IBM InfoSphere Identity Insight

Guide d'utilisation

Version 9 Edition 0

SC11-7004-00

IBM InfoSphere Identity Insight

Guide d'utilisation

Version 9 Edition 0

SC11-7004-00

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales à la section «Remarques», à la page 423.

Notice d'édition

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Cette édition s'applique à la version 9 édition 0 d'IBM InfoSphere Identity Insight (référence produit 5724-L71) ainsi qu'à toutes les éditions et modifications ultérieures sauf indication contraire dans les nouvelles versions.

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	**IBM Canada**
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Préface

IBM InfoSphere Identity Insight aide les organisations à résoudre les questions relatives à la détermination de la véritable identité d'une personne ou d'un objet ("qui est qui") et à la reconnaissance de la valeur ou du risque potentiel de certaines relations ("qui connaît qui") entre clients, employés, fournisseurs et autres forces externes. Cette analyse est effectuée en temps réel dans le contexte d'applications professionnelles existantes. IBM InfoSphere Identity Insight fournit des informations immédiates et exploitables permettant de prévenir des vols, fraudes, abus et collusions, dans tous les secteurs.

A propos de cette publication

IBM InfoSphere Identity Insight V8.1 est une plateforme de résolution d'entité et d'analyse pour lutter contre les menaces et la fraude. Le présent guide fournit des informations sur la façon d'utiliser et d'appliquer une technologie de désambiguïsation des identités et des relations pour permettre à votre société de déterminer qui est qui, qui connaît qui, et qui fait quoi. En accumulant des contextes d'identité, InfoSphere Identity Insight V8.1 utilise différentes sources d'informations pour déterminer si les personnes sont réellement ce qu'elles déclarent être. Vous pouvez appliquer des algorithmes d'identité complexes et des analyses de noms multiculturelles brevetées pour déterminer si une personne a déjà été identifiée, si elle est nouvelle dans votre société ou si des suppositions antérieures doivent être corrigées en fonction de nouvelles informations.

Public visé

Le présent guide s'adresse aux administrateurs système, aux développeurs d'applications, aux analystes de données et au personnel IBM Professional Services pour utiliser efficacement le produit au sein de votre environnement.

Prérequis et informations connexes

Ce guide d'utilisation est un extrait des informations disponibles dans le centre de documentation en ligne (http://publib.boulder.ibm.com/infocenter/easii/v8r1m0/index.jsp). Il vous est fourni pour faciliter l'utilisation du logiciel. D'autres sources d'informations du produit comprennent :

- IBM InfoSphere Identity Insight version 8, édition 1 - Notes sur l'édition
- Documentation du serveur WebSphere Application Server
- Documentation relative à votre logiciel de base de données
- Documentation du logiciel IBM Cognos Business Intelligence
- Documentation du logiciel IBM ILOG Visualization
- Selon votre déploiement, l'une des informations suivantes :
  - Documentation relative à votre logiciel de mise en file d'attente
  - Documentation relative à votre logiciel de correction d'adresse
  - Documentation relative à votre outil ETL

Envoi de commentaires

Votre avis est important. Il nous aide à fournir des données précises et de qualité. Si vous souhaitez nous envoyer vos commentaires concernant ce manuel ou tout autre documentation relative à IBM InfoSphere Identity Insight, utilisez le formulaire suivant :

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

Vous pouvez également accéder au centre de documentation et utiliser les formulaires de commentaires imbriqués et les options de commentaires associées.

Joindre l'assistance logicielle IBM

L'assistance logicielle IBM fournit une aide en cas d'incident survenu avec ce produit.

Avant de commencer

Avant de contacter l'assistance logicielle IBM, votre société doit disposer d'un contrat de maintenance logicielle IBM en vigueur, et vous devez être autorisé à soumettre des problèmes à IBM. Pour tout renseignement sur les types de contrats de maintenance disponibles, voir la rubrique «Enhanced Support» du manuel *Software Support Handbook*, à l'adresse techsupport.services.ibm.com/guides/services.html

Pourquoi et quand exécuter cette tâche

Pour joindre l'assistance logicielle IBM au sujet d'un incident, procédez comme suit :

Procédure

1. Définissez l'incident, déterminez sa gravité et recueillez des informations sur le contexte. Pour obtenir de l'aide, voir la rubrique «Contacting IBM» du manuel *Software Support Handbook*, à l'adresse techsupport.services.ibm.com/guides/beforecontacting.html
2. Rassemblez des données de diagnostic.
3. Préparez-vous à indiquer les informations suivantes dans le rapport d'incident, afin d'aider le service d'assistance logicielle IBM :
   - Nom et version du produit
   - Nom et version de la base de données
   - Nom et version du système d'exploitation
4. Soumettez votre problème à l'assistance logicielle IBM, par l'une des méthodes suivantes :
   - En ligne : cliquez sur **Submit and track problems**, sur le site d'assistance logicielle IBM, à l'adresse http://www.ibm.com/software/support/probsub.html
   - Par téléphone : pour connaître le numéro à composer depuis votre pays, consultez la page Contacts du manuel IBM Software Support Handbook, à l'adresse techsupport.services.ibm.com/guides/contacts.html

Que faire ensuite

Si l'incident que vous soumettez concerne un défaut logiciel ou une documentation manquante ou inexacte, l'assistance logicielle IBM crée un rapport officiel d'analyse de programme (APAR). Cet APAR décrit l'incident en détail. Dans la mesure du possible, l'assistance logicielle IBM fournit un palliatif que vous pouvez utiliser jusqu'à ce que l'APAR ait été résolu et qu'un correctif ait été diffusé. IBM publie quotidiennement les APAR résolus, sur le site Web de l'assistance logicielle, afin que les autres utilisateurs confrontés au même problème puissent bénéficier de la même solution.

Chapitre 1. Présentation d'IBM InfoSphere Identity Insight

IBM® InfoSphere Identity Insight permet aux entreprises de résoudre des problèmes liés à la reconnaissance de la véritable identité de quelqu'un ou de quelque chose ("qui est qui") et de déterminer l'évaluation de l'intérêt ou le danger des relations ("qui connaît qui") entre les clients, les employés, les vendeurs et d'autres forces externes. IBM InfoSphere Identity Insight fournit des informations immédiates et exploitables permettant de prévenir des vols, fraudes, abus et collusions, dans tous les secteurs.

Dans nombre d'entreprises, les données brutes qui représentent les identités et relations existent déjà. L'inconvénient de la plupart des systèmes, c'est qu'ils n'offrent aucun moyen simple de gérer, analyser et résoudre le volume de données qui vous est nécessaire pour en tirer un discernement optimal.

Avec IBM InfoSphere Identity Insight, les entreprises peuvent gérer, analyser et intégrer des données en temps réel à partir de n'importe quelle source, notamment des bases de données de clients, listes de fournisseurs, bases de données d'employés, listes de conformité légales et sources de données en flux continu. IBM InfoSphere Identity Insight envoie des alertes en temps réel aux analystes, personnels de sécurité et autres pour une recherche plus approfondie. IBM InfoSphere Identity Insight contribue également à identifier la valeur du réseau des clients ou leur segment de marché, grâce à une vison exhaustive de la clientèle.

Grâce à IBM InfoSphere Identity Insight, les entreprises peuvent bâtir une base de données d'entités centrale et dynamique pouvant faire office de plateforme pour l'ensemble de leurs applications cognitives. IBM InfoSphere Identity Insight s'intègre à d'autres système d'entreprise via un large éventail de protocoles et technologies.

Reconnaissance des identités

Fort de son processus fondamental de résolution d'entité, IBM InfoSphere Identity Insight résout les fiches d'identité incohérentes et ambiguës, issues de multiples fichiers, en entités exhaustives, en déjouant les tentatives de duperie délibérées.

Au cours de la résolution d'entité, IBM InfoSphere Identity Insight :

- Détermine quand plusieurs fiches qui semblent correspondre à des entités différentes sont en fait une seule et même entité.
- Pour chaque entité résolue, fusionne les fiches d'identité disparates en une vue composite de l'entité, tout en consignant l'historique d'attribution intégrale de chaque fiche. L'attribution intégrale garantit que les données ne soient jamais perdues et qu'il soit toujours possible de remonter à leur source originale.
- A mesure que de nouvelles données se chargent dans le système, IBM InfoSphere Identity Insight met à jour et gère en contexte les informations sur les entités de la base de données d'entités. Il peut parfaitement cerner la signification de données nouvelles ou modifiées, au fil de leur chargement, en tirant ainsi le meilleur parti de chaque transaction et en optimisant la vision exhaustive de chaque entité de la base de données.

Détection des relations

S'appuyant sur le processus de relation d'entité, IBM InfoSphere Identity Insight détecte les relations entre entités dans la base de données d'entités à mesure que des fiches provenant de multiples sources de données sont chargées et traitées.

Au cours du processus de résolution d'entité, IBM InfoSphere Identity Insight :

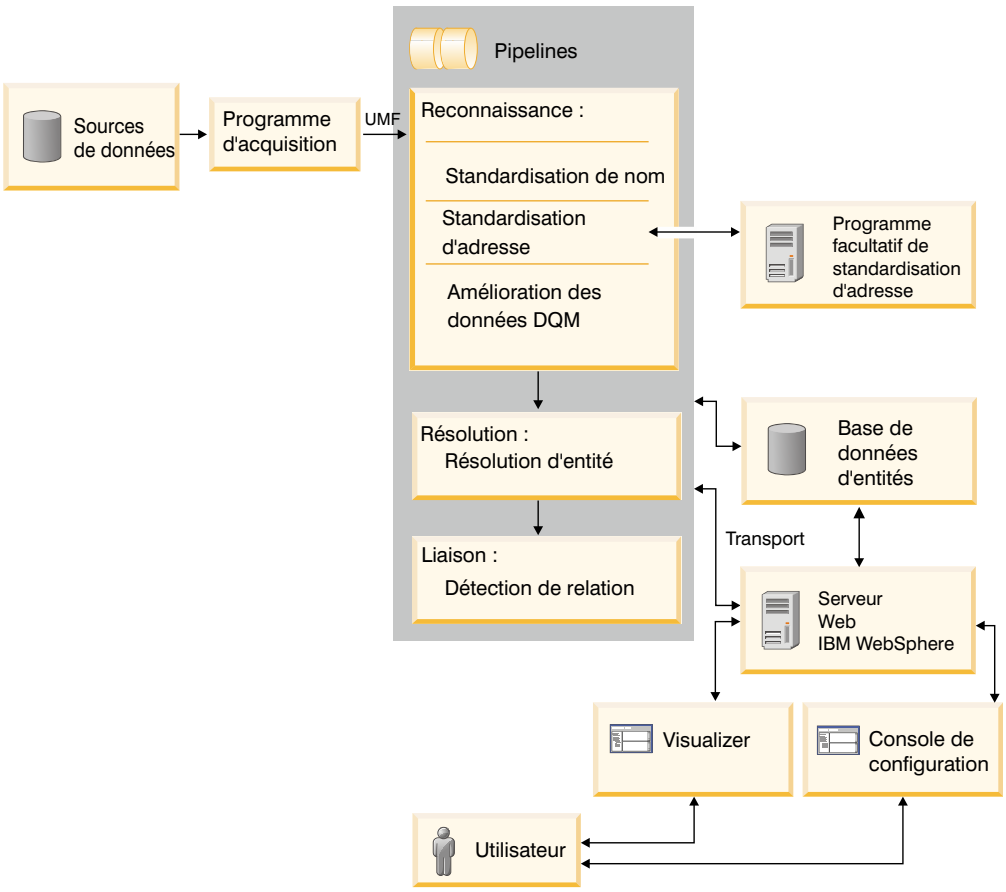
- Relie les entités par attributs d'identité, tels que numéros de téléphone et adresses, afin de repérer les relations pertinentes, quoi que non flagrantes.
- Assemble les réseaux d'associations et entités au moyen des attributs de données individuels (tels que numéros d'identification et noms), des emplacements (tels qu'adresses IP), des infrastructures (entrepôts, écoles, aéroports, hôtels, etc.), des organismes (comités, clubs, associations, bandes, etc.), de critères financiers (espèces, virements, etc.), et de comptes (carte de fidélité, compte bancaire, compte chèque, compte de crédit ou compte épargne).
- Identifie les relations suspectes ou intéressantes, y compris celles qui sont dissimulées ou déguisées, et envoie des alertes en temps réel, selon un ensemble de règles définies par l'utilisateur. IBM InfoSphere Identity Insight permet aux analystes et investigateurs de mener des recherches élaborées dans la base de données d'entités afin d'étudier davantage chaque entité apparentée et chaque entité ou attribut auquel ces entités sont liées.

IBM InfoSphere Identity Insight prend également en charge les rapports sur les exceptions personnalisables par règle, afin que les entreprises puissent désigner les entités résolues ou les relations détectées qui déclenchent des alertes.

Architecture du produit

IBM InfoSphere Identity Insight est un système multiniveaux dans lequel les données issues de sources de données sont chargées dans le système à partir de programmes d'acquisition et traitées par les pipelines hébergés sur les noeuds de pipelines. Les résultats de ce traitement sont transcrits dans la base de données des entités et peuvent être acheminés vers d'autres systèmes ou bases de données.

Dans le cadre d'un déploiement standard, les données professionnelles de plusieurs sources de données sont envoyées aux programmes d'acquisition, dans lesquels elles sont converties au format UMF (Universal Messaging Format). Chaque programme d'acquisition fait appel à un transport pour l'envoi des données à un ou plusieurs pipelines. La plupart de ces transports sont bidirectionnels et le système peut être configuré de façon à fournir des réponses au programme d'acquisition.



Un ou plusieurs processus de pipelines s'exécutent sur les noeuds de pipelines. Chaque pipeline gère sa propre connexion à la base de données des entités. Au fur et à mesure que le pipeline reçoit les données UMF d'un ou plusieurs programmes d'acquisition, il traite une à une les fiches via ses trois processus de base : reconnaissance, résolution et lien. Dès que le traitement d'une fiche est terminé, le pipeline en stocke les résultats dans la base de données des entités.

Les utilisateurs peuvent interagir avec le système via les interfaces suivantes :

- la console de configuration, qui permet de configurer et de contrôler le système ;
- les applications Analyst Toolkit, qui permettent d'analyser et de gérer les alertes, d'étudier les relations, d'effectuer des recherches et de générer des rapports ;
- les interfaces de ligne de commande, qui permettent d'exécuter les pipelines ;
- les services Web, qui permettent d'exécuter les pipelines ou d'intégrer le produit à d'autres systèmes professionnels, notamment à des interfaces utilisateur personnalisées.

IBM InfoSphere Identity Insight utilise IBM WebSphere Liberty. Ce serveur d'application héberge la console de configuration, les élément d'Analyst Toolkit, ainsi que les services Web.

Cette architecture robuste offre une grande évolutivité pour tous les types de déploiement. Les pipelines peuvent être déployés sur plusieurs machines, petites ou grosses. Leurs performances peuvent atteindre n'importe quel niveau, à condition que les bases de données aient une capacité suffisante.

Programmes d'acquisition

Un programme d'acquisition contient les outils et programmes qui permettent d'obtenir des données, de les convertir au format UMF (Universal Message Format) et d'envoyer ces données converties au pipeline pour traitement.

Pour convertir des données au format UMF, vous pouvez utiliser comme programme d'acquisition soit les utilitaires fournis avec le produit, soit des outils d'extraction transformation et chargement tels que WebSphere QualityStage.

Format UMF (Universal Message Format)

Le format UMF (Universal Message Format) est un dialecte XML extensible qui sert à structurer les fichiers de sources de données. Il contient des balises standard qui représentent des éléments clés des identités, des relations et des activités. Pour que les pipelines puissent traiter les données, celles-ci doivent être converties au format UMF et doivent correspondre à la spécification UMF.

Le format UMF est constitué des composants hiérarchiques suivants :

UMF, documents
Collection de segments UMF structurant les données et indiquant le type de la fiche de source de données.

Segments UMF
Partie du document UMF qui structure les données de la source de données.

Eléments UMF
Valeurs et balises XML définissant les données d'un segment UMF d'un document UMF.

La spécification UMF répertorie les types spécifiques des documents UMF, des segments UMF de chaque type de document UMF ainsi que les éléments UMF valides de chaque segment UMF.

Pipelines

Les pipelines sont les composants qui effectuent la standardisation et l'uniformisation de nom et d'adresse, la gestion de la qualité des données et la résolution d'entité. Ils réalisent également la résolution des relations et génèrent des alertes en fonction de la configuration du système.

Les pipelines exécutent trois processus de base :

- Reconnaissance - impliquant l'optimisation des données entrantes via la vérification de la standardisation, du nettoyage, de l'amélioration et de la qualité
- Résolution - impliquant la résolution d'entités
- Lien - impliquant la détection de relations et la génération d'alertes

Les pipelines sont hébergés par des noeuds.

Vous pouvez configurer les pipelines pour un traitement en parallèle, de façon à ce qu'une commande pipeline génère plusieurs unités d'exécution en parallèle des pipelines, ce qui permet au système de traiter simultanément plusieurs requêtes de données. Cette fonctionnalité permet d'améliorer les performances du système, de réduire le temps de traitement des données et de limiter les contraintes de mémoire liées au matériel.

La configuration de la fonctionnalité de traitement en parallèle des pipelines s'effectue à deux endroits différents :

- Le paramètre de simultanéité globale est contrôlé par le paramètre système `Accès concurrent par défaut du pipeline` de l'onglet **Configuration système**, dans la console de configuration. La valeur indiquée ici définit le nombre d'unités d'exécution en parallèle qui sont démarrées à partir de la commande de démarrage d'un pipeline. La valeur par défaut de ce paramètre est 1, ce qui signifie que sauf modification du paramètre, une seule unité d'exécution de traitement de pipeline démarre.
- Il est possible de configurer un paramètre d'accès concurrent local (par noeud de pipeline) dans le fichier de configuration du pipeline. Si vous indiquez un paramètre d'accès concurrent et une valeur dans le fichier de configuration du pipeline par noeud de pipeline, cette valeur remplace celle du paramètre système global. Lorsque vous émettez une commande de démarrage du pipeline sur ce noeud, vous démarrez le même nombre d'unités d'exécution de pipeline en simultané que celui indiqué dans le fichier de configuration du pipeline.

Noeuds de pipelines

Les noeuds de pipelines sont les machines physiques qui hébergent un ou plusieurs processus de pipelines.

Le noeud de pipeline est l'endroit où vous installez et démarrez l'exécutable des processus d'un pipeline. Vous configurez et gérez le fichier de configuration de tous les pipelines hébergés sur cette machine. Le système inscrit également les messages du pipeline dans les fichiers journaux qui se trouvent sur les noeuds du pipeline.

Les noeuds de pipelines assurent la connexion entre les processus du pipeline et les composants de l'architecture du produit suivants :

Programmes d'acquisition
Dans le cadre du processus d'extraction, transformation et chargement, les programmes d'acquisition utilisent des transports pour envoyer des données UMF aux pipelines pour traitement. Vous devez utiliser le mode de transport approprié au type de programme d'acquisition pour vous connecter aux pipelines. Par exemple, si vous utilisez l'utilitaire de fichier UMF comme programme d'acquisition, utilisez le transport Fichier.

Base de données des entités
La base de données des entités contient des informations relatives aux entités. Les pipelines accèdent à ces informations lors du traitement des fiches entrantes pour la résolution des entités et des relations. Pour que les pipelines puissent accéder à la base de données des entités, le client de base de données approprié doit être installé et configuré sur le noeud de pipeline.

Files d'attente
Si votre système fait appel à des files d'attente comme mode de transport pour l'envoi pour traitement de données aux pipelines, vous devez installer et configurer le logiciel Message Queuing approprié sur chaque noeud de pipeline.

Serveurs de nettoyage d'adresses
Si votre système utilise des produits de nettoyage d'adresses d'autres société, chaque noeud de pipeline doit être configuré de telle sorte qu'il puisse se connecter aux serveurs de nettoyage d'adresses.

Services Web

Vous devez utiliser un transport HTTP pour connecter les processus de pipeline du noeud de pipeline aux services Web.

Application Monitor

La console de configuration comprend un composant Application Monitor qui vous permet de contrôler les pipelines (état, statistiques et erreurs) et d'acheminer les résultats entre pipelines ainsi que vers d'autres systèmes ou bases de données.

