが作動可能になった最初の日からの UMF 例外をすべて表示します。このフィールドに日付を入力する場合でも、「終了日 **(Thru Date)**」フィールドには必ずしも日付を入力する必要はありません。
4. オプション: 「終了日 **(Thru Date)**」 フィールドに、表示する UMF 例外の終了日を mm/dd/yyyy 形式で入力します。 このフィールドをブランクのままにした場合、システムは、指定されたその他の基準を満たす、今日の日付までの

UMF 例外をすべて表示します。このフィールドに日付を入力する場合でも、「開始日 **(From Date)**」フィールドには必ずしも日付を入力する必要はありません。

5. オプション: 「元のパイプライン **(From Pipeline)**」フィールドに、UMF 例外を表示する特定のパイプラインの登録済みの名前を入力します。 このフィールドをブランクのままにした場合、システムは、指定されたその他の基準を満たす、すべてのパイプラインの UMF 例外を登録済みの名前別にすべて表示します。
6. オプション: 「最大カウント **(Max Count)**」ドロップダウン・リストから、表示する UMF 例外の最大数を選択します。 システムは、指定されたその他の基準をすべて満たす UMF 例外をその最大数までの件数、表示します。指定された数よりも多い例外が存在する場合でも、システムはそれらを表示しません。指定されたその他の基準をすべて満たす例外の数が、指定された数より少ない場合、すべての例外が表示されます。
7. 必須: 「検索 **(Search)**」ボタンをクリックします。

例

例えば、pipeline08 で今日発生した最後 50 件の UMF 例外を表示するには、以下のような基準を指定します。

- 「開始日 **(From Date)**」フィールドに、今日の日付を入力します。
- 「終了日 **(Thru Date)**」フィールドに、今日の日付を入力します。
- 「発生元ノード **(From Node)**」フィールドに、「pipeline08」と入力します。
- 「最大カウント **(Max Count)**」フィールドで、「50」を選択します。

次のタスク

特定の UMF 例外をクリックすると、その詳細を詳しく調べることができます。表示される情報は、例外発生時にその例外に関してログに記録されたものです。

新規アイデンティティーの表示

構成コンソールの「新規アイデンティティー **(New Identities)**」タブには、過去 7 日間にシステム・パイプラインによって処理された新しいアイデンティティーが表示されます。このタブを使用して、入力データ・ボリュームを確認し、表示される数値が入力データの量またはアクティブ・パイプラインの数から見て適当かどうかを確認できます。また、パイプラインにロードされているデータ・ソースをスポット・チェックして、システムにデータを供給しているソースを確認できます。

手順

1. 「状況 **(Status)**」ボタンをクリックします。
2. 「新規アイデンティティー **(New Identities)**」ボタンをクリックします。

タスクの結果

システムによって、過去 7 日間に処理されたすべての新規アイデンティティーのリストが表示されます。

ヘルプ・トピック

「パイプラインの状況 **(Pipeline Status)**」タブ

このタブを使用して、アプリケーション・モニターおよび SNMP エージェントによるモニター対象として構成されている登録済みパイプラインの現在の状況、統計、およびパフォーマンス情報を確認します。システムは、1 分間に 1 回、SNMP エージェントから状況と統計を収集し、「パイプラインの状況 **(Pipeline Status)**」タブを最新表示します。

注**:** 各パイプライン・ノード上で実行される SNMP エージェントはすべて、システム全体で同じポート番号を使用する必要があります。このポート番号は、パイプライン・ノード上にパイプラインをインストールするときに構成されます。デフォルトの SNMP エージェント・ポート番号の値は 13516 ですが、server.xml ファイル内で、構成されている SNMP ポート番号を見つけることができます。

「合計パイプライン数 **(Total Pipelines)**」
: 構成コンソールでアプリケーション・モニターの対象として登録されているパイプラインの総数が表示されます。(「合計パイプライン数 (Total Pipelines)」=「アクティブ・パイプライン (Active Pipelines)」+「失効パイプライン (Stale Pipelines)」+「ダウン中のパイプライン (Pipelines Down)」)

「アクティブ・パイプライン **(Active Pipelines)**」
: 構成コンソールでモニターの対象として構成されている登録済みパイプラインのうち、現在実行中のパイプラインの総数が表示されます。

「失効パイプライン **(Stale Pipelines)**」
: パイプラインが開始された後に構成が変更されたパイプラインの総数が表示されます。これらのパイプラインは、新しい構成変更を有効にするために、停止してから再始動される必要があります。

「ダウン中のパイプライン **(Pipelines Down)**」
: 構成コンソールでモニターの対象として構成されている登録済みパイプラインのうち、現在実行中でないか、統計を報告していないパイプラインの総数が表示されます。現時点でダウンしているパイプラインはすべてこの合計に含まれます。したがって、パイプライン・ノードが稼働していない場合、そのサーバー上でモニターの対象として構成されているパイプラインはすべてダウン中としてカウントされます。

TPM
: 構成コンソールでモニターの対象として構成されているすべてのアクティブなパイプラインで処理されているトランザクションの毎分の平均総数が表示されます。この数値は、全体的なシステム・パフォーマンスを示しています。数値が大きいほど、各アクティブ・パイプラインのパフォーマンスも高いことになります。この数値は、アクティブ・パイプラインが実行されている各パイプライン・ノード上で稼働している各 SNMP エージェントから受け取った情報に基づいて、1 分間に 1 回更新され、再計算されます。(合計 TPM = アクティブ・パイプラインの TPM ÷ 合計アクティブ・パイプライン数)

TPS
: 構成コンソールでモニターの対象として構成されているすべてのアクティブ・ノードで処理されているトランザクションの毎秒の平均総数が表示されます。この数値は、全体的なシステム・パフォーマンスを示しています。数

値が大きいほど、各アクティブ・ノードのパフォーマンスも高いことになります。この数値は、アクティブ・ノードが実行されている各ホスト・マシン上で稼働している各 SNMP エージェントから受け取った情報に基づいて、1 分間に 1 回更新され、再計算されます。(合計 TPS = アクティブ・ノードの TPS ÷ 合計アクティブ・ノード数)

「パイプライン名 **(Pipeline Name)**」
構成コンソールでモニターの対象として登録されている各パイプラインの名前が英数字順でリストされます。

ホスト名
このパイプラインに登録されているパイプライン・ノードの名前が表示されます。このパイプラインの状況が予期せず「ダウン (Down)」と表示された場合、パイプライン・ノード名を問題のトラブルシューティングに役立てることができます。(例えば、特定のパイプライン・ノード上のすべてのパイプラインが予期せず「ダウン (Down)」とリストされた場合、トラブルシューティングの手始めはパイプライン・ノードになります。)

状況　このパイプラインの最後の既知の状況が表示されます。「アクティブ (Active)」 (実行中) または「ダウン (Down)」 (実行されていない) です。システムは、パイプライン・ノード上で実行されている SNMP エージェントから受け取った情報に基づいて、1 分間に 1 回、状況情報を更新します。

TPM　このパイプラインで処理されているトランザクションの毎分の平均数が表示されます。パイプラインが「ダウン (Down)」状況である場合、システムは「なし (Not Available)」と表示します。この数値は、パイプライン・パフォーマンスを示しています。数値が大きいほど、パイプラインのパフォーマンスも高いことになります。

TPS　このパイプラインで処理されたトランザクションの毎秒の総数が表示されます。パイプラインが「ダウン (Down)」状況である場合、システムは「なし (Not Available)」と表示します。この数値は、パイプライン・パフォーマンスを示しています。数値が大きいほど、パイプラインのパフォーマンスも高いことになります。

「UMF 例外 (UMF Exceptions)」タブ

このタブを使用して、アプリケーション・モニターの対象として登録されているパイプラインによってロードされたデータを基にログに記録された UMF 例外を表示します。最初に、UMF 例外の画面表示用のレポートを生成して表示します。次に、特定の UMF 例外を選択し、その詳細を詳しく調べることができます。この情報は、データ・ファイルに含まれる UMF 例外を解決するうえで役立つ可能性があります。これらのエラーを解決した後、訂正したそのファイル内のレコードを安全に再処理できます。

UMF 例外は、データ主導型エラーです。パイプラインによって処理されている入力データ・ソース・ファイル内の UMF データ構造に問題がある場合に発生します。デフォルトで、UMF 例外はパイプラインのエラー限界カウント (パイプライン構成ファイル内で設定されます) には影響しません。したがって、通常、UMF 例外のみが原因でパイプラインがシャットダウンされることはありません。アプリケーショ

ン・モニターの対象として登録されていないパイプラインの UMF 例外まで含めて、UMF 例外の完全なリストを、UMF_EXCEPT 表または *pipeline_name*.msg ログ内で確認できます。

画面表示用のレポートの基準

これらのフィールドを使用して、画面表示用の UMF 例外レポートの基準を指定します。基準の指定が終わったら、「検索 **(Search)**」ボタンをクリックしてレポートを生成します。

「開始日 **(From Date)**」

指定されたその他の基準に該当する UMF 例外のレポートの開始日。(このフィールドはオプションであり、ブランクのままにすることができます。このフィールドをブランクのままにすることは、指定したその他の基準に該当する、システムが作動可能になった最初の日からの UMF 例外を表示することを意味します。)

このフィールドはデフォルトで今日の日付に設定されます。mm/dd/yyyy 形式を使用して日付を入力します。

「終了日 **(Thru Date)**」

指定されたその他の基準に該当する UMF 例外のレポートの終了日。(このフィールドはオプションであり、ブランクのままにすることができます。このフィールドをブランクのままにすることは、指定したその他の基準に該当する、今日までの UMF 例外を表示することを意味します。)

このフィールドはデフォルトで今日の日付に設定されます。mm/dd/yyyy 形式を使用して日付を入力します。

「発生元ノード **(From Node)**」

UMF 例外を表示する登録済みパイプラインの名前。(このフィールドはオプションであり、ブランクのままにすることができます。このフィールドをブランクのままにすることは、指定したその他の基準に該当する、すべての登録済みパイプラインの UMF 例外を表示することを意味します。)

このタブには、アプリケーション・モニターの対象として登録済みのパイプラインの UMF 例外のみが表示される点に注意してください。すべての UMF 例外を確認する必要がある場合は、UMF_EXCEPT 表または *pipeline_name*.msg ログを参照してください。

「データ・ソース・コード **(Data Source Code)**」

UMF 例外を表示する (正確な) データ・ソースコード。(このフィールドはオプションであり、ブランクのままにすることができます。このフィールドをブランクのままにすることは、指定したその他の基準に該当する、すべてのデータ・ソースの UMF 例外を表示することを意味します。)

「最大カウント **(Max Count)**」

指定されたその他の基準に該当する、表示対象の UMF 例外の最大数に関するオプションが含まれているドロップダウン・リスト。その件数まで (最大数も含まれます) の UMF 例外のみが画面上に表

示されます。基準を満たす UMF 例外がさらに存在する場合でも、システムはそれらを表示しません。

「検索 **(Search)**」ボタン
このボタンをクリックすると、システムによって検索が実行され、入力された基準に一致するレコードがすべて検出され、表示されます。

画面表示用のレポート結果の表示
ウィンドウのこのセクションには、ユーザーが入力した基準に基づいて、画面表示用の UMF 例外レポートが表示されます。リストは、UMF ID 番号でソートされます。

UMF ID
この UMF 例外に関連付けられている、システムによって割り当てられたシーケンス番号が表示されます。UMF ID は、UMF 例外がログに記録されている UMF_EXCEPT 表に直接マップされます。

「元のパイプライン **(From Pipeline)**」
UMF 例外の発生時にレコードを処理していたパイプラインの名前が表示されます。

「作成日 **(Created On)**」
UMF 例外が発生した日付が表示されます。

「出力文書 **(Output Document)**」
この UMF 例外に関連付けられている UMF 出力文書のタイプが表示されます。

「データ・ソース・コード **(Data Source Code)**」
UMF 例外が発生した入力データ・ファイルに関連付けられているデータ・ソース・コードが表示されます。

「外部参照 **(External Reference)**」
UMF 例外が発生した特定のデータ・レコードの外部参照が表示されます。この情報は、データ・ファイル内で訂正する必要のあるレコードを特定するのに役立ちます。

アクション
UMF 例外が発生した入力データ・レコードに関連付けられているアクションが表示されます。(このアクションは、データ・レコードの UMF にコーディングされています。)

- A: 追加
- C: 変更
- D: 削除

「イベント」タブ

このタブを使用して、アプリケーション・モニターと、モニターまたはルーティングのために登録されたパイプラインとの間で交換されたメッセージを表示します。ロギングに関してシステムがどのように構成されているかにもよりますが、通常、これらのメッセージはシステム・ログ・ファイルにも記録されます。最初に、アプリケーション・モニター・イベントの画面表示用のレポートを生成して表示しま

す。次に、特定のイベントを選択し、その詳細を詳しく調べることができます。この情報は、通知目的の場合もあれば、パイプラインのエラーまたは警告を解決するうえで役立つ場合もあります。

通常、アプリケーション・モニター・イベントにはパイプライン処理の中で交換されたメッセージやエラーが含まれます。例えば、パイプラインの開始、パイプラインの停止、またはパイプライン処理中に生成される警告やエラーです。このタブに組み込まれないエラーおよび警告の唯一のタイプは、UMF 例外です。UMF 例外は、処理情報や処理例外というよりもむしろ、データ主導型の例外です。

画面表示用のレポートの基準

これらのフィールドを使用して、画面表示用のアプリケーション・モニター・イベント・レポートの基準を指定します。基準の指定が終わったら、「検索 **(Search)**」ボタンをクリックしてレポートを生成します。デフォルトで、このタブには、アプリケーション・モニターの対象として登録されているパイプラインで、今日発生したアプリケーション・モニター・イベントが表示されます。

「開始日 **(From Date)**」

指定されたその他の基準に該当するアプリケーション・モニター・イベントのレポートの開始日。(このフィールドはオプションであり、ブランクのままにすることができます。このフィールドをブランクのままにすることは、指定したその他の基準に該当する、システムが作動可能になった最初の日からのアプリケーション・モニター・イベントを表示することを意味します。)

「終了日 **(Thru Date)**」

指定されたその他の基準に該当するアプリケーション・モニター・イベントのレポートの終了日。(このフィールドはオプションであり、ブランクのままにすることができます。このフィールドをブランクのままにすることは、指定したその他の基準に該当する、今日までのアプリケーション・モニター・イベントを表示することを意味します。)

「元のパイプライン **(From Pipeline)**」

アプリケーション・モニター・イベントを表示する登録済みパイプラインの名前。 (このフィールドはオプションであり、ブランクのままにすることができます。このフィールドをブランクのままにすることは、指定したその他の基準に該当する、すべての登録済みパイプラインのアプリケーション・モニター・イベントを表示することを意味します。)

このタブには、アプリケーション・モニターの対象として登録済みのパイプラインのアプリケーション・モニター・イベントのみが表示される点に注意してください。

「最大カウント **(Max Count)**」

指定されたその他の基準に該当する、表示対象のアプリケーション・モニター・イベントの最大数に関するオプションが含まれているドロップダウン・リスト。その件数まで (最大数も含まれます) のアプリケーション・イベントのみが画面上に表示されます。基準

を満たすアプリケーション・イベントがさらに存在する場合でも、システムはそれらを表示しません。

「検索 **(Search)**」ボタン
このボタンをクリックすると、システムによって検索が実行され、入力された基準に一致するアプリケーション・イベント・モニター・レコードがすべて検出され、表示されます。

画面表示用のレポート結果の表示
ウィンドウのこのセクションには、ユーザーが入力した基準に基づいて、画面表示用のアプリケーション・モニター・イベント・レポートが表示されます。リストは ID 番号によってソートされます。

「**ID**」
このアプリケーション・モニター・イベントに関連付けられている、システムによって割り当てられたシーケンス番号が表示されます。

「元のパイプライン **(From Pipeline)**」
アプリケーション・モニター・イベントの影響を受ける、またはアプリケーション・モニター・イベントに関係する登録済みパイプラインが表示されます。これが、トラブルシューティングが必要なパイプラインである可能性があります。

「日時 **(Date/Time)**」
アプリケーション・モニター・イベントが発生した日付とタイム・スタンプが表示されます。

イベント
発生したアプリケーション・モニター・イベントのタイプが表示されます。「イベント記述 **(Event Description)**」列と「エラー・レベル **(Error Level)**」列に、このイベントに関する詳細が含まれており、イベント・タイプの重大度が示されます。現時点では、2 つのアプリケーション・モニター・イベント・タイプが表示される可能性があります。

- NODE-INFO は、影響を受けたパイプラインで発生したメモまたはその他のタイプの通知イベントです。一般に、このイベント・タイプは、影響を受けたパイプラインが開始または停止したときに表示されます。
- NODE-ERROR は、影響を受けたパイプラインで発生したエラーです。「エラー・レベル **(Error Level)**」列を見て、即時アクションが必要かどうか確認してください。通常、このようなアプリケーション・モニター・イベントに関する情報は詳しく調べる必要があります。それが、このパイプラインでの問題の解決につながることがあります。

「イベント記述 **(Event Description)**」
アプリケーション・モニター・イベントに関する詳細情報が最大 30 文字まで提供されます。

「エラー・レベル **(Error Level)**」

アプリケーション・モニター・イベントのエラー・レベルのタイプが表示されます。現時点では、2 つのイベント・タイプが表示される可能性があります。

- NOTE は、NODE-INFO イベントに関連付けられるエラー・レベルです。通常、このエラー・レベル・タイプは通知目的であるため、ユーザー処置は一般的には不要です。
- ERR は、NODE-ERROR イベントに関連付けられるエラー・レベルです。通常、このタイプのエラー・レベルは、このアプリケーション・モニター・イベントの詳細を詳しく調べて、エラーを解決する必要があることを示しています。クリックすると、イベントの完全な詳細を確認できます。

「イベント - 詳細 (Events - detail)」タブ

「イベント」タブから特定のアプリケーション・モニター・イベントを選択すると、その選択したイベントの詳細が新しい画面に表示されます。これらの詳細は、システム・ログ・ファイルから直接取り出されます。ただし、UMF 例外のログ・ファイルは対象外です。(このログ・ファイルには、専用の「**UMF 例外 (UMF Exceptions)**」タブがあり、ユーザーはそこで表示できます。) ここに表示される詳細は、パイプライン・エラーのトラブルシューティングに役立つことがあります。

「**ID**」

システムによってこのアプリケーション・モニター・イベントに割り当てられたシーケンス番号。

パイプライン

このアプリケーション・モニター・イベントが発生したパイプラインの名前がリストされます。

「日時 **(Date/Time)**」

この CME イベントの日時が Month, DD, YYYY HH:MM:SS A/PM Time Zone 形式で表示されます。この日時は、イベントがログ・ファイルに記録された日付と時刻に対応します。

イベント

以下の、アプリケーション・モニター・イベントのタイプが表示されます。

- NODE-INFO は、影響を受けたパイプラインで発生したメモまたはその他のタイプの通知イベントです。一般に、このタイプのイベントは、影響を受けたパイプラインが開始または停止したときに表示されます。
- NODE-ERROR は、影響を受けたパイプラインで発生したエラーです。「エラー・レベル **(Error Level)**」列を見て、即時アクションが必要かどうか確認してください。通常、このようなイベントの情報は詳しく調べる必要があります。それが、このパイプラインでの問題の解決につながることがあります。

「イベント記述 **(Event Description)**」

ログ・ファイルに記録されている、アプリケーション・モニター・イベントの最初の一部の文字が表示されます。この記述は、何によってこのイベント・タイプがトリガーされたかについて、より具体的な情報を提供するためのものです。

「エラー・レベル **(Error Level)**」
アプリケーション・モニター・イベントのエラー・レベルのタイプが表示されます。

- NOTE は、NODE-INFO イベントに関連付けられるエラー・レベルです。通常、このエラー・レベル・タイプは通知目的であるため、ユーザー処置は一般的には不要です。
- ERR は、NODE-ERROR イベントに関連付けられるエラー・レベルです。通常、このタイプのエラー・レベルは、このイベントの詳細を詳しく調べて、エラーを解決する必要があることを示しています。クリックすると、イベントの完全な詳細を確認できます。

「新規アカウント **(New Accounts)**」タブ

このタブを使用して、過去 7 日分のデータ・ロードを確認します。処理対象のファイルを提供したデータ・ソースと、それらの処理の結果として生成された新規アイデンティティーの数を一目で確認できます。これらの統計から処理のボリュームを把握することができ、入力データ・ボリュームが、予期していた入力データの量に対して妥当かどうかを素早く確認できます。

このタブをクリックすると、過去 7 日分のデータが表示されます。表示されるページに追加のレコードが含まれている場合、スクロール・バーを使用して、その他のレコードを表示してください。「新規アカウント **(New Accounts)**」タブは、データ・ソース・コードの英数字順にソートされています。

「データ・ソース・コード **(Data Source Code)**」
この新規アイデンティティー・レコードに関連したデータ・ソース・コードが表示されます。この情報は、処理された入力ファイル内のデータ・ソース・コード Universal Message Format (UMF) タグに基づいています。

注**:** 構成コンソールで、「セットアップ **(Setup)**」タブと「ソース **(Sources)**」タブを順にクリックすると、すべてのデータ・ソース・コードを含んだ完全なリストを表示できます。

説明　構成コンソールでこのデータ・ソースに構成されているデータ・ソースの説明が表示されます。この説明は、これらのアイデンティティー・レコードを提供したデータ・ソースを識別するのに役立つ詳細情報を提供します。

「ロード日付 **(Load Date)**」
このデータ・ソース・ファイルが処理され、「レコード・カウント **(Record Count)**」列に含まれる数の新規アイデンティティーを提供した日付が表示されます。日付は、Month DD, YYYY 形式で表されます。

「レコード・カウント **(Record Count)**」
「ロード日付 **(Load Date)**」列に示される日付に、このデータ・ソース・コードから処理された新規アイデンティティーの総数が表示されます。この数値から処理のボリュームを把握できる可能性があります。

第 7 章 データのロード

IBM InfoSphere Identity Insight を使用するには、データを Universal Message Format (UMF) フォーマットに変換し、システムにロードする必要があります。

新規データ・ソースの追加

エンティティー・データベース用に新しいデータのソースを使用するときは、新規データ・ソースを追加する必要があります。

このタスクについて

すべての結果は品質データの産物です。したがって、品質の高いデータをエンティティー・データベースに取り込むことは最も基本的なタスクの 1 つになりますが、これを行うには、データの重要な分析と構成が必要です。

手順

1. データのソースを識別します。データ問題を解決するために、どこを調べるべきか知ることが重要です。
2. メタデータを分析します。エンティティー・データベースがすべてのデータをそのオリジナル・ソースに起因するものと完全に明らかにできるように、エンティティー・データベース内の構成済みの各データ・ソースは、そのレコード上にユニーク ID を持つ必要があります。レコードのユニークさを示すフィールドを見つけ、それが真にユニークであることを確認します。
3. 調達プログラムを使用して、ネイティブ・フォーマットから UMF にデータを変換します。
4. データを構成します。
   a. データ・ソースのロールを定義します。
   b. データ・ソースを構成します。
   c. 必須の番号タイプがあれば作成します。
   d. 必須の特性タイプがあれば作成します。
   e. 解決構成を確認し、必要であればカスタマイズします。
   f. 新規 DQM ルールを構成します。
   g. 新規 DQM ルールを検証します。
   h. ロール・アラート・ルールを構成します。
5. データを確認します。
   a. パイプラインが開始されていることを確認します。
   b. パイプラインが構成済みのトランスポートを使用することができ、調達プログラムから UMF を受け取ったことを確認します。
   c. `.bad` ファイルを調べて、調達ノードが整形式の XML メッセージを生成したことを確認します。

d. 無効なマッピングまたは構成の結果として UMF 例外が発生しなかったことを確認します。
e. データ・ソース要約レポートおよびロード要約レポートを表示して、予期された結果をチェックします。
f. Visualizer を使用して解決された 1 つ以上のエンティティーを検索します。
g. 該当する場合、ロール・アラートを調べます。

UMF へのデータの変換

システムが入力データを処理するためには、データを Universal Message Format (UMF) に変換する必要があります。入力データを UMF に変換する処理は、さまざまなツールで実行できます。例えば、この製品や標準的な XML 変換の製品に含まれている基本ユーティリティーを使用できます。

手順

1. システム用に作成したエンティティー・モデルを使用して、入力データを分析し、入力データがどの程度 UMF 標準に適合しているかを確認します。 次のステップに進む前に、既存の UMF セグメントとタグを明確に理解しておく必要があります。
2. ご使用のエンティティー・モデルに一致する UMF レコードを生成するように、変換ユーティリティーを構成します。
3. 変換ユーティリティーを実行します。

次のタスク

データを UMF に変換した後は、それらの UMF レコードをパイプラインに送信して処理することができます。

調達プログラム

調達プログラムには、データを獲得して Universal Message Format (UMF) に変換し、変換したデータを処理用のパイプラインに送るためのツールとプログラムが含まれています。

製品に含まれている調達プログラム・ユーティリティーを使用して、データを UMF に変換できます。また、WebSphere QualityStage などの抽出、変換、およびロード用のツール (ETL ツール) を調達プログラムとして使用することもできます。

キューへの UMF ファイルの転送

キュー・ユーティリティーを使用して、UMF ファイルをキューに転送できます。

手順

1. 送信するデータが横長フォーマット (1 行あたり 1 レコード) になっていることを確認します。
2. 構成ファイルで構成設定を指定します。
3. キュー・ユーティリティーを実行します。

キュー・ユーティリティー

IBM は、プロセスまたはファイルからキューへの UMF データの転送を管理するキュー・ユーティリティーを提供します。

キュー・ユーティリティーの主なジョブはデータを 1 つ以上のキューに移動することですが、キュー・ユーティリティーは以下のことにも使用できます。

- キューの作成
- キューからのレコードの削除
- キューの状況の表示
- キュー内のレコードの表示

キュー・ユーティリティーは、以下のような特定のフォーマットのデータを予期しています。

- 横長フォーマットの UMF (1 つのレコードを 1 行で記述するフォーマット)
- 各レコードの末尾に改行が 1 つある
- レコードにそれ以外の改行が含まれていない

キュー・ユーティリティーを使用するには、以下のいずれかのキュー・マネージャーを使う必要があります。

Microsoft Windows Server x86
Microsoft Message Queuing (Microsoft Windows Server 2003 または 2008 のコンポーネント)

IBM Websphere MQ 6.0

Microsoft Windows Server x86_64
Microsoft Message Queuing (Microsoft Windows Server 2003 または 2008 のコンポーネント)

IBM Websphere MQ 7.0

Solaris オペレーティング環境
IBM Websphere MQ 6.0

Linux IBM Websphere MQ 6.0

AIX IBM Websphere MQ 6.0

パイプラインがキュー・モードで実行されるときは、キュー・マネージャーが常に必要であり、インストールされて稼働していなければなりません。パイプラインがファイル・モードで実行されるとき、キュー・マネージャーはインストールされていなければなりませんが、Windows プラットフォームと AIX プラットフォームの場合は、稼働している必要はありません。Solaris または Linux の場合は、キュー・マネージャーのインストールも稼働も不要です。

キュー・ユーティリティーの構成ファイル

構成ファイルを使用すれば、キュー・ユーティリティーでレコードを複数のキューに送信できます。

データの 1 つのセットを複数のキューに送信する場合は、その配布のセットアップ方法をキュー・マネージャーに指示する必要があります。具体的には、最初のキューが 1 つのレコードを受け取り、次のキューが 1 つのレコードを受け取り、...と続いていく配布のタイプを作成します。

キュー・ユーティリティーの構成ファイルは qutil.ini という名前で、キュー・ユーティリティーの実行可能ファイルと同じディレクトリーにあります。

パラメーター

[sectionname]
セクションの名前。1 つの構成ファイル内に構成設定の複数のグループを指定し、それぞれにセクション名を付けることで、コマンド行で各設定を参照できます。例えば、2 つのセクションに CFG1 (構成 1) と CFG2 (構成 2) という名前を付けて、キュー・ユーティリティー・コマンドの発行時にこれらのセクションを参照できます。

MessageCountMax
任意の時点で各キューに許可されるレコードの最大数。キューがフルの場合、ユーティリティーはレコードの処理を停止します。

FullCountMax
1 つのキューではなく、すべてのキューに存在できるレコードの総数を指定します。すべてのキューがフルになると、ユーティリティーはデータのフローを一時停止し、レコードが処理のためにパイプラインへと移動してキュー内のスペースが解放されるまで待ちます。FullPause とともに機能します。

FullPause
キュー・ユーティリティーがデータのフローを一時停止するミリ秒数で、FullCountMax に達したときにキュー内のデータが処理されるようにします。

Qout*n*=qname
このセクションの出力キューの名前。出力キューの名前は意味のあるものなら何でもかまいませんが、パラメーターは Qout*n* にしてください。n は 0 始まりの整数です。*n* の値は 0 から *n* までの連続する整数でなければならず、n は定義済みの最後のキューです。このフォーマットは必須です。Qout*n* ID の数値と qname のみ変更してください。

例

以下の例では、2 セットの指示を持っていることが示されています (一方は 2 つのキューを使用し、もう一方は 4 つのキューを使用します)。任意の時点で各キューの最大レコード数は 2,500、すべてのキューのレコード総数は 10,000 です。FullCountMax に到達後、キュー・ユーティリティーは 3 秒間一時停止してから、任意のキューでレコードのロードを試みます。さらに、使用する 4 つのキューの名前がリストされています。

```
[CFG1]
MessageCountMax=2500
FullCountMax=10000
FullPause=3000
Qout0=qnameA
Qout1=qnameB
[CFG2]
```

```
MessageCountMax=2500
FullCountMax=10000
FullPause=3000
Qout0=qnameA
Qout1=qnameB
Qout2=qnameC
Qout3=qnameD
```

キュー・ユーティリティーのコマンド構文

キュー・ユーティリティーのコマンドは、operation (オペレーション) と modifier (修飾子) で構成されています。

キュー・ユーティリティー・コマンドの基本構文は次のとおりです。

qutil -operation *qname* **-modifier**

qname はキューの名前です。

コマンドのオペレーション

オペレーションは、キュー・ユーティリティーのさまざまな機能を定義します。 1 つの qutil コマンドには、1 つのオペレーションのみ追加できます。

-C 新規キューを作成します。

qname のユニーク名が必要です。

大文字の C にしてください。

-f stdin をキューにコピーします。

qname が必要です。

-i stdin を複数のキューにコピーします。

qutil.ini ファイルで定義されたセクション名が必要です。メッセージを複数のキューに配布するために、qutil.ini からロードするセクションを指定します。

-k 各レコードのパージ・カウント。

qname が必要です。

-c 修飾子とともに使用して、処理されるレコード数を制限できます。

-p 各レコードのピーク・カウント。

レコードをキューから削除しません。

qname が必要です。

stdout に書き込みます。

-c 修飾子とともに使用して、処理されるレコード数を制限できます。

-r 各レコードの読み取りカウント。

レコードをキューから削除します。

qname が必要です。

stdout に書き込みます。

-c 修飾子とともに使用して、処理されるレコード数を制限できます。

-s キュー状況

qname が必要です。

-x *qname* を削除します。

qname が必要です。

コマンドの修飾子

修飾子は、キュー・ユーティリティー・オペレーションの追加パラメーターを構成します。1 つの qutil コマンドに複数の修飾子を使用できます。

-T キューがトランザクションであるかどうかを指定します。

デフォルトでは、作成時に -T 修飾子を使用してトランザクションとして指定しない限り、すべての新規キューは非トランザクションです。

キューがアプリケーション・モニターからルーティング情報を受け取る可能性があるときは、トランザクション・キューを使用しないでください。

Microsoft Message Queueing のトランザクション・キューでは、メッセージの優先順位の指定や、受信した順序以外の順序でのメッセージの処理は許可されていません。

-c レコードのカウントを処理した後で停止するよう指定します。

整数を入力します。

小文字の c にしてください。

-l 各レコードの優先順位を指定します。

整数を入力します。

有効な整数値は以下のとおりです。

0-7
Microsoft Message Queueing
優先順位は 0 から 7 です。0 は優先度が最も低く、7 は優先度が最も高くなります。

デフォルトは 3 です。

0-9
IBM Websphere MQ
優先順位は 0 から 9 です。0 は優先度が最も低く、9 は優先度が最も高くなります。

デフォルト値はキューのプロパティーによって異なります。このプロパティーは、IBM Websphere MQ マネージャーで変更できます。

-m キュー・マネージャーを指定します。

AIX、**HP-UX**、**Linux**、および **Solaris** のみ

-o メッセージが期限切れになるまでの秒数を指定します。

整数を入力します。

-q キュー・タイプを指定します。

Microsoft Windows のみ

有効な値は以下のとおりです。

mq IBM WebSphere MQ

msmq
Microsoft Message Queueing (MSMQ)

-t 各レコード間の待ち時間をミリ秒数で指定します。

整数を入力します。

コマンドのオペレーションと修飾子の関係

特定の修飾子は、特定のオペレーションでのみ使用することが推奨されています。各オペレーションと使用可能な修飾子の関係を下表に示します。

表 *31.* キュー・ユーティリティー・コマンドのオペレーションと修飾子の関係

オペレーション	有効な修飾子
`-C`	`-T, -q` 例: qutil -C *qname* -T -q mq
`-f`	`-c, -t, -l, -o, -q` *EXAMPLE:* qutil -f *qname* -c 50 -t 20 -l 4 -o 10 -q msmq
`-i`	修飾子なし。例: qutil -i configsection
`-k`	`-c` 例: qutil -k *qname* -c 50
`-p`	`-c` 例: qutil -p *qname* -c 50
`-r`	`-c` 例: qutil -r *qname* -c 50
`-s`	修飾子なし。例: qutil -s *qname*
`-x`	修飾子なし。例: qutil -x *qname*

適切なフォーマットへの UMF ファイルの変換

UMF フォーマット・ユーティリティーを使用して、UMF レコードを横長フォーマットと縦長フォーマットの間で切り替えることができます。

UMF フォーマット・ユーティリティー

UMF フォーマット・ユーティリティーを使用して、UMF レコードを横長フォーマットと縦長フォーマットの間で変換できます。UMF フォーマット・ユーティリティーは、指定のタグで定義された UMF データを抽出することもできます。

UMF レコードは、単一行 (横長フォーマット) で表示することも、各行が 1 つの XML エレメントと値を持つインデントされた複数行(縦長フォーマット) で表示することもできます。

例: 横長フォーマット

```
<name><name_type>M</name_type><first_name>John</first_name>
<last_name>Smith</last_name></name>
```

例: 縦長フォーマット

```
<name>
 <name_type>M</name_type>
 <first_name>John</first_name>
 <last_name>Smith</last_name>
</name>
```

UMF フォーマット・ユーティリティーのコマンド構文

UMF フォーマット・ユーティリティーは、さまざまなコマンドを使用してデータのフォーマットと抽出を行います。

UMF フォーマット・ユーティリティー・コマンドの基本構文は次のとおりです。

```
xutil -o[switch] option
```

パラメーター

-o **Out** 出力を stdout に送信します。必須パラメーターです。パラメーター・スイッチは以下のとおりです。

- **w** 出力のフォーマットを定義します。1 レコード用のすべての UMF を 1 行で記述します。すべてのリターンと改行を削除します。
- **t** 出力のフォーマットを定義します。1 レコード用の UMF を複数行で記述します。 1 行あたり 1 つのタグを配置し、タブを挿入して文書を読みやすくします。

-t **Tagname:** タグ名に基づいてレコードをフィルターに掛けます。このタグで選別されたレコードのみが stdout に出力されます。エラーはすべて stderr に送信されます。

tagname パラメーターは、レコードをフィルターに掛けたい場合に使用します。例えば、エンティティーとアクティビティーのレコードが混合するファイルがあります。アクティビティーの前にエンティティーを処理すれば、アクティビティーがマッチング用の既存エンティティーを持つことができ好都合です。

例

次のコマンドは、入力ソースとして mixedlist.xml を使用し、出力ファイルとして entity.xml を使用して、フィルターによってエンティティーのみ出力します。

```
xutil -ow -t UMF_ENTITY < mixedlist.xml > entity.xml
```

次のコマンドは、UMF フォーマット・ユーティリティー処理の出力をパイプライン、つまりキュー・ユーティリティーに送ります。

```
xutil -ow < file.xml |qutil -f qname
```

エンティティー・モデルの拡張

エンティティー・モデルとは、何をエンティティーとみなすかを定義するデータのセットです。以下の説明を使用して、デフォルトのエンティティー・モデルを拡張します。これは共通のタスクではありませんが、ご使用の環境に合わせてエンティティー・モデルを拡張できます。

Universal Message Format (UMF)

Universal Message Format (UMF) は、データ・ソース・ファイルの構造化に使用される拡張可能な XML の方言です。UMF には、アイデンティティー、関係、およびアクティビティーの主要な部分を表す標準タグが含まれています。データをパイプラインで処理する前に、データを UMF に変換して UMF 仕様に従う必要があります。

UMF は以下の階層コンポーネントで構成されています。

UMF 文書
: データを構成する UMF セグメントの集合であり、データ・ソース・レコードのタイプを示します。

UMF セグメント
: データ・ソースのデータを構成する UMF 文書の一部です。

UMF エレメント
: UMF 文書の UMF セグメント内のデータを定義する XML タグと値です。

UMF 仕様には、UMF 文書の具体的なタイプ、各 UMF 文書タイプ内の UMF セグメント、および各 UMF セグメント内の有効な UMF エレメントがリストされています。

ソース・データの分析

ソース・データをエンティティー・データベースに取り込む最初のタスクは、UMF へのマッピングに向けてソース・データを分析することです。

手順

1. エンティティー・データベースにロードするデータを識別します。
2. データが一貫していて、完全であることを確認します。
3. 対応するデータベース表の列幅に対して、入力 UMF セグメント・エレメント値の長さがどれぐらいか識別します。
4. ソース・データ内の無効文字を識別します。

タスクの結果

分析の結果に応じて、以下のようなオプションが考えられます。

- DQM ルールを使用して、無効文字を持つデータを修正する。
- DQM ルールを使用して、対応するデータベース表の列幅よりも長いデータを切り捨てる。

- 外部のデータ・ソース・プロバイダーに、より完全なデータを提供するよう依頼する。
- 有効なデータを持つフィールドのみロードする。

デフォルト UMF 仕様の確認

カスタマイズした UMF 仕様やエンティティー・モデルの作成を補助するために、デフォルト UMF 仕様を確認する必要があります。これらの項目は、データ・ソースから、エンティティー・データベースに取り込まれる UMF タグへのデータ転送を策定するものです。

エンティティー・データベースへの UMF セグメントのマッピング

データに新しい UMF セグメントが必要なときは、必ずその UMF セグメントのデータ用に新規データ・マッピングを作成する必要があります。有効なデータ・マッピングがないと、データをエンティティー・データベースに正常にロードできません。

エンティティー・データベースを変更することのリスク

エンティティー・データベースの変更にはリスクがともなうため、十分な経験や専門知識なしに変更を実行すべきではありません。

- 十分な経験や専門知識なしに、表をエンティティー・データベースに追加しないでください。
- データベース表へのフィールドの追加は、該当する表だけに限らず、それ以外のものにも関連する処理です。可能な限り、既存の表とフィールドを使用して新規データを分類することが推奨されています。
- データベース表の索引は変更しないでください。データベース表の索引を変更すると、Visualizer のハングなど、予測不能で望ましくない結果が生じるおそれがあります。
- 十分な専門知識を持って、あるいは IBM の補助を受けて、DQM の変更を行うことのみが推奨されています。
- 新しい構成を実稼働環境に適用する前に、必ずテスト・データベースを使用してその新しい構成を検証してください。

エンティティー・データベースへの表の追加

新しいデータ・ソースを追加するときに、新規データベース表の追加が必要になることがあります。

このタスクについて

エンティティー・データベースに表を追加しても、新規データの解決が可能になるわけではなく、データを保管する場所としてのみ使用されます。

新規構成を実稼働環境に適用する前に、テスト・データベースを使用してその新規構成を検証することが推奨されています。

可能な限り、既存の表とフィールドを使用して新規データを分類することが推奨されています。

新しい表を追加すると、システムでまだ構成されていない予期されるデータに適応できます。現行のデータ・モデルと整合性のある新規データベース表を作成する必要があります。

以下に示す必須の関連フィールドを含めてください。

- ENTITY_ID
- DSRC_ACCT_ID
- HIST_STAT - 順次ヒストリー・トラッキングを使用する場合は必須です。
- SYS_CREATE_DT
- SYS_DELETE_DT
- SYS_LSTUPD_DT
- SYS_LSTUPD_US

手順

1. エンティティー・データベースに新規表を作成します。
2. 新規表のデータ・マッピングを作成します。
3. 新規データベース表をディクショナリーに追加します。
4. 新規表のデータ・マッピングを定義します。
5. 新規セグメントに適用する適切な DQM ルールを決定し、コンソールでそのルールを構成します。
6. パイプラインを通じて既知のテスト・データを実行し、結果のログ・ファイルをチェックして、新規構成を検証します。
   a. テストの実行でエラーが発生しないことを検証します。
   b. コンソールで UMF 例外をチェックします。
   c. ログ・ファイル `nodename.Sql.Err.log` と `nodename.err` でエラーをチェックします。
   d. テスト結果が予想どおりの結果になっているか検証します。
   e. UMF_LOG 表をチェックし、すべてのレコードが正常にロードされていることを確認します。

エンティティー・データベース表へのフィールドの追加:

新しいデータに適応するために、既存のエンティティー・データベース表に新規フィールドの追加が必要になることがあります。

このタスクについて

新しい UMF セグメントにまったく新規の表が必要ない場合は、既存の表に新規フィールドを追加できます。

既存のエンティティー・データベース表にフィールドを追加しても、新規データの解決が可能になるわけではなく、データを保管する場所としてのみ使用されます。

新規構成を実稼働環境に適用する前に、テスト・データベースを使用してその新規構成を検証することが推奨されています。

可能な限り、既存の表とフィールドを使用して新規データを分類することが推奨されています。

手順

1. 新規フィールドを適切なデータベース表に追加します。
2. コンソールで、新規フィールド用のデータ・マッピングを作成します。
3. 新規フィールドに適用する適切な DQM ルールを決定し、コンソールでそのルールを構成します。
4. パイプラインを通じて既知のテスト・データを実行し、結果のログ・ファイルをチェックして、新規構成を検証します。
   a. テストの実行でエラーが発生しないことを検証します。
   b. コンソールで UMF 例外をチェックします。
   c. ログ・ファイル `nodename.Sql.Err.log` と `nodename.err` でエラーをチェックします。
   d. テスト結果が予想どおりの結果になっているか検証します。
   e. UMF_LOG 表をチェックし、すべてのレコードが正常にロードされていることを確認します。

ディクショナリーへの新規データベース表の追加:

データ (および UMF) にとって新規データベース表の作成が必要な場合は、システムが使用するデータベース表のディクショナリーにその表を追加しなければなりません。表がディクショナリーに存在しないと、UMF と表のためにデータ・マッピングを作成できません。

始める前に

ユーザーに、データベース表でデータの読み取りと保存を行うための適切なアクセス権限が付与されている必要があります。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「ディクショナリー **(Dictionary)**」タブをクリックします。
4. 「新規 **(New)**」ボタンをクリックします。
5. 「表名 **(Table Name)**」フィールドに、新規データベース表の名前を入力します。

データ・マッピングの定義

新しい UMF セグメントとタグのためにデータ・マッピングを作成する必要があります。新しいソース・システムが製品に追加されると、その結果として、新規 UMF セグメントとタグが作成されることがあります。データ・マッピングは、UMF 内のデータをエンティティー・データベース内の対応する表と表列にマップします。

データ・マッピング:

データ・マッピングは、UMF ファイルのデータをエンティティー・データベース内の対応する表と表列にマップします。

有効なデータ・マッピングがないと、データをエンティティー・データベースに正常にロードできません。データに新しい UMF セグメントが必要なときは、必ずその UMF セグメントのデータ用に新規データ・マッピングを作成する必要があります。

例

Finn の Auto Service は最近、顧客向けに保険会社データの収集を開始しました。例えば、新しい保険会社の UMF データが、以下の UMF セグメントを使用しているものとします。

```
<ATTRIBUTE>
<INSURANCECOMPANY>Mooninite Casualty Company</INSURANCECOMPANY>
</ATTRIBUTE>
```

エンティティー・データベース内の適切な表列を対象として、<ATTRIBUTE><INSURANCECOMPANY> UMF データ・パスの新規データ・マッピングを作成する必要があります。UMF データ・パスの XPath 値は `./ATTRIBUTE/INSURANCECOMPANY/` です。

データ・マッピングの表示:

データ・マッピングは、UMF ファイルのデータをエンティティー・データベース内の対応する表と表列にマップします。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「データ・マップ **(Data Map)**」タブをクリックします。
4. 「セグメント **(Segment)**」ドロップダウンで、表示する UMF セグメントを選択します。
5. 「表 **(Table)**」ドロップダウンで、マッピングを表示する UMF セグメント表を選択します。

データ・マッピングの作成:

データ・マッピングは、UMF データをエンティティー・データベース内の対応する表と表列にマップします。新しい UMF タグを持つ入力データがシステムによって処理される場合は、新規データ・マッピングが必要です。

始める前に

このデータ・マッピングがデータを複数の表にマップする場合は、パイプラインのオペレーション中にこれらの表が正しいロード・シーケンスで挿入されることをチェックする必要があります。この表がディクショナリーに存在しない場合は、UMF と表のためにデータ・マッピングを作成できるように、新規表をディクショナリーに追加しなければなりません。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「データ・マップ **(Data Map)**」タブをクリックします。
4. 「セグメント」ドロップダウンで、新規データ・マッピングを表に追加する UMF セグメントを選択します。
5. 「表」ドロップダウンで、新規データ・マッピングを追加する UMF セグメント表を選択します。
6. 以下のいずれかのステップを実行します。
   - 新規データ・マッピングを作成するために、「新規 **(New)**」ボタンをクリックします。
   - 既存のデータ・マッピングに基づいてデータ・マッピングを作成するために、リストからデータ・マッピングを選択して「複製 **(Clone)**」 ボタンをクリックします。
7. これが新規セグメントの場合は、UMF セグメントの名前を「セグメント **(Segment)**」フィールドに入力します。
8. 「表 **(Table)**」ドロップダウン・リストで、目的のデータベース表を選択します。
9. 「表列 **(Table Column)**」フィールドに、UMF データ・パスをマップするデータベース表の列の名前を入力します。
10. 「フィールド・タイプ **(Field Type)**」ドロップダウンで、データベース内の表列のフィールド・タイプを表す適切なフィールド・タイプを選択します。
11. 「データ・タイプ **(Data Type)**」ドロップダウンで、データの値を表す適切なデータ・タイプを選択します。
12. 「**UMF** データ・パス **(UMF Data Path)**」フィールドに UMF タグを入力します。
13. 「更新メソッド **(Update Method)**」ドロップダウンで、どちらの値 (インバウンド値または以前に保存された値) を保持するのかを決める適切な更新メソッドを選択します。
14. 「状況 **(Status)**」フィールドで、ドロップダウン・リストからデータ・マッピングの適切な状況を選択します。
15. 「保存 **(Save)**」ボタンをクリックします。

データ・マッピングの削除**:**

データ・マッピングは、UMF データをエンティティー・データベース内の対応する表と表列にマップします。システムで使用されなくなったデータ・マッピングは削除できます。

手順

1. 「セットアップ **(Setup)**」ボタンをクリックします。
2. 「**UMF**」ボタンをクリックします。
3. 「データ・マップ **(Data Map)**」タブをクリックします。

4. 「セグメント **(Segment)**」ドロップダウンで、データ・マッピングを削除する表が含まれる UMF セグメントを選択します。
5. 「表」ドロップダウンで、データ・マッピングを削除する UMF セグメント表を選択します。
6. リストからデータ・マッピングを選択して、「削除 **(Delete)**」ボタンをクリックします。

ヘルプ・トピック**:**

データ・マッピング **-** 「一般 ***(General)***」タブ*:*

「一般 **(General)**」タブを使用して、データ・マッピングの詳細を指定します。

セグメント
: データ・マッピングを作成するセグメントの名前を入力します。このセグメント名は大文字で入力する必要があります。

表
: ドロップダウン・リストで、作成するデータ・マッピング用の表を選択します。

表列名
: 作成する表列の名前を入力します。

表列タイプ
: ドロップダウン・リストで、表列名の表列タイプを以下の中から選択します。

  ユニーク **ID**
  : この表列は、データベース・エンジンによって生成されて自動的に 1 つずつ増加するユニーク・キーです。1 つの表列のみ、この値を構成できます。

  エンティティー・キー
  : これを選択すると、表列は常に ENTITY_ID に設定されます。

  ビジネス・キー
  : この表列と、指定済みの他のビジネス・キー表列によって、同じレコードの存在を判断するための複合ルックアップ・キーが構成されます。

  属性
  : この表列は単にデータの保存にのみ使用され、表の挿入/更新/削除に関して機能的な効力はまったく持ちません。

  キー属性
  : この表列の値は、同じ値を持つ既存のレコードが存在するか判断するために使用されます。データベースは、時間の経過にともなうこれらの値への変更を追跡します。例: ADDR1 値の変更によってレコードのバージョンを維持する場合は、ADDR1 値をキー属性として指定します。

    この値は索引とは無関係です。

  ヒストリー・シーケンス
  : この表列は、指定のソースから提供されたどのレコードが現在の最新で、どのレコードが過去のものであるかを判断するために使用されます。

ヒストリー・シーケンスは常に HIST_STAT 表列に割り当てられます。

タイム・スタンプの削除
この表列は、レコードが削除された最終日時を保管するために使用されます。

タイム・スタンプの更新
この表列は、レコードが更新された最終日時を保管するために使用されます。

データ・タイプ
ドロップダウン・リストから、表列のデータ・タイプを選択します。

「**CHAR**」
文字データ (英数字)。

INT 整数データ。

「**DATE**」
日付データ。例: yyyy-mm-dd または mm-dd-yyyy

DATE/TIME
日付/時刻データ。例: yyyy-mm-dd hh:mm:ss または mm-dd-yyyy hh:mm:ss

UMF データ・パス
UMF タグの XPath ロケーションを入力します。

更新メソッド
ドロップダウン・リストで、作成するデータ・マッピング用の更新メソッドを選択します。更新メソッドによって、どちらの値 (インバウンド値または以前に保存された値) を保持するのかが決められます。

更新しない
UMF エレメントの値がデータベース表に存在する場合、その値は更新できません。

常に更新
UMF エレメントの値がデータベース表に存在する場合、その値を更新できます。

最大値
入力または保管済みにかかわらず、より大きい値が保持または更新されます。

表列のデータ・タイプが、INT、DATE、または DATE/TIME に等しい場合に限ります。

最小値
入力または保管済みにかかわらず、より小さい値が保持または更新されます。

表列のデータ・タイプが、INT、DATE、または DATE/TIME に等しい場合に限ります。

状況 ドロップダウン・リストで、作成するデータ・マッピング用の状況を選択します。

アクティブ
: データ・マッピングはアクティブです。

非アクティブ
: データ・マッピングは非アクティブです。

IBM InfoSphere QualityStage と AddressDoctor を使用した住所標準化

住所クレンジングと住所標準化は、エンティティー解決の処理を最適化するために、住所情報の修正および標準化を可能にするパイプライン処理です。IBM® InfoSphere™ Identity Insight のこの新機能により、AddressDoctor®、IBM InfoSphere Information Server、IBM InfoSphere DataStage®、および IBM WebSphere® QualityStage™ など、業界標準の住所データ標準化ソリューションを使用できるようになります。

AddressDoctor が提供する住所標準化モジュールのサポートによって、Worldwide Address Verification and Enhancement System (WAVES) など、他のモジュールとの依存関係と制限が解消されます。AddressDoctor 住所標準化モジュールは、DataStage と QualityStage 住所検証インターフェース (QS-AVI) を用いることで、Identity Insight エンティティーの解決に使用できます。QualityStage は IBM Information Server のコンポーネントです。

AddressDoctor® には次の利点があります。

- 240 を超える国と地域をサポートします。
- ストリート・レベルで広い範囲を対象とします。
- ユニコードに対応し、主な文字セットをすべてサポートします。
- 文字変換があります。
- 住所がどれぐらい到達可能かを示す検証状況を提供します。
- 地域の郵便規格に対応するフォーマットを提供します。

AddressDoctor と QS-AVI の実装は簡単なタスクではありません。実装の支援について、IBM 担当員に問い合わせることをお勧めします。

QS-AVI 住所クレンジングの要件とタスクの概要

IBM QualityStage と AddressDoctor インターフェース (QS-AVI) を使用して Identity Insight の住所クレンジングを実行するときの詳細な処理ステップについては、ibm.com の techdoc を参照してください。このトピックでは、処理の概要、要件、および詳細情報へのリンクについて説明します。

始める前に

以下の製品が必要です。

- IBM InfoSphere Information Server (IBM InfoSphere DataStage と IBM InfoSphere QualityStage Version 8.0.1 を含む)
- QS-AVI Data Quality ステージ
- 必要な国向けの AddressDoctor(R) Database

このタスクについて

処理は以下の一般的な手順に従います。

手順

1. DataStage と QualityStage Designer で QS-AVI ステージ・ジョブを定義します。
2. 「AddressValidateWS.dsx」ファイルをステージにインポートします。(これはあらかじめ定義された住所クレンジング・ジョブであり、EAS と QS-AVI の統合用に設計されています。)このファイルは、フィックスパックのインストール・ディスクの <RR_INSTALL>/srd-home/qsavi/AddressValidateWS.dsx にあります。
3. 住所検証ステージを変更し、Information Services 用の DataStage ジョブを有効にします。
4. Information Server コンソールで DataStage ジョブをサービスとして定義します。
5. WebSphere Information Services Director (WISD) を使用してデプロイメントを確認し、この新規サービス用の Web サービス記述言語 (WSDL) 文書を生成して調べます。
6. WebSphere Integration Developer などの環境で、このサービスをテストします。
7. pipeline.ini ファイルの OAC セクションにある AddrConnection を以下のフォーマットに変更することにより、QSAVI 機能を活動化します。

   [OAC]
   AddrConnection=qsavi://host:port/?timeout=ms

   host Infoserver のホスト名または IP アドレスです。

   port ポート番号です。デフォルト・ポートは 9080 です。

   timeout
   オプション・パラメーターです。接続タイムアウト・パラメーターを外部で設定できます。デフォルトの接続タイムアウトは 10000 ミリ秒 (10 秒) です。

次のタスク

この処理の詳細な手順については、「IBM InfoSphere Identity Insight の Web プロセスとしての QS-AVI 住所クレンジング」を参照してください。

QS-AVI トラブルシューティング

QS-AVI は住所クレンジングの品質を示す「valstatus_qsav」を返し、関連問題のトラブルシューティングを可能にします。

例外

例外はハンドル値状況に基づいて生成されます。

```
// handle value status
// V  - Validated
// C  - Corrected
```

```
// P3 - Not corrected - Deliverability High
// P2 - Not corrected - Deliverability Fair
// P1 - Not corrected - Deliverability Small
// N1 - Not checked - Country not recognized
// N2 - Not checked - Country DB not found
// N3 - Not checked - Country not unlocked
// N4 - Not checked - Validation not called
// N5 - Insufficient information
// Q1 - No suggestions
// Q2 - Suggestions incomplete
// Q3 – Suggestions
```

QS-AVI は住所クレンジングの可能性を示す「resultstatus_qsav」も返します。

```
// handle delivery probability
// 0 - Empty
// 1 - Not checked
// 2 - Not checked, but standardized
// 3 - Checked and corrected
// 4 - Validated, but changed
// 5 - Validated, but standardized
// 6 - Validated and unchanged
// 7 - No value given because of multiple matches
```

エラー・メッセージ

6301E - 無効な応答です。

6302E - InforServer サーバーに接続できません
このメッセージは、EAS が InfoServer への接続に失敗したときに表示されます。このエラーは InforServer からの「soapenv:Fault」応答によって生成されることもあり、その場合は無効な応答として処理されます。

6303E - エラー、サーバーへの接続に失敗 **: {0}", __serverName**
このメッセージは、EAS が正しい InfoServer サーバーへの接続に失敗したときに表示されます。

第 8 章 データの分析

Analyst ツールキットは、Identity Insight に対するアプリケーション開発およびカスタマイズの機能セットを提供します。これらはユーザー・インターフェースとレポートのセットであり、それらは必要に応じて変更したり、その他のアプリケーションから参照したりできます。

Visualizer を使用したデータの分析

Visualizer を使用して、さまざまな分析タスクを実行できます。タスクには、アラートのレビューと後処理、エンティティーの検索、エンティティー・データの表示、エンティティーとそれらのエンティティーの他のエンティティーに対する関係を表すグラフの表示、属性アラート・ジェネレーターの作成と管理、単一エンティティーの追加または複数のエンティティーを含んだ小さいファイルの追加、エンティティー間の関係の開示、レポートの印刷などがあります。

Visualizer のセットアップ

Visualizer をうまく使用するには、Visualizer にアクセスする方法や、Visualizer で情報を表示する方法を自分の好みに合わせてカスタマイズする方法を理解する必要があります。

Visualizer

Visualizer は、アナリストや調査員がアラート、関係、エンティティー解決の結果を分析するために使用するグラフィカル・ユーザー・インターフェースです。

Visualizer は、組み込みバージョンの IBM WebSphere Application Server によってホストされます。Visualizer の構成は、構成コンソールから行うか、Visualizer の「ファイル **(File)**」メニューの「設定 **(Preferences)**」選択から行います。

Visualizer ユーザーは、以下のような各種の分析タスクを実行できます。

アラートの分析と後処理
: エンティティー解決処理によって生成されるアラートは、組織にとって関心のある関係やエンティティー解決を表します。通常はアナリストがアラートを確認し、アラート情報に基づいて、アクションが必要な場合には、実行するアクションを決定します。アラートには、ロール・アラート、属性アラート、およびイベント・アラートの 3 つのタイプがあります。

  Visualizer はアラートを表示し、アナリストに対し、アラートおよびアラートに含まれるエンティティーのテキスト・ビューとグラフィカル・ビューの両方を提供します。アナリストは詳細にドリルダウンしてから、アラートの後処理の状況を適切に設定できます。

属性アラート・ジェネレーターの作成と管理
: Visualizer を使用することで、アナリストは、属性アラート・ジェネレーター機能を介して永続検索を作成および管理でき、属性アラートを表示する方法と受け取る方法を管理できます。アナリストは、属性データに基づいて属

性アラート・ジェネレーターを作成して、属性データに基づいてエンティティーに解決されたアイデンティティーを見つけることができます。また、アナリストは、属性アラート・ジェネレーターを作成して、エンティティー・データベースで特定のエンティティーを永続的に検索することもできます。

エンティティーの検索

Visualizer ユーザーは、以下のようにいくつかの方法を使用して、さらに分析を行うためにエンティティーを検索することもできます。

- 属性による検索
- データ・ソース・アカウントによる検索
- エンティティー ID による検索
- 解決による検索 (最小解決スコアしきい値に基づいて、入力された基準がエンティティー・データベース内のアイデンティティーやエンティティーとどれくらい正確に一致しているか)

エンティティーおよび開示された関係の追加

アナリストは、Visualizer を使用してエンティティー解決や関係検出のレコードを追加できます。単一アイデンティティー・レコードを追加することも、数千件のアイデンティティー・レコードを含んだ UMF ファイルをロードすることもできます。調達プログラムを通じてアイデンティティー・レコードが追加される場合と同様に、Visualizer から追加されたレコードも、エンティティー解決および関係検出のためにパイプラインによって処理されます。処理の結果はエンティティー・データベースに書き込まれ、アラートがある場合は Visualizer に公開されます。

アナリストは、アイデンティティー間にリンクがあることをわかっている場合、(アイデンティティーによって) エンティティー間の関係を開示することもできます。開示される関係の例として、求人の申込書にリストされている緊急時連絡先や身元保証人に基づいた関連エンティティーなどがあります。エンティティーにより、申込書にあるこれらの関係が開示されます。

レポートの生成と印刷

Visualizer には、アナリストが Visualizer での作業を管理および追跡するのに役立てるために、アナリストが表示したり印刷したりできる複数のレポートも含まれています。

Visualizer の構成

Visualizer の設定を構成して、Visualizer セッションで情報を表示する方法を調整できます。

Visualizer 表示オプションの設定**:**

「ウィンドウ設定 **(Window Preferences)**」タブで背景色、フォント、およびその他の表示オプションを変更することにより、Visualizer の表示をカスタマイズできます。

このタスクについて

Visualizer 表示オプションは、Visualizer クライアントごとに構成されます。以下の手順を実行することで表示が変更される対象は、現在ログオンしている Visualizer クライアントのみです。

手順

1. Visualizer で、「ファイル」 > 「設定 **(Preferences)**」 > 「ウィンドウ設定 **(Window Preferences)**」を選択します。
2. 使用する外観表示オプションを選択します。 「外観 **(Look and Feel)**」で「メタル *(Metal)*」オプションを選択した場合、「テーマ **(Theme)**」、「フォント **(Font)**」、および「サイズ **(Size)**」の各ドロップダウン・リストのみ設定を変更できます。
3. 「送信 **(Submit)**」をクリックします。 確認メッセージによって、変更を有効にするには Visualizer の再始動が必要なことが通知されます。
4. 「**OK**」をクリックします。
5. Visualizer を閉じます。Visualizer を開始し、再度ログインします。

タスクの結果

これで、選択した新しいウィンドウ表示オプションを使用して Visualizer が表示されます。

UMF ファイルのデフォルト・パスの設定**:**

Visualizer による処理のためにアイデンティティー・レコードを UMF データ・ファイルで定期的にロードする場合、デフォルト・パスを設定することで手順を 1 つ省略できます。

このタスクについて

デフォルト・パス設定は、Visualizer クライアントごとに構成されます。このタスクに従ってデフォルト・パスを指定することでパスが設定される対象は、現在ログインしている Visualizer のみです。

手順

1. Visualizer で、「ファイル **(File)**」 > 「設定 **(Preferences)**」 > 「システム設定 **(System Preferences)**」を選択します。
2. 「ファイル・ロードのデフォルト・パス **(Default path for File Load)**」で、以下のいずれかを実行します。
   - 使用するディレクトリーの絶対パスを入力します。
   - または、ディレクトリーを参照して選択します。
3. 「送信 **(Submit)**」をクリックします。 確認メッセージによって、変更を有効にするには Visualizer の再始動が必要なことが通知されます。
4. 確認メッセージで「**OK**」をクリックします。
5. Visualizer を閉じて、Visualizer を再始動し、再度ログインします。

タスクの結果

UMF ファイルをロードするとき、ここで指定したディレクトリーが、毎回デフォルト・パスになります。

Centrifuge のデフォルト・パスの設定**:**

オプションである Centrifuge Systems の Centrifuge Desktop を使用してエンティティー・グラフを視覚化および表示する場合、Visualizer 設定に Centrifuge Desktop ファイル・パスを指定する必要があります。

このタスクについて

デフォルト・パス設定は、Visualizer クライアントごとに構成されます。このタスクに従ってデフォルト・パスを指定することでパスが設定される対象は、現在ログインしている Visualizer のみです。

手順

1. Visualizer で、「ファイル **(File)**」 > 「設定 **(Preferences)**」 > 「システム設定 **(System Preferences)**」をクリックします。
2. 「**Centrifuge** パス **(Centrifuge path)**」の「ファイル・パス **(File Paths)**」セクションの下で、以下を実行します。
   - Centrifuge Desktop アプリケーションのファイル・パスまたは URL (Uniform Resource Locator) をフィールドに入力します。
   - または、Centrifuge Desktop アプリケーションを参照し、開きます。
3. 「送信 **(Submit)**」をクリックします。 確認メッセージによって、変更を有効にするには Visualizer の再始動が必要なことが通知されます。
4. 確認メッセージで「**OK**」をクリックします。
5. Visualizer を閉じて、Visualizer を再オープンし、再度ログインします。

タスクの結果

パスが構成されると、「調査 **(Research)**」ウィンドウの「ロール・アラート詳細 **(Role Alert Detail)**」画面および「エンティティー・レジュメ **(Entity Resume)**」画面に「**Centrifuge**」ボタンが表示されます。そのボタンをクリックすると、Visualizer から直接、Centrifuge Desktop アプリケーションが起動されます。

Visualizer クエリーの最小しきい値スコアの値の設定**:**

Visualizer で「解決による検索 (Find by Resolution)」機能または属性アラート・ジェネレーターを使用してエンティティーを検索するときは、基準の一部として最小相似スコアを選択します。この選択によって、システムがエンティティーを検索して返すときに使用するエンティティー解決および関係解決の強度が決まります。これらの 1 つ以上のしきい値のデフォルト値を Visualizer の「システム設定 **(System Preferences)**」タブで変更できます。

このタスクについて

これらの設定は、Visualizer クライアントごとに構成されます。このタスクを実行することで最小スコアしきい値が変更される対象は、現在ログインしている Visualizer のみです。

手順

1. Visualizer で、「ファイル **(File)**」 > 「設定 **(Preferences)**」 > 「システム設定 **(System Preferences)**」をクリックします。

2. 「最小スコア値 **(Minimum Score Values)**」セクションで、表示する検索結果を判別するために使用する最小相似スコアを指定します。 この数値が高いほど、エンティティー・データが検索基準により正確に一致しなければならないため、返される結果の数は減る可能性があります。
3. 「送信 **(Submit)**」をクリックします。 確認メッセージによって、変更を有効にするには Visualizer の再始動が必要なことが通知されます。
4. 確認メッセージで「**OK**」をクリックします。
5. Visualizer を閉じて、Visualizer を再オープンし、再度ログインします。

デフォルトの「アラート要約 **(Alert Summary)**」ウィンドウのフィルター・オプションの設定**:**

「システム設定 **(System Preferences)**」画面の「アラート表示フィルター設定 **(Alert Display Filter Settings)**」タブを使用して、「アラート要約 **(Alert Summary)**」ウィンドウのフィルター・オプションのデフォルト設定をカスタマイズします。

このタスクについて

これらの設定は、Visualizer の以下のデフォルト値を制御します。

- 「アラート・リスト **(Alert List)**」に表示されるアラートの最大数
- 表示するロール・アラートの最小関係スコア
- 表示するアラート要約の日数 (現在日付から過去にさかのぼる日数)

ここで設定する値によって、ユーザーが新しい「アラート要約 **(Alert Summary)**」ウィンドウを開くたびに Visualizer インスタンスが使用するデフォルトのフィルター値が決まります。

手順

1. Visualizer で、「ファイル **(File)**」 > 「設定 **(Preferences)**」 > 「システム設定 **(System Preferences)**」を選択します。
2. 「アラート表示フィルター設定 **(Alert Display Filter Settings)**」セクションの下で、「アラート・リストに表示する最大アラート数 **(Maximum alerts to display in alert list)**」に、「アラート・リスト **(Alert List)**」表に表示するアラートの最大数を表す数値を入力します。 デフォルト設定は 100 です。すなわち、アラート要約を選択すると、「アラート・リスト **(Alert List)**」には関連した最初の 100 件のアラートが表示されます。デフォルト設定を変更して、表示するアラートの件数を減らすこともできます。
3. 「最小関係スコア **(Minimum relationship score)**」で、ロール・アラートを表示するためのしきい値として使用する最低関係スコアを入力します。 関係スコアを高くするほど、表示されるロール・アラートおよびロール・アラート要約の数が減ります。
4. 「表示するアラートの日数 **(**今日を含む**) (Number of days of alerts to display (including today))**」に、表示するアラートの日数を示す 1 から 99 までの数値を入力します。 この数値は現在日付で始まり、後方にカウントされます。したがって、1 と入力した場合、その日に生成されたアラートのみが表示されます。10 と入力した場合は、合計 10 日分 (その日と前日 9 日分) のアラートのみが表示されます。デフォルト値は 99 です。

5. オプション: システム・アドミニストレーターが構成コンソールでアラートしきい値オーバーライドを有効にしていた場合は、「フィルターで除外されたロール・アラートを含める **(Include filtered role alerts)**」チェック・ボックスが表示されます。
   - 「フィルターで除外されたロール・アラートを含める **(Include filtered role alerts)**」チェック・ボックスを選択すると、ロール・アラート・ルールに定義されている最小アラートしきい値の範囲外にある関係スコアのものも含めて、すべてのロール・アラートおよびロール・アラート要約が「アラート要約 **(Alert Summary)**」ウィンドウに表示されます。
   - 「フィルターで除外されたロール・アラートを含める **(Include filtered role alerts)**」チェック・ボックスをクリアすると、最小アラートしきい値を満たす関係スコアを持つロール・アラートおよびロール・アラート要約のみが「アラート要約 **(Alert Summary)**」ウィンドウに表示されます。
6. 「送信 **(Submit)**」をクリックします。 確認メッセージによって、変更を有効にするには Visualizer の再始動が必要なことが通知されます。
7. 確認メッセージで「**OK**」をクリックします。
8. Visualizer セッションを閉じて、Visualizer を再始動し、再度ログインします。

Visualizer ログ・オプションの設定**:**

Visualizer ログ・オプションを構成することで、Visualizer クライアント・ロギングをオンまたはオフにすることができます。デフォルトでは、Visualizer クライアント・ロギングはオフです。一般に、ユーザーやアドミニストレーターによるトラブルシューティングを支援する場合にのみ Visualizer クライアント・ロギングをオンにします。

このタスクについて

これらの設定は、Visualizer クライアントごとに構成されます。このタスクを実行することでロギング・オプションが変更される対象は、現在ログインしている Visualizer のみです。

手順

1. Visualizer で、「ファイル」 > 「設定 **(Preferences)**」 > 「ログとリンクの設定 **(Log and Link Settings)**」をクリックします。
2. 「ロギングをオンにする **(Turn on logging)**」チェック・ボックスで、以下のいずれかのアクションを実行します。
   - Visualizer クライアント・ロギングをオンにする場合はチェック・ボックスを選択します。
   - Visualizer クライアント・ロギングをオフにする場合はチェック・ボックスをクリアします。
3. ロギングをオンにする場合は、「ログ詳細レベル **(Log detail level)**」でオプションを選択することによってロギングのタイプを指定します。 選択するレベルがわからない場合は、システム・アドミニストレーターに問い合わせてください。一般的には、問題のトラブルシューティングを行うときにのみ Visualizer クライアント・ロギングをオンにするので、通常はデバッグ・レベルを選択します。デバッグ・レベルでは、Visualizer 内でユーザーが行うすべてのアクション

と、発生したすべてのメッセージ (エラー、警告、および情報) がログに記録されます。このロギング・レベルでは、Visualizer ログ・ファイルがすぐにいっぱいになります。これは、定期的なファイルの削除が必要になる可能性があることを意味します。

4. 「ログ・ファイル・ディレクトリー・パス **(Log file directory path)**」で、以下のようにします。
   - Visualizer ログ・ファイルを保管するパスを入力します。
   - または、ディレクトリーを参照して選択します。
5. 「送信 **(Submit)**」をクリックします。 確認メッセージによって、変更を有効にするには Visualizer の再始動が必要なことが通知されます。
6. 確認メッセージで「**OK**」をクリックします。
7. Visualizer を閉じて、Visualizer を再始動し、再度ログインします。

カスタム属性を表示するための **Visualizer** ハイパーリンク・オプションの設定**:**

ユーザーの組織で、アイデンティティー・レコード属性の一部として他のシステム内にあるファイルまたは画像へのリンクが組み込まれている場合、Visualizer ではそれらのファイルへのハイパーリンクを表示できます。ハイパーリンクをクリックすると、Web ブラウザーまたはアプリケーションが起動され、選択されたファイルまたは画像が表示されます。Visualizer システム設定を使用して、ハイパーリンクをクリックしたときに、どのブラウザーまたはプログラムでファイルを開くか選択します。

このタスクについて

これらの設定は、Visualizer クライアントごとに構成されます。このタスクを実行することでハイパーリンク・オプションが変更される対象は、現在ログインしている Visualizer のみです。

手順

1. Visualizer で、「ファイル」 > 「設定 **(Preferences)**」 > 「ログとリンクの設定 **(Log and Link Settings)**」を選択します。
2. 「ハイパーリンク処理設定 **(Hyperlink Handling Settings)**」の下で、以下のいずれかのオプションを選択します。
   - 「デフォルトのブラウザー設定 **(Default browser setting)**」
   - または、「プログラムを使用 **(Use program)**」を選択し、ハイパーリンクを開くときに使用するブラウザーまたはプログラムを指定します。

   注**:** セキュアな Web サイト (https://) 上に保管されているリンクを開く場合にのみ、Web ブラウザーまたはその他のプログラムを指定する必要が生じる可能性があります。
3. 「送信 **(Submit)**」をクリックします。 確認メッセージによって、変更を有効にするには Visualizer の再始動が必要なことが通知されます。
4. 確認メッセージで「**OK**」をクリックします。
5. Visualizer を閉じて、Visualizer を再始動し、再度ログインします。

Visualizer グラフ・オプションの設定**:**

「グラフ設定 **(Graph Preferences)**」タブで色や線の太さを変更することで、Visualizer に表示されるグラフの設定をカスタマイズできます。

このタスクについて

Visualizer のグラフ表示設定は、Visualizer クライアントごとに構成されます。以下の手順を実行することで影響を受けるのは、現在ログインしている Visualizer クライアントの設定のみです。

手順

1. Visualizer で、「ファイル」 > 「設定 **(Preferences)**」 > 「グラフ設定 **(Graph Preferences)**」をクリックします。
2. 使用する線の太さおよび色を選択します。
3. 「送信 **(Submit)**」をクリックします。 確認メッセージによって、変更を有効にするには Visualizer の再始動が必要なことが通知されます。
4. 確認メッセージで「**OK**」をクリックします。
5. Visualizer を閉じて、Visualizer を再オープンし、再度ログインします。

タスクの結果

これで、選択した新しい表示オプションを使用して Visualizer がグラフを表示するようになります。

ヘルプ・トピック**:**

「ウィンドウ設定 ***(Window Preferences)***」タブ*:*

このタブを使用して、Visualizer セッションで、Visualizer が背景色、フォント、およびナビゲーション・アイコンを表示する方法を構成します。このタブで構成する設定は、ローカル Visualizer クライアントの設定のみに影響します。これらの設定のいずれかを変更した場合、Visualizer を終了し、再オープンし、ログインして変更を確認してください。

「外観 **(Look and Feel)**」
: 事前フォーマット設定された表示設定のグループを選択します。グループ表示設定は、「テーマ」、「フォント」、および「サイズ」で使用可能な選択項目を制御します。

  注**:** ほとんどの表示設定で、ユーザーがその他のいずれかのフィールドを選択することは許可されていません。現在、ユーザーがその他の表示設定を選択できるオプションは「メタル **(Metal)**」のみです。

  デフォルトのグループ表示設定は「**EAS Visualizer**」です。

テーマ
: 「外観 **(Look and Feel)**」で選択したグループ表示設定用の事前フォーマット設定された画面の色の組み合わせを選択します。

フォント
: 表示フォントを選択します。

サイズ
: フォント・サイズを選択します。

サンプル
: 選択された項目に基づいて、Visualizer の表示がどのようになるか例が表示されます。

背景色
: 背景色を選択するには、このボタンをクリックします。このフィールドは、「外観 **(Look and Feel)**」フィールドで「メタル **(Metal)**」を選択した場合にのみ使用できます。

「コントロールの色 **(Control color)**」
: コントロールのアウトライン色を選択する場合にクリックします。

「テキストの色 **(Text color)**」
: テキストの色を選択する場合にクリックします。

「システム設定 ***(System Preferences)***」タブ*:*

このタブを使用して、Visualizer セッションのシステム設定を構成します。ここで構成する設定は、ローカル Visualizer クライアントのシステム設定のみに影響します。これらの設定のいずれかを変更した場合、Visualizer を終了し、再オープンし、ログインして変更を確認してください。

「ファイル・パス **(File Paths)**」セクション
: UMF ファイルをロードしたり、Centrifuge Desktop グラフ・ツールを開いたりするために Visualizer が使用するデフォルトのファイル・パスを指定します。Centrifuge Desktop アプリケーションを使用してエンティティー・グラフやエンティティー・データを視覚化する場合、アプリケーションへの絶対パスを入力してください。ここに絶対パスを入力することにより、Visualizer から Centrifuge に直接アクセスできます。

「最小スコア値 **(Minimum Score Values**）」セクション
: 「解決による検索 (Find By Resolution)」クエリーまたは属性アラート・ジェネレーターを作成するときに選択できる最小相似スコアのしきい値を定義します。

  デフォルトで、このセクションには、これらのしきい値のそれぞれの推奨値が含まれています。これらの推奨値は、返される誤検出の件数を減らすために慎重な値になっています。これらの値は、ユーザーの目標に合わせて再定義できます。

  一般的に、最小スコアしきい値を高く設定するほど、返される結果は少なくなります。低い値を設定すれば、返される結果は増えます。

  「同一エンティティー **(Is Entity)**」
  : 「解決による検索 (Find By Resolution)」クエリーまたは属性アラート・ジェネレーターで定義された検索エンティティーとエンティティー・データベース内のエンティティーを同一エンティティーと見なすための条件を定義する最低解決スコアを入力します。

デフォルト値は 100 です。このデフォルトは、検索エンティティーとアイデンティティーが比較されたとき、解決スコアが 100 の場合に、返されるエンティティーは検索エンティティーと同じものであることを意味します。

「近似エンティティー **(Close Entity Match)**」

「解決による検索 (Find By Resolution)」クエリーまたは属性アラート・ジェネレーターで定義された検索エンティティーとエンティティー・データベース内のエンティティーの間に「近似」が存在すると見なすための条件を定義する最低解決スコアを入力します。

デフォルト値は 85 です。このデフォルトは、検索エンティティーとエンティティー・データベース内のエンティティーが比較されたとき、解決スコアが 85 以上ありながら、「同一エンティティー **(Is Entity)**」スコアを満たさない場合に、返されるエンティティーは検索エンティティーに近似したエンティティーであることを意味します。

「有効関係 **(Good Relationship)**」

「解決による検索 (Find By Resolution)」クエリーまたは属性アラート・ジェネレーターで定義された検索エンティティーとエンティティー・データベース内のエンティティーの間に近い関係または強力な関係が存在すると見なすための条件を定義する最低スコアを入力します。この値は、関係の強度を表します。

デフォルト値は 35 です。これは、検索エンティティーとエンティティー・データベース内のエンティティーが比較されたとき、最小解決スコアが 35 以上であれば、2 つのエンティティー間の関係は有効であることを意味します。

「任意の関係 **(Any Relationship)**」

「解決による検索 (Find By Resolution)」クエリーまたは属性アラート・ジェネレーターで定義された検索エンティティーとエンティティー・データベース内のエンティティーの間に何らかの関係が存在すると見なすための条件を定義する最低スコアを入力します。(この値は、関係の強度を表します。)

デフォルト値は 1 です。このデフォルトは、検索エンティティーとエンティティー・データベース内のエンティティーが比較されたとき、最小解決スコアが 1 以上であれば、2 つのエンティティー間に関係が存在することを意味します。

「アラート表示フィルター設定 **(Alert Display Filter Settings)**」セクション

このセクションを使用して、「アラート要約 **(Alert Summary)**」ウィンドウに表示されるアラート要約に影響するデフォルトのアラート・フィルター設定を構成します。ユーザーが新しい「アラート要約 **(Alert Summary)**」ウィンドウを開くとき、システムは毎回このデフォルト設定を使用します。

「アラート・リストに表示する最大アラート数 **(Maximum alerts to display in alert list)**」

「アラート要約 **(Alert Summary)**」ウィンドウの「アラート・リスト **(Alert List)**」表に表示するアラートの最大数を表す数値を入力します。

デフォルトのフィルター値は 100 であり、これはデフォルトでは、選択したアラート要約の最初の 100 アラートのみが表示されることを意味します。

「最小関係スコア **(Minimum relationship score)**」
未割り当てのロール・アラート要約をフィルタリングするための最低関係スコアを入力します。このスコアより低いものは「アラート要約 **(Alert Summary)**」ウィンドウでの表示から除外されます

例えば、比較対象の 2 つのエンティティー間の関係スコアが 50 以上のロール・アラート要約のみを表示するには、このフィールドに 50 と入力します。

デフォルトは 0 であり、ユーザー自身の Visualizer アナリスト・グループ向けのアラート要約のうち、現在「未割り当て」状況にあるすべてのアラート要約がデフォルトで表示されることを意味します。

「表示するアラートの日数 **(**今日を含む**) (Number of days of alerts to display (including today))**」
現在日付を起点に、表示するアラートの日数を示す 1 から 99 までの数値を入力します。この「日」とは、0:00:00 で始まり、23:59:59 で終了する暦日 (丸 1 日) を指すことを覚えておいてください。

この数値は現在日付で始まり、後方にカウントされます。過去 90 日間 (現在日とその前の 89 日間) に生成されたアラートを表示する場合は、90 と入力します。

デフォルト値は 99 であり、今日と今日より前の暦日 98 日間に生成されたアラートが表示されます。

「フィルターで除外されたロール・アラートを含める **(Include filtered role alerts)**」チェック・ボックス
(オプション) ロール・アラート・ルール構成で指定された最小アラートしきい値を下回るアラートまで含めて、生成されたすべての未割り当てロール・アラートを表示する場合、このチェック・ボックスを選択します。このチェック・ボックスは、システム・アドミニストレーターがこの機能を有効にした場合にのみ表示されます。

デフォルトではクリアが選択されます。すなわち、(ロール・アラート・ルールで定義された) 最小アラートしきい値を満たすか超える、現在未割り当てのロール・アラートのみが Visualizer に表示されます。

「各種設定」セクション
このセクションを使用して、吹き出しヘルプや終了確認ウィンドウを使用可能にします。

「ツールチップを使用可能にする **(Enable Tooltips)**」
ツールチップが使用可能である場合、ツールバー・アイコンの上や、追加情報が用意されているエリアの上にカーソルを移動すると、吹き出しヘルプが表示されます。デフォルトでは、ツールチップは使用可能です。

「終了確認ダイアログの表示**: (Show Exit Confirmation Dialog:)**」

このオプションにより、ユーザーが Visualizer を終了するときに、システムが確認ダイアログを表示するかどうかが決まります。

- Visualizer を終了するとき、毎回終了の選択を確認する場合、このチェック・ボックスを選択します。デフォルト設定では選択されています。
- Visualizer を終了してログアウトしようとするとき、毎回「終了確認 **(Exit Confirmation)**」ダイアログを表示せず Visualizer を終了するにはこのチェック・ボックスをクリアします。

「ログとリンクの設定 ***(Log and Link Settings)***」タブ***:***

このタブを使用して、Visualizer クライアントのロギングおよびハイパーリンクの設定を構成します。ここで構成する設定は、ローカル Visualizer クライアントの設定のみに影響します。これらの設定のいずれかを変更した場合、Visualizer を終了し、再オープンし、ログインして変更を確認してください。

「ログの設定 **(Log Settings)**」

Visualizer クライアント・ロギングをオンにする場合はこのチェック・ボックスを選択し、クライアント・ロギングをオフにする場合はこのチェック・ボックスをクリアします。一般的に、Visualizer クライアント・ロギングを有効にするのは、Visualizer セッションの中で発生したエラー・メッセージまたは問題をシステム・アドミニストレーターと協力して解決する場合に限られます。デフォルトでは、Visualizer クライアント・ロギングはオフです。

ログ詳細レベル

ロギング詳細のレベルを選択します。Visualizer クライアント・ロギングがオンの場合にのみ使用可能です。詳細レベルは、Visualizer を使用するときに Visualizer ログに収集される情報量を制御します。選択を行う前に、システム・アドミニストレーターに相談してください。一般的には、Visualizer で問題をトラブルシューティングするためにロギングをオンにします。したがって、通常はロギング詳細の最高レベルであるデバッグ・レベルを選択します。デバッグ・レベルでは、Visualizer の使用中に発生したすべてのアクションおよびメッセージがログに記録されます。しかし、同時にこのログ・レベルでは、Visualizer クライアント・ログ・ファイルがすぐにいっぱいになるため、ログ・ファイルを定期的にクリアすることをお勧めします。通常、問題が解決した時点でロギングをオフにするのはこのためです。

ログ・ファイル・ディレクトリー・パス

Visualizer クライアント・ログ・ファイルのファイルおよびディレクトリーの場所を指定します。通常、ログ・ファイルの確認が必要になるのは、メッセージまたは問題をトラブルシューティングするときに限られます。ログ・ファイルはすぐに情報でいっぱいになります。デバッグ・レベルでは特にそうです。Visualizer クライアント・ロギングをオンにする場合は、ファイルが大きくなりすぎないように、定期的にログ・ファイルをパージする必要があります。

「ハイパーリンク処理設定 **(Hyperlink Handling Settings)**」

Visualizer がハイパーリンクを開いて表示するために使用するプログラムまたはブラウザーを決定するオプションを選択します。入力アイデンティティー・レコードには、分析に関係するアイデンティティーまたはエンティティーの情報を含んでいるその他のファイル、Web サイト、またはシステムへとユーザーを誘導する、ハイパーリンクが含まれていることがあります。ハイパーリンクは、アイデンティティー・レコードの一部であり、エンティティー・レジュメやエンティティー解決のグラフ上に属性として表示されます。

ハイパーリンクをクリックしたときに問題が発生した場合、「プログラムを使用 **(Use program)**」オプションを選択し、ハイパーリンクを開くために使用するブラウザーまたはプログラムを指定してください。例えば、ユーザーの組織が指紋ファイルをセキュア Web サイト (https://) 上に保管している場合、このオプションを使用して、指紋ファイルがあるセキュア・サイトにアクセスするリンクを開くための Web ブラウザーまたはその他のプログラムを指定します。

「グラフ設定 ***(Graph Preferences)***」タブ*:*

このタブを使用して、Visualizer のグラフ上でエンティティー同士を接続する線の表示プロパティーを指定します。ここで構成する設定は、ローカル Visualizer クライアントの設定のみに影響します。これらの設定のいずれかを変更した場合、Visualizer を終了し、再オープンし、ログインして変更を確認してください。

「線の太さ **(Line Thickness)**」

線の太さを選択します。デフォルトの線の太さは 2 ピクセルです。

「線の色 **(Line Color)**」

線の色を選択します。デフォルトの線の色はミディアム・ブルーです。

「線のサンプル **(Sample Line)**」

選択した内容に基づいたサンプル・グラフ線が表示されます。

Visualizer の開始

Visualizer を使用してエンティティー・データベース内のエンティティーやエンティティー・データを表示するには、最初に Visualizer を開始し、ログインする必要があります。

Visualizer を開始するために、システムのデフォルト・バージョンの Java によって、製品アプリケーション・サーバーがユーザーのワークステーション・クライアントにダウンロードした Java Web Start JNLP (Java Network Launch Protocol) ファイルが処理されます。JNLP ファイルはさまざまな方法でアクセスすることができます。ただし、Visualizer を正常に開くためには、必要なクライアント・バージョンの Java Web Start が JNLP ファイルを開く必要があります。

クライアント・マシンに複数のバージョンの Java がインストールされている場合、システムのデフォルト・バージョンの Java Web Start が、必要なクライアント・バージョン以外のバージョンに設定されていることがあります。この場合も

Visualizerを正常に開いて実行できます。ただし、まず、必要なクライアント・バージョンの Java Web Start を使用するように Web ブラウザーを構成する必要があります。

注: Visualizer を開いて実行するために必要なクライアント Java バージョンは、Java の最新バージョンであるとは限りません。

Visualizer へのログイン

Visualizer にログインするためには、Visualizer ユーザー・アカウント (ユーザー名とパスワード) が必要です。Visualizer ユーザー・アカウント情報はシステム・アドミニストレーターから入手できます。

手順

1. 以下のいずれかのステップを実行します。
   - デスクトップ上にある Visualizer アイコンをダブルクリックします。
   - インターネット・ブラウザーを開き、アドレス行に Visualizer の Uniform Resource Locator (URL) を入力します。

   Visualizer を起動するための URL は以下のとおりです。

   `http://server:install_port`

   例えば、`http://localhost:13510` です。Visualizer のインストール時、デフォルトの *install_port* は 13510 ですが、ポート番号は変更可能です。正しいサーバー名またはポート番号が不明な場合は、システム・アドミニストレーターに問い合わせてください。
2. ユーザー名とパスワードを入力してログインします。

   注: ユーザー名およびパスワードの両方のフィールドが大/小文字を区別します。最初にログインするときは、システム・アドミニストレーターから割り当てられたパスワードを使用してください。最初のログインが成功した後、通常は、Visualizer アカウントのセキュリティーを保護するために Visualizer パスワードを変更します。
3. 「ログイン **(Login)**」をクリックします。

必要な **Java Web Start** のクライアント・バージョンを使用するための **Web** ブラウザーの設定:

ワークステーションに複数のバージョンの Java が含まれており、Visualizer を開くときに問題がある場合、必要な Java Web Start のクライアント・バージョンを選択するように Web ブラウザー設定を変更できます。そうすれば、Web ブラウザーは、必要な Java Web Start のクライアント・バージョンを自動的に使用して、毎回 Visualizer を正常に開くようになります。

必要な ***Java Web Start*** を使用するための ***Microsoft Windows Internet Explorer*** の設定:

Microsoft Internet Explorer は、Microsoft Windows オペレーティング・システムに定義されているデフォルトのファイルの関連付けを使用して、JNLP (Java Network Launch Protocol) ファイルの処理方法を判断します。JNLP ファイルの処理に関連付けられるデフォルトのファイル・アプリケーションを定義または変更す

ることで、正しい Java Web Start バージョンを使用するように Internet Explorer をリダイレクトできます。複数のバージョンの Java がインストールされている場合、この設定を変更することで、Visualizer を開く際の問題を回避できることがあります。

このタスクについて

この手順は、Web アプリケーションを開始するときはすべて Java Web Start バージョンを使用するように Internet Explorer を誘導します。これより後のバージョンの Java を必要とするその他の Web Start アプリケーションを実行している場合は、代わりに直接起動アプローチを使用してください。

注**:** Java バージョン 1.6 には、留意すべき既知の問題がいくつかあります。

- Java バージョン 1.6 は、JNLP ファイルに対するデフォルトの Windows のファイルの関連付けをオーバーライドすることがあります。システム JVM (Java 仮想マシン) として Java バージョン 1.6 を使用している場合に、下記のステップに従っても Visualizer を正常に開始および開くことができなければ、代わりに、別の Web ブラウザーを使用して Visualizer を起動してみるか、直接起動アプローチを使用してください。
- ワークステーションで Java バージョン 1.6 を使用している場合、自動ダウンロードを受け入れるための JRE (Java ランタイム環境) の構成が必要になることもあります。ワークステーションにこの問題がある場合、Visualizer を開始しようとすると、ローカルにインストールされていない JRE のバージョンをアプリケーションが要求していることを示すエラー・メッセージが表示されます。

手順

1. Windows の「コントロール パネル」から、以下のいずれかのステップを実行します。
   - カテゴリー・ビューで、「パフォーマンスとメンテナンス」をダブルクリックします。ウィンドウの左上隅にある「関連項目」ナビゲーション・ペインから「ファイルの種類」を選択します。
   - クラシック表示で、「フォルダ オプション」をダブルクリックします。
2. 「フォルダ オプション」ダイアログで、「ファイルの種類」タブをクリックします。
3. 「拡張子」列の下で、「**JNLP**」エントリーを見つけて選択します。 エントリーは拡張子のアルファベット順に並んでいます。

   注**:** JNLP エントリーが存在しない場合は、「新規」をクリックしてエントリーを作成してください。
4. 「変更」をクリックします。
5. 「プログラムから開く」ダイアログで、「**Java WebStart Executable**」が選択されていることを確認します。「参照」をクリックして、インストールされている Java ディレクトリーにナビゲートします。
6. `javaws` という名前の実行可能ファイルを選択し、「**OK**」をクリックします。
7. 「**OK**」をクリックして、「フォルダ オプション」ダイアログを閉じます。 (「コントロール パネル」ウィンドウも閉じてかまいません。)

タスクの結果

これで、Internet Explorer は関連付けられた Java Web Start ファイルを使用して、Visualizer を正常に処理して開きます。

必要な ***Java Web Start*** を使用するための ***Mozilla Firefox*** の設定**:**

Mozilla Firefox が JNLP (Java Network Launch Protocol) ファイルを扱う方法を設定または変更することで、必要なクライアント Java Web Start バージョンを自動的に使用して Visualizer を開始するように Firefox を誘導できます。複数のバージョンの Java がインストールされている場合、この設定を変更することで、Visualizer を開く際の問題を回避できることがあります。

このタスクについて

この手順は、Web アプリケーションを開始するときはすべて Java Web Start バージョンを使用するように Firefox を誘導します。これより後のバージョンの Java を必要とするその他の Web Start アプリケーションを実行している場合は、代わりに直接起動アプローチを使用してください。

手順

1. Mozilla Firefox を起動します。
2. 「ツール」 > 「オプション」を選択します。
3. 「プログラム」を選択します。
4. 「ファイルの種類 **(Content Type)**」の下で、「**JNLP File**」のエントリーを見つけます。

   注**:** 「**JNLP File**」のエントリーが表示されない場合は、「オプション」ダイアログを閉じてください。 Visualizer Web Start ページから、「**IBM Identity Insight Visualizer** を開始するにはここをクリック **(Click here to start the IBM Identity Insight Visualizer)**」リンクをクリックして Visualizer を開始してみてください。次に、ステップ 1 から再度開始します。
5. 「**JNLP File**」エントリーを選択します。
6. 「取り扱い方法」の下で、「他のプログラムを選択」オプションを選択します。
7. 「ヘルパーアプリケーションを選択してください」ダイアログで、「参照」をクリックし、必要なクライアント Java バージョンがインストールされているディレクトリーにナビゲートし、`javaws` 実行可能ファイルを選択します。
8. 「**OK**」をクリックして、「ヘルパーアプリケーションを選択してください」ダイアログを閉じます。
9. 「**OK**」をクリックして、「オプション」ダイアログを閉じます。

タスクの結果

これで、Mozilla Firefox は、選択された Java Web Start ファイルを使用して、すべての JNLP ファイル・タイプを処理します。Visualizer は正常に開かれます。

Java Web Start 実行可能ファイルから **Visualizer** を直接開始する**:**

Java またはその他のシステム設定を変更せずに Visualizer を開始する必要がある場合、直接起動アプローチを使用できます。このアプローチは、Java Web Start 実行可能ファイルから直接、Visualizer を起動します。ワークステーションに複数のバージョンの Java がインストールされていて、Visualizer 以外の Web Start アプリケーションも使用している場合、直接起動アプローチを使用することをお勧めします。

始める前に

ワークステーション上の必要な Java Web Start 実行可能ファイル (`javaws`) へのパスを見つけます。

このタスクについて

また、`javaws` ファイルを選択し、「ターゲット **(Target)**」フィールドに Visualizer への URL を入力することで、Java Web Start 実行可能ファイルへのショートカットをデスクトップ上に作成することもできます。

手順

1. デスクトップから、DOS コマンド・ウィンドウを開きます。
2. コマンド行で、次の直接起動コマンドを入力します:
   path_to_Java_installationpath_to_javaws_exe_file`>javaws.exe` *URL for the Visualizer* 例えば、**C:/IBM/Java60/jre/bin>javaws.exe http://localhost:13510/docs/rrmdi.jnlp** です。

   重要**:** Java Web Start 実行可能ファイル拡張子と URL の間のスペースに注意してください。

タスクの結果

Visualizer は正常に開かれます。

Microsoft Windows ワークステーション上で **Visualizer** を実行するための **Java v1.6** の構成**:**

Visualizer を開始しようとしたときに、ローカルにインストールされていない JRE のバージョンをアプリケーションが要求していることを示すエラー・メッセージが表示された場合、Java の自動ダウンロード設定を変更してみてください。このエラー・メッセージは、Java バージョン 1.6 がインストールされている Microsoft Windows ワークステーションでの既知の問題です。

手順

1. Windows の「コントロール パネル」から、以下のいずれかのオプションを選択します。
   - IBM Java のインストール済み環境の場合、「**IBM Java** コントロール・パネル」を選択します。
   - Sun Java のインストール済み環境の場合、「**Java**」を選択します。

2. 「詳細」タブで、「**JRE** 自動ダウンロード」設定を展開します。 このオプションが表示されず、さらにこのワークステーションに複数のバージョンの Java がインストールされている場合、「**Java** コントロール・パネル」を閉じ、他の項目を選択してください。
3. 「**JRE** 自動ダウンロード」設定が「常に自動ダウンロード」 (推奨) または「ユーザーに尋ねる」のいずれかに設定されていることを確認します。 「自動ダウンロードしない」設定だと、Visualizer と構成コンソールのオープンが禁止されます。
4. 「適用 **(Apply)**」をクリックします。
5. 「**OK**」をクリックします。
6. 「コントロール パネル」ウィンドウを閉じます。

Visualizer の終了

Visualizer の使用が終了したら、アプリケーションを閉じます。 Visualizer を閉じることによって、ユーザーはログアウトされます。休憩を取る際など、数分間のみワークステーションを保護する必要がある場合は、代わりに Visualizer をロックできます。

手順

Visualizer を終了し、ログアウトするには、以下のようにします。

- 「ファイル **(File)**」 > 「終了 **(Exit)**」を選択します。
- または、**Ctrl** + **Q** を押します。

Visualizer のロック

短い休憩を取る場合またはワークステーションから数分離れる場合、Visualizer を閉じてログアウトする代わりに、Visualizer をロックできます。Visualizer をロックすると、保護されたスクリーン・セーバーのような役割を果たすことになり、ユーザーの作業を保護できます。Visualizer をロックした場合は、「ログイン」ウィンドウが表示されます。ユーザー・パスワードを入力することで、Visualizer セッションに戻ることができます。

手順

Visualizer をロックするには、以下のようにします。

- 「ファイル」 > 「アプリケーションのロック **(Lock application)**」を選択します。
- または、**Ctrl** + **L** を押します。

タスクの結果

これで、Visualizer セッションは安全にロックされました。

次のタスク

Visualizer の使用を再開するには、パスワードを入力し、「アンロック **(Unlock)**」をクリックします。

Visualizer のパスワードの変更

Visualizer のパスワードを定期的に変更することは、Visualizer ユーザー・アカウントのセキュリティーを保護するための良い方法です。

始める前に

パスワードを変更するには、Visualizer にログインする必要があります。

このタスクについて

Visualizer のパスワードに必要な最小文字数はありません。文字 (大文字または小文字)、特殊文字、および数字の任意の組み合わせを使用できます。パスワードには大/小文字の区別があります。ログイン時に入力するパスワードは、Visualizer アカウントのパスワードと一致しなければなりません。例えば、パスワードが `PASSw0rd` の場合に `passw0rd` を使用してログインしようとすると、パスワードが一致していないため、エラー・メッセージが表示されます。

手順

1. Visualizer で、「ファイル」 > 「パスワードの変更 **(Change password**）」をクリックします。
2. 「現行パスワード **(Current password)**」に、今回の Visualizer セッションにログインするために使用したパスワードを入力します。 このパスワードが、割り当てられたパスワードまたは再設定されたパスワードである場合、このパスワードはシステム・アドミニストレーターから提供されたパスワードです。
3. 「新規パスワード **(New password)**」に、Visualizer のパスワードにする新規パスワードを入力します。
4. 「新規パスワードの再入力 **(Repeat new password)**」に、今、「新規パスワード **(New password)**」に入力したのと同じパスワードを入力します。
5. 「パスワードの変更 **(Change password)**」をクリックします。

タスクの結果

- 「新規パスワード **(New password)**」と「新規パスワードの再入力 **(Repeat new password)**」の両方の入力が一致していれば、パスワードが変更されたことを示すメッセージが表示されます。「**OK**」をクリックします。次回 Visualizer にログインするときは、新規パスワードを使用してください。
- 入力が一致していない場合は、システムによって、新規パスワードが一致していないことを示すエラー・メッセージが表示されます。「**OK**」をクリックします。パスワードは変更されていません。パスワードを変更するには、再度ステップ 2 から開始してください。

Visualizer でのアラートの分析

Visualizer ユーザーが実行する最も一般的なタスクの 1 つは、アラートを評価して、レビューを行うアラートと他の Visualizer グループに委任するアラートとを判別することです。

アラートは、Visualizer の「アラート要約 **(Alert Summary)**」ウィンドウに表示されます。このウィンドウは、アラートの評価、割り当てまたは委任、およびレビューを行う場合の開始点となります。

アラートは、アラート要約にグループ化されます。アラート要約には、同じ説明、アラート重大度、状況、解決ルール、関係スコア、および解決 (相似) スコアを持つ同じアラート・タイプのアラートがすべて含まれます。通常、1 つのアラート要約に個別のアラートが複数含まれ、それぞれのアラートがレビューと分析を必要とします。レビューの一部に、アラートへの後処理の割り当てがあります。これにより、ユーザー自身やその他の Visualizer ユーザーが分析の状況を把握できるようになり、調査結果を示すコメントも確認できます。

「アラート要約 **(Alert Summary)**」ウィンドウには、以下の項目のみが表示される点に注意してください。

- ユーザー自身の Visualizer アナリスト・グループ向けの、未割り当てアラートを含んだアラート要約
- ユーザーがすでに自身に割り当て済みのアラート

ユーザーの Visualizer アナリスト・グループに属しているその他のアナリストが彼ら自身に割り当てたアラートは、ユーザーには表示されません。他の Visualizer アナリスト・グループに割り当てられているアラートも表示されません。

アラート要約の評価

分析を行うために自分自身に割り当てるアラートを決定します。そのためには「アラート要約 **(Alert Summary)**」ウィンドウでアラート要約を確認することから始めます。アラート要約を見るときは、そのアラート要約を構成する情報の重要度と自身の分析目標とを比較します。決定するためには、アラート情報の 1 つ以上の部分の評価が必要になることがあります。

アラート要約の優先順位付けに役立つヒント

- アラート重大度**:** アラート要約を重大度でソートするところから開始します。「アラート重大度 **(Alert Severity)**」列見出しをクリックします。分析を開始するうえで、この情報があれば最も重大または重要なアラートを判別するのに十分な場合もあります。例えば、ユーザーの組織で、重大度がクリティカルのアラートに対して「C」を使用している場合、単にアラートの重大度を見れば、どのアラートが重大かすぐに把握できます。
- アラート説明**:** 重大度のみでは情報が十分でない場合があります。同じアラート重大度を持つアラート要約が複数存在する場合、優先順位においてリストの上位にくるアラートを選択するのにアラート説明が役立つ可能性があります。例えば、「搭乗者が従業員を知っている」という説明でグループ化されているアラートよりも「搭乗禁止対象者が搭乗者を知っている」という説明でグループ化されているアラートを分析するほうがより重要であると考えられます。
- 相似スコアと関係スコア**:** これらのスコアが高いほど、関心のある関係が存在する可能性またはアイデンティティーとエンティティーが同一である可能性も高くなります。「搭乗禁止対象者が搭乗者を知っている」の例の場合、相似スコアと関係スコアの両方が 100 であれば、搭乗禁止リストに記載されている人物はその搭乗者であり、すぐにアクションを取る必要があります。相似スコアが 70 未満、関係スコアが 85 未満の場合、このアラートは、やはり重要である可能性はありますが、クリティカルではないと考えられます。この場合もアラートに含まれるエンティティーを分析することをお勧めしますが、すぐにアクションを実行する必要はない可能性もあります。

Visualizer ユーザーは、組織の目標についてよく理解していることから、アラートに優先順位を付けるときに使用する個人的な要素を独自に追加できます。作業を開始するにあたって、以下のヒントを参考にしてください。

アラートの割り当て

優先順位に基づいて、作業が必要なアラートが分かったら、それらのアラートをユーザー自身に割り当てることができます。アラートを割り当てることで、ユーザーの Visualizer アナリスト・グループが着信アラートのリストを分割統治できるようになります。ユーザー自身に割り当てられたアラートは、自身の「アラート要約 (Alert Summary)」ウィンドウのみに表示され、同じアラートを別の Visualizer ユーザーが重複して作業するのを防ぎます。自分が専任で現在調査しているアラートをすぐに確認できます。

別の Visualizer アナリスト・グループに属すものと思われる 1 つ以上のアラートが自分の「アラート要約 (Alert Summary)」ウィンドウに表示された場合は、それらのアラートを委任できます。例えば、ユーザーは予約担当者であり、新しい予約または変更された予約によって生成されたアラートを評価しているとします。そこに、セキュリティーが扱うアラートがリストされたとします。この場合、そのアラートはセキュリティー・グループの管轄であるため、アラートをセキュリティー・グループに割り当てることができます。

アラートのレビューと後処理

自分自身に 1 つ以上のアラートを割り当てると、それらのアラートを調査および分析する業務に取り掛かることができます。Visualizer には、そのタスクを容易にする「調査 (Research)」ウィンドウがあります。アラートに関連する必要なすべての情報が、この 1 つのウィンドウに表示されます。「調査 (Research)」ウィンドウから、分析の一環として以下のタスクを実行できます。

- アラート詳細を確認する
- 関連エンティティーのエンティティー・レジュメを見る
- 関連付けられたエンティティー・グラフまたはアラート・グラフを表示して、アラートの一部であるエンティティーや属性の共通点を視覚化および検討する
- 分析の調査結果を示すコメントを追加する
- 分析の進行に伴いアラートの状況を変更する (後処理)

属性アラート

属性アラートは、属性アラート・ジェネレーターによって生成されるアラートです。属性アラート・ジェネレーターは、エンティティー・データベース内で特定の属性またはアイデンティティーを検索する永続システム・クエリーを作成します。エンティティーの属性が属性アラート・ジェネレーターの基準に一致するたびに、システムによって属性アラートが作成されます。

Visualizer ユーザーは、ユーザー個人用の属性アラート・ジェネレーターを独自に作成します。特定の属性のセットに一致する特定のアイデンティティーまたは任意のアイデンティティーかエンティティーを探している場合、指定された有効期限まで一致を検索する、ユーザー個人用の属性アラート・ジェネレーターを独自に作成できます。

通知が必要になる可能性があるエンティティー属性の例を以下に示します。

- 名前とユニーク番号 (クレジット・カード番号など)
- 名前と電話番号
- 住所
- 名前と非ユニーク番号

属性アラート・ジェネレーターの構成と表示には、Visualizer を使用します。作成した属性アラート・ジェネレーターは、作成した本人のみが使用できます。

住所属性アラートの例

「675 Hickory Street Las Vegas, NV」という住所を監視しているとします。エンティティー・データベースに追加される入力アイデンティティー・レコードにその住所が関連づけられている場合に属性アラートを作成するように、属性アラート・ジェネレーターを構成できます。

イベント・アラート

イベント・アラートは、1 つ以上の複合イベントが、指定の存続期間にわたって設定基準を満たす場合に発生します。イベント・アラートは、イベント・ルール・ファイル (`cep.xml`) に含まれている複合イベントのビジネス・ルールやその他の構成に基づいています。アラートは、例えば、「過去 1 時間以内に相互に 200 マイル離れた場所で 10,000 米ドルを超える購入トランザクションが複数発生した」という、関心のある状態を示している場合があります。

ロール・アラート

ロール・アラートは、関係を通してリンクされている 1 つのエンティティーまたは 2 つのエンティティーが、構成されているロール・アラート・ルールを満たすか上回ったことを識別します。ロール・アラートは、構成されているロールとロール・アラート・ルールに基づいています。それらは、警告または問題 (「顧客が問題人物を知っている」など) を示していることもあれば、単純に関心のある関係 (「顧客が従業員を知っている」など) を示していることもあります。

単一エンティティー内に存在すべきでないロールまたは 1 つ以上のエンティティー間でリンクされてはならないロールを識別するロール・アラート・ルールを構成することで、関心のある 関係または 競合 とする関係を定義します。構成コンソールを使用して、ロール・アラートのフィルターを構成します。このフィルターで、新しい情報 (新規アイデンティティーまたは新規データ・ソース・コードなど) がある場合に、システムが再度アラートを発行するかどうかを決定します。

エンティティー解決時、パイプラインによって、入力アイデンティティーと候補リストにあるエンティティーの間の関係が評価されます。システムは、入力アイデンティティーと候補エンティティーの間に関係が存在するかどうかを判別してから、割り当てられているロールが構成済みのロール・アラート・ルールを満たしているかどうかを評価します。満たしている場合、システムはロール・アラートを生成します。

ロール・アラートが識別するエンティティー・データはロール・アラート作成時のものです。ロール・アラートの詳細画面には、ロール・アラートが作成されたときのエンティティー・データが当時のまま示されます。エンティティー・データは時

間とともに変化するため、エンティティー・レジュメには最新のエンティティー・データが含まれます。特定のエンティティーの現在のデータを表示する必要がある場合は、エンティティー・レジュメを表示してください。

ロール・アラートは Analyst ツールキットのコンポーネント (Cognos Report、i2 用の Identity Insight プラグイン、および Identity Insight エクスプローラー) で表示および処理できます。

アラートの表示

「アラート要約 **(Alert Summary)**」ウィンドウでアラートを表示して、どのアラートを分析するか、またどのアラートを自分自身に割り当てて、どのアラートを別の Visualizer アナリスト・グループに委任するかを評価します。その後、自分自身に割り当てたアラートの調査と後処理を開始できます。

このタスクについて

ユーザー自身の「アラート要約 **(Alert Summary)**」ウィンドウに表示されるアラートには、以下が含まれます。

- 分析のために自分自身に割り当てたアラート。
- ユーザー自身の Visualizer アナリスト・グループ向けの未割り当てアラート。
- ユーザー自身の属性アラート・ジェネレーターのいずれかによって生成された属性アラート。

未割り当てのアラート要約は、「画面設定の構成 **(Configure Screen Preferences)**」ウィンドウの「システム設定 **(System Preferences)**」タブで構成される、「アラート要約 **(Alert Summary)**」ウィンドウのデフォルトのアラート表示フィルター値に基づいてフィルタリングされます。「表示フィルター **(Display Filters)**」グループ・ボックスで、1 つ以上のアラート表示フィルター値を変更できます。

手順

1. 「表示 **(View)**」 > 「アラート要約 **(Alert Summary)**」を選択します。
2. 次に、表示するアラートのタイプを選択するか、「すべてのアラート・タイプの表示 **(Show All Alert Types)**」を選択します。

タスクの結果

「アラート要約 **(Alert Summary)**」ウィンドウから、処理するアラートを決定できます。アラートを自分自身に割り当てるか、アラートを別の Visualizer アナリスト・グループに委任することができます。自分自身に割り当てたアラートは、分析のために選択でき、自身の分析に関するコメントを追加できます。

「アラート要約 (Alert Summary)」ウィンドウに表示されるアラートのフィルタリング

「アラート要約 **(Alert Summary)**」ウィンドウでアラートを確認する際、「表示フィルター **(Display Filters)**」グループ・ボックスの値を変更することで、表示するアラート要約をフィルタリングできます。表示フィルターは、現在「未割り当て」状況にあるアラート要約にのみ影響します。

このタスクについて

これらのアラート・フィルターのデフォルト値は、「画面設定の構成 **(Configure Screen Preferences)**」ウィンドウの「システム設定 **(System Preferences)**」タブで構成されます。「アラート要約 **(Alert Summary)**」ウィンドウでアラート表示フィルターを変更すると、それらのデフォルト値を一時的にオーバーライドすることになります。次回、新しい「アラート要約 **(Alert Summary)**」ウィンドウを開くと、フィルターはそれぞれのデフォルト値に戻っています。

手順

1. 「アラート要約 **(Alert Summary)**」ウィンドウで、「表示フィルター **(Display Filters)**」グループ・ボックス・ツイスティーを開きます。
2. 1 つ以上のアラート表示フィルターに変更を加えます。
3. 「適用」をクリックして「アラート要約 **(Alert Summary)**」ウィンドウを最新表示し、指定したアラート・フィルターを適用します。

自分自身へのアラートの割り当て

アラートを自分自身に割り当てることで、そのアラートのレビュー、調査、および後処理に関する責任を負います。自分自身にアラートを割り当てると、そのアラートは自身の「アラート要約 **(Alert Summary)**」ウィンドウのみに表示されることになり、自身のアラートを識別しやすくなります。

手順

1. Visualizer の「アラート要約 **(Alert Summary)**」ウィンドウで、「アラート要約 **(Alert Summary)**」表から、未割り当てのアラート要約をクリックします。アラート要約には、同じ説明、状況、解決ルール、相似スコア、および関係スコアを共有する 1 つ以上のアラートが、アラート・タイプ別にグループ化された状態で含まれています。
2. 「アラート・リスト **(Alert List)**」表で、自分自身に割り当てるアラートをダブルクリックします。
3. 「調査 **(Research)**」ウィンドウで、「状況の設定 **(Set Status)**」をクリックします。
4. 「状況の設定 **(Set Status)**」で、以下のアクションを実行します。
   a. 「実行するアクションを選択してください **(Select the action you want to perform)**」で、「状況の設定 **(Set Status)**」を選択します。 対応するアクティビティー・コードが「アクティビティー・コードの選択 **(Select Activity Code)**」に表示されます。
   b. 必須: 「状況の選択 **(Select Status)**」で、「割り当て済み **(Assigned)**」を選択します。 別の状況を選択すると、アラートは自分自身に割り当てられません。
   c. オプション: 別のアクティビティー・コードを割り当てるには、「アクティビティー・コードの選択 **(Select Activity Code)**」からそのコードを選択します。 選択する必要があるアクティビティー・コードが表示されない場合は、システム・アドミニストレーターに連絡して、アクティビティー・コードの構成を手配してください。

d. 「コメント **(Comments)**」テキスト・ボックスにコメントまたはメモを入力します。 例えば、状況を変更した理由についてのコメントを入力したり、このアラートの分析に関するメモを組み込んだりできます。

e. 「**OK**」をクリックして変更内容を保存します。

タスクの結果

これで、ウィンドウを最新表示すると、アラートの割り当て済みの状況が反映され、アラートが自身の「アラート要約 **(Alert Summary)**」ウィンドウのみに表示されるようになります。Visualizer アナリスト・グループ内の他のアナリストがそれぞれの「アラート要約 **(Alert Summary)**」ウィンドウを最新表示すると、そこにこのアラートは表示されなくなります。

他のアナリスト・グループへのアラートの割り当て

アラートを別の Visualizer アナリスト・グループに割り当てる必要があると判断した場合、そのアラートを委任できます。アラートを特定の Visualizer ユーザーに委任することはできませんが、そのユーザーが属する Visualizer アナリスト・グループにそのアラートを委任することはできます。

手順

1. Visualizer の「アラート要約 **(Alert Summary)**」ウィンドウで、「アラート要約 **(Alert Summary)**」表から、該当のアラートが関連付けられているアラート要約をクリックします。
2. 「アラート・リスト **(Alert List)**」表で、委任するアラートをダブルクリックします。
3. 「調査 **(Research)**」ウィンドウで、「状況の設定 **(Set Status)**」をクリックします。
4. 「状況の設定 **(Set Status)**」で、以下を実行します。
   a. 「実行するアクションを選択してください **(Select the action you want to perform)**」から、「アラートの委任 **(Transfer Alert)**」を選択します。
   b. 「アラートの委任先 **(Transfer Alert to)**」で、アラートを委任する Visualizer アナリスト・グループを選択します。 選択する必要がある Visualizer アナリスト・グループが表示されない場合は、システム・アドミニストレーターに連絡して、アナリスト・グループの構成を手配してください。 対応するアクティビティー・コードが「アクティビティー・コードの選択 **(Select Activity Code)**」に表示されます。
   c. オプション: 別のアクティビティー・コードを割り当てるには、「アクティビティー・コードの選択 **(Select Activity Code)**」からそのコードを選択します。 選択する必要があるアクティビティー状況コードが表示されない場合は、システム・アドミニストレーターに連絡して、アクティビティー・コードの構成を手配してください。
   d. 「コメント **(Comments)**」テキスト・ボックスにコメントまたはメモを入力します。 例えば、アラートを委任する理由についてのコメントを入力できます。
   e. 「**OK**」をクリックすると委任が完了します。

タスクの結果

これで、アラートは選択された Visualizer アナリスト・グループに委任され、その Visualizer アナリスト・グループのアナリストの「アラート要約 **(Alert Summary)**」ウィンドウに表示されます。(そのグループのアナリストは、まず「アラート要約 **(Alert Summary)**」ウィンドウを最新表示する必要がある可能性があります。)「アラート要約 **(Alert Summary)**」ウィンドウが最新表示された後は、ユーザー自身を含め、ユーザー自身の Visualizer アナリスト・グループに属すアナリストの「アラート要約 **(Alert Summary)**」ウィンドウにこのアラートは表示されなくなります。

アラートの状況の変更

ユーザー自身またはユーザー自身の Visualizer アナリスト・グループに割り当てられているアラートを分析する際、Visualizer を使用して、自身が行った調査、コメント、およびアラートの後処理方法を追跡できます。

このタスクについて

ユーザー自身またはユーザー自身の Visualizer アナリスト・グループに割り当てられているアラートのアラート状況はいつでも更新できます。また、いつでもこれらのアラートにコメントを追加することもできます。ただし、既存のコメントを編集することはできません。