Pour tirer parti de Application Monitor, vous devez enregistrer les pipelines que vous souhaitez contrôler ou à partir desquels vous souhaitez acheminer des résultats dans la console de configuration.

Contrôle des pipelines

Application Monitor fonctionne avec un agent SNMP qui s'exécute sur le noeud de pipeline qui héberge les pipelines que vous souhaitez contrôler. L'agent SNMP envoie à Application Monitor des statistiques relatives à tous les pipelines enregistrés d'un noeud de pipeline, qui les publie dans la console de configuration. Application Monitor actualise l'état et les statistiques des pipelines toutes les 60 secondes.

Acheminement des résultats des pipelines

Application Monitor vous permet d'acheminer les résultats des données traitées par les pipelines vers d'autres systèmes ou bases de données. Pour configurer les règles d'acheminement des résultats du traitement d'un pipeline, utilisez la console de configuration, qui permet d'indiquer le pipeline à partir duquel procéder à l'acheminement ainsi que la destination de l'acheminement.

Par exemple, au lieu que les analystes créent des requêtes de rapport par rapport à la base de données des entités (qui peut être très volumineuse), certaines entreprises choisissent d'acheminer un sous-ensemble des résultats vers une base de données de rapports. Les analystes créent alors leurs requêtes de rapport d'investigation par rapport à cette base de données de rapports, qui ne contient que les informations sur les entités et les relations dont ils ont besoin.

Transports

Les transports permettent de déplacer des données d'un endroit à un autre : entre programmes d'acquisition et pipelines, entre pipelines et base de données des entités et même entre pipelines et systèmes externes.

Pour transporter des données, vous devez utiliser un format de syntaxe spécifique au type du mode de transport utilisé, qui comprend un URI (ID ressource universel).

IBM InfoSphere Identity Insight prend en charge plusieurs méthodes de transport :

- Bases de données
- Fichiers
- HTTP
- Files d'attente de messages (IBM WebSphere MQ)

Sources de données

Les sources de données contiennent les identités que vous souhaitez traiter pour la résolution des entités et le chargement dans la base de données correspondante. Elles contiennent des données d'identification (identificateurs personnels uniques d'une identité) ainsi que d'autres types de données (autres attributs et points de données d'une identité). Les fiches d'identités de la source de données doivent être exportées au format UMF (Universal Message Format) pour que le système puisse les traiter ou pour qu'elles puissent être chargées dans la base de données des entités. Voici quelques exemples, entre autres, de sources de données : listes d'employés, de surveillance, de clients ou encore listes de fournisseurs.

Les sources de données contiennent des informations vitales, telles que celles relatives à la source d'origine (les données d'origine étant été converties au format UMF) ou la référence externe à la source de données. Ces détails font de chaque source de données un élément unique dans le système.

Lors de la résolution d'entités, si deux d'entre elles ne sont pas résolues, le système fait appel aux informations de la source de données pour définir de quelle entité proviennent les informations.

Emplacements des sources de données et systèmes source

Vous pouvez classer les sources de données entrantes en créant des emplacements source et des systèmes source et en établissant ensuite une association avec vos sources de données. Les emplacements source et les systèmes source permettent de faire la distinction entre des types de sources de données similaires.

Par exemple, si vous traitez des données de réservation et des données de ressources humaines à partir de plusieurs emplacements, un emplacement de source de données vous permet de définir l'emplacement qui contribue aux données :

- Propriété X, Données de réservation
- Propriété X, Données de ressources humaines
- Propriété Y, Données de réservation
- Propriété Y, Données de ressources humaines

Configurations par source de données

Pour optimiser les résultats des opérations de résolution d'entité et de détection de relations, configurez chaque source de données à l'aide des paramètres suivants :

Rôles Les sources de données étant des regroupement de données d'un même type, vous pouvez affecter automatiquement le même rôle à toutes les fiches d'identité d'une même source de données entrante. Par exemple, si vous associez le rôle Employé à une source de données Ressources humaines, ce rôle est automatiquement affecté à toutes les fiches entrantes de la liste des employés.

Niveaux de chargement
Vous pouvez définir si toutes les données d'une source de données entrante doivent être chargées, ou seulement les données qui permettent de résoudre une ou plusieurs entités, ou encore celles qui y sont liées.

Paramètres de résolution de relations
Vous pouvez configurer le niveau de détection de relations en fonction de la source de données. Par exemple, vous pouvez désactiver la fonction de

résolution de relations d'une source de données ou sélectionner le nombre de degrés de séparation pour la détection de relations au sein de cette source de données.

Base de données des entités

La base de données des entités est celle dans laquelle sont stockées les identités, les entités et les données utilisées pour les relations, les résolutions et les alertes.

La base de données des entités constitue le lieu de stockage permanent de toutes les entités résolues et de leurs relations. Au fur et à mesure que les pipelines traitent les fiches UMF entrantes, les nouvelles données sont constamment comparées à celles qui se trouvent déjà dans la base de données des entités. Les opérations de résolution des entités et de détection des relations s'effectuent donc par rapport aux entités composites contenant tous les attributs cumulés de toutes les fiches précédentes.

Interfaces utilisateur

IBM InfoSphere Identity Insight propose plusieurs interfaces utilisateur permettant d'interagir avec les fonctions du produit.

Console de configuration

La console de configuration fournit une interface orientée tâche pour vous aider à effectuer plus facilement certaines des tâches les plus essentielles à la prise en main d'Identity Insight.

La console de configuration est hébergée par IBM WebSphere Liberty.

Gestion de la configuration du système

La console de configuration permet de configurer la plupart des paramètres système et des options dans un ensemble d'interfaces simplifiées et rationalisées. La console écrit ensuite les changements dans la base de données de configuration. Les modifications qui sont apportées directement à la base de données de configuration ne sont pas prises en charge. Elles entraînent le plus souvent un mauvais fonctionnement du produit.

Visualizer

Le Visualizer est une interface utilisateur graphique que les analystes et les investigateurs utilisent pour analyser les résultats des alertes, des relations et des résolutions d'entités.

Le Visualizer est hébergé par une version intégrée d'IBM WebSphere Application Server. Pour configurer le Visualizer , utilisez la console de configuration et les **Préférences** du menu **Fichier**.

Les utilisateurs du Visualizer peuvent réaliser plusieurs tâches d'analyse :

Analyse et définition d'alertes
Les alertes générées par le processus de résolution d'entité représentent les relations ou les résolutions d'entités qui peuvent concerner directement une entreprise. Généralement, les analystes consultent les alertes et décident le cas échéant de l'action à entreprendre, en fonction des informations de l'alerte. Il existe trois types d'alertes : les alertes de rôle, les alertes d'attribut et les alertes d'événements.

Le Visualizer affiche les alertes, offrant aux analystes à la fois un texte et un graphique relatifs à ces alertes ainsi qu'aux entités directement concernées. Les analystes peuvent explorer les détails en aval, puis définir l'état de l'alerte en conséquence.

Création et gestion des générateurs d'alertes d'attribut
Le Visualizer permet aux analystes de créer et gérer des recherches permanentes dans la fonction du générateur d'alertes d'attribut, mais aussi de gérer l'affichage et la réception des alertes d'attribut. Les analystes peuvent créer des générateurs d'alertes d'attribut basés sur des données d'attributs afin de localiser les identités résolues en entités en fonction de ces données d'attributs. Ils peuvent également créer un générateur d'alertes d'attribut afin de rechercher de façon permanente une entité spécifique dans la base de données de l'entité.

Recherche d'entités
Les utilisateurs du Visualizer peuvent également rechercher des entités pour une analyse approfondie à l'aide de plusieurs méthodes :

- Par attribut
- Par compte de source de données
- Par ID d'entité
- Par résolution (dans quelle mesure les critères saisis correspondent aux identités et aux entités dans la base de données de l'entité, en fonction de seuils de score de résolution minimum)

Ajout d'entités et de relations divulguées
Le Visualizer permet aux analystes d'ajouter des fiches pour la résolution d'entités et la détection de relations. Ils peuvent ajouter une seule fiche d'entité ou charger un fichier UMF contenant quelques milliers de fiches d'identités. Comme pour l'ajout de fiches d'identités via un programme d'acquisition, les fiches ajoutées via le Visualizer sont traitées par un pipeline pour la résolution d'entités et la détection de relations. Les résultats de ce traitement sont transcrits dans la base de données des entités et toute alerte est publiée dans le Visualizer .

Les analystes peuvent également divulguer les relations entre des entités (par identité), lorsqu'un lien existe entre des identités. L'association d'entités basées sur des contacts d'urgence ou de références répertoriées sur une application d'emploi est un exemple de relation divulguée. L'entité a révélé ces relations sur l'application.

Génération et impression de rapports
Le Visualizer contient également plusieurs rapports que les analystes peuvent consulter et imprimer afin de gérer et d'effectuer un suivi du travail accompli avec le Visualizer .

Interfaces de ligne de commande

Ce produit utilise des interfaces de ligne de commande pour l'exécution des pipelines. Pour démarrer et arrêter des pipelines, il suffit de saisir des commandes sur une ligne de commande.

Utilitaire de configuration

L'utilitaire de configuration permet aux utilisateurs de consulter et de modifier les paramètres d'installation une fois les correctifs logiciels installés.

Vous pouvez installer des correctifs et des correctifs logiciels pour les applications suivantes :

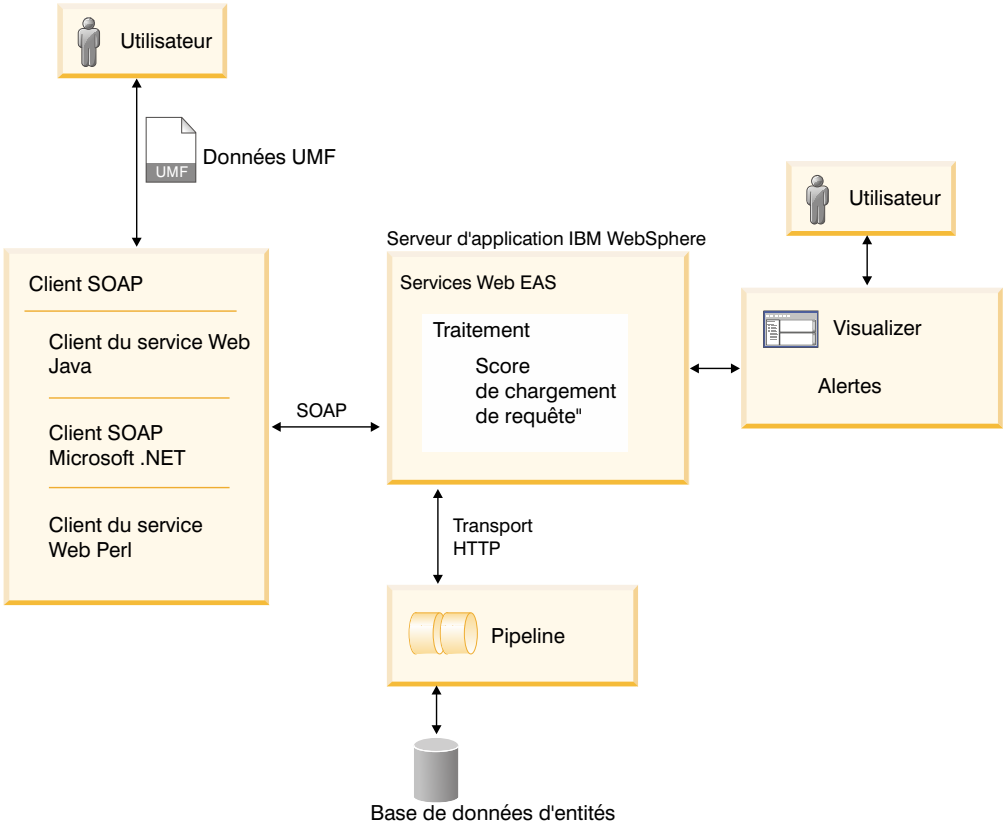
- Console de configuration
- Visualizer
- Rapports du Visualizer
- Application Java™ Web Start
- Services Web
- Application de création de diagramme
- Application de recherche d'entité
- Documentation produit

Vous pouvez aussi modifier les paramètres pour ce qui suit :

- Console de configuration
- Configuration WebSphere
- Connectivité de la base de données
  - Connectivité de la base de données des entités
  - Connectivité de la base de données Application Monitor
  - Connectivité de la base de données de la console de configuration
  - Paramètres JDBC

Services Web

IBM InfoSphere Identity Insight fournit un ensemble de services Web qui vous permettent de créer des applications externes pouvant charger des données UMF (Universal Message Format) pour le traitement pipeline ou la recherche d'entités dans la base de données d'entités. Pour ce faire, utilisez le mode de transport HTTP (hypertext transfer protocol) bidirectionnel, qui est une fonction standard du pipeline.



Les services Web d'IBM InfoSphere Identity Insight utilisent quatre méthodes SOAP (Simple Object Access Protocol) : traitement, recherche, chargement et notation. Ce produit prend en charge SOAP version 1.1.

Le produit comprend plusieurs composants destinés à vous aider lors de vos premières utilisation des services Web.

srd.wsdl
ce fichier contient la définition WSDL (Web services description language) des services Web du produit. Vous pouvez utiliser ce fichier avec n'importe quel toolkit ou technologie SOAP pour lancer les services Web. Pour le trouver, démarrez WebSphere Liberty et chargez-le à partir de http://hostname:port/easws/resources/wsdl/srd.wsdl

wsutil.jar
Ce fichier est un client test de service Web fourni pour tester l'installation et la configuration de vos services Web. Cet utilitaire se trouve dans le répertoire `ibm-home/easws`.

Concepts fondamentaux

Pour utiliser IBM InfoSphere Identity de façon efficace, vous devez comprendre ses concepts clés, comme les entités, les identités et les attributs.

Entités

Une entité est une collection d'une ou plusieurs identités représentant les mêmes personne, organisme, lieu ou élément. Elles sont stockées dans la base de données d'entités.

Bien que les entités soient souvent perçues comme des personnes,il peut également s'agir de choses telles que des entreprises ou des véhicules. En fait, vous pouvez utiliser la configuration extensible du système pour mapper les données de votre organisme et créer n'importe quel type d'entité à résoudre ou apparenter.

Les entités se composent généralement d'identités issues de plusieurs systèmes source différents. La résolution d'entité détermine quelles identités sont en réalité la même entité et crée une entité composite renfermant toutes les identités qui lui sont associées. Le système consigne l'historique d'attribution intégrale des fiches, en identifiant ainsi la source associée à chaque identité de l'entité composite.

Il convient de configurer le système de façon à résoudre et apparenter les entités d'une manière qui satisfasse les objectifs de votre organisme.

Identités

Les identités sont une collection d'attributs issus d'une source de données et représentant une personne, un organisme, un lieu ou un élément.

Via la résolution d'entité, les identités sont résolues et des entités composites sont créées à partir des identités individuelles, lorsque les entités partagent des attributs communs avec l'entité composite.

Il se peut que les identités aient auparavant été désignées par le terme "comptes".

Attributs

Les attributs sont les caractéristiques ou traits qui décrivent une personne, un organisme, un lieu ou un élément. Parmi les attributs courants figurent les informations telles que noms, adresses, numéros de téléphone, numéros de carte de crédit, numéros d'identification fiscale et numéros de permis.

Le système accepte les types d'attributs suivants :

Noms Les attributs de nom définissent le nom de la personne, de l'organisme du lieu ou de l'élément, tels que définis par le modèle d'entité et l'identité entrante. Les attributs de nom représentent généralement des personnes et entreprises, mais ils peuvent s'étendre aux noms de véhicules (voitures, camions, bateaux ou avions), de groupes, ou de n'importe quel autre type d'entité que votre entreprise définit dans son modèle d'entité.

Adresses
Les attributs d'adresse définissent une localisation de l'identité et contiennent généralement les informations d'adresse standard : numéro et nom de rue, numéro du bâtiment, code postal, localité et pays.

Numéros
Les attributs de numéro se composent de données qui sont généralement décrites comme un numéro, tel que numéro de carte de crédit, numéro de téléphone et numéro de passeport. Les numéros ne sont toutefois pas limités aux caractères numériques, car nombre d'entre eux comportent des caractères alphanumériques.

Caractéristiques
Les attributs de caractéristique définissent d'autres traits ou informations identitaires qui ne sont pas exprimés par les autres types d'attributs. Vous pouvez, à l'aide des attributs de caractéristique, personnaliser le système afin de définir les caractéristiques identitaires dont vous souhaitez vous

servir pour résoudre les entités ou détecter les relations. Parmi les types de caractéristique courants figurent la date de naissance et le sexe.

Courriel
Les attributs de courriel définissent les adresses de messagerie Internet. Les adresses électroniques tendent à être uniques ; certaines études suggèrent que les gens enclins à utiliser plus d'un seul nom ont néanmoins tendance à ne se servir que de la même ou des deux mêmes adresses électroniques.

Au format UMF (Universal Message Format), les divers types d'attributs sont exprimés en segments UMF. Chaque type d'attribut est son propre segment UMF.

Résolution d'entité

La résolution d'entité désigne le processus qui résout les entités et détecte les relations. Les pipelines effectuent la résolution d'entité, à mesure qu'ils traitent les fiches d'identité entrantes, en trois phases : reconnaître, résoudre, apparenter.

Reconnaissance

Au cours de la résolution d'entité, les pipelines doivent reconnaître les données en validant, optimisant et rationalisant les données identitaires entrantes. Durant cette phase de reconnaissance du processus de pipeline, les pipelines nettoient et standardisent les valeurs de données, de même qu'ils effectuent des vérifications de la qualité des données afin de protéger l'intégrité de la base de données d'entités.

Gestion de la qualité des données (DQM)

La gestion de la qualité des données (DQM) désigne le processus de pipeline qui vérifie dans les données si les valeurs obligatoires, les types de données valides et les codes valides sont présents. Vous pouvez également configurer la DQM de façon à corriger les données en fournissant des valeurs par défaut, en formatant les numéros et dates et en ajoutant de nouveaux codes.

La gestion de la qualité des données, de même que la standardisation et uniformisation des noms et adresses, vise à optimiser et perfectionner la qualité des données. Cette préparation de la qualité des données est une étape essentielle de la résolution d'entité, car elle accroît la fiabilité des entités résolues et relations détectées qui en résultent.

Pour appliquer la gestion de la qualité aux données chargées dans le système, il faut configurer des règles de gestion de la qualité des données (ou règles DQM). Les règles DQM peuvent accomplir toute une palette d'opérations de réparation, nettoyage et standardisation sur les valeurs de données d'identité entrantes, notamment en formatant convenablement les numéros, en repérant et rectifiant les coquilles ou erreurs de transposition, ainsi qu'en repérant et rectifiant les inexactitudes délibérées introduites par les personnes soucieuses de dissimuler leur identité.

Ce produit est préconfiguré d'origine avec plusieurs règles DQM par segment UMF et qui remédient aux problèmes de qualité de données les plus typiques de ce segment UMF. Vous pouvez néanmoins configurer des règles DQM supplémentaires, au gré des besoins. Toutefois, avant d'y procéder, vous devez être familiarisé avec la qualité originale des données et avec le processus ETL (extraction, transformation et chargement) qui a servi à convertir les données identitaires en UMF. Une fois que vous savez quelle amélioration des données

s'impose, vous pouvez sélectionner les règles DQM, fonctions et valeurs adéquates à appliquer à chaque type de données identitaires nécessitant une optimisation plus poussée.

Exemple d'application d'une règle DQM

Supposons par exemple que le format de date de votre système soit JJ/MM/AAAA. Par contre, dans plusieurs de vos sources de données, les dates sont au format MM-JJ-AAAA. Vous pouvez alors ajouter la règle DQM 204 au segment UMF `<NUMBER>`, en le configurant ainsi de façon à convertir au format de date JJ/MM/AAAA toutes les dates entrantes formatées en MM-JJ-AAAA.

Standardisation et uniformisation de nom :

Au cours du traitement par le pipeline, les noms sont nettoyés et standardisés afin de préparer la fiche d'identité en vue d'un traitement de résolution d'entité optimal.

Les processus du pipeline fournissent les informations de nom les plus précises sur les entités dans l'optique d'un usage actuel, futur et historique. A mesure que des données de nom d'identité nouvelles ou modifiées parviennent au système, elles sont comparées au dictionnaire de standardisation de noms de produit, qui renferme une liste de noms racines et de leurs dérivés connus, afin d'identifier le nom racine. Une fois le nom racine identifié, le système conserve à la fois le nom racine et le nom original pour la fiche d'identité entrante.