手順

1. Visualizer から、「アラート要約 **(Alert Summary)**」ウィンドウの「アラート要約 **(Alert Summary)**」表で、更新対象のアラートを含んでいるアラート要約をクリックします。
2. 「アラート・リスト **(Alert List)**」から、状況を変更するアラートをダブルクリックします。
3. 「調査 **(Research)**」ウィンドウで、「状況の設定 **(Set Status)**」をクリックします。
4. 「状況の設定 **(Set Status)**」で、以下を実行します。
   a. 「実行するアクションを選択してください **(Select the action you want to perform)**」から、「状況の設定 **(Set Status)**」を選択します。 対応するアクティビティー・コードが「アクティビティー・コードの選択 **(Select Activity Code)**」に表示されます。
   b. オプション: 別のアクティビティー・コードを割り当てるには、「アクティビティー・コードの選択 **(Select Activity Code)**」からそのコードを選択します。 選択する必要があるアクティビティー状況コードが表示されない場合は、システム・アドミニストレーターに連絡して、アクティビティー・コードの構成を手配してください。
   c. 「コメント **(Comments)**」にコメントまたはメモを入力します。 例えば、状況を変更した理由を示すコメントを入力したり、このアラートの分析に関するメモを組み込んだりできます。
   d. 「**OK**」をクリックして変更内容を保存します。

タスクの結果

これで、「アラート要約 **(Alert Summary)**」ウィンドウにアラートの新しい状況が反映されます。

属性アラートに対する最も新しい状況更新またはコメント更新が、「状況要約 **(Status Summary)**」セクションの先頭に表示されます。

自分自身への属性アラートの割り当てが原因で状況の変更が発生している場合は、最新表示を行った後、その属性アラートは自身の「アラート要約 **(Alert Summary)**」ウィンドウのみに表示されることになります。Visualizer アナリスト・グループ内の他のアナリストがそれぞれの「アラート要約 **(Alert Summary)**」ウィンドウを最新表示すると、彼らにそのアラートは表示されなくなります。

ヘルプ・トピック

「アラート要約 **(Alert Summary)**」ウィンドウ**:**

このウィンドウを使用して、ユーザー自身の Visualizer アナリスト・グループ向けの未割り当てアラートの要約や、自分自身に割り当てたアラートを表示します。

ツイスティーを使用して画面のセクションを展開または省略して、特定の詳細に集中できるようにします。

アラートをタイプ別に表示
: 表示するアラート・タイプを選択するか、すべてのアラート・タイプを表示します。

「表示フィルター **(Display Filters)**」グループ・ボックス
: 「アラート要約 **(Alert Summary)**」ウィンドウに表示されるアラート要約を決定するデフォルトのフィルター設定を変更します。これらのフィルターは、現在未割り当てのアラート要約の表示を変更するのみで、変更はあくまでも一時的なものです。「アラート要約 **(Alert Summary)**」ウィンドウを閉じ、別の機会に再オープンした場合、これらの設定はデフォルトのフィルター設定に戻されます。

  デフォルト設定は、ワークステーションに構成されているアラート・フィルター設定です。(デフォルト設定は、「画面設定の構成 **(Configure Screen Preferences)**」ウィンドウの「システム設定 **(System Preferences)**」タブで変更できます。)

「アラート要約 **(Alert Summary)**」表
: 同じアラート・タイプ、説明、重大度、状況、解決ルール、相似スコア、および関係スコアを共有するアラートは、アラート要約にグループ化されます。「カウント **(Count)**」列には、要約にグループ化された個々のアラートの数が示されます。

  表の列見出しをクリックして、表をソートできます。 1 回目のクリックで、列値は昇順にソートされます。2 回目にクリックすると、列値は降順にソートされます。

  デフォルトでは、表はアラート・タイプでソートされています。

タイプ
アラート要約に表示されているアラートのタイプ。

説明　この要約のアラートの説明。

属性アラートの場合、この説明は、ケース番号です。イベント・アラートの場合、この説明は、イベント状態の説明です。ロール・アラートの場合、この説明は、ロール・アラート・ルールの説明です。

状況　この要約に含まれるアラートの現行アクティビティー状況。

「解決ルール **(Resolution Rule)**」
このアラート要約に含まれるアラート内でエンティティー同士を関連付けるために使用された解決ルールの名前。

「相似スコア **(Likeness Score)**」
関連付けられたエンティティーが同一エンティティーである可能性を示すスコア (0 から 100)。

「関係スコア **(Relationship score)**」
アラート内のエンティティーが互いにどれくらい強い関連があるかを示すスコア (0 から 100)。

「カウント **(Count)**」
現在選択されている「表示フィルター **(Display Filters)**」グループ・ボックスの基準を満たして、このアラート要約にグループ化されている個々のアラートの数。

「アラート・リスト **(Alert List)**」表
「アラート要約 **(Alert Summary)**」表から特定のアラート要約を選択すると、その要約に含まれている個々のアラートがこのセクションに表示されます。表示されるアラートの数 (行数) は、要約に含まれるアラートの総数 (「アラート要約 (Alert Summary)」表の「カウント **(Count)**」列を見るとわかります) と、「表示フィルター **(Display Filters)**」グループ・ボックスの「アラート・リストの最大行数 **(Maximum Lines in Alert List)**」フィールドの数値に応じて変わります。「アラート・リスト **(Alert List)**」表のタイトル・バーにあるリスト・カウントは、この要約のアラートの総数に対して、現在表示されているアラートの数がどれくらいであるかを示しています。

表の列見出しをクリックして、表をソートします。1 回目のクリックで、列値は昇順にソートされます。2 回目にクリックすると、列値は降順にソートされます。

表示されるフィールドは、選択されたアラート要約のタイプに基づきます。

「属性アラート」画面**:**

この画面を使用して、属性アラートの分析状況を設定または変更したり、アラートを構成する詳細を確認したりします。

ツイスティーを使用して画面のセクションを展開または省略して、特定の詳細に集中できるようにします。

「状況要約 **(Status Summary)**」
アラートの現在の分析状況および後処理を要約します。

「アラート要約 **(Alert Summary)**」
アラート要約の説明とアラートが生成された日時を提供します。

「エンティティーに対する一致 **(Match to Entity)**」セクション
属性アラート・ジェネレーターの検索基準とエンティティー・データベース内の既存のエンティティーの間でどの属性が一致したかについての詳細が含まれます。特定の属性をクリックすると、一致したエンティティーのアイデンティティーの一致情報が強調表示されます。

「属性アラート・ジェネレーター詳細 **(Attribute Alert Generator Details)**」
この属性アラートを生成した属性アラート・ジェネレーターの基準を要約します。データ・ソースをクリックすると、すべての基準が強調表示されます。

「エンティティー」セクション
属性アラート・ジェネレーターの基準に一致したエンティティーに関する情報が表示されます。データ・ソースをクリックすると、このデータ・ソースからアイデンティティー・レコードに取り込まれたデータが強調表示されます。

「エンティティー・レジュメ **(Entity Resume)**」ボタン
クリックすると、一致したエンティティーのエンティティー・レジュメが表示されます。このアラートを詳細に分析するために、エンティティーに関連した他のアイデンティティーを調べることもお勧めします。

「イベント・アラート **(Event Alert)**」画面**:**

「イベント・アラート **(Event Alert)**」画面を使用して、分析状況を設定または変更したり、イベント・アラートの詳細を確認したりします。イベント・アラートは、システムの Event Manager が有効で、イベント・アラート用のアクティビティー・コードが構成済みで、かつ 1 つ以上のイベント・アラートが存在する場合にのみ表示されます。

ツイスティーを使用して画面のセクションを展開または省略して、特定の詳細に集中できるようにします。

「状況要約 **(Status Summary)**」
イベント・アラートの現在の分析状況および後処理を要約します。

「アラート要約 **(Alert Summary)**」
イベント・アラートの説明とアラートが生成された日時を提供します。

「イベント・アラート **(Event Alert)**」セクション
このイベント・アラートを構成するイベントの詳細を提供します。

「エンティティー」セクション
このイベント・アラートに含まれる各エンティティーの簡単なレジュメを提供します。

「レポート」ボタン
クリックすると、「イベント・アラート詳細 **(Event Alert Detail)**」レポートが作成されます。

「ロール・アラート **(Role Alert)**」画面**:**

この画面を使用して、ロール・アラートの詳細を表示したり、ロール・アラートの分析状況を設定または変更したりします。

ツイスティーをクリックして画面のセクションを展開または省略して、特定の詳細に集中できるようにします。

隔たり度合い
: このロール・アラート内のエンティティー間の隔たり度合いを示します。

「状況要約 **(Status Summary)**」
: アラートの現在の分析状況および後処理を要約します。

「アラート要約 **(Alert Summary)**」
: アラート要約の説明、このアラートのアラート重大度コード、アラート内でエンティティー同士のマッチングに使用された解決ルール、2 つのエンティティーがどれくらい似ているかを示す解決スコア、およびこれら 2 つのエンティティーが互いを知っている可能性を示す関係スコアを提供します。

「マッチング詳細 **(Matching Details)**」タブ
: 2 つのエンティティー間で一致した属性に関する詳細が含まれます。特定の属性をクリックすると、一致したエンティティーのアイデンティティーの一致情報が強調表示されます。

  属性アラート・ジェネレーターの検索基準とエンティティー・データベース内の既存のエンティティーの間でどの属性が一致したかについての詳細が含まれます。

「レポート」ボタン
: クリックすると、このロール・アラートの「ロール・アラート詳細 **(Role Alert Detail)**」レポートが作成されます。

「エンティティー・レジュメ **(Entity Resume)**」ボタン
: クリックすると、選択したエンティティーのエンティティー・レジュメが表示されます。このアラートを詳細に分析するために、エンティティーに関連した他のアイデンティティーを調べることもお勧めします。

「エンティティー・イベント **(Entity Events)**」画面**:**

「エンティティー・イベント **(Entity Events)**」画面を使用して、特定の日付範囲内に発生したエンティティーのイベントを確認します。最初、この画面にアクセスするには、「エンティティー・レジュメ **(Entity Resume)**」画面から「イベントの表示 **(Show Events)**」をクリックします。

「イベント要約 **(Event Summary)**」セクション
: 示された日付範囲におけるこのエンティティーのすべてのイベントの要約が表示されます。デフォルトでこの画面には、最初のイベント日付から現在日付までの範囲で、エンティティーに関連するすべてのイベントが表示されます。別の日付範囲内のイベントを表示するには、イベント日付フィルターを使用して日付範囲を変更します。

  画面上のイベントの日付フィルター
  : 「ビューの更新 **(Update View)**」をクリックすると、表示されるイベントが、指定した日付範囲でフィルタリングされます。

「開始日 **(From Date)**」
日付を入力するか、カレンダー・コントロールをクリックして、日付範囲の開始日を選択します。

日付を入力することを選択する場合には、以下のいずれかの日付形式を使用してください。

- MM/dd/yyyy、MM-dd-yyyy、MM.dd.yyyy、または MMddyyyy
- yyyy/MM/dd、yyyy-MM-dd、または yyyy.MM.dd
- January 3, 2008 または January 03, 2008
- January 3, 08 または January 03, 08
- Jan 03, 2008 または Jan 3, 2008
- Jan 3, 08 または Jan 03, 08

このフィールドは、デフォルトで最初のイベント日付例の形式になります。

「終了日 **(Through Date)**」
日付範囲の終了日として使用する日付を入力するか、カレンダー・コントロールをクリックします。

日付を入力することを選択する場合には、以下のいずれかの日付形式を使用してください。

- MM/dd/yyyy、MM-dd-yyyy、MM.dd.yyyy、または MMddyyyy
- yyyy/MM/dd、yyyy-MM-dd、または yyyy.MM.dd
- January 3, 2008 または January 03, 2008
- January 3, 08 または January 03, 08
- Jan 03, 2008 または Jan 3, 2008
- Jan 3, 08 または Jan 03, 08

このフィールドは、デフォルトで現在日付になります。

「ビューの更新 **(Update View)**」ボタン
クリックすると、指定した日付範囲に含まれるこのエンティティーのイベントが表示されます。このボタンは、日付フィールドでデフォルトの日付が変更されるまでは使用不可になります。

「レポート」ボタン
クリックすると、このエンティティーの「すべてのイベント **(All Events)**」レポートが生成されます。

画面上の表示
画面のこのセクションには、指定された日付範囲に含まれるこのエンティティーのイベントがイベント・タイプ別に要約されます。

イベント・タイプ
イベント・タイプの説明です。

「カウント **(Count)**」
指定された日付範囲に含まれる、このエンティティーのイベント・タイプ別のイベントの総数を示します。(例えば、カ

ウントが 4 の場合、指定された日付範囲内で、このエンティティーを対象に同一イベント・タイプのイベントが 4 件発生したことになります。)

値　指定された日付範囲に含まれる、このエンティティーのイベント・タイプ別のイベントの合計値を示します。(例えば、4 件のイベントがある場合、この数値は、それら 4 つのイベントの値の合計になります。)

数量　指定された日付範囲に含まれる、このエンティティーのイベント・タイプ別のイベントの合計単位数を示します。

「計測単位 **(Unit of Measure)**」
イベント値の計測単位を示します。計測単位は、構成コンソールでイベント・タイプ別に構成されます。

「合計カウント **(Total Count)**」
指定された日付範囲に含まれる、このエンティティーのすべてのイベントの総数を表す数値を示します。

「合計値 **(Total Value)**」
指定された日付範囲に含まれる、このエンティティーのすべてのイベントの合計値を表す数値を示します。

「イベント詳細 **(Event Details)**」セクション
「イベント要約 (Event Summary)」セクション内で特定のイベント行を選択すると、イベント・タイプの要約に含まれている個々のイベントに関する詳細が表示されます。このセクション内のいずれかのイベント行をダブルクリックすると、選択したイベントに関するより一層詳細な情報を示す「イベント詳細 **(Event Details)**」画面が表示されます。

日付　イベントの日時を示します。

データ・ソース **-** 説明
イベントに関連したデータ・ソースの説明です。

外部 **ID**
このイベントの元のデータ・ソース内のインバウンド・レコードを識別するユニーク・キーが表示されます。

「イベント参照 **(Event Reference)**」
元のデータ・ソースに含まれるイベントに関する追加情報がインバウンド・レコードの一部である場合、その情報を提供します。

値　イベントの数量値を示します。

数量　イベントの単位の数を示します。

「メモ **(Memo)**」またはカスタム・ラベル
イベント・トランザクションの詳細なコンテキストを提供する、メモやコメントなど、イベントに関する追加情報を提供します。

ユーザーは、構成コンソールでイベント・タイプを構成するときにオプションの 1 つとして、この列のカスタム・ラベルを定義できます。したがって、「メモ **(Memo)**」の代わりに、より説明的なカスタム・ラベル (「電信送金メモ」など) が表示される場合があります。

エンティティーの検索

Visualizer ではいくつかの検索方法を使用してエンティティー・データベース内のエンティティーを検索できます。システムが特定の名前、住所、番号、または E メール・アドレスを含んだレコードを処理したら、必ず通知を受けるようにする場合、エンティティーを自動的に「見つける」ための属性アラート・ジェネレーターを作成します。

属性によるエンティティーの検索

Visualizer を使用しているときに、エンティティー・データベース内の特定のエンティティーを見つける必要がある場合、エンティティーに関連付けられている属性に関する基準を入力して、エンティティーを検索できます。属性基準を指定すると、Visualizer によってその基準に基づいたクエリーが作成されます。このタイプのエンティティー・クエリーは、検索結果を返すにあたってエンティティー解決処理は使用しません。

手順

1. Visualizer で、以下のいずれかを実行します。
   a. 「表示 **(View)**」 > 「検索方法 **(Find By)**」 > 「属性 **(Attribute)**」をクリックします。
   b. ツールバーで、(「検索」) アイコンをクリックします。
   c. ツールバーで、矢印をクリックして「属性 **(Attribute)**」を選択します。
   d. 「検索方法 **(Find By)**」ウィンドウで、「検索方法 **(Find By)**」ドロップダウン・リストから「属性 **(Attribute)**」を選択します。
2. エンティティーを検索するために使用する各属性タイプの基準を入力します。
   a. 別の属性タイプの基準を指定する行を追加するには、「**+**」をクリックします。
   b. 選択したクエリー基準項目を削除するには、「**-**」をクリックします。
3. オプション: 「要約の表示 **(Show Summary)**」をクリックして、「属性による検索」クエリーの要約を表示します。 要約は、意図した値がクエリーに含まれていることを確認するのに役立つ方法です。意図したとおりになっていない場合は、要約を閉じ、クエリー基準を修正してください。

   クエリー基準に同じ属性タイプが 2 つ含まれていると、「OR」節が組み立てられます。その他のクエリー基準はすべて「AND」節として結合されます。

   基準に含まれる属性タイプの順序は結果に影響しません。
4. 「検索」をクリックします。

タスクの結果

クエリー基準に一致するエンティティーが「結果」ペインに表示されます。

デフォルトで、「属性による検索」クエリーに対して表示される結果は、一致したエンティティーの最初の 1,000 件に制限されます。1,000 件を超える一致がある場合は、追加の結果が存在することが「結果」ペインに示されます。(表示される結果

の数は、システム・アドミニストレーターが構成コンソールで、システム・パラメーターの下にある MAX_ENTITIES_RETURNED パラメーターを設定することで構成できます。)

注: システムで追加の住所クレンジング・アプリケーションを使用している場合、特殊文字を含んでいる住所は文字変換されている可能性があります。例えば、住所に 1 つ以上のウムラウト記号が含まれるドイツの住所の検索結果では、一致するウムラウト記号が含まれない結果が返される可能性があります。

次のタスク

エンティティーをクリックして、選択したエンティティーのエンティティー・レジュメを表示します。

データ・ソース・アカウントによるエンティティーの検索

アイデンティティーのアカウント番号 (または外部 ID) がわかっているときに、そのアイデンティティーを含んでいるエンティティーを検索する必要がある場合、Visualizer の「データ・ソース・アカウントによる検索 (Find By Datasource Account)」を使用します。「エンティティーの追加 **(Add Entity)**」画面から追加したエンティティーも検索できます。

始める前に

アイデンティティー (またはアカウント) のデータ・ソース説明と外部 ID がわかっている必要があります。名前によってエンティティーを検索しようとしている場合は、「属性による検索 (Find By Attribute)」方法を使用してください。

手順

1. Visualizer で、以下のいずれかを実行します。
   a. 「表示 **(View)**」 > 「検索方法 **(Find By)**」 > 「データ・ソース・アカウント **(Datasource Account)**」をクリックします。
   b. ツールバーで、矢印をクリックし、「データ・ソース・アカウント **(Datasource Account)**」を選択します。
   c. 「検索方法 **(Find By)**」ウィンドウで、「検索方法 **(Find By)**」ドロップダウン・リストから「データ・ソース・アカウント **(Datasource Account)**」を選択します。
2. 「外部 **ID** の入力 **(Enter External ID)**」で、アイデンティティーのアカウント番号を入力します。 アカウントは、元のデータ・ソース内でそのアイデンティティーを特定するための手段です。
3. 「データ・ソース **(Data Source)**」で、データ・ソース・コードおよび説明を選択します。
4. 「検索」をクリックします。

タスクの結果

システムが、指定された外部 ID とデータ・ソース基準に該当するアイデンティティーを含んだエンティティーを検出した場合、Visualizer にそのエンティティーの「エンティティー・レジュメ **(Entity Resume)**」が表示されます。

エンティティー ID によるエンティティーの検索

エンティティーのエンティティー ID 番号がわかっている場合、Visualizer の「エンティティー ID による検索 (Find By Entity ID)」方法を使用して、素早くエンティティーを見つけて、そのエンティティーのエンティティー・レジュメを表示します。

始める前に

検索するエンティティーのエンティティー ID 番号がわかっている必要があります。名前によってエンティティーを検索しようとしている場合は、代わりに「属性による検索 (Find By Attribute)」方法を使用してください。

手順

1. Visualizer で、以下のいずれかを実行します。
   a. 「表示 **(View)**」 > 「検索方法 **(Find By)**」 > 「エンティティー **ID (Entity ID)**」をクリックします。
   b. ツールバーで、矢印をクリックして「エンティティー **ID (Entity ID)**」を選択します。
   c. 「検索方法 **(Find By)**」ウィンドウで、「検索方法 **(Find By)**」ドロップダウン・リストから「エンティティー **ID (Entity ID)**」を選択します。
2. 「エンティティー **ID** の入力 **(Enter Entity ID)**」で、検索するエンティティーのエンティティー ID 番号を入力します。
3. 「検索」をクリックします。

タスクの結果

エンティティー ID が、エンティティー・データベース内のエンティティーと一致した場合、Visualizer にそのエンティティーのエンティティー・レジュメが表示されます。

解決によるエンティティーの検索

「解決による検索 (Find by Resolution)」を使用して、検索エンティティーを作成します。この検索エンティティーが、エンティティー・データベース内のいずれかのアイデンティティーがクエリーの基準に適合しているかどうかを判定するエンティティー解決処理で使用されることになります。

始める前に

「解決による検索 (Find by Resolution)」機能には、Visualizer サーバーが通信可能な稼働中のパイプラインが必要です。パイプラインは、エンティティー解決と関係解決が行われるコンポーネントです。

このタスクについて

エンティティー解決を使用して結果が求められることから、「解決による検索 (Find by Resolution)」機能を最大限に生かすために、エンティティー解決の仕組みと、システムにエンティティー解決がどのように構成されているかを理解することが重要になります。例えば、名前のみに基づいて一致を探すようにエンティティー解決が構成されていない場合、名前の値のみに基づいて検索が実行されると、「解

決による検索 (Find by Resolution)」は結果を何も返しません。同様に、エンティティー解決は、郵便番号のみに基づいたエンティティーの解決は行わないため、郵便番号のみを指定しても結果は何も返されません。

「解決による検索 (Find by Resolution)」は、「ファイル」メニューの「システム設定 **(System Preferences)**」タブに定義されている最小スコア値を使用します。

手順

1. Visualizer で、以下のいずれかを実行します。
   a. 「表示 **(View)**」 > 「検索方法 **(Find By)**」 > 「解決 **(Resolution)**」をクリックします。
   b. ツールバーで、矢印をクリックして「解決 **(Resolution)**」を選択します。
   c. 「検索方法 **(Find By)**」ウィンドウで、「検索方法 **(Find By)**」ドロップダウン・リストから「解決 **(Resolution)**」を選択します。
2. アイデンティティーに関してわかっている属性をできるだけ多く入力します。
   - 「名前」セクションに何らかの入力を行う場合、「ラストネーム **(Last Name)**」は必須になります。
   - 「住所リスト **(Address List)**」セクションに何らかの情報を入力する場合、「住所 **(Address)**」は必須になります。
   - 「番号リスト **(Number List)**」セクションで「タイプ」を選択する場合、「値」フィールドに番号値を入力する必要があります。 (「ロケーション **(Location)**」はオプションです。)
   - 「特性リスト **(Characteristic List)**」セクションで「タイプ」を選択する場合、「値」フィールドに特性の値を入力する必要があります。
   - 「**E** メール・リスト **(Email List)**」セクションで「タイプ」を選択する場合、「アドレス **(Address)**」フィールドに E メール・アドレスの値を入力する必要があります。
3. 「検索 **(Search)**」をクリックします。

属性アラート・ジェネレーターによるエンティティーの検索

監視しているエンティティーがある場合、そのエンティティーに関する基準を指定した属性アラート・ジェネレーターを作成できます。基準に一致する属性がアイデンティティー・レコードまたはエンティティーに含まれていると、システムによって属性アラートが生成されます。各 Visualizer ユーザーが、特定の日付範囲を対象にした個人用の属性アラート・ジェネレーターを作成し、管理します。

属性アラート・ジェネレーターはパイプラインを通して送信されるため、エンティティー解決処理は、それらの検索要求に対しても、以下のとおり、入力エンティティー・データに対して行われるのと同じ方法で実行されます。

- 名前と住所が標準化されます。
- 後続の属性アラートで該当エンティティーを識別できるように、部分検索またはファジー検索と比較が実行されます。

属性アラートの結果を得るために、エンティティー解決が使用されます。このため、属性アラート・ジェネレーターを最大限に生かすためには、エンティティー解決の仕組みと、システムにエンティティー解決がどのように構成されているかを理

解することが重要になります。例えば、名前のみに基づいて一致を探すようにエンティティー解決が構成されていない場合、名前の値のみを検索するように構成されている属性アラート・ジェネレーターは結果を何も返しません。同様に、エンティティー解決は、郵便番号のみに基づいたエンティティーの解決は行わないため、郵便番号のみを指定した属性アラート・ジェネレーターは結果を何も返しません。

属性アラート・ジェネレーターを作成するときは、以下のガイドラインを使用してください。

- 属性アラートの結果をフィルタリングするには、「最小スコア **(Minimum Score)**」を使用します。このフィールドのデフォルト値は、「任意の関係 (Any Relationship)」です。これを選択すると、最も多数の結果を得られます。結果を少なくするには、高いレベルを選択します。これらの値は、「ファイル」メニューから使用できる、Visualizer システム設定で構成されます。
- 名前: ラストネームとファーストネームの組み合わせ、またはラストネームとミドルネームの組み合わせのいずれかを指定します。ラストネーム、ファーストネーム、またはミドルネームのいずれか 1 つのみを指定した属性アラート・ジェネレーターは結果を何も返しません。
- 住所: 住所と郵便番号の両方が必要です。市区町村、都道府県、郵便番号、番地または国のいずれか 1 つのみを指定した属性アラート・ジェネレーターは結果を何も返しません。

属性アラート・ジェネレーターの作成**:**

特定の属性値または属性値の組み合わせがシステムによって処理されるたびにアラートを受け取るには、属性アラート・ジェネレーターを作成します。属性アラート・ジェネレーターは、指定された有効期限がくるまでアラートの生成を継続します。

手順

1. Visualizer で、以下のいずれかを実行します。
   a. 「表示 **(View)**」 > 「属性アラート・ジェネレーター・マネージャー **(Attribute Alert Generator Manager)**」を選択します。
   b. ツールバーから、(「属性アラート・ジェネレーター・マネージャー (Attribute Alert Generator Manager)」) アイコンをクリックします。
2. 「属性アラート・ジェネレーター・マネージャー **(Attribute Alert Generator Manager)**」ウィンドウで、「作成」をクリックします。
3. ドロップダウン・リストと各フィールドを使用して、新しい属性アラートの具体的な基準を有効期限も含めて入力します。 デフォルトの有効期限は、今日の日付から 6 カ月後に設定されます。
4. 「作成」をクリックします。

タスクの結果

指定した基準に該当するデータがエンティティー解決によって処理されるたび、新しい属性アラートがユーザーの「アラート要約 **(Alert Summary)**」ウィンドウに表示されます。探している情報がその時点でエンティティー・データベース内に存在する場合、新しい属性アラートが「アラート要約 **(Alert Summary)**」ウィンドウに表示されます。

属性アラート・ジェネレーターの編集:

ケース番号、コメント、または有効期限を変更する必要がある場合、アクティブな属性アラート・ジェネレーターを編集します。

このタスクについて

属性およびそれらの属性の最小解決スコアを変更することはできません。そのような変更が必要な場合は、属性アラート・ジェネレーターを作成してください。また、新しい属性アラート・ジェネレーターで既存のものを置き換える場合は、以下のステップを使用して、不要になった属性アラート・ジェネレーターを期限切れにします。

手順

1. Visualizer で、以下のいずれかを実行します。
   a. 「表示 **(View)**」 > 「属性アラート・ジェネレーター・マネージャー **(Attribute Alert Generator Manager)**」をクリックします。
   b. ツールバーから、(「属性アラート・ジェネレーター・マネージャー (Attribute Alert Generator Manager)」) をクリックします。
2. 編集する属性アラート・ジェネレーターを選択し、「作成」をクリックします。
3. 「属性アラート・ジェネレーター情報 **(Attribute Alert Generator Info)**」ウィンドウで、必要な変更を行います。
   - 有効期限を変更できます。これには、属性アラート・ジェネレーターを無効にするために日付を過去の日付に設定することも含まれます。
   - ケース番号とコメントを更新することもできます。
   - 理由コード、属性アラート・ジェネレーターの作成時に選択した属性、および最小解決スコアを変更することはできません。
4. 「更新 **(Update)**」をクリックします。

タスクの結果

システムによって、属性アラート・ジェネレーターに対する変更内容がログに記録されます。属性アラート・ジェネレーターに対するすべての変更内容を確認するには、「属性アラート・ジェネレーター・ヒストリー・レポート **(Attribute Alert Generator History report)**」を表示または印刷してください。

ヘルプ・トピック:

「属性による検索 ***(Find By Attribute)***」画面:

このウィンドウを使用して、エンティティー・データベース内のエンティティーを属性 (名前、住所、各種番号、特性など) で検索するクエリーを作成します。このタイプのクエリーは、クエリー結果を返すためにエンティティー解決処理は使用しません。

属性タイプ
: クエリーの基準として使用するエンティティー属性のタイプ。名前、住所、各種番号、特性、E メール・アドレス、データ・ソース、またはファイル・

ロード日付。属性タイプを選択すると、そのタイプに適したクエリー基準フィールドがウィンドウに表示されます。

作成するクエリー・ステートメントは、クエリーの基準として選択した属性タイプによって異なります。

- 単一クエリーで、複数の同じ属性タイプを基準にする場合は、OR クエリー・ステートメントを作成します。例えば、「"Bob Hayes" OR "Rob Hays"」です。
- 単一クエリーで、複数の属性タイプを基準にする場合は、AND クエリー・ステートメントを作成します。例えば、「"Bob Hayes" AND credit card number "5252-1010-5252-1010"」です。

上記の例を使用して、以下の 2 つの名前とクレジット・カードを入力する場合、クエリー・ステートメントは次のステートメントのようになります: Bob Hayes" OR "Rob Hays AND credit card number "5252-1010-5252-1010"

完全なクエリー・ステートメントを表示するには、「要約の表示 **(Show Summary)**」ボタンを使用します。

「値」フィールド
: エンティティーを検索するために使用する属性タイプの特定の値を入力します。各属性タイプに独自の値フィールドのセットがあります。値フィールドをブランクのままにした場合、クエリーはすべての可能性のある値を探します。ただし、すべての値フィールドにデータを入力したほうがクエリーの実行時間が短縮され、クエリーが返す結果も向上します。

  - 名前基準は必須です。
  - 住所または E メールの基準フィールドに情報を入力する場合、すべての住所またはアドレスのフィールドが必須になります。
  - 各種番号タイプまたは特性タイプを選択する場合、「値」フィールドが必須になります。

「**+**」ボタン
: 基準に新しい属性行を追加します。

「**-**」ボタン
: 選択済みの属性行と基準項目を削除します。

「属性による検索 **- 結果 (Find by Attribute - Results)**」ペイン
: 基準項目に基づいた、「属性による検索」クエリーの結果が含まれています。デフォルトで、表示域にはクエリー基準に一致する最初の 1,000 レコードのみが表示されます。(ただし、このオプションはシステム・アドミニストレーターが設定できます。)

  結果はエンティティー別に表示され、各エンティティーに関する最新情報が提示されます。結果ペイン内のエンティティーをダブルクリックすると、Visualizer にそのエンティティーのエンティティー ・レジュメが開かれます。

  「エンティティー **ID (Entity ID)**」
  : クエリー基準を満たすエンティティーの ID が表示されます。

名前 **(*count*)**
: クエリー基準を満たすエンティティーの最有力の名前と、このエンティティーに関連付けられた名前の数を表す数値が表示されます。例えば、「Bob M. Smith (4)」は、このエンティティー Bob Smith に 4 つの名前が関連付けられていることを示します。

住所 **(*count*)**
: クエリー基準を満たすエンティティーの最有力の住所と、このエンティティーに関連付けられた住所の数を表す数値が表示されます。例えば、「1024 Daisy Lane, Akron, OH 43596 (24)」は、このエンティティーに 24 の住所が関連付けられていることを示します。

番号タイプ**: *value***
: クエリー基準を満たすエンティティーの最有力の番号タイプと番号の値が表示されます。

特性タイプ**: *value***
: クエリー基準を満たすエンティティーの最有力の特性タイプと値が表示されます。

関係
: クエリー基準を満たすエンティティーによって保持されている関係の数が表示されます。

アラート
: クエリー基準を満たすエンティティーに関連付けられているアラートの数が表示されます。

「データ・ソース・アカウントによる検索 ***(Find by Datasource Account)***」画面**:**

このウィンドウを使用して、元のデータ・ソースからのアカウント情報でエンティティーを検索します。

「外部 **ID** の入力 **(Enter External ID)**」
: エンティティーに関連付けられている、「データ・ソース **(Data Source)**」で指定されたデータ・ソース内のデータ・ソース・アカウント情報を入力します。

「データ・ソース **(Data Source)**」
: 「外部 **ID** の入力 **(Enter External ID)**」で指定したアカウントに対応するデータ・ソースを選択します。

「エンティティー ***ID*** による検索 ***(Find By Entity ID)***」画面**:**

この検索方法を使用して、エンティティー・データベース内のエンティティー ID を使用してエンティティーを素早く見つけます。クエリーがエンティティー・データベース内でエンティティーを見つけた場合、Visualizer にそのエンティティーのエンティティー・レジュメが表示されます。

「解決による検索 ***(Find By Resolution)***」画面**:**

「解決による検索 **(Find By Resolution)**」ウィンドウを使用して、エンティティー・データベース内のアイデンティティーと比較する検索エンティティーを作成します。

データ・ソース・コード - 説明
「解決による検索 (Find By Resolution)」処理で検索するアイデンティティーに関連付けられているデータ・ソース・コードと説明を選択します。

「最小解決スコア **(Minimum Resolution Score)**」
アイデンティティーを「解決による検索 (Find By Resolution)」クエリーに指定された基準と比較するときに使用する最小解決スコアを選択します。

選択したスコアで、クエリーが返す結果の数とタイプが決まります。

「解決による検索 **(Find By Resolution)**」基準セクション
エンティティー・データベース内のアイデンティティーと比較する検索エンティティーを作成するための属性を指定します。システムは、指定された最小解決スコアに基づいてアイデンティティーを返します。

「名前リスト **(Name List)**」
特定の名前を探している場合、名前リスト・フィールドに名前基準を入力します。いずれかの名前フィールドに入力する場合、「姓 **(Last Name)**」は必須です。

「住所リスト **(Address List)**」
特定の住所を探している場合、住所リスト・フィールドに住所基準を入力します。いずれかの住所フィールドに入力する場合、「番地 **(Street)**」は必須です。

「番号リスト **(Number List)**」
パスポート番号またはクレジット・カード番号など、特定の番号基準を番号リスト・フィールドに入力します。「タイプ **(Type)**」と「値」の両方が必須です。

「特性リスト **(Characteristic List)**」
性別または生年月日など、特定の特性基準を特性フィールドに入力します。「タイプ **(Type)**」と「値」の両方が必須です。

「**E** メール・リスト **(E-mail List)**」
特定の E メール・アドレス基準を E メール・アドレス・リスト・フィールドに入力します。「タイプ **(Type)**」と「アドレス」の両方が必須です。

「属性アラート・ジェネレーター・マネージャー ***(Attribute Alert Generator Manager)***」ウィンドウ*:*

このウィンドウを使用して、現在アクティブな属性アラート・ジェネレーターを表示および管理します。「属性アラート・ジェネレーター・マネージャー **(Attribute Alert Generator Manager)**」ウィンドウには、有効期限が切れた属性アラート・ジェネレーターは表示されません。

「有効期限 **(Expiration Date)**」
属性アラート・ジェネレーターの有効期限が切れる日付が表示されます。

「作成日 **(Creation Date)**」
属性アラート・ジェネレーターが作成された日付が表示されます。

「エンティティー **ID (Entity ID)**」
属性アラート・ジェネレーター基準によって作成された検索エンティティーのエンティティー ID。

「理由 **(Reason)**」
属性アラート・ジェネレーターの作成プロセスで割り当てられた理由コード。

「最小解決スコア **(Minimum Resolution Score)**」
属性アラート基準をエンティティー・データベース内の既存のエンティティーと比較して、そのエンティティーを対象に属性アラートを生成する場合に、そのエンティティーが満たしていなければならない最小解決スコアが表示されます。

「ケース番号 **(Case Number)**」
属性アラート・ジェネレーターの作成プロセスで割り当てられたケース番号が表示されます。

「作成」ボタン
「属性アラート・ジェネレーターの作成 **(Create Attribute Alert Generator)**」ウィンドウが表示され、属性アラート・ジェネレーターを作成できるようになります。

「編集」ボタン
「属性アラート・ジェネレーター情報 **(Attribute Alert Generator Info)**」ウィンドウが表示され、選択した属性アラート・ジェネレーターを編集できるようになります。(属性アラート・ジェネレーターを選択してからこのボタンをクリックします。)

「属性アラート・ジェネレーターの作成 ***(Create Attribute Alert Generator)***」ウィンドウ*:*

このウィンドウを使用して、属性アラート・ジェネレーターを作成します。属性アラート・ジェネレーターは、指定された属性基準を使用して、一致する属性データを持つエンティティーをエンティティー・データベースで永続的に検索します。

データ・ソース・コード **-** 説明
この属性アラート・ジェネレーターから作成される属性アラートに関連付けるデータ・ソース・コードと説明をドロップダウン・リストから選択します。デフォルトの選択は、通常「検索 (Search)」に設定されます。

「最小解決スコア **(Minimum Resolution Score)**」
アイデンティティーを属性アラート・ジェネレーターで指定された基準と比較するときに使用する最小解決スコアをドロップダウン・リストから選択します。

理由コード
この属性アラート・ジェネレーターに関連付ける理由コードをドロップダウン・リストから選択します。

「ケース番号 **(Case Number)**」
この属性アラート・ジェネレーターから作成される属性アラートのオプションのケース番号を入力します。

コメント
この属性アラート・ジェネレーターから作成される属性アラートのオプションのコメントを入力します。

「有効期限 **(Expiration Date)**」
この属性アラート・ジェネレーターの有効期限が切れる日付を選択するか、カレンダー・アイコンをクリックしてカレンダー・コントロールを使用して日付を選択します。有効期限は、デフォルトでは今日の日付から 6 カ月後に設定されます。属性アラート・ジェネレーターは、常にバックグラウンドで実行されるため、有効期限を設定することをお勧めします。

「属性 **(Attribute)**」基準セクション
指定された属性を含むアイデンティティー・レコードをシステムが処理するたびに、属性アラートが生成される必要がある属性を指定します。

「名前リスト **(Name List)**」
特定の名前を探す場合、名前リスト・フィールドに名前基準を入力します。

「住所リスト **(Address List)**」
特定の住所を探す場合、住所リスト・フィールドに住所基準を入力します。

「番号リスト **(Number List)**」
特定の番号 (パスポート番号またはクレジット・カード番号など) を探す場合、番号リスト・フィールドに番号基準を入力します。

「特性リスト **(Characteristic List)**」
特定の特性 (性別または生年月日など) を探す場合、特性リスト・フィールドに特性基準を入力します。

「**E** メール・リスト **(E-mail List)**」
特定の E メール・アドレスを探す場合、E メール・アドレス・リスト・フィールドに E メール・アドレス基準を入力します。

「属性アラート・ジェネレーター情報 ***(Attribute Alert Generator Info)***」ウィンドウ*:*

このウィンドウを使用して、既存の属性アラート・ジェネレーターを編集します。ケース番号、有効期限、およびコメントのみを変更できます。

理由コード
(表示のみ) この属性アラート・ジェネレーターで選択された理由コードが表示されます。

「ケース番号 **(Case Number)**」
属性アラート・ジェネレーターを作成したユーザーによって入力されたオプションの英数字のケース番号が表示されます。

コメント
属性アラート・ジェネレーターを作成したユーザーによって入力されたコメントが表示されます。

「有効期限 **(Expiration Date)**」
属性アラート・ジェネレーターの現在の有効期限が表示されます。

「使用される名前 **(Names Used)**」
(表示のみ) この属性アラート・ジェネレーターの基準として名前情報が入力された場合、このセクションには、属性アラート・ジェネレーターを作成したユーザーによって入力されたすべての名前情報がリストされます。

住所　(表示のみ) この属性アラート・ジェネレーターの基準として住所情報が入力された場合、このセクションには、属性アラート・ジェネレーターを作成したユーザーによって入力されたすべての住所情報がリストされます。

番号　(表示のみ) この属性アラート・ジェネレーターの基準として番号情報が入力された場合、このセクションには、属性アラート・ジェネレーターを作成したユーザーによって入力されたすべての番号情報がリストされます。

「その他の属性 **(Other Attributes)**」
(表示のみ) この属性アラート・ジェネレーターの基準として特性情報が入力された場合、このセクションには、属性アラート・ジェネレーターを作成したユーザーによって入力されたすべての特性情報がリストされます。

「更新」ボタン
クリックすると変更が適用されます。

エンティティーの分析

Visualizer を使用して、エンティティー・データベース内のエンティティーのレビュー、分析、およびグラフ化を実行できます。

エンティティー

エンティティーは、同じ個人、組織、場所、またはアイテムを表す 1 つ以上のアイデンティティーの集合です。エンティティーは、エンティティー・データベースに保管されます。

エンティティーは、人を表すものと考えられることが多いですが、企業や車両などを表す場合もあります。実際に、システムの拡張可能な構成を使用して、組織のデータをマップし、解決または関連付けが必要な任意のタイプのエンティティーを作成できます。

エンティティーは、多くの場合、いくつかの異なるソース・システムから取得されるアイデンティティーで構成されます。エンティティー解決は、どのアイデンティティーが実際には同じエンティティーであるかを判別し、複合エンティティーを作成します。複合エンティティーには、その複合エンティティーに関連付けられているすべてのアイデンティティーが含まれています。システムは、複合エンティティー内の各アイデンティティーに関連付けられたソースを識別して、レコードのフル属性情報を維持します。

組織の目標を満たすような方法で、エンティティーの解決と関連付けが行われるようにシステムを構成してください。

エンティティー・レジュメ

エンティティー・レジュメは、特定のエンティティーに関するエンティティー・データベース内のすべての情報を統合したコレクションです。

エンティティーはエンティティー ID を使用してエンティティー・データベース内に編成されます。エンティティー ID ごとに独自のエンティティー・レジュメが存在します。

エンティティー・レジュメを表示するには Visualizer を使用します。エンティティー・レジュメには、以下のタイプの情報が含まれる可能性があります。

- ソース・ドキュメント参照
- ロール
- 「使用される名前 (Names Used)」
- 住所
- 番号
- 特性
- 「開示 (Disclosures)」
- 関連エンティティー
- 「ロール・アラート・ヒストリー (Role Alert History)」
- 「イベント・アラート・ヒストリー (Event Alert History)」
- E メール・アドレス

エンティティー・レジュメの表示

エンティティー・データベース内の特定のエンティティーに関するすべての情報を表示するには、エンティティー・レジュメを表示します。

このタスクについて

以下の Visualizer 内のいずれかの場所からエンティティー・レジュメにアクセスできます。

- 任意のアラート詳細ウィンドウ
- 任意のグラフ・ウィンドウ
- 任意の「検索方法**: (Find By:)**」ウィンドウ

手順

- 「ロール・アラート詳細 **(Role Alert Detail)**」ウィンドウ、「属性アラート詳細 **(Attribute Alert Detail)**」ウィンドウ、または「イベント・アラート詳細 **(Event Alert Detail)**」ウィンドウで、「エンティティー・レジュメ **(Entity Resume)**」をクリックします。
- エンティティー・グラフから、情報を表示するエンティティー ID を含んでいる「エンティティー」アイコンを右クリックし、「エンティティー・レジュメ **(Entity Resume)**」を選択します。
- 「検索方法**: (Find By:)**」ウィンドウの「結果」セクションで、レジュメを表示するエンティティーを含んでいる行をダブルクリックします。

エンティティー・レジュメの印刷

エンティティー・レジュメのハードコピーが必要な場合、PDF 版のエンティティー・レジュメが必要な場合、またはエンティティー・レジュメの情報をワード・プロセッサーやスプレッドシートなどの別のアプリケーションにコピーする必要がある場合、エンティティー・レジュメを印刷するいくつかの方法があります。

手順

- 「エンティティー・レジュメ **(Entity Resume)**」ウィンドウのスナップショットを印刷するには、以下のようにします。

1. 「エンティティー・レジュメ **(Entity Resume)**」ウィンドウで、「印刷 **(Print)**」をクリックします。
2. プリント・ダイアログで、印刷設定を指定します。
3. 「**OK**」をクリックします。

- エンティティー・レジュメを PDF ファイルに印刷するには、「エンティティー・レジュメ **(Entity Resume)**」ウィンドウで、「レポート **(Report)**」をクリックします。
- エンティティー・レジュメの情報をコピー (印刷) して、別のアプリケーションに貼り付けるには、以下のようにします。
  1. 「エンティティー・レジュメ **(Entity Resume)**」ウィンドウで、「編集」メニューから「画面をクリップボードにコピー **(Copy Screen to Clipboard)**」を選択します。

     注**: Ctrl + C** のキーの組み合わせは、単一フィールド値しかコピーしません。
  2. 使用するアプリケーションにクリップボードの内容を貼り付けます。
  3. アプリケーションの印刷機能を使用して、エンティティー・レジュメの情報を印刷します。

現行ウィンドウの印刷

グラフおよびエンティティー・レジュメを含め、Visualizer 内のウィンドウは、いずれも印刷コマンドを使用してそのウィンドウから直接印刷できます。

手順

1. Visualizer で、印刷する必要があるウィンドウから「ファイル」メニューの「印刷 **(Print)**」を選択します。
2. 「印刷 **(Print)**」ダイアログで、印刷設定を指定します。
3. 「**OK**」をクリックします。

エンティティー・グラフの表示

Visualizer の主なメリットの 1 つに、エンティティー関係とロール・アラート情報をグラフ化できることがあります。グラフは、選択されたエンティティーに関する情報のビジュアル表示を提供します。

このタスクについて

以下の Visualizer 内のいずれかの場所からエンティティー・グラフにアクセスできます。

- 「エンティティー・レジュメ **(Entity Resume)**」ウィンドウ
- 「グラフ **(Graph)**」ウィンドウ
- 「イベント・アラート詳細 **(Event Alert Detail)**」ウィンドウ

手順

- 「エンティティー・レジュメ **(Entity Resume)**」ウィンドウで、「グラフ **(Graph)**」をクリックします。

- 「グラフ **(Graph)**」ウィンドウで、情報を表示するエンティティー ID を含んでいる「エンティティー」アイコンを右クリックし、「エンティティー・グラフの表示 **(Show Entity Graph)**」を選択します。 グラフ内のエンティティーのエンティティー・レジュメを表示するには、エンティティーを右クリックし、「エンティティー・レジュメ **(Entity Resume)**」を選択します。
- 「イベント・アラート詳細 **(Event Alert Detail)**」ウィンドウで、「グラフ **(Graph)**」をクリックします。
- オプション: グラフ内での情報の表示方法を変更するには、グラフ内の任意のブランク・スペースを右クリックしてから、以下のようにします。
  1. グラフ内の情報のビジュアル編成を変更するには、別の「グラフ・レイアウト **(Graph Layout)**」設定を選択します。
  2. 現在のズーム・レベルを変更するには、別の「ズーム **(Zoom)**」設定を選択します。

  グラフ設定を変更するたび、その新しい設定が、現行 Visualizer セッションの間に追加で表示する各グラフのデフォルト設定として使用されます。

ロール・アラート・グラフの表示

ロール・アラート内で識別されたエンティティー同士がどのように関連しているかをグラフィカル表現で確認する場合、ロール・アラート・グラフを表示できます。

手順

1. Visualizer で、「アラート要約 **(Alert Summary)**」ウィンドウからロール・アラートをダブルクリックします。
2. 「ロール・アラート詳細 **(Role Alert Detail)**」画面で、「グラフ **(Graph)**」をクリックします。
3. オプション: グラフ内での情報の表示方法を変更するには、グラフ内の任意のブランク・スペースを右クリックしてから、以下のようにします。
   a. グラフ内の情報のビジュアル編成を変更するには、別の「グラフ・レイアウト **(Graph Layout)**」設定を選択します。
   b. 現在のズーム・レベルを変更するには、別の「ズーム **(Zoom)**」設定を選択します。

   グラフ設定を変更するたび、その新しい設定が、現行 Visualizer セッションの間に追加で表示する各グラフのデフォルト設定として使用されます。
4. オプション: グラフ内のエンティティーのエンティティー・レジュメを表示するには、エンティティーを右クリックし、「エンティティー・レジュメ **(Entity Resume)**」を選択します。

グラフ・アイコンのカスタマイズ

Visualizer のグラフはすべて、事前定義アイコンを使用して、エンティティーおよび、住所や各種番号などの属性のタイプを表現します。 Visualizer のグラフに表示するアイコンをカスタマイズしたり、新しい属性タイプに使用するアイコンを指定したりできます。

始める前に

Visualizer のグラフ・アイコンをカスタマイズする前に、以下の制約を留意してください。

- カスタム・アイコンはアプリケーション・サーバー上に常駐します。アプリケーション・サーバーに対する管理特権を持つユーザーのみが、カスタム・グラフ・アイコンを追加したり変更したりできます。そのアプリケーション・サーバーをベースとする Visualizer クライアントはすべて同じアイコン・セットを使用します。したがって、ここで行う変更は、Visualizer のグラフに表示されるアイコンに関してそれらすべてのクライアントに影響します。
- カスタム・アイコンは、アプリケーション・サーバー上で別のアイコン・フォルダーに保存してください。Visualizer の新しい *.EAR ファイルをインストールすると、すべてのカスタム・グラフ・アイコンが削除されます。新しい Visualizer *.EAR ファイルをインストールした後、アイコン・フォルダーからカスタム・グラフ・アイコンをアプリケーション・サーバーの指定のアイコン・フォルダーにコピーできます。
- アイコンは .GIF フォーマットでなければなりません。イメージの推奨サイズは 24 x 24 ピクセルです。
- アイコンの名前は、それぞれの対応する属性タイプと一致しなければなりません。また、名前はすべてが小文字でなければなりません。例えば、「Evidence Photo」(証拠写真) という新しい属性タイプを追加する場合、Visualizer がこのカスタムの証拠写真タイプを認識できるようにするには、ファイルの名前を「evidence photo.gif」にする必要があります。この例で、属性タイプ名とアイコン・ファイル名の両方にスペースが含まれている点に注目してください。

このタスクについて

デフォルトの Visualizer アイコン・イメージ・ファイルは、アプリケーション・サーバー上、通常は `images` というフォルダーに保管されます。

手順

1. アプリケーション・サーバーを停止します。
2. アプリケーション・サーバー上で、デフォルトの Visualizer グラフ・アイコン・フォルダーを見つけます。通常、このフォルダーは *IBM Infosphere Identity Insight application server install_path*/ `was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images` にあります。
3. 必須: カスタム・グラフ・アイコンのイメージ・ファイル用に `graph` という名前のフォルダーをデフォルトの Visualizer グラフ・アイコン・フォルダー (`/images` フォルダー) の下に作成します。

   注: フォルダー名は、`graph` にしてください。
4. 各アイコン・イメージ・ファイルを新規フォルダーに保存、コピー、または移動します。

例

FINGERPRINT_FILE という名前の属性タイプを作成済みで、Visualizer のグラフ上でその属性タイプを表すカスタム・グラフ・アイコンが必要だとします。この場合、以下のステップを実行します。

1. FINGERPRINT_FILE 属性タイプを表す、24 x 24 ピクセルの適切な .GIF イメージ・ファイルを作成または入手します。イメージ・ファイル名が属性タイプ名と一致していること、ファイル名にすべて小文字が使用されていることを確認します。例えば、ファイル名は、fingerprint_file.gif のようになります。
2. IBM InfoSphere Identity Insight アプリケーション・サーバー上で、images フォルダーを見つけます。例えば、イメージ・フォルダーは IBM-II_install/was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images にあります。
3. イメージ・フォルダーの下に、graph という名前のフォルダーを作成します。その結果、ファイル・パスは、次のパスのようになります。IBM-II_install/was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images/graph
4. fingerprint_file.gif イメージ・アイコンを graph フォルダーにコピーします。

次のタスク

アプリケーション・サーバーを再始動します。

ヘルプ・トピック

「エンティティー・レジュメ **(Entity Resume)**」画面**:**

この画面を使用して、エンティティーに関連付けられているアイデンティティーの属性、すべての関連エンティティー、エンティティーに関連したすべてのアラートのヒストリーなど、エンティティーに関してわかっているすべての情報の詳細を確認します。

ツイスティーを使用して画面のセクションを展開または省略して、特定の詳細に集中できるようにします。

データ・ソース情報
: このエンティティーに解決されたアイデンティティー・レコードを提供したデータ・ソースを示します。データ・ソースをクリックすると、このデータ・ソースから処理されたアイデンティティー・レコードを構成する属性が強調表示されます。データ・ソース情報は、アイデンティティー・レコードをトレースして元のソースを突き止めるのに役立ちます。

  エンティティーに複数のアイデンティティーがある場合、強調表示することで、アイデンティティー同士を区別したり、そのアイデンティティーが常駐する元のデータ・ソースを識別するのに役立ちます。

ロール
: このエンティティーに解決されたアイデンティティーに割り当てられたロールが表示されます。

名前
: このエンティティーに解決されたアイデンティティーによって使用されている名前が表示されます。

住所　このエンティティーに解決されたアイデンティティーによって使用された既知の住所が、各住所がこのアイデンティティーに対して有効であった日付範囲を含めて (そのような情報を入手できた場合) 表示されます。

番号　このエンティティーに解決されたアイデンティティーによって使用された既知の各種番号が、各番号がこのアイデンティティーに対して有効であった日付範囲を含めて (そのような情報を入手できた場合) 表示されます。

特性　このエンティティーに解決されたアイデンティティーによって使用された既知の特性が、各特性がこのアイデンティティーに対して有効であった日付範囲を含めて (そのような情報を入手できた場合) 表示されます。

E メール・アドレス
このエンティティーに解決されたアイデンティティーによって使用された既知の E メール・アドレスが、各 E メール・アドレスがこのアイデンティティーに対して有効であった日付範囲を含めて (そのような情報を入手できた場合) 表示されます。

「開示 **(Disclosures)**」
2 つのアイデンティティーをリンクするために、アナリストまたは権限がある Visualizer ユーザーによって明示的に追加された、開示された関係が表示されます。開示によって、2 つのアイデンティティーの間に 100% の強度の関係が作成されます。

関連エンティティー
このエンティティーに関連したその他のエンティティーに関する基本情報をリストします。関連エンティティーを選択すると、関係を作成した情報が強調表示されます。

「ロール・アラート・ヒストリー **(Role Alert History)**」
このエンティティーに関連付けられたロール・アラートに関する基本情報をリストします。

「イベント・アラート・ヒストリー **(Event Alert History)**」
このエンティティーに関連付けられたイベント・アラートに関する情報が表示されます。

「印刷 **(Print)**」ボタン
エンティティー・レジュメを印刷できるように、プリント・ダイアログを開きます。

「レポート」ボタン
エンティティー・レジュメのすべての情報を含んだ「エンティティー・レジュメ **(Entity Resume)**」レポートを生成します。

「エンティティー関係グラフ **(Entity Relationship Graph)**」画面**:**

この画面を使用して、エンティティー属性、関連エンティティー、エンティティー・イベントなど、選択済みエンティティーの関係詳細をビジュアル表示します。

グラフ・エリア **(**キャンバス**)**

グラフの本体をキャンバスと呼びます。これには、関係のグラフィック表示が含まれ、エンティティー同士をリンクしている属性が示されます。

グラフ上でオブジェクト (ノード) をクリックして、グラフ上でそれらを位置変更します。ハイパーリンク属性が存在する場合は、**Ctrl** を押しながらクリックしてリンクをたどります。

右クリックのメニュー・オプション

グラフ・レイアウト

現在のレイアウトやグラフ・ノードの位置を変更します。グラフ上の各オブジェクトをノードと呼びます。

適切な設定が見つかるまで、いろいろなグラフ・レイアウト設定を試してください。これらの設定は、あくまでこのグラフでエンティティー関係を確認するためのものであり、ユーザーの好みやニーズに合わせて調整できます。

「アニーリング **(Anneal)**」
ノードを均等に分散させる場合、この設定を選択します。アニーリング設定は、グラフの辺の長さを均一にし、線の交差を最小限に抑え、ノードがグラフの端に寄りすぎるのを防ぎます。

「階層 **(Hierarchical)**」
階層に従ってノードを表示する場合、この設定を選択します。階層設定は、全体的なフローを示す有向グラフ、またはいくつかの開始ポイント、いくつかの終了ポイント、およびそれらのポイント間にあるいくつかの全体的なフローを示すグラフに最も適しています。

「オーガニック **(Organic)**」
グラフの頂点を均等に分散させる場合、この設定を選択します。オーガニック設定は、辺の長さを均一にし、グラフを対称に示します。ただし、関連エンティティーを表示することはできません。

「自己編成 **(Self Organizing)**」
リンクされたグラフ・ノードの等間隔クラスターを作成する場合、この設定を選択します。

「ランダム **(Random)**」
グラフ・ノードをランダムに分散させる場合、この設定を選択します。

「傾斜 **(Tilt)**」
以前に選択したグラフ・レイアウトのグラフ・ノードの配置を移動するか傾ける場合、この設定を選択します。

「円 **(Circle)**」
グラフ・ノードを整列させて、隣接するグラフ・ノードが等間隔に配置された円にする場合、この設定を選択します。

ズーム

現在の画面サイズ内でキャンバスのディスプレイ・サイズを変更するための設定を選択します。

75% グラフを元のサイズの 75% で表示します。

50% グラフを元のサイズの 50% で表示します。

「すべての属性の表示 **(Show All Attributes)**」
そのエンティティーに割り当てられているすべての属性が表示されます。

「属性の非表示 **(Hide Attribute)**」
選択した属性を非表示にします。

「関連エンティティーの表示 **(Show Related Entities)**」
そのエンティティーに関連したその他すべてのエンティティーが表示されるとともに、それらのエンティティー間の関係のグラフィカル表現も表示されます。現在のグラフ・レイアウトの設定が「オーガニック **(Organic)**」である場合、このオプションは使用できません。

「エンティティー・レジュメ **(Entity Resume)**」
「エンティティー・レジュメ (Entity Resume)」ウィンドウが開き、そのエンティティーに関してわかっているすべての情報の詳細な要約が表示されます。

「エンティティー・イベント **(Entity Events)**」
「エンティティー・イベント (Entity Events)」画面が開き、エンティティーに関連付けられているイベントに関する情報が表示されます。このオプションは、選択されたエンティティーに関連付けられたイベントがある場合にのみ使用可能です。

「エンティティー・グラフの表示 **(Show Entity Graph)**」
「エンティティー・グラフ (Entity Graph)」ウィンドウが開き、そのエンティティーのみに関する情報のビジュアル表示が提供されます。

グラフの調整オプション

ズーム・スライダー
キャンバスをサイズ変更する場合、ズーム・インディケーターを移動します。

「レイアウト制約 **(Layout Constraint)**」
キャンバス・サイズのレイアウト境界線制約を選択します。

プロパティー表

グラフ上でノードを選択すると、この表に、選択されたノード (属性またはエンティティー) のプロパティーが表示されます。

「ロール・アラート・グラフ **(Role Alert Graph)**」画面**:**

この画面を使用して、エンティティー属性、関連エンティティー、エンティティー・イベントなど、選択済みエンティティーのロール・アラート詳細をビジュアル表示します。

グラフ・エリア **(**キャンバス**)**

グラフの本体をキャンバスと呼びます。そこには、ロール・アラートの詳細のグラフィック表示が含まれています。

グラフ上でオブジェクト (ノード) をクリックして、グラフ上でそれらを位置変更します。ハイパーリンク属性が存在する場合は、**Ctrl** を押しながらクリックしてリンクをたどります。