Le tableau suivant montre deux exemples de dérivés possibles du même nom racine, dont ses variantes orthographiques. Les noms de gauche sont tous des dérivés du nom racine de droite.

Tableau 1. Exemples de dérivés possibles des noms racines Richard et Mohammad

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

Au besoin, le processus de standardisation et uniformisation de nom corrige en outre toute faute d'orthographe, mais, là encore, en conservant comme renseignements de la fiche à la fois l'orthographe originale et toute correction éventuelle. La plupart des autres systèmes (dont l'ETL et les outil marketing de base de données) ne le font pas.

La standardisation et uniformisation de nom constitue une étape importante pour accroître les niveaux de fiabilité de la résolution d'entité. Ce processus est particulièrement important sachant que l'individu moyen emploie pas moins de cinq variantes de son nom, à des fins administratives et personnelles.

Standardisation et uniformisation d'adresse :

La standardisation et uniformisation d'adresse est le processus par pipeline qui normalise et homogénéise les informations d'adresse afin de corriger des erreurs et transpositions éventuelles et de préparer la fiche d'identité en vue d'un traitement de résolution d'entité optimal.

Dans le cadre du processus de standardisation d'adresse, les pipelines effectuent une analyse syntaxique et standardisent les informations de l'adresse. Par exemple, `Street` par `St` ou `123-A Main St` par `123 Main St Apt A`.

Ce processus par pipeline compare également les informations nouvelles ou modifiées à une base de données globale et à un logiciel de standardisation d'adresse fourni par IBM InfoSphere QualityStage ou par un autre produit de standardisation d'adresse, comme l'application CODE-1 de Group 1 Software. Le produit de standardisation d'adresse choisi détermine si les informations d'adresse sont correctement formatées, détecte et corrige les éventuelles fautes d'orthographe (dans les noms de rue par exemple), et rectifie toute information manquante ou erronée (par exemple en conformant le nom de la localité au code postal et à l'adresse).

Le tableau suivant montre des exemples de nettoyage et uniformisation, de l'adresse originale à l'adresse corrigée standardisée.

Tableau 2. Exemples comparatifs de deux adresses originales avec les adresses standardisées obtenues

Adresse originale	Adresse standardisée

`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`

Le processus de standardisation et d'uniformisation d'adresse conserve à la fois l'adresse d'origine et l'adresse corrigée, améliorant ainsi le niveau de fiabilité de la résolution d'entité et de la détection de relations ultérieures. En outre, la conservation de ces informations fournit au système des données historiques de meilleure qualité.

Vérification de la qualité des données :

A mesure que les données parviennent au système en vue de leur traitement, le pipeline en vérifie la qualité afin de protéger l'intégrité de la base de données d'entités. Chaque fiche d'identité entrante est testée afin de vérifier si sa structure, ses valeurs obligatoires, ses types de données valides et ses codes de sources de données configurés sont corrects.

Tandis que le processus vérifie la qualité des donnée, il tente de remédier aux problèmes, dans la mesure du possible et si le système est configuré en ce sens. Pour déterminer s'il doit ou non remédier aux problèmes de qualité, le système applique les règles de gestion de la qualité des données (DQM) configurées. Les règles DQM définissent quelles anomalies des données des fiches d'identité entrantes sont acceptables pour correction par le système, et lesquelles il est acceptable de laisser telles quelles tout en traitant quand même les fiches.

Pour consulter la qualité des données d'une source de données particulière, vous pouvez afficher ou imprimer le rapport récapitulatif de chargement. La section récapitulative Qualité peut vous apporter de précieux éclairages sur la qualité globale des données d'une source particulière ou d'un ensemble de fiches d'identité chargées depuis cette même source. A l'aide de ces informations, vous pouvez ajuster votre processus ETL, au fil des besoins, selon une source de données précise.

La consignation et le traitement d'erreurs standard consignent toutes les erreurs de qualité et les corrections de données, ainsi que les erreurs que le système n'a pas ou n'a pu corriger. Consultez fréquemment les journaux système afin d'être tenu au courant des erreurs de qualité des données qui n'ont pas été corrigées par le traitement de pipeline. Dans la plupart des cas, vous devrez corriger ces erreurs, puis recharger les fiches d'identité corrigées dans un pipeline en vue du traitement de résolution d'entité.

Exemples de vérification de la qualité des données

Le système peut ajouter automatiquement les codes qui ne sont pas reconnus comme nouveaux codes, s'il est configuré à cet effet. Le journal UMF_EXCEPT affiche les résultats soit des nouveaux codes ajoutés par le système, soit des fiches rejetées et non traitées car le système n'a pas reconnu un code et n'était pas configuré pour l'ajouter comme nouveau.

Le tableau ci-dessous illustre deux exemples de codes de fiches entrantes qui n'étaient pas encore configurés dans le système.

Tableau 3. Exemples de deux codes non configurés dans le système et du résultat du traitement

Code	Contrôle de qualité	Journal UMF_EXCEPT
Addr_Type x	Nouveau code ajouté	écriture dans le journal
Num_Type xxx	Nouveau code rejeté	écriture dans le journal

- Dans le premier exemple, le système est configuré pour ajouter automatiquement le nouveau code de type d'adresse.
- Dans le second exemple, le système n'est configuré ni pour ajouter automatiquement le nouveau code, ni pour permettre de traiter la fiche en vue de la résolution d'entité.

Dans les deux cas, le système consigne l'action dans le fichier journal pertinent.

Résolution

Au cours de la résolution d'entité, les pipelines résolvent les identités en entités. Une fois que les valeurs de données des fiches d'identité ont été nettoyées, standardisées ou rationalisées, le pipeline, à l'aide d'algorithmes de recherche sophistiqués, compare les valeurs de données de la fiche d'identité entrants aux entités existantes de la base de données d'entités afin de déterminer s'il s'agit de la même entité.

La résolution des entités implique les phases suivantes :

Générer les listes de candidats
Le système se sert des informations figurant dans la fiche d'identité entrante pour les confronter aux entités déjà présentes dans la base de données d'entités et dresser la liste de candidats potentiels à la résolution

d'entité. Chaque candidat partage suffisamment de valeurs d'attributs pour continuer à évaluer le candidat à la résolution d'entité. Vous pouvez configurer les critères qu'applique le système pour établir les listes de candidats.

Exécution de la résolution d'entité
Une fois les listes de candidats établies, le système applique les règles de résolution à chaque entité y figurant, ce au moyen d'un barème qui calcule un score de résolution servant à déterminer s'il faut résoudre l'identité entrante et l'entité existante. Vous pouvez configurer des règles de résolution et fixer les seuils des scores de résolution pour déterminer à quel degré les valeurs d'attributs doivent concorder pour que l'identité entrante et l'entité candidate soient résolues en une même entité.

Listes de candidats

Les listes de candidats sont les listes des entités possédant le potentiel pour concorder avec la fiche d'identité entrante. La liste de candidats s'élabore en récupérant les entités qui partagent des attributs avec l'identité entrante, en fonction des attributs indiqués dans la configuration du générateur de candidats.

Le processus de résolution d'entité n'utilise les entités de la liste de candidats que pour résoudre les entités et les relations.

La résolution d'entité et la détection de relation étant déterminées en fonction d'attributs, il convient d'étudier soigneusement les attributs de vos sources de données afin de déterminer lesquels engendrent les candidats les mieux qualifiés.

Une fois la liste de candidats générée, le processus de résolution d'entité compare l'identité entrante au premier candidat de la liste, au moyen des règles de résolution configurées. Le système applique les règles de résolution, dans l'ordre, pour calculer un score de résolution qui indique quel est le degré de concordance entre les attributs de l'identité entrante et ceux de l'entité candidate. Si les attributs de l'identité entrante atteignent ou dépassent le score de résolution de cette règle, la fiche d'identité entrante est résolue dans l'entité candidate.

Si en revanche le score de résolution n'atteint pas celui fixé pour cette règle de résolution, le système passe à la règle suivante jusqu'à ce que la fiche d'identité entrante ait été résolue en une entité candidate et que toutes les règles de résolution ait été épuisées.

Si la fiche d'identité entrante n'est pas résolue en une entité existante, le système résout la fiche en une nouvelle entité et stocke cette dernière dans la base de données.

Règles de résolution

Les règles de résolution sont l'ensemble de critères qu'applique le système pour établir comment des entités comparées se résolvent (à savoir s'il s'agit ou non de la même entité) et se rattachent (à savoir, si elles ne se résolvent pas en une même entité, combien d'attributs elles partagent).

Quand vous définissez des règles de résolution, vous devez indiquer les seuils qui contribuent au score de résolution total, qui détermine si une identité entrante se résout en une entité existante.

- Les seuils de candidat indiquent quelles valeurs de données d'attributs sont comparées pour déterminer si une identité et une entité se résoudront en une seule entité composite. Le seuil est le score minimum auquel une valeur

d'attribut particulière doit concorder entre l'identité entrante et une entité existante pour satisfaire la règle de résolution.
- Les seuils de concordance et discordance indiquent quelle pondération du score (positive ou négative) est appliquée aux valeurs de données d'attributs concordantes ou conflictuelles quand vous activez l'utilisation des discordances.

Vous pouvez également indiquer en quoi les valeurs conflictuelles des mêmes attributs affectent le score de résolution. Ces valeurs conflictuelles sont appelées discordances. Vous pouvez configurer des règles de résolution stipulant que la règle n'est pas satisfaite si les valeurs d'attributs présentent de quelconques conflits (discordances). Par ailleurs, vous pouvez moduler les seuils d'une règle de résolution afin de créer des discordances automatiques, en fonction des scores de comparaison qui ne satisfont les scores seuils désignés. Plus le score seuil fixé est élevé, plus la concordance doit être exacte pour satisfaire la règle de résolution.

Re-résolution

Le processus de re-résolution survient au cours du processus de résolution d'entité lorsque deux entités sont résolues en tant que même entité, et qu'une fiche d'entité composite est créée. La résolution d'entité se sert de la nouvelle fiche d'entité composite pour relancer entièrement le processus afin de savoir si elle peut être résolue en tant que l'une quelconque des autres entités de la base de données d'entités.

Tout comme avec une nouvelle entité entrante, le processus de résolution d'entité tente de générer une liste d'entités candidates à partir de la base de données d'entités. Si une liste de candidates peut être générée, le processus de résolution d'entité commence, en comparant chaque candidate de la liste à la nouvelle entité composite. Si par contre il est impossible de générer une liste de candidates, le processus de résolution d'entité passe au processus de détection de relation.

Non-résolution

Le processus de non-résolution survient au cours du processus de résolution d'entité lorsque les valeurs d'attribut de l'identité entrante fournissent de nouvelles informations signalant qu'une entité composite se compose en fait de deux entités et que la fiche d'entité composite est scindée en ces deux entités. Le système sait quelles fiches appartiennent à quel entité grâce à la source de données associée à chaque fiche. Une fois que le processus de non-résolution est achevé, le système entame le processus de re-résolution.

Exemple de non-résolution

Auparavant, le système résolvait une fiche d'identité entrante de Will Smith à l'adresse 1234 Main Street, Anytown, USA, numéro de téléphone (201) 555-2244, et adresse électronique jrsmith@fai.com en William Smith, Sr. à cette même adresse et avec ce même numéro de téléphone.

Désormais, une nouvelle fiche d'identité entrante est traitée pour Will Smith, Jr. à l'adresse jrsmith@fai.com, avec la carte de crédit 123-54-9999.

En fonction des nouvelles informations de Junior et du numéro de carte de crédit, le système peut déterminer que la fiche d'entité composite William Smith, Sr. doit subir le processus de non-résolution en William Smith, Sr. et William Smith, Jr. Une fois que l'entité est scindée en deux entités, le système entame le processus de re-résolution afin de vérifier si une autre entité de la base de données se résout maintenant en William Smith, Jr, en fonction des nouvelles informations.

Apparentement

Au cours de la résolution d'entité, les pipelines accomplissent également le processus de détection, qui détecte les relations entre identités et entités et déclenche des alertes pour les relations intéressantes.

Le système utilise des rôles, à savoir la classification d'une identité qui définit l'essence ou le but de cette identité, pour détecter et établir des relations entre entités. Dans le système, il faut définir des rôles puis les attribuer aux identités soit par source de données, soit dans le cadre de la conversion des données source originales au format UMF (Universal Message Format).

Quand le pipeline traite les identités entrantes pour la résolution d'entité et résout l'identité en une entité existante, les deux fiches ont une relation à 0 degré, à savoir que l'identité entrante et l'entité sont la même. Le processus de résolution d'entité peut cependant aller au-delà des relations à 0 degré, en fonction de la façon dont le système est configuré.

Une fois que le pipeline a épuisé toutes les possibilités de la phase de résolution d'entité, le processus de détection de relation évalue les entités qu'il reste dans la liste de candidats, c'est-à-dire celles qui ne se sont pas résolues dans l'identité entrante, afin de voir s'il existe une relation entre elles. En général, les entités figurant sur la liste de candidats sont liées avec l'identité entrante à 1 degré de séparation pour au moins un attribut, ce qui signifie que les deux entités partagent les mêmes valeurs de données d'attributs pour au moins un attribut, raison pour laquelle l'entité figure sur la liste des candidats.

Une fois que le processus a détecté une relation, le système compare les rôles attribués entre l'identité et les entités aux règles d'alertes de rôle configurées. S'il s'aperçoit que les rôles attribués à l'identité et une entité satisfont aux critères de cette règle, le système déclenche une alerte signalant qu'il a détecté une relation intéressante. La relation peut être à 0 degré, 1 degré, ou plusieurs degrés, selon la façon dont le système et les règles d'alertes de rôle sont configurés.

Relations

Les relations sont des liens entre deux ou plusieurs entités. Les relations sont détectées à la fin du processus de résolution d'entité, quand deux entités partagent plusieurs valeurs d'attributs de données.

Les relations peuvent reposer sur les liens découverts par le système, divulgués par un analyste, ou les deux. Néanmoins, toute relation n'est pas forcément assez intéressante pour justifier le déclenchement d'une alerte en vue d'une analyse ou investigation plus poussée. Les relations intéressantes se définissent en configurant des règles d'alertes de rôle qui désignent quelle combinaison de rôles attribués à des entités doivent déclencher des alertes.

Exemples de relations

Exemples de relations susceptibles d'être détectées au cours de la résolution d'entité :

- Un client est également fournisseur. en fonction des règlements et procédures de votre organisme, ceci peut être considéré comme une relation intéressante.
- Un employé connaît un client. A moins que les règlements et procédures de votre n'interdisent une telle association, ou peut-être en fonction des données partagées par l'employé et le client, il se peut que ceci ne soit pas considéré comme une relation intéressante.

- Un client connaît un autre client. Si l'un de vos clients représente une part importante de votre chiffre d'affaires, savoir qui ce client connaît peut s'avérer un moyen de tirer parti de votre réseau de clientèle pour y promouvoir vos produits et prestations.

Présentation de la fonction Degrees of Separation :

La fonction Degrees of Separation développe les capacités de mise en correspondance de relations d'IBM Relationship Resolution.

Le comportement par défaut d'IBM InfoSphere Identity Insight consiste à identifier les relations importantes et à établir une correspondance avec des entités à un degré de séparation à partir d'une identité entrante résolue en entité. L'activation de la fonction Degrees of Separation étend ces capacités pour atteindre une gamme quasi illimitée de degrés de séparation définis par l'utilisateur à partir d'une identité entrante résolue en entité.

La fonction Degrees of Separation utilise des configurations de séparation, des rôles, des règles d'alerte de rôle et des scores relationnels pour effectuer une analyse de liens en temps réel par rapport à des ensembles de données très volumineux.

Lorsqu'une identité entrante est résolue en entité, un diagramme d'entité est généré à partir des relations à un degré détectées par IBM InfoSphere Identity. Le diagramme d'entité utilise les relations à un degré pour élaborer des chaînes relationnelles à plusieurs degrés émanant de l'entité qui résulte de la résolution d'identité entrante. Une chaîne d'alertes de rôle peut ensuite être créée en reliant les chaînes relationnelles à plusieurs degrés, chacune d'elles émanant de l'entité qui résulte de la résolution d'identité entrante. La chaîne d'alertes de rôle peut ensuite servir à rechercher une relation entre les entités situées en fin de chaque chaîne relationnelle à degrés multiples, y compris cette chaîne.

La fonction Degrees of Separation facilite la tâche en évaluant tous les chemins reliant deux entités et en utilisant le chemin le plus fiable lors de la signalisation des relations. Cette fonction peut être configurée en vue de signaler une alerte de rôle pour chaque règle d'alerte de rôle configurée par entité vers laquelle l'identité entrante a été résolue.

La configuration des degrés de séparation peut être définie dans la console à l'aide de l'onglet de **Configuration système**, valeur Degrés de séparation.

Découverte de relation impersonnelle :

La découverte de relation impersonnelle est une fonction qui étend le processus de résolution de relation traditionnel afin de détecter et analyser des relations impersonnelles. Le processus de détection de relation détecte les relations entre entités en fonction des valeurs d'attribut associées à ces entités. Il importe parfois de détecter les relations entre entités en fonction des activités ou d'autres identifiants impersonnels. Ces relations entre entités en fonction des activités ou autres identifiants impersonnels sont appelées relations *impersonnelles*, les activités ou identifiants impersonnels qui apparentent des personnes étant appelés *faits relationnels*.

Les relations impersonnelles s'établissent toujours à au moins deux degrés de séparation, car le fait relationnel est en lui-même une entité. Par conséquent, pour activer la découverte de relations impersonnelles et rechercher des relations

impersonnelles, configurez vos sources de données pour qu'elles utilisent la fonction Degrees of Separation qui étend l'entité et la résolution de relations afin de détecter des relations à plus de deux degrés de séparation.

Soit par exemple une transaction téléphonique où figurent des données sur les numéros de téléphone, à savoir à la fois le numéro émetteur et le numéro récepteur. Bien qu'une personne ait effectué l'appel téléphonique à destination d'une autre personne, d'après la transaction téléphonique seule, aucune donnée commune ne peut être attribuée à ces personnes. Souvent, le fait relationnel (l'appel téléphonique) est connu avant que toute autre information sur les entités apparentées (les deux personnes impliquées dans l'appel téléphonique) ne le soit. Ces faits relationnels ne pouvant être attribués à une personne, il faut les représenter en tant qu'entités distinctes qui ne sont pas des personnes, mais concernent des personnes. Toutefois, la découverte de relation impersonnelle reconnaît qu'il existe une relation entre deux personnes en conséquence l'appel téléphonique.

Le format UMF comporte une fonction de type d'entité qui permet de définir des faits relationnels comme types d'entités. Grâce à cette fonction, les faits relationnels deviennent des entités distinctes dans la base de données d'entités et peuvent servir à détecter les relations entre entités Personne. En configurant de nouveaux types d'entités, en indiquant le type d'entité adéquat dans l'UMF, et en créant de nouvelles configurations de résolution, ces faits relationnels peuvent servir à détecter automatiquement les relations impersonnelles et les conflits entre entités.

Les entités de types différents ne s'entre-résolvent jamais, ce même si les règles de résolution l'autorisent et même si les données admettent la résolution. Cela signifie qu'un type d'entité Appel téléphonique ne se résout jamais en un type d'entité Personne .

Analyst Toolkit génère des graphiques et des rapports pour les relations impersonnelles et les alertes associées tout comme pour les relations personnelles et les alertes associées.

Exemple de découverte de relation impersonnelle

Si par exemple vous souhaitez découvrir les relations impersonnelles au moyen d'appels téléphoniques, il faut créer un nouveau type d'entité nommé Appel téléphonique et ajuster votre noeud d'acquisition afin d'attribuer à chaque fiche d'appel téléphonique le type d'entité *Appel téléphonique*.

Lors de l'intégration des fiches téléphoniques au système, la résolution de relations et d'entités standard détecte une relation à un degré entre l'entité Appel téléphonique et l'entité appelante (Personne). Une relation à un degré entre la personne appelée et l'entité Appel téléphonique est également détectée. Le système, de lui-même, ne trouve aucune relation entre les personnes.

Toutefois, lorsque la fonction Degrees of Separation est configurée, elle continue d'analyser et de détecter la relation impersonnelle à deux degrés entre l'appelant et la personne appelée. Une relation impersonnelle existe, d'après les numéros de téléphone qui sont des attributs du type d'entité Appel téléphonique. La fonction Degrees of Separation analyse ensuite cette relation impersonnelle et déclenche une alerte en cas de conflit.