右クリックのメニュー・オプション

右クリック・メニューから、グラフ表示を制御でき、関連したエンティティー・ウィンドウにナビゲートできるオプションも提供されます。

グラフ・レイアウト
: 現在のレイアウトやグラフ・ノードの位置を変更します。グラフ上の各オブジェクトをノードと呼びます。

  適切な設定が見つかるまで、いろいろなグラフ・レイアウト設定を試してください。これらの設定は、あくまでこのグラフでロール・アラートを確認するためのものであり、ユーザーの好みやニーズに合わせて調整できます。

  「アニーリング **(Anneal)**」
  : ノードを均等に分散させる場合、この設定を選択します。アニーリング設定は、グラフの辺の長さを均一にし、線の交差を最小限に抑え、ノードがグラフの端に寄りすぎるのを防ぎます。

  「階層 **(Hierarchical)**」
  : 階層に従ってノードを表示する場合、この設定を選択します。階層設定は、全体的なフローを示す有向グラフ、またはいくつかの開始ポイント、いくつかの終了ポイント、およびそれらのポイント間にあるいくつかの全体的なフローを示すグラフに最も適しています。

  「オーガニック **(Organic)**」
  : グラフの頂点を均等に分散させる場合、この設定を選択します。オーガニック設定は、辺の長さを均一にし、グラフを対称に示します。ただし、関連エンティティーを表示することはできません。

  「自己編成 **(Self Organizing)**」
  : リンクされたグラフ・ノードの等間隔クラスターを作成する場合、この設定を選択します。

  「ランダム **(Random)**」
  : グラフ・ノードをランダムに分散させる場合、この設定を選択します。

  「傾斜 **(Tilt)**」
  : 以前に選択したグラフ・レイアウトのグラフ・ノードの配置を移動するか傾ける場合、この設定を選択します。

  「円 **(Circle)**」
  : グラフ・ノードを整列させて、隣接するグラフ・ノードが等間隔に配置された円にする場合、この設定を選択します。

ズーム
: 現在の画面サイズ内でキャンバスのディスプレイ・サイズを変更するための設定を選択します。

  75% グラフを元のサイズの 75% で表示します。

  50% グラフを元のサイズの 50% で表示します。

「すべての属性の表示 **(Show All Attributes)**」
: そのエンティティーに割り当てられているすべての属性が表示されます。

「属性の非表示 **(Hide Attribute)**」
: 選択した属性を非表示にします。

「関連エンティティーの表示 **(Show Related Entities)**」
そのエンティティーに関連したその他すべてのエンティティーが表示されるとともに、それらのエンティティー間の関係のグラフィカル表現も表示されます。現在のグラフ・レイアウトの設定が「オーガニック **(Organic)**」である場合、このオプションは使用できません。

「エンティティー・レジュメ **(Entity Resume)**」
「エンティティー・レジュメ (Entity Resume)」ウィンドウが開き、そのエンティティーに関してわかっているすべての情報の詳細な要約が表示されます。

「エンティティー・イベント **(Entity Events)**」
「エンティティー・イベント (Entity Events)」画面が開き、エンティティーに関連付けられているイベントに関する情報が表示されます。このオプションは、選択されたエンティティーに関連付けられたイベントがある場合にのみ使用可能です。

「エンティティー・グラフの表示 **(Show Entity Graph)**」
「エンティティー・グラフ (Entity Graph)」ウィンドウが開き、そのエンティティーのみに関する情報のビジュアル表示が提供されます。

グラフの調整オプション

ズーム・スライダー
キャンバスをサイズ変更する場合、ズーム・インディケーターを移動します。

「レイアウト制約 **(Layout Constraint)**」
キャンバス・サイズのレイアウト境界線制約を選択します。

プロパティー表

グラフ上でノードを選択すると、この表に、選択されたノード (属性またはエンティティー) のプロパティーが表示されます。

Visualizer によるデータの追加

一般に、エンティティー・データは、システム・オペレーターによって UMF データ・ファイルを使用して、バッチ・モードまたはリアルタイム処理でパイプラインにロードされます。しかし、Visualizer のユーザーは、Visualizer を使用して単一のエンティティーを手動で追加したり、2 つのエンティティー間の関係を (アイデンティティーによって) 開示したり、UMF データ・ファイルをロードして処理したり、UMF データ・ファイルの妥当性をロード前に検査したりすることができます。

始める前に

データを追加するには、データを処理するために使用可能な稼働中のパイプラインが常に必要です。しかし、Visualizer のユーザーは、ユーザー独自のパイプラインを開始したり実行したりする必要はありません。Visualizer は、データを追加するとき、指定された Visualizer パイプラインを介してデータを自動的に送信します。

単一のエンティティーの追加

UMF レコードを手動で作成しなくても、単一のエンティティーをエンティティー・データベースに追加することができます。エンティティーは名前情報を指定するだけでも作成できますが、最適なエンティティー解決と関係解決のために、そのエンティティーについて分かっている情報 (既知の住所、番号、特性、E メール・アドレス) をできるだけ多く入力してください。

手順

1. Visualizer で、以下のいずれかを実行します。
   a. 「表示 **(View)**」 > 「追加 **(Add)**」 > 「エンティティー **(Entity)**」をクリックします。
   b. ツールバーで、(追加) アイコンをクリックして「エンティティー **(Entity)**」を選択します。
   c. ツールバーで、矢印をクリックして「エンティティー **(Entity)**」を選択します。
   d. 「追加 **(Add)**」ウィンドウの「追加 **(Add)**」ドロップダウンで、「エンティティー **(Entity)**」を選択します。
2. ドロップダウン・リストと各フィールドを使用して、エンティティーに関する情報を入力します。 データを入力するとき、ユーザーのためのガイドとして、画面の必須フィールドが黄色で強調表示されます。黄色で強調表示されるフィールドは、その画面でのユーザーによる他の選択に基づいて、黄色で強調表示されるすべてのフィールドにデータを入力する必要があることを示しています。
   - 「参照 **(Reference)**」フィールド: このフィールドには、必ず情報を入力してください。この参照情報は、アイデンティティーの ID です。例えば、銀行口座など、データ・ソース・アカウント番号を入力します。
   - 名前フィールド: 名前のいずれかの部分 (ファーストネーム、ミドルネーム、または世代) を入力する場合、ラストネームは必須です。
   - 住所フィールド: 市区町村、都道府県、郵便番号、または国を入力しなくても、「住所 **(Address)**」フィールドに情報を追加できます。ただし、住所の他の部分を入力した場合は、必ず「住所 **(Address)**」フィールドに情報を入力する必要があります。
   - 番号、特性、または E メールのフィールド: これらの属性のいずれかに情報を入力する場合は、属性のタイプを選択して、値を入力する必要があります。

   重要**:** この画面で入力したすべての情報は、追加するエンティティーの一部になります。他のエンティティーとの関係や、共有される特性や番号を示すものではありません。追加するエンティティーに属する情報だけを入力してください。例えば、そのエンティティーに関連付けられている別名や他の名前、そのエンティティーに関連付けられている住所、番号、特性、および E メール・アドレスなどです。
3. 「送信 **(Submit)**」をクリックします。

タスクの結果

Visualizer は、このエンティティーについて入力されたすべての情報を含む UMF アイデンティティー・レコードを作成し、パイプラインへ送信します。そのレコー

ドはパイプラインでエンティティー解決と関係解決のために処理され、エンティティー・データベースに追加されます。

ファイルからのデータのロード

Visualizer の「ファイル・ロード **(File Load)**」機能を使用して、UMF ファイルに定義されている複数のアイデンティティーのデータをロードします。「ファイル・ロード **(File Load)**」では、<UMF_ENTITY> レコードのみがロードされます。 UMF ファイルを選択すると、システムによってファイルが開かれ、データがパイプラインにロードされます。その後、パイプラインによってファイル内のアイデンティティーが処理されます。この処理によりアイデンティティーがエンティティー・データベースに追加され、エンティティーおよび識別された関係が解決されます。構成されたルールに基づいてアラートが生成されます。

このタスクについて

エンティティー解決と関係解決はパイプライン・コンポーネント内で行われます。Visualizer から UMF ファイルをロードして処理するには、稼働中で、Visualizer サーバーと通信できるパイプラインが存在しなければなりません。

ファイルをロードする前に、ファイル内の UMF を検証し、ファイルにエラーが含まれないことを確認することをお勧めします。

手順

1. Visualizer で、以下のいずれかのアクションを実行します。
   a. 「表示 **(View)**」 > 「**UMF**」 > 「ファイル・ロード **(File Load)**」をクリックします。
   b. ツールバーから、(UMF) アイコンをクリックします。
   c. 「**UMF**」ウィンドウの「**UMF**」ドロップダウン・フィールドで、「ファイル・ロード **(File Load)**」を選択します。
2. 「ファイルのロード**... (Load File...)**」をクリックしてロードする UMF ファイルを選択し、「開く **(Open)**」をクリックします。 システムによって選択済みファイルがパイプラインにロードされ、パイプラインがファイル内のデータの処理を開始します。「ファイル進行状況表示バー **(File progress bar)**」に、処理の経過時間、処理されたレコード数、およびファイル・ロードの状況が表示されます。
   a. ファイルのロードと処理を停止するには、(「停止 (Stop)」) アイコン・ボタンをクリックします。
   b. ファイルのロードと処理を一時停止するには、(「一時停止 (Pause)」) アイコン・ボタンをクリックします。
   c. 一時停止した後、ファイルのロードと処理を再開するには、(「続行 (Continue)」) アイコン・ボタンをクリックします。

   ファイル内のデータがロードされるのにともない、パイプラインは、エンティティー解決および関係解決によってデータを処理します。エラーが表示された場合、システム・アドミニストレーターに連絡してください。エラーの原因はパイプラインの問題である可能性が高いといえます。

新しいアイデンティティーは、解決されたエンティティーおよび関係とともにデータベースに追加されます。システムは、構成されているシステム・ルールに基づいて、データに関するアラートを生成します。

3. オプション: ファイルがロードされ、処理されたら、「結果の表示 **(View Results)**」をクリックして「ファイル・ロードの結果 **(File Load Results)**」ダイアログを表示します。このダイアログには以下の情報が組み込まれています。
   - パイプラインに送信されたレコードの数。
   - ロードしたファイル内のデータに基づいて、エンティティー・データベースに作成された新規エンティティーの数。
   - このファイル内のデータを処理中にパイプラインで検出された UMF 例外の数。(この数値は、パイプラインによるデータの完全な処理を妨害した UMF ファイル内のエラーまたは構文の問題を示していることがあります。)

次のタスク

「ファイル・ロードの結果 **(File Load Results)**」ダイアログに、ロードしたファイル内に UMF 例外が存在したことが示されている場合、エラーを修正できるように、ファイル内のエラーを見つけるのを支援する「UMF ファイル検証 (UMF File Validation)」機能を使用してファイルを確認してください。エラーの修正が終了したら、エラーが含まれていたデータを再ロードし、パイプラインがそのデータを完全に処理できるようにしてください。

データをロードする前の UMF ファイルの検証

Visualizer を使用して小さい UMF ファイルでレコードをロードして処理する予定がある場合は、まず、ファイル内のデータを検証することをお勧めします。

このタスクについて

検証処理では、データがエンティティー解決処理および関係解決処理の最小要件を満たしているかどうかが検査されます。また、検証処理によって、データをロードして処理する前に確認または訂正すべきファイルの領域に関する有用な情報も提供されます。システムに入力されるデータの品質が高いほど、良好な結果が得られます。

手順

1. Visualizer で、以下のいずれかのアクションを実行します。
   - 「表示 **(View)**」 > 「**UMF**」 > 「**UMF ファイル検証 (UMF Validate File)**」をクリックします。
   - ツールバーで、アイコンの右側の矢印をクリックし、「**UMF ファイル検証 (UMF Validate File)**」をクリックします。
   - 「**UMF**」ウィンドウの「**UMF**」リストで、「**UMF ファイル検証 (UMF Validate File)**」を選択します。
2. 「ファイルの検証**... (Validate File...)**」をクリックします。
3. 検証する UMF ファイルを選択します。

   注**:** 既に 1 つ以上の UMF ファイルの検証を行っていて、「**UMF**」ウィンドウを開いたままにしていた場合、「検証するファイル **(File to Validate)**」と「エ

ラー/警告ファイル **(Error/Warning File)**」の両方のフィールドが、前回の UMF ファイル検証の値を含んでいます。

4. オプション: 「**UMF** 検証セットアップ **(UMF Validation Setup)**」ウィンドウで検証処理のログ・ファイルのディレクトリー・パスまたはファイル名を変更するには、以下のいずれかのアクションを選択します。
   - 使用するディレクトリーとファイル名を選択し、「参照**... (Browse...)**」をクリックし、「開く **(Open)**」をクリックします。
   - 検証エラーおよび警告ログ・ファイルの絶対パスとファイル名を入力します。既存のログ・ファイルの名前または新規ログ・ファイルの名前を入力できます。

   注**:** 複数の UMF ファイルを検証し、「**UMF**」ウィンドウを開いたままにしていた場合、「**UMF** 検証セットアップ **(UMF Validation Setup)**」ウィンドウのログ・ファイルの値は、デフォルトで前回の検証エラーおよび警告ログ・ファイルと同じパスおよびファイル名に設定されるので注意してください。「**UMF**」ウィンドウを閉じると、パスおよびログ・ファイルのフィールドはクリアされます。
5. 「**UMF** ファイルの検証 **(Validate UMF File)**」をクリックして検証処理を開始します。 検証処理の実行中は、完了したパーセンテージ、経過時間、処理されたレコード数、および処理の状況に関する動的情報を含む、検証の統計が表示されます。検証処理はいつでも一時停止したり停止したりできます。
6. オプション: 「**UMF** ファイルの検証 **(Validate UMF File)**」をクリックしたときに、ステップ 4 で入力した名前と同じ名前を持つ別の検証ログ・ファイルが同じ場所に存在していた場合、システムは情報メッセージを表示してユーザーに通知します。メッセージには、ファイルの名前とロケーションが含まれています。以下のいずれかのアクションを実行してください。
   - 同じ検証エラーおよび警告ログ・ファイルを使用する場合は、「はい **(Yes)**」をクリックします。これを選択すると、前のログ・ファイルは上書きされます。
   - 別の検証エラーおよび警告ログ・ファイルを作成または使用する場合は、「いいえ **(No)**」をクリックします。システムによって「**UMF** 検証セットアップ **(UMF Validation Setup)**」ウィンドウが表示されるので、ユーザーはそこに戻って、検証エラーおよび警告ログ・ファイルのパスとファイル名を手動で変更できます。
7. 検証処理が完了した後、結果の要約を確認する必要がある場合は、「結果の表示 **(View Results)**」をクリックします。

次のタスク

「**UMF** 検証結果ビュー **(UMF Validation Results View)**」ウィンドウの情報を使用して、結果やエラーおよび警告ログ・ファイル内の情報を表示します。

アイデンティティー間の関係の開示

2 つのアイデンティティー (またはアカウント) をリンクしているデータが存在すると判断した場合、Visualizer を使用して、そのリンクを指定して関係を開示できます。

手順

1. Visualizer で、以下のいずれかを実行します。
   a. 「表示 **(View)**」 > 「追加 **(Add)**」 > 「開示 **(Disclosure)**」をクリックします。
   b. ツールバーで、(追加) アイコンの右側の矢印をクリックし、「開示 **(Disclosure)**」を選択します。
   c. 「追加 **(Add)**」ウィンドウの「追加 **(Add)**」ドロップダウンで、「開示 **(Disclosure)**」を選択します。
2. 必須: 「エンティティー **ID (Entity ID)**」フィールドで、関連付ける各アイデンティティーを含んでいるエンティティーのエンティティー ID 番号を入力します。
3. 必須: 各エンティティー ID の「ルックアップ **(Lookup)**」をクリックして、関連したアイデンティティーを取得します。 取得されたアイデンティティーのリストを見直して、意図したエンティティー ID を入力したことを確認します。
4. エンティティーごとに、関係を開示するアイデンティティー (またはデータ・ソース・アカウント) のオプション・ボタンを選択します。
5. 「開示された関係の説明 **(Disclosed Relationship Description)**」に、アイデンティティー同士がどのように関連しているかの説明を入力します。
6. 「作成」をクリックします。 開示された関係が正常に作成されたことを示す確認ボックスが表示されます。

ヘルプ・トピック

「エンティティーの追加」ウィンドウ**:**

このウィンドウを使用して、Visualizer から単一の新しいアイデンティティーをエンティティー・データベースに追加します。この画面で入力する情報はすべて、新しく作成されるアイデンティティーの属性になります。(アイデンティティーは 1 つずつ作成します。) アイデンティティー用に入力したデータを送信すると、エンティティー解決および関係解決のためにシステムによってパイプライン経由でデータが処理されます。この処理の間に、アイデンティティーは 1 つ以上の既存のエンティティーに関連付けられます。

データ・ソース・コード **-** 説明
: 追加するアイデンティティーに関連付けるデータ・ソースを選択します。データ・ソースはシステム内に存在しなければなりません。(ここで新規データ・ソースを追加することはできません。使用する必要があるデータ・ソース・コードと説明が表示されない場合は、システム・アドミニストレーターに連絡して、データ・ソースの作成を依頼してください。)

  アイデンティティーを追加するには、データ・ソース・コードと説明が必要です。

「参照 **(Reference)**」
: このデータ・ソース・アカウントの ID を入力します。これは、アカウントを現在入力中のアイデンティティーと関連付けるために使用されます。 (参照番号の例には、ケース番号、銀行口座番号、カスタマー・ポイントカード番号などがあります。)

アイデンティティーを追加するには、参照が必要です

「名前リスト **(Name List)**」

追加する単一アイデンティティーに関連付ける名前を入力します。アイデンティティーを追加するには、名前情報 (少なくともラストネームとファーストネーム) が必要です。追加するアイデンティティーが複数の名前を保持している場合、名前のそれぞれを別々の行に入力することで、そのことを指示できます。例えば、アイデンティティーの正式な名前と、1 つ以上の別名 (通称) の両方がわかっている場合、それらのすべてをこの画面で入力できます。

注**:** 1 行につき 1 つの名前のみを入力してください。

このリストに入力したすべての名前が、そのアイデンティティーの属性として、新しく作成されたアイデンティティーに自動的に関連付けられます。例えば、「Robert Hays」と「Bob J. Hayes, Jr.」を入力した場合、この両方の名前が、新しく作成されるアイデンティティーに関連付けられます。

「住所リスト **(Address List)**」

追加するアイデンティティーに関連付けられる 1 つ以上の住所を入力します。例えば、アイデンティティーの現在および以前の住所がわかっている場合、すべての完全な住所を 1 行に 1 住所ずつ入力します。このリスト・セクションに入力したすべての住所が、追加するアイデンティティーに自動的に関連付けられます。

アイデンティティーを追加する際、住所は必須ではありません。このアイデンティティーに関してわかっている住所がない場合、このリスト・セクションはブランクのままにできます。

住所　通常、この情報は、「住所 1 (Address 1)」の行と「住所 2 (Address 2)」の行に入力された情報です。例: 555 Main Street Building 17 Suite 102-B

いずれかの住所フィールドにデータを入力した場合、「住所」フィールドにもデータを入力しなければなりません。

「開始日 **(From Date)**」

このアイデンティティーに対してこの住所情報が有効になった日付がわかっている場合、それを入力します。例えば、このアイデンティティーが 1999 年 3 月 15 日からこの住所であることがわかっている場合、その日付を入力します。

「終了日 (Thru Date)」がなくとも「開始日 (From Date)」を入力できます。

「終了日 **(Thru Date)**」

このアイデンティティーに対してこの住所情報が無効になった日付がわかっている場合、それを入力します。例えば、このアイデンティティーが 2001 年 6 月 1 日を最後にこの住所を離れたことがわかっている場合、その日付を入力します。

「開始日 (From Date)」がなくとも「終了日 (From Date)」を入力できます。

「番号リスト **(Number List)**」
追加するアイデンティティーに関連付けられる 1 つ以上の番号を指示します。例えば、アイデンティティーによって使用されるクレジット・カード、運転免許証の番号、ID 番号、パスポート番号、電話番号などがわかっている場合、それぞれの番号を別々の行に入力します。このリスト・セクションに入力したすべての番号が、追加するアイデンティティーに自動的に関連付けられます。

アイデンティティーを追加する際、各種番号は必須ではありません。したがって、このリスト・セクションはブランクのままにできます。ただし、いずれかの番号データを入力する場合、「番号タイプ **(Number Type)**」フィールドと「値」フィールドの両方が必須になります。

「番号タイプ **(Number Type)**」
使用可能な番号タイプのドロップダウン・リストから番号タイプを選択します。これらの番号タイプはシステム内に存在しなければなりません。(ここで新規番号タイプを追加することはできません。使用する必要がある番号タイプが表示されない場合は、システム・アドミニストレーターに連絡して、作成を依頼してください。)

追加するアイデンティティーに番号を関連付ける場合は、番号タイプを選択する必要があります。

値　選択した番号タイプの番号の値を入力します。例えば、このアイデンティティーにパスポートを関連付ける場合、ここでパスポート番号を入力します。

追加するアイデンティティーに番号を関連付ける場合は、番号タイプに対応する番号の値を入力する必要があります。

「ロケーション **(Location)**」
番号に関連したロケーションがわかっている場合、またはそのようなロケーションが存在する場合、それを入力します。例えば、このアイデンティティーにパスポートを関連付ける場合、パスポートを発行した国の名前をここに入力します。または、運転免許証であれば発行した都道府県の名前を入力します。

「開始日 **(From Date)**」
このアイデンティティーに対してこの番号情報が有効になった日付がわかっている場合、それを入力します。「終了日 (Thru Date)」がなくとも「開始日 (From Date)」を入力できます。

「終了日 **(Thru Date)**」
このアイデンティティーに対してこの番号情報が無効になった日付がわかっている場合、それを入力します。例えば、運転免許証、パスポート、またはクレジット・カードの有効期限です。

「開始日 (From Date)」がなくとも「終了日 (From Date)」を入力できます。

「特性リスト **(Characteristic List)**」
追加するアイデンティティーに属している、または関連付けられる 1 つ以上の特性を指示します。例えば、システムで生年月日、婚姻状況、目の色、身長などの特性を収集する場合、すべてのわかっている特性をこのリストで

1 行に 1 つずつ入力できます。このリスト・セクションに入力したすべての特性が、追加するアイデンティティーに自動的に関連付けられます。

アイデンティティーを追加する際、特性は必須ではありません。したがって、このリスト・セクションはブランクのままにできます。ただし、いずれかの特性データを入力する場合、すべての特性フィールドが必須になります。

タイプ

使用可能なタイプのドロップダウン・リストから特性タイプを選択します。特性タイプはシステム内に存在しなければなりません。(ここで新規タイプを追加することはできません。使用する必要がある特性タイプが表示されない場合は、システム・アドミニストレーターに連絡して、特性タイプの作成を依頼してください。)

追加するアイデンティティーに特性を関連付ける場合は、特性タイプを選択する必要があります。

値　特性の値を入力します。追加するアイデンティティーに特性を関連付ける場合は、特性タイプに対応する特性の値を入力する必要があります。

「開始日 **(From Date)**」

このアイデンティティーに対してこの特性が有効になった日付がわかっている場合、それを入力します。「終了日 (Thru Date)」がなくとも「開始日 (From Date)」を入力できます。

「終了日 **(Thru Date)**」

このアイデンティティーに対してこの特性が無効になった日付がわかっている場合、それを入力します。「開始日 (From Date)」がなくとも「終了日 (From Date)」を入力できます。

「**E** メール・リスト **(Email List)**」

追加するアイデンティティーに属している、または関連付けられる 1 つ以上の E メール・アドレスを指示します。すべてのわかっている E メール・アドレスをこのリストに入力します。1 行に 1 つの E メール・アドレスを入力します。このリスト・セクションに入力したすべての E メール・アドレスが、追加するアイデンティティーに自動的に関連付けられます。

アイデンティティーを追加する際、E メール・アドレスは必須ではありません。したがって、このリスト・セクションはブランクのままにできます。ただし、E メール・データを入力する場合、「タイプ」フィールドと「アドレス」フィールドの両方が必須になります。

タイプ

使用可能なタイプのドロップダウン・リストから E メール・アドレスのタイプを選択します。E メール・アドレス・タイプはシステム内に存在しなければなりません。(ここで新規タイプを追加することはできません。使用する必要がある E メール・アドレス・タイプが表示されない場合は、システム・アドミニストレーターに連絡して、E メール・アドレス・タイプの作成を依頼してください。)

追加するアイデンティティーに E メール・アドレスを関連付ける場合は、タイプを選択する必要があります。

値　　完全な E メール・アドレスを入力します。追加するアイデンティティーに E メール・アドレスを関連付ける場合は、E メール・アドレス・タイプに対応する E メール・アドレスの値を入力する必要があります。

「開始日 **(From Date)**」
このアイデンティティーに対してこの E メール・アドレス情報が有効になった日付がわかっている場合、それを入力します。例えば、この E メール・アカウントが開設された日付がわかっている場合は、それをここに入力できます。

「終了日 (Thru Date)」がなくとも「開始日 (From Date)」を入力できます。

「終了日 **(Thru Date)**」
このアイデンティティーに対してこの E メール・アドレス情報が無効になった日付がわかっている場合、それを入力します。例えば、この E メール・アカウントが解約された日付がわかっている場合は、それをここに入力できます。

「開始日 (From Date)」がなくとも「終了日 (From Date)」を入力できます。

「送信 **(Submit)**」ボタン
追加するアイデンティティーに関してわかっている情報および必要な情報をすべて入力したら、エンティティー解決および関係解決を通してアイデンティティーを処理し、アイデンティティーをエンティティー・データベースに追加するために、「送信 **(Submit)**」をクリックします。

「リセット」ボタン
情報を送信しないで、入力したすべての情報をウィンドウからクリアするには、「リセット」ボタンをクリックします。アイデンティティーは、エンティティー解決および関係解決によって処理されず、エンティティー・データベースにも追加されません。

「開示の追加 **(Add Disclosure)**」ウィンドウ**:**

このウィンドウを使用して、既存の 2 つのアイデンティティー間の関係を開示します。関係を開示することにより、アイデンティティー間のリンクを作成するとともに、それらのアイデンティティーを含んでいるエンティティー間のリンクも作成します。関係を開示することは、これら 2 つのアイデンティティー間のリンクがエンティティー解決と関係解決のいずれによっても事前に検出されなかったこと、2 つのアイデンティティーを手動でリンクする明確な理由があることを示しています。

「エンティティー **ID (Entity ID)**」
関連付ける必要がある各アイデンティティーのエンティティー ID 番号を各「エンティティー **ID (Entity ID)**」フィールドに 1 つずつ入力します。

「ルックアップ **(Lookup)**」
クリックして、入力したエンティティー ID に対応するアイデンティティー情報を表示します。両方のエンティティー ID 番号に対してこれを実行します。表示される情報を確認することで、エンティティー ID が、関連付けようと意図したアイデンティティーに対応していることを確認できます。対応

していなければ、アイデンティティーをリンクする前に、一方または両方のアイデンティティーのエンティティー ID を訂正できます。

オプション・ボタン **(**各エンティティー **ID** に関連付けられた各アイデンティティーの横**)**

両方のエンティティー ID に対して 1 つのアイデンティティーを選択します。これらの ID は、関連付ける必要がある 2 つのアイデンティティーです。

注**:** 各エンティティーに対して 1 つのアイデンティティーしか表示されない場合があります。これは、その時点でエンティティーがシステム内に 1 つのアイデンティティーしか保持していないことを意味します。

「開示された関係の説明 **(Disclosed Relationship Description)**」

選択済みの 2 つのアイデンティティーがどのようにリンクしているかについて、説明を入力します。この説明は、他の Visualizer ユーザーがこの関係を表示したとき、彼らにとって役立つ情報になります。そのようなユーザーが、これら 2 つのアイデンティティーがなぜ、どのようにリンクされているのかを理解するうえで役立ちます。

作成 「作成」をクリックすると、選択済みの 2 つのアイデンティティー間の関係が開示されます。システムは、両方のアイデンティティーに関する情報を処理のためにパイプラインから送信し、次に、両方のアイデンティティーならびにこれらのアイデンティティーに関連したすべてのエンティティーのデータを更新します。

「**UMF** ファイル・ロード **(UMF File Load)**」ウィンドウ**:**

このウィンドウを使用して、UMF ファイルから Visualizer 経由でエンティティー・データベースにデータをロードします。

ファイル・ロードのステータス・バー

開いてロードする UMF ファイルを選択してから「ファイルのロード**... (Load File...)**」ボタンをクリックすると、このステータス・バーに、ファイル内のデータの処理の進行状況が示されます。システムは、完了パーセンテージ、ファイルの処理が開始されてからの経過時間、およびシステム処理の状況などの統計を表示します。

「**(**続行**)**」ボタン

「(一時停止)」ボタンを使用してファイルのロードと処理を一時停止した場合に、ファイル内の残りの未処理レコードのロードと処理を再開するには、このボタンをクリックします。システムは、選択されたファイル内の次のレコードから処理を続行します。

「**(**一時停止**)**」ボタン

ファイルのロードと処理を一時的に休止する場合、このボタンをクリックします。ファイルはメモリー内に保持され、システムはどのレコードが既に処理されたかをトラッキングします。まだ処理されていないファイル内のレコードは、ユーザーがファイル・ロードを続行するまでエンティティー・データベース内には存在しません。

このボタンは、システムがファイルをロードしている間のみアクティブになります。

「**(停止)**」ボタン

ファイルのロードと処理を停止する場合、このボタンをクリックします。ファイルはメモリーからクリアされます。まだ処理されていないファイル内のレコードは、エンティティー・データベース内に存在しません。このファイル内のレコードのロードを続行するには、ファイルを再度ロードする必要があります。ファイルの再ロード時、既に処理されたレコードがあると、それらは再度処理されます。

このボタンは、システムがファイルをロードしている間のみアクティブになります。

「結果の表示 **(View Results)**」ボタン

このボタンをクリックすると、「ファイル・ロードの結果 **(File Load Results)**」ダイアログが表示されます。このダイアログには以下の情報が組み込まれています。

- パイプラインに送信されたレコードの数。
- ロードしたファイル内のデータに基づいて、エンティティー・データベースに作成された新規エンティティーの数。
- このファイル内のデータを処理中にパイプラインで検出された UMF 例外の数。(この数値は、パイプラインによるデータの完全な処理を妨害した UMF ファイル内のエラーまたは構文の問題を示していることがあります。UMF 例外の修正にあたっては、システム・アドミニストレーターに連絡して支援を求めてください。システム・アドミニストレーターは UMF 例外ログを確認して、詳細を入手できます。)
- ロードしたファイル内のデータに基づいて、作成されたロール・アラートの数。

「ファイルのロード**... (Load File...)**」ボタン

ファイルをパイプラインにロードし、エンティティー解決および関係解決のためにファイル内の各レコードの処理を開始するには、このボタンをクリックします。

「**UMF** ファイル検証 **(UMF Validate File)**」ウィンドウ**:**

このウィンドウを使用して、エンティティー解決および関係解決を介してロードおよび処理する必要がある UMF ファイル内のデータを検証します。最初にデータを検証することで、ファイルのロードおよび処理を行う前に、潜在的なエラーや警告を訂正できます。

「検証**... (Validate...)**」ボタン

「**UMF** 検証セットアップ **(UMF Validation Setup)**」ウィンドウが表示されます。ユーザーはそこで、検証する UMF ファイルを選択し、エラーおよび警告ログ・ファイルのパスとファイル名を設定し、UMF 検証プロセスを開始します。

「**UMF** 検証セットアップ **(UMF Validation Setup)**」ウィンドウを開いたまま別の UMF ファイルを検証した場合、「検証**... (Validate...)**」をクリックすると、パスやログ・ファイルのフィールドには、最後に検証された UMF ファイルのロケーションや最後のエラーおよび警告ログ・ファイルのロケーションが取り込まれます。同じファイルを再度検証することも、検証する新しい UMF ファイルを選択することもできます。

「**UMF** 検証セットアップ **(UMF Validation Setup)**」ウィンドウを閉じると、パスやログ・ファイルのフィールドはクリアされます。

Visualizer からのレポートの実行

Visualizer から、データ・ソース別に統計の要約を示すレポートや、アラートおよび開示された関係の表示や管理に役立つレポートを表示および印刷できます。

Visualizer でのレポートの表示と印刷

Visualizer 内のレポートを使用して、データ・ソース・ファイルの統計および品質要約を表示したり、自分自身に割り当てられたアラートの管理に役立てたり、開示された関係、イベント・アラート、またはイベント情報を確認したりします。レポートはオンラインで表示することも、ハードコピーを印刷することも可能です。

このタスクについて

大部分の Visualizer レポートは、「表示 **(View)**」メニューまたはツールバーからアクセスできます。しかし、「エンティティー・レジュメ (Entity Resume)」レポートや「イベント・アラート詳細 (Event Alert Detail)」レポートなどの一部のレポートは、特定の画面からのみ表示および印刷が可能になります。

レポートは、選択された Web ブラウザーに Adobe Acrobat Reader を使用して表示されます。Visualizer レポートを表示および印刷するには、Adobe Acrobat Reader バージョン 7.0 以降がワークステーションにインストールされている必要があります。

注**:** Visualizer クライアントからレポートに印刷されるシステム生成の日付とタイム・スタンプは、Visualizer アプリケーション・サーバーのタイム・ゾーンに合わせて調整されます。画面上に表示する場合は、Visualizer クライアントのタイム・ゾーンに合わせた正しい日付が表示されます。例えば、太平洋標準時 (PST) の Visualizer アプリケーション・サーバーに接続している東部標準時 (EST) の Visualizer クライアントの場合、画面上にはシステム生成の日付とタイム・スタンプとして 8:00 PM が表示されますが、EST Visualizer クライアントから印刷されるレポートには 5:00 PM と印刷されます。

手順

- 「属性アラート・ジェネレーター・ヒストリー・レポート (Attribute Alert Generator History Report)」、「属性アラート・ジェネレーター・レポート (Attribute Alert Generator Report)」、「属性アラート・レポート (Attribute Alert Report)」、「データ・ソース要約レポート (Data Source Summary Report)」、「開示レポート (Disclosure Report)」、「ロード要約レポート (Load Summary Report)」、または「ロール・アラート状況レポート (Role Alert Status report)」を表示するには、以下のようにします。
  1. 「表示 **(View)**」 > 「レポート **(Reports)**」をクリックしてから、表示または印刷するレポートを選択します。
  2. レポート基準を入力します。
  3. 「レポートの実行 **(Run Report)**」をクリックして、選択したレポートを生成します。

- 「エンティティー・レジュメ (Entity Resume)」レポートを表示するには、「エンティティー・レジュメ **(Entity Resume)**」画面で「レポート **(Report)**」をクリックします。
- 「ロール・アラート詳細 (Role Alert Detail)」レポートを表示するには、「ロール・アラート **ID (Role Alert ID)**」画面で「レポート **(Report)**」をクリックします。
- 「イベント・アラート詳細 (Event Alert Detail)」レポートを表示するには、「イベント・アラート **ID (Event Alert ID)**」画面で「レポート **(Report)**」をクリックします。
- 「すべてのイベント (All Events)」レポートを表示するには、「エンティティー・イベント **(Entity Events)**」画面で「レポート **(Report)**」をクリックします。

タスクの結果

システムにより、指定されたすべての基準に基づいて、選択されたレポートが生成され、レポートが別のウィンドウに表示されます。レポートを印刷するには、「プリンター **(Printer)**」アイコン・ボタンをクリックするか、Web ブラウザーの「印刷 **(Print)**」機能を使用してください。

「属性アラート・ジェネレーター・ヒストリー・レポート **(Attribute Alert Generator History report)**」**:**

「属性アラート・ジェネレーター・ヒストリー・レポート (Attribute Alert Generator History report)」には、有効期限、ケース番号、コメント、または状況の変更など、属性アラート・ジェネレーターに対して行われた変更がリストされます。このレポートは、「検索エンティティー ID (Search Entity ID)」でソートされます。

「検索エンティティー **(Search Entity)**」
: 属性アラート・ジェネレーターの検索基準から取得したエンティティー ID (および、名前が指定されていた場合は名前も) が表示されます。

「作成日時 **(Date and Time Created)**」
: この属性アラート・ジェネレーターが作成された日時が表示されます。

「状況ヒストリー **(Status history)**」セクション
: レポートのこのセクションには、属性アラート・ジェネレーターに対して行われた各更新が、最新 (最後) の更新から順に表示されます。

  コメント
  : 更新を行ったユーザーが入力したコメントが表示されます。

  「更新日時 **(Date and time updated)**」
  : この属性アラート・ジェネレーターが最後に変更された日時が表示されます。この属性アラート・ジェネレーターがこれまで変更されたことがない場合、この日時は「作成日時 **(Date and Time Created)**」と同じ日時になります。

「有効期限日時 **(Date and time of expiration)**」
この属性アラート・ジェネレーターの有効期限に設定された日時、またはこの属性アラート・ジェネレーターが属性アラートを生成する最後の日付が表示されます。

状況　属性アラート・ジェネレーターがアクティブか期限切れかを示します。

ユーザー
この更新を行ったユーザーの名前が表示されます。

「アナライザー・グループ **(Analyzer Group)**」
この属性アラート・ジェネレーターを最後に変更したユーザーが属している Visualizer アナライザー・グループが表示されます。

「最小解決スコア **(Min. Resolution Score)**」
属性アラート・ジェネレーターの基準の一部として選択された最小解決スコアと最小スコアの説明を示します。このスコアしきい値によって、属性がどれくらい正確に一致している場合にこの属性アラート・ジェネレーターのアラートを生成するかを指示します。したがって、「同一エンティティー (Is Entity)」が、最も近い一致候補であり、「任意の関係 (Any Relationship)」が、最も遠い一致候補です。これらの各スコアのしきい値は、「画面設定の構成 **(Configure Screen Preferences)**」ウィンドウの「システム設定 **(System Preferences)**」画面で設定できます。

理由コード
この属性アラート・ジェネレーターに対してユーザーが選択した、理由を示すコードが表示されます。

「ケース番号 **(Case Number)**」
属性アラート・ジェネレーターを作成したユーザーによって入力されたオプションの英数字のケース番号が表示されます。

「属性アラート・ジェネレーター・レポート (Attribute Alert Generator report)」:

「属性アラート・ジェネレーター・レポート (Attribute Alert Generator report)」を使用して、属性アラート・ジェネレーターを管理します。このレポートを表示することで、システム内のすべての属性アラート・ジェネレーターの簡潔な要約を確認できます。そこには、各属性アラート・ジェネレーターが作成された日時、それぞれの有効期限が切れる日時、状況、属性アラート・ジェネレーターが最後に更新された日時などが含まれます。このレポートは、「検索エンティティー ID (Search Entity ID)」でソートされます。

「検索エンティティー **(Search Entity)**」
属性アラート・ジェネレーターによって作成された「検索エンティティー (Search Entity)」の ID を示します。

「作成日時 **(Date and Time Created)**」
この属性アラート・ジェネレーターが作成された日時を示します。

コメント
属性アラート・ジェネレーターの一部としてユーザーが追加したコメント・テキストが表示されます。

「更新日時 **(Date and time updated)**」
この属性アラート・ジェネレーターが最後に変更された日時を示します。この属性アラート・ジェネレーターがこれまで変更されたことがない場合、この日時は「作成日時 **(Date and Time Created)**」と同じ日時になります。

「期限切れの日時 **(Date and time expired)**」
この属性アラート・ジェネレーターの有効期限に設定された日時を示します。

状況　この属性アラート・ジェネレーターが最後に更新された日時における、この属性アラート・ジェネレーターのその時点での状況。

ユーザー
この属性アラート・ジェネレーターを最後に変更したユーザーを示します。属性アラート・ジェネレーターがこれまで変更されたことがない場合、このユーザー名は、元の属性アラート・ジェネレーターを作成したユーザーになります。

「アナライザー・グループ **(Analyzer Group)**」
この属性アラート・ジェネレーターを最後に変更したユーザーが属しているアナライザー・グループの名前を示します。

「最小解決スコア **(Min. Resolution Score)**」
属性アラート・ジェネレーターの作成時に「最小スコア **(Minimum Score)**」ドロップダウン・リストで選択された内容が表示されます。このスコアしきい値によって、属性がどれくらい正確に一致している場合にこの属性アラート・ジェネレーターのアラートを生成するかが決まります。

これらの各スコアのしきい値は、「ファイル」メニューからアクセスする「画面設定の構成 **(Configure Screen Preferences)**」ダイアログの一部である「システム設定 **(System Preferences)**」タブで設定します。

理由コード
属性アラート・ジェネレーターの理由を示す、ユーザーが選択したコード。

「ケース番号 **(Case Number)**」
属性アラート・ジェネレーターを作成したユーザーによって入力されたオプションの英数字のケース番号。

「属性アラート・レポート **(Attribute Alert Report)**」**:**

「属性アラート・レポート (Attribute Alert Report)」を使用して、個々の属性アラートを管理します。このレポートを表示することで、属性アラート・ジェネレーターの基準に一致したすべてのエンティティーのリストと、アラートの状況やアラートの最新のアクティビティーを確認します。

このレポートは、「検索エンティティー ID (Search Entity ID)」の昇順でソートされます。検索エンティティーごとに一致したエンティティーが複数存在する場合、一致したエンティティーはエンティティー ID の昇順でソートされます。

「検索エンティティー **(Search Entity)**」
属性アラート検索によって作成されたエンティティー ID が表示されます。

「一致エンティティー **(Matched Entity)**」
属性アラート・ジェネレーターの基準に基づいて、「検索エンティティー (Search Entity)」に一致したエンティティーの ID と名前が表示されます。属性アラートに複数の「一致エンティティー (Matched Entity)」がある場合、エンティティー ID の英数字順に表示されます。例えば、`Entity ID 37` は `Entity ID 1003` の前に表示されます。

「属性アラート情報 **(Attribute alert information)**」
レポートのこのセクションには、アラート結果に関する一般情報が表示されます。

「属性アラート状況 **(Attribute alert status)**」
この属性アラートの最新の状況が表示されます。

「検索結果の日時 **(Search result date and time)**」
属性アラートが作成された日時が表示されます。

「属性検索状況 **(Attribute search status)**」
この属性アラートを生成した属性アラート・ジェネレーターの最新の状況が表示されます。

「最小解決スコア **(Minimum resolution score)**」
属性アラート・ジェネレーターの基準の一部として選択された最小解決スコアと最小スコアの説明が表示されます。このスコアしきい値によって、属性がどれくらい正確に一致している場合に属性アラートを生成するかを指示します。

「属性アラート状況情報 **(Attribute Alert status information)**」
レポートのこのセクションには、このアラートに関する各状況のヒストリーが表示されます。状況情報は更新順に表示されます。したがって、最後に更新された状況が最初に表示されます。

「状況の日時 **(Date and Time of Status)**」
属性アラート更新が発生した日時が表示されます。

ユーザー
アラートを更新したユーザーの名前が表示されます。

「アクティビティー・コード **(Activity Code)**」
この属性アラートに対してユーザーが実行したアクションを示すユーザー定義のコードが表示されます。ユーザーはアラートを更新するとき、アクティビティー・コードを選択します。アクティビティー・コードの例の一部として「オープン (Open)」、「割り当て済み (Assigned)」、「保留 (Hold)」、「クローズ済み (Closed)」などがあります。アクティビティー・コードは構成コンソールで構成します。

状況　「状況の日時 (Status Date and Time)」に変更された、このアラート更新の後処理の状況が表示されます。後処理の状況は更新順に表示されます。したがって、最後に更新された状況が最後にリストされます。

コメント

このアラートに対する更新を行ったユーザーが入力したコメントが表示されます。

「マッチング情報 **(Matched information)**」

このセクションには、「検索エンティティー (Search Entity)」と「一致エンティティー (Matched Entity)」間でマッチングされた属性がデータ・タイプと値で表示されます。

「データ・タイプ **(Data Type)**」

「検索エンティティー (Search Entity)」と「一致エンティティー (Matched Entity)」間でマッチングされた属性の名前が表示されます。このマッチング属性の 2 つの値が、「マッチング値 (Match Value)」列と「検索基準 (Search Criteria)」列にそれぞれ表示されます。

「検索基準 **(Search Criteria)**」

「一致エンティティー (Matched Entity)」列に表示されている対応する値とマッチングされた「検索エンティティー (Search Entity)」に属するデータ値が表示されます。

「マッチング値 **(Match Value)**」

「検索エンティティー (Search Entity)」の同じデータ・タイプおよびデータ値とマッチングされた、「一致エンティティー (Matched Entity)」に属する実際のデータ値が表示されます。

「精度の説明 **(Precision Description)**」

「検索基準 (Search Criteria)」と「マッチング値 (Match Value)」のマッチングが行われた精度のレベルを記述したテキストが表示されます。精度レベルは、エンティティー解決構成時に属性別に構成されます。

「精度/最大精度 **(Precision/Max Precision)**」

最初の数値はシステムにより生成された精度スコアで、「検索基準 (Search Criteria)」の値と「マッチング値 (Match Value)」の値がどれくらい正確に一致したかを示します。2 番目の数値は、達成可能な最大精度スコアです。

2 つの数値を比較することで、「検索エンティティー (Search Entity)」と「一致エンティティー (Matched Entity)」の間の一致具合に関する詳細を判別できます。また、これらのスコアを使用して、属性アラートの検索基準を調整する必要があるかどうかを判別することもできます。

「スコア調整 **(Score Adjustment)**」

エンティティー解決時に解決スコアを上下に調整するのに使用された、この属性に関連付けられている数値が表示されます。この数値は全体的なエンティティー解決構成の一部として構成されます。

「データ・ソース要約レポート **(Data Source Summary Report)**」**:**

「データ・ソース要約レポート (Data Source Summary Report)」は、処理のためにシステムにロードされたレコードの簡潔な統計的要約をデータ・ソース別に提供

します。このレポートから、処理されたレコードの合計数をロード ID 別に確認できます。レポートでは、ロードされた合計レコード数のうち、新規アイデンティティーまたは新規エンティティーを表していたレコード数が表示されるほか、新規アイデンティティーに該当したレコードのパーセンテージと、新しく作成されたエンティティーに該当したレコードのパーセンテージが計算されます。

データ・ソース内のロード別統計

「ロードされた日付 **(Date Loaded)**」
このデータ・ソース・ファイルがロードされた日付が表示されます。

ロード **ID**
システムによって割り当てられたロード ID 番号が表示されます。

データ・ソース
ロードされたデータ・ソース・ファイルのデータ・ソース・コードと説明 (ダッシュで区切られています) が表示されます。

「ロードされた **UMF** レコード数 **(UMF Records Loaded)**」
ロードされたこのデータ・ソース・ファイル内のアイデンティティー・レコードの総数を示します。

「新規アイデンティティー数 **(New Identities)**」
ロードされたデータ・ファイルで発見された新しいアイデンティティーの総数を示します。(この数値は、以前にシステムによって処理されたことがないアイデンティティーの数を示します。)

「新規アイデンティティー **% (New Identity %)**」
新規アイデンティティーを表す、ロードされた合計レコード数のパーセンテージ (「新規アイデンティティー数 (New Identities)」を「ロードされた UMF レコード数 (UMF Records Loaded)」で除算した値) を示します。

「新規エンティティー数 **(New Entities)**」
このデータ・ロードによって作成された新規エンティティーの総数を示します。

「新規エンティティー **% (New Entities %)**」
新規エンティティーを表す、ロードされた合計レコード数のパーセンテージ (「新規エンティティー数 (New Entities)」を「ロードされた UMF レコード数 (UMF Records Loaded)」で除算した値) を示します。

データ・ソース別の統計グラフ

「データ・ソース別のロードされたレコード数 **(Records Loaded by Data Source)**」
指定されたその他のレポート基準に基づいて、各データ・ソースからシステムにロードされたレコードの数をグラフィカルに示した棒グラフが表示されます。最も多くのレコードまたは最も少ないレコードを提供したデータ・ソースを確認し、予想していたロード数と比較できます。

- 縦軸は、データ・ソース・コード別のデータ・ソース数を示します。
- 横軸は、ロードされたレコードの数を示します。

特定のデータ・ソースでロードされたレコード数が予想より少ない場合、このデータ・ソースのデータ・ファイルを調べることができます。 (データ品質はロードされるレコード数に直接的に影響するため、「ロード要約レポー

ト (Load Summary Report)」を実行して、このデータ・ソースでロードされたファイルのデータ品質を確認することも検討してください。)

「データ・ソース別の新規エンティティー数 **(New Entities by Data Source)**」
指定されたその他のレポート基準に基づいて、どのデータ・ソースが最も多い数の新規エンティティーを生成したかをグラフィカルに示した棒グラフが表示されます。

- 縦軸は、データ・ソース・コード別のデータ・ソース数を示します。
- 横軸は、作成された新規エンティティーの数を示します。

「開示レポート **(Disclosures report)**」**:**

このレポートを使用して、アイデンティティー間に作成された、開示された関係を表示および管理します。開示された関係とは、Visualizer ユーザーによって「開示の追加 **(Add Disclosures)**」画面で手動で作成されるか、開示された関係のタグ・ペア (<DR> と </DR>) を入力アイデンティティー・レコードに組み込むことで作成される関係です。

このレポートは関係 ID でソートされます。

「関係 **ID (Relationship ID)**」
関係の作成時に、各開示された関係に割り当てられる、システムによって生成される番号が表示されます。

「作成日時 **(Date and Time Created)**」
開示された関係が作成された日時が表示されます。

「関係の説明 **(Relationship description)**」
開示された関係を作成する理由を記述したテキストが表示されます。このテキストは、開示された関係を作成したユーザーによって入力されたものです。

「更新日時 **(Date and time updated)**」
この開示された関係が最後に更新された日時が表示されます。

状況　この開示された関係の状況が表示されます。

「削除された日付 **(Date deleted)**」
開示された関係が手動で削除された日時が表示されます。このフィールドは、ユーザーが関係を無効と判断し、開示された関係を削除した場合にのみ日時が埋められます。

データ・ソース
この開示された関係によってリンクされることになったエンティティーそれぞれのデータ・ソース・コードと説明が (それぞれに 1 つずつ、別々の行に) リストされます。データ・ソース・コードは、元のソース・ファイルを指しています。

外部 **ID**
この開示された関係によってリンクされることになったエンティティーそれぞれの外部 ID が (それぞれに 1 つずつ、別々の行に) リストされます。多くの場合、外部 ID は、エンティティーに排他的に属する、元のソース・ファイル内のアカウント番号を示します。

「イベント・アラート詳細 **(Event Alert Detail)**」レポート**:**

「イベント・アラート詳細 (Event Alert Detail)」レポートを使用して、特定のイベント・アラートおよびアラートに含まれるエンティティーに関する完全な詳細を表示します。このレポートは、「調査 **(Research)**」ウィンドウの「イベント・アラート **(Event Alert)**」タブのハードコピー・レポートが必要な場合に便利です。

アラート **ID**
: 特定のイベント・アラートの説明およびアラート ID が表示されます。レポートの見出しでは、アラート ID が説明の前に現れます。

「イベント・アラート情報 **(Event alert information)**」
: このセクションには、このアラートをトリガーしたイベント・アラート・ルールの説明、イベント・アラートの状況など、イベント・アラート全体の一般情報が表示されます。

  「アラートの日時 **(Alert date and time)**」
  : このイベント・アラートが生成された日時を示します。

  「ルール **ID (Rule ID)**」
  : イベント・アラート・ルールが最初に構成されたとき、システムによって生成された内部番号が表示されます。この ID は、このイベント・アラートをトリガーしたイベント・アラート・ルールに関連付けられています。

  「ルールの説明 **(Rule description)**」
  : イベント・アラート・ルールを構成したユーザーによって定義された、イベント・アラート・ルールを記述するテキストが表示されます。

  状況　このイベント・アラートの現在の状況を示します。

「イベント詳細 **(Event Details)**」
: このセクションは、イベント・アラート・データに関する詳細情報を提供します。

  「日付と時刻 **(Date and Time)**」
  : イベント・アラートが生成された日時を示します。

  データ・ソース
  : イベントごとに、イベント・データを提供したデータ・ソース・コードと説明が表示されます。この情報は元のソース・ファイルを識別します。

  外部 **ID**
  : イベントごとに、イベント・データを提供したデータ・ソース・コードに関連付けられている外部 ID が表示されます。多くの場合、この情報は、元のソース・ファイル内のエンティティーのアカウント番号を識別します。

  「イベント参照 **(Event Reference)**」
  : イベントごとに、イベント・プロセッサーの中で複合イベント・プロセッサーによって作成されたユニーク・コードが表示されます。

数量　イベントごとに、このイベントに含まれる数量を表す数値を示します。例えば、「1」は、「値」列の値が 1 回の電信送金を意味する場合があります。

値　イベントごとに、このイベントの合計値を示します。

エンティティー情報
このセクションは、イベントに含まれるエンティティーを対象に、イベントに関係していた属性タイプと属性タイプに関連付けられていた値のリストを提供します。

「アラートの後処理 **(Alert Dispositions)**」
このセクションは、イベント・アラートの状況の要約を提供します。

「アクティビティー・コード **(Activity Code)**」
このイベント・アラートの状況を変更したユーザーが選択したイベント・アクティビティー・コードが表示されます。

状況　イベント・アクティビティー・コードに関連付けられている状況 (「アクティブ」または「非アクティブ」) が表示されます。

「状況のコメント **(Status Comments)**」
この状況の更新に関して入力されたアナリストのコメントが表示されます。

ユーザー
このイベント・アラートの状況を変更したユーザーのユーザー ID を示します。

「日付と時刻 **(Date and Time)**」
状況が変更された日時を示します。

「ロール・イベント・アラート・ヒストリー **(Role Event Alert History)**」セクション　このセクションには、このイベント・アラートの原因であるエンティティーが含まれるすべてのロール・アラートがリストされます。

「イベント・アラート・ヒストリー **(Event Alert History)**」セクション
レポートのこのセクションには、メイン・イベント・アラートに含まれるエンティティーの完全なヒストリーがリストされます。このセクションを使用して、このエンティティーが含まれているイベント・アラートの数を表示します。

「アラート日時 **(Date and Time Alerted)**」
イベント・アラートが生成された日時を示します。

アラート **ID**
このイベント・アラートの ID が表示されます。

説明　このイベント・アラートをトリガーした複合イベント処理ルールを記述したテキストが表示されます。

「アクティビティー・コード **(Activity Code)**」
このアラートに対してユーザーが実行したアクションを示すユーザー定義のコードが表示されます。アクティビティー・コードは構成コンソールで構成され、アラートの更新時に Visualizer でドロップダウン・リストから選択されます。アクティビティー・コードの例

の一部として「割り当て済み (Assigned)」、「クローズ済み (Closed)」、「保留 (Pending)」などがあります。

状況
「状況の日時 (Status Date and Time)」に変更された、このアラート更新の状況が表示されます。状況は更新順に表示されます。したがって、最後に更新された状況が最後にリストされます。

「すべてのイベント **(All Events)**」レポート**:**

「すべてのイベント (All Events)」レポートを使用して、イベントによってイベント・アラートが生成されたかどうかにかかわらず、単一エンティティーに関連付けられているすべてのイベントを表示します。このレポートは、「調査 **(Research)**」ウィンドウの「エンティティー・イベント **(Entity Events)**」画面のハードコピー・レポートが必要な場合に便利です。レポートに表示されるイベントは、その画面で選択したイベント・タイプおよび日付範囲によって異なります。

イベント・タイプを選択しなかった場合、レポートには、定義した日付範囲内に含まれる、指定されたエンティティーのすべてのタイプのイベントが表示されます。イベント・タイプを選択した場合は、定義した日付範囲内に含まれるそのタイプのイベントのみが表示されます。

「基本レポート情報 **(Basic report information)**」
このセクションには、レポートの日付範囲や、イベントに関連付けられたエンティティーに関する詳細など、基本的なレポートのヘッダー情報が表示されます。

「レポート日付**:** 開始と終了 **(Report dates: From and Through)**」
レポートの開始日および終了日を示します。このエンティティーを対象に、日付範囲内で発生したイベントのみがレポートに表示されます。

「関連エンティティー **(Associated Entity)**」
これらのイベントに関連付けられているエンティティーのエンティティー ID を示します。

「現在の名前 **(Current name)**」
エンティティー・データベース内のエンティティーの最新の名前を示します。

「現在の住所 **(Current address)**」
エンティティー・データベース内のエンティティーの最新の住所を示します。

イベント情報
このセクションには、このエンティティーに関連付けられたイベントの詳細がイベント・タイプ別に表示されます。

イベント・タイプ
イベント・タイプの説明です。この説明は、構成コンソールでイベント・タイプに構成されます。

イベント **ID**
この特定のイベントを識別する、システムによって生成された番号が表示されます。

「作成日時 **(Create Date and Time)**」
イベントが発生した日時が表示されます。

データ・ソース
イベントに関連したデータ・ソース・コードおよびデータ・ソース説明が表示されます。

外部 **ID**
このイベントの元のデータ・ソース内のインバウンド・アイデンティティー・レコードを識別するユニーク・キーが表示されます。

「イベント参照 **(Event Reference)**」
イベントに関する追加情報が表示されます。通常は、イベントが発生したロケーションの名前になります。

「ロケーション **(Location)**」
イベントが発生したロケーションの住所情報が表示されます。

値　イベントに関連した数量値が表示されます。

数量　イベントに関連した単位の数が表示されます。

「計測単位 **(Unit of Measure)**」
イベント値に関連した計測単位を示します。計測単位は、構成コンソールでイベント・タイプ別に構成されます。計測単位は、値を理解するのに役立ちます。例えば、計測単位が米ドルで、イベントの値が 5000 である場合、このイベントに $5,000.00 が含まれていることがわかります。

「メモ **(Memo)**」またはカスタム・ラベル
イベント・トランザクションの詳細なコンテキストを提供する、メモやコメントなど、イベントに関する追加情報が表示されます。

ユーザーは、構成コンソールでイベント・タイプを構成するときにオプションの 1 つとして、この列のカスタム・ラベルを定義できます。「メモ **(Memo)**」の代わりに、ユーザーには、より説明的なカスタム・ラベルが表示される場合があります。例えば、「電信送金メモ」などです。

「追加メモ **(Additional Memo)**」またはカスタム・ラベル
使用可能な場合、イベントに関する詳細情報が表示されます。

ユーザーは、構成コンソールでイベント・タイプを構成するときにオプションの 1 つとして、この列のカスタム・ラベルを定義できます。「追加メモ **(Additional Memo)**」の代わりに、ユーザーには、より説明的なカスタム・ラベルが表示される場合があります。例えば、「担当者コメント」などです。