Rôles

Un rôle est une classification d'une identité qui en définit l'essence ou le but. Vous pouvez associer plusieurs rôles à une identité. A mesure que identités se résolvent en entités, ces dernières héritent de tous les rôles associés.

Les rôles servent à configurer les règles d'alertes de rôle, qui définissent les relations intéressantes et déclenchent les alertes.

Un rôle est attribué à chaque identité, de l'une de deux manières :

Par source de données entrante
: Quand vous configurez une nouvelle source de données, vous y associez un rôle, ce qui aura pour effet d'attribuer ce rôle à toutes les identités contenant ce code de source de données.

Par UMF
: Quand vous convertissez au format UMF (Universal Message Format) la source de données, vous pouvez attribuer des rôles directement comme élément de la fiche UMF au moyen du segment UMF <SEP_ROLES>, avec la balise UMF <ROLE_CODE>. Si vous configurez par UMF, il faudra ajouter les règles DQM et une table de consultation.

Exemples de rôles utiles : employés, fournisseurs, clients ou liste noire.

Exemple d'attribution de rôles à l'aide du format UMF

Pour attribuer le rôle d'employé à une fiche d'identité à l'aide du format UMF, il faut saisir le segment UMF <SEP_ROLES> et la balise UMF <ROLE_CODE> suivants de cette fiche :

```
<SEP_ROLES>

  <ROLE_CODE>employé</ROLE_CODE>

</SEP_ROLES>
```

Alertes

Les alertes sont des messages ou autres indications qui signalent qu'un événement est survenu.

Les alertes sont générées de l'une de deux manières :

- Les alertes d'attribut sont générées dès que des entités concordent avec la série d'attributs indiquée.
- Les alertes de rôle sont déclenchées dès que des entités qui sont liées par une relation partagent des rôles que l'utilisateur a désignés comme *intéressants* ou *conflictuels*.

Il est important de définir quelles alertes satisfont les objectifs de votre entreprise. En premier lieu, il faut vous demander quelles relations entre entités présentent un intérêt pour votre entreprise. Les relations reposent sur les rôles définis par l'utilisateur, qui sont attribués aux fichiers entrants par le système source. Quand deux entités partagent suffisamment de valeurs de données d'attributs sans aboutir à la même entité, ces entités forment une relation. Veillez à ce que les règles d'alerte de rôle configurées pour votre entreprise définissent clairement quels rôles d'entité créent une relation que vos analystes seront chargés d'examiner plus attentivement.

Exemples d'alertes

Exemples de relations intéressantes dont il est judicieux qu'elles déclenchent des alertes :

- L'un des employés de votre entreprise est également un fournisseur de biens ou services facturés à votre entreprise.
- L'un de vos clients possède une adresse et un nom figurant sur une liste noire du gouvernement.
- Deux des personnes qui ont déposé une déclaration d'accident du travail dans votre entreprise possèdent les mêmes nom, adresse et numéro de téléphone.

Alertes d'attribut :

Les alertes d'attribut sont des alertes produites par les générateurs d'alertes d'attribut qui créent une requête système permanente à la recherche d'attributs ou d'identités spécifiques dans la base de données de l'entité. Chaque fois que des attributs d'entités correspondent aux critères du générateur d'alertes d'attribut, le système crée une alerte d'attribut.

Les utilisateurs du Visualizer créent leurs propres générateurs d'alertes d'attribut personnels. Si vous recherchez une identité spécifique ou n'importe quelle identité ou entité correspondant à un ensemble d'attributs spécifiques, vous pouvez créer votre propre générateur d'alertes d'attribut personnel qui recherche des correspondances jusqu'à une date d'expiration spécifiée.

Exemples d'attributs d'entité possibles dont il est souhaitable d'être informé :

- Nom et numéro unique (par exemple un numéro de carte de crédit)
- Nom et numéro de téléphone
- Adresse
- Nom et numéro non unique

Les générateurs d'alertes d'attribut sont configurés et consultables à l'aide du Visualizer . Vous êtes le seul à pouvoir accéder aux générateurs d'alertes d'attribut dont vous êtes l'auteur.

Exemple d'alerte d'attribut d'adresse

Vous surveillez l'adresse 675 Hickory Street Las Vegas, NV. Vous pouvez configurer un générateur d'alertes d'attribut afin qu'il crée une alerte d'attribut chaque fois que cette adresse est associée à une fiche d'identité entrante qui est ajoutée à la base de données d'entités.

Alertes de rôle :

Une alerte de rôle identifie les situations où une ou deux entités, liées par une relation, répondent ou surpassent une règle d'alerte de rôle configurée. Les alertes de rôle se basent sur des rôles configurés et des règles d'alertes de rôle. Elles peuvent émettre un avertissement ou signaler un incident (par exemple, un client connaît un "paria") ou simplement une relation intéressante (par exemple, un client connaît un employé).

Définissez des relations *intéressantes* ou *conflictuelles* en configurant les règles d'alertes de rôle qui désignent quels rôles ne peuvent ni exister dans une seule entité, ni être liés à une seule ou plusieurs entités. Utilisez la Console de

configuration pour configurer les filtres des alertes de rôle, qui déterminent si le système vous alerte de nouveau en cas de nouvelles informations (telles qu'une nouvelle identité ou un nouveau code de source de données).

Au cours de la résolution d'entité, le pipeline évalue les relations entre l'identité entrante et les entités de la liste de candidats. Une fois qu'il a établi l'existence d'une relation entre l'identité entrante et une entité candidate, le système évalue ensuite si les rôles attribués répondent ou pas à une règle d'alerte de rôle configurée. Dans l'affirmative, le système déclenche une alerte de rôle.

Une alerte de rôle identifie les données d'entité au moment où l'alerte a été créée. L'écran d'informations Alerte de rôle affiche les données de l'entité telles qu'elles se présentaient lors de la création de l'alerte de rôle. Au fil des modifications de ces données, le récapitulatif d'entité renferme les plus récentes données d'entité. Si vous souhaitez consulter les données actuelles d'une certaine entité, reportez-vous au récapitulatif.

Vous pouvez afficher les alertes de rôle et les manier dans les composants d'Analyst Toolkit (rapports Cognos, le plug-in Identity Insight pour i2, et Identity Insight Explorer).

Règles d'alerte de rôle :

Les règles d'alerte de rôle, définies par l'utilisateur, sont des règles qui identifient les rôles qui ne peuvent ni exister dans une même entité, ni être reliés entre plusieurs entités. Lors de la résolution d'entité, si les critères d'une règle d'alerte de rôle sont satisfaits, le système déclenche une alerte de rôle.

Bien que la plupart des règles d'alerte de rôle servent à signaler les conflits de rôles, vous pouvez également définir une règle d'alerte de rôle signalant qu'une entité à laquelle est attribué un rôle connaît une autre entité à laquelle est attribué le même rôle. Il peut par exemple vous sembler intéressant, lorsque des clients se connaissent, d'en être informé, et donc de définir une règle d'alerte de rôle (*le client connaît le client*) qui déclenche une alerte dès qu'une entité client est apparentée à une autre entité client de la base de données d'entités.

Les entités se composant de plusieurs fiches (souvent issues de différentes sources de données), et les rôles étant généralement attribués par source de données, il est possible d'attribuer plusieurs rôles à une même entité. Il est donc également possible de définir une règle d'alerte de rôle qui déclenche une alerte dès que sont attribués à une même entité à la fois le rôle de client et le rôle de "paria", en fonction des données entrante.

Remarque : Songez bien que si un système est configuré pour utiliser un grand nombre de rôles, le nombre de règles d'alerte de rôle augmente de façon exponentielle.

Bien que le système détecte toute relation qui enfreint une règle d'alerte de rôle par défaut, il ne signale qu'une seule alerte de rôle pour chaque entité. Par exemple, si le système détecte qu'une entité à laquelle est attribué un rôle d'employé est apparentée à deux entités fournisseur différentes, est qu'une règle d'alerte de rôle est configurée pour déclencher une alerte de rôle dès qu'un employé connaît un fournisseur, les conflits sont tous deux détectés et transcrits dans la base de données. Par défaut toutefois, une seule alerte de rôle est signalée.

Quand vous configurez des règles d'alerte de rôle, vous pouvez aussi désigner des filtres d'alerte qui déterminent si le système vous alerte de nouveau dès que de nouvelles identités ou de nouveaux codes de source de données sont introduits dans des entités existantes concernées par une alerte déclenchée auparavant.

Invalidation d'une alerte de rôle :

Lorsque des données sont traitées pour la résolution d'entité et de relation, les entités et les relations qui les lient évoluent. Cette évolution, basée sur une analyse constante des données existantes et nouvelles, peut entraîner l'invalidation des alertes de rôle. La fonction d'invalidation d'InfoSphere Identity Insight fournit le contexte le plus récent aux analystes afin qu'ils n'aient pas à examiner des conflits qui ne sont plus valides.

L'invalidation d'alerte de rôle supprime les alertes de rôle basées sur des relations qui sont encore à l'état En attente. En règle générale, les alertes à l'état En attente n'ont pas encore été visualisées ou traitées par un analyste. Si l'état d'une alerte de rôle est autre, comme terminé ou affecté, et que les données prennent en charge l'invalidation de cette alerte de rôle, l'alerte n'est pas invalidée. Un seul état peut être affecté à une alerte ; par conséquent, si l'alerte est déjà à l'état Affectée ou Terminée, elle n'est pas invalidée.

Les alertes de rôle déclenchées au degré 0 sont également invalidées lorsqu'une identité est supprimée ou non résolue dans l'entité.

Fonctionnement de l'invalidation de l'alerte de rôle

Les alertes de rôle basées sur des relations peuvent être invalidées pour plusieurs raisons :

- Si une entité modifie son ID d'entité dans le cadre d'un processus de nouvelle résolution ou d'annulation de résolution lors de la résolution d'entité, la relation peut disparaître ou être transmise à un nouvel ID d'entité.
- Si une entité devient deux entités distinctes basées sur de nouvelles données, les nouvelles entités reçoivent chacune un nouvel ID. La procédure d'attribution totale permet de supprimer toutes les données appartenant à l'ancienne entité et de les ajouter à la nouvelle entité, y compris les rôles qui créent des alertes de rôle basées sur des relations.
- Lorsque des données sont supprimées de la base de données d'entités, l'ensemble d'une entité ou un composant clé d'une relation peut être supprimé et entraîner l'invalidation de l'alerte de rôle.
- Lorsque des données sont marquées comme génériques, leur utilisation pour la détection de relations est limitée ou supprimée. Si une relation est supprimée, toutes les alertes de rôle qui en dépendent sont invalidées.

Alertes de rôle de remplacement

Lorsqu'une alerte de rôle est invalidée, le pipeline réévalue automatiquement chaque conflit dans le chemin de relation et recherche les données signalant un autre conflit lié aux relations.

Un *chemin de relation* est la chaîne d'entités et d'attributs qui relie une entité à une autre. La longueur du chemin de relation est déterminée par la configuration des degrés de séparation. Les configurations de séparation sont définies via la console de configuration.

Score

Au cours de la résolution d'entité, le système calcule quel est le degré de concordance entre les attributs d'une identité entrante et ceux d'une entité existante. Les résultats de cette analyse mathématique sont des scores dont le système se sert pour résoudre les identités en entités et détecter les relations entre entités.

Scores de résolution

Le score de résolution est la valeur qui est attribuée au cours de la résolution d'entité à l'issue du traitement de concordance et discordance, et qui établit la probabilité que les identités comparées représentent la même entité. Ce score, défini par l'utilisateur, sert à résoudre une nouvelle identité en une entité existante.

A mesure que le pipeline traite les identités entrantes pour la résolution d'entité, il compare les valeurs des attributs partagés de l'identité entrante et de chaque entité de la liste de candidats. L'un des aspects de la comparaison consiste à calculer des scores qui représentent le degré de concordance des valeurs d'attribut. Ces scores sont alors comparés aux seuils configurés et au score de résolution de chaque règle de résolution. Une fois que le processus de résolution d'entité a appliqué un processus de concordance et discordance afin d'empêcher les faux positifs, le système attribue un score de résolution de base à la fois pour l'identité entrante et l'entité de la liste des candidats.

Si certains attributs sont configurés pour approfondir la concordance et la discordance, le processus évalue ensuite ces attributs. Les résultats affectent les scores de résolution de base de l'identité entrante et de l'entité candidate. Si les valeurs d'attributs concordent, le score de résolution peut être affecté positivement en ajoutant le nombre de points configuré. Si les valeurs d'attributs ne concordent pas, le score de résolution peut être affecté négativement en soustrayant le nombre de points configuré. Quand vous configurez un attribut à appliquer à la concordance ou discordance, il faut indiquer le nombre de points en plus ou en moins qui module le score de résolution de base.

Le système compare alors le score de résolution obtenu par l'identité entrante et l'entité candidate à chaque règle de résolution. Si le score de résolution atteint ou dépasse le score de fiabilité configuré pour la règle de résolution, le système résout l'identité entrante en tant que l'entité candidate, et crée une entité composite dans la base de données d'entités.

Scores de relation

Le score de relation est la valeur qui est attribuée au cours de la résolution d'entité à l'issue de l'application des règles de résolution, et qui établit le degré auquel les deux identités comparées sont apparentées. Ce score, défini par l'utilisateur, sert à apparenter les entités.

Au cours de la résolution d'entité, le pipeline compare l'identité entrante (dont il se peut qu'elle ne se résolve pas en une entité) aux entités restantes de la liste de candidats. Bien qu'il soit possible que ces entités candidates ne se résolvent pas dans l'identité entrante, elles sont néanmoins évaluées en termes de relations.

Durant le processus de détection de relation, les pipelines déterminent les relations en calculant un score de relation pour chaque valeur de donnée d'attribut partagé entre l'identité entrante et les entités de la liste de candidats, en commençant par la première entité :

- Si le score de relation satisfait les critères configurés pour les relations (par degrés de séparation), le système détermine que les deux entités sont apparentées. La relation est alors transcrite dans les deux fiches d'entité composite. Le système vérifie ensuite les règles d'alertes de rôle configurées pour déterminer si la relation est considérée comme intéressante. Dans l'affirmative, le système déclenche une alerte. Dans la négative, il passe à l'entité suivante de la liste de candidats.
- Si le score de relation ne satisfait pas les critères configurés pour les relations, le processus passe à l'entité suivante de la liste de candidats, jusqu'à ce que la totalité des entités aient été évaluées en termes de relations.

Gestionnaire d'événements

Le gestionnaire d'événements étend les capacités d'IBM InfoSphere Identity Insight en associant l'analyse d'événements quasiment en temps réel et la surveillance d'événements à la résolution d'identités et de relations. Une fois activé, le gestionnaire d'événements permet à votre entreprise d'effectuer un suivi des événements métier et d'émettre une alerte en cas d'événements suspects ou intéressants, afin que vous puissiez appliquer des actions métier adéquates dans les meilleurs délais pour que votre entreprise puisse faire face à toute menace et tentative de fraude.

Etant donné que les scénarios de menace et de fraude changent constamment, la flexibilité du gestionnaire d'événements vous permet de définir les types d'événements à suivre et de configurer des règles métier pour le traitement des événements et la génération d'alertes d'événements. Ces règles correspondent à un ensemble de critères que le gestionnaire d'événements utilise pour déterminer la façon dont les événements sont traités et ce qui déclenche une alerte d'événement. Vous pouvez configurer les règles métier, en fonction de vos besoins métier et des scénarios.

Définissez également ce qui constitue une alerte d'événement. En règle générale, les alertes d'événement ne sont pas déclenchées par un événement unique, mais par une série d'événements complexes qui se produisent tous à des moments et dans des contextes différents. Par exemple, vous pouvez définir une règle métier qui regroupe des transferts d'argent par client sur une période donnée et qui génère une alerte si le montant total dépasse la limite légale. Sinon, vous pouvez définir une règle métier qui vous alerte lorsque deux achats par carte de crédit, utilisant le même numéro de carte, se produisent en une heure à plus de 200 kilomètres de distance.

Fonctionnement du traitement d'événement

Le gestionnaire d'événements d'IBM InfoSphere Identity Insight fonctionne avec le processeur CEP d'IBM Active Middleware Technology, qui comprend deux composants : Le moteur CEP et l'outil Rule Author d'Eclipse. Vous configurez les règles métier d'événement et les alertes d'événement dans l'outil Rule Author, puis vous exportez cette configuration en tant que fichier `CEP.XML`. Après l'activation du gestionnaire d'événement activé et chaque fois que le pipeline détecte des données UMF entrantes formatées à l'aide du segment de données EVENT, il traite les données pour la résolution d'entité, puis transmet les données traitées au moteur CEP. Le moteur CEP traite les données d'événement en fonction des règles métier configurées dans le fichier `CEP.XML` et renvoie les informations de décision au pipeline IBM InfoSphere Identity Insight pour qu'elles soient stockées dans la base de données d'entités. Si des alertes d'événements sont associées à un événement ou à une combinaison d'événements, vous pouvez configurer le Gestionnaire

d'événements afin qu'il affiche ces alertes dans le Visualizer, ou un autre outil du Visualizer pour analyse approfondie et disposition.

Vous pouvez également configurer votre application client afin que le moteur CEP renvoie des décisions immédiates à l'application client, fournissant ainsi aux représentants de votre entreprise des informations instantanées. Par exemple, le moteur CEP peut immédiatement demander aux représentants de votre service client d'arrêter une transaction, par exemple un virement dont la somme dépasse la limite légale autorisée en dollars pour un client dans un délai de 24 heures.

Evénements

Les événements correspondent à des informations sur quelque chose qui s'est produit dans un domaine métier, par exemple : "un client ouvre un compte" ou "un client transfère une somme d'argent". Dans le gestionnaire d'événements, les événements contiennent des attributs qui se basent sur leurs types d'événements correspondants.

Alertes d'événements

Une alerte d'événement est déclenchée lorsqu'un ou plusieurs événements complexes remplissent des critères définis au cours d'un cycle de vie spécifié. Les alertes d'événement reposent sur des règles d'événement complexes et d'autres configurations incluses dans un fichier de règles d'événement (`cep.xml`). Ces alertes peuvent indiquer des situations présentant un intérêt, par exemple "Au moins deux achats de plus de 10000 dollars ont été effectués il y a une heure sur des sites situés à 200 miles l'un de l'autre".

Types d'événements

Les types d'événements classent les événements par catégorie et définissent l'unité de mesure pour la valeur associée aux événements dans le gestionnaire d'événements. Quelques exemples de types d'événements : virement, ouverture de compte ou transaction par carte de crédit.

Les types d'événements sont requis pour le traitement d'événements car les règles métier définies par l'utilisateur, que le processeur d'événements utilise, exigent un type d'événement spécifique. Si le type d'événement n'existe pas, le processeur d'événements ne peut pas traiter l'événement en question.

Règles d'événements

Les règles d'événement représentent un ensemble de règles métier qui déterminent comment le moteur CEP (Complex Event Processing) traite les enregistrements d'événement entrants et qui définissent le type de réponse (telle qu'une alerte d'événement) renvoyée au pipeline et à l'application client. Vous configurez des règles d'événement dans l'outil CEP Rule Author d'Eclipse. Les règles d'événement sont regroupées sous un projet CEP et sont exportées dans un fichier de règles d'événement appelé `cep.xml`.

Vous pouvez configurer des règles d'événement pour renvoyer des informations et des alertes en fonction d'éléments qui intéressent votre société ou vos analystes. Des règles d'événement peuvent être configurées pour signaler les données d'un enregistrement d'événement entrant unique. Toutefois, la plupart des règles d'événement regroupent un ensemble de données d'événement complexes et déclenchent une alerte lorsqu'un seuil ou une condition est atteinte.

Dans l'outil Rule Author, les règles métier d'événement sont appelées des *situations*. Pour plus d'informations, voir «Terminologie CEP», à la page 33.

Les règles d'événement courantes comprennent des fonctions d'addition ou de comptabilisation. Par exemple, vous pouvez configurer une règle d'événement pour générer une alerte lorsqu'une entité effectue un virement de plus de 15000 dollars en 24 heures.

Mise en route du gestionnaire d'événements

Utilisez les étapes suivantes comme liste de contrôle pour configurer et utiliser le gestionnaire d'événements.