「ロード要約レポート **(Load Summary Report)**」**:**

「ロード要約レポート (Load Summary Report)」には、データ・ソース別の統計および品質特性の要約が示されます。そこには、データ・ソース・ファイルに関する情報が含まれています。このレポートを使用して、ロード・パフォーマンスの統計、ロードによって作成されたエンティティーおよびアラートの数、ロードされた

データのデータ品質に関する一般情報、UMF レコードに関するアクションのロード別の要約、およびロードによって生成された UMF 例外を判定します。レポートはロード ID ごとにグループ化されます。

レポートでは、ロードごとに統計が以下のセクションに分割されます。

- 「ロード要約 (Load Summary)」
- 「ロール・アラート要約 (Role Alert Summary)」
- 「関係要約 (Relationship Summary)」
- 「品質要約 (Quality Summary)」
- 「UMF 文書要約 (UMF Document Summary)」
- 「例外要約 (Exception Summary)」

「ロード要約 **(Load Summary)**」

このセクションを使用して、特定のファイルの処理にかかった時間を判定できるほか、このデータ・ソース・ファイルがエンティティー解決および関係検出の全体にとって、どれくらい有効であったかを総合的に判断します。

「開始日時 **(Date and Time Started)**」
データ・ロードが開始された日時を示します。

「完了日時 **(Date and Time Completed)**」
データ・ソース・ファイルのロードが終了した日時を示します。

「**UMF** レコード・カウント **(UMF Record Count)**」
「開始日時 **(Date and Time Started)**」から「完了日時 **(Date and Time Completed)**」の範囲内にこのデータ・ソース・ファイルからロードされたレコードの総数を示します。

「完了日時 **(Date and Time Completed)**」の数値から「開始日時 **(Date and Time Started)**」の数値を引くと、この特定のデータ・ソース・ファイルをロードするのにかかった分数がわかります。この分数を見るとシステム・パフォーマンスを推定できます。また、処理時間を短縮するために、大きいデータ・ソース・ファイルを小さいファイルに分割する必要があることを示唆している場合もあります。

「新規アイデンティティー数 **(New Identities)**」
「開始日時 **(Date and Time Started)**」から「完了日時 **(Date and Time Completed)**」の時間フレーム内でロードされた新規アイデンティティーの総数を示します。

「新規アイデンティティー **% (New Identity %)**」
このデータ・ロード内で、新規アイデンティティー (エンティティー・データベースにとって新しいアイデンティティー) であったアイデンティティー数合計のパーセンテージを示します。

「新規エンティティー数 **(New Entities)**」
「開始日時 **(Date and Time Started)**」から「完了日時 **(Date and Time Completed)**」の時間フレーム内で新しく作成されたエンティティーの総数を示します。

「新規エンティティー **% (New Entity %)**」

このデータ・ソース・ロードの結果として新しく作成されたエンティティーに該当するエンティティー数合計のパーセンテージを示します。

新規アイデンティティーおよび新規エンティティーの数から、このデータ・ソースがエンティティー解決および関係検出の全体にとって、どれくらい価値のあるものであったかという概要を把握できます。これらの数値が低く、かつ長期的に低いままであれば、このデータ・ソースは、ユーザーの会社のエンティティー解決の目標を達成するうえであまり有益でない可能性があります。

「ロール・アラート要約 **(Role Alert Summary)**」

このセクションを使用して、ロール・アラートの生成につながった、検出された関係に共通する解決ルールと解決スコアを確認します。各行に、リストされている基準に基づいて生成されたロール・アラートの数が提示されます。

「解決ルール **(Resolution Rule)**」

エンティティー解決および関係検出の中で、アイデンティティーとエンティティーを評価するために使用された解決ルールの名前が表示されます。

「アラート説明 **(Alert Description)**」

ロール・アラートをトリガーしたロール・アラート・ルールの名前が表示されます。

「重大度 **(Severity)**」

このロール・アラートの優先度または重要度を測るユーザー定義のインディケーターが表示されます。

「解決スコア **(Resolution Score)**」

ロール・アラートに含まれるアイデンティティーとエンティティーに対して判定された、解決ルールの解決スコア (0 から 100) が表示されます。このスコアは、アイデンティティーとエンティティー間の相似の度合いを示します。スコアが 100 の場合、そのアイデンティティー・レコードがそのエンティティーに解決されたことを意味します。

「アラート・カウント **(Alert Count)**」

ロール・アラート・ルールの説明、解決ルール、および解決スコアに基づいて生成されたロール・アラートの総数を示します。

「関係要約 **(Relationship Summary)**」

このセクションを使用して、ロール・アラートを生成しなかった、検出された関係に共通する属性を確認します。各行に、リストされている基準に基づいて検出された関係の数が提示されます。

「解決ルール **(Resolution Rule)**」

エンティティー解決および関係検出の中で、入力アイデンティティー・レコードと既存のエンティティーを評価するために使用された解決ルールの名前が表示されます。

「解決スコア **(Resolution Score)**」

エンティティー解決時にアイデンティティーとエンティティーに対して判定された、解決ルールの解決スコア (0 から 100) が表示されます。このスコ

アは、アイデンティティーとエンティティー間の相似の度合いを示します。スコアが 100 の場合、そのアイデンティティー・レコードがそのエンティティーに解決されたことを意味します。

「関係スコア **(Relationship Score)**」
関係解決時にアイデンティティーとエンティティーに対して判定された、解決ルールの関係スコア (0 から 100) が表示されます。このスコアは、アイデンティティーとエンティティー間の関係の度合いを示します。

マッチング属性に基づいて、関係スコアが高いほど、アイデンティティーとエンティティーがより密接に関連していることになります。

「関係カウント **(Relationship Count)**」
解決ルール、解決スコア、および関係スコアに基づいて検出された関係の総数を示します。

「品質要約 **(Quality Summary)**」

このセクションの情報を使用して、各データ・ソース・ファイル内のデータの品質を評価します。このセクションでは、UMF セグメントおよび UMF 文書タイプ内の属性タイプ別の品質を示します。品質要約と UMF 例外要約を一緒に確認することで、対応が必要な、品質の問題を含むデータ・ソース・ファイルや誤った形式の UMF を含むデータ・ソース・ファイルがわかります。通常は、データ・ソース・ファイルを処理する前に、ETL や DQM/データ・ソース構成によってこれらの問題を解決できます。

場合によって、このセクションから、特定のデータ・ソースの品質が低すぎるためにエンティティー解決にそのデータ・ソースを使用すべきでないと判断できます。

「文書タイプ **(Document Type)**」
「データ・タイプ (Data Type)」にリストされているデータ・タイプを含んでいる UMF 文書タイプの名前が表示されます。通常、この値は UMF_ENTITY です。

「表名 **(Table Name)**」
類似した名前の UMF セグメントからのデータを保管するデータベース表の名前が表示されます。例えば、NUMBER セグメントからのデータは NUMS 表に保管されます。

「データ・タイプ **(Data Type)**」
入力レコード属性タイプ UMF タグにリストされているデータ・タイプを示します。このタイプは、「表名 (Table Name)」にリストされる UMF セグメントに対応します。例えば、「表名 (Table Name)」が *ADDRESS* で、「データ・タイプ (Data Type)」に *H* とリストされる場合、品質情報の評価対象は住所タイプ *Home* (自宅) です。

データ・タイプに見覚えがない場合、データ・ソース・ファイルが、UMF 文書、UMF セグメント、および UMF タグの適切な組み合わせに正しくマップされていない可能性があります。「例外要約 (Exception Summary)」セクションで、同じ UMF セグメントおよび UMF タグによって 1 つ以上のセグメント例外が発生していないかどうか確認してください。無効な UMF が問題である場合、たいていは「品質要約 (Quality Summary)」セクションの「低品質カウント (Low Quality Count)」の数値と「UMF 例外

(UMF Exception section)」セクションの「セグメント例外カウント (Segment Exception Count)」の数値が一致します。

「レコード・カウント **(Record Count)**」
特定の「文書タイプ (Document Type)」、「表名 (Table Name)」、および「データ・タイプ (Data Type)」の入力アイデンティティー・レコードの総数を示します。

「汎用カウント **(Generic Count)**」
汎用値と見なされる値を含んでいる、特定の「文書タイプ (Document Type)」、「表名 (Table Name)」、および「データ・タイプ (Data Type)」を持つ入力アイデンティティー・レコードの総数を示します。

「低品質カウント **(Low Quality Count)**」
品質が低いと見なされる、特定の「文書タイプ (Document Type)」、「表名 (Table Name)」、および「データ・タイプ (Data Type)」を持つ入力アイデンティティー・レコードの総数を示します。この数値は、データ・ソース・ファイルのデータ入力または ETL 変換に問題があることを示している場合があります。

「使用可能パーセント **(Usable Percent)**」
特定の「文書タイプ (Document Type)」、「表名 (Table Name)」(この UMF セグメントの) 、および「データ・タイプ (Data Type)」を持ち、エンティティー解決および関係検出に使用可能な、入力アイデンティティー・レコードのパーセンテージを示します。 (「レコード・カウント (Record Count)」 - 「汎用カウント (Generic Count)」 - 「低品質カウント (Low Quality Count)」) ÷「レコード・カウント (Record Count)」= 「使用可能パーセント (Usable Percent)」です。

「アイデンティティー・パーセント **(Identity Percent)**」
特定の「文書タイプ (Document Type)」、「表名 (Table Name)」、および「データ・タイプ (Data Type)」を含んでいた入力アイデンティティー・レコードのパーセンテージを示します。

「属性要約 **(Attribute Summary)**」

このセクションを使用して、関係の検出やロール・アラートの生成に役立った、データ・ソース・ファイル内の属性を確認します。各属性は特定の UMF セグメントにマップされ、このセクションには、入力 UMF セグメント内のデータに基づいて検出された関係の数と生成されたロール・アラートの数が表示されます。

「セグメント名 **(Segment Name)**」
特定の属性に直接マップされる UMF セグメントの名前が表示されます。

「データ・タイプ **(Data Type)**」
「精度の説明 (Precision Description)」に対応している UMF セグメント内の属性タイプ (またはデータ・タイプ) がリストされます。レポートには特定の属性タイプがリストされる場合と、*ALL* がリストされる場合があります。後者は、UMF セグメントのすべての属性タイプを示しています。

「精度の説明 **(Precision Description)**」
インバウンド・アイデンティティーの属性と既存のエンティティーの属性間のマッチングしきい値を記述します。

ロール・アラート
この UMF セグメント、データ・タイプ、および精度の説明に基づいて生成されたロール・アラートの総数を示します。

関係　この UMF セグメント、データ・タイプ、および精度の説明に基づいて検出された関係の総数を示します。

「**UMF** 文書要約 **(UMF Document Summary)**」

このセクションを使用して、レコードに対して実行されるアクションに基づいて、データ・ソース・ファイル内の入力レコードの総数を検証できます。これらの数値を「ロード要約 (Load Summary)」セクションの「レコード・カウント (Record Count)」と照合できます。

「文書タイプ **(Document Type)**」
UMF 文書タイプの名前が表示されます。通常、この値は UMF_ENTITY です。

アクション
入力アイデンティティー・レコードに対するアクションのタイプを示します。以下に、最もよく使用されるアクションのリストを示します。

- *A* - 追加
- *C* - 変更
- *D* - 削除

システム処理時に各入力レコードに対してどのようなアクションを取るべきか指示するために、通常、ETL 処理の一環としてアイデンティティー・レコードには UMF によってタグが付けられます。

「**UMF** レコード・カウント **(UMF Record Count)**」
文書タイプ内でアクション・タイプごとの処理されたレコードの総数を示します。

「パーセント **(Percent)**」
「レコード・カウント (Record Count)」が表す、ロードされた合計レコード数のパーセンテージを示します。(合計は 100% を超えてはなりません。)

「例外要約 **(Exception Summary)**」

この情報を使用して、誤った形式の UMF など、問題のあるアイデンティティー・レコードを特定します。例外にはどのような問題かが記述され、表名とエレメントは、問題のあるセグメントとレコードを示しています。カウントには、ファイル内でそのような誤った UMF を含んでいたレコードの数が示されます。

「文書タイプ **(Document Type)**」
UMF 文書タイプの名前が表示されます。通常、この値は UMF_ENTITY です。

アクション
入力アイデンティティー・レコードに対するアクションのタイプを示します。

- *A* - 追加
- *C* - 変更

- *D* - 削除

システム処理時に各入力レコードに対してどのようなアクションを取るべきか指示するために、通常、ETL 処理の一環としてアイデンティティー・レコードには UMF によってタグが付けられます。

セグメント
例外が発生した UMF セグメントの名前が表示されます。

「**UMF** タグ **(UMF Tag)**」
UMF 例外の原因となった UMF タグの値が表示されます。

例外　発生した UMF 例外のタイプを示すメッセージ ID またはその他の例外コードが表示されるほか、例外を解決する方法についての情報が与えられます。この情報は、UMF_EXCEPT 表にも提供されます。

「セグメント例外カウント **(Segment Exception Count)**」
このタイプの UMF 例外の総数を示します。

「品質要約 (Quality Summary)」セクションの「低品質カウント (Low Quality Count)」で、一致するデータ・タイプが低品質または使用に耐えない品質として報告されていないかどうか確認してください。正しくない UMF が問題である場合、同じ UMF セグメントおよび UMF タグを対象に、たいていは「品質要約 (Quality Summary)」セクションの「低品質カウント (Low Quality Count)」の数値と「UMF 例外 (UMF Exception section)」セクションの「セグメント例外カウント (Segment Exception Count)」の数値が一致します。

「ロール・アラート詳細 **(Role Alert Detail)**」レポート**:**

「ロール・アラート詳細 (Role Alert Detail)」レポートを使用して、特定のロール・アラートに関する完全な詳細、および各隔たり度合いでアラートに含まれるエンティティーに関する完全な詳細を表示します。このレポートは、各ロール・アラートに含まれるエンティティーをさらに詳しく分析する場合に役立ちます。

このレポートは、隔たりの次数ごとに、アラートに含まれる 2 つのエンティティーをユーザーが比較対照できるように、それらのエンティティーに関する情報を表示します。次に、レポートは各エンティティーに関連付けられているその他のアラートを表示し、ユーザーが各エンティティーとそれに関連したロール・アラートの全体像を把握できるようにします。通常、各ロール・アラートに関する詳細は複数ページにまたがります。

アラート **ID**
特定のロール・アラートの説明およびアラート ID。レポートの見出しでは、アラート ID が説明の前に現れます。

「ロール・アラート情報 **(Role alert information)**」
このセクションには、このアラートをトリガーしたロール・アラート・ルールの説明、ロール・アラートの状況など、ロール・アラート全体の一般情報が表示されます。

「アラート日時 **(Date and time alerted)**」
このロール・アラートが生成された日時。

「ルール **ID (Rule ID)**」
ロール・アラート・ルールが最初に構成されたとき、システムによって生成された内部番号。この ID は、このロール・アラートをトリガーしたロール・アラート・ルールに関連付けられています。

「ルールの説明 **(Rule description)**」
ロール・アラート・ルールを構成したユーザーによって定義された、ロール・アラート・ルールを記述するテキスト。

「重大度 **(Severity)**」
このアラートの優先度または重要度を示すために使用されるユーザー定義のコード。

状況　このロール・アラートの現在の後処理。

「関係の信頼度 **(Relationship confidence)**」
「マッチング詳細: *n* 次 (Matching Details: Degree *n*)」セクションの下にリストされている 2 つのエンティティーがどれくらい密接に関連しているかを表すスコア。スコアが高いほど、より密接に関連していることになります。スコアが 100 の場合、インバウンド・エンティティーとマッチング・エンティティーが同じエンティティーであることを示しています。

「関係の信頼度 (Relationship confidence)」のスコアは、エンティティー解決処理の一環としてシステムによって生成されます。

「解決スコア **(Resolution score)**」
2 つのエンティティーがどれくらい一致しているかを表すスコア。スコアが高いほど、より正確に一致していることになります。スコアが 100 の場合、インバウンド・エンティティーとマッチング・エンティティーが同じエンティティーであることを示しています。

解決スコアは、エンティティー解決処理の一環としてシステムによって生成されます。

「解決の信頼度 **(Resolution confidence)**」
エンティティー解決の一部として構成される、インバウンド・エンティティーとマッチング・エンティティーを同一エンティティーに解決するための最小スコアを表す基本解決スコア。多くの場合、「解決スコア (Resolution score)」と「解決の信頼度 (Resolution confidence)」は同じスコアです。

「マッチング詳細**:** *n* 次 **(Matching Details: Degree** *n***)**」
このセクションは、アラートに含まれるエンティティーのマッチング詳細と、該当するエンティティーのアイデンティティー情報を提供します。2 つのエンティティーは、「エンティティー *x*」(インバウンド・アイデンティティー) と「エンティティー *y*」(マッチング・アイデンティティー) として表現されます。

レポートには、エンティティーごと、および属性データ・タイプごとに、一致したデータ値と、各エンティティーのデータ値に関連付けられているデータ・ソースと外部 ID がリストされます。その後、レポートには精度の説明とマッチング属性のスコアが表示されます。マッチング属性の 1 つが「Name」である場合、レポートには、エンティティー解決に構成されてい

る名前スコアリング・オプションに応じて、エンティティー解決で判定された名前のスコアに関する詳細もリストされることがあります。

「データ・タイプ **(Data Type)**」
: マッチング属性の名前。

値
: マッチングされたデータ値。

データ・ソース
: エンティティーごとに、マッチング属性とデータ値を提供したデータ・ソース・コードと説明。この情報は元のソース・ファイルを識別します。

外部 **ID**
: エンティティーごとに、マッチング属性とデータ値を提供したデータ・ソース・コードに関連付けられている外部 ID。多くの場合、この情報は、元のソース・ファイル内のエンティティーのアカウント番号を識別します。

「精度の説明 **(Precision Description)**」
: エンティティー同士のマッチングが行われた精度のレベルを記述したテキスト。

  精度レベルは、エンティティー解決構成時に属性別に構成されます。

「精度/最大精度 **(Precision/Max Precision)**」
: 最初の数値はシステムにより生成された精度スコアで、エンティティー *x* (インバウンド・アイデンティティー) とエンティティー *y* (マッチング・アイデンティティー) がどれくらい正確に一致したかを示します。2 番目の数値は、達成可能な最大精度スコアです。

  2 つの数値を比較することで、エンティティー間の一致具合に関する詳細を判別して、一致をさらに検討するかどうかなどを決定できます。また、これらのスコアを使用して、アラートの検索基準を調整する必要があるかどうかを判別することもできます。

「スコア調整 **(Score Adjustment)**」
: 解決スコアはこの数値で調整されました。この数値は、エンティティー解決構成時に構成されます。

「名前スコアリング詳細 **(Name Scoring Details)**」
: マッチング属性の 1 つが「Name」データ・タイプである場合、レポートには、エンティティー解決処理で判定された名前一致のスコアに関する詳細も提供されることがあります。レポートのこのセクションが表示されるには、エンティティー解決の一部として、以下の名前オプションが 1 つ以上構成されている必要があります。

  - Name Manager
  - Name Comparator 2

  「フルネーム **(Full Name)**」
  : 両方のエンティティーのフルネームがどれくらい正確に一致したかを表すスコア (0 から 100)。このスコアは、エンティティー解決の一部として構成されます。

「姓 **(Surname)**」
両方のエンティティーの姓がどれくらい正確に一致したかを表すスコア (0 から 100)。このスコアは、エンティティー解決の一部として構成されます。

「名 **(Given Name)**」
両方のエンティティーの名がどれくらい正確に一致したかを表すスコア (0 から 100)。このスコアは、エンティティー解決の一部として構成されます。

「エンティティー *x* と *y* のアイデンティティー情報 **(Entity *x* and *y* Identity Information)**」セクション
レポートのこのセクションには、各アイデンティティーに関する特定の情報がリストされます。

「データ・タイプ **(Data Type)**」
特性の名前。(例えば、「Name」。)

値　特性の値。(例えば、「SMITH」、「BRUCE」。)

「エンティティー *x* と *y* のその他のアラート **(Other Alerts for Entity *x* and *y*)**」セクション
レポートのこのセクションには、インバウンド・エンティティー (エンティティー *x*) およびマッチング・エンティティー (エンティティー *y*) のそれぞれに関連付けられているすべてのその他のロール・アラートのロール・アラート・ヒストリーと関係がリストされます。また、インバウンド・エンティティー (エンティティー *x*) およびマッチング・エンティティー (エンティティー *y*) のそれぞれに関連付けられているすべてのイベント・アラートのイベント・アラート・ヒストリーもリストされます。この情報は、各エンティティー、エンティティーに関連したアラート、その他のエンティティーに対する関係の全体像をより把握できるようにし、そうすることでユーザーによる分析を支援します。

「ロール・アラート・ヒストリー **(Role Alert History)**」
エンティティー・レジュメのロール・アラート・ヒストリーの情報が含まれます。

「アラートの日時 **(Alert Date and Time)**」
ロール・アラートが生成された日時。

アラート **ID**
このロール・アラートの説明とアラート ID。

説明　このアラートをトリガーしたロール・アラート・ルールを記述したテキスト。

エンティティー **ID**
エンティティー x またはエンティティー y のいずれかに一致した、その他のアラート内のその他のエンティティーのエンティティー ID 番号。

名前　エンティティー x またはエンティティー y のいずれかに一致した、その他のアラート内のその他のエンティティーの名前。

関係　関連エンティティーに関連付けられている関係の数。

「関係スコア **(Relationship Score)**」
2 つのエンティティーがどれくらい密接に関連しているかを表すスコア。スコアが高いほど、より密接に関連していることになります。スコアが 100 の場合、インバウンド・エンティティーとマッチング・エンティティーが同じエンティティーであることを示しています。

このスコアは、エンティティー解決処理の一環としてシステムによって生成されます。

「アクティビティー・コード **(Activity Code)**」
このアラートに対してユーザーが実行したアクションを示すユーザー定義のコード。アクティビティー・コードは構成コンソールで構成され、アラートの更新時に Visualizer でドロップダウンから選択されます。アクティビティー・コードの例の一部として「オープン (Open)」、「割り当て済み (Assigned)」、「保留 (Hold)」、「クローズ済み (Closed)」などがあります。

状況
「状況の日時 (Status Date and Time)」に変更された、このアラート更新の後処理の状況。状況は更新順に表示されます。したがって、最後に更新された状況が最後にリストされます。

「イベント・アラート・ヒストリー **(Event Alert History)**」
エンティティー・レジュメのイベント・アラート・ヒストリーの情報が含まれます。

「アラート日時 **(Date and Time Alerted)**」
イベント・アラートが生成された日時。

アラート **ID**
イベント・アラートに対してシステムにより生成されるユニーク ID。

説明
構成コンソールのイベント構成から取得される、イベント・アラートの説明。

「ロール・アラート状況レポート **(Role Alert Status report)**」**:**

「ロール・アラート状況レポート (Role Alert Status report)」は、指定された期間におけるすべてのロール・アラートの状況の要約です。このレポートを使用して、ロール・アラートを表示および管理します。

このレポートは、ロール・アラート ID とアラート日時でソートされます。

「アラート **ID -** 説明 **(Alert ID - Description)**」
システムによって生成されたロール・アラート ID と、関連したロール・アラート・ルールから取得されるロール・アラートの説明が表示されます。

「アラートの日時 **(Alert Date and Time)**」
ロール・アラートが作成された日時を示します。

「マッチング・エンティティー情報 **(Matching entity information)**」
このセクションには、最後に状況が更新されたアラートを先頭に、アラートの後処理のヒストリーが表示されます。

「エンティティー **1** と エンティティー **2 (Entity 1 and Entity 2)**」
このロール・アラートの基準に基づいて (アラート ID と説明によって)、一致した 2 つのエンティティーのエンティティー ID と、通常はエンティティーのフルネームが表示されます。

「アクティビティー・コード **(Activity Code)**」
このアラートに対してユーザーが実行したアクションを示すユーザー定義のコードが表示されます。アクティビティー・コードは構成コンソールで構成され、アラートの更新時に Visualizer でドロップダウンから選択されます。アクティビティー・コードの例の一部として「オープン (Open)」、「割り当て済み (Assigned)」、「保留 (Hold)」、「クローズ済み (Closed)」などがあります。

状況
「状況の日時 (Status Date and Time)」に変更された、このアラート更新の後処理の状況が表示されます。状況は更新順に表示されます。したがって、最後に更新された状況が最後にリストされます。

「状況の日時 **(Status Date and Time)**」
アラート状況が発生した日時を示します。

ユーザー
アラートをこのアラート状況で更新したユーザーの名前が表示されます。

ヘルプ・トピック

「属性アラート・ジェネレーター・ヒストリー・レポート基準 **(Attribute Alert Generator History report criteria)**」ウィンドウ**:**

この Visualizer ウィンドウを使用して、「属性アラート・ジェネレーター・ヒストリー・レポート (Attribute Alert Generator History Report)」を表示する際の基準を指定します。このレポートは、有効期限、ケース番号、コメント、または状況の変更など、属性アラート・ジェネレーターに対して行われた変更を確認および監査するのに役立ちます。属性アラート・ジェネレーターの結果を表示する場合は、「属性アラート・ジェネレーター・レポート (Attribute Alert Generator Report)」を表示してください。

「開始日 **(From Date)**」
選択済みレポートでデータを表示する日付範囲の最初の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「開始日 **(From Date)**」は今日の日付です。

「終了日 **(Thru Date)**」
選択済みレポートでデータを表示する日付範囲の最後の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「終了日 **(Through Date)**」は今日の日付です。

1 日分のデータを表示するには、「開始日 **(From Date)**」フィールドと「終了日 **(Thru Date)**」フィールドの両方に同じ日付を使用します。

「状況」ドロップダウン・リスト
特定の状況を選択します。また、すべての属性アラート・ジェネレーターのすべての状況を対象にレポート作成する場合は「すべて **(All)**」を選択します。例えば、指定された日付範囲内で、現在オープン状態の属性アラート・ジェネレーターに対する変更のみを表示する場合、ドロップダウン・リストから「オープン **(Open)**」を選択します。

「状況」ドロップダウン・リストのデフォルトの状況は「すべて **(All)**」であり、アクティブな属性アラート・ジェネレーターと有効期限が切れた属性アラート・ジェネレーターの両方が表示されます。

「ユーザー」ドロップダウン・リスト
自身の属性アラート・ジェネレーターを表示するオプションか、Visualizer ユーザー・グループ内の誰かが作成した属性アラート・ジェネレーターを表示するオプションを選択します。

デフォルト・オプションは「**マイ・サーチ** (My Searches)」です。

「レポートの実行 **(Run Report)**」ボタン
レポートを生成する場合、このボタンをクリックします。

「属性アラート・ジェネレーター・レポート基準 **(Attribute Alert Generator report criteria)**」ウィンドウ**:**

このウィンドウを使用して、Visualizer から「属性アラート・ジェネレーター・レポート (Attribute Alert Generator Report)」を表示する際の基準を指定します。「属性アラート・ジェネレーター・レポート (Attribute Alert Generator Report)」を使用して、属性アラート・ジェネレーターや、Visualizer ユーザー・グループ内のアナリストを管理できます。属性アラート・ジェネレーターの変更ヒストリーを表示する場合は、代わりに「属性アラート・ジェネレーター・ヒストリー・レポート (Attribute Alert Generator History Report)」を使用してください。

「開始日 **(From Date)**」
日付範囲の最初の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「開始日 **(From Date)**」は今日の日付です。

「終了日 **(Thru Date)**」
日付範囲の最後の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「終了日 **(Through Date)**」は今日の日付です。

1 日分のデータを表示するには、「開始日 **(From Date)**」フィールドと「終了日 **(Thru Date)**」フィールドの両方に同じ日付を使用します。

「状況」ドロップダウン・リスト
特定の状況を選択します。また、すべての属性アラート・ジェネレーターの

すべての状況を対象にレポート作成する場合は「すべて **(All)**」を選択します。例えば、指定された日付範囲内で、現在アクティブな属性アラート・ジェネレーターのみを表示する場合、「オープン **(Open)**」を選択します。

デフォルトの状況は「すべて **(All)**」であり、有効期限が切れた属性アラート・ジェネレーターとアクティブな属性アラート・ジェネレーターが両方レポートに表示されることを意味します。

「ユーザー」ドロップダウン・リスト
以下のいずれかを選択します。

- 自身の属性アラート・ジェネレーターのみを表示する場合は、「マイ・サーチ **(My Searches)**」を選択します (デフォルトの選択項目)。
- Visualizer ユーザー・グループ内のユーザーによって作成されたすべての属性アラート・ジェネレーターを表示する場合は、「マイ・グループ **(My Group)**」を選択します。

「レポートの実行 **(Run Report)**」ボタン
レポートを生成する場合、このボタンをクリックします。

「属性アラート・レポート基準 **(Attribute Alert report criteria)**」ウィンドウ**:**

この Visualizer ウィンドウを使用して、属性アラートを表示および管理するのに役立つ「属性アラート・レポート (Attribute Alert Report)」を表示する際の基準を指定します。

「開始日 **(From Date)**」
選択済みレポートでデータを表示する日付範囲の最初の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「開始日 **(From Date)**」は今日の日付です。

「終了日 **(Thru Date)**」
選択済みレポートでデータを表示する日付範囲の最後の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「終了日 **(Through Date)**」は今日の日付です。

1 日分のデータを表示するには、「開始日 **(From Date)**」フィールドと「終了日 **(Thru Date)**」フィールドの両方に同じ日付を使用します。

「状況」ドロップダウン・リスト
特定の状況を選択します。また、すべての属性アラートのすべての状況を対象にレポート作成する場合は「すべて **(All)**」を選択します。例えば、指定された日付範囲内で、現在オープン状態の属性アラートに対する変更のみを表示する場合、ドロップダウン・リストから「オープン **(Open)**」を選択します。

「状況」ドロップダウン・リストのデフォルトの状況は「すべて **(All)**」であり、アクティブな属性アラート・ジェネレーターと有効期限が切れた属性アラート・ジェネレーターの両方が表示されます。

「ユーザー」ドロップダウン・リスト
ユーザー名で Visualizer ユーザーを選択するか、すべての Visualizer ユーザーを対象に属性アラートのレポート作成する場合は「すべて **(All)**」を選択します。

ドロップダウン・リストのデフォルト・ユーザーは自身のユーザー名です。

「レポートの実行 **(Run Report)**」ボタン
レポートを生成する場合、このボタンをクリックします。

「データ・ソース要約レポート基準 **(Data Source Summary report criteria)**」ウィンドウ**:**

このウィンドウを使用して、Visualizer から「データ・ソース要約レポート (Data Source Summary Report)」を表示する際の基準を指定します。「データ・ソース要約レポート (Data Source Summary Report)」には、システムにロードされたデータがデータ・ソース別に表示されます。データ・ソースは、アイデンティティー・データの発生元を知るのに役立ちます。

「データ・ソース **(Data Source)**」ドロップダウン・リスト
特定のデータ・ソースを選択するか、すべてのデータ・ソースからのデータを表示する場合は「**[**すべて**] ([all])**」を選択します。

「開始日 **(From Date)**」
選択済みレポートでデータを表示する日付範囲の最初の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「開始日 **(From Date)**」は今日の日付です。

「終了日 **(Thru Date)**」
選択済みレポートでデータを表示する日付範囲の最後の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「終了日 **(Through Date)**」は今日の日付です。

1 日分のデータを表示するには、「開始日 **(From Date)**」フィールドと「終了日 **(Thru Date)**」フィールドの両方に同じ日付を使用します。

「レポートの実行 **(Run Report)**」ボタン
レポートを生成する場合、このボタンをクリックします。

「開示レポート基準 **(Disclosure report criteria)**」ウィンドウ**:**

この Visualizer ウィンドウを使用して、開示された関係の表示と管理に役立つ「開示レポート (Disclosure Report)」を表示する際の基準を指定します。開示された関係は、エンティティー解決または関係解決によってディスカバーされるものでなく、2 つのアイデンティティー間の手動リンクです。これらの手動リンクは、通常、Visualizer 内で作成されますが、開示された関係を示す UMF タグ・ペア (<DR> と </DR>) を、パイプラインによってロードおよび処理されるアイデンティティー・レコードに設定することで作成することもできます。

「開始日 **(From Date)**」
選択済みレポートでデータを表示する日付範囲の最初の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「開始日 **(From Date)**」は今日の日付です。

「終了日 **(Thru Date)**」
選択済みレポートでデータを表示する日付範囲の最後の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「終了日 **(Through Date)**」は今日の日付です。

1 日分のデータを表示するには、「開始日 **(From Date)**」フィールドと「終了日 **(Thru Date)**」フィールドの両方に同じ日付を使用します。

「レポートの実行 **(Run Report)**」ボタン
レポートを生成する場合、このボタンをクリックします。

「ロード要約レポート基準 **(Load Summary report criteria)**」ウィンドウ**:**

このウィンドウを使用して、Visualizer から「ロード要約レポート (Load Summary Report)」を表示する際の基準を指定します。「ロード要約レポート (Load Summary Report)」を使用して、Visualizer にロードした UMF ファイルのデータ品質に関する一般情報に加えて、パフォーマンス統計、ファイル・ロードによって生成されたエンティティー解決やアラートの数などの有用な情報を判別できます。

「データ・ソース・コード **-** 説明」ドロップダウン・リスト
特定のデータ・ソースを選択するか、すべてのデータ・ソースからロードされたデータを表示する場合は「**[**すべて**] ([all])**」を選択します。例えば、ある 1 日に複数の UMF ファイルからアイデンティティー・レコードをロードした場合、該当するデータ・ソース・コードを選択することで、レポートに表示するデータを単一データ・ソースに絞り込むことができます。

「開始日 **(From Date)**」
選択済みレポートでデータを表示する日付範囲の最初の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「開始日 **(From Date)**」は今日の日付です。

「終了日 **(Through Date)**」
選択済みレポートでデータを表示する日付範囲の最後の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「終了日 **(Through Date)**」は今日の日付です。

1 日分のデータを表示するには、「開始日 **(From Date)**」フィールドと「終了日 **(Thru Date)**」フィールドの両方に同じ日付を使用します。

「レポートの実行 **(Run Report)**」ボタン
レポートを生成する場合、このボタンをクリックします。

「ロール・アラート状況レポート基準 **(Role Alert Status report criteria)**」ウィンドウ**:**

この Visualizer ウィンドウを使用して、「ロール・アラート状況レポート (Role Alert Status Report)」を生成する際の基準を指定します。このレポートは、指定された期間内のロール・アラートの状況を要約したものであり、これを使用してロール・アラートを管理できます。

「開始日付 **(From Date)**」と「開始時刻 **(From Time)**」
レポートのデータを生成する日付範囲の最初の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

レポートのデータを生成する時刻範囲の最初の時刻を 24 時間制を使用して入力します。HH:MM 形式を使用します。例えば、09:00 は 9:00 AM を表し、20:30 は 8:30 PM を表します。

デフォルトの「開始日付 **(From Date)**」と「開始時刻 **(From Time)**」は、今日の日付の 00:00 です。

「終了日付 **(Through Date)**」と「終了時刻 **(Through Time)**」
レポートにデータを表示する日付範囲の最後の日付を入力します。MM/DD/YY 形式を使用します。例えば、01/01/01 は、2001 年 1 月 1 日を表します。または、カレンダー・コントロールをクリックして、日付を選択します。

デフォルトの「終了日付 **(Through Date)**」と「終了時刻 **(Through Time)**」は、今日の日付の 23:59 です。

1 日分のデータを表示するには、以下のオプションのいずれかを選択します。

- 「開始日付 **(From Date)**」フィールドと「終了日付 **(Through Date)**」フィールドの両方に同じ日付を入力する。
- 「開始時刻 **(From Time)**」フィールドに 00:00、「終了時刻 **(Through Time)**」フィールドに 23:59 と入力する。

「関係スコア・レポート範囲 **(Relationship Score Reporting Range)**」
関係スコアで結果を絞り込む場合、「開始 **(From)**」フィールドと「終了 **(To)**」フィールドに関係スコアの範囲を入力します。

デフォルトの範囲は 0 から 100 まで、すなわち、すべての関係スコアです。

「ロール・アラート・ルール **(Role Alert Rule)**」ドロップダウン・リスト
レポートの対象とする特定のロール・アラート・ルールを選択します。

「ロール・アラート・レベル **(Role Alert Level)**」ドロップダウン・リスト
特定のロール・アラート・レベルを選択するか、すべてのロール・アラートをレポートの対象にする場合は「すべて **(All)**」を選択します。

「レポートの実行 **(Run Report)**」ボタン
レポートを生成する場合、このボタンをクリックします。

Analyst ツールキットを使用したデータの分析

Identity Insight Analyst ツールキットに含まれるツールやテンプレートを使用して、ブラウザー・ベースのアプリケーション環境で分析レポートおよび情報を作成したりカスタマイズしたりできます。

IBM Cognos レポートを使用したデータのレポート

Analyst ツールキットは、カスタマイズされた Identity Insight レポートの作成に使用できる、一連の Cognos レポートを提供します。

IBM Cognos の Identity Insight への統合により、必要な情報に合わせて Identity Insight レポートをカスタマイズする機能のための基盤が作成されます。

Analyst ツールキットには、IBM Cognos で使用される以下のエレメントが含まれています。

- クエリーおよびアプリケーション開発用の Cognos Business Intelligence ツール
- Identity Insight データ・モデル (Cognos Framework Manager で開発される) の作成とデプロイメント
- 「エンティティー・レジュメ (Entity Resume)」と「ロール・アラート詳細 (Role-Alert Detail)」のテンプレート・レポート。これらは、カスタマイズおよびアプリケーション開発のための開始ポイントとして意図されています。

Cognos レポート作成およびフレームワーク・モデルには、Identity Insight リポジトリーに基づいたカスタム Cognos ユーザー・ インターフェースやレポートを作成するのに必要なツールがあります。組み込みの Cognos ツールを使用して、カスタム・インターフェースを作成したり、EAS 提供のテンプレートを変更したりできます。

この製品情報では、以下の用語と概念が使用されています。

Analyst ツールキット
: インストール済み Cognos コンポーネント向けの Identity Insight パッケージとサンプル・テンプレート。

EntitySearcher
: ブラウザー・ベースのクライアントに「属性による検索」機能と「解決による検索」機能の最も良い部分を組み合わせたシン・クライアント・ブラウザー・アプリケーション。

IBM Cognos Business Intelligence
: Identity Insight に組み込まれている Cognos コンポーネントの汎用的な製品名。

Cognos Report
: Cognos Viewer 内の対話式 UI、PDF ファイル、XML ファイル (カスタム・レンダリング用)、または複数の Excel フォーマット (CSV など) としてレンダリングできる XML ベースの出力仕様。

Active Report
: Cognos 10 で導入された Active Report は、ルック・アンド・フィールが標準 Cognos レポートよりも Web アプリケーションに似た自己完結型レポートです。

Cognos Framework Manager
データ・ソース (通常はデータベース) をモデル化するために使用される Cognos ツール。 Identity Insight データ・モデルは、Framework Manager を使用して作成されています。

Cognos データ・モデル
1 つ以上のデータ・ソースの論理表現。Cognos レポート作成者はデータ・モデルを使用して対話式レポートを作成します。

Cognos Content Store
レポート定義、データ・モデル、クエリーなどの Cognos オブジェクトを保管するために Cognos によって使用される独立したデータベース。このコンテンツ・ストアは、Identity Insight データの保管には使用されません。

EntitySearcher シン・クライアントを使用したデータの分析

EntitySearcher シン・クライアントは、「属性による検索」機能と「解決による検索」機能の最も良い部分を兼ね備えたブラウザー・ベースのクライアントです。

Identity Insight は、エンティティーを検索するための 2 つの基本的な検索機能を提供します。「解決による検索」(Find-by-resolution) は、PSearch またはパイプライン検索と呼ばれることもあり、エンティティー解決を使用して結果を検索します。「属性による検索」(Find-by-attribute) は、EQ または拡張クエリーと呼ばれ、より従来型の SQL ルックアップを使用します。

EntitySearcher には、最適な結果を生成し、どちらのアプローチを使用するか迷わなくて済むように、これら 2 つの検索アプローチが組み合わされています。クライアント・インターフェースは、検索基準を入力するためにユーザーが使い慣れている、属性による検索インターフェースを提供しています。入力基準およびそれぞれの検索の結果に応じて、一方または両方の検索タイプが呼び出されます。両方の検索で得られた結果が集められ、重複排除され、ランク付けされたうえで検索結果グリッドに表示されます。

追加の検索拡張機能により、生年月日が、指定された日付範囲内にあるエンティティーを検索することができます。「検索条件の拡張 **(Expand search by)**」チェック・ボックスとドロップダウン・リストが使用されると、この検索が実行されます。例えば、1960 年 6 月 1 日という日付と 30 日間の範囲を指定した場合、検索で使用される有効な日付範囲は 1960 年 5 月 2 日 から 1960 年 7 月 1 日になります (1960 年 6 月 1 日 - 30 日と 1960 年 6 月 1 日 + 30 日)。範囲には両端が含まれます。

「厳密な検索」オプションを選択できます。この場合、属性による検索 (EQ) のみが使用されます。以下のいずれかの条件が満たされる場合、デフォルトで厳密な検索が実行されます。

- 検索基準に単一属性が入力された。
- 属性検索基準に不完全なエレメントが存在する。
- いずれかの属性検索基準にワイルドカード文字が使用されている。例えば、* です。
- DOB (生年月日) 属性検索基準に日付範囲が含まれている。

EntitySearcher を起動するための URL は次のとおりです。

`http://server:install_port/EntitySearcher/`

システム・アドミニストレーターが COMPONENT_CONFIG データベース表の URL_ENTITY_DETAIL および URL_ENTITY_GRAPH の値を構成すると、ユーザーが、検索結果から Identity Insight エンティティー・レジュメの Cognos レポート・バージョン、グラフ・コンポーネント、およびその他の HTTP リンク可能なターゲットを閲覧できるようになります。

EntitySearcher を使用したエンティティーの検索:

属性データおよび実行する検索の種類に基づいてエンティティーを検索します。

このタスクについて

EntitySearcher シン・クライアントは、「属性による検索」機能と「解決による検索」機能の最も良い部分を兼ね備えたブラウザー・ベースのクライアントです。検索の実行後には、検索結果を表示するためのユーザー・インターフェースを使用できます。

手順

1. ブラウザーで EntitySearcher を開きます。

   EntitySearcher を起動するための URL は次のとおりです。

   `http://server:install_port/EntitySearcher/`

   例えば、`http://localhost:13510/EntitySearcher/` です。デフォルトの *install_port* は 13510 ですが、ポート番号は変更可能です。正しいサーバー名またはポート番号が不明な場合は、システム・アドミニストレーターに問い合わせてください。
2. 「エンティティーの検索 **(Search Entities)**」ペインで、検索基準を入力します。 デフォルトでは、エンティティー検索のための単一属性が表示されます。
   a. 「属性リスト **(Attribute list)**」から、属性検索基準の属性タイプを選択します。
   b. 検索基準を入力します。

オプション	説明
追加の属性検索基準がある。	既存の属性の右側にある「**+**」をクリックします。
追加の属性検索基準がない。	次のステップへ進みます。 **注:** 検索基準に単一属性のみが入力された場合、厳密な検索が実行されます。

3. 組み合わせ検索を実行するのか、厳密な検索のみを実行するのか決定します。

オプション	説明
組み合わせ検索の実行	組み合わせ検索はデフォルトで実行されます。

オプション	説明
厳密な検索のみの実行	「厳密な検索 **(Strict search)**」チェック・ボックスを選択します。 **注:** 以下のいずれかの条件が満たされる場合、デフォルトで厳密な検索が実行されます。 • 検索基準に単一属性が入力された。 • 属性検索基準に不完全なエレメントが存在する。 • いずれかの属性検索基準にワイルドカード文字が使用されている。例えば、* です。 • DOB (生年月日) 属性検索基準に日付範囲が含まれている。

4. 「検索 **(Search)**」をクリックします。

タスクの結果

「検索結果 **(Search Results)**」ペインにエンティティー検索結果がリストされます。結果は、相似スコアと、名前スコア (使用可能な場合) に従ってランク付けされます。解決による検索のスコアが高い (>86) 検索結果が先頭にランク付けられ、その後に属性による検索のスコアが高い検索結果が続きます。解決スコアがそれより低い検索結果がその後に続きます。

次のタスク

検索結果のエンティティー・レジュメを表示する。

「検索結果 **(Search Results)**」ペインで、目的の検索結果行の「エンティティー **ID (Entity ID)**」列から、下線付きの「エンティティー **ID (Entity ID)**」番号の値をクリックします。

注**:** この機能を有効にするには、システム・アドミニストレーターが COMPONENT_CONFIG データベース表の URL_ENTITY_DETAIL 値を構成する必要がある場合があります。

検索結果のエンティティー・グラフを表示する。

「検索結果 **(Search Results)**」ペインで、目的の検索結果行の「エンティティー **ID (Entity ID)**」列から、グラフ・アイコンをクリックします。

注**:** この機能を有効にするには、システム・アドミニストレーターが COMPONENT_CONFIG データベース表の URL_ENTITY_GRAPH 値を構成する必要がある場合があります。

サンプル Cognos ロール・アラート・レポート

サンプル Cognos ロール・アラート・レポートは、アラートに関わるエンティティーおよびエンティティー関係に関する情報を表示し、Cognos ツールを使用してカスタマイズ可能です。

ロール・アラート・レポートでは、Cognos 10 で導入された Active Report テクノロジーが利用され、より優れたユーザー・エクスペリエンスが提供されます。

アラート情報は、動的に作成される別のタブにアラートの各パスが現れるように表示されます。ロール・アラート要約情報がレポートの先頭に表示され、必要な場合は、エンティティー・スナップショット (アラートが生成された時点でのエンティティーの状態) も表示できます。展開されたマッチング詳細セクションには、Identity Insight スコア情報が表示されます。

データ・アクセス

ロール・アラート詳細レポートは、新しい Identity Insight データベース・ビューをフルに活用します。このアプローチにより、データ・アクセスをより細かく制御できるようになります。例えば、結合やクエリーの構造はビュー SQL によって定義され、Cognos エンジンに任せられることはありません。また、基礎のデータ表から抽象化の層も提供します。こうすることで、Cognos レポートに直接的に影響を与えることなく基礎のスキーマを変更できるようにします。

Cognos ロール・アラート詳細画面をサポートするために新しい Identity Insight データベース・ビューが用意されていますが、データ・アクセスは、モデルを介して Cognos サーバーによって提供および制御されます。

技術上の注意点

Cognos ロール・アラート詳細レポートは Active Report テクノロジーを利用しています。これは、サポートされる出力タイプが HTML のみであることを意味します。標準 Cognos レポートと異なり、レポートによって使用されるデータはすべてレポートを表示する前にクエリーが行われます。これにより、Active Report は、Cognos サーバーから切断されても対話性を維持できます。Active Report は .MHT ファイル (MIME HTML) として配布でき、Cognos ホーム・ページから作成されるか、MHT ファイルをサポートする任意の Web ブラウザーからレポートの URL にアクセスすることで作成されます。すべてのレポート・データを事前にロードすることによる別の副次作用としては、ユーザーが UI と対話する際にページを再ロードする必要がなくなることが挙げられます。

Cognos ロール・アラート・レポートは、パラメーターとしてロール・アラート ID が必要です。レポートに直接アクセスした場合、ユーザーはロール・アラート ID を要求されます。コンポーネントとしてレポートにアクセスする場合は、URL パラメーターとしてロール・アラート ID を渡すことができます。URL 経由で Cognos パラメーターを渡す場合のパラメーター・フォーマットでは、プロンプト名の先頭に「p_」を追加します。ロール・アラート・レポートの場合、レポートで予期されるパラメーターは **pAlertID** であるため、構文は **p_pAlertID** になります。例えば、**&p_pAlertID=55&** です。

Cognos コンポーネントをサポートするために作成された Identity Insight データベース・ビューは、それらを識別しやすくするためにプレフィックス COG を使用した名前が付けられています。

Firefox 3.x では、これらのビューで MHT ファイルを正常に表示するために追加のプラグインをインストールする必要があります。

サンプル Cognos エンティティー・レジュメ・レポート

サンプル Cognos エンティティー・レジュメ・レポートには、エンティティーに関してわかっているすべての情報が表示され、Cognos ツールを使用してカスタマイズできます。

Cognos のレジュメ・レポートでは、エンティティー・データは要約されており、ユーザーは検討するエンティティー詳細を決定できます。

技術上の注意点

Cognos エンティティー・レジュメは、実際のデータベース・ビューの代わりに、レポートで定義されたクエリー・オブジェクトを大いに利用します。これらの仮想クエリーは Cognos データ・モデルに基づいており、モデル・オブジェクトをレポート・クエリー・ビルダーにドラッグしてプロパティーを設定することで作成されます。レジュメは「条件付きブロック」オブジェクトを使用して詳細セクションを表示します。条件付きブロックが使用される理由は、表示画面の印象を (レポートではなく) ユーザー・インターフェースに近いものにするためなので、このレポートの PDF、テキスト、および Excel 版の出力は、デフォルトの HTML 出力とは見た目も動作も異なります。

Cognos レポート・サーバーは、レポートの表示されているセクションを表示するために必要な情報のみのクエリーを行います。例えば、ロール・アラート情報のクエリーは、ユーザーがその情報を表示するように選択してはじめて行われます。これにより、初期ロード時間が短縮され、データ・アクセスもさらにスマートになります。ただし、これにはコストも伴います。詳細セクションが変更されると、ページを再ロードする必要があります。このページの再ロードは自動的に行われ、ユーザー対話は必要ありませんが、ユーザーは追加のユーザー対話を実行する場合、ページが最新表示されるまで待たなければなりません。

Cognos レジュメ・レポートは、唯一のパラメーターとして Identity Insight エンティティー ID を必要とします。Cognos ホーム・ページからレポートを実行する場合、ユーザーにはエンティティー ID の入力を求めるプロンプトが表示されます。ユーザーが Cognos ホーム・ページから Cognos レジュメを立ち上げてエンティティー ID を入力することは可能ですが、Cognos レジュメが統合コンポーネントになり、ワークフローやケース管理ツールなどの別のアプリケーションから呼び出されるほうが可能性としては高くなります。後者のユース・ケースでは、Identity Insight エンティティー ID を URL パラメーターとして Cognos レジュメに渡すことができ、エンティティー ID のプロンプト・ページは表示されません。

URL 経由で Cognos パラメーターを渡す場合のパラメーター・フォーマットでは、プロンプト名の先頭に「p_」を追加します。レジュメ・レポートの場合、必要なパラメーターは **pEntityID** であるため、構文は **p_pEntityID** になります。例えば、**&p_pEntityID=5&** です。

Cognos コンポーネントの識別とインストール

IBM Identity Insight Cognos レポート機能を使用および変更するために、IBM Cognos コンポーネントをインストールします。

始める前に

IBM Identity Insight Cognos レポートをデプロイする前に、IBM Business Intelligence Reporting をインストールする必要があります。

注**:** IBM Cognos Business Intelligence Reporting v10.1.0 以降の既存のインスタンスがインストールされている場合は、そこに IBM Identity Insight Cognos レポートをデプロイできます。

Identity Insight Cognos レポートのメタデータを変更するには、IBM Cognos Framework Manager をインストールする必要があります。

手順

1. IBM Business Intelligence Reporting v10.1.0 以降をインストールします。
   a. 詳細な Cognos の手順に従って Cognos Reporting コンポーネントをインストールします。
2. IBM Cognos Framework Manager v10.1.0 以降をインストールします。
   a. 詳細な Cognos の手順に従って Cognos Reporting コンポーネントをインストールします。

次のタスク

Identity Insight レポートを Cognos にデプロイします。

Cognos への **Identity Insight** レポートのデプロイ**:**

IBM Identity Insight Cognos ロール・アラートおよびエンティティー・レジュメのレポートを使用可能にするには、最初にそれらのレポートを IBM Cognos Business Intelligence Reporting にデプロイする必要があります。

始める前に

IBM Cognos Business Intelligence Reporting をインストールします。

手順

1. Identity Insight Cognos レポート・デプロイメント・パッケージを IBM Cognos Business Intelligence Reporting インストール済み環境にコピーします。ユーザーが Cognos の動的クエリー・モードと互換クエリー・モードのいずれを活用することを望んでいるかに応じて、Identity Insight は 2 つのバージョンのレポートを提供します。

表 *32. Identity Insight Cognos* レポート・デプロイメント・パッケージの場所

ファイルのコピー元	ファイルのコピー先
<製品インストール・ディレクトリー>ibm-home/cognos/deployment/IdentityInsight_v9.0_CompatibleQueryMode.zip または <製品インストール・ディレクトリー>/ibm-home/cognos/deployment/IdentityInsight_v9.0_DynamicQueryMode.zip	*<Cognos* インストール・ディレクトリー>/deployment/

2. ブラウザーで Cognos Connection ページにアクセスします。 ページの場所は、http://<*cognos_server_name_or_IP_address*>:<*cognos_port_#*>:cognos/index.html です。
3. 「起動」 > 「**IBM Cognos Administration**」をクリックします。

   注**:** IBM Cognos Administration にアクセスするには、保護されている特性である「管理タスク」に対する権限が必要です。
4. 「構成」 タブをクリックし、「コンテンツ管理」をクリックします。ツールバーで、「インポートの新規作成」アイコン  をクリックします。
5. 使用可能なデプロイメント・パッケージのリストから、`IdentityInsight_v9.0_Cognos` を選択します。パスワードを求められたら、`ISII4YOU` と入力します。「**OK**」をクリックします。
6. 「名前と説明」ペインで、「次へ」をクリックします。 「名前と説明」ペインは変更する必要はありません。
7. 「共有フォルダー・コンテンツ (public folder content)」ペインで、使用可能な「共有フォルダー・コンテンツ **(public folders content)**」のリストから「**ISII**」フォルダーのチェック・ボックスを選択します。「次へ」をクリックします。
8. 「ディレクトリーの内容」ペインで、「次へ」をクリックします。 「ディレクトリーの内容」ペインは変更する必要はありません。
9. 「全般オプション」ペインで、「次へ」をクリックします。 「全般オプション」ペインは変更する必要はありません。
10. 要約を確認し、「次へ」をクリックします。
11. 「保存して **1** 回実行」を選択します。「終了」をクリックして、レポートをインポートします。「実行」をクリックします。 実行オプションは変更する必要はありません。
12. ダイアログ・ボックスを閉じる前に、インポートの詳細を表示するように選択します。「**OK**」をクリックします。 状況に「**実行中**」と表示される場合、「最新表示」をクリックします。デプロイメントが成功すると、状況は「**成功**」と表示されます。「閉じる」をクリックします。

次のタスク

1. レポートがデプロイされたことを確認します。
2. Identity Insight Cognos レポート・デプロイメント・データベース構成を変更します。

Identity Insight レポート・デプロイメントの確認**:**

レポートをデプロイした後は、レポートを実行する前にデプロイメントを確認する必要があります。

始める前に

Identity Insight レポートを Cognos にデプロイします。

手順

1. ブラウザーで Cognos Connection ページにアクセスします。 ページの場所は、http://<*cognos_server_name_or_IP_address*>:<*cognos_port_#*>:cognos/index.html です。
2. 「共有フォルダー」タブで、共有フォルダー **ISII** が存在することを確認します。
3. 「**ISII**」フォルダーを選択します。
4. 単一の「**Identity_Insight**」パッケージ・オブジェクトが存在することを確認します。 パッケージ・オブジェクトは、青いフォルダーとして表示されます。
5. 「**ISII_EntityResume**」レポートと「**ISII_RoleAlertDetailActive**」レポートが両方存在することを確認します。

次のタスク

Identity Insight Cognos レポート・デプロイメント・データベース構成を変更します。

Identity Insight Cognos レポート・デプロイメント・データベース構成の変更**:**

レポートのデプロイと確認が終了したら、Identity Insight Cognos レポート・デプロイメント・データベース構成を変更する必要があります。注: 動的クエリー・モードのレポートを使用する場合、(下記にリストされている手順に従う代わりに) Cognos の資料を参照して、Cognos 内部から JDBC 接続を作成してください。

始める前に

Identity Insight レポートを Cognos にデプロイします。

手順

1. ブラウザーで Cognos Administration ページにアクセスします。
2. 左側で、「データ・ソース接続」をクリックします。
3. 「**ISII**」データ・ソース・オブジェクトを選択します。
4. 「**ISII**」データ・ソース接続オブジェクトを選択します。
5. 「**ISII**」サインオン・オブジェクトを選択します。
   a. 「プロパティーを設定」をクリックします。
   b. 「サインオン」タブで、「サインオンを編集**...**」をクリックします。
   c. リンクを変更して、Identity Insight データベースのユーザー名とパスワードを組み込みます。「**OK**」をクリックします。
   d. 「**OK**」をクリックします。
6. データ・ソース接続オブジェクトの「プロパティーを設定」をクリックします。
7. 「接続」タブで、使用する Identity Insight データベース・タイプに応じた下記の手順を完了します。

Identity Insight データベース・タイプ	手順
DB2	1. タイプに「**IBM DB2**」を選択します。 2. 「接続文字列を編集」アイコンを選択します。 3. DB2 データベース名の値を変更します。スキーマが必要な場合は、`currentSCHEMA=<schema>` を DB2 接続ストリング・パラメーターに追加します。 4. 「接続をテスト**...**」をクリックします。 5. 「テスト」をクリックします。 6. 状況が「**成功**」であることを確認します。
Oracle	1. タイプに「**Oracle**」を選択します。 2. 「**現在の接続文字列は失われます (current connection string will be lost)**」という警告が表示されたら、「**OK**」をクリックします。 3. 「接続文字列を編集」アイコンを選択します。 4. SQL*Net 接続文字列を変更します。 5. 「接続をテスト**...**」をクリックします。 6. 「テスト」をクリックします。 7. 状況が「**成功**」であることを確認します。

8. 「閉じる」をクリックして、「テスト結果」パネルを閉じます。
9. 「閉じる」をクリックして、「接続のテスト」パネルを閉じます。
10. 「**OK**」をクリックして、「接続のテスト」パネルを閉じます。
11. 「**OK**」をクリックして、「プロパティーを設定」パネルを閉じます。

グラフ・ツールを使用したデータ分析

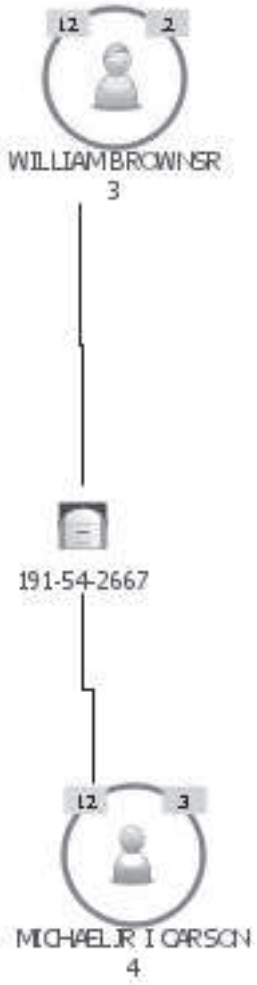
InfoSphere Identity Insight グラフ・ツールは、Identity Insight のアラート、エンティティー関係、およびその他のエンティティー情報を視覚化した Web ベースのグラフを分析できる機能をユーザーに提供します。

グラフをレンダリングするために、グラフ・ツールは、製品のパイプラインがバックグラウンドで稼働中であることを必要とします。

グラフ・ツールによってレンダリングされるグラフは、i2 Analyst Notebook コンポーネント内でレンダリングされるグラフに似ています。しかし、グラフ・ツールを使用すると、既存のケース管理ツールまたはその他のアプリケーション内にグラフを組み込んだり、そこから起動したりできるメリットがあります。また、ユーザーは、URL または Web Start ページを使用して、Web ブラウザー内でグラフを表示および起動できます。グラフ・ツールによってレンダリングされるグラフを表示する場合、i2 Analyst Notebook をインストールしたり起動したりする必要はありません。

アラート・グラフ

グラフ・ツールによって生成されるアラート・グラフには、アラート ID に基づいた特定のロール・アラートが表示されます。アラート・グラフは、ロール・アラートに含まれるエンティティーとエンティティー同士をリンクしている属性を視覚化するのに役立ちます。



ロール・アラートは、1 つのエンティティー、または関係を通してリンクされている複数のエンティティーが、構成されているロール・アラート・ルールを満たすか上回ると発生します。ロール・アラートは、構成されているロールとロール・アラート・ルールに基づいており、以下のことを示している場合があります。

- 警告または問題 (顧客が、警戒リストに記載されている容疑者にリンクされているなど)
- 関心のある関係 (顧客が同時にベンダーでもある、ある従業員が特定の電話番号を介して複数の顧客にリンクされているなど)

アラート・グラフの使用に関するヒント

- アラートに含まれるエンティティーに対して「関連エンティティー (Related Entities)」インディケーターが表示されている場合、右クリックのメニュー・オ

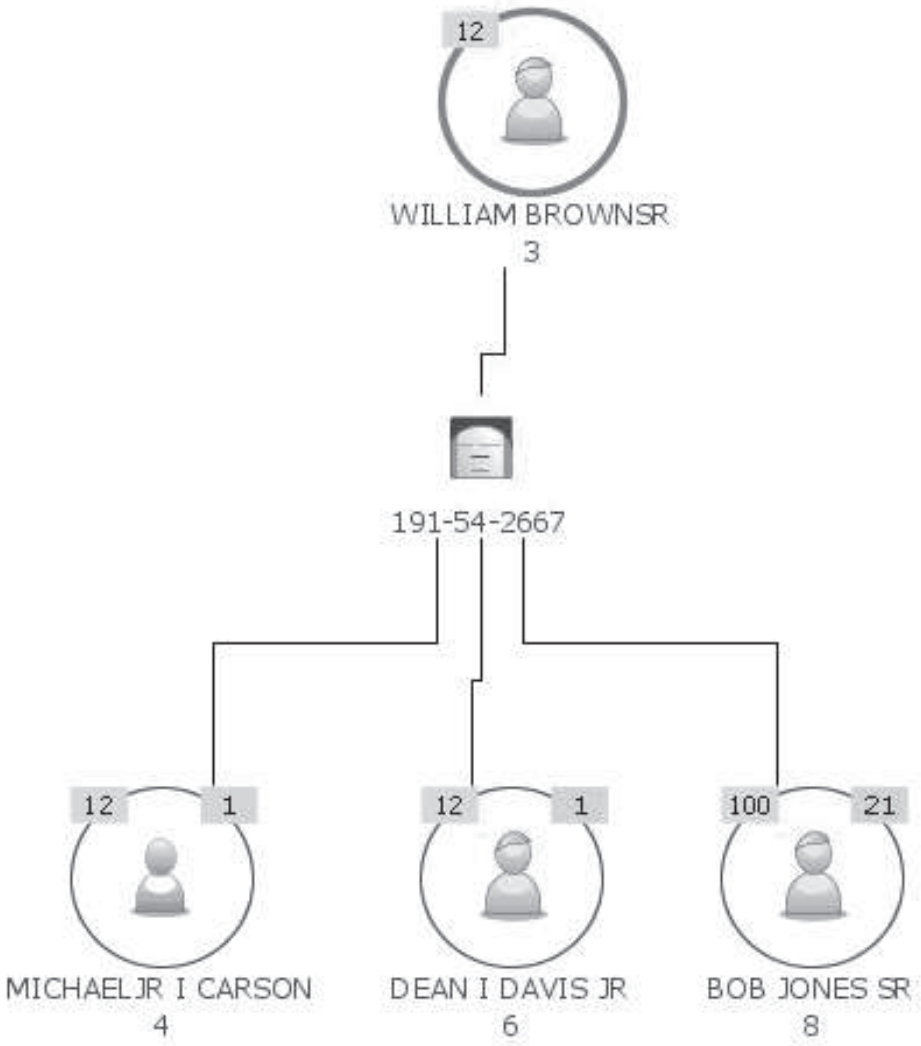
プション「残りの関連エンティティーの表示 **(Show remaining related entities)**」を使用して、残りの関連エンティティーを表示します。グラフが再作成され、選択済みエンティティーに関連したすべてのエンティティーが表示されます。グラフによって、そのような残りのエンティティーも、それらのエンティティーの関連先であるグラフ上の既存のエンティティーに自動的にリンクされます。

- アラート・グラフには、各エンティティーの属性のうちアラートの原因となった属性のみが表示されます。特定のエンティティーに関連付けられたすべての属性を表示するには、エンティティーを右クリックし、「残りの属性の表示 **(Show remaining attributes)**」を選択します。
- グラフ上の特定のエンティティーのエンティティー・レジュメを表示するには、エンティティーを右クリックし、「レジュメの表示 **(Show resume)**」を選択します。エンティティー・レジュメは、そのエンティティーのアイデンティティーや、エンティティーが含まれているその他のアラートなど、エンティティーに関する追加の詳細を提供します。この右クリックのメニュー・オプションは、リンクが正しく構成されており、エンティティー・レジュメを生成する製品 (Analyst ツールキットなど) にアクセスできる場合にのみ使用できます。

エンティティー・グラフ

グラフ・ツールによって生成されるエンティティー・グラフは、指定したエンティティーとそのエンティティーに関連したすべてのエンティティーの間の関係を、共有する属性に基づいて視覚化するのを支援します。

エンティティー・グラフは、エンティティーと属性が交互に重なった層を使用して、エンティティー間の関係を示します。



第 **1** 層 **-** メイン・エンティティー

最初にグラフを表示すると、第 1 層には、メイン・エンティティーが含まれています。メイン・エンティティー は、常に、エンティティー・グラフをレンダリングするためにユーザーが指定または選択したエンティティーです。メイン・エンティティー・ノードを囲む線は常に他より太く表示されるため、メイン・エンティティーが実際、グラフ上のどこに表示されるかに関係なく、ユーザーはメイン・エンティティーを識別できます。

トップ・エンティティー は、先頭にある、グラフの第 1 層に表示されるエンティティーです。当初は、メイン・エンティティーがトップ・エンティティーでもあります。しかし、「先頭に移動 **(Move to top)**」右クリック・オプションを使用して、簡単に任意のエンティティーをトップ・エンティティーにすることができます。

第 **2** 層 **(**および追加の偶数の層**) -** 共有属性

第 2 層は、トップ・エンティティーをグラフの第 3 層のエンティティーにリンクする共有属性で構成されます。グラフに表示される属性には、属性のタイプと値の両方が示されます。

グラフに追加の層が存在する場合、偶数の層には常に、属性の層の上下に表示されるエンティティーをリンクしている共有属性が含まれます。

第 3 層 (および追加の奇数の層) - 関連エンティティー
グラフの第 3 層には、トップ・エンティティーに 1 次の隔たりで関連しているエンティティーが表示されます。

グラフに追加の層が存在する場合、奇数の層には常に、その前のエンティティー層に関連したエンティティーが含まれます。この関連は、2 つのエンティティー層の間の共有属性層に基づいています。これらの後続エンティティー層に表示されるエンティティーは、対応する隔たり度合いでトップ・エンティティーに関連しています。すなわち、第 4 層のエンティティーは、2 次の隔たりでトップ・エンティティーに関連しています。第 5 層のエンティティーは、3 次の隔たりでトップ・エンティティーに関連し、以下も同様に続きます。

エンティティー・グラフの使用に関するヒント

エンティティー・グラフには多数の層が含まれる場合があります。エンティティー・グラフに表示されるすべての属性およびエンティティーの情報を調べるうえで役立ついくつかのヒントを以下に示します。

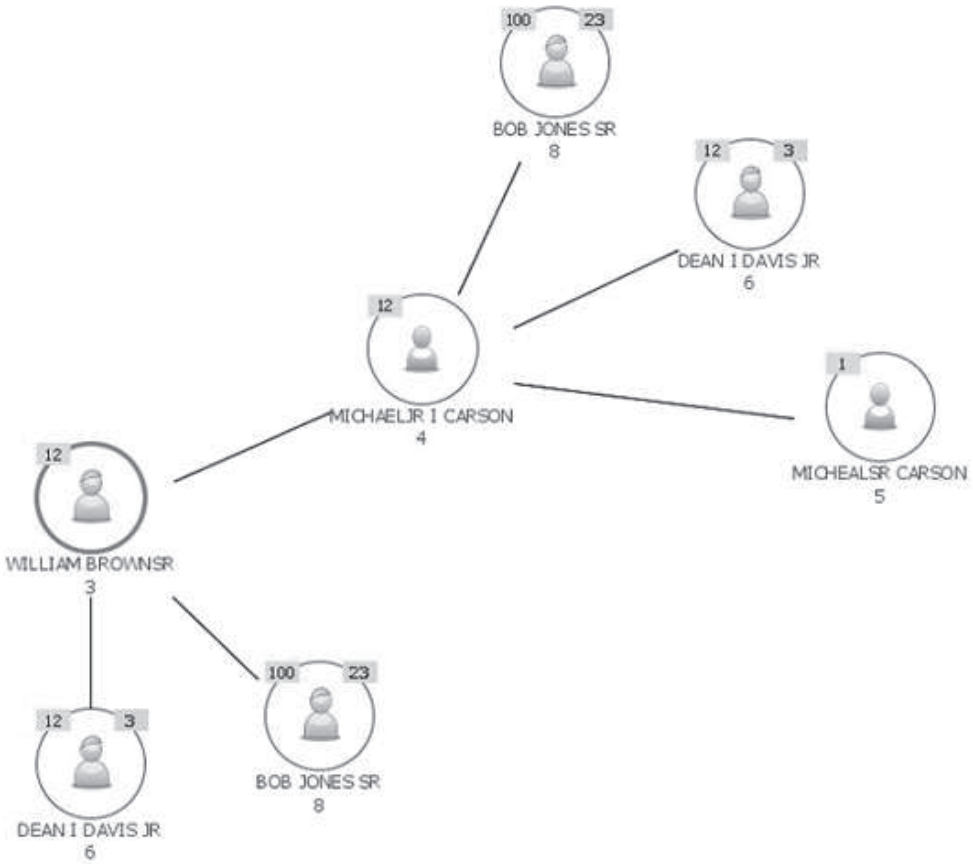
- エンティティーに関する詳細をさらに表示する。
  - 右クリックのメニュー・オプション「残りの関連エンティティーの表示 **(Show remaining related entities)**」を使用して、現在グラフに表示されていない、特定のエンティティーの関係を調べます。
  - 「トップへのパスを表示 **(Show path to top)**」クイック・フィルターを使用して、エンティティーまたは属性がトップ・エンティティーにどのように関連しているかを表示します。このフィルターは、関連のないエンティティーおよび属性をグラフから一時的に隠します。
  - ソーシャル・ネットワーク・グラフに切り替えて、エンティティー間の関係を表示し、そこに集中できるようにするグラフを作成します。ソーシャル・ネットワーク・グラフでは、グラフ上に共有属性は表示されません。ただし、共有属性は「属性エクスプローラー (Attribute Explorer)」にリストされます。ソーシャル・ネットワーク・グラフを作成する元となるエンティティーを右クリックし、「新規グラフの作成 **(Create new Graph)**」>「ソーシャル・ネットワーク **(Social Network)**」を選択します。
  - 「関連エンティティーのみを表示 **(Show related Entities only)**」クイック・フィルターを使用して、ソーシャル・ネットワーク・グラフの「ミニ」版を作成します。このクイック・フィルターは、グラフ上のすべての属性を隠し、選択済みエンティティーに 1 次の隔たりで関連しているエンティティーのみを表示します。(選択済みエンティティー とは、クイック・フィルターを適用するために右クリックしたエンティティーです。)
  - 「関連属性およびエンティティーのみを表示 **(Show related Attributes and Entities only)**」クイック・フィルターを使用して、エンティティーを強調表示し、選択済みエンティティーに関連した属性とエンティティーのみを表示します。
  - 右クリックのメニュー・オプション「レジュメの表示 **(Show Resume)**」を使用して、グラフ上の任意のエンティティーのエンティティー・レジュメを表

示します。エンティティー・レジュメは、エンティティーに関連付けられているアイデンティティー、エンティティーが含まれているその他のアラートなど、そのエンティティーに関する追加の詳細と背景情報を提供します。(Analyst ツールキット内のエンティティー・レジュメへのリンクなどのような、エンティティー・レジュメへのリンクが構成されていない場合、このオプションは右クリック・メニューに表示されません。)

- グラフ上の 2 つのエンティティー間のパスを表示する。
  - 「トップへのパスを表示 **(Show path to top)**」クイック・フィルターを使用して、グラフ上の特定のエンティティーがトップ・エンティティーにどのように関連しているかを視覚化します。このクイック・フィルターは、グラフに複数の層が含まれている場合に特に役立ちます。
  - 右クリックのメニュー・オプション「先頭に移動 **(Move to top)**」を使用して、エンティティーをグラフの先頭に移動し、既存の属性とエンティティーが新しいトップ・エンティティーにどのように関連しているかに基づいてそれらを再表示します。新しい情報はグラフに追加されません。
- 属性に関する詳細をさらに表示する。
  - 「属性のみを表示 **(Show Attributes only)**」クイック・フィルターを使用して、グラフ上の 1 つのエンティティーの情報にフォーカスします。このフィルターは、選択したエンティティーの属性のみを表示するのに便利です。
  - 右クリックのメニュー・オプション「残りの属性の表示 **(Show remaining Attributes)**」を使用して、現在のグラフ上で他のエンティティーと共有されていない属性も含め、特定のエンティティーのすべての属性を視覚化します。
  - 「属性エクスプローラー **(Attribute Explorer)**」を使用して、特定の属性を共有しているグラフ上のエンティティーを強調表示します。「エンティティー」列の値をガイドとして使用できます。この列の数値が大きいほど、グラフに表示されているより多くのエンティティーが、その属性を共有しています。
- エンティティーと属性を再配置して他のパターンやシェイプにするには、右クリック・メニューを使用してグラフ・レイアウトを「階層化 **(Layered)**」から「放射状 **(Radial)**」に変更します。

ソーシャル・ネットワーク・グラフ

ソーシャル・ネットワーク・グラフは、選択したエンティティーと選択したエンティティーがリンクされているすべてのエンティティーの間の関係を視覚化するのに役立ちます。このユニークなグラフを使用することで、「誰が誰を知っているか」を確認する新しい手段を得られます。



ソーシャル・ネットワーク・グラフには以下が表示されます。

- エンティティー間のリンク: メイン (ハブ) エンティティーに関連したすべてのエンティティーが表示されます。ただし、エンティティー同士をリンクする属性はグラフに表示されません。しかし、グラフと組み合わせて「属性エクスプローラー (Attribute Explorer)」を使用することで、属性にはアクセス可能です。
- 関係クラスター: ソーシャル・ネットワーク・グラフは、関連エンティティーをグループまたはクラスターで表示するという点でユニークです。このグラフは、特定のエンティティーが属しているすべての関係クラスターを表示し、クラスターや関係に含まれるパターンを見つけるのに役立ちます。

任意のエンティティーのすべての関連エンティティーを表示するようにグラフを展開できます。特定のエンティティーに関連したすべてのエンティティーを表示するたび、そのエンティティー・ノードが新しい関係クラスター内のハブ・エンティティーになります。

各関係クラスターの整合性を維持するために、同じエンティティーがグラフ上で、複数の関係クラスターに表示されることがあります。ただし、各関係クラスター内に各エンティティーが表示されるのは 1 回のみです。そのエンティティーが一部として含まれている関係クラスターをすべて確認するには、該当ノードをクリックすることでエンティティーを選択してください。選択したエンティティー・ノードの内部が、そのエンティティーが一部として含まれている各関係クラスター内で青色に変わります。

あるエンティティーがハブ・エンティティーである場合、ハブ・エンティティーに関連したエンティティーはすべて関係クラスターに既に表示されているため、「関連エンティティー (Related Entities)」インディケーターは表示されません。エンティティーが関係クラスター内のいずれかの関連エンティティーであり、そのクラスターに表示されていない他の関係を保持している場合は、「関連エンティティー (Related Entities)」インディケーターが表示されます。

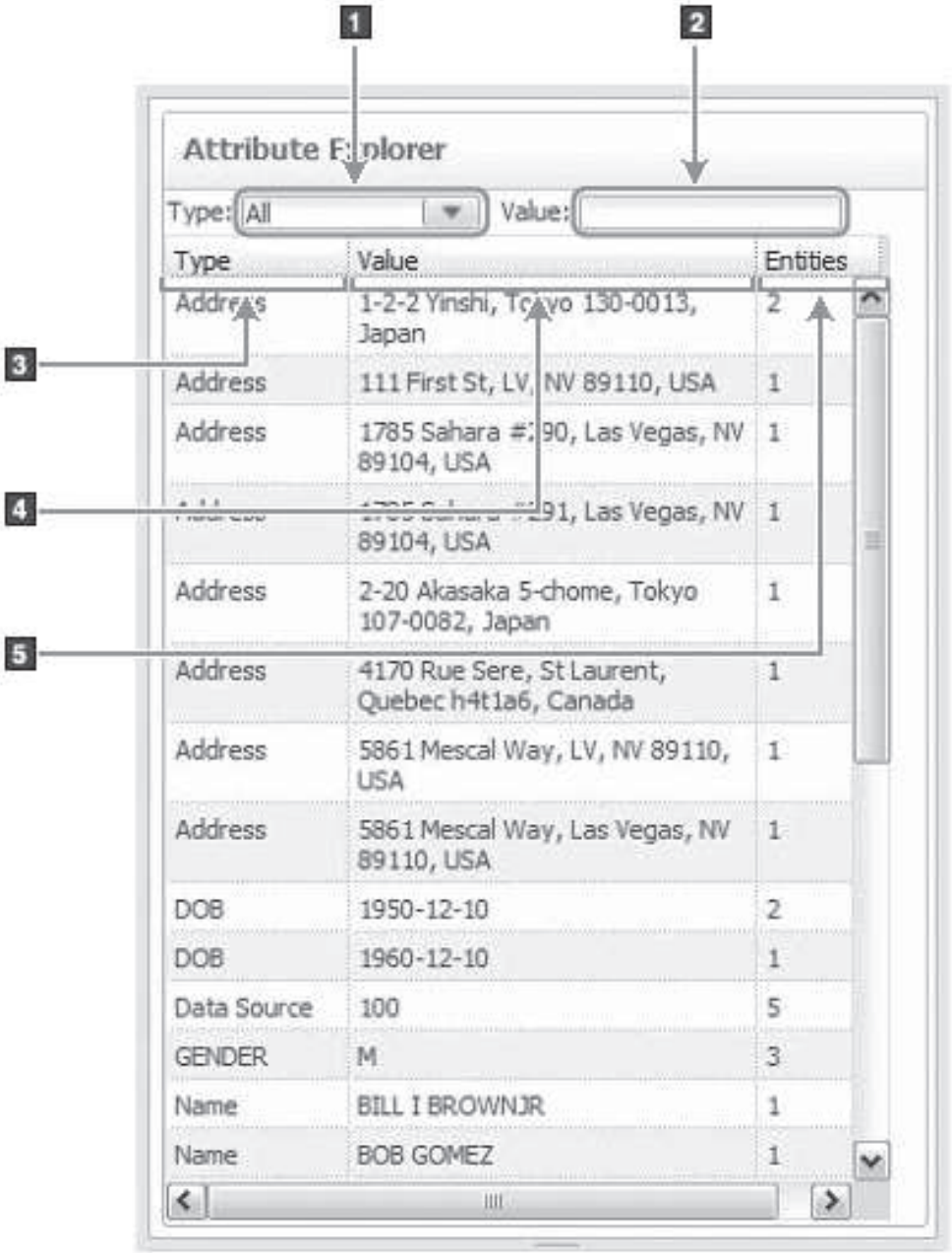
ソーシャル・ネットワーク・グラフの使用に関するヒント

- 右クリック・オプション「残りの関連エンティティーの表示 **(Show remaining related Entities)**」を使用して、グラフ上の 1 つ以上のエンティティーの関連エンティティーを展開します。展開するごとに別の関係クラスターが作成されます。クラスター間でパターンを探します。
- 複数の関係クラスターがグラフ化されている場合、ズームアウトして、それらのクラスターに含まれる、より大きなパターンや背景情報を探してみてください。例えば、特定のエンティティーがすべてのクラスターまたは多数のクラスターに出現する場合、そのエンティティーは特定の範囲内における重要なインフルエンサーである可能性があります。あるいは、そのエンティティーは、複数の関係クラスターを接続するキーになる可能性があります。
- 関連エンティティー同士をリンクしている属性を確認するには、「属性エクスプローラー **(Attribute Explorer)**」を使用します。特定の属性の行を選択すると、その属性を共有するすべてのエンティティーがグラフ上で強調表示されます。「エンティティー」列の値を見ると、どの属性がほとんどのエンティティーによって共有されているかがわかります。

「属性エクスプローラー (Attribute Explorer)」

グラフ・ツールのコンポーネントである「属性エクスプローラー (Attribute Explorer)」は、現在表示されているグラフ上のすべてのエンティティーに関連付けられているタイプ別の属性と値がすべてリストされた表です。「属性エクスプローラー (Attribute Explorer)」は、グラフ・キャンバスの右側に自動的に配置されます。

「属性エクスプローラー **(Attribute Explorer)**」の各パート



イメージ上のコールアウト番号	項目	説明
1	「タイプ」ドロップダウン・リスト	「属性エクスプローラー (Attribute Explorer)」に表示される属性データをフィルタリングするための属性タイプを選択します。 「タイプ」ドロップダウン・リストを使用して、グラフをフィルタリングするわけではありません。フィルタリングされるのは、「属性エクスプローラー (Attribute Explorer)」内のデータのみです。例えば、「**SSN**」を選択して「属性エクスプローラー (Attribute Explorer)」内のデータをフィルタリングして、社会保障番号のみを表示するようにできます。 このドロップダウン・リストには、製品のすべての構成済み属性タイプが含まれるわけではありません。このリストには、現在グラフに表示されているエンティティーに関連付けられた属性タイプのみが含まれます。
2	「値」テキスト・ボックス	属性値に基づいて、表に表示される属性情報を絞り込む場合、このフィールドにデータを入力します。「属性エクスプローラー (Attribute Explorer)」は、入力された各文字を調べて、データが完全一致か部分的な一致かにかかわらず、入力と正確に一致する属性値のリストを返します。 例えば、123 と入力した場合、「属性エクスプローラー (Attribute Explorer)」は、属性のリストをフィルタリングして、属性値の任意の場所に 123 が含まれる属性タイプのみに絞り込みます。 **注:** 「属性エクスプローラー (Attribute Explorer)」は、ワイルドカード文字を認識しません。テキスト・ボックスに入力された文字が何であろうと、「属性エクスプローラー (Attribute Explorer)」はその文字に正確に一致するリテラルを検索します。したがって、* (アスタリスク) などの典型的なワイルドカード文字を入力すると、「属性エクスプローラー (Attribute Explorer)」は * 文字に一致するリテラル・データ値を探します。

イメージ上のコールアウト番号	項目	説明
3	「タイプ」列	グラフに現在表示されている属性タイプが表示されます。この列の項目は、構成コンソールで「属性タイプ (Attribute Types)」に構成された記述と一致します。例えば、クレジット・カード属性タイプの場合、構成コンソールでどのように構成されたかに応じて、「**CC**」または「クレジット・カード」と表示される可能性があります。 この列には、製品のすべての構成済み属性タイプが含まれるわけではありません。この列には、現在グラフに表示されている属性タイプのみが含まれます。
4	「値」列	グラフに現在表示されている属性タイプの値が表示されます。 例えば、「生年月日」属性タイプに対応する **04-01-1962** という値が表示されます。
5	「エンティティー」列	この属性タイプおよび値を共有している、グラフに表示されているエンティティーの数を示します。この情報は、さらに調査を進めるうえで、最も多く共有されている属性を識別するのに役立ちます。

「属性エクスプローラー (Attribute Explorer)」の使用に関するヒント

「属性エクスプローラー (Attribute Explorer)」は、グラフの分析、特にグラフに多くの情報が含まれている場合、役に立ちます。

- 「エンティティー」列を使用して、グラフ上の 1 エンティティーのみに関連付けられた属性を探します。列内で「1」を見つけます。グラフにはエンティティー同士をリンクする属性のみが表示されますが、「属性エクスプローラー (Attribute Explorer)」には、グラフ上のすべてのエンティティーに関連付けられたすべての属性が表示されます。そのような属性はグラフ上でエンティティーを他のエンティティー・ノードにリンクしていませんが、それらの属性から、さらに調査する価値がある特定のエンティティーが見つかる場合があります。
- 「タイプ」ドロップダウン・リストからタイプを選択して、「属性エクスプローラー (Attribute Explorer)」に表示される情報を 1 つの属性タイプに絞ります。例えば、「電話番号」が表示されている場合にそれを選択すると、「属性エクスプローラー (Attribute Explorer)」には電話番号属性とその値のみが表示されます。
- 「属性エクスプローラー (Attribute Explorer)」内で属性 (表の行) を選択すると、グラフ上で同じ属性を共有しているすべてのエンティティーが強調表示されます。

- 「値」にデータを入力して、既存のグラフ・データ上で一致または共通する属性値を検索します。例えば、123 と入力した場合、「属性エクスプローラー (Attribute Explorer)」には以下のマッチング属性のいずれかまたはすべてが返される可能性があります。

タイプ	値
住所	**123** Main Street, Anywhere, California, 1**123**4, USA
住所	97-**123** Rue Sere, St. Laurent, Quebec, H4T1A6, Canada
電話番号	555-222-5**123**
納税 ID	554-**123**-3**123**

- 完全な値または部分的な値を一度に複数、「値」に入力することもできます。「属性エクスプローラー (Attribute Explorer)」は、そのような複数の値を「AND」クエリーとして扱います。例えば、dog cat と入力した場合、「属性エクスプローラー (Attribute Explorer)」はすべての行から dog と cat の両方を含んでいる行を検索します。クエリーに複数含まれる値の順序は任意です。例えば、「属性エクスプローラー (Attribute Explorer)」内のある属性値が her cats and his dogs であるとします。この値は、dog cat 値クエリーの結果の一部に含まれます。
- 「属性エクスプローラー (Attribute Explorer)」内の情報を列でソートします。列見出しをクリックすると、ソートの方向を示す矢印が表示されます。

「選択済みプロパティー (Selected Properties)」

グラフ・ツールのコンポーネントである「選択済みプロパティー (Selected Properties)」表には、グラフ上で選択された属性ノードまたはエンティティー・ノードのプロパティーが表示されます。表に一度に表示されるのは、選択された 1 つのノード (属性またはエンティティー) のプロパティーのみです。

- エンティティーを選択した場合、このセクションには、選択されたエンティティーに関連付けられているすべての属性 (タイプと値) が表示されます。
- 属性を選択した場合、このセクションには、選択された属性を共有するすべてのエンティティー (各エンティティーのエンティティー ID など) が表示されます。このセクションの 3 列目には、属性データの入手元であるデータ・ソースのアイデンティティー ID も表示されます。

グラフ・ツールのグラフのナビゲートと探索

ナビゲーション・ツールバーまたは各グラフの右クリックのメニュー・オプションを使用して、グラフ・ツールにレンダリングされるグラフをナビゲートしたり探索したりできます。

ナビゲーション・ツールバー

グラフ・タイトルのすぐ下にあるナビゲーション・ツールバーには、標準的なグラフ・ナビゲーション用のアイコンが含まれています。

- 選択モード・オプション: 個々のグラフ項目または複数のグラフ項目の選択 (またはグラフの特定のエリアの選択)

- キャンバス上のグラフの位置変更
- グラフのデフォルト・ビューへのリセット
- ズーム・オプション: ズームインまたはズームアウト

選択と強調表示

アラート・グラフおよびエンティティー・グラフで、ノードを選択 (左マウス・クリック) すると、直接関連付けられている属性およびエンティティーが強調表示されます。選択されたノードの外観が変わり、ノード上に青色の長方形選択が表示されます。強調表示されたノードの内部が青色に変わります。

表 33. グラフ・ツールの右クリックのメニュー・オプションの説明

選択するノードのタイプ...	グラフのタイプ...	強調表示されるデータ...
属性	アラート・グラフ エンティティー・グラフ	その属性を共有するすべてのエンティティー すべての関連属性
エンティティー	アラート・グラフ エンティティー・グラフ	選択されたエンティティーに次数 1 で関連しているすべてのエンティティー 1 次の関係の原因となる属性
エンティティー	ソーシャル・ネットワーク・グラフ	そのエンティティーがグラフ上に表示されるたび、選択されたエンティティーが関連しているすべてのハブ。(このグラフ・タイプの場合、1 つのエンティティーが複数のハブに複数回表示される可能性があります。)

Ctrl を使用して複数のノードを選択できます。また、現在選択済みのノードをグラフ上でドラッグ・アンド・ドロップすることで、それらを移動することもできます。

右クリックのメニュー・オプション

カーソルでエンティティーまたは属性をポインティングすることでそれを選択し、右クリックします。

表 34. グラフ・ツールの右クリックのメニュー・オプションの説明

右クリックのメニュー・オプション...	実行するアクション...	アラート・グラフ	エンティティー・グラフ	ソーシャル・ネットワーク・グラフ
ズーム	ズームイン、ズームアウト、または画面サイズにグラフ・キャンバスが収まるようにします。	X	X	X
クイック・フィルター **(**全般**)**	関心が低いデータを一時的に非表示にすることで、興味のあるグラフ・データに集中できるようにします。クイック・フィルターによってグラフにデータが追加されたり、データが削除されるわけではありません。 クイック・フィルターがオンになっている場合、グラフ・タイトル・バーに「[クイック・フィルター・オン] ([Quick Filter On])」と表示されます。 一度にアクティブにできるクイック・フィルターは 1 つのみですが、クイック・フィルターがアクティブであれば別のクイック・フィルターを選択できます。 **注:** クイック・フィルターがアクティブである場合、フィルターによって、現在選択されているエンティティーまたは属性に適用されたグラフ・データのみが表示されます。例えば、エンティティー ABC を選択し、「関連エンティティーのみを表示 **(Show related Entities only)**」クイック・フィルターを選択すると、次数 1 で ABC に関連したエンティティーのみがグラフ上に表示されます。	X	X	

表 34. グラフ・ツールの右クリックのメニュー・オプションの説明 (続き)

右クリックのメニュー・オプション...	実行するアクション...	アラート・グラフ	エンティティー・グラフ	ソーシャル・ネットワーク・グラフ
「クイック・フィルター **(Quick Filter)**」 - 「属性のみを表示 **(Show Attributes only)**」	エンティティーを非表示にし、右クリックしたエンティティーに関連付けられた属性のみが表示されるようにします。	X	X	
「クイック・フィルター **(Quick Filter)**」 - 「関連エンティティーのみを表示 **(Show related only)**」	エンティティー同士をリンクしている属性を含め、すべての属性を非表示にし、右クリックしたエンティティーに次数 1 で関連しているエンティティーが表示されるようにします。 このクイック・フィルターは、アラート・グラフまたはエンティティー・グラフからソーシャル・ネットワーク・グラフのような外観を提供します。	X	X	
「クイック・フィルター **(Quick Filter)**」 - 「関連属性およびエンティティーを表示 **(Show related Attributes and Entities)**」	右クリックしたエンティティーに次数 1 でリンクされたエンティティーならびに 1 次の関係の原因となる属性を除き、すべてのグラフ・データを非表示にします。 このクイック・フィルターは、グラフ上に多くのデータが存在する場合に、余分な混乱を取り除くのに特に役立ちます。	X	X	

表 34. グラフ・ツールの右クリックのメニュー・オプションの説明 (続き)

右クリックのメニュー・オプション...	実行するアクション...	アラート・グラフ	エンティティー・グラフ	ソーシャル・ネットワーク・グラフ
「クイック・フィルター **(Quick Filter)**」 - 「トップへのパスを表示 **(Show path to top)**」	グラフ・データをフィルタリングして、エンティティーまたは属性とトップ・エンティティーを接続しているパスを表示します。 属性を右クリックしていた場合、フィルターによって、トップ・エンティティーへの関係パス上に存在するすべてのエンティティーと属性が組み込まれます。 エンティティーを右クリックしていた場合、フィルターによって、トップ・エンティティーへのパス上に存在するすべての属性とエンティティーが組み込まれます。	X	X	
「クイック・フィルター **(Quick Filter)**」 - 「クイック・フィルターをオフにする **(Turn off quick filtering)**」	現在のクイック・フィルターをオフにし、グラフからフィルタリングされていたデータを再表示します。	X	X	
「先頭に移動 **(Move to top)**」	選択済みエンティティーをグラフの先頭に移動し、そのエンティティーをトップ・エンティティーにします。 このオプションは、グラフまたは「属性エクスプローラー (Attribute Explorer)」に新規データを追加するわけではありません。その代わり、グラフが再作成され、新しいトップ・エンティティーの視点からデータが表示されます。	X	X	

表 34. グラフ・ツールの右クリックのメニュー・オプションの説明 (続き)

右クリックのメニュー・オプション...	実行するアクション...	アラート・グラフ	エンティティー・グラフ	ソーシャル・ネットワーク・グラフ
「残りの属性の表示 **(Show remaining Attributes)**」	右クリックしたエンティティーに関連付けられたすべての属性 (グラフ上でエンティティーがその属性を介して他のエンティティーにリンクされていなくとも) を表示します。 「属性エクスプローラー (Attribute Explorer)」には、エンティティーに関連付けられたすべての属性が常にリストされるため、「属性エクスプローラー (Attribute Explorer)」では、このオプションによるデータの変化はありません。 エンティティーのその他の属性を表示すると、パズルのピースが新しく見つかることもあれば、エンティティーや属性のさらに詳しい調査に導かれる可能性もあります。	X	X	
「残りの属性の非表示 **(Hide remaining Attributes)**」	グラフ上に表示されているエンティティーをリンクしていない属性をグラフから削除します。 グラフ上に表示されているすべての属性が、現在グラフに表示されているエンティティーをリンクしている場合、このオプションは使用できません。	X	X	
「残りの関連エンティティーの表示 **(Show remaining related Entities)**」	右クリックしたエンティティーを対象にまだ表示されていないすべての関係を表示します。関係の原因となる属性も表示されます。	X	X	X

表 34. グラフ・ツールの右クリックのメニュー・オプションの説明 (続き)

右クリックのメニュー・オプション...	実行するアクション...	アラート・グラフ	エンティティー・グラフ	ソーシャル・ネットワーク・グラフ
「新規グラフの作成 **(Create new Graph)**」	ユーザーが右クリックしたエンティティーをメイン・エンティティーとしてフィーチャーした、選択されたタイプの新しいグラフを作成します。	X	X	X
グラフ・レイアウト	グラフ・レイアウトの表示を制御します。 • 「階層化 (Layered)」: グラフ・データを層で表示し、属性およびそれらの属性にリンクされているエンティティーの行を交互に示します。このレイアウトが、アラート・グラフとエンティティー・グラフ両方のデフォルトのレイアウトです。 • 「放射状 (Radial)」: グラフ・データをグラフ・キャンバス上でランダムに分散されたノードと接続線として表示します。このレイアウトは、エンティティーおよび属性を自身で整列する場合に便利です。	X	X	

表 34. グラフ・ツールの右クリックのメニュー・オプションの説明 (続き)

右クリックのメニュー・オプション...	実行するアクション...	アラート・グラフ	エンティティー・グラフ	ソーシャル・ネットワーク・グラフ
「レジュメの表示 **(Show Resume)**」	graph.properties ファイル内にリンクが構成されている場合、エンティティー・レジュメを新しいウィンドウに表示します。 エンティティー・レジュメは、エンティティーが含まれているすべてのアラートやエンティティーに関連付けられたすべてのアイデンティティーなど、選択されたエンティティーに関する詳細情報を提供します。レジュメは便利な分析ツールであり、グラフ・ツールのグラフと併用すると特に便利です。 この右クリック・オプションは、エンティティー・レジュメ URL が graph.properties ファイル内に構成されている場合にのみ使用可能です。例えば、ユーザーの組織が Analyst ツールキットをインストールしてある場合、Identity Insight システム・アドミニストレーターがリンクを構成して、Cognos ベースのエンティティー・レジュメを新しい Web ブラウザー・ウィンドウで表示するようにできます。 このリンクが表示されない場合は、Identity Insight システム・アドミニストレーターに連絡してください。	X	X	X

グラフ・ツールのグラフの共通要素

グラフには、アイコン、インディケーター、線の太さなど、多くの共通要素があります。これらの共通要素は、ユーザーが各グラフのストーリーをより完璧に把握したり、関心のあるエリアをより簡単に識別したりできるように助ける、新たな意味をもたらします。

エンティティー・アイコン

各エンティティー・ノードは、実線の円で囲まれたアイコンとして表示されます。

エンティティーは、人、場所、または物事 (組織、船舶、航空機など) として定義できます。一般的には、エンティティーは人です。最も一般的なエンティティー・ノードは、男性、女性、または不明の個人アイコンとして表されます。アイコンによって表示される性別は、以下に示す、可能性がある 2 回の性別割り当てのいずれかに基づきます。

- エンティティー解決の名前分析時に割り当てられる性別
- 入力アイデンティティー・レコードのデータの一部である GENDER 属性の値

性別が不明の場合は、汎用的な個人エンティティー・アイコンが表示されます。

以下の表に、グラフ・ツールのグラフで使用されるデフォルトの個人エンティティー・アイコンを示します。

表 *35.* グラフ・ツールのグラフで使用されるデフォルトのエンティティー・アイコンのサンプル

アイコン...	表しているエンティティー・タイプ...
 グラフ・ツールの女性の個人エンティティー・インディケーター	女性 (個人) エンティティー
 グラフ・ツールの男性の個人エンティティー・インディケーター	男性 (個人) エンティティー
 グラフ・ツールの性別不明の個人エンティティー・インディケーター	性別不明エンティティー

エンティティー・グラフまたはソーシャル・ネットワーク・グラフ上のメイン・エンティティーは、必ず太い円で囲まれます。メイン・エンティティーがグラフ上のどこに表示されていても、太い円を手掛かりに必ず識別できます。

アラート・グラフの場合、アラート・パス上のすべてのエンティティーが太い円で囲まれます。残りの関連エンティティーを表示するように選択した場合など、グラ

フ上にいくつエンティティーが表示されているかに関係なく、アラートに関係するエンティティーを常に識別できます。

属性アイコン

属性ノードは、グラフ・ツールのグラフ上でアイコンとして示されます。各アイコンは、特定の属性タイプを表します。以下の表に、グラフ・ツールのグラフに表示されるデフォルトの属性アイコンのサンプルを示します。

表 *36.* グラフ・ツールに表示されるデフォルトのアイコンのサンプル

アイコン...	表している属性タイプ...
 グラフ・ツールの「住所」属性アイコン	住所
 グラフ・ツールの「名前」属性アイコン	名前
 グラフ・ツールの「社会保障番号」属性アイコン	社会保障番号
 グラフ・ツールの「生年月日」属性アイコン	生年月日
 グラフ・ツールのその他の属性タイプ・アイコン	その他の属性 (既存の属性アイコンに割り当てられていない属性)

デフォルトの属性アイコンを取り替えるか、ユーザーの組織に固有の属性を表すアイコンを追加することで、グラフ上の属性を表すアイコンをカスタマイズできます。詳細については、 397 ページの『グラフ・ツールのグラフへのカスタム・アイコンの追加』を参照してください。

「アラート」インディケーター

各エンティティーに、そのエンティティーのアラートの数を示すインディケーターが表示されます。「アラート」インディケーターは、エンティティー・アイコンを囲む実線の円の左上隅に表示されます。

「アラート」インディケーターは背景が金色で、そこにアラートの数が黒いテキストで表示されます。例えば、あるエンティティー・アイコンの次の「アラート」イ

ンディケーター  は、このエンティティーに 25 件のアラートがあることを示しています。

「関連エンティティー (Related Entities)」インディケーター

エンティティー・ノードには、共有属性に基づいて、このエンティティーに属している関係の数を示すインディケーターもあります。これらの関係は、まだこのエンティティーの一部としては表示されていません。

「関連エンティティー (Related Entities)」インディケーターは背景が薄い青色で、そこに関係の数が太字の黒いテキストで表示されます。例えば、次の「関連エンティティー (Related Entities)」インディケーター  は、このエンティティーと関係を持つエンティティーとしてまだ表示されていない 6 個の追加エンティティーが存在することを示しています。

「関連エンティティー (Related Entities)」インディケーターは、グラフのタイプに応じて動作が異なります。

- アラート・グラフの場合: アラートに含まれる両方のエンティティーで、そのエンティティーがグラフ上に現在表示されていない追加のエンティティーに関連している場合、「関連エンティティー (Related Entities)」インディケーターが表示されます。グラフに表示されている各エンティティーに関連したすべてのエンティティーを表示するようにグラフを展開できます。この場合、いずれのエンティティーにも「関連エンティティー (Related Entities)」インディケーターは表示されなくなります。
- エンティティー・グラフの場合:
  - メイン・エンティティーに「関連エンティティー (Related Entities)」インディケーターはありません。グラフには、そのメイン・エンティティーに関連したすべてのエンティティーが自動的に表示されます。
  - エンティティー・グラフ上の他のエンティティーについては、それらのエンティティーがグラフ上にまだ表示されていないその他のエンティティーに関連している場合、「関連エンティティー (Related Entities)」インディケーターが表示されます。右クリック・メニューを使用して、そのようなエンティティーの残りのエンティティーを表示でき、そうすると「関連エンティティー (Related Entities)」インディケーターは表示されなくなります。
  - アラート・グラフと同様に、グラフに表示されている各エンティティーに関連したすべてのエンティティーを表示するようにグラフを展開できます。この場合、いずれのエンティティーにも「関連エンティティー (Related Entities)」インディケーターは表示されません。
- ソーシャル・ネットワーク・グラフの場合:
  - グラフにはハブ・エンティティーに対して、クラスター情報内のすべての関連エンティティーが自動的に表示されるため、ハブ・エンティティー (クラスターの中央) に「関連エンティティー (Related Entities)」インディケーターはありません。

– 関係クラスター内のハブ・エンティティー以外のエンティティーについては、それらのエンティティーが、指定されたノードにまだリンクされていないその他のエンティティーに関連している場合、「関連エンティティー (Related Entities)」インディケーターが含まれることがあります。
– 複数の関係クラスターを組み込むようにグラフを展開した場合、同じエンティティーがグラフに複数回表示される可能性があります。エンティティーがクラスターのハブである場合、「関連エンティティー (Related Entities)」インディケーターは表示されません。しかし、その同じエンティティーが関係クラスターの一部に含まれ、かつ、そこではハブ・エンティティーでない場合に、そのエンティティーに対してまだグラフ上に表示されていない追加の関連エンティティーが存在すると、「関連エンティティー (Related Entities)」インディケーターが表示されます。このため、グラフには必ずいくつかの「関連エンティティー (Related Entities)」インディケーターが表示されています。

線インディケーター

エンティティー・ノードを囲む線やエンティティーと属性を接続する線が、追加情報を提供する場合があります。

- 属性を接続する破線は、属性の近似を示しています。
- エンティティー・ノードを囲む太い線は、メイン・エンティティー、すなわち、この特定のグラフを作成するときに選択または要求されたエンティティーであることを示しています。

グラフ・ツールの URL 構文およびパラメーター

グラフ・ツールのグラフにアクセスするには、適切な URL にリンクする必要があります。URL は、既存のカスタム・アプリケーション内 (Web Start ページ、ダッシュボード、ケース管理ツールなど) に組み込むことも、Web ブラウザーに手動で入力することもできます。

グラフ・コンポーネントのグラフの正しい URL 構文およびパラメーターは、以下のようになります。

`http://`*`server`*`:`*`port`*`/graphs/run/`*`graphtype`*`.jsp?height=`*`nnnn`*`&width=`*`yyyy`*`&`*`identifier`*`=`*`xxxx`*

hostserver*:*port
製品アプリケーション・サーバーの名前と IBM InfoSphere Identity Insight が配置されているポート番号を示します。通常、製品アプリケーション・サーバーは WebSphere サーバーです。

ポート番号のデフォルトは 13510 です。

/graphs/run
グラフ・ツールのファイルが配置されている製品ディレクトリーを指します。`/graphs/run` ディレクトリーは、製品インストール・プログラムがグラフ・ツールをデフォルトでインストールする場所です。

***graphtype*.jsp**
作成するグラフを示します。

- アラート・グラフの場合は、`role-alert.jsp` と入力します。
- エンティティー・グラフの場合は、`entity.jsp` と入力します。

- ソーシャル・ネットワーク・グラフの場合は、social-network.jsp と入力します。

? URL エレメントを示します。

height=*nnnn*
グラフ・キャンバスの高さ、すなわち、Web ブラウザーのウィンドウ内にグラフ・キャンバスをレンダリングするときの高さを示します。ピクセル数を入力します。

グラフの高さは以下の方法で決定されます。

- 高さが URL に指定されている場合は、それがデフォルトのグラフの高さになります。
- 値が graph.properties ファイル内の **defaultGraphHeight** プロパティーに設定されている場合は、それがデフォルトのグラフの高さになります。
- URL にも **defaultGraphHeight** プロパティーにもグラフの高さが指定されていない場合、デフォルトのグラフの高さは 800 ピクセルに設定されます。

.

概算で、グラフ・キャンバスを 1024 x 768 の標準的な Web ブラウザーのウィンドウに収まるようにするには、高さを 450 ピクセルに設定してください。

? パラメーター間の URL セパレーター・トークンを示します。

width=*yyyy*
グラフ・キャンバスの幅、すなわち、Web ブラウザーのウィンドウ内にグラフ・キャンバスをレンダリングするときの幅を示します。「属性エクスプローラー (Attribute Explorer)」は、Web ブラウザーのウィンドウ内でグラフ・キャンバスの右隣に配置される別コンポーネントであるため、この数値には含まれません。

グラフの幅は以下の方法で決定されます。

- 幅が URL に指定されている場合は、それがデフォルトのグラフの幅になります。
- 値が graph.properties ファイル内の **defaultGraphWidth** プロパティーに設定されている場合は、それがデフォルトのグラフの幅になります。
- URL にも **defaultGraphWidth** プロパティーにもグラフの幅が指定されていない場合、デフォルトのグラフの幅は 800 ピクセルに設定されます。

.

概算で、グラフ・キャンバスを 1024 x 768 の標準的な Web ブラウザーのウィンドウに収まるようにするには、幅を 640 ピクセルに設定してください。

identifier=xxxx
ID のタイプ (エンティティーまたはアラート) とそのエンティティーまたはアラートの特定の番号を示します。エンティティー ID を使用する場合、ID の値は、エンティティー・グラフであればメイン・エンティティー、ソ

ーシャル・ネットワーク・グラフであればハブ・エンティティーにします。アラート ID を使用する場合、値は、アラート・グラフに表示するアラートにします。

- アラート・グラフの場合は、`alertID=specific_alert_ID_number` と入力します。
- エンティティー・グラフまたはソーシャル・ネットワーク・グラフの場合は、`entityID=specific_entity_ID_number` と入力します。

グラフ・ツールの一般的な管理用タスク

グラフ・ツールの一部のタスクは、アドミニストレーター・ユーザーのみが実行できます。

グラフ・ツールのグラフへのカスタム・アイコンの追加**:**

グラフ・ツールには、グラフに表示されるさまざまなタイプの属性を表す標準アイコンが含まれています。1 つ以上の属性のデフォルト・アイコンを変更したり、製品で構成したカスタム属性用のアイコンを追加したりできます。グラフ・ツールのグラフはすべて、製品アプリケーション・サーバー上にある同じイメージ・アイコンのセットを使用します。したがって、属性アイコン・セットをカスタマイズすると、すべてのユーザーに同じ属性アイコンが表示されます。

始める前に

グラフ・アイコンは、Scalable Vector Graphics (SVG) ファイルとして開始します。SVG ファイルは、さまざまなベクトル・ベースの描画ツールを使用して作成したり、さまざまなインターネット・ソースからダウンロードしたりできます。アイコンに使用する SVG ファイルは、(画像が拡大縮小されるときの見やすさを向上させるために) 合理的に小さなサイズに保たれるようにすることを強くお勧めします。

グラフには、Javascript Object Notation (JSON) フォーマットで保管されているシェイプ定義が必要です。SVG から JSON への変換には、**xlstproc** と **sed** の 2 つの個別のコマンド・ユーティリティーを使用する必要があります。

UNIX ベースのコンピューターの場合は、既にこれらのツールがある可能性があります。Windows ベースのコンピューターの場合は、UNIX エミュレーター (無料の Cygwin アプリケーションのような) を使用してこれらの UNIX ベースのツールを入手する必要があります。注*: Cygwin* を使用する場合は、必要なユーティリティーを取得するために、インストール済み環境に必ず *libxml2* ライブラリーと *libxslt* ライブラリーを含めてください。

最後に、無料の DOJO ライブラリーに含まれているファイル svg2gfx.xsl が必要です (https://dojotoolkit.org/download から入手可能)。DOJO をダウンロードすると、<インストール・ルート>/dojox/gfx/resources ディレクトリー内に svg2gfx.xsl ファイルが配置されています。

手順

1. DOJO の場所から、変換する SVG ファイルが含まれる同じディレクトリーに、svg2gfx.xsl ファイルをコピーします。

2. UNIX 端末/コマンド行ウィンドウを開き、SVG ファイルが含まれるディレクトリーに移動します。
3. コマンド `xsltproc ./svg2gfx.xsl <your .SVG file> > <temp_file_name>.json` を実行します。
4. コマンド `sed -e 's/,}/}/g' -e 's/,]/]/g' <temp_file_name.json> > <final name>.json` を実行します。
5. Identity Insight インストール・フォルダーを見つけます。
6. インストール・フォルダーの下の /ibm-home/graphs に移動します。
7. customImages という名前のフォルダーを作成します。名前は大/小文字の区別があります。
8. カスタム・アイコン (.json ファイル) を customImages フォルダーに移動します。

例

FLIGHT という名前の属性タイプを作成済みで、グラフ・ツールのグラフ上でその属性タイプを表すカスタム・グラフ・アイコンが必要だとします。この場合、以下のステップを実行します。

1. FLIGHT 属性タイプを表す適切なイメージ・ファイルを作成または入手します。イメージ・ファイル名が、構成コンソールで構成した属性タイプ名と一致していること、ファイル名にすべて小文字が使用されていることを確認します。例えば、ファイル名は、flight.svg のようになります。
2. svg2gfx.xsl が flight.svg と同じディレクトリーにあることを確認します。
3. UNIX 端末/コマンド行ウィンドウを開き、flight.svg と同じディレクトリーに移動します。
4. コマンド `xsltproc ./svg2gfx.xsl flight.svg > flight_tmp.json` を実行します。
5. コマンド `sed -e 's/,}/}/g' -e 's/,]/]/g' flight_tmp.json > flight.json` を実行します。
6. flight.json アイコン・ファイルを /customImages フォルダーにコピーします。

カスタム・グラフ・アイコンの要件:

グラフに表示される属性アイコンをカスタマイズできます。ただし、グラフがアイコンを認識して表示できるようにするために、新しいアイコンはカスタム・グラフ・アイコンの要件を満たしている必要があります。

カスタム・アイコンの要件

製品のグラフがカスタム・アイコンを認識して表示するためには、属性アイコンが以下の要件を満たしていなければなりません。

- ファイル形式: Scalable Vector Graphics (SVG)
- 名前:
  - カスタム・アイコン名は、構成コンソールで構成された、対応する属性タイプの名前と一致しなければなりません。

– カスタム・アイコン名に使用できるのは、小文字のみです。

- SVG ファイルは JSON シェイプ定義に変換する必要があります (397 ページの『グラフ・ツールのグラフへのカスタム・アイコンの追加』を参照)。

例えば、属性アイコンを構成コンソールで構成された属性タイプ FINGERPRINTS に関連付ける場合、アイコン・ファイルの名前を `fingerprints.svg` にする必要があります。

名前の例

既存の基本タイプのアイコンをオーバーライドする場合、 カスタム・アイコンは、以下のいずれかの名前にする必要があります (すべて小文字)。

- address.json
- female.json
- male.json
- name.json
- undetermined_gender.json

エンティティー番号の場合、.json アイコン・ファイルは、番号タイプ・コード (データベースの NUM_TYPE.NUM_TYPE) と同じ名前にする必要があります。例:

- cc.json
- dl.json
- ff.json
- ssn.json
- pp.json
- ph.json

エンティティー特性の場合、.json アイコン・ファイルは、属性タイプ・コード (データベースの ATTR_TYPE.ATTR_TYPE) と同じ名前にする必要があります。例:

- dob.json
- died.json
- marital.json
- circa_dob.json
- pop.json
- nat.json
- cit.json

グラフ・ツールからエンティティー・レジュメへのリンク**:**

エンティティー・レジュメは、個々のエンティティーに関する詳細情報を提供し、アラートやエンティティー関係を分析する場合に有用です。URL プロパティーをエンティティー・レジュメを生成する Web アプリケーションに設定しておくと、グラフ・ツールのユーザーがグラフ・ツールのグラフ内からエンティティー・レジュメを開くことができます。

このタスクについて

リンクの設定は、グローバル・タスクです。リンクが設定された後は、グラフ・ツールのグラフを表示するすべてのユーザーが、右クリック・メニューからリンクにアクセスできるようになります。リンク・プロパティーが設定されていない場合、右クリック・オプション「レジュメの表示 **(Show Resume)**」は表示されません。

手順

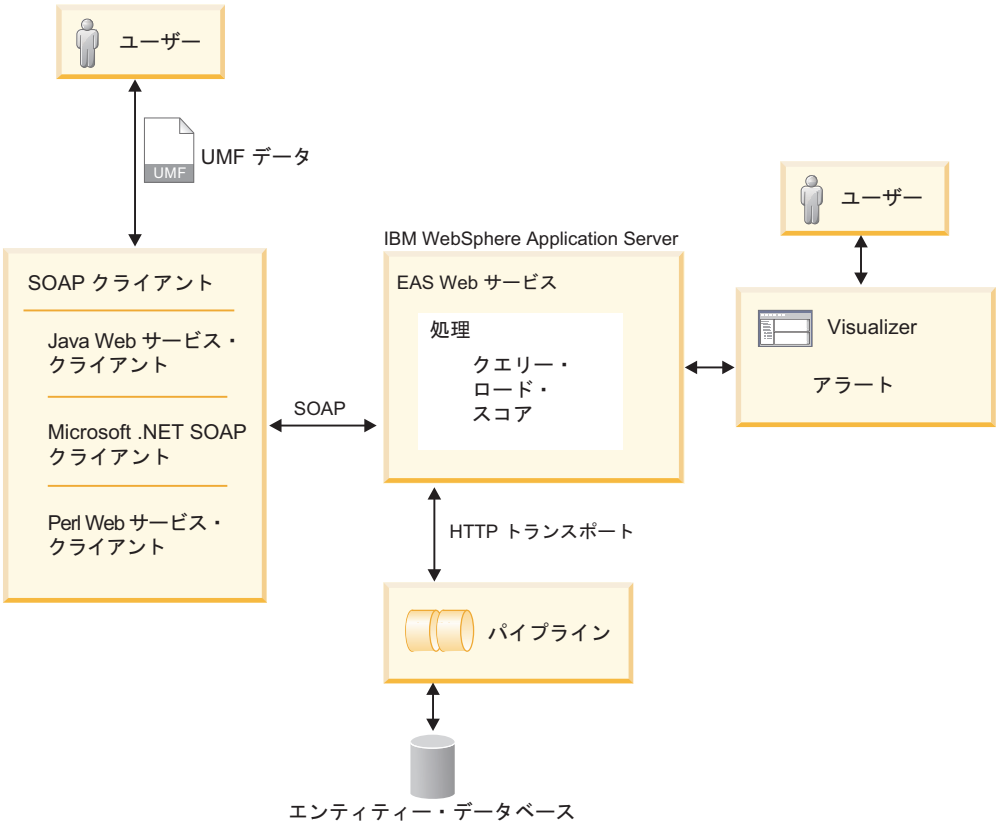
1. システム・アドミニストレーターが COMPONENT_CONFIG 表の RESUMESERVER プロパティーを Cognos ツールキット・レポートへのリンクで更新します。
   a. このプロパティーの値を実際の URL に置き換えます。ホスト・サーバー、ポート名、および Web アプリケーションへのパスを指定します。 パスがどのようになるかを理解するには、サンプル値を参考にしてください。例えば、組織が Cognos ベースの Analyst ツールキットをインストールして使用している場合、Analyst ツールキットによって生成されるエンティティー・レジュメへのパスを指定します。
   b. トークン **%ISIIEntityID%** がパラメーター値内にあることを確認します。このパラメーターによって、正しいエンティティー・レジュメを生成するために適切なエンティティー ID が Web アプリケーションに送信されます。
2. オプション: リンクをテストします。

第 9 章 開発

ご使用の環境で Web サービスを使用する必要がある場合、IBM InfoSphere Identity Insight によってシンプルな XML ベースの Web サービスが提供されます。

Web サービス

IBM InfoSphere Identity Insight は、外部アプリケーションを作成するために使用できる一連の Web サービスを提供しています。外部アプリケーションにより、パイプライン処理のため、またはエンティティー・データベース内のエンティティーの検索のために Universal Message Format (UMF) データをロードできます。パイプラインの標準機能である双方向の HTTP (Hypertext Transfer Protocol) トランスポート・メソッドを使用します。



IBM InfoSphere Identity Insight の Web サービスでは、4 つの SOAP (Simple Object Access Protocol) メソッド (process、search、load、および score) が使用されます。本製品は SOAP バージョン 1.1 をサポートしています。

本製品には、Web サービスの初めての使用を支援する複数のコンポーネントが含まれます。

srd.wsdl

このファイルには、製品の Web サービスの Web サービス記述言語 (WSDL) 定義が含まれます。このファイルと任意の SOAP ツールキットまたはテクノロジーを使用することで Web サービスを開始できます。ファイルは、WebSphere Liberty を開始し、http://hostname:port/easws/resources/wsdl/srd.wsdl からファイルをロードすることで見つけることができます。

wsutil.jar

このファイルは、Web サービスのインストールおよび構成をテストするために提供されている Web サービス・テスト・クライアントです。このユーティリティーは、`ibm-home/easws` ディレクトリーにあります。