Procédure

1. Obligatoire : Installez l'outil CEP (Complex Event Processor) Rule Author d'Eclipse. L'outil de création de règles basé sur Eclipse™ est installé automatiquement avec le produit. (La fonction Gestionnaire d'événements et le moteur CEP sont automatiquement installés.) L'outil de création de règles est inclus dans un fichier ZIP disponible dans le téléchargement du produit.
2. Obligatoire : Utilisez l'outil Rule Author pour créer un projet CEP et regrouper toutes les règles d'événement et les configurations pour le gestionnaire d'événements.
3. Obligatoire : Dans l'outil Rule Author, importez le fichier de règles d'événement `cep.xml` dans le projet CEP et personnalisez le fichier en créant les règles d'événement en fonction des scénarios de traitement des événements et d'utilisation des alertes. Avant de modifier le fichier d'origine, sauvegardez ou copiez-le dans un autre répertoire par précaution.

   Important : La casse utilisée pour nommer le fichier de règles d'événement doit être impérativement respectée, notamment dans un environnement UNIX. Le nom de fichier doit être uniquement indiqué en minuscules.
4. Obligatoire : Exportez le fichier de règles d'événement `cep.xml`. Le moteur CEP et le gestionnaire d'événements utilisent ce fichier de règles d'événement XML pour traiter les événements et déterminer quand des alertes doivent être lancées. Le fichier XML exporté doit être nommé `cep.xml`, et il doit être situé dans le répertoire suivant : *`rép_installation-produit`*`/ibm-home/gem/`.
5. Obligatoire : Configurer les paramètres système du Gestionnaire d'événements dans la Console de configuration.

   A faire : Avant que les modifications du système ne deviennent effectives, vous devrez arrêter et redémarrer tous les pipelines en cours d'exécution. Vous pouvez soit arrêter tous les pipelines en cours d'exécution avant de configurer les paramètres système du Gestionnaire d'événements et les types d'événement, soit arrêter et redémarrer tous les pipelines en cours d'exécution après avoir configuré les paramètres système du Gestionnaire d'événements et les types d'événement.
6. Obligatoire : Configurer les types d'événement dans la Console de configuration.

   A faire : Avant que les modifications du système ne deviennent effectives, vous devrez arrêter et redémarrer tous les pipelines en cours d'exécution. Vous pouvez soit arrêter tous les pipelines en cours d'exécution avant de configurer les paramètres système du Gestionnaire d'événements et les types

d'événement, soit arrêter et redémarrer tous les pipelines en cours d'exécution après avoir configuré les paramètres système du Gestionnaire d'événements et les types d'événement.

7. Pour voir les alertes d'événement dans les applications Analyst Toolkit, procédez comme suit :
   a. Facultatif : Identity Insight contient déjà les codes d'activité par défaut pour la gestion des alertes d'événement (En attente, Attribué, et Fermé). Mais, si vous le souhaitez, vous pouvez créer des codes d'activité supplémentaires pour les alertes d'événement dans la Console de configuration. Avant de créer les codes d'activité, arrêtez tous les pipelines en cours d'exécution puis redémarrez-les une fois les codes d'activité créés.
   b. Facultatif : Vous pouvez passer en revue les alertes d'événement, modifier l'état des alertes d'événement, affecter des alertes d'événement à vous-même, ou affecter des alertes d'événement à d'autres groupes d'alertes de l'analyste.
   c. Facultatif : Si vous souhaitez afficher tous les détails d'un alerte d'événement spécifique, vous pouvez générer le rapport détaillé d'une alerte d'événement.
   d. Facultatif : Vous pouvez afficher l'historique d'alerte d'événement d'une entité dans le récapitulatif d'entité.
   e. Facultatif : Dans le récapitulatif d'entité, vous pouvez cliquer sur **Afficher les événements** pour afficher tous les événements associés à l'entité, et même les événements qui n'ont pas généré d'alerte d'événement. Vous pouvez aussi cliquer sur **Rapport** pour imprimer un rapport sur Tous les événements montrant également tous les événements associés à l'entité.
8. Obligatoire : Utilisez les définitions du segment de données EVENT pour inclure les informations de traitement des événements dans les données UMF que vous convertissez et les envoyer aux pipelines.
9. Facultatif : Si vous souhaitez envoyer des messages système (y compris des messages du Gestionnaire d'événements) à votre application client, veillez à utiliser un pipeline HTTP, et assurez-vous que votre application client peut recevoir les messages du document de retour SYSTEM_MESSAGE standard.
10. Facultatif : Une fois que le gestionnaire d'événements a traité les événements, vous pouvez vous reporter aux fichiers journaux du gestionnaire d'événements et aux fichiers journaux de la console de configuration associés.

Activation du gestionnaire d'événements dans la console de configuration

Pour traiter des événements à l'aide du gestionnaire d'événements, vous devez activer et configurer le gestionnaire d'événements dans la console de configuration.

Pourquoi et quand exécuter cette tâche

Procédure

1. Dans la console de configuration, cliquez sur l'onglet **Configuration système**.
2. Pour activer le traitement des événements, modifiez la valeur **Activation du traitement d'événement**.
3. Pour configurer l'identificateur URI (Universal Resource Indicator) sur CEP, modifiez la valeur **URI du processeur d'événement**. La valeur par défaut doit être http://localhost:13510/gem
4. Pour augmenter le paramètre de durée totale de traitement des événements, modifiez la valeur **Délai d'attente du processeur d'événement**. Cette valeur

indique, en secondes, le délai pendant lequel le pipeline attend une réponse du processeur CEP avant d'arriver à expiration et de générer une erreur.

5. Pour modifier le nombre de jours de l'historique des événements envoyés au pipeline qui serviront à l'évaluation d'un nouvel événement entrant, modifiez la valeur **Fenêtre d'historique d'événements**.
6. Cliquez sur **Enregistrer**.

Configuration du module CEP du gestionnaire d'événements

Dans IBM InfoSphere Identity Insight, *CEP* désigne les outils CEP (Complex Event Processing) fournis avec le produit. Ces outils sont des composants du gestionnaire d'événements qui étendent la résolution d'identité et de relation pour traiter des transactions d'événement et générer des alertes d'événement. La présente section contient les informations de configuration nécessaires pour permettre aux outils CEP de fonctionner avec le gestionnaire d'événements.

Architecture

Le composant CEP du gestionnaire d'événements comprend deux outils :

Outil Rule Author d'Eclipse
L'outil CEP Rule Author d'Eclipse est le composant que vous utilisez pour configurer et exporter des règles d'événement dans le fichier `cep.xml`. Le fichier de règles d'événement détermine comment les événements sont traités et l'événement qui déclenche une alerte.

Lorsque vous installez IBM InfoSphere Identity Insight, vous installez également un fichier compressé contenant l'outil et le guide d'utilisation associé. Toutefois, vous devez d'abord décompresser les fichiers de l'outil pour pouvoir configurer les règles d'événement.

Moteur CEP (Complex Event Processing)
Le moteur CEP (Complex Event Processing) est le composant qui traite les données d'événement entrantes en fonction des règles d'événement configurées dans le fichier `cep.xml`.

Lorsque le pipeline reçoit des données formatées à l'aide du segment de données EVENT d'un document UMF entrant, il les envoie au moteur CEP pour effectuer le traitement des événements. Une fois que le moteur CEP a traité les données d'événement à l'aide du fichier `cep.xml`, il renvoie les résultats au pipeline. Si les données d'événement correspondent ou sont supérieures à une règle d'événement configurée, le moteur CEP renvoie un signal au pipeline pour générer une alerte d'événement. Qu'une alerte soit générée ou non, les données d'événement finales reçues sur le pipeline sont placées dans la base de données d'entités.

Le moteur CEP est installé par défaut avec IBM InfoSphere Identity Insight.

Les composants CEP font partie d'une version spécifique d'IBM Active Middleware Technology incluse avec le gestionnaire d'événements. Ces composants sont inclus dans le produit acheté.

Fichier cep.xml

Le fichier `cep.xml` contient des règles d'événement et d'autres paramètres nécessaires pour traiter les données d'événement et générer des alertes d'événement. La fonction du gestionnaire d'événements du pipeline et du moteur

CEP peuvent uniquement traiter les événements en utilisant le fichier de règles d'événement cep.xml. Ce fichier est au format XML (**E**xtensible **M**arkup **L**anguage) car les données transmises au pipeline sont au format UMF (**U**niversal **M**essaging **F**ormat), un format basé sur XML.

Un fichier cep.xml initial est inclus avec le produit installé et contient les nombreux paramètres de configuration nécessaires au gestionnaire d'événements pour fonctionner avec le moteur CEP. Vous pouvez importer le fichier cep.xml initial dans un projet CEP, puis configurer les règles d'événement.

Remarque : Avant d'importer, de modifier ou d'exporter le fichier de règles d'événement cep.xml, sauvegardez et stockez le fichier d'origine dans un autre répertoire. Envisagez d'utiliser un système de gestion des versions ou de contrôle source lorsque vous modifiez le fichier de règles.

Ressources supplémentaires pour CEP

Pour obtenir des informations plus détaillées sur l'utilisation de l'outil Rule Author d'Eclipse, reportez-vous au guide d'utilisation de l'outil. Le guide, nommé AMT3.0.UserGuide.PDF, se trouve dans le répertoire *chemin_installation*/cep/.

Installation de l'outil CEP Rule Author d'Eclipse

Pour installer l'outil Rule Author d'Eclipse sur un poste de travail, suivez les instructions ci-après. Le gestionnaire d'événements et le moteur CEP sont tous deux installés par le programme d'installation du produit. Vous devez cependant installer l'outil de création de règles à partir d'un fichier ZIP qui est inclus dans l'installation.

Avant de commencer

L'outil Rule Author fonctionne uniquement sous Microsoft Windows et requiert Java version 1.5 ou suivante.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'outil Rule Author pour configurer les règles et les seuils utilisés pour surveiller votre activité, puis exporter ces informations dans le fichier de règles d'événement (cep.xml). Le gestionnaire d'événements et le moteur CEP utilisent le fichier de règles d'événement pour traiter des événements et détecter des alertes d'événement. Les alertes d'événement peuvent être associées à un événement unique ou à une combinaison d'événements. Vous pouvez configurer le gestionnaire d'événements afin qu'il affiche ces alertes dans Analyst Toolkit, ou un autre outil de visualisation pour une analyse approfondie.

Pour installer l'outil Rule Author d'Eclipse à partir du fichier ZIP :

Procédure

1. Accédez au répertoire d'installation du produit.
2. Accédez au sous-répertoire /cep.
3. Copiez le fichier CEP_3.0.1.1.03.zip dans un système client Microsoft Windows.
4. Décompressez le fichier CEP_3.0.1.1.03 dans *identificateur d'unité*:/CEP/

Que faire ensuite

Pour obtenir des informations d'utilisation plus approfondies sur l'outil de création de règles, reportez-vous au Guide utilisateur qui se trouve dans le fichier `cep/AMT3.0_UserGuide.PDF`.

Démarrage de l'outil Rule Author :

Pour utiliser l'outil Rule Author d'Eclipse, vous devez d'abord le démarrer. L'outil Rule Author est installé et démarré indépendamment des composants IBM InfoSphere Identity Insight.

Pourquoi et quand exécuter cette tâche

L'outil Rule Author fonctionne uniquement sur un client Microsoft Windows et requiert Java version 1.5 ou suivante.

Procédure

1. Ouvrez l'explorateur Microsoft Windows et accédez au répertoire où l'outil Rule Author d'Eclipse est installé.
2. Cliquez deux fois sur le script de commandes `AmitIDE.cmd`. Le script de commandes ouvre l'exécutable de l'outil Rule Author.

Terminologie CEP

Certains des termes utilisés dans l'outil Rule Author d'Eclipse peut différer légèrement des termes utilisés dans IBM InfoSphere Identity Insight et ses composants. Ce glossaire a pour objectif de vous aider à mieux comprendre les termes utilisés pour le traitement des événements complexes et la manière dont ils s'associent au Gestionnaire d'événements et autres composants.

Fichier cep.xml

Le fichier `cep.xml` contient toutes les règles d'événement et les paramètres de configuration CEP nécessaires pour permettre au gestionnaire d'événements et au moteur CEP de traiter des enregistrements d'événement entrants. Un fichier des règles d'événements avec ce nom doit être exporté vers l'emplacement *répertoire_installation_produit*`\ibm-home\gem\`.

Important : Le nom de fichier doit être indiqué en minuscules, en particulier dans des environnements UNIX.

Vous gérez et exportez le fichier de règles d'événement à l'aide de l'outil Rule Author.

Un fichier de règles d'événement `cep.xml` initial est inclus avec le produit IBM InfoSphere Identity Insight. Ce fichier de démarrage contient déjà un grand nombre des paramètres et des configurations nécessaires pour fonctionner avec le gestionnaire d'événements. Vous pouvez importer le fichier de règles d'événement `cep.xml` initial dans l'outil Rule Author en effectuant au préalable une copie de sauvegarde du fichier d'origine pour ajouter des règles métier d'événement et exporter le fichier dans l'emplacement requis. Vous pouvez envisager d'utiliser un système de gestion des versions ou de contrôle source pour stocker le fichier avant et après sa modification.

Moteur CEP

Le moteur CEP (Complex Event Processing) est le mécanisme qui traite les données d'événement entrantes du pipeline et traite les données en

fonction des règles définies dans un projet CEP. Le projet CEP est défini dans le fichier `cep.xml`, qui est configuré et exporté par l'outil Rule Author.

Le moteur CEP que le gestionnaire d'événements utilise est inclus dans le produit IBM Active Middleware Technology. La version du moteur CEP utilisée par le gestionnaire d'événements est incluse et installée avec IBM InfoSphere Identity Insight. Toutefois, vous devez configurer le gestionnaire d'événements dans la console de configuration et définir les règles d'événement dans l'outil Rule Author pour pouvoir traiter les événements avec le moteur CEP.

Projets CEP

Les projets correspondent à un groupe de niveau supérieur que le processeur d'événements complexes utilise pour stocker un regroupement d'événements, de cycles de vie et de règles. Pour utiliser le gestionnaire d'événements, vous devez créer **un seul** projet CEP qui contient toutes les informations d'événement, notamment les règles métier d'événement, à surveiller. Le gestionnaire d'événements utilise un seul projet CEP à la fois mais un même projet peut tester plusieurs types d'événement et plusieurs règles par type d'événement.

Vous pouvez créer et gérer le projet CEP au sein de l'outil Rule Author.

Outil Rule Author (outil Rule Author basé sur Eclipse)

Cet outil permet de définir des projets CEP, des événements et d'autres configurations inclus dans le fichier de règles d'événement `cep.xml` pour permettre au moteur CEP de traiter des événements et générer des alertes d'événement.

Classes d'événements

Pour utiliser le gestionnaire d'événements, le projet CEP doit inclure les classes d'événement suivantes, qui sont préconfigurées dans le fichier `cep.xml` initial :

- `EAS_START.event` : Utilisé pour indiquer l'initiateur du cycle de vie du gestionnaire d'événements.
- `EAS_STOP.event` : Utilisé pour indiquer le terminateur du cycle de vie du gestionnaire d'événements.
- `EVENT.event` : Utilisé pour définir les règles métier (ou situations) du gestionnaire d'événements qui permettent de traiter les données d'événement entrantes et de générer des alertes d'événement.

EVENT.event

Cette classe d'événement CEP mappe les données d'entrée transmises par le pipeline au moteur CEP pour traitement. Ce mappage est directement lié à la table `GEM_EVENT` de la base de données d'entités. Vous devez utiliser l'outil Rule Author pour vous assurer que les attributs associés à `EAS_EVENT` correspondent aux mappages de données de la table `GEM_EVENT`.

Cycles de vie

Dans CEP, les cycles de vie sont des intervalles pendant lesquels des situations (règles d'événement) sont applicables. Un cycle de vie commence toujours par un initiateur et finit toujours par un terminateur. Il est associé à une classe d'événement.

Pour le gestionnaire d'événements, la classe d'événement EVENT doit inclure l'initiateur de cycle de vie `EAS_START` et le terminateur de cycle de vie `EAS_STOP`.

Situations

Dans Rule Author, les situations sont l'équivalent des *règles d'événement*.

Vous pouvez utiliser l'outil Rule Author pour configurer des situations qui définissent les règles métier déterminant les événements ou la combinaison d'événements pertinents pour votre société et les éléments déclencheurs d'une alerte.

Les situations sont associées à un projet CEP et à une classe d'événement et sont incluses dans le fichier de règles d'événement `cep.xml` .

Lorsque les données UMF passent dans le pipeline, les enregistrements (ou les documents d'entrée `UMF_ENTITY`) qui contiennent une définition de segment de données `EVENT` sont envoyés au moteur CEP. Le moteur CEP traite les données d'événement entrantes en fonction des situations configurées dans le fichier de règles d'événement cep.xml. Si un événement satisfait ou dépasse une situation définie, le moteur CEP renvoie une alerte d'événement dans le pipeline ; cette alerte peut être affichée dans les applications Analyst Toolkit ou à l'aide d'un outil de visualisation de votre choix.

Condition de seuil

Les conditions de seuil sont définies dans une règle d'événement (situation). Elles s'apparentent à des filtres de données ou à des contrôles rapides de données. Lors du traitement, le moteur CEP vérifie les données d'événement entrantes pour déterminer si elles remplissent la condition de seuil indiquée avant de les traiter en utilisant la règle. Si les données remplissent la condition de seuil, le moteur CEP traite les données d'événement en fonction de la règle. Si elles ne remplissent pas la condition de seuil, le moteur CEP passe à la règle d'événement suivante.

Par exemple, pour traiter uniquement les événements de la filiale 102, créez une condition de seuil indiquant `EVENT_LOC='102'`.

Clé UMF_LOG_ID

Le numéro `UMF_LOG_ID` est un numéro séquentiel unique attribué à chaque enregistrement lors de son traitement. Dans un projet CEP, le numéro `UMF_LOG_ID` est une clé de regroupement associée à l'ensemble des classes d'événement et des indicateurs de cycle de vie requis du gestionnaire d'événements. Cette clé de regroupement permet de s'assurer que tous les enregistrements entrants dotés du même numéro `UMF_LOG_ID` sont traités ensemble.

Si vous importez le fichier `cep.xml` initial inclus avec le produit dans un projet CEP, la clé `UMF_LOG_ID` est déjà configurée et affectée aux classes d'événement et aux indicateurs de cycle de vie du gestionnaire d'événements.

Configuration du fichier de règles d'événement cep.xml

Les informations configurées dans le fichier des règles d'événements `cep.xml` déterminent la manière dont le Gestionnaire des événements et le moteur CEP traitent des données d'événement entrantes et les réponses renvoyées à votre application client, au pipeline, à la base de données de l'entité et aux applications. Les règles d'événement représentent une grande partie des informations incluses dans le fichier `cep.xml` mais d'autres informations doivent également y figurer. Il est nécessaire d'indiquer d'autres éléments et paramètres pour traiter correctement des événements via le gestionnaire d'événements.

Le produit contient un fichier de règles d'événement `cep.xml` initial qui contient les éléments et les paramètres nécessaires, déjà configurés pour vous. Si vous importez le fichier `cep.xml` initial, il est inutile de configurer ou de modifier ces éléments ou ces paramètres ; En revanche, vous pouvez vous concentrer sur la configuration

des règles métier d'événement et l'ajout des règles au fichier cep.xml. Les règles d'événement variant d'une société à l'autre, le fichier cep.xml initial ne contient pas de règles d'événement préconfigurées (ou types de situation).

Eléments et paramètres obligatoires du fichier cep.xml

Ces informations sont fournies à titre de référence. Si vous choisissez de ne pas importer le fichier cep.xml initial fourni et décidez de créer intégralement le fichier par vous-même, utilisez les informations suivantes pour vous assurer que le fichier contient tous les éléments et les paramètres obligatoires. Si le fichier de règles d'événement cep.xml que vous exportez pour l'utiliser avec le gestionnaire d'événements est incomplet (sans ces informations), le gestionnaire d'événements ne peut pas traiter les données d'événement entrantes.

Classes d'événements
Les classes d'événement décrivent les différentes structures d'événement que le moteur CEP doit connaître. Pour traiter des événements, les classes d'événement suivantes doivent faire partie du fichier de règles d'événement cep.xml :

EAS_START.event
Cette classe d'événement devient l'initiateur de cycle de vie ou le signal indiquant au moteur CEP de lancer le traitement de l'événement.