Web サービス・ソフトウェア要件

IBM InfoSphere Identity Insight Web サービスは、所定のソフトウェアがインストールされており、作動可能であることを必要とします。

Web サービスの使用を開始する前に、以下のソフトウェアがインストールされており、作動可能であることを確認してください。

- IBM InfoSphere Identity Insight Web サービスがインストールされており、稼働している必要があります。
- IBM InfoSphere Identity Insight Web サービスがデプロイされる場所で、組み込み IBM WebSphere Application Server が稼働している必要があります。ほとんどの場合、これは構成コンソールおよび Visualizer がインストールされているのと同じアプリケーション・サーバーです。
- Web サービス・パイプラインが開始済みであり、適切な HTTP URL を listen している必要があります。アプリケーション・サーバーは、SOAP 要求を受け取ると、指定された HTTP URL を介してこの Web サービス・パイプラインに UMF データを送信しようとします。

  注**:** アプリケーション・サーバーとパイプラインの間の通信に使用される HTTP URL は、SOAP 要求を送信しようとする Web サービス・クライアントが使用する URL とは異なります。 Web サービス・パイプラインの HTTP URL に直接 SOAP 要求を送信しようとするとエラーになります。

  例えば、WebSphere Application Server が、デフォルトのポート範囲を使用してセットアップされている場合、ポート番号とその用途は以下のようになります。

  – *nnn*0 - Web サーバー用 HTTP ポート
  – *nnn*1 - Web サーバー用 HTTPS ポート
  – *nnn*2 - HTTP 管理ポート
  – *nnn*3 - HTTPS 管理ポート
  – *nnn*4 - SOAP ポート
  – *nnn*5 - アプリケーション・サーバーのポート
- 組み込み WebSphere Application Server が、Web サービス要求を処理するパイプラインを見つけられるように、webservices.properties ファイルには実行中

のパイプラインの HTTP URL が構成されている必要があります。通常、このファイルは次のディレクトリーにあります: *product_home*/srd-home/easws

- IBM InfoSphere Identity Insight Web サービスを呼び出すために使用される、SOAP および WSDL 互換の Web サービス・クライアントが存在している必要があります。以前のリリースのサービスをテストするためのサンプル・クライアント wsutil.jar が IBM InfoSphere Identity Insight Web サービスとともにインストールされますが、バージョン 8.0 フィックスパック 2 の拡張サービスには適用されません。

Web サービス・パイプラインの開始

Web サービス経由で送信されるデータを送信および処理するために、双方向の HTTP トランスポートを使用してパイプラインを開始します。通常、Web サービスで使用されるパイプラインはバックグラウンドで常に実行を続け、処理するデータがないかどうか、割り当てられたポートを listen し続けます。以下の手順に従って、Web サービス・パイプラインを開始します。

始める前に

- webservices.properties ファイル内に構成されているパイプライン URL 設定がわかっている必要があります。この設定は、パイプラインの組み込み IBM WebSphere Application Server 上で実行されている Web サービス・コンポーネントを指しており、Web サービス・パイプラインを開始するのに使用される URL に一致しなければなりません。
- パイプラインをホストするパイプライン・ノードに、パイプライン実行可能ファイルがインストールされている必要があります。
- 開始するパイプラインに使用するパイプライン構成ファイルが、少なくとも 1 つ構成されている必要があります。使用するパイプライン構成ファイルをパイプライン開始コマンドの一部として指定できます。パイプライン・コマンドの一部として構成ファイルの名前を指定しない場合は、パイプライン・ノード上でパイプライン構成ファイルが見つからなければならず、ファイル名は、デフォルトのパイプライン構成ファイル名である pipeline.ini でなければなりません。
- スクリプトを使用してパイプラインを開始する場合は、必ず、開始するパイプラインと同じディレクトリーにスクリプトを配置してください。
- このパイプラインからの処理結果をルーティングする場合、またはこのパイプラインの統計情報と状況をモニターする場合は、構成コンソールの「パイプライン **(Pipelines)**」タブでパイプラインを登録してください。モニターやルーティングが正常に実行されるためには、既に登録済みのいずれかのパイプライン名を使用して、このパイプラインを開始する必要があります。
- アプリケーション・モニターを使用してパイプラインの状況と統計情報をモニターする場合は、必ず、SNMP エージェントがパイプライン・ノードにインストールされており、このパイプラインを開始する前に稼働しているようにしてください。
- このパイプラインが結果を別のシステムまたは別のデータベースにルーティングする場合、必ず、パイプラインを開始するディレクトリーと同じディレクトリーにこのパイプラインのルーティング・ファイルを置いてください。
- *DEFAULT_CONCURRENCY* システム・パラメーターが 1 より大きい値に設定されている場合、またはパイプライン・ノードのパイプライン構成ファイルに

concurrency パラメーターを構成してある場合は、単一のパイプライン開始コマンドを使用して複数の並列パイプライン処理スレッドを開始することができます。

このタスクについて

パイプラインを開始するには、3 つのステップがあります。

手順

1. 開始しようとしているパイプラインと同じ名前のパイプラインがパイプライン・ノード上で他に現在稼働していないことを確認してください。各パイプラインには、そのパイプライン・ノードにおいて一意の名前が必要です。(デフォルトのパイプライン名は `pipeline` です。) これを確認するには、以下の 2 つの方法があります。
   a. アプリケーション・モニターを使用してパイプラインの状況を確認したり、結果を他のシステムにルーティングしたりしている場合は、「パイプラインの状況 **(Pipeline Status)**」タブを見て、使用しようとしている名前と同じ名前を持つ別のパイプラインが稼働していないかどうか調べてください。
   b. または、コマンド・プロンプトで、次のコマンドを入力します。

   ```
   pipeline -n pipelinename -l
   ```

   ここで、*pipelinename* は新規パイプラインを開始するために使用する名前です。この名前が、構成コンソールに登録されているこのパイプラインの名前に一致することを確認してください。
2. コマンド・プロンプトで、次の形式で適切なパイプライン・コマンドのオプションとパラメーターを指定して、1 つ以上のパイプラインを開始します。

   ```
   pipeline -option parameter
   ```

   注**:** このパイプラインにアプリケーション・モニターを使用しており、構成コンソールでこのパイプラインがモニターまたはルーティングの対象として登録されている場合は、必ず、パイプライン開始コマンドの一部として `-n` オプションを使用し、登録済みのパイプライン名を指定してください。指定したパイプライン名が登録済みのパイプライン名に (大/小文字も含めて) 正確に一致しない場合、パイプラインの状況が構成コンソールの「パイプラインの状況 **(Pipeline Status)**」タブに正しく表示されず、このパイプライン用に構成されたルーティングは、どれも正常に機能しません。

   注**:** 通常、`-s` または `-d` のいずれかのパイプライン・オプションを適宜使用して、サービス/デーモン・モードまたはデバッグ・モードのいずれかでパイプラインを開始します。
3. コマンドが機能し、パイプラインが開始され、アクティブであることを確認します。
   a. アプリケーション・モニターを使用しており、このパイプラインが構成コンソールに登録済みである場合は、「パイプラインの状況 **(Pipeline Status)**」タブを調べます。 パイプラインがアクティブである場合、状況は「アクティブ (Active)」として表示されます。

b. システムが Microsoft Windows プラットフォームで稼働しており、サービス・パイプライン・オプションを使用している場合は、パイプラインの状況を Microsoft Windows サービスのコントロール・パネルで見ることができます。

c. システムが UNIX プラットフォームで稼働しており、デーモン・パイプライン・オプションを使用している場合は、次のコマンドを入力して、実行中の処理を確認できます。

```
ps -fu userid
```

ここで、*userid* はパイプラインを開始しているユーザーの ID です。

d. または、コマンド・プロンプトで、次のコマンドを入力します。

```
pipeline -n pipelinename -l
```

ここで、*pipelinename* は、開始したばかりのパイプラインの名前です。 パイプラインがアクティブである場合、コマンド・プロンプトは `Running` を返します。

次のタスク

このパイプライン・コマンドは、パイプライン構成ファイル内の並行性パラメーターに等しい数のパイプライン処理スレッドを開始します。同時に処理されるレコードの数は、HTTP トランスポート・オプションに組み込まれている並行性パラメーターによって決まります。

Web サービスのテスト

提供されるテスト・クライアント wsutil.jar を使用して、IBM InfoSphere Identity Insight Web サービスのインストールと構成をテストできます。

始める前に

- Web サービスがインストールされている必要があります。
- 組み込み WebSphere Application Server が実行中であることを確認してください。
- アプリケーション・サーバーに Web サービス・パイプライン用のパイプライン構成ファイルが、少なくとも 1 つ構成されている必要があります。
- webservices.properties ファイルに正しいパイプライン URL 設定が構成されていることを確認してください。この Web サービス・パイプラインは稼働している必要があります。
- テストで使用するテスト UMF 入力文書を 1 つ以上作成します。

手順

1. 組み込み WebSphere Application Server 上で、wsutil.jar を含んでいるディレクトリーに移動します。 このファイルは、通常 *installation_root*`/ewas/webservice/wsutil.jar` にあります。
2. このディレクトリーのコマンド行から、実行する操作に応じた wsutil.jar コマンド構文を入力します。 `java -jar wsutil.jar --<SOAP method>=<URI> --input=<URL> --output=<URI>`

Web サービス load メソッドのテストの例

以下の wsutil.jar コマンドは、raw_entities.umf という名前の UMF ファイルからレコードをロードし、結果を results.umf という名前の UMF ファイルに保存します。

```
java -jar wsutil.jar --load=http://localhost:13510/easws/services/SRDWebService
 --input=raw_entities.umf --output=results.umf
```

srd.wsdl ファイル

IBM InfoSphere Identity Insight Web サービスと通信するためには、Web サービス・クライアントが必要です。IBM InfoSphere Identity Insight Web サービスをインストールすると、InfoSphere Identity Insight Web サービスとの通信に使用される SRDWebService のメソッドが含まれた srd.wsdl ファイルもインストールされます。srd.wsdl ファイルを使用して、IBM InfoSphere Identity Insight Web サービスで使用するための Web サービス・クライアントを作成できます。

srd.wsdl ファイルには、Web サービスをホストしている組み込み WebSphere Application Server にアクセスすることで、Web ブラウザーからアクセス可能です。通常、このファイルはアプリケーション・サーバー上の以下のルート URL で見つけることができます。

`http://`*`IBM_WebSphere_Application_Server_host`*`:`*`install_port`*`/easws/resources/wsdl/srd.wsdl`

以下に例を示します。

```
http://localhost:13510/easws/resources/wsdl/srd.wsdl
```

注: 必ずアプリケーション・サーバーが稼働していることを確認してから srd.wsdl ファイルにアクセスしてください。

また、Web サービスと SOAP ツールキットをサポートする、以下のような任意の開発プラットフォームを使用して Web サービスの WSDL クライアントを作成することもできます。

- Java と IBM WebSphere Application Server
- Java と Apache Axis
- Microsoft .NET
- Perl

WSDL ファイルを使用して Web サービス・クライアントを作成する方法については、開発プラットフォームの資料を参照してください。

srd.wsdl Web サービス・クライアント以外の Web サービス・クライアント WSDL を作成する場合、デプロイメント URL が正しい WSDL クライアントを指すようにしてください。

SRDWebService のメソッド

srd.wsdl ファイルには、IBM InfoSphere Identity Insight Web サービスと通信するのに使用される SRDWebService のメソッドが含まれています。
SRDWebService には、3 つのメソッドが含まれています。すなわち、エンティティ

ー・データベースにデータをロードするためのメソッド、検索を実行してエンティティー・データベースをクエリーするためのメソッド、および UMF を介して使用可能なパイプライン機能を処理するためのメソッドです。

loadRecord メソッド

```
LoadResult loadRecord(String umfEntity)
```

loadRecord() メソッドから返される LoadResult オブジェクトには、以下の 2 つのメンバーが含まれます。

メンバー	説明	タイプ
entityID	返されるエンティティーの ID	long
merged	エンティティーが、既存のエンティティーに解決されたか、新規エンティティーであったかを示すフラグ。	ブール

umfEntity パラメーターは、単一エンティティーのデータを表す、UMF 形式の XML ストリングです。UMF_ENTITY レコードを適切に構成する方法について、UMF 仕様を参照し、DSRC_ACCT および DSRC_REF に適切な値を定義してください。

load メソッドは、UMF_ENTITY 文書の処理を可能にしますが、メソッドからの結果として未加工の UMF 出力文書を返すことはしません。その代わりに、LoadResult オブジェクトを返します。このオブジェクトにはエンティティー ID と、そのエンティティーが新規エンティティーであったか、あるいは既存のエンティティーに解決されたかを示すフラグが含まれています。UMF 出力文書を構文解析することに支障がない場合は、load メソッドの代わりに process メソッドを使用できます。load メソッドを使用すると、ロード操作の結果として生成される UMF 出力文書を構文解析する処理を省くことができます。

basicQuery() メソッド

```
String basicQuery(String umfSearch)
```

basicQuery() メソッドに対する入力ストリングは UMF_SEARCH レコードの形式でなければなりません。basicQuery() から返される XML ストリングには、クエリーからの UMF_SEARCH_RESULT が含まれています。

組み込みクエリーには、要約 (結果セット) クエリーと詳細 (ドリルダウン) クエリーの 2 つのタイプがあります。

注**:** このメソッドは、後方互換性のためにのみ存在します。このリリースにおけるこのメソッドの機能は、process メソッドと同等です。新しいクライアント・アプリケーションではすべて、basicQuery() メソッドの代わりに process メソッドを使用してください。

process() メソッド

```
String process(String umfRequestDocument)
```

任意の UMF 入力文書を処理し、その結果として UMF 出力文書を受け取るには、process メソッドを使用します。process メソッドは、パイプラインでサポートされるすべての要求および応答を取り扱うように意図されており、すべての操作において最適な選択になるメソッドです。

このメソッドは、String パラメーターを受け取って、String で結果を返します。

wsutil.jar

wsutil.jar は、コマンド行ベースの Java アプリケーションであり、IBM InfoSphere Identity Insight Web サービスのインストール時に一緒にインストールされます。このサンプル・クライアントを使用して、各 Web サービス SOAP メソッドを試してみたり、Web サービスのインストールと構成をテストしたりできます。

wsutil.jar テスト・クライアントは、以下の場所にあります。

installation_root/ewas/webservice

wsutil.jar 使用法構文

wsutil.jar は、コマンド行ベースの Java アプリケーションであり、IBM InfoSphere Identity Insight Web サービスのインストールと構成をテストするためのテスト・クライアントとして提供されています。wsutil.jar を使用するには、wsutil.jar オペレーターと、対応する入力修飾子と出力修飾子を指定します。

wsutil.jar 使用法構文は、テストする Web サービス操作に基づきます。

wsutil (unix) または wsutil.bat (win) *--operator=URI --input=URI --output=URI*

help

wsutil.jar テスト・クライアントのオンライン・ヘルプおよびコマンド行情報を表示します。

wsutil (unix) または wsutil.bat (win) --help

load=*URI*

IBM InfoSphere Identity Insight Web サービス・インターフェースにパイプライン・スタイル UMF レコードと Uniform Resource Identifier (URI) を指定します。

wsutil (unix) または wsutil.bat (win) --load=*URI* [--xslt=*URI*][--*input=URI*][--*output=URI*]

この操作は、エンティティー解決処理のために、指定された URI から UMF レコードを Web サービス・パイプラインへロードします。処理が終わると、操作はエンティティー ID とともに、インバウンド・エンティティーが既存のエンティティーとマージされたか、あるいはインバウンド・エンティティーによって新しいエンティティーが作成されることになったかを示す標識を返します。

process=*URI*

IBM InfoSphere Identity Insight Web サービス・インターフェースに汎用 XML または UMF レコードと Uniform Resource Identifier (URI) を指定します。

wsutil (unix) または wsutil.bat (win) --process=*URI* [--xslt=*URI*][--*input=URI*][--*output=URI*]

任意の UMF 入力文書を処理し、その結果として UMF 出力文書を受け取る場合、この操作を使用します。process メソッドは、パイプラインでサポートされ

るすべての要求および応答を取り扱うように意図されています。通常、すべての操作において最適な選択になるメソッドです。

search=*URI*
IBM InfoSphere Identity Insight Web サービス・インターフェースにパイプライン検索スタイル UMF 要求および応答と Uniform Resource Identifier (URI) を指定します。

`wsutil (unix) または wsutil.bat (win) --score=URI [--xslt=URI][--input=URI][--output=URI]`

この操作では、特定のエンティティーに関してエンティティー・データベースに対する検索を実行し、そのエンティティーに関する要求された情報を返すか、または所定の属性に一致するエンティティーに関してエンティティー・データベースのクエリーを行い、クエリーに一致したエンティティーのリストを返すかのいずれかを実行できます。

xslt=*URI*
XSLT 変換と、操作が UMF レコードに変換する XML ファイルを指定します。

`wsutil (unix) または wsutil.bat (win) --xslt=URI][--input=URI][--output=URI]`

いずれかの Web サービス操作を使用する前に、この操作を使用して XML レコードを UMF に変換します。

wsutil.jar 修飾子

これらの修飾子を wsutil.jar オペレーターと組み合わせて使用して、Web サービス・コマンドの input メソッドと output メソッドを指定します。

input=*URI*
UMF レコードの input メソッドを指定します。デフォルトの input メソッドは、STDIN です。

output=*URI*
UMF レコードの output メソッドを指定します。デフォルトの output メソッドは、STDOUT です。このメソッドを使用して、UMF 出力をファイルに保存するときの場所とファイル名を指定できます。

wsutil.jar 使用例

以下の UNIX システム上での wsutil.jar コマンドは、ファイルからレコードをロードし、それらのレコードを UMF に変換し、結果をコマンド行インターフェースのコンソールに表示します。

```
wsutil --load=http://localhost:13510/easws/services/SRDWebService
--input=raw_entities.xml --xslt=transform.xsl
```

以下の Windows システム上での wsutil.jar コマンドは、STDIN から要求を獲得し、結果をコマンド行インターフェースのコンソールに表示します。

```
wsutil.bat --process=http://localhost:13510/SRDWebService
```

エンティティー・データベースに対するクエリーの作成

IBM InfoSphere Identity Insight では、いくつかの方法でエンティティー・データベースをクエリーできます。Web サービス・パイプライン検索を作成して、エンティティー・データベースを検索して特定の属性検索基準に一致するエンティティーを見つけることができます。また、Web サービス・パイプライン検索を作成して、特定のエンティティーに関してデータベースをクエリーすることもできます。

Web サービス・パイプライン検索

パイプラインへの組み込みは、動的な検索およびクエリーのインターフェースであり、Web サービスがエンティティー・データベースをクエリーする際の統合アクセス・ポイントとなります。ユーザーは UMF 入力文書を使用して要求を構成し、その後、Web サービスを介して処理のために UMF 入力文書をパイプラインに送信します。パイプラインは、処理が終わると、結果が入った UMF 出力文書を返します。

Web サービス・パイプライン検索では、2 種類の質問に対する答えが提供されます。

エンティティー・データベース内のどのエンティティーが特定の属性または属性セットに一致しているか**? (UMF_SEARCH)**

このタイプの Web サービス・パイプライン検索は、エンティティー解決をフルに活用して、入力検索基準を認識および標準化し、その後、検索基準をデータベース内のエンティティーに突き合わせます。これは要約クエリーまたは結果セット・クエリーと呼ばれ、要求された属性値または属性値のリストに一致するデータ値を持つエンティティーのリストを返します。

要約クエリーまたは結果セット・クエリーを実行するには、エンティティー解決を実行するためにパイプラインが使用する検索基準を含んだ UMF_SEARCH 入力文書を作成します。パイプラインは、クエリー結果が入った UMF_SEARCH_RESULT 出力文書を返すことで応答します。クエリー結果は、検索基準に一致したエンティティーのリストです。

特定のエンティティーに関してエンティティー・データベースが把握していることは何か**? (UMF_QUERY)**

このタイプの Web サービス・パイプライン検索は、SQL ステートメントとパラメーターを使用してエンティティー・データベースのクエリーを行います。これは詳細クエリーまたはドリルダウン・クエリーと呼ばれ、単一エンティティーに関する詳しい情報のリストを返します。

詳細クエリーまたはドリルダウン・クエリーを実行するには、エンティティー・データベース内のどのエンティティーに関する情報が必要かを指示した UMF_QUERY 入力文書を作成します。パイプラインは、要求されたエンティティーに関する詳細が入った UMF_QUERY_RESULT 出力文書を返すことで応答します。

Web サービス・パイプライン検索の実行時、パイプラインは、ロギングを含め、すべての標準のパイプライン機能を実行します。

Web サービス・パイプライン検索の入力 (要求) と出力 (応答) は、いずれも UMF 文書を使用し、情報を UMF で構造化します。

Web サービス・パイプライン検索フォーマット

製品には、各 Web サービス・パイプライン検索用の組み込みフォーマットが付属しています。

UMF_SEARCH フォーマット

WS_SUMMARY_TOP10
データベース内のエンティティーから、検索基準で指定された属性データに最も近い上位 10 件のリストを返します。

WS_SUMMARY_TOP100
データベース内のエンティティーから、検索基準で指定された属性データに最も近い上位 100 件のリストを返します。

WS_SUMMARY
データベース内のエンティティーから、検索基準で指定された属性データに一致したすべてのエンティティーのリストを返します。

UMF_QUERY フォーマット

WS_DETAIL
要求されたエンティティー ID について、エンティティー・データベースからすべてのデータを返します。

WS_RELATION
エンティティー・データベース内のエンティティーから、入力エンティティーに次数 1 で関連しているすべてのエンティティーのリストを返します。

WS_ALERT
エンティティー・データベース内のアラートから、入力エンティティー ID に関連しているすべてのアラートのリストを返します。

ユーザーは、適切な UMF 入力文書内で FORMAT_CODE タグを使用して、どの組み込みフォーマットを使用するかを指示します。

パフォーマンスに関する考慮事項

一般的に、Web サービス・パイプライン検索要求に含まれる検索基準が増えるほど、システムが比較対象とするデータベース内のエンティティーの数は減ることになります。これはすなわち、システムが結果を返す速さも、検索基準が少ない要求よりも速くなることを意味します。

特定のエンティティーを検索する Web サービス・クエリーの作成

ここに記載されている手順に従って、エンティティー・データベース内で特定のエンティティーを検索する UMF_QUERY 入力文書を作成します。UMF_QUERY 入力文書は、Web サービス経由で処理のために Web サービス・パイプラインに送信されます。パイプラインがクエリーを処理した後、Web サービスによって、要求された入力エンティティーに関する詳細を含んだ UMF_QUERY_RESULT 出力文書が返されます。

始める前に

UMF_QUERY 入力文書を受け取り、処理するために、組み込み WebSphere Application Server が稼働している必要があるほか、少なくとも 1 つの Web サービス・パイプラインが開始済みで、稼働している必要があります。

このタスクについて

検索要求は UMF 入力文書であるため、基準は有効な UMF タグを使用してフォーマット設定されている必要があります。任意のテキスト・エディターまたは UMF を作成するユーティリティーを使用できます。

手順

1. 新規 UMF_QUERY 入力文書を作成します。
2. ROOT セグメントで、必須の UMF タグと値を入力します。
   a. DSRC_CODE タグにデータ・ソース・コードを入力します。Web サービス・パイプライン検索のデフォルトのデータ・ソース・コードは、1589 です。 Web サービス・パイプライン検索のデフォルトのデータ・ソース・コード以外のデータ・ソース・コードを使用する場合、そのコードがエンティティーを解決する目的で構成されていないことを確認してください。
   b. DSRC_REF タグに、要求側メッセージ・トランザクションを指すデータ・ソース参照コードを入力します。 データ・ソース参照コードは呼び出し側アプリケーションに返されるため、分かりやすいコードにしてください。
   c. FORMAT_CODE タグを使用して、結果の出力フォーマットを示すフォーマット・コードを入力します。 パイプラインには、UMF_QUERY を使用する Web サービス・パイプライン検索用の 3 つの組み込みフォーマット・コードが付属しています。
      - WS_DETAIL - 入力エンティティー ID に関して入手可能なすべてのエンティティー・データを返します。
      - WS_RELATION - 入力エンティティー ID に 1 次の関係で関連しているすべてのエンティティーのリストを返します。
      - WS_ALERT クエリー - 入力エンティティー ID に関連がある、システム内のすべてのロール・アラートを返します。

      他のフォーマット・コードを使用する場合、そのフォーマット・コードは UMF_OUTPUT_FORMAT 表内に構成されていなければなりません。
   d. ENTITY_ID タグに、情報を返す必要があるエンティティーのエンティティー ID を入力します。
3. その他のクエリー基準がある場合、その他のオプションの UMF セグメントである <NAME>、<ADDRESS>、<EMAIL>、<ATTRIBUTE>、および <NUMBER> を使用して入力します。
4. UMF_QUERY 入力文書を Web サービス・パイプラインに送信します。

タスクの結果

Web サービス・パイプラインは、UMF_QUERY 文書を取り込み、指定された基準を使用してクエリーに一致するエンティティーをデータベース内で検索します。パイプラインはその後クエリーを処理し、通常のログ・ファイルを作成し、呼び出し

側アプリケーションに対して、Web サービス経由で結果を UMF_QUERY_RESULT 出力文書で返します。

サンプル UMF_QUERY 検索

このサンプル UMF_QUERY は、エンティティー ID 1223 に関するすべての情報を検索します。

注: この例は、見やすいようにフォーマットされており、本来必要な UMF レコード 1 件につき 1 行のフォーマットには従っていません。

```
<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 入力文書

UMF_QUERY 入力文書には、エンティティー・データベースのクエリーを行い、特定のエンティティーに関する情報を見つけ、その情報を呼び出し側アプリケーションに返すための入力データを構造化する UMF セグメントの集合が含まれています。そこには、Web サービス・パイプライン・クエリーの要求と検索基準が含まれています。

UMF_QUERY 入力文書内の情報は、SQL ステートメントに基づいています。この Web サービス・パイプライン検索の結果は、UMF_QUERY_RESULT 出力文書として呼び出し側アプリケーションに返されます。UMF_QUERY は、「拡張クエリー / 属性による検索」クエリーを実行します。

下記の必須 UMF エレメントとセグメントによって UMF_QUERY 入力文書は構成されます。

DSRC_CODE

データ・ソース・コード UMF タグ。このタグによって呼び出し側アプリケーションを参照し、識別するため、これは必須です。通常のパイプライン・ロギングの一環として、処理された UMF_QUERY ごとに、このデータ・ソース・コードが UMF_LOG 表内に記録されます。

システムには、すべての Web サービス・パイプライン検索に対して使用できるデータ・ソース・コード 1589 があらかじめ構成されています。このデータ・ソース・コードは、入力検索基準をエンティティー・データベース内で検索に一致するエンティティーに解決することなく、エンティティー解決処理を実行します。ユーザーは、特定の呼び出し側アプリケーションに対応する独自のデータ・ソース・コードを作成できます。ただし、その際は、データ・ソース・コードがエンティティー解決を行わないように設定してください。

DSRC_REF

データ・ソース参照 UMF タグ。このタグは要求側メッセージ・トランザクションを参照し、呼び出し側アプリケーションに返されるため、必須です。

FORMAT_CODE

UMF_OUTPUT_FORMAT 表内に指定されている UMF 出力文書フォーマットに相関している UMF タグ。IBM InfoSphere Identity Insight には、UMF_QUERY を使用する Web サービス・パイプライン検索用の 3 つの組み込みフォーマット・コードが付属しています。

- WS_DETAIL - 要求されたエンティティー ID に関して入手可能なすべてのエンティティー・データを返します。
- WS_RELATION - 入力エンティティーに次数 1 で関連しているすべてのエンティティーのリストを返します。
- WS_ALERT クエリー - 入力エンティティー ID に関連がある、システム内のすべてのアラートを返します。

この入力文書を介して開始される EQ (拡張クエリー / 属性による検索) のために、以下の FORMAT_CODE が指定されている必要があります。

ENHANCED_QUERY_RESULT の例を以下に示します。

```
<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

この必須 UMF タグで、検索対象のエンティティーのエンティティー ID を指定します。システムは、その他のクエリー基準に基づいて、エンティティー・データベースに含まれるこのエンティティーに関する既知のデータの詳細が入った応答を返します。

次に、使用可能なその他の UMF セグメントとそれぞれの有効なタグを使用して、名前、住所、番号、特性、および E メール・アドレスに関するオプションの検索基準を指定します。

NAME

エンティティー・モデルと入力アイデンティティーによって定義される、個人、組織、場所、またはアイテムの名前を定義する名前属性のクエリーを行います。

NUMBER

一般に番号で示されるデータ (クレジット・カード番号、電話番号、パスポート番号など) で構成される番号属性のクエリーを行います。

ADDRESS

アイデンティティーの場所を定義し、標準的な住所情報 (街区名や番地、ユニット番号や建物番号、市区町村、都道府県、国、郵便番号) を一般的に含んでいる住所属性のクエリーを行います。

ATTRIBUTE

他の種類の属性では表現されない、その他のアイデンティティーの特質や情報を定義する特性属性のクエリーを行います。

EMAIL

インターネット E メール・アドレスを定義する E メール属性のクエリーを行います。

サンプル UMF_QUERY 検索

このサンプル UMF_QUERY は、WS_DETAIL フォーマット・コードを使用してエンティティー・データベースのクエリーを行い、エンティティー ID 1223 に関するすべての既知の情報を返します。

注**:** この例は、見やすいようにフォーマットされており、本来必要な UMF レコード 1 件につき 1 行のフォーマットには従っていません。

```
<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>
```

WS_DETAIL フォーマット・コード**:**

エンティティー・データベース内の特定のエンティティーに関する詳細を返す Web サービス・パイプライン検索を作成するときは、組み込みフォーマット・コード WS_DETAIL を使用します。このフォーマット・コードを、クエリー基準を含んだ UMF_QUERY 入力文書内に指定します。

WS_DETAIL フォーマット・コードを使用した **Web** サービス・パイプライン検索の例

このサンプル Web サービス・パイプライン検索は、エンティティー・データベース内に含まれる、エンティティー ID 87 (Joe Franklin) に関するすべての情報を返します。

注**:** この例は、見やすいようにフォーマットされており、本来必要な UMF レコード 1 件につき 1 行のフォーマットには従っていません。

エンティティー ID 87 (Joe Franklin) の詳細を要求するには、要求と新しい UMF_QUERY 入力文書を作成します。

```
<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>
```

この UMF_QUERY 文書を Web サービス・パイプラインによる処理のために Web サービスを介して送信すると、呼び出し側アプリケーションは、以下の UMF_QUERY_RESULT 文書を応答で受け取ります。

```
<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>
```

この応答から、Joe Franklin に関する情報があるデータ・ソースが 3 つ存在することがわかります。それらは、OFAC リスト、FBI リスト、および A9 リストです。Joe は 2 つの異なる住所を使用していますが、いずれのケースでも、同じ電話番号とクレジット・カードを使用しています。

WS_ALERT フォーマット・コード**:**

特定のエンティティーに関与しているエンティティー・データベース内のすべてのロール・アラートを返す Web サービス・パイプライン検索を作成するときは、組み込みフォーマット・コード WS_ALERT を使用します。このフォーマット・コードを、クエリー基準を含んだ UMF_QUERY 入力文書内に指定します。

WS_ALERT フォーマット・コードを使用した **Web** サービス・パイプライン検索の例

このサンプル Web サービス・パイプライン検索は、エンティティー ID 87 (Joe Franklin) が関与しているすべてのロール・アラートのリストを返します。

注**:** この例は、見やすいようにフォーマットされており、本来必要な UMF レコード 1 件につき 1 行のフォーマットには従っていません。

エンティティー ID 87 (Joe Franklin) に関するロール・アラートを要求するには、要求と新しい UMF_QUERY 入力文書を作成します。

```
<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>
```

この UMF_QUERY 文書を Web サービス・パイプラインによる処理のために Web サービスを介して送信すると、呼び出し側アプリケーションは、以下の UMF_QUERY_RESULT 文書を応答で受け取ります。

```
<UMF_QUERY_RESULT>
  <ALERT>
  <CONFLICT_ID>2</CONFLICT_ID>
  <CONFLICT_RULES_DESC>Bad Guy Knows Employee</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>Bad Guy Knows Vendor</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>
```

この応答から、Joe Franklin に関するロール・アラートが 2 つ存在することがわかります。それらは、「従業員 Susan Miller は Joe を知っている」というアラートと、「ベンダー Julio Martinez は Joe を知っている」というアラートです。

WS_RELATION フォーマット・コード**:**

特定のエンティティーに次数 1 で関連しているすべてのエンティティーのリストを返す Web サービス・パイプライン検索を作成するときは、組み込みフォーマット・コード WS_RELATION を使用します。このフォーマット・コードを、クエリー基準を含んだ UMF_QUERY 入力文書内に指定します。

WS_RELATION フォーマット・コードを使用した **Web** サービス・パイプライン検索の例

このサンプル Web サービス・パイプライン検索は、エンティティー ID 87 (Joe Franklin) に次数 1 で関連しているすべてのエンティティーのリストを返します。

注**:** この例は、見やすいようにフォーマットされており、本来必要な UMF レコード 1 件につき 1 行のフォーマットには従っていません。

```
<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>
```

この UMF_QUERY 文書を Web サービス・パイプラインによる処理のために Web サービスを介して送信すると、呼び出し側アプリケーションは、以下の UMF_QUERY_RESULT 文書を応答で受け取ります。

```
<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>
```

類似した属性を持つエンティティーを検索する Web サービス・クエリーの作成

ここに記載されている手順に従って、検索基準で指定された属性のデータ値に一致するエンティティーをエンティティー・データベース内で検索する UMF_SEARCH 入力文書を作成します。UMF_SEARCH 入力文書は、Web サービス経由で処理のために Web サービス・パイプラインに送信されます。パイプラインがクエリーを処理した後、Web サービスによって、検索基準に一致したエンティティーのリストを含んだ UMF_SEARCH_RESULTS 出力文書が返されます。

始める前に

UMF_SEARCH 入力文書を受け取り、処理するために、組み込み WebSphere Application Server が稼働している必要があるほか、少なくとも 1 つの Web サービス・パイプラインが開始済みで、稼働している必要があります。

このタスクについて

検索要求は UMF 入力文書であるため、基準は有効な UMF タグを使用してフォーマット設定されている必要があります。任意のテキスト・エディターまたは UMF を作成するユーティリティーを使用できます。

手順

1. 新規 UMF_SEARCH 入力文書を作成します。
2. ROOT セグメントで、必須の UMF タグと値を入力するとともに、検索基準を指定するために使用する必要があるオプションの UMF タグと値を入力します。最低でも、以下の UMF タグの値は入力してください。
   a. DSRC_CODE タグにデータ・ソース・コードを入力します。Web サービス・パイプライン検索のデフォルトのデータ・ソース・コードは、1589 です。 Web サービス・パイプライン検索のデフォルトのデータ・ソース・コード以外のデータ・ソース・コードを使用する場合、そのコードがエンティティーを解決する目的で構成されていないことを確認してください。
   b. DSRC_REF タグに、要求側メッセージ・トランザクションを指すデータ・ソース参照コードを入力します。 データ・ソース参照コードは呼び出し側アプリケーションに返されるため、分かりやすいコードにしてください。

c. FORMAT_CODE タグを使用して、結果の出力フォーマットを示すフォーマット・コードを入力します。 パイプラインには、UMF_SEARCH を使用する Web サービス・パイプライン検索用の 3 つの組み込みフォーマット・コードが付属しています。

- WS_SUMMARY_TOP10 - 検索基準に一致する上位 10 件のエンティティーを返します。
- WS_SUMMARY_TOP100 - 検索基準に一致する上位 100 件のエンティティーを返します。
- WS_SUMMARY クエリー - 検索基準に一致するすべてのエンティティーを返します。

他のフォーマット・コードを使用する場合、そのフォーマット・コードは UMF_OUTPUT_FORMAT 表内に構成されていなければなりません。

d. MIN_LIKE_SCORE タグに最小解決スコアを入力して、検索基準に含まれる属性値と、それと同じ属性を含んでいるエンティティー・データベース内のエンティティーを一致と見なすための最小数値スコアを設定します。 スコアが高くなるほど、より正確な一致が要求されます。100 というスコアは完全一致を表します。

3. その他の有効な UMF 入力文書セグメントを使用して、検索基準を構成する属性のデータ値を入力します。 これらの値は Web サービス・パイプライン検索が探す属性であり、Web サービス・パイプライン検索は、それらに一致する値を持つエンティティーまたは類似した値を持つエンティティーのリストを作成します。一致の程度は MIN_LIKE_SCORE の値によって変わります。
4. UMF_SEARCH 入力文書を Web サービス経由で送信します。

タスクの結果

Web サービス・パイプラインは、エンティティー解決処理を使用して UMF_SEARCH 文書を取り込み、指定された基準を使用してデータベース内のエンティティーを検索します。パイプラインはその後クエリーを処理し、通常のログ・ファイルを作成し、選択されたフォーマットを使用して、呼び出し側アプリケーションに対し Web サービス経由で結果を UMF_SEARCH_RESULTS 文書で返します。

サンプル UMF_SEARCH 文書クエリー

このサンプル UMF_SEARCH 入力文書は、WS_SUMMARY_TOP10 フォーマット・コードを使用してエンティティー・データベースのクエリーを行い、社会保障番号のデータ値が 555-09-8761 と正確に一致する社会保障番号を含んでいる上位 10 件のエンティティーを探します。

注: この例は、見やすいようにフォーマットされており、本来必要な UMF レコード 1 件につき 1 行のフォーマットには従っていません。

```
<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 入力文書

UMF_SEARCH 入力文書には、Web サービス・パイプライン検索の要求と検索基準が含まれています。そこには、検索基準に一致する属性値を含んでいるエンティティーをエンティティー・データベースで検索し、それらのエンティティーのリストを呼び出し側アプリケーションに返すための入力データを構造化する UMF セグメントの集合が含まれています。この Web サービス・パイプライン検索の結果は、UMF_SEARCH_RESULT 出力文書として呼び出し側アプリケーションに返されます。UMF_SEARCH では、「解決による検索 (Find By Resolution)」プロセスがフルに実行されます。

下記の必須 UMF エレメントとセグメントによって UMF_SEARCH 入力文書は構成されます。

DSRC_CODE

データ・ソース・コード UMF タグ。このタグによって呼び出し側アプリケーションを参照し、識別するため、これは必須です。通常のパイプライン・ロギングの一環として、処理された UMF_SEARCH ごとに、このデータ・ソース・コードが UMF_LOG 表内に記録されます。

システムには、すべての Web サービス・パイプライン検索に対して使用できるデータ・ソース・コード 1589 があらかじめ構成されています。このデータ・ソース・コードは、入力検索基準をエンティティー・データベース内で検索に一致するエンティティーに解決することなく、エンティティー解決処理を実行します。ユーザーは、特定の呼び出し側アプリケーションに対応する独自のデータ・ソース・コードを作成できます。ただし、その際は、データ・ソース・コードがエンティティー解決を行わないように設定してください。

DSRC_REF

データ・ソース参照 UMF タグ。このタグは要求側メッセージ・トランザクションを参照し、呼び出し側アプリケーションに返されるため、必須です。

SRC_CREATE_DT

ソース作成日 UMF タグ。このタグはオプションです。このタグに値が含まれている場合、その値はロギングに使用されます。

SRC_LSTUPD_DT

ソース最終更新日 UMF タグ。このタグはオプションです。このタグに値が含まれている場合、その値はロギングに使用されます。

SRC_LSTUP_US

ソース最終更新ユーザー UMF タグ。このタグはオプションです。このタグに値が含まれている場合、その値はロギングに使用されます。

MIN_LIKE_SCORE

最小解決スコア (または相似スコア) UMF タグ。このタグは、指定されているその他の UMF セグメントおよびタグの最小マッチング値を設定するため、必須です。この数値スコアによって、要求された属性値と、エンティ

ティー・データベース内にあるそれと同じ属性を含んでいるエンティティーを一致と見なすかどうかが判断されます。スコアが高くなるほど、より正確な一致が要求されます。100 というスコアは完全一致を表します。

例えば、特定の社会保障番号が関係するすべてのエンティティーを見つける検索の場合、データベース内のエンティティーの社会保障番号がクエリーで指定された社会保障データ値にどれくらい正確に一致していれば、そのエンティティーをこのクエリーの結果セットの一部としてリストに含めるかを MIN_LIKE_SCORE で決定します。

FORMAT_CODE

UMF_FORMAT_CODE 表内に指定されている UMF 出力文書フォーマットに相関している UMF タグ。IBM InfoSphere Identity Insight には、UMF_SEARCH を使用する Web サービス・パイプライン検索用の 3 つの組み込みフォーマット・コードが付属しています。

- WS_SUMMARY_TOP10 - 検索基準に一致する上位 10 件のエンティティーを返します。
- WS_SUMMARY_TOP100 - 検索基準に一致する上位 100 件のエンティティーを返します。
- WS_SUMMARY クエリー - 検索基準に一致するすべてのエンティティーを返します。

これらのクエリー間の違いは、クエリー名が示すとおり、返されるレコードの数のみです。

次に、使用可能なその他の UMF セグメントとそれぞれの有効なタグを使用して、名前、住所、番号、特性、および E メール・アドレスに関するオプションの検索基準を指定します。

NAME

エンティティー・モデルと入力アイデンティティーによって定義される、個人、組織、場所、またはアイテムの名前を定義する名前属性を検索します。

NUMBER

一般に番号で示されるデータ (クレジット・カード番号、電話番号、パスポート番号など) で構成される番号属性を検索します。

ADDRESS

アイデンティティーの場所を定義し、標準的な住所情報 (街区名や番地、ユニット番号や建物番号、市区町村、都道府県、国、郵便番号) を一般的に含んでいる住所属性を検索します。

ATTRIBUTE

他の種類の属性では表現されない、その他のアイデンティティーの特質や情報を定義する特性属性を検索します。

EMAIL

インターネット E メール・アドレスを定義する E メール属性を検索します。

サンプル UMF_SEARCH クエリー

このサンプル UMF_SEARCH クエリーは、エンティティー・データベース内で社会保障番号 555-09-8761 に完全一致する社会保障番号を持つ上位 5 件のエンティティーを返します。それを超える数のエンティティーが検出された場合でも、リストで返されるエンティティーは上位 5 件のみです。

注**:** この例は、見やすいようにフォーマットされており、本来必要な UMF レコード 1 件につき 1 行のフォーマットには従っていません。

```
<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>
```

WS_SUMMARY フォーマット・コード**:**

IBM InfoSphere Identity Insight には、UMF_SUMMARY 入力文書で使用するための、事前作成された 3 つのフォーマット・コード、すなわち WS_SUMMARY、WS_SUMMARY_TOP10、および WS_SUMMARY_TOP100 が付属しています。これらのフォーマット・コードは、UMF_SUMMARY 入力文書で指定された条件に一致するエンティティーのリストを返します。これらのフォーマット・コード間の違いは、フォーマット・コード名が示すとおり、返されるレコードの最大数のみです。

WS_SUMMARY_TOP10 フォーマット・コードを使用した **Web** サービス・パイプライン検索の例

このサンプル Web サービス・パイプライン検索は、エンティティー・データベース内のエンティティーから、以下の検索基準に最も近い上位 10 件を返します。

- 名前: Joe Franklin
- 電話番号: 415-555-3325
- 生年月日: 1956 年 1 月 2 日

これは UMF_SEARCH 入力文書を使用してこの条件を指定するとともに、WS_SUMMARY_TOP10 フォーマット・コードも指定します。

注**:** この例は、見やすいようにフォーマットされており、本来必要な UMF レコード 1 件につき 1 行のフォーマットには従っていません。

```
<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>
```

この UMF_SEARCH 文書を Web サービス・パイプラインによる処理のために Web サービスを介して送信すると、呼び出し側アプリケーションは、以下の UMF_SEARCH_RESULT 文書を応答で受け取ります。

```
<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>
```

このケースの場合、エンティティー・データベース内で検索基準に一致し、最小相似スコア 80 に該当するエンティティーは 3 件のみでした。

第 10 章 トラブルシューティングとサポート

このセクションでは、IBM InfoSphere Identity Insight ソフトウェアに関する問題のトラブルシューティング方法 (知識ベースの検索、フィックスのダウンロード、およびサポートへの連絡方法など) について説明します。

トラブルシューティングの概要

トラブルシューティングは、問題解決のための体系的手法です。その目的は、予期したとおりに動作しなかった理由を判別し、その問題の解決策を決定することです。

トラブルシューティング作業での最初のステップは、当該の問題を詳しく記述することです。問題の説明がない場合は、IBM もお客様ご自身も、問題の原因究明をどこから始めればよいかがわかりません。このステップには、以下のような基本的な質問が含まれます。

- 問題の症状はどのようなものか?
- どこで問題が発生するか?
- いつ問題が発生するか?
- どのような条件下で問題が発生するか?
- 問題を再現できるか?

通常は、これらの質問に答えることで問題を適切に記述できます。問題解決を始めるには、これが最適な方法です。

問題の症状はどのようなものか?

問題を記述し始める際にまず考えられる質問は「何が問題か」というものです。これは簡単な質問のように見えますが、さらに焦点を絞ってこの質問をいくつかの質問に分解すると、問題点をより明確にすることができます。例えば次のような質問が考えられます。

- 誰が、あるいは、何が問題を報告しているか?
- エラー・コードおよびメッセージはどのようなものか?
- システムでどのような障害が発生するのか? 例えば、ループ、ハング、異常終了、パフォーマンス低下、結果の誤りなど。
- その問題が業務に与える影響はどのようなものか?

どこで問題が発生するか?

問題の発生箇所の判別は必ずしも容易ではありませんが、問題の解決において最も重要なステップの 1 つです。報告を行うコンポーネントと障害が発生したコンポーネントの間には、多数のテクノロジー層が存在する場合があります。ネットワーク、ディスク、ドライバーなどは、問題を調査するときに考慮すべきコンポーネントのほんの数例です。

以下の質問は、問題がある層を切り分けるために、問題の発生箇所に焦点を絞る場合に役立ちます。

- 1 つのプラットフォームまたはオペレーティング・システムに固有の問題か?
- 複数のサーバーに共通の問題か?
- 現行の環境および構成はサポートされているか?

ある層で問題が報告されても、その層で問題が発生しているとは限りません。問題の発生場所を特定するには、その問題が存在する環境を理解することも必要です。ある程度時間をかけて、問題となっている環境を完全に記述してください。これには、オペレーティング・システムとそのバージョン、対応するすべてのソフトウェアとそのバージョン、ハードウェア情報などが含まれます。実行している環境が、サポートされている構成であることを確認してください。多くの場合、問題の原因をたどると、同時に実行することが想定されていない、または同時に作動させた状態で十分にテストされていない、非互換レベルのソフトウェアによるものであることがわかります。

いつ問題が発生するか?

障害に至るまでのイベントをタイムラインで詳細に記述します。特に発生が一回限りである場合にはこれが必要です。これを行う最も容易な方法は、さかのぼりながら作業することです。エラーが報告された時間 (ミリ秒まで、できるだけ正確に) から開始し、使用可能なログおよび情報を使用してさかのぼっていきます。通常、調べる必要があるのは、診断ログで見つかった最初の疑わしいイベントまでです。ただし、この作業は必ずしも簡単ではなく、練習が必要です。複数のテクノロジーの層が関係しており、それぞれに独自の診断情報がある場合には、どこまで調べて止めるかという判断が特に難しくなります。

イベントの詳細なタイムラインを作成するには、以下の質問に答えてみてください。

- 日中または夜間の特定の時刻にのみ問題が発生するか?
- 問題はどのくらいの頻度で発生するか?
- 問題が報告された時刻までにイベントがどのような順序で発生したか?
- 環境の変更 (ソフトウェアまたはハードウェアのアップグレードまたはインストールなど) の後に問題が発生したか?

このような問題に答えることによって、問題を調査するための基準となる枠組みが得られます。

どのような条件下で問題が発生するか?

問題が発生したときに、他にどのようなシステムおよびアプリケーションが実行されていたかを知ることは、トラブルシューティングにおいて重要なことです。環境に関する以下のような質問は、問題の根本原因の識別に役立ちます。

- その問題は、常に同じタスクの実行中に発生するか?
- 問題が表面化するには、特定の順序でイベントが発生する必要があるか?
- 同時に他のアプリケーションにも障害が発生するか?

この種の質問に答えることは、問題が発生する環境について説明し、依存関係の相関付けをする上で役立ちます。ほぼ同時に複数の問題が発生したからといって、それらの問題に関連があるとは限りません。

問題を再現できるか?

トラブルシューティングの観点からいうと、「理想的な」問題は、再現できる問題です。通常、再現できる問題の場合、調査のために自由に使用できるツールや手順の数が多くなります。そのため多くの場合、再現可能な問題の方が、デバッグおよび解決が容易です。ただし、再現可能な問題にも不便な点があります。問題が業務に重大な影響を与える場合は、問題を再発させることは避けるべきでしょう。可能であればテスト環境または開発環境で問題を再現します。そうすれば通常、調査時の柔軟性が高まり、制御もしやすくなります。

- テスト・マシンで問題を再現できますか?
- 複数のユーザーまたは複数のアプリケーションで同じタイプの問題が発生していますか?
- 問題は、単一のコマンド、一連のコマンド、特定のアプリケーション、またはスタンドアロン・アプリケーションを実行することにより再現できますか?

IBM InfoSphere Identity Insight のトラブルシューティング

以下の質問を使用すると、IBM InfoSphere Identity Insight で発生する問題に対する解決策を特定したり見つけたりする際に役立ちます。

1. インストール時に、1 つ以上のコンポーネントが正常にインストールされなかったことを示す通知がインストール・プログラムから出されましたか? そうであれば、インストール・ログ・ファイルを確認して、問題を判別し、修正してください。
2. サービス更新は最新レベルですか?
3. エラー・メッセージが出ていますか?
4. コンポーネントのログ・ファイルに問題に関するメッセージが含まれているかどうかを確認しましたか?
5. 以下のいずれかのコンポーネントの使用中に問題が発生しますか?
   - Analyst ツールキット Web アプリケーション - 429 ページの『Analyst ツールキット Web アプリケーションのトラブルシューティング・チェックリスト』を確認してください。
   - パイプライン - パイプラインのトラブルシューティング・チェックリストを確認してください
6. 問題を解決する可能性のある情報について製品の知識ベースを確認しましたか?
7. 適用できるこれらのオプションをそれぞれ試してもまだ問題が解決しない場合は、IBM ソフトウェア・サポートにお問い合わせください。

パイプラインのトラブルシューティング・チェックリスト

パイプラインで問題が生じた場合は、IBM ソフトウェア・サポートに連絡する前にこのリストを確認してください。このリストには、パイプラインで検出される最も一般的な問題が示されています。

1. パイプラインが「ダウン」状況を報告する、または何の状況も報告しない

2. パイプラインがシャットダウンする
3. 構成変更コンソールで行った構成変更がパイプラインに適用されない
4. パイプラインが AIX で開始されない
5. パイプラインが入力レコードの一部しか処理しない
6. トランスポートが機能しない
7. パイプラインが浮動小数点数をロードしない
8. パイプラインを開始すると、ルートが定義されていないことを示す警告メッセージを受け取る

1. パイプラインが「ダウン」状況を報告する、または何の状況も報告しない
   - パイプライン・ノードにエラーがあったり、パイプライン・ノードが実行されていなかったりすることはありませんか?
   - pipeline コマンドに指定したトランスポートで正しい構文を使用しましたか?
   - パイプラインがシャットダウンしましたか?
2. パイプラインがシャットダウンまたは異常終了する
   - 入力データ・ファイルの処理中にパイプラインで検出されたエラーが多すぎませんでしたか?
     - ログ・ファイルでエラーの詳細を確認してください。その情報を使用して問題を解決してください。
     - パイプライン構成ファイル内の *ErrorLimit* 設定を確認してください。この数値を増やすことが必要な場合があります。
   - パイプラインでメモリー・リソースの不足が発生しましたか?
   - データベースで以下のいずれかの理由により問題が発生していますか?
     - ディスク・スペースが不十分か?
     - パイプラインへの接続が失われたか?
     - このデータベースのユーザー名およびパスワードを変更したか?
3. 構成変更コンソールで行った構成変更がパイプラインに適用されない
   - 構成変更を適用する前に、パイプラインを停止してから再始動する必要があります。パイプラインの再始動時に、パイプライン初期化処理の一部として、構成変更が適用されます。
   - データ保全性を確保するため、構成変更の後で、実行中のすべてのパイプラインを停止してから再始動してください。
4. パイプラインが **AIX** で開始されない
   - 「依存モジュール libicuio.a が見つかりません (dependent module libicuio.a could not be found)」というエラー・メッセージを受け取りましたか?
     - 受け取った場合は、ディレクトリー `/usr/lib`、`/lib`、`$DB2INSTHOM/sqllib/lib` のいずれかにこのライブラリーがあるか確認してください。または、`LIBPATH` 環境変数を設定して、製品の *`installation_home`*`/lib` ディレクトリーを組み込んでください。
   - C++ ランタイム・ライブラリーのバージョンと場所を確認してください。`RunTime Update` 環境および `LIBPATH` 環境の設定に誤りがある結果として、この問題が発生した可能性があります。最新のサポート情報については、

「IBM InfoSphere Identity Insight インストールおよび構成ガイド (IBM InfoSphere Identity Insight Installation and Configuration Guide)」を参照してください。

5. パイプラインが入力レコードの一部しか処理せず、レコード全体を処理しない
   - *.BAD ログ・ファイルで無効な UMF メッセージがないか調べます。このログ・ファイルには、処理していた入力データ・ソース・ファイルの名前が示されています。
   - 構成コンソールの「**UMF 例外 (UMF Exceptions)**」タブを調べます。
6. パイプライン・トランスポートが機能しない
   - トランスポートに使用する構文が正しいことを確認してください。例えば、データベース・トランスポートを指定している場合、適切な場所に引用符を含めましたか?
   - トランスポートがキュー・トランスポートである場合、メッセージ・キューが存在していますか?
   - トランスポートがファイルである場合、そのファイルが存在していますか? トランスポートで指定したディレクトリーにそのファイルがありますか?
7. パイプラインが浮動小数点数をロードしない
   - これは、既知のパイプラインの制限です。UMF 内の浮動小数点数を訂正して指数を展開し、数値が標準的な数値表記になるようにしてください。例えば、`-1.267E-05` を展開すると、`-0.00001267` になります。
8. パイプラインを開始すると、ルートが定義されていないことを示す警告メッセージを受け取る
   - これは単なる警告の通知メッセージです。これは無視して構いません。(このメッセージは、このパイプラインにルートが定義されていないことを通知するだけのものです。パイプラインの実行にルートは必要ではありません。)

Analyst ツールキット Web アプリケーションのトラブルシューティング・チェックリスト

Web アプリケーションで問題が発生した場合、IBM ソフトウェア・サポートに連絡する前にこのリストを確認してください。このリストには、最も一般的な問題が示されています。

1. 構成コンソールの「ログイン」画面を表示できない
2. 構成コンソールにログインできない
3. Web ブラウザーでレポートは開くが、レポートに何も表示されない
4. 「パイプラインの状況 (Pipeline Status)」タブにパイプラインの状況を表示できない
5. 構成コンソールで行った構成変更がパイプラインに適用されない

1. 「ログイン」画面を表示できない
   - 「ページを表示できません」というメッセージが表示されますか?
     - Web アプリケーション URL が正しくない可能性があります。URL を再入力してください。正しい URL が不明な場合は、システム・アドミニストレーターまたは社内テクニカル・サポートに連絡して支援を依頼してください。

- その他の考えられる原因: ご使用のマシンを WebSphere Liberty サーバーに接続するポートがブロックされているか、WebSphere Liberty サーバーが開始されていない可能性があります。システム・アドミニストレーターまたは社内テクニカル・サポートに連絡して支援を依頼してください。

- 画面がブランクですか?
  - システム・アドミニストレーターまたは社内テクニカル・サポートに連絡してください。ご使用のマシンを WebSphere Liberty サーバーに接続するポートが開始されていないか、Identity Insight データベース・パスワードが変更された可能性があります。
- これらのソリューションのいずれでも問題が解決しない場合は、システム・アドミニストレーターまたは社内テクニカル・サポートに連絡して支援を依頼してください。

2. **Web** アプリケーションにログインできない
   - 正しいユーザー名とパスワードを入力したことを確認してください。Analyst ツールキット・アプリケーションでは、ログイン試行で何回間違えようとユーザー・アカウントはロックされないので、再度ユーザー名とパスワードを入力してください。
   - ユーザー名とパスワードを忘れた場合は、システム・アドミニストレーターまたは社内テクニカル・サポートに連絡して支援を依頼してください。パスワードの再設定が必要な場合もあります。
3. 構成コンソールで行った構成変更がパイプラインに適用されない
   - 構成変更を適用する前に、パイプラインを停止してから再始動する必要があります。パイプラインの再始動時に、パイプライン初期化処理の一部として、構成変更が適用されます。
   - データ保全性を確保するため、構成変更の後で、実行中のすべてのパイプラインを停止してから再始動してください。

Visualizer のトラブルシューティング・チェックリスト

Visualizer で問題が生じた場合は、IBM サポートに連絡する前にこのリストを確認してください。このリストには、Visualizer の使用時に検出される最も一般的な問題が示されています。Visualizer の問題をご自身で解決できる可能性があります。

1. Visualizer を開始できない
2. Visualizer にログインできない
3. Visualizer レポートを生成したが、そのレポートを Web ブラウザーで開いてもレポートに何も表示されない
4. パイプラインに関するエラー・メッセージを受け取る
5. Visualizer が「停止」または「フリーズ」する
6. 「属性による検索 (Find by Attribute)」で予期した結果が返されない
7. 「属性による検索 (Find by Attribute)」ウィンドウの使用時に「不十分な索引」に関するエラー・メッセージを受け取る
8. Visualizer のグラフのカスタム・アイコンが表示されない (または正しく表示されない)
9. Visualizer 内のリンク (またはハイパーリンク) が動作しない

1. **Visualizer** を開始できない
   - まず、ご使用のワークステーション・クライアントに必須なクライアント・バージョンの Java がインストールされていることを確認してください。
   - ご使用のクライアント・マシンに複数のバージョンの Java がインストールされている場合は、Java Web Start のデフォルトのシステム・バージョンが Visualizer の実行に必要なバージョンではない可能性があります。また、Visualizer を開いて実行するために必要なクライアント Java バージョンが、ご使用のマシンにインストールされている最新バージョンの Java ではない可能性があることも念頭においてください。この問題を解決する方法は 2 つあります。ご使用の Web ブラウザーで必要なクライアント・バージョンの Java Web Start を関連付けるか、直接起動方式を使用してください。
     – このワークステーション・クライアントで使用する Web Start アプリケーションは Visualizer だけですか? その場合は、Web ブラウザーに *.JNLP ファイル・タイプの関連付けを設定し、必要なクライアント・バージョンの Java Web Start を使用するようにしてください。
     – このワークステーション上の Visualizer に加えて追加の Web Start アプリケーションを実行しますか、また、システムおよび Java の設定を変更しないようにしますか? その場合は、Java Web Start ファイルから直接 Visualizer を起動してください。
   - アプリケーションに必要なバージョンの JRE がインストールされていないことを示すエラー・メッセージを受け取りましたか? 受け取った場合は、Java バージョン 1.6 を構成して自動ダウンロードを受け入れるようにしてください。
   - Visualizer の Web Start ページが表示されますか？
     – はい、Visualizer の Web Start ページは表示されますが、「Visualizer の起動には Java Web Start が必要」であることを示すメッセージが表示されます。「**IBM InfoSphere Identity Insight Visualizer** を開始するにはここをクリック **(Click here to start the IBM InfoSphere Identity Insight Visualizer)**」リンクは表示されません。
       - このワークステーション・クライアントを Visualizer 用にのみ使用しますか? その場合は、Web ブラウザーに JNLP ファイル・タイプの関連付けを設定し、必要なクライアント・バージョンの Java Web Start を使用するようにしてください。
       - このワークステーション・クライアントを使用してその他の Web Start アプリケーションを開きますか? また、システムおよび Java の設定を変更しないようにしますか? その場合は、Java Web Start ファイルから直接 Visualizer を起動してください。
     – はい、Visualizer の Web Start 起動ページと Visualizer のスプラッシュ画面は表示されますが、Visualizer の「ログイン」ウィンドウを表示できません。
       - 「**IBM InfoSphere Identity Insight Visualizer** を開始するにはここをクリック **(Click here to start the IBM InfoSphere Identity Insight Visualizer)**」リンクをクリックしましたか?
         - クリックした場合は、Java が Visualizer のオープン処理の最中である可能性があります。これには数分かかる場合があります。

Visualizer がオープン処理の最中である場合、通常は Java スプラッシュ画面か 「Java Web Start」ウィンドウが表示されます。
    - クリックしていない場合は、リンクをクリックして Visualizer を開始してください。
  - 可能性として最も高いのは、組み込み WebSphere Application Server の問題です。アプリケーション・サーバーにエラーまたは問題が発生しているため、再始動が必要な可能性があるか、アプリケーション・サーバーが正しい製品データベースに接続できていません。システム・アドミニストレーターまたは社内テクニカル・サポートに連絡してください。
- いいえ、Visualizer の Web Start ページが表示されません。
  - 「ページを表示できません」というメッセージが表示される場合は、Visualizer の URL を確認してください。URL にタイプミスがあるか、Visualizer の URL が誤っている場合があります。URL を再入力してください。Visualizer の URL が不明な場合は、システム・アドミニストレーターまたは社内テクニカル・サポートに連絡してください。
  - URL が正しい場合は、Visualizer の Web Start ページが表示されない別の理由がある可能性があります。
    - WebSphere Application Server にエラーまたは問題が発生しているため、再始動が必要な可能性があります。
    - WebSphere Application Server にワークステーション・クライアントを接続するポートが、ブロックされているか、既に別のアプリケーションによって使用されている可能性があります。
- 上記のいずれのアクションでも問題が解決しない場合は、システム・アドミニストレーターまたは社内テクニカル・サポートに依頼して、IBM ソフトウェア・サポートに連絡してください。

2. **Visualizer** にログインできない
   - Visualizer の「ログイン」画面が表示されますか?
     - いいえ、Visualizer の「ログイン」画面は表示されません。
       - 可能性として最も高いのは、組み込み WebSphere Application Server の問題です。アプリケーション・サーバーにエラーまたは問題 (接続されない) が発生しているか、アプリケーション・サーバーが正しい製品データベースに接続できていません。システム・アドミニストレーターまたは社内テクニカル・サポートに連絡して支援を要請してください。
     - はい、Visualizer の「ログイン」画面は表示されますが、ログインできません。
       - Visualizer ユーザー・アカウントの正しいユーザー名とパスワードを入力したことを確認してください。Visualizer では、ログイン試行の誤りの回数に関係なく、ユーザー・アカウントはロックされません。ユーザー名とパスワードを再入力してください。ご自身のアカウントからお客様ご自身をロックすることはできません。
       - 「ログイン」をクリックしてください。「ログイン」ボタンは自動的に選択されないため、ユーザー名とパスワードを入力して「**Enter**」を

押すと、この状況が発生します。マウスを使用して「ログイン」をクリックするか、キーボードを使用して「ログイン」を選択する必要があります。

- ユーザー名とパスワードを忘れましたか?
  - はい。システム・アドミニストレーターまたは社内テクニカル・サポートに連絡してユーザー名を調べるか、構成コンソールで Visualizer アカウントのパスワードを再設定してください。

3. **Visualizer** のレポートを生成したが、そのレポートを **Web** ブラウザーで開いてもレポートに何も表示されない
   - 1 分から 2 分余り待ってください。レポートをまだ生成中の可能性があります。システムがレポートを生成中である場合、開始時にブラウザーに空白画面が表示されます。レポートの生成が完了して表示できる状態になったら、システムはレポートを表示します。
   - ご使用のローカル・マシンに Adobe Acrobat Reader バージョン 7.0 以降をインストール済みであることを確認してください。インストールしていない場合は、Adobe Web サイトから最新の Adobe Acrobat Reader を無料でダウンロードできます。
   - ご使用のシステムにファイアウォールがありますか? ある場合は、ファイアウォールを調べて、ローカル・ホストとアプリケーション・サーバーの両方にファイアウォール経由のアクセス権限が付与されていることを確認してください。
4. パイプラインに関するエラー・メッセージを受け取る
   - 問題の原因が何かを示す詳細情報がないか、エラー・メッセージをよく調べてください。
   - Visualizer のパイプラインが HTTP パイプラインであることを確認してください。
   - ご使用のワークステーションで Visualizer クライアントのロギングをオンにしていますか?
     - いいえ。
       - ご使用のマシン上で 453 ページの『Visualizer クライアントのロギングをオンに設定』してください。ログ・レベルを「デバッグ」に設定してください。次に、システム・アドミニストレーターまたは社内テクニカル・サポートに連絡し、エラー・メッセージのテキストを提供して、その担当者に Visualizer クライアントのロギングをオンにしたことを知らせてください。システム・アドミニストレーターまたは社内テクニカル・サポートから、パイプラインに接続し直してからログ・ファイルを調べるように指示される可能性があります。
       - 問題が解決したら、Visualizer クライアントのロギングをオフにします。
     - はい。
       - *installation_directory*/logs/ewas にある Visualizer クライアント・ログ・ファイルを確認してください。

- システム・アドミニストレーターまたは社内テクニカル・サポートに連絡してください。システム・アドミニストレーターまたは社内テクニカル・サポートが Visualizer クライアント・ログ・ファイルを調べる場合があります。

5. **Visualizer** が「停止」または「フリーズ」する
   - 組み込み WebSphere Application Server にマシンを接続するポートがブロックされているか、または組み込み WebSphere Application Server が開始されていない可能性があります。システム・アドミニストレーターまたは社内テクニカル・サポートに連絡してください。
   - DBA、システム・アドミニストレーター、または社内テクニカル・サポート用の情報:
     – Visualizer に影響を与えるエンティティー・データベース表に対して stat を実行することを検討してください。
     – すべての Visualizer ユーザーに Visualizer の「停止」障害が発生している場合は、データベース表の索引が変更されていないことを確認してください。データベース表の索引を変更すると、予測不能かつ望ましくない結果を引き起こす場合があります。索引が変更されたことが判明した場合は、IBM ソフトウェア・サポートに連絡してください。
6. 「属性による検索 **(Find by Attribute)**」で予期した結果が返されない
   - 検索基準を確認してください。
     – 表示される結果が想定より少ない場合は、基準を広げることが必要な場合があります。
     – 表示される結果が想定より多い場合は、検索基準を狭くすることが必要な場合があります。
     – デフォルトでは、システムは、検索ごとに最大 1000 レコードを返すだけです。(ただし、この設定は構成可能です。この設定は、構成コンソールの「システム・パラメーター」タブにある `MAX_ENTITIES_RETURNED` パラメーターによって制御されます。システム・アドミニストレーターまたは社内テクニカル・サポートに連絡して、この設定の確認または変更を依頼することができます。)
   - この問題は、大/小文字の区別に関するデータベース構成に関連している可能性があります。システム・アドミニストレーターまたは社内テクニカル・サポートに連絡して、大/小文字の区別の設定についてデータベース構成の確認を依頼してください。
     – DB2 データベースの場合: DBA、システム・アドミニストレーター、または社内テクニカル・サポートは、大/小文字を区別しないデータベース検索をサポートするためのスクリプトを適用する必要がある可能性があります。スクリプトと、その実行方法に関する説明を入手するには、IBM ソフトウェア・サポートへ連絡するようにシステム・アドミニストレーターに要請してください。
     – Microsoft SQL サーバー・データベースの場合: データベースが大/小文字を区別するように設定されている可能性があります。DBA、システム・アドミニストレーター、または社内テクニカル・サポートは、データベースの大/小文字の区別の設定を変更することが必要になる場合があります。

- Oracle データベースの場合: DBA、システム・アドミニストレーター、または社内テクニカル・サポートは、大/小文字を区別しないデータベース検索をサポートするために、UPPER を使用して関数ベースの索引を作成することが必要になる場合があります。

7. 「属性による検索 **(Find by Attribute)**」ウィンドウの使用時に「不十分な索引」に関するエラー・メッセージを受け取る
   - 索引の付いていないフィールドで検索しようとしています。
     - 追加の検索基準を入力して、検索を絞り込んでみてください。
     - あるいは、システム・アドミニストレーターまたは社内テクニカル・サポートに連絡してください。システム・パフォーマンスに与える影響に応じて、システム・アドミニストレーターがこのフィールドに新しい索引を作成する可能性があります。(システム・アドミニストレーターまたはテクニカル・サポートは、構成コンソールの「システム・パラメーター」タブにある ENABLE_SEARCH_INDEX_CHECK パラメーターも確認する可能性があります。この設定が 1 に設定されていない場合、システム・パフォーマンスに影響を与える場合があります。)
8. **Visualizer** のグラフのカスタム・アイコンが表示されない **(**または正しく表示されない**)**
   - アイコンがアプリケーション・サーバー上の正しいディレクトリーに配置されていない可能性があります。カスタム・グラフ・アイコンのパス位置を確認するには、システム・アドミニストレーターまたは社内テクニカル・サポートに連絡してください。
   - アイコン名がすべて小文字ではなく大/小文字混合になっているか、対応する属性タイプと一致していない可能性があります。例えば、属性タイプの名前が **Evidence Photo** の場合、イメージ・ファイル名はすべて小文字にし、単語の evidence と photo との間にスペースを入れる必要があります。このファイル名は **evidence photo.gif** のようになっていなければなりません。システム・アドミニストレーターまたは社内テクニカル・サポートに連絡して、アイコン・ファイル名が正しいことを確認してください。
   - アイコンが推奨の .GIF ファイル・フォーマットでない可能性があります。または、アイコンが推奨サイズ (24 x 24 ピクセル) でない可能性があります。システム・アドミニストレーターまたは社内テクニカル・サポートに連絡して、アイコンが正しいファイル・フォーマットであり、推奨イメージ・サイズを使用していることを確認してください。
9. **Visualizer** 内のリンク **(**またはハイパーリンク**)** が動作しない。属性リンクをクリックするとエラー・メッセージが表示される
   - ワークステーションのハイパーリンク設定の構成を実行してください。Visualizer システム設定で、アイデンティティー・レコード属性に関連付けられたファイルを開くために使用する Web ブラウザーまたはプログラムを選択します。この設定は、Visualizer を実行する各ワークステーションで構成する必要があります。
   - ハイパーリンク設定を構成した後、必ず Visualizer を閉じてからもう一度再始動してください。

システム・ヘルス

DBA およびシステム・アドミニストレーターが IBM InfoSphere Identity Insight システムを正常な状態に保つためのヒントをいくつか以下にします。

パフォーマンスのヒント

システム全体のパフォーマンスの低下に気付いた場合、考えられる原因について、このリストを確認してください。

- データベースの調整: 前回、IBM InfoSphere Identity Insight 表に対するデータベース統計を実行したのはいつか。
- 非常に大きいエンティティー: エンティティー・データベースに非常に大きいエンティティー (多数のアイデンティティーを持つエンティティー) が含まれているか。

このリストにはすべてが含まれているわけではありませんが、システムのパフォーマンスがピークに達しているかどうかを確認するための開始点になります。

エンティティー・データベースのモニターのヒント

ここでは、エンティティー・データベースの正常性をモニターするのに役立つ具体的な確認項目をいくつか示します。

- データベースの調整: IBM InfoSphere Identity Insight 表に対するデータベース統計の実行のスケジュールはどのようなものか?
- ユニーク番号: エンティティー・データベースに同じユニーク番号を共有する複数のエンティティーが含まれているか?
- エンティティー: エンティティー・データベースに複数のユニーク番号を持つエンティティーが含まれているか?
- 過剰解決: エンティティー・データベースに非常に大きいエンティティー (多数のアイデンティティーを持つエンティティー) が含まれているか。

このリストにはすべてが含まれているわけではありませんが、システム全体の正常性をモニターするためのクイック・ヒントをいくつか提供します。

システム・パフォーマンスに影響を与えるデータベース表

システム・パフォーマンスが低いと思われる場合、データベース・アドミニストレーターは、いくつかのエンティティー・データベース表に対してデータベース統計を実行して、パイプラインのパフォーマンスと Visualizer のユーザー・エクスペリエンスの両方を改善することができます。

パイプライン表

パイプラインのパフォーマンスが低いと思われる場合、以下のエンティティー・データベース表に対してデータベース統計を実行してみてください。

- DQM_NAME_DICT
- NAME
- ADDRESS
- NUMS
- ATTRIBUTES

- EMAIL_ADDR
- DSRC_ACCT
- SEP_RELATIONS
- SEP_ROLES
- ENTITY
- DISCLOSED_RELATIONS
- UMF_LOG
- UMF_EXCEPT

Visualizer 表

Visualizer ユーザーから Visualizer のパフォーマンスが低いようだと不満が出た場合は、以下のエンティティー・データベース表に対してデータベース統計を実行してみてください。

- 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

また、Visualizer はバックグラウンド・パイプラインを使用していくつかの Visualizer タスク (エンティティーの追加、エンティティー解決によるエンティティーの検索、および関係の開示など) を実行するので、データベース・アドミニストレーターは、パイプライン表セクションにリストされているデータベース表に対するデータベース統計も実行する必要があります。

ラージ・エンティティー・クエリー

この SQL クエリーでは、大きいエンティティーを検索します。エンティティーに含まれるアイデンティティー・レコードの数が多くなるほど、そのエンティティーは大きくなります。場合によっては、入力アイデンティティー・データの処理結果が原因で、エンティティーと関係の解決時にシステムでアイデンティティー・レコ

ードの過剰解決が起こることがあります。大きいエンティティーによって、システム・パフォーマンスが著しく低下する可能性があります。

ラージ・エンティティー SQL クエリー・ステートメント

```
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;
```

次の操作

i2 用の Identity Insight プラグインまたはエクスプローラー・アプリケーションで、「エンティティー **ID** による検索 **(Find by Entity ID)**」画面を使用して、ラージ・エンティティー・クエリーの結果から返されるエンティティー ID を検索します。このエンティティーに関連付けられたアイデンティティーが正しく関連付けられていることを確認します。適切に構成されたエンティティーの場合、そのエンティティーには多数の異なるデータ・ソース・アカウントがありますが、関連付けられた名前、住所、および番号のデータはほとんどの場合非常によく似ています。エンティティーが適切に構成されているかどうかについて疑問がある場合には、IBM サービスまたは IBM サポートに連絡して支援を依頼してください。

ラージ・エンティティー・クエリーの結果の例

ラージ・エンティティー・クエリーの実行結果の例を以下に示します。

ENTITY_ID	IDENTITY_CNT
3015	22
5241	41
7854	36

エンティティー別のユニーク番号の合計のクエリー

このクエリーは、特定のエンティティーに異なるユニーク番号がいくつ関連付けられているかについての情報を、エンティティー ID 別に返します。各エンティティーに通常はユニーク番号が 1 つのみ存在する場合に、このクエリーが役立つことがあります。エンティティーに異なるタイプの複数のユニーク番号が含まれているかどうかを調べる検査は、データ異常をチェックし、解決ルールが想定どおり機能していることを検証するための優れた方法です。

単一エンティティーに関連付けられているユニーク番号の合計数の SQL クエリー・ステートメント

```
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;
```

次の操作

i2 用の Identity Insight プラグインまたはエクスプローラー・アプリケーションで、「エンティティー **ID** による検索 **(Find by Entity ID)**」画面を使用して、エンティティー ID 別のユニーク番号の合計数のクエリー結果から返されるエンティティー ID を検索します。各エンティティーのエンティティー・レジュメを検討することで、そのエンティティーに複数のユニーク番号があることが正当かどうかを判別できます。場合によっては、これは不正な状態であることを示しています。例えば、アメリカ合衆国の社会保障番号 (SSN) はユニーク番号です。通常、各 U.S. エンティティーに 1 つの SSN のみが存在します。このクエリーによって複数の SSN を持つエンティティーが見つかった場合、次のステップはおそらく、そのエンティティーに複数の SSN が存在する理由の詳しい調査と分析を行うことです。

エンティティー別のユニーク番号の合計数のクエリー結果の例

エンティティー別のユニーク番号の合計数のクエリーを実行した結果を、次の例に示します。

ENTITY_ID	UNIQUE_NUMBER_CNT
3003	2
3030	2
3039	2

複数エンティティーで共有されるユニーク番号のクエリー

ユニーク番号は通常は 1 つのエンティティーのみに属する番号で、複数のエンティティーで共有されることはありません。複数のエンティティーで同じユニーク番号を共有しているかどうかを調べる検査は、データ異常の有無をテストし、解決ルールが想定どおり機能していることを検証するための優れた方法です。複数エンティティーで共有されるユニーク番号のクエリーを使用して、同じユニーク番号を共有しているエンティティーを検出できます。このクエリーは、特定のエンティティーに同一ユニーク番号を持つアイデンティティー・レコードがいくつ含まれているかに関わらず、単一エンティティーのユニーク番号を 1 回だけカウントします。

複数エンティティーで共有されるユニーク番号の SQL クエリー・ステートメント

```
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;
```

次の操作

i2 用の Identity Insight プラグインまたはエクスプローラー・アプリケーションで、「属性による検索 **(Find by Attribute)**」画面を使用して、複数エンティティーで共有されるユニーク番号の SQL クエリーで返される各番号を検索します。「結果」ペインで、ユニーク番号を共有している各エンティティーのエンティティー情報を確認します。これらのエンティティーのエンティティー・レジュメを検討して、複数エンティティーが同じユニーク番号を共有する理由の判別に役立てることもできます。

ユニーク番号に基づいて、エンティティー間の興味深い関係をディスカバーする場合もあります。例えば、2 つの異なるエンティティーが同じ社会保障番号を使用していることをディスカバーする場合があります。

また、ユニーク番号の UMF コーディングの問題を検出する可能性もあります。例えば、2 つのエンティティー間で同じパスポート番号を共有していることをディスカバーする場合があります。これは、パスポート番号を発行する国 (場所) を示す NUM_LOC を入力 UMF アイデンティティー・レコードで使用していなかったことが原因です。パスポートや運転免許証などの番号は、国または都道府県など、特定の場所のみでユニークなものです。これらの番号自体は、一般的に考えられているほどユニークではないことがあります。

複数エンティティーで共有されるユニーク番号のクエリー結果の例

複数エンティティーで共有されるユニーク番号のクエリーを実行した結果を次の例に示します。

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

知識ベースの検索

多くの場合、IBM 知識ベースを検索することで問題の解決策を見つけることができます。このトピックでは、使用可能なリソース、サポート・ツール、および検索方式を使用することによって結果を最適化する方法について説明します。

使用可能なテクニカル・リソース

疑問に答えて問題を解決するために、このインフォメーション・センターに加えて以下のテクニカル・リソースが役立ちます。

IBM InfoSphere Identity Insight 技術情報 (www.ibm.com/software/support/isa/)

サポート・ツールによる検索

IBM 知識ベース全体の検索を支援する、以下のデスクトップ・ツールを使用できます。

- **IBM Support Assistant (ISA)** は、IBM ソフトウェア製品に関する疑問や問題を解決するのに役立つ無償のソフトウェア保守ワークベンチです。ISA のダウンロードおよびインストールの手順については、ISA の Web サイト (www.ibm.com/software/support/isa/) を参照してください。
- **IBM Software Support Toolbar** は、IBM サポート・サイトで検索を容易に行うためのメカニズムを提供するブラウザー・プラグインです。このツールバーは www.ibm.com/software/support/toolbar/ からダウンロードできます。

検索のヒント

以下のリソースでは、検索結果を最適化する方法について説明します。

- IBM Support Web サイトの検索
- Google 検索エンジンの使用

自動更新の受信

- 「**My** サポート **(My support)**」。フィックスおよびその他のサポート・ニュースに関する E メール通知を毎週受け取るには、以下のステップに従ってください。
  1. IBM ソフトウェア・サポートの Web サイト (www.ibm.com/software/support/) にアクセスします。
  2. ページの一番右上隅の「パーソナライズ・サポート **(Personalized support)**」の下にある「**My** サポート **(My support)**」をクリックします。
  3. 既に「My サポート (My support)」に登録済みの場合は、サインインして次のステップに進みます。まだ登録していない場合は、「今すぐ登録 **(register now)**」をクリックします。お客様の E メール・アドレスを IBM ID として使用し、登録フォームに入力して、「送信 **(Submit)**」をクリックします。
  4. 「プロファイルの編集 **(Edit profile)**」をクリックします。
  5. 「製品リスト **(Products list)**」で、「ソフトウェア **(Software)**」を選択します。2 番目のリストが表示されます。
  6. 2 番目のリストで、製品セグメント (例えば「システム管理 **(Systems management)**」) を選択します。3 番目のリストが表示されます。
  7. 3 番目のリストで、製品のサブセグメント (例えば「アプリケーションのパフォーマンスおよび可用性 **(Application Performance & Availability)**」を選択します。使用可能な製品のリストが表示されます。

8. 更新情報を受け取る製品を選択します。
9. 「製品の追加 **(Add products)**」をクリックします。
10. 関心のある製品をすべてを選択したら、「プロファイルの編集 **(Edit profile)**」タブの「**E** メールをサブスクライブ **(Subscribe to email)**」をクリックします。
11. 「これらの文書を毎週 **E** メールで送信してください **(Please send these documents by weekly email)**」を選択します。
12. 必要に応じて E メール・アドレスを更新します。
13. 「文書リスト **(Documents list)**」で、「ソフトウェア **(Software)**」を選択します。
14. 情報の受信を希望する文書のタイプを選択します。
15. 「更新 **(Update)**」をクリックします。

メッセージの概要

システム・コンポーネントからメッセージを受け取った場合、メッセージ・テキスト全体と、そのメッセージに関連付けられているリカバリー・アクションを確認することで、問題を解決できることがよくあります。

メッセージ ID の長さは 10 文字です。メッセージ ID の文字は、メッセージに関する詳細情報を提供します。

- 最初の 3 文字は製品を識別します。
  - **CWU**: IBM InfoSphere Identity Insight の製品 ID。
- 次の 2 文字は、製品内でメッセージを生成している特定のコンポーネントを識別します。
  - **AE**: パイプラインのコンポーネント ID。
  - **AI**: 構成コンソールのコンポーネント ID。
  - **AK**: Event Manager のコンポーネント ID。
  - **AL**: Web サービスのコンポーネント ID。
- 次の 4 文字は、メッセージ番号です。
- 最後の文字は、メッセージ・タイプ・コードで、以下のようにメッセージの重大度を示します。
  - **E**: エラー・メッセージを示します。このタイプのメッセージは、特定の製品コンポーネントに即時アクションを必要とする問題があることを示します。コンポーネント・ログ・ファイルで、エラーのトラブルシューティングと解決に役立つ情報を確認してください。
  - **I**: 通知メッセージを示します。このタイプのメッセージには即時アクションは必要ありませんが、コンポーネント・ログ・ファイルで詳細を確認することをお勧めします。
  - **W**: 警告メッセージを示します。このタイプのメッセージは、注意が必要になる可能性がある状態が発生したことを示します。警告状態の内容とその状態を解決する方法の詳細について、コンポーネント・ログ・ファイルを確認してください。

メッセージ例

CWUAE0001E というメッセージ ID を持つメッセージを受け取ったとします。このメッセージは、パイプラインからのエラー・メッセージであり、パイプラインがシャットダウンして処理を停止した可能性があることを示します。パイプラインを再始動できるように、パイプライン・ログ・ファイルを確認して問題を解決する必要があります。

CWUAE325W というメッセージ ID を持つメッセージを受け取ったとします。このメッセージは、パイプラインで警告メッセージが発生したが、この警告によってパイプラインの入力レコード処理の続行は停止しなかったことを示します。警告についての詳細をパイプライン・ログ・ファイルで確認し、問題または入力データ・レコードを訂正するために取る必要のあるアクションを調べることができます。この特定のパイプラインをアプリケーション・モニターでモニターしている場合は、構成コンソールのアプリケーション・モニター・ウィンドウで詳細を確認することもできます。

UMF 解析エラー

入力 UMF アイデンティティー・レコードのフォーマットが不適切な場合 (終了タグが欠落している、UMF 内に無効文字があるなど)、UMF 解析エラーが発生します。

表 *37. UMF* 解析エラー

UMF エラー・コード	コードの説明	重大度
005	タグ名 *string* では、先行スペースは許可されません	重大
010	ルート・レベルの開始タグ *<string>* が欠落しています	重大
015	予期しない終了タグ *</string>* が検出されました	重大
020	不適切な終了タグ *</string>* が検出されました。予期されているタグは *</string>* です	重大
025	文書が不完全です。終了タグが足りません...最終セグメント: *<string>*	重大
030	文書が空です	警告
035	子が存在している場合、セグメントにタグ・データ「*string*」を含めることはできません	重大

ログ

IBM InfoSphere Identity Insight には、一連のログ・ファイルに情報を書き込むロギング・メカニズムが含まれています。通常は、該当する条件が特定のシステム・コンポーネントに発生したときに (例えばコンポーネントのインストール時や開始時、ユーザーがコンポーネントにログオンする時、または処理中にエラーが発生した場合)、システムはログ・ファイルへの情報の書き込みを開始します。

以下のシステム・コンポーネントでログ・ファイルが作成されます。

- パイプライン
- Analyst ツールキット Web アプリケーション

- Web サービス
- Event Manager

パイプライン・ログ・ファイル

パイプラインを開始するたびに、パイプライン構成ファイル内の現行のパイプライン・ロギング構成に基づいて、システムが自動的にロギングを開始します。同じ構成ファイルを使用して複数のパイプラインを開始した場合でも、パイプライン名別に、各パイプラインのロギング・ファイルが作成されます。

パイプライン・ログ・ファイルのタイプ

デフォルトでは、すべてのパイプライン・ログ・ファイルは、そのパイプラインが開始されたパイプライン・ノードのディレクトリーに書き込まれます。パイプライン・ログ・ファイルには、いくつかの異なるタイプがあります。どのメッセージがどのファイルに記録されるかは、パイプラインが開始されたモード (デバッグ・モード `-d` またはデーモン/サービス・モード `-s`)、ログに記録されるメッセージのタイプ、および現行のロギング構成に応じて異なります。

表 *38.* メッセージのタイプ、ログ・ファイル名、およびロギング・モード別のパイプライン・ロギング・ファイル

メッセージのタイプ	ログ・ファイル名	アクション	ロギング・モード
エラー・メッセージ	*pipeline_name*.err パイプラインで発生したクリティカル・エラーを記録します。	ログ・ファイルを確認した後、パイプラインについて示されたエラーまたは問題を修正してください。	サービス デバッグ
SQL エラー・メッセージ	*pipeline_name*.SqlErr.log パイプラインで発生した SQL エラーを記録します。 このファイルには 1 メガバイトのサイズ制限があります。ファイルがこのサイズ制限に達すると、システムは自動的に現行ログ・ファイルをアーカイブし、新規ログ・ファイルを作成します。	このログ・ファイルを確認した後、示されている SQL のエラーまたは問題を修正してください。	サービス デバッグ
キュー・エラー	*pipeline_name*.MQErr.log キュー・エラーを記録します。	このログ・ファイルを確認した後、示されている MQ のエラーまたは問題を修正してください。	

表 38. メッセージのタイプ、ログ・ファイル名、およびロギング・モード別のパイプライン・ロギング・ファイル (続き)

メッセージのタイプ	ログ・ファイル名	アクション	ロギング・モード
Windows の「イベント ビューア」	(Microsoft Windows プラットフォームのみ) パイプラインにインストール済みのサービスがあり、サービス・モード (-s パイプライン・オプション) を使用して開始された場合、パイプラインはエラーおよび重要なメッセージを Windows の「イベント ビューア」にも送信します。	Windows の「イベント ビューア」でメッセージをモニターし、示されているエラーまたは問題を修正してください。	サービス (Microsoft Windows プラットフォームのみ)
処理できなかった不良/無効な UMF メッセージ	*pipeline_name*.bad 誤った形式の UMF または無効な UMF が含まれているレコードが入力データ・ソース・ファイル内にある場合に、それらのレコード関する情報を記録します。 パイプラインはこの不良または無効な UMF が含まれたレコードの一部を処理できませんでした。これは、パイプラインが部分レコードを処理していることを意味する場合があります。	このログ・ファイルを確認した後、不良または無効な UMF が含まれた入力データ・ソース・ファイル内のレコードを修正してください。次に、修正済みレコードを処理するためにパイプラインに送り戻します。	サービス デバッグ
例外を生成した UMF メッセージ	*pipeline_name*.msg 処理中に生成された例外が含まれているレコードが入力データ・ソースファイル内にある場合に、それらのレコード関する情報を記録します。 パイプラインは、このレコードを処理しました。 このタイプのメッセージは、このデータ・ソース・ファイルのデータ品質に問題があることを示している場合があります。	このログ・ファイルを確認した後、UMF 例外を生成した、入力データ・ソース・ファイル内のレコードを修正することが必要な場合があります。次に、修正済みレコードを処理するためにパイプラインに送り戻します。 「ロード要約レポート (Load Summary Report)」または「データ・ソース要約レポート (Data Source Summary Report)」で、詳細を確認することもできます。	サービス デバッグ

表 38. メッセージのタイプ、ログ・ファイル名、およびロギング・モード別のパイプライン・ロギング・ファイル (続き)

メッセージのタイプ	ログ・ファイル名	アクション	ロギング・モード
デバッグ・トレース	デバッグ・モード (-d パイプライン・オプション) を使用してパイプラインが開始された場合に、デバッグ・トレース情報を記録します。ログ・ファイルはありません。パイプラインはフォアグラウンドで実行され、出力メッセージはコマンド・シェルに直接送信されます。以下のように、リダイレクト機能を使用して pipeline コマンド出力からファイルを作成できます。 `pipeline -d -f my_umf.xml > my_log_file.log`		デバッグ
SQL ステートメントおよびパフォーマンス統計	*pipeline_name*.SqlDebug.log SQL ステートメントおよびパフォーマンス統計を記録します。これは、問題のトラブルシューティングおよびパフォーマンスのモニターに役立ちます。 このファイルには 48 メガバイトのサイズ制限があります。ファイルがこのサイズ制限に達すると、システムは自動的に現行ログ・ファイルをアーカイブし、新規ログ・ファイルを作成します。		デバッグ
ファイル処理中のパイプラインのシャットダウン	*pipeline_name*.cnt パイプラインは、入力レコードを処理する際に、正常に処理した、ファイル内の 100 レコードごとに、処理対象のデータ・ソース・ファイルの名前およびレコード・カウントを記録します。 入力データ・ソース・ファイルの処理中にパイプラインがシャットダウンした場合、データ・ソース・ファイルのどのレコードを処理のためにパイプラインに再ロードする必要があるのかを判別するために、このファイルが役立つ場合があります。	このログ・ファイルを確認して、パイプラインをシャットダウンした問題を修正した後、未処理レコードを処理するためにパイプラインに再ロードしてください。	ファイル

パイプライン・ロギング構成

IBM InfoSphere Identity Insight には、パイプラインのイベントおよびエラーを記録するデフォルトのロギング構成があります。パイプライン構成ファイルにカスタムのパイプライン・ロギング構成が指定されていない限り、このデフォルトのロギング構成が自動的に使用されます。

パイプラインを開始するには 2 つの主な方法があります。デバッグ・モード (-d パイプライン・オプション) とサービス/デーモン・モード (-s パイプライン・オプション) です。

- デバッグ・モードは、システムのトラブルシューティングおよびテストを行う場合に役立ちます。これは通常、実稼働環境では使用されません。デバッグ・モードのロギングには、詳細なトレース情報およびパイプライン操作情報が含まれています。
- サービス/デーモン・モードは、標準的な実稼働環境モードです。サービス/デーモン・モードのロギングは、通常、アクションを必要とするエラーおよび問題に限定されます。

すべてのパイプライン・ロギング構成 (デフォルトおよびカスタムの両方) で、デバッグ・モードおよびサービス/デーモン・モードでのパイプライン・イベントの記録方法を指定する必要があります。デフォルトのロギング構成がニーズを満たしていない場合は、カスタム・ロギング構成を作成できます。それには、パイプライン構成ファイルにロギング・セクションを追加し、パイプライン構成コンポーネントを使用して、システムがパイプラインのイベントおよびエラーを記録する方法を、デバッグ・パイプライン・モードおよびサービス/デーモン・パイプライン・モードの両方について指定します。

デフォルトのデバッグ・モード・ロギング構成

```
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.*
```

デフォルトの Microsoft Windows サービス・モード・ロギング構成

```
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.*
```

デフォルトの UNIX デーモン・モード・ロギング構成

```
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.*
```

パイプライン・ロギング・コンポーネント

パイプライン・ロギング・コンポーネントは、カスタム・パイプライン・ロギング構成を作成するのに役立ちます。これらのコンポーネントは、パイプラインのイベントおよびメッセージをログに記録する方法に関する指示をシステムに提供します。

ログ・ライター
: ログ・ファイルの書き込みまたは表示に使用するログ・ライターを指定します。

  file
  : 指定した名前のファイルにログ・イベントおよびメッセージを書き込みます。

    file ログ・ライターは、パス、パラメーター、空白、およびフィルターの各ロギング・コンポーネントを使用します。例:

    `file://absolute path?parameters [white space] filter`

  cmeadmin
  : cmeadmin ログにログ・イベントおよびメッセージを書き込みます。

    cmeadmin ログ・ライターは、空白およびフィルターの各ロギング・コンポーネントを使用します。例:

    `cmeadmin://[white space] filter`

  console
  : コマンド行コンソールにログ・イベントおよびメッセージを書き込みます。

    console ログ・ライターは、位置、パラメーター、およびフィルターの各ロギング・コンポーネントを使用します。例:

    `console://file location?parameters filter`

  eventlog
  : (Microsoft Windows プラットフォームのみ) Microsoft Windows の「イベント ビューア」にログ・イベントおよびメッセージを書き込みます。

    eventlog ログ・ライターは、フィルター・ロギング・コンポーネントを使用します。例:

    `eventlog://./filter`

パス　ログ情報の書き込み先のファイルの場所および名前を指定します。

ファイルの場所
: 有効な値は以下のとおりです。

  - stdout - console ログ・ライターと共に使用します。
  - stderr - console ログ・ライターと共に使用します。
  - *absolute path* - file ログ・ライターと共に使用します。

ファイル名
: 情報の書き込み先となる標準製品ログ・ファイルを示します。ファ

イル名拡張子によってログ・ファイルのタイプが決まります。有効なログ・ファイル拡張子名は以下のとおりです。

- .err
- .bad
- .msg
- .SqlDebug.log
- .SqlErr.log
- .MQErr.log

パラメーター

オプションのロギング・パラメーターを指定します。有効な値は以下のとおりです。

style=bare

ロギングにタイム・スタンプや他のヘッダー情報を組み込まないことを示します。このパラメーターは、通常、UMF メッセージを記録するファイルに組み込まれます。

rotateSize=*maximum file size number*

ログ・ファイルの最大ファイル・サイズをキロバイトで示します。ファイルがこの最大ファイル・サイズを超えると、システムは自動的にログ・ファイルをアーカイブし、ロギング用に使用する新規ログ・ファイルを作成します。システムは、アーカイブ・ファイル名に 0 を付加し、新規ファイルが元のファイル名になります。システムが `keep` パラメーターで指定されたアーカイブ・ファイルの最大数に達するまで、この処理が続行されます。

keep=*maximum number of archive files*

`rotateSize` パラメーターに基づいて、自動ファイル循環時に維持するアーカイブ・ファイルの最大数を示します。ファイルの最大数を超えると、システムは、最も古いアーカイブ・ログ・ファイルに新しいログ情報を上書きします。

空白　ログ・ファイルに配置する空白のタイプを示します。有効な値は以下のとおりです。

- Space
- Tab

フィルター

記録するログ情報を示します。有効な値は以下のとおりです。

モジュール

記録するメッセージのタイプを示します。有効な値は以下のとおりです。

- $NODE_NAME - 汎用メッセージ
- sql - SQL メッセージ
- mq - メッセージ・キュー・メッセージ
- bad_xml - 無効または誤った形式の UMF メッセージ
- msg - UMF 例外

- logger - ロガー・メッセージ

すべてのモジュール・タイプを組み込むには、ワイルドカード文字のアスタリスクを使用します。例:

```
console://stdout *.ERR
```

「重大度 **(Severity)**」

ログ・メッセージの重大度レベルを示します。有効な値は以下のとおりです。

- CRIT - 重大メッセージ
- ERR - エラー・メッセージ
- WARN - 警告メッセージ
- NOTE - 注意
- INFO - 通知メッセージ
- PERF - パフォーマンス・メッセージ
- DBUG - デバッグ・メッセージ

すべての重大度タイプを組み込むには、ワイルドカード文字のアスタリスクを使用します。例:

```
console://stdout *.*
```

いずれかの重大度をレポートから除外するには、感嘆符を使用します。例:

```
console://stdout mq.!DBUG
```

カスタム・パイプライン・ロギングの構成

IBM InfoSphere Identity Insight は、デフォルトのパイプライン・ロギング構成を提供します。このパイプライン・ロギング構成は、デバッグ・モードおよびサービス/デーモン・モードの両方でパイプラインがエラーおよびメッセージを記録する方法を決定します。しかし、デフォルトのパイプライン・ロギング構成を変更することもでき、組織のニーズに合わせてカスタム・ロギング構成を作成することもできます。そのためには、カスタム・ロギング構成を指定する 2 つのロギング・ファイルを作成してから、それらのカスタム・ロギング・ファイルを使用するようにパイプライン構成ファイルを変更する必要があります。

このタスクについて

パイプライン・ロギングはパイプライン・ノード別であるため、それぞれのパイプライン・ノードに対してこれらの変更を行う必要があります。変更を作成した後、デバッグ構成ファイルおよび標準構成ファイルを各パイプライン・ノードにコピーできます。また、あるパイプライン構成ファイルの [logging] セクションから別のパイプライン構成ファイルにテキストをコピーして貼り付けたり、あるパイプライン・ノードから別のパイプライン・ノードにパイプライン構成ファイル全体をコピーしたりすることもできます。必ず、必要に応じて接続設定を調整するようにしてください。

手順

1. 任意のテキスト・エディターを使用して、以下の 2 つのファイルを作成します。

a. デバッグ構成ファイル。デバッグ・モードで作動するパイプラインにロギングを指定する場合に使用します。
b. 標準構成ファイル。サービス/デーモン・モードで作動するパイプラインにロギングを指定する場合に使用します。

2. 各ファイルで、適切なパイプライン・ロギング・コンポーネントを使用して、該当のモードで記録する方法をシステムに指示します。
3. 各ファイルを保存します。パイプライン構成ファイルがあるディレクトリーと同じディレクトリーに、これらのファイルを保存すると便利です。
4. パイプライン構成ファイルに、[logging] という名前の新規セクションを追加します。 このセクションに、作成した 2 つのロギング構成ファイルの名前を指定します。
5. [logging] セクションの見出しの下に、以下の 2 つの設定を追加します。
   a. DebugConfigFile=*debug logging configuration filename*
   b. ConfigFile=*service/daemon logging configuration filename*

   注: パイプライン構成ファイルが置かれているディレクトリー以外のディレクトリーにロギング構成ファイルを保存した場合は、必ずファイルの絶対パスを指定してください。
6. パイプライン構成ファイルに対する変更内容を保存します。

次のタスク

これらのロギングの変更を有効にする前に、影響を受ける各パイプライン・ノード上で実行中のすべてのパイプラインを停止して再始動する必要があります。

Analyst ツールキット Web アプリケーションのログ・ファイル

Web アプリケーションは、IBM InfoSphere Identity Insight との通信および接続を IBM WebSphere Liberty に依存しています。WebSphere Liberty ログ・ファイルには、Web サービス、Analyst ツールキット・アプリケーション、および WebSphere Liberty のエラーに関する情報が含まれています。ご使用のシステムで (Event Manager を使用して) イベント処理を有効にしている場合は、イベント・エラーも Web エラー・ログ・ファイルに記録されます。

アプリケーション・サーバーには、以下の 2 つの 1 次ログ・ファイルが含まれており、これらのログ・ファイルを使用して問題のトラブルシューティングを行うことができます。

- 標準出力とエラー・ストリーム。console.log という名前のファイルに記録されます。
- ロギング・コンポーネントによって収集されたメッセージ。messages.log という名前のファイルに記録されます。このファイルに書き込まれるメッセージには、メッセージのタイム・スタンプや、メッセージを書き込んだスレッドの ID などの追加情報が含まれています。

これらのログ・ファイルは以下のディレクトリーにあります。

installation_directory/wlp/usr/servers/iiServer/logs

WebSphere Liberty ログ・ファイルは、システム・アドミニストレーターによってアプリケーション・サーバー上で構成されます。

Visualizer のログ・ファイル

Visualizer では、ユーザーが Visualizer の問題またはメッセージのトラブルシューティングを行う場合に役立つ 2 つのタイプのログ・ファイルを使用できます。各 Visualizer クライアント用のローカル・ログ・ファイルと、Visualizer をホストする WebSphere Application Server 用のログ・ファイルです。

Visualizer クライアントのロギング

Visualizer を構成して、ローカルの Visualizer クライアントで発生するエラー、警告、および通知メッセージを記録することができます。各ワークステーションには Visualizer クライアントが 1 つ含まれているため、ワークステーションごとに、Visualizer メッセージを記録するか否かを決定できます。

デフォルトでは、Visualizer クライアント・ロギングはオフです。Visualizer のロギングをオンまたはオフにして、「画面設定の構成 **(Configure Screen Preferences)**」ウィンドウの「ログ設定」タブでロギングの設定を選択します。

Visualizer クライアントのロギングをオンにした場合は、ディレクトリーの名前を入力するか既存のディレクトリーを参照して、Visualizer クライアント・ログ・ファイルのディレクトリーの場所を決定します。Visualizer クライアント・ログ・ファイルのデフォルト名は visualizer.log です。このファイルはテキスト・ファイルであるため、任意のテキスト・エディターを使用して表示できます。

最大ファイル・サイズに達するまでは、既存のログ・ファイルにメッセージが追加されます。Visualizer クライアント・ログの最大サイズは 1 メガバイトです。

- ログ・ファイルが最大ファイル・サイズに達すると、システムは、構成されているディレクトリーの場所に別の Visualizer クライアント・ログ・ファイルを作成し、そのログ・ファイルでメッセージのロギングを開始します。
- 2 番目のログ・ファイルが最大サイズの制限に達すると、システムは自動的にメッセージ・ロギングを最初のログ・ファイルに循環させて、そのログ・ファイルがいっぱいになるまで記録します。

現行のログ・ファイルがファイル・サイズ制限に達するたびに、この自動ログ・ファイル循環が継続されます。システムでログ・ファイルが循環されると、そのログ・ファイル内の以前のメッセージが上書きされます。

WebSphere Application Server のロギング

Visualizer は、IBM InfoSphere Identity Insight との通信および接続を WebSphere Application Server に依存しています。Visualizer のイベントは、構成コンソール・ログ・ファイルと共にアプリケーション・サーバー・ログ・ファイルにも記録されます。また、Web サービスのイベントも、Web サービスが WebSphere Application Server に依存しているため、アプリケーション・サーバー・ログ・ファイルに記録されます。

アプリケーション・サーバーには、以下の 2 つの 1 次ログ・ファイルが含まれており、これらのログ・ファイルを使用して問題のトラブルシューティングを行うことができます。

- システム・メッセージ。これは、SystemOut.log という名前のファイルに記録されます。
- システム・エラー・メッセージ。これは、SystemErr.log という名前のファイルに記録されます。

これらのログ・ファイルは以下のディレクトリーにあります。

installation_directory/logs/ewas

WebSphere Application Server ログ・ファイルは、アプリケーション・サーバーのシステム・アドミニストレーターまたは IBM InfoSphere Identity Insight 構成ユーティリティーによって構成されます。

Visualizer クライアントのロギングをオンに設定

以下の手順を使用して、Visualizer クライアントのロギングをオンにし、Visualizer クライアントのロギングに関する設定を構成します。Visualizer クライアントのロギングまたは設定に変更を加える場合は、変更を有効にする前に Visualizer を再始動する必要があります。

このタスクについて

Visualizer クライアントのロギング設定は、ローカルの Visualizer クライアントごとに構成されます。以下の手順を使用してロギングをオンにすることで、このローカル・マシン上の Visualizer クライアントに対してのみ設定が有効になります。

手順

1. 「ファイル」メニューから、「設定」を選択します。
2. 「ログ設定」タブを選択します。
3. 「ロギングをオンにする」チェック・ボックスにある「ログ設定」で、チェック・ボックスを選択してボックス内にチェック・マークが表示されるようにします。(ロギングをオンにする場合、このチェック・ボックスにはチェック・マークを入れる必要があります。)
4. 「ログ詳細レベル」選択ボックスから、ログ詳細のレベルを選択します。
   a. エラー・メッセージの原因となった Visualizer クライアント・イベントをログに記録するには、「エラー」を選択します。 このログ・レベルは、ロギングをオンにした場合のデフォルトのログ・レベルです。このログ・レベルは、パフォーマンス情報とロギング情報をバランス良く提供します。
   b. 警告メッセージまたはエラー・メッセージの原因となった Visualizer クライアント・イベントをログに記録するには、「警告」を選択します。
   c. 通知メッセージ、警告メッセージまたはエラー・メッセージの原因となった Visualizer クライアント・イベントをログに記録するには、「通知」を選択します。
   d. すべての Visualizer イベントのトレース・メッセージをログに記録するには、「デバッグ」を選択します。 このログ・レベルを設定するのは、通常は特定の Visualizer エラーのトラブルシューティングを行う場合のみで、

多くの場合 IBM サポートの支援を受けて使用します。デバッグ・ログ・レベルでは、大量のトレース・メッセージが生成されることがあります。これは、トラブルシューティングには役立ちますが、Visualizer の通常操作のパフォーマンスに悪影響を与える可能性があります。

5. 「ログ・ファイルのディレクトリー・パス **(Log file directory path)**」フィールドで、Visualizer クライアント・ログ・ファイルのディレクトリーの絶対パスおよびファイル名を入力するか、既存のディレクトリーを参照してください。
   - Visualizer クライアント・ログ・ファイルのディレクトリーの絶対パスを入力してください。
   - または、ローカル・マシン上の既存のディレクトリーを参照し、そのディレクトリーを Visualizer クライアント・ログ・ディレクトリーとして選択してください。
6. 「送信 **(Submit)**」ボタンをクリックして変更を保存します。
7. Visualizer からログアウトしてから再びログインし、Visualizer を再始動します。 Visualizer クライアントのロギング設定に行った変更は、Visualizer を再始動するまでは有効になりません。

Visualizer クライアントのロギングをオフに設定

以下の手順は、Visualizer クライアントのロギングをオフにするために使用します。これは特に、デバッグ・レベル・ロギングをオンにして Visualizer の特定の問題のトラブルシューティングを行う場合に使用します。ログ・ファイルは問題のトラブルシューティングに役立ちますが、デバッグ・ログ・レベルなど、一部のレベルのロギングは、Visualizer のパフォーマンスに影響を与える可能性があります。Visualizer クライアントのロギングまたは設定に変更を加える場合は、変更を有効にする前に Visualizer を再始動する必要があります。

始める前に

アクティブな Visualizer セッションにログインしていることを確認してください。

このタスクについて

Visualizer クライアントのロギング設定は、ローカルの Visualizer クライアントごとに構成されます。以下の手順を使用してロギングをオフにすることで、このローカル・マシン上の Visualizer クライアントに対してのみ設定が有効になります。

手順

1. 「ファイル」メニューから、「設定」を選択します。
2. 「ログ設定」タブを選択します。
3. 「ロギングをオンにする」チェック・ボックスにある「ログ設定」で、チェック・ボックスを選択してボックス内にチェック・マークが表示されないようにします。(ロギングをオフにする場合、このチェック・ボックスは空でなければなりません。) ロギングをオフにすると、ロギングの構成設定が無効になります。
4. 「送信 **(Submit)**」ボタンをクリックして変更を保存します。
5. Visualizer からログアウトしてから再びログインし、Visualizer を再始動します。 Visualizer クライアントのロギング設定に行った変更は、Visualizer を再始動するまでは有効になりません。

Event Manager ログ・ファイル

ご使用のシステムが Event Manager を使用してイベントを処理できるようになっている場合、システムはイベントに関するプログラム情報が含まれたログ・ファイルを作成します。外部イベント・プロセッサーからのエラー・メッセージは、WebSphere Liberty エラー・ログ・ファイルに記録されます。パイプライン処理中に検出された標準パイプライン・エラーは、現行のパイプライン・ロギング構成に基づいて、パイプライン・ログ・ファイルに記録されます。

アプリケーション・サーバーには、Event Manager のメッセージおよび問題のトラブルシューティングに使用できる 1 次ログ・ファイルが含まれています。

- Event Manager プログラム情報。これは、gem_prog_*date*.log という名前のファイルに記録されます。
- Event Manager エラー・メッセージ。これは、*installation_directory*/logs ディレクトリー内に記録されます。

メッセージは、イベント日付に基づいてプログラム・ログおよびデータ・ログに追加されます。これらのログ・ファイルを定期的に確認し、組織のポリシーに従ってアーカイブまたは削除する必要があります。

これらのログ・ファイルは以下のディレクトリーにあります。

installation_directory/logs

トレース

トレースは、コンポーネント処理またはトランザクション処理のレコードです。トレースで収集された情報は、問題およびパフォーマンスを評価するために使用できます。IBM InfoSphere Identity Insight では、トレースはデバッグ・コンポーネント・ロギングの一部です。

フィックスの入手

問題を解決するために製品のフィックスを使用できる場合があります。以下の手順に従って、製品のフィックスをダウンロードできます。

手順

1. 必要なフィックスを判別します。http://www-1.ibm.com/support/docview.wss?rs=2216&uid=swg27008307にある *IBM InfoSphere Identity Insight* のバージョン別フィックス *(Fixes by version for IBM InfoSphere Identity Insight)* の文書に進み、リストされているフィックスのいずれかをクリックすると、その特定バージョンのすべてのフィックスに関する詳細情報が表示されます。(フィックスは、バージョン、リリース、モディフィケーションの形式でリストされています。)
2. フィックスをダウンロードします。フィックス・リストから、「ダウンロード (Download)」情報リンクをクリックします。「ダウンロード・パッケージ (Download package)」セクションで、ご使用の環境に対応する「ダウンロード・オプション (Download Options)」リンクをクリックします。

- IBM ご使用条件の画面が表示されたら、情報を読み、ご使用条件に同意してフィックスのダウンロードを続行する場合は「同意する **(I Accept)**」をクリックします。
- 「同意しない **(I Do Not Accept)**」をクリックすると、フィックスはダウンロードされません。

「ファイルのダウンロード **(File Download)**」ウィンドウで、「保存 **(Save)**」をクリックしてフィックス・ファイルをローカルに保存します。

3. フィックスを適用します。フィックス・ファイルを保存した場所に移動します。zip されたフィックス・ファイルを解凍 (unzip) して、「readme」文書の指示に従ってフィックスをインストールしてください。

フィックスおよびサービス更新の概要

IBM InfoSphere Identity Insight で問題が生じた場合は、まず推奨される更新のリストを調べて、ご使用のソフトウェアが最新の保守レベルになっていることを確認してください。次に、修正された問題のリストを調べて、IBM が既にその問題を解決するための個別フィックスを公開しているかどうかを確認します。

個別フィックスは、製品の問題点を解決する必要が生じるたびに公開されます。さらに、フィックスパックとリフレッシュ・パックと呼ばれる 2 種類のフィックスの累積コレクションが定期的に公開され、ユーザーに最新の保守レベルが提供されます。問題を回避するには、こうした更新パッケージをできるだけ早くインストールする必要があります。

フィックスおよび更新の通知を毎週受け取るには、My サポートの E メールによる更新情報をサブスクライブしてください。

以下の表に、それぞれの保守配信手段の特性について示します。

表 *39.* フィックス、フィックスパック、およびリフレッシュ・パックの特性

名前	特性
フィックス	• 更新から次の更新までの間に、特定の問題を解決するために公開される単一のフィックス (例えば、PQ79582)。 • フィックスをインストールしたら、フィックスを適用されたコンポーネントにより影響を受ける機能をすべてテストしてください。

表 39. フィックス、フィックスパック、およびリフレッシュ・パックの特性 (続き)

名前	特性
フィックスパック	• 前回のフィックスパックまたはリフレッシュ・パック以降に公開されたすべてのフィックスを含む、累積的なフィックス・パッケージ。フィックスパックには、新しいフィックスが入っている場合もあります。 • フィックスパックによって製品のモディフィケーション・レベルが上がり、それに合わせてフィックスパックの名前が付けられます (例えば、4.0.2)。 • フィックスパックは特定のコンポーネントを更新する場合も、製品イメージ全体を更新する場合もあります。 • フィックスパックのインストール時に、以前に適用されたフィックスはすべて自動的にアンインストールされます。 • リフレッシュ・パックのインストール後は、重要なすべての機能についてリグレッション・テストを実施してください。 • 最新の 2 個のフィックスパックがダウンロード可能です (例えば、4.0.2 および 4.0.1)。それ以前のフィックスパックは利用できません。
リフレッシュ・パック	• 前回のフィックスパックまたはリフレッシュ・パック以降に公開されたすべてのフィックス、および新規フィックスが含まれる累積フィックス・パッケージ。 • リフレッシュ・パックには通常、フィックスに加えて新規機能も含まれており、製品イメージ全体が更新されます。 • リフレッシュ・パックによって製品のモディフィケーション・レベルが上がり、それに合わせてリフレッシュ・パックの名前が付けられます (例えば、4.0.2)。 • リフレッシュ・パックのインストール時に、以前に適用されたフィックスはすべて自動的にアンインストールされます。 • リフレッシュ・パックのインストール後は、重要なすべての機能についてリグレッション・テストを実施してください。

サービス更新

サービス更新は、ご使用のシステムを最新のソフトウェア保守レベルに保つために役立ちます。

IBM InfoSphere Identity Insight 製品サポート・ページから最新のサービス更新にアクセスできます。URL は次のとおりです

```
https://www-947.ibm.com/support/entry/portal/Overview/Software/
Information_Management/InfoSphere_Identity_Insight
```

ご使用のシステムのパイプライン・サービス・レベルを判別するには、以下のようにします。

1. パイプライン・ノードのコマンド行で、以下のコマンドを入力します。

```
pipeline
```

2. パイプラインのバージョンは最初の行に示されています。この数値でサービス・レベルを特定します。

ご使用のシステムの構成コンソールのサービス・レベルを判別するには、以下のようにします。

1. 構成コンソールを開始します。
2. 構成コンソールにログインします。
3. 上部メニューから「製品情報 **(About)**」を選択します。
4. 「製品情報 (About)」ウィンドウにリストされているバージョン番号を見つけます。この数値でサービス・レベルを特定します。

IBM ソフトウェア・サポートへの連絡

IBM ソフトウェア・サポートは、製品の障害に関する支援を提供します。

始める前に

IBM ソフトウェア サポートに問い合わせるには、お客様の会社が有効な IBM ソフトウェア保守契約を結んでいること、およびお客様が IBM に問題を送信することを許可されていることが必要です。利用可能な保守契約の種類については、「*Software Support Handbook*」(techsupport.services.ibm.com/guides/services.html) の『Enhanced Support』を参照してください。

このタスクについて

問題について IBM ソフトウェア・サポートに連絡するには、以下の手順を実行します。

手順

1. 問題を明確にし、背景情報を収集し、問題の重大度を判断します。詳しくは、「*Software Support Handbook*」 (techsupport.services.ibm.com/guides/beforecontacting.html) の『Contacting IBM』を参照してください。
2. 診断情報を収集します。
3. IBM ソフトウェア・サポートを支援するために、問題レポートで以下の情報を提供できるように準備してください。
   - 製品の名前およびバージョン
   - データベースのタイプおよびバージョン
   - オペレーティング・システムの名前およびバージョン
4. 以下のいずれかの方法で問題を IBM ソフトウェア・サポートにお送りください。
   - オンライン: IBM ソフトウェア・サポート・サイト (http://www.ibm.com/software/support/probsub.html) の「**Submit and track problems**」をクリックします。
   - 電話: お住まいの国でおかけになる電話番号については、「IBM Software Support Handbook」(techsupport.services.ibm.com/guides/contacts.html) の「Contacts」のページにアクセスしてください。

次のタスク

お送りいただいた問題がソフトウェアの欠陥、資料の不足、資料の不正確さに関するものの場合、IBM ソフトウェア・サポートではプログラム診断依頼書 (APAR) を作成します。この APAR には該当の問題が詳細に記載されます。IBM ソフトウェア・サポートでは、APAR が解決されてフィックスが配布されるまでの間実装できる回避策を可能な限り提供しています。IBM では、解決済みの APAR をソフトウェア・サポート Web サイトで毎日公開しています。これにより、同じ問題を抱える別のユーザーが同じ解決策を利用できるようになります。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。 IBM InfoSphere Identity Insight バージョン 9.0。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。 IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することが

できます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

本書では、IBM の商標および IBM 以外の商標の一部につき、それぞれが最初に出現する個所でマークを付けています。

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

インテル、Intel、Intel ロゴ、Intel Inside、Intel Inside ロゴ、Centrino、Intel Centrino ロゴ、Celeron、Xeon、Intel SpeedStep、Itanium、および Pentium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ナ行]

[ハ行]

[マ行]

[ヤ行]

[ラ行]

［ワ行］

A

B

C

D

E

V

W

X

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21