EAS_STOP.event
Cette classe d'événement devient le terminateur du cycle de vie du gestionnaire d'événements ou le signal indiquant au moteur CEP d'arrêter le traitement de l'événement.

EVENT.event
Cette classe d'événement est la base de chaque règle métier d'événement que vous créez. Elle contient des informations qui mappent les données d'enregistrement entrantes à la table du gestionnaire d'événements (GEM_EVENT) et au segment de données EVENT.

Délai Dans CEP, un cycle de vie est un intervalle au cours duquel des règles d'événement sont applicables. Le pipeline traitant les données pratiquement en temps réel, le cycle de vie a pour seule fonction de signaler le début et la fin d'un enregistrement d'événement.

Les informations de cycle de vie nécessaires pour le traitement du gestionnaire d'événements comprennent les éléments suivants :

EAS_START
Cet élément est l'initiateur obligatoire du cycle de vie et signale le début d'un événement. Vous pouvez définir cet élément de cycle de vie dans la table **Event Initiators** dans l'onglet **Lifespan: Initiators**.

EAS_STOP
Cet élément est le terminateur obligatoire du cycle de vie et signale la fin d'un événement. Vous sélectionner le terminateur pour **Terminate By Event** dans l'onglet **Lifespan: Terminators & Keys**.

Clé de regroupement UMF_LOG_ID
Un numéro UMF_LOG_ID est un numéro séquentiel unique attribué à chaque enregistrement lors de son traitement. Dans un projet CEP, la clé de regroupement UMF_LOG_ID permet de s'assurer

que tous les enregistrements entrants dotés du même numéro UMF_LOG_ID sont traités ensemble. Cette clé de regroupement est affectée à l'ensemble des classes d'événement et des indicateurs de cycle de vie.

Attributs EVENT.event

Les attributs obligatoires de cette classe d'événement sont directement mappés au segment de données EVENT, qui correspond aux zones de la table GEM_EVENT dans la base de données d'entités. Si l'un de ces attributs obligatoires ne figure pas dans le fichier EVENT.event, le traitement des événements échoue. Il est possible qu'un ou plusieurs messages d'erreur s'affichent pour signaler des données XML non valides ou mal structurées ou des informations manquantes dans le fichier XML de configuration CEP.

Indiquez ces attributs dans l'onglet **Situation**: **General & Event** de chaque règle d'événement.

Création d'un projet CEP :

Les projets CEP sont des regroupements de règles d'événement, de cycles de vie et d'autres informations d'événement utilisés par le gestionnaire d'événements et le moteur CEP. Ils font partie du fichier de règles d'événement cep.xml et sont créés et gérés dans l'outil CEP Rule Author d'Eclipse. Avant de configurer les règles métier d'événement pour le gestionnaire d'événements, vous devez définir un projet CEP.

Avant de commencer

- Vous devez avoir installé l'outil CEP Rule Author et décompressé ses fichiers.
- L'outil CEP Rule Author fonctionne uniquement sur un système Microsoft Windows et requiert Java version 1.5 ou suivante.

Procédure

1. Dans l'outil CEP Rule Author, sélectionnez **File** > **New** > **Project**.
2. Sélectionnez **Event Processing Project** et cliquez sur **Next**.
3. Cliquez sur **Finish**. Le projet CEP s'affiche dans le volet de navigation de gauche.

Que faire ensuite

Importez le fichier des règles d'événements ibm-home\gem\cep.xml de démarrage inclus dans l'installation de votre produit. Ce fichier contient déjà les éléments et les paramètres nécessaires pour utiliser le gestionnaire d'événements. Après avoir importé les objets nécessaires dans le projet CEP, vous pouvez configurer les règles métier d'événement, puis exporter le fichier de règles d'événement cep.xml final pour lancer le traitement des événements via le gestionnaire des événements.

Importation du fichier de règles d'événement cep.xml :

Le fichier de règles d'événement cep.xml contient les informations que le moteur CEP et le gestionnaire d'événements utilisent pour traiter les événements et générer des alertes d'événement. Un fichier cep.xml initial qui contient déjà les éléments et les paramètres requis pour fonctionner avec le gestionnaire d'événements est inclus avec le produit installé. Au lieu de créer complètement le fichier, importez le fichier cep.xml existant dans un projet CEP.

Avant de commencer

- Effectuez une copie de sauvegarde du fichier de règles d'événement `cep.xml` d'origine pour pouvoir le restaurer, si nécessaire. Envisagez de conserver le fichier dans un système de gestion de versions ou un système de contrôle source.
- Vous devez avoir installé l'outil Rule Author d'Eclipse et avoir décompressé ses fichiers.
- L'outil Rule Author fonctionne uniquement sur un client Microsoft Windows et requiert Java version 1.5 ou suivante.
- Vous devez avoir déjà créé un projet CEP dans l'outil Rule Author.

Procédure

1. Dans l'outil Rule Author, sélectionnez **File** > **Import**.
2. Sélectionnez **Event Processing Definition** et cliquez sur **Next**.
3. Recherchez et sélectionnez le fichier `cep.xml`. Veillez à modifier le type de fichier par défaut en remplaçant `DEF` par `XML`. D'une manière générale, ce fichier se trouve dans le répertoire *répertoire_installation_produit*`\ibm-home\gem`.
4. Vérifiez les éléments suivants :
   - Vérifiez que tout le contenu du fichier est sélectionné. (Développez le dossier de niveau supérieur pour examiner le contenu du fichier, si nécessaire.)
   - Vérifiez que le nom du projet CEP approprié s'affiche. (Naviguez pour sélectionner le projet, si nécessaire.)
5. Cliquez sur **Finish**. Cliquez sur **OK** pour remplacer le fichier existant, si vous recevez ce message. Une fois que le fichier est importé, plusieurs signes plus s'affichent dans le sous-panneau de navigation de gauche de l'outil Rule Author.

Que faire ensuite

Ajoutez des règles d'événements métier, puis exportez le fichier des règles d'événements `cep.xml` dans le répertoire *répertoire_installation_produit*`\ibm-home\gem\`.

Exportation du fichier de règles d'événement cep.xml :

Pour permettre au gestionnaire d'événements d'exécuter les règles CEP (Complex Event Processing), vous devez exporter le fichier de règles d'événement `cep.xml` configuré dans l'outil Rule Author d'Eclipse.

Avant de commencer

L'outil Rule Author fonctionne uniquement sur un client Microsoft Windows et requiert Java version 1.5 ou suivante.

Pourquoi et quand exécuter cette tâche

- Si le moteur CEP est déjà en cours d'exécution lorsque vous exportez le fichier de règles d'événement, vous devez le recharger sur le système IBM WebSphere Server pour appliquer les modifications apportées au nouveau fichier de règles d'événement `cep.xml` exporté.

Procédure

1. Dans l'outil Rule Author, sélectionnez **File** > **Export**.
2. Sélectionnez **Event Processing Definition** et cliquez sur **Next**.

3. Sélectionnez le projet CEP.
4. Définissez le fichier de définition de traitement d'événements dans le nouveau fichier de règles d'événement `cep.xml`. D'une manière générale, le fichier se trouve dans *répertoire_installation_produit*`\ibm-home\gem\cep.xml`.
5. Cliquez sur **Finish**. Si le système vous invite à remplacer un fichier `cep.xml` existant, cliquez sur **OK**.
6. Facultatif : Si le système IBM WebSphere Server est en cours d'exécution, rechargez les règles CEP. Lorsque le moteur CEP démarre sur le serveur d'applications du produit, CEP charge le fichier de règles d'événement `cep.xml` en cours. Si le serveur WebSphere est en cours d'exécution lors de l'exportation du fichier, les modifications ne sont pas appliquées jusqu'au rechargement du nouveau fichier `cep.xml`.
   a. Ouvrez une fenêtre du navigateur Web et accédez au serveur WebSphere. Par exemple, `http://localhost:13510/gem`.
   b. Cliquez sur **Reload Rules** (Règles de rechargement).

      Remarque : Le serveur WebSphere n'indique pas explicitement que les règles ont été rechargées.

Instructions de configuration des résultats d'une règle d'événement

Les règles d'événement définissent le mode de traitement des événements et les situations qui génèrent des alertes. Les règles d'événement (appelées *types de situation* dans l'outil CEP Rule Author d'Eclipse) sont incluses dans le fichier de règles d'événement `cep.xml` que le gestionnaire d'événements et le moteur CEP utilisent pour traiter les données d'événement entrantes. Les règles d'événement complexes que vous définissez sont propres à votre société.

Avant de commencer à définir des règles d'événement, prenez en compte les éléments suivants pour que la règle fonctionne avec le gestionnaire d'événements :

- N'oubliez pas que les règles d'événement doivent s'appliquer à une entité et aux transactions qu'une entité peut effectuer. Les entités sont généralement des personnes mais elles peuvent également représenter un site ou un bien matériel. Par exemple, une entité peut être un navire.
- Les règles d'événement doivent être indiquées sous la forme d'une instruction déclarative (telle que 'Location=Texas') ou d'une expression mathématique (sum, count, average) appliquée à une période donnée.

Attributs de situation requis pour chaque règle métier d'événement

Pour renvoyer les données d'événement d'un processeur d'événements complexes à la base de données d'entités, vous devez ajouter manuellement les attributs de situation requis à chaque règle métier d'événement que vous créez. Ces attributs ne font pas partie du fichier de règles d'événement `cep.xml` initial. L'importation du fichier initial ne crée donc pas automatiquement des règles métier d'événement (situations) ni n'ajoute ces attributs à des règles nouvelles ou existantes.

Ces attributs de situation mappent directement les données d'événement à la table `GEM_EVENT` du gestionnaire d'événements (et correspondent au segment UMF de chaque enregistrement d'événement entrant). Si vous omettez ces attributs obligatoires, aucune donnée traitée par le moteur CEP n'est renvoyée au gestionnaire d'événements via le pipeline.

Tableau 4. Attributs de situation obligatoires pour les règles métier d'événement complexes

Nom d'attribut	Type d'attribut	Expression d'attribut	Description d'attribut
EVENT_SIT_STATUS	chaîne	"PENDING" (EN ATTENTE)	Indique le statut de l'alerte d'événement. Dans le plug-in i2, Explorer, et dans le rapport récapitulatif d'alerte Cognos, l'état d'alerte d'événement est affiché dans le Récapitulatif d'alerte. L'état de toutes les alertes nouvellement générées est généralement "en attente", ce qui signifie qu'un analyste doit analyser et prendre les dispositions relatives à cette alerte. N'oubliez pas qu'un statut d'alerte d'événement peut être n'importe quel événement pertinent pour votre société et qu'il est configuré en tant que statut d'événement dans la console de configuration. Si vous ne souhaitez pas voir l'événement s'afficher dans les interfaces utilisateur du composant Analyst Toolkit, utilisez l'état d'alerte d'événement "FERMÉ".

Tableau 4. Attributs de situation obligatoires pour les règles métier d'événement complexes (suite)

Nom d'attribut	Type d'attribut	Expression d'attribut	Description d'attribut
REASON_DESC	chaîne	"<*Description de la règle ou de l'alerte d'événement*>"	Décrit la règle d'événement qui a déclenché l'alerte d'événement. Indiquez une description aussi explicite que possible pour vos analystes. Par exemple, si la règle d'événement génère une alerte lorsqu'une entité effectue une transaction de plus de 1500 dollars en 24 heures, vous pouvez entrer "Sommesupérieurà1500" comme REASON_DESC.
ALERT_GROUP	chaîne	"<*groupe d'alertes*>"	Indique à quel groupe d'alertes attribuer les alertes d'événements générées à partir de cette règle d'événement. D'une manière générale, cette valeur est "DEFAULT" (VALEUR PAR DEFAUT), vous pouvez aussi entrer n'importe quel groupe d'alertes configuré dans la console de configuration.

Affichage des détails des alertes d'événement

Les alertes d'événement sont généralement déclenchées par plusieurs événements complexes. Vous pouvez afficher les alertes d'événements dans les applications Analyst Toolkit ou dans une application client, mais par défaut, les détails des événements qui constituent cette alerte ne sont pas inclus.

Si vous souhaitez inclure les détails des événements qui composent l'alerte des événements, vous devez inclure l'attribut de situation suivant:

Tableau 5. Paramètres nécessaires pour créer l'attribut de situation EVENTS dans une règle d'événement

Nom	Type	Expression	Dimension (bouton Show Advanced (Affichage avancé))
EVENTS	entier	Event.EventID	[] (pour indiquer que l'élément EventID est un tableau] Vous devez modifier l'attribut de situation et cliquez sur Show Advanced pour afficher et définir le paramètre pour cette colonne.

Meilleures pratiques

Si vous affichez vos alertes d'événement dans les applications Analyst Toolkit, conservez pour l'attribut de situation REASON_DESC une chaîne de texte simple, au lieu d'ajouter au message des valeurs issues de l'événement. Analyst Toolkit regroupe les alertes communes dans un récapitulatif d'alerte qui inclut un compte du nombre d'alertes figurant dans le récapitulatif. Les analystes cliquent sur un récapitulatif d'alerte pour connaître toutes les alertes incluses dans ce récapitulatif.

Si vous définissez des valeurs de l'événement dans l'attribut REASON_DESC, chaque alerte d'événement s'affiche sous la forme d'un récapitulatif d'alerte distinct ; Cela signifie que les analystes visualisent toutes les alertes d'événement dans le récapitulatif d'alerte comme dans les sections d'alerte de la fenêtre Récapitulatif des alertes.

Création d'une règle d'événement pour calculer la somme d'événements complexes

Vous pouvez créer une règle d'événement de base SUM pour calculer la somme totale d'événements et créer une alerte si la somme de ces événements dépasse un seuil défini. Par exemple, vous pouvez créer une règle d'événement qui calcule la somme de tous les virements effectués par une personne en 24 heures et qui envoie une alerte d'événement si la somme de ces virements (événements) est supérieure à 15000 dollars.

Avant de commencer

Vous devez disposer d'un projet CEP, qui regroupe des règles d'événement et toutes les configurations de règles.

Pourquoi et quand exécuter cette tâche

Les étapes suivantes contiennent les instructions de base pour créer une règle métier simple qui calcule la somme de la valeur de votre choix. Pour certaines étapes, il existe plusieurs méthodes qui aboutissent au même résultat final. Pour connaître les autres options disponibles, reportez-vous à la section relative aux *situations* du document IBM Advanced Middleware Technology User's Guide (guide de l'outil CEP Rule Author d'Eclipse), inclus avec le produit.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez à l'aide du bouton droit de la souris sur **Situation** et sélectionnez **New** > **Situation**. Vérifiez que le nom de projet approprié s'affiche dans la section **Event Processing Project**.
2. Entrez un nom de règle unique dans la zone **Situation name**. Le nom de la situation correspond au nom de la règle d'événement qui s'affiche dans la base de données d'entités et dans le composant Visualizer, si vous décidez d'afficher les alertes d'événement dans cette application. Indiquez un nom pertinent pour les utilisateurs qui analysent les alertes d'événement. Par exemple, si vous créez une règle pour obtenir la somme de tous les événements, puis envoyer une alerte si la somme des événements dépasse le seuil 15000, vous pouvez nommer cette règle `SommePlusde15K`.
3. Dans la zone **Select source**, sélectionnez **Empty of Type**, puis **atleast** dans la liste déroulante. La situation **atleast** peut effectuer la somme des valeurs d'événement et conserver les informations des événements qui respecte la règle d'événement. Pour plus d'informations sur les types de situation, reportez-vous à la section relative aux *propriétés de situation* dans le guide d'utilisation.
4. Cliquez sur **Finish**. Lorsque l'écran principal des situations s'affiche, il est possible que des erreurs apparaissent dans la section **Problems**. Ces erreurs indiquent les valeurs manquantes mais vous pouvez ignorer les erreurs à ce stade. Au fur et à mesure que vous suivez ces étapes, les erreurs disparaissent.
5. Dans la section **Events**, sélectionnez `EVENT` comme événement de base pour cette règle. `EVENT` est toujours l'événement de base de chaque règle métier d'événement. Il contient le mappage nécessaire vers la base de données `GEM_TABLE` et le segment de données `EVENT`.
6. Facultatif : Vous pouvez créer une *condition de seuil* pour filtrer les événements avant de les évaluer avec cette règle afin de ne prendre en compte que les événements respectant la condition de seuil indiquée.
7. Pour générer l'expression de calcul, cliquez sur **Show Advanced**, puis sur **Edit**.
8. Dans la zone **Quantifier**, sélectionnez `each`. Cette option permet de s'assurer que chaque enregistrement d'événement entrant qui remplit les conditions de cette règle d'événement est inclus dans la somme totale.
9. Dans la zone **Weight**, cliquez sur **...** pour modifier la zone. Utilisez le **générateur d'expression** pour sélectionner la zone d'événement à additionner. Vérifiez que l'expression s'affiche dans la zone **Expression Builder Text** (Texte du générateur d'expression), puis cliquez sur **OK**. Par défaut, le poids de chaque événement correspond à 1. Lorsque la règle d'événement est évaluée, la somme de tous les poids est comparée à l'attribut **Quantity** dans l'onglet **Condition & Results**. Lorsque le total est au moins égal à la quantité indiquée, une alerte d'événement est générée. Par exemple, pour additionner les valeurs de chaque événement qui respecte la règle d'événement, sélectionnez `EVENT.EVENT_VALUE`.
10. Facultatif : Si la zone sélectionnée en tant que poids contient des valeurs décimales (type double), utilisez le générateur d'expression pour générer l'expression suivante :
    a. Multipliez les résultats du calcul par 100 pour conserver les valeurs décimales et convertir les dollars en cents.
    b. Convertissez le type double en type entier. Vous pouvez effectuer cette opération en utilisant des fonctions.

Par exemple, si vous effectuez le total des événements (EVENT.EVENT_VALUE), vous pouvez entrer EVENT.EVENT_VALUE*100 dans la zone **Expression Builder Text** . Vous pouvez sélectionner **Functions** > **Math** > **Round** pour arrondir le résultat à l'entier le plus proche. L'expression finale apparaît sous la forme Round(EVENT.EVENT_VALUE*100).

11. Dans la zone **Sum Expression**, cliquez sur **...** pour modifier la zone et sélectionnez la zone d'événement à additionner. Par exemple, pour additionner la valeur de chaque événement qui respecte ou dépasse la règle d'événement, sélectionnez EVENT_VALUE .
12. Facultatif : Pour calculer la somme des événements qui remplissent une condition spécifique, entrez la condition dans la zone **Threshold Condition** ou utilisez le générateur d'expression pour vous assister. Par exemple, pour additionner uniquement les valeurs d'événement de la filiale 102, entrez EVENT.EVENT_LOC="102". Cette zone agit comme un filtre et ignore automatiquement les événements qui ne respectent pas ou qui dépasse la condition.

    Conseil : Pour simplifier la vue et visualiser plus facilement la section **Threshold Condition**, cliquez sur **Hide Advanced**.
13. Dans l'onglet **Condition & Results** de la section **Lifespan**, sélectionnez EASLifeSpan. Cette zone apparaît en rouge jusqu'à ce que vous effectuiez une sélection. La couleur rouge indique que la zone est obligatoire et qu'elle fait partie des erreurs répertoriées à la section **Problems**. Lorsque vous sélectionnez un cycle de vie, l'erreur disparaît de la section **Problems**.
14. Dans la quantité **Quantity**, entrez la quantité minimale que la règle d'événement doit atteindre avant de générer une alerte. Veillez à multiplier les montants en dollars par 100. Par exemple, pour générer une alerte d'événement lorsque la somme atteint au moins 15000 dollars, entrez 150000.
15. Dans la zone **Detection Mode**, notez que l'option immediate est sélectionnée. Conservez-la. Le mode de détection détermine quand la somme doit être calculée et les résultats envoyés. L'option immediate génère une alerte dès que la somme atteint la quantité.
16. Dans la zone Situation Attributes, entrez les valeurs de situation requises pour les attributs de situation suivants :
    - EVENT_SIT_STATUS
    - REASON_DESC
    - ALERT_GROUP
17. Facultatif : Pour conserver les détails de tous les événements inclus dans la somme, ajoutez l'attribut de situation EVENTS en utilisant les informations suivantes :
    a. Dans la zone **Name**, entrez EVENTS,
    b. Dans la zone **Type**, entrez integer.
    c. Dans la zone **Expression**, entrez EVENT_ID (ou sélectionnez-le dans le **générateur d'expression**).
    d. Cliquez sur **Show Advanced** pour afficher la colonne **Dimensions** et entrez [] dans la colonne pour indiquer que le type est un tableau d'événements.

    Ces valeurs demandent à CEP de renvoyer au pipeline le numéro interne EVENT_ID de chaque événement inclus dans le total avec l'alerte d'événement. Le pipeline stocke chaque numéro EVENT_ID dans la base de données d'entités et envoie les informations au composant Visualizer ou à l'application client

utilisée pour afficher les alertes d'événement. Le numéro `EVENT_ID` est un numéro séquentiel interne (ID) créé par le pipeline lorsqu'il envoie les données d'événement au moteur CEP.

18. Enregistrez la règle d'événement.

Création d'une règle d'événement pour comptabiliser des événements complexes

Vous pouvez créer une règle d'événement de base COUNT pour comptabiliser des événements et créer une alerte d'événement si la valeur totale dépasse un seuil défini. Par exemple, vous pouvez créer une règle d'événement qui comptabilise toutes les transactions de virement au cours des dernières 24 heures et qui envoie une alerte d'événement si le nombre de transactions est supérieur à 500.

Avant de commencer

Vous devez disposer d'un projet CEP, qui regroupe des règles d'événement et toutes les configurations de règles.

Pourquoi et quand exécuter cette tâche

Les étapes suivantes contiennent les instructions de base pour créer une règle métier simple qui comptabilise la valeur de votre choix. Pour certaines étapes, il existe plusieurs méthodes qui aboutissent au même résultat final. Pour connaître les autres options disponibles, reportez-vous à la section relative aux *situations* du document IBM Advanced Middleware Technology User's Guide (guide de l'outil CEP Rule Author d'Eclipse), inclus avec le produit.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez à l'aide du bouton droit de la souris sur **Situation** et sélectionnez **New** > **Situation**. Vérifiez que le nom de projet approprié s'affiche dans la section **Event Processing Project**.
2. Entrez un nom de règle unique dans la zone **Situation name**. Le nom de la situation correspond au nom de la règle d'événement qui s'affiche dans la base de données d'entités et dans le composant Visualizer, si vous décidez d'afficher les alertes d'événement dans cette application. Indiquez un nom pertinent pour les utilisateurs qui analysent les alertes d'événement. Par exemple, si vous créez une règle pour comptabiliser tous les événements d'une filiale spécifique, vous pouvez nommer cette règle `NombreTransactionsFiliale102`.
3. Dans la zone **Select source**, sélectionnez **Empty of Type**, puis sélectionnez l'une des valeurs suivantes dans la liste déroulante :
   - **atleast** : Au moins *n* événements ont été transmis lors du cycle de vie.
   - **atmost** : Pas plus de *n* événements ont été transmis avant la fin du cycle de vie.

   Les deux types de situation peuvent comptabiliser des valeurs d'événement et conserver les informations de chaque événement qui respecte la règle d'événement. Pour plus d'informations sur les types de situation, reportez-vous à la section relative aux *propriétés de situation* dans le guide d'utilisation.
4. Cliquez sur **Finish**. Lorsque l'écran principal des situations s'affiche, il est possible que des erreurs apparaissent dans la section **Problems**. Ces erreurs indiquent les valeurs manquantes mais vous pouvez ignorer les erreurs à ce stade. Au fur et à mesure que vous suivez ces étapes, les erreurs disparaissent.

5. Dans la section **Events**, sélectionnez EVENT comme événement de base pour cette règle. EVENT est toujours l'événement de base de chaque règle métier d'événement. Il contient le mappage nécessaire vers la base de données GEM_TABLE et le segment de données EVENT.
6. Facultatif : Vous pouvez créer une *condition de seuil* pour filtrer les événements avant de les évaluer avec cette règle afin de ne prendre en compte que les événements respectant la condition de seuil indiquée.
7. Dans l'onglet **Condition & Results** de la section **Lifespan**, sélectionnez EASLifeSpan. Cette zone apparaît en rouge jusqu'à ce que vous effectuiez une sélection. La couleur rouge indique que la zone est obligatoire et qu'elle fait partie des erreurs répertoriées à la section **Problems**. Lorsque vous sélectionnez un cycle de vie, l'erreur disparaît de la section **Problems**.
8. Dans la section **Quantity**, entrez la quantité "atleast" ou "atmost" que la règle d'événement doit atteindre avant de générer l'alerte d'événement.
9. Dans la zone **Detection Mode**, notez que l'option immediate est sélectionnée. Conservez-la. Le mode de détection détermine quand la somme doit être calculée et les résultats envoyés. La sélection de l'option immediate génère une alerte dès que la quantité est atteinte.
10. Dans la zone Situation Attributes, entrez les noms, les types et les expressions d'attribut de situation requis :
    - EVENT_SIT_STATUS
    - REASON_DESC
    - ALERT_GROUP
11. Pour conserver les détails de tous les événements pris en compte dans la comptabilisation, ajoutez l'attribut de situation EVENTS en utilisant les informations suivantes :
    a. Dans la zone **Name**, entrez EVENTS,
    b. Dans la zone **Type**, entrez integer.
    c. Dans la zone **Expression**, entrez EVENT_ID (ou sélectionnez-le dans le **générateur d'expression**).
    d. Cliquez sur **Show Advanced** pour afficher la colonne **Dimensions** et entrez [] dans la colonne pour indiquer que le type est un tableau d'événements.

    Ces valeurs demandent à CEP de renvoyer au pipeline le numéro interne EVENT_ID de chaque événement inclus dans le total avec l'alerte d'événement. Le pipeline stocke chaque numéro EVENT_ID dans la base de données d'entités et envoie les informations au composant Visualizer ou à l'application client utilisée pour afficher les alertes d'événement. Le numéro EVENT_ID est un numéro séquentiel interne (ID) créé par le pipeline lorsqu'il envoie les données d'événement au moteur CEP.
12. Enregistrez la règle d'événement.

Accessibilité

Les fonctions d'accessibilité ont pour vocation d'aider les personnes atteintes d'un handicap physique, par exemple une mobilité réduite ou une vue déficiente, à se servir efficacement de leurs logiciels.

La liste suivante répertorie les principale fonctions d'accessibilité :

- La totalité des fonctions de l'interface sont disponibles lors de la navigation au moyen du clavier au lieu de la souris, sous réserve d'utiliser le navigateur Internet Explorer recommandé.

- Ce produit est compatible avec les technologies d'assistance aux personnes handicapées.
- La documentation d'IBM InfoSphere Identity Insight est disponible dans un format accessible.

Accès par le clavier

La console de configuration et le Visualizer d'IBM InfoSphere Identity Insight sont intégralement accessibles lorsqu'ils sont visualisés dans le navigateur Internet Explorer.

Vous pouvez utiliser la console de configuration ou le Visualizer en ne vous servant que du clavier. Vous pouvez, à l'aide de touches ou de combinaisons de touches, effectuer des opérations également possibles à l'aide d'une souris. Les touches de système d'exploitation standard servent aux opérations de système d'exploitation standard.

Dans tous les systèmes d'exploitation et navigateurs gérés, la partie de la fenêtre active où la touche actionnée produira son effet est en surbrillance. Les champs de saisie et de texte affichent un curseur de point d'insertion clignotant. les autres champs sont mis en surbrillance avec une bordure en tirets.

Remarque : La console de configuration est accessible via le clavier à l'aide du navigateur Mozilla Firefox, mais le problème suivant a été signalé : les raccourcis au moyen des touches **Alt** + ***numéro*** ne sont pas compatibles avec ce navigateur.

Affichage accessible

La console de configuration et le Visualizer bénéficient de fonctions qui en améliorent l'accessibilité à l'intention des personnes souffrant d'une vue médiocre ou autres déficiences visuelles. Parmi ces perfectionnements de l'accessibilité figurent la possibilité de personnaliser les propriétés des polices.

Vous pouvez choisir la couleur, la taille et la police du texte des menus des boîtes de dialogue, par interface :

- Console de configuration : via les paramètres de votre navigateur
- Visualizer : via les paramètres **Configuration des préférences d'écran**

Aucune des fonctions de ce produit ne nécessite de distinguer les couleurs.

Compatibilité avec les technologies d'assistance aux personnes handicapées

L'interface du Visualizer gère l'interface de programme d'application Java Accessibility, qui permet d'utiliser les lecteurs d'écran et autres technologies d'assistance aux handicapés. Dans la console de configuration, vous pouvez activer des lecteurs d'écran dans les navigateurs compatibles.

Documentation accessible

La documentation d'IBM InfoSphere Identity Insight est disponible au format XHTML 1.0, consultable avec la plupart des navigateurs Web. Le format XHTML permet de consulter une documentation selon les préférences définies dans votre navigateur. Il permet également de recourir à des lecteurs d'écran et autres technologie d'assistance aux handicapés.

Raccourcis clavier de la console de configuration

La console de configuration est pleinement accessible lorsqu'elle est affichée avec les navigateurs pris en charge, c'est-à-dire que vous pouvez, à l'aide de touches ou de combinaisons de touches, effectuer des opérations également possibles à l'aide d'une souris.

Remarque : La console de configuration peut être parcourue à l'aide du clavier dans le navigateur Mozilla Firefox, mais les combinaisons de touches **Alt** + ***chiffre*** indiquées ne fonctionnement pas correctement dans ce navigateur.

Tableau 6. Raccourcis clavier généraux

Action	**Raccourci**
Passer à l'élément suivant de l'écran (zone de saisie, bouton, lien) en évidence (ignore les zones en lecture seule)	**Tabulation**
Revenir à l'élément précédent de l'écran (zone de saisie, bouton, lien) en évidence (ignore les zones en lecture seule)	**Maj** + **Tabulation**
Effectuer une opération (lien ou bouton)	**Entrée**

Tableau 7. Navigation inter-zone

Action	**Touche ou raccourci**
Monter ou descendre dans une liste déroulante Monter ou descendre dans les lignes d'une zone de saisie	Flèches vers le haut et le bas
Se déplacer vers la gauche ou la droite dans une zone de saisie	Flèches vers la gauche ou la droite
Aller au début d'une zone de saisie Revenir au début de la ligne actuelle dans une zone de texte importante	**Origine**
Aller à la fin d'une zone de saisie Aller à la fin de la ligne actuelle dans une zone de texte importante	**Fin**
Aller à la fin d'une zone de saisie Aller à la page suivante d'une zone de saisie	**Page suivante**
Aller au début d'une zone de saisie Aller à la page précédente d'une zone de saisie	**Page précédente**
Développer ou condenser une liste déroulante	**Alt** + flèche vers le haut ou le bas
Aller au début d'une zone de texte	**Ctrl** + **Page précédente**
Aller à la fin d'une zone de texte	**Ctrl** + **Page suivante**

Tableau 8. Navigation à l'écran

Action	**Raccourci**
(A utiliser avec les lecteurs d'écran) Ignorer tous les liens de navigation et d'action dans l'en-tête de la page.	**Alt** + **0**

Tableau 8. Navigation à l'écran (suite)

Action	Raccourci
Mettre en évidence les actions de la zone d'emplacement et de l'angle supérieur droit	**Alt** + **1**
Mettre en évidence les menus ou sous-menus	**Alt** + **2**
Mettre en évidence les onglets de niveau supérieur	**Alt** + **3**
Mettre en évidence les liens de niveau supérieur	**Alt** + **4**
(Ecrans Détails uniquement) Mettre en évidence les éléments du volet de navigation de gauche	**Alt** + **5**
(Ecrans Détails uniquement) Mettre en évidence les sous-onglets et les boutons d'action de détail	**Alt** + **6**
Mettre en évidence toute zone de formulaire de la zone de contenu principal	**Alt** + **7**
(A utiliser avec les lecteurs d'écran) Ignorer le répertoire d'accès aux zones des écrans Détails	**Alt** + **8**
(A utiliser avec les lecteurs d'écran) Passer au pied de page d'aide situé au bas de l'écran	**Alt** + **9**

Tableau 9. Modification d'actions (dans des zones de saisie)

Action	Raccourci
Copier	**Ctrl** + **C**
Couper	**Ctrl** + **X**
Coller	**Ctrl** + **V**
Sélectionner tout	**Ctrl** + **A**
Annuler	**Ctrl** + **Z**
Supprimer le caractère situé à gauche du curseur	**Retour arrière**
Supprimer le caractère situé à droite du curseur	**Suppr**

Raccourcis clavier du Visualizer

Le Visualizer est pleinement accessible, c'est-à-dire que vous pouvez, à l'aide de touches ou de combinaisons de touches, effectuer des opérations également possibles à l'aide d'une souris.

Tableau 10. Raccourcis clavier généraux

Action	Raccourci
Passer à l'élément d'écran suivant (zone de saisie, bouton, lien) en évidence	**Tabulation**
Revenir à l'élément d'écran précédent (zone de saisie, bouton, lien) en évidence	**Maj** + **Tabulation**
Effectuer une opération (lien ou bouton)	**Entrée** ou pression sur la barre d'espace

Tableau 10. Raccourcis clavier généraux (suite)

Action	Raccourci
Afficher l'écran des critères de rapports et afficher par défaut le rapport du générateur d'alertes d'attribut	**Ctrl** + **A**
Afficher l'écran de chargement du fichier UMF	**Ctrl** + **B**
Afficher la boîte de dialogue de changement de mot de passe	**Ctrl** + **H**
Verrouiller l'application – l'utilisateur actuel demeure en session Visualizer , mais l'écran est verrouillé	**Ctrl** + **L**
Afficher la boîte de dialogue d'impression dans les fenêtres ou onglets dont les informations ou rapports peuvent être imprimés (comme le récapitulatif d'entité)	**Ctrl** + **P**
Déconnecter l'utilisateur actuel de la session Visualizer et quitter l'application	**Ctrl** + **Q**
Afficher la boîte de dialogue de configuration des préférences d'écran	**Ctrl** + **R**
Afficher le centre de documentation du produit	**F1**
Afficher la fenêtre A propos qui contient le numéro de version du produit	**Maj** + **F1**

Tableau 11. Navigation inter-zone

Action	Touche ou raccourci
Passer à la zone supérieure ou inférieure Monter ou descendre dans une liste déroulante Monter ou descendre dans les lignes de texte d'une zone de saisie	Flèches vers le haut et le bas
Se déplacer vers la gauche ou la droite dans une zone de saisie	Flèches vers la gauche ou la droite
Aller au début d'une zone de saisie Revenir au début de la ligne actuelle dans une importante zone de texte	**Origine**
Aller à la fin d'une zone de saisie Aller à la fin de la ligne actuelle dans une importante zone de texte	**Fin**
Aller à la fin d'une zone de saisie	**Page suivante**
Aller au début d'une zone de saisie	**Page précédente**
Développer ou condenser une liste déroulante	**Alt** + flèche vers le haut ou le bas
Développer ou réduire un triangle (si le triangle est sélectionné)	Barre d'espace
Passer d'une table à la commande suivante	**Ctrl** + **Tabulation**

Tableau 12. Actions de modification

Action	**Raccourci**
Copier	**Ctrl** + **C**
Couper	**Ctrl** + **X**
Coller	**Ctrl** + **V**
Sélectionner tout le texte dans les zones de texte	**Ctrl** + **A**
Annuler	**Ctrl** + **Z**
Supprimer le caractère situé à gauche du curseur	**Retour arrière**
Supprimer le caractère situé à droite du curseur	**Suppr**

Chapitre 2. Configuration requise et planification

Cette section de référence contient des informations sur les plateformes prises en charge, la configuration requise et l'architecture système.

Détail de la configuration système requise

La configuration requise identifie les composants matériels et logiciels que vous devez installer avant de créer un rapport d'incident avec l'équipe de support technique IBM.

Configuration système requise pour une exécution sur IBM AIX

La liste suivante identifie les produits pris en charge lorsqu'IBM InfoSphere Identity s'exécute sur le système d'exploitation AIX.

Tableau 13. Configuration système requise pour une exécution sur IBM AIX

Systèmes d'exploitation	• IBM AIX 7.1L
Configuration matérielle requise	• POWER7 (64 bits) • POWER6 • POWER5
Java	Les éléments suivants sont installés avec le produit : • Environnement d'exécution Java IBM 64 bits, Version 8
Bases de données	• IBM DB2 Database pour Linux, UNIX et Windows 11.1 • IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Oracle 12c • Oracle 11g Edition 2 (11.2.0.1, 11.2.0.2 ou version supérieure)
Clients de base de données	• Client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1 • Client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Client Oracle 12c lors de la connexion à Oracle 12c • Client Oracle 11g Release 2 lors de la connexion à Oracle 11g Release 2.

Tableau 13. Configuration système requise pour une exécution sur IBM AIX (suite)

Clients JDBC (Java Database Connectivity)	• Pilote JDBC version 9.5 du client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1. • Pilote JDBC version 9.5 du client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5. • Pilotes JDBC Oracle 12c lors de la connexion à Oracle 12c. • Pilotes JDBC Oracle 11g lors de la connexion à Oracle 11g.
Navigateurs Web	• Mozilla Firefox
Logiciel de mise en file d'attente des messages	• IBM WebSphere MQ
Autre	• Composants de l'environnement d'exécution IBM C++ pour AIX, Pour plus d'informations sur cette configuration, consultez les informations suivantes : http://www-01.ibm.com/support/docview.wss?uid=swg24025181

Configuration système requise pour une exécution sur HP-UX

La liste ci-dessous répertorie les produits pris en charge lors de l'exécution d'IBM InfoSphere Identity Insight sur le système d'exploitation HP-UX.

Tableau 14. Configuration système requise pour une exécution sur HP-UX

Systèmes d'exploitation	• HPUX 11i v3
Configuration matérielle requise	• Intel Itanium 2 (IA64)
Java	Les éléments suivants sont installés avec le produit : • Environnement d'exécution Java IBM 64 bits pour HPUX, Java Technology Edition, Version 6
Exigences Java du client	HPUX n'est pas une plateforme client prise en charge. Tous les postes client, dont la plateforme est prise en charge, connectés à la console de configuration ou au Visualizer doivent avoir l'environnement JRE (Java Runtime Environment) SUN version 6 installé.
Bases de données	• IBM DB2 Database pour Linux, UNIX et Windows 11.1 • IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Oracle 12c • Oracle 11g Edition 2 (11.2.0.1, 11.2.0.2 ou version supérieure)

Tableau 14. Configuration système requise pour une exécution sur HP-UX (suite)

Clients de base de données	• Client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1 • Client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Client Oracle 12c lors de la connexion à Oracle 12c • Client Oracle 11g Release 2 lors de la connexion à Oracle 11g Release 2.
Clients JDBC (**Java Database Connectivity) pour la console de configuration et le Visualizer**	• Pilote JDBC version 9.5 du client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1. • Pilote JDBC version 9.5 du client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5. • Pilotes JDBC Oracle 12c lors de la connexion à Oracle 12c. • Pilotes JDBC Oracle 11g lors de la connexion à Oracle 11g.
Navigateurs Web	• Mozilla Firefox
Logiciels de mise en file d'attente des messages pris en charge	• IBM WebSphere MQ

Configuration système requise pour une exécution sur Linux x86

La liste ci-dessous répertorie les produits pris en charge lors de l'exécution d'IBM InfoSphere Identity Insight sur le système d'exploitation Linux x86.

Tableau 15. Configuration système requise pour une exécution sur Linux x86

Systèmes d'exploitation	• Red Hat Enterprise Linux AS, version 6.0 • Red Hat Enterprise Linux AS, Version 5.0 • Novell SUSE Linux Enterprise Server, Version 10
Configuration matérielle requise	• Intel x86 (IA32)
Java	Les éléments suivants sont installés avec le produit : • Environnement d'exécution IBM 32 bits pour Linux sur l'architecture Intel, Java Technology Edition, Version 6
Exigences Java du client	Tous les postes client, dont la plateforme est prise en charge, connectés à la console de configuration ou au Visualizer doivent avoir l'environnement JRE (Java Runtime Environment) SUN version 6 installé.

Tableau 15. Configuration système requise pour une exécution sur Linux x86 (suite)

Bases de données	• IBM DB2 Database pour Linux, UNIX et Windows 11.1 • IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Oracle 12c • Oracle 11g Edition 2 (11.2.0.1, 11.2.0.2 ou version supérieure)
Clients de base de données	• Client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1 • Client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Client Oracle 12c lors de la connexion à Oracle 12c • Client Oracle 11g Release 2 lors de la connexion à Oracle 11g Release 2.
Clients JDBC (**Java Database Connectivity) pour la console de configuration et le Visualizer**	• Pilote JDBC version 9.5 du client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1. • Pilote JDBC version 9.5 du client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5. • Pilotes JDBC Oracle 12c lors de la connexion à Oracle 12c. • Pilotes JDBC Oracle 11g lors de la connexion à Oracle 11g.
Navigateurs Web	• Mozilla Firefox
Logiciels de mise en file d'attente des messages pris en charge	• IBM WebSphere MQ

Configuration système pour une exécution sur Linux for System x

La liste suivante identifie les produits pris en charge lorsqu'IBM InfoSphere Identity Insight s'exécute sur le système d'exploitation Linux for System x.

Tableau 16. Configuration système pour une exécution sur Linux for System x

Systèmes d'exploitation	• Red Hat Enterprise Linux AS, Version 7.0 • Red Hat Enterprise Linux AS, version 6.0
Configuration matérielle requise	• Intel x86_64
Java	Les éléments suivants sont installés avec le produit : • Environnement d'exécution Java IBM 64 bits, Version 8

Tableau 16. Configuration système pour une exécution sur Linux for System x (suite)

Bases de données	• IBM DB2 Database pour Linux, UNIX et Windows 11.1 • IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Oracle 12c • Oracle 11g Edition 2 (11.2.0.1, 11.2.0.2 ou version supérieure)
Clients de base de données	• Client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1 • Client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Client Oracle 12c lors de la connexion à Oracle 12c • Client Oracle 11g Release 2 lors de la connexion à Oracle 11g Release 2.
Clients JDBC (Java Database Connectivity)	• Pilote JDBC version 9.5 du client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1. • Pilote JDBC version 9.5 du client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5. • Pilotes JDBC Oracle 12c lors de la connexion à Oracle 12c. • Pilotes JDBC Oracle 11g lors de la connexion à Oracle 11g.
Navigateurs Web	• Mozilla Firefox
Logiciels de mise en file d'attente des messages pris en charge	• IBM WebSphere MQ

Configuration système requise pour une exécution sur Linux for System z

La liste suivante identifie les produits pris en charge lorsqu'IBM InfoSphere Identity Insight s'exécute sous Linux for System z 64 bits.

Tableau 17. Configuration système requise pour l'exécution de Linux 64 bits sur System z

Systèmes d'exploitation	• Red Hat Enterprise Linux AS, Version 7.0
Configuration matérielle requise	• IBM System z
Java	Les éléments suivants sont installés avec le produit : • Environnement d'exécution Java IBM 64 bits, Version 8

Tableau 17. Configuration système requise pour l'exécution de Linux 64 bits sur System z (suite)

Bases de données	• IBM DB2 Database pour Linux, UNIX et Windows 11.1 • IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Oracle 12c • Oracle 11g Edition 2 (11.2.0.1, 11.2.0.2 ou version supérieure)
Clients de base de données	• Client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1 • Client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Client Oracle 10g Release 2 (10.2.0.2.0) pour la connexion à Oracle 11g Release 1 (11.2.0.1) ou 11g Release 2 (11.2.0.2)
Clients JDBC (Java Database Connectivity)	• Pilote JDBC version 9.5 du client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1. • Pilote JDBC version 9.5 du client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5. • Client Oracle 10g Release 2 (10.2.0.2.0) pour la connexion à Oracle 11g Release 1 (11.2.0.1) ou 11g Release 2 (11.2.0.2)
Navigateurs Web	• Mozilla Firefox
Logiciels de mise en file d'attente des messages pris en charge	• IBM WebSphere MQ

Configuration système requise pour une exécution sur Sun Solaris

La liste ci-dessous répertorie les produits pris en charge lors de l'exécution d'IBM InfoSphere Identity Insight sur le système d'exploitation Sun Solaris.

Tableau 18. Configuration système requise pour une exécution sur Sun Solaris

Systèmes d'exploitation	• Sun Solaris 10.0
Configuration matérielle requise	• UltraSPARC T2 • UltraSPARC IV et suivante
Java	Les éléments suivants sont installés avec le produit : • IBM 64-bit Java Runtime Environment for Solaris, Java Technology Edition, Version 6

Tableau 18. Configuration système requise pour une exécution sur Sun Solaris (suite)

Exigences Java du client	Tous les postes client, dont la plateforme est prise en charge, connectés à la console de configuration ou à Visualizer doivent avoir l'environnement JRE (Java Runtime Environment) SUN Version 6 installé.
Bases de données	• IBM DB2 Database pour Linux, UNIX et Windows 11.1 • IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Oracle 12c • Oracle 11g Edition 2 (11.2.0.1, 11.2.0.2 ou version supérieure)
Clients de base de données	• Client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1 • Client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Client Oracle 12c lors de la connexion à Oracle 12c • Client Oracle 11g Release 2 lors de la connexion à Oracle 11g Release 2.
Clients JDBC (**Java Database Connectivity) pour la console de configuration et le Visualizer**	• Pilote JDBC version 9.5 du client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1. • Pilote JDBC version 9.5 du client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5. • Pilotes JDBC Oracle 12c lors de la connexion à Oracle 12c. • Pilotes JDBC Oracle 11g lors de la connexion à Oracle 11g.
Navigateurs Web	• Mozilla Firefox
Logiciels de mise en file d'attente des messages pris en charge	• IBM WebSphere MQ
Autres logiciels	• GNU Compiler Collection, package gcc (ou gcc_small) Version 3.3.2.

Configuration système requise pour une exécution sur Microsoft Windows Server

La liste ci-dessous répertorie les produits pris en charge lors de l'exécution d'IBM InfoSphere Identity Insight sur un système d'exploitation Microsoft Windows Server 64 bits.

Tableau 19. Configuration système requise pour une exécution sur Microsoft Windows Server

Systèmes d'exploitation	• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 R2
Configuration matérielle requise	• Intel x86_64
Java	Les éléments suivants sont installés avec le produit : • Environnement d'exécution Java IBM 64 bits, Version 8
Bases de données	• IBM DB2 Database pour Linux, UNIX et Windows 11.1 • IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Oracle 12c • Oracle 11g Edition 2 (11.2.0.1, 11.2.0.2 ou version supérieure)
Clients de base de données	• Client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1 • Client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5 • Client Oracle 12c lors de la connexion à Oracle 12c • Client Oracle 11g Release 2 lors de la connexion à Oracle 11g Release 2.
Clients JDBC (Java Database Connectivity)	• Pilote JDBC version 9.5 du client DB2 version 11.1 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 11.1. • Pilote JDBC version 9.5 du client DB2 version 10.5 pour la connexion à IBM DB2 Database pour Linux, UNIX et Windows 10.5. • Pilotes JDBC Oracle 12c lors de la connexion à Oracle 12c. • Pilotes JDBC Oracle 11g lors de la connexion à Oracle 11g.
Navigateurs Web	• Windows Internet Explorer 10 et versions ultérieures • Mozilla Firefox
Logiciels de mise en file d'attente des messages pris en charge	• IBM WebSphere MQ

Définition de l'architecture du système

Vous devez planifier les configurations de la base de données et du serveur de l'installation du produit.

Configuration de la base de données du produit

Les installations d'IBM InfoSphere Identity Insight peuvent contenir jusqu'à trois bases de données distinctes pour les configurations du produit et le stockage des données d'entité.

Les différentes bases de données sont les suivantes :

Base de données des entités
Base de données dans laquelle sont stockées les identités, les entités et les données utilisées pour les relations, les résolutions et les alertes.

Base de données de la console de configuration
Base de données dans laquelle sont stockées les ressources de la console de configuration

Base de données Application Monitor
Base de données dans laquelle sont stockées les informations relatives à l'acheminement et au contrôle des pipelines.

Les nouvelles installations peuvent fusionner ces bases de données en une seule, selon les fonctions installées. L'option qui permet de réaliser cette fusion se trouve dans l'écran de configuration de chaque base de données, dans le programme d'installation. La configuration préférée est une base de données unique.

Déploiements de pipelines

Les pipelines peuvent être installés sur un ou plusieurs serveurs, selon la configuration système requise et les ressources du serveur.

Lors du déploiement des pipelines, tenez compte des facteurs de performances suivants :

- Les pipelines peuvent être exécutés seuls ou configurés pour exécuter simultanément des unités d'exécution parallèles.
- Chaque unité centrale peut gérer de 1,5 à 2 pipelines ou unités d'exécution de pipeline en parallèle.
- Les pipelines en parallèle peuvent recevoir des données de plusieurs sources à la fois, vous n'avez donc pas besoin de séparer manuellement les fichiers pour que le nombre de fichiers soit égal à celui des pipelines.

Lors du déploiement des pipelines, tenez également compte des facteurs suivants :

- Les pipelines peuvent être exécutés sur n'importe quel matériel pris en charge, avec n'importe quelle configuration du système d'exploitation.
- Même si c'est possible, les pipelines ne doivent pas être exécutés sur la machine sur laquelle se trouve la base de données.
- Les pipelines en parallèle sont plus faciles à configurer que plusieurs pipelines.
- La configuration de plusieurs serveurs est plus compliquée à gérer.
- La configuration d'un seul serveur nécessite du matériel coûteux, qui augmente de façon exponentielle avec le nombre d'unités centrales.

Création d'un utilisateur protégé pour les installations non Windows

Pour toutes les plateformes non Windows, créez un utilisateur protégé pour exécuter le programme d'installation du produit.

Pourquoi et quand exécuter cette tâche

N'exécutez pas le programme d'installation du produit en tant qu'utilisateur ROOT.

Rôles et responsabilités de l'utilisateur

Les rôles utilisateur permettent de catégoriser les tâches typiques qui doivent être exécutées pour correctement déployer et utiliser IBM InfoSphere Identity Insight. De nombreux types d'utilisateurs peuvent utiliser IBM InfoSphere Identity Insight pour des raisons variées, à savoir qu'ils endossent les responsabilités d'un ou plusieurs rôles au moment d'utiliser le produit.

Vous pouvez définir des groupes d'utilisateurs en fonction des différents rôles et responsabilités de chaque utilisateur.

Les rôles utilisateur les plus courants sont les suivants :

Analyste
Analyse les données et vérifie les entités, les relations et les alertes. L'analyste définit les résultats les plus pertinents et s'assure qu'ils sont bien renvoyés par le système. Il travaille en étroite collaboration avec l'opérateur et l'administrateur d'application.

Opérateur
Charge les données dans le système, exécute les pipelines et vérifie que le système fonctionne correctement, rédigeant le cas échéant des rapports sur la qualité des données chargées. L'opérateur vérifie également les résultats, les exceptions et les événements. Il travaille en étroite collaboration avec l'analyste, l'administrateur de sources de données et l'administrateur d'application.

Administrateur de sources de données
Prépare les données avant leur chargement dans le système, ce qui consiste à les convertir en fichier UMF et à valider ce fichier. L'administrateur de sources de données travaille en étroite collaboration avec les opérateurs, les administrateurs d'application et les administrateurs de base de données.

Administrateur d'application
Procède à la configuration de l'application, notamment celle des données, des modèles d'entités et des règles. L'administrateur d'application travaille en étroite collaboration avec les administrateurs de sources de données et les opérateurs pour définir le modèle d'entité et coordonne les modifications de configuration avec l'administrateur de base de données, l'administrateur de sources de données et les opérateurs. Il assure également la coordination et consulte les administrateurs système généraux, s'ils existent.

Administrateur de base de données
Vérifie que la base de données est correctement configurée et réglée pour pouvoir être utilisée avec l'application. L'administrateur de base de données travaille en étroite collaboration avec l'opérateur, l'administrateur de sources de données et l'administrateur d'application.

Architecte système
Evalue les configurations matérielle et logicielle requises pour la planification du déploiement de l'application. L'architecte système travaille en étroite collaboration avec le responsable de l'installation, l'administrateur de base de données, l'administrateur de sources de données et l'administrateur d'application pour assurer un déploiement qui

correspond à la vision, aux stratégies et aux objectifs prévus et qui s'intègre à vos processus métier tout en offrant les résultats attendus.

Responsable de l'installation
Gère l'installation et la configuration initiale de l'application. Le responsable de l'installation configure les utilisateurs initiaux dans le système. Il est très souvent aidé par IBM Professional Services pour définir ces responsabilités.

Programmeur
Conçoit et développe des interfaces graphiques ou en personnalise pour les diverses fonctions, de telle sorte que le déploiement de l'application s'intègre à votre environnement de façon transparente. Le programmeur travaille en étroite collaboration avec l'architecte système et l'administrateur d'application, souvent pour envoyer des alertes aux personnes concernées, de la façon la plus appropriée pour votre environnement.

Architecte de la sécurité
Vérifie que l'équipe du projet respecte et implémente un système sécurisé. L'architecte de la sécurité travaille en étroite collaboration avec l'architecte système, le responsable de l'installation et l'administrateur de base de données.

Chapitre 3. Configuration des bases de données

Avant d'installer le produit vous devez configurer les bases de données requises.

Définition des variables d'environnement

Pour les bases de données DB2 ou Oracle, vous devez définir des variables d'environnement.

Variables d'environnement DB2

Paramétrez toutes les variables d'environnement requises ci-dessous pour le système d'exploitation installé sur la machine cible.

Variables d'environnement AIX

Remarque : Vous devez vous assurer que la valeur de ces variables d'environnement est ajoutée devant les entrées existantes des mêmes variables d'environnement.

Toutes les variables d'environnement doivent être en lettres majuscules.

Tableau 20. Variables d'environnement AIX pour les bases de données DB2

Variable d'environnement	Valeur	Conditions
DB2DIR	Chemin d'installation du logiciel DB2	où *DB2DIR* correspond à l'emplacement où le logiciel du client/serveur DB2 est installé.
DB2INSTANCE	Nom de l'instance de la base de données DB2	où *DB2INSTANCE* correspond au nom de l'instance de la base de données DB2 que vous avez créée.
LIBPATH	$*DB2DIR*/lib64: *INSTALLDIRECTORY*/lib	où *DB2DIR* correspond à l'emplacement où le logiciel du client/serveur DB2 est installé et où *INSTALLDIRECTORY* correspond à l'emplacement où le produit va être installé.

Variables d'environnement Linux

Tableau 21. Variables d'environnement Linux pour les bases de données DB2

Variable d'environnement	Valeur	Conditions
DB2DIR	Chemin d'installation du logiciel DB2	où *DB2DIR* correspond à l'emplacement où le logiciel du client/serveur DB2 est installé.

Tableau 21. Variables d'environnement Linux pour les bases de données DB2 (suite)

Variable d'environnement	Valeur	Conditions
DB2INSTANCE	Nom de l'instance de la base de données DB2	où *DB2INSTANCE* correspond au nom de l'instance de la base de données DB2 que vous avez créée.
LD_LIBRARY_PATH	`$DB2DIR/lib64:INSTALLDIRECTORY/lib`	où *DB2DIR* correspond à l'emplacement où le logiciel du client/serveur DB2 est installé et où *INSTALLDIRECTORY* correspond à l'emplacement où le produit va être installé.

Variables d'environnement Microsoft Windows

Vous devez utiliser la convention de dénomination Microsoft Windows 8.3 pour configurer les variables d'un environnement Microsoft Windows. Les variables d'environnement ne doivent contenir aucun espace.

Tableau 22. Variables d'environnement Microsoft Windows pour les bases de données DB2

Variable d'environnement	Valeur	Conditions
DB2DIR	Chemin d'installation du logiciel DB2	où *DB2DIR* correspond à l'emplacement où l'instance DB2 a été créée. Certaines versions de DB2 définissent plutôt *DB2_HOME* ou *DB2PATH*. Le programme d'installation recherchera ces derniers si *DB2DIR* est introuvable .
DB2INSTANCE	Nom de l'instance de la base de données DB2	où *DB2INSTANCE* correspond au nom de l'instance de la base de données DB2 que vous avez créée.
DB2CODEPAGE	Défini sur une valeur égale à la valeur CODEPAGE de la base de données DB2.	Une non-concordance peut entraîner des problèmes de codage pour les données Latin-1/UTF-8 lors du chargement des données.

Variables d'environnement Oracle

Paramétrez toutes les variables d'environnement requises ci-dessous pour le système d'exploitation installé sur la machine cible.

Remarque : Vous devez vous assurer que la valeur de ces variables d'environnement est ajoutée devant les entrées existantes des mêmes variables d'environnement.

Toutes les variables d'environnement doivent être en lettres majuscules.

Variables d'environnement AIX

Tableau 23. Variables d'environnement AIX pour les bases de données Oracle

Variable d'environnement	Valeur	Conditions
ORACLE_HOME	répertoire d'installation du logiciel client Oracle	où *ORACLE_HOME* correspond à l'emplacement où le logiciel client est installé.
LIBPATH	$*ORACLE_HOME*/lib:<*répertoire d'installation du produit*>/lib	où *ORACLE_HOME* est le répertoire d'installation du logiciel client Oracle et où <*répertoire_installation_produit*> est l'emplacement où le produit doit être installé.

Variables d'environnement Linux 64 bits

Tableau 24. Variables d'environnement Linux 64 bits pour les bases de données Oracle

Variable d'environnement	Valeur	Conditions
ORACLE_HOME	répertoire d'installation du logiciel client Oracle	où *ORACLE_HOME* correspond à l'emplacement où le logiciel client est installé.
LD_LIBRARY_PATH	$*ORACLE_HOME*/lib:<*répertoire d'installation du produit*>/lib	où *ORACLE_HOME* est le répertoire d'installation du logiciel client Oracle et où <*répertoire_installation_produit*> est l'emplacement où le produit doit être installé.

Variables d'environnement Microsoft Windows

Vous devez utiliser la convention de dénomination Microsoft Windows 8.3 pour configurer les variables d'un environnement Microsoft Windows. Les variables d'environnement ne doivent contenir aucun espace.

Tableau 25. Variables d'environnement Microsoft Windows pour les bases de données Oracle

Variable d'environnement	Valeur	Conditions
ORACLE_HOME	répertoire d'installation du logiciel client Oracle	où *ORACLE_HOME* correspond à l'emplacement où le logiciel client est installé.

Variables d'environnement Microsoft SQL Server

Paramétrez toutes les variables d'environnement requises ci-dessous pour le système d'exploitation installé sur la machine cible.

Variables d'environnement Microsoft Windows

Vous devez utiliser la convention de dénomination Microsoft Windows 8.3 pour la configuration des variables d'environnement dans un environnement Microsoft Windows. Les variables d'environnement ne doivent contenir aucun espace.

Tableau 26. Variables d'environnement Microsoft Windows pour les bases de données Microsoft SQL Server

Variable d'environnement	Valeur	Conditions
MSSQL_JDBC	L'emplacement du pilote Microsoft JDBC.	où *MSSQL_JDBC* correspond à l'emplacement du serveur où se trouvent le pilote Microsoft JDBC ainsi que les fichiers `.jar`. Ce chemin d'accès sera choisi par le programme d'installation du produit.

Configuration du nom de source de données ODBC pour Microsoft SQL Server

Le nom de source de données (DSN - Data Source Name) ODBC de Microsoft SQL doit correspondre exactement au nom de la base de données de Microsoft SQL Server.

Pourquoi et quand exécuter cette tâche

Le type de connexion du nom DSN doit être défini conformément au mécanisme d'authentification avec lequel Microsoft SQL Server est configuré (authentification de l'utilisateur du système d'exploitation ou du serveur SQL).

Activation des transactions XA pour Microsoft SQL Server

Vous devez activer les transactions XA pour que la console de configuration et le Visualizer fonctionnent correctement.

Procédure

1. Activez les transactions XA à l'aide de l'outil d'administration Component Services de Windows.
2. Exécutez le service de coordination des transactions réparties à l'aide du bureau de Microsoft SQL Server.
3. Installez les procédures stockées JTA (Java Transaction API) comme indiqué dans la documentation Microsoft SQL Server correspondante.
4. Définissez des droits d'accès aux utilisateurs afin qu'ils puissent exécuter des procédures stockées JTA à l'aide de Microsoft SQL Server Enterprise Manager.

Attribution de droits CREATE VIEW à des utilisateurs Oracle

Pour permettre au produit de fonctionner correctement, les utilisateurs des bases de données Oracle doivent disposer de droits CREATE VIEW.

Pourquoi et quand exécuter cette tâche

Les privilèges CREATE VIEW doivent être directement attribués à l'utilisateur et non pas affectés en fonction de son rôle.

Création et configuration des bases de données

Créez une base de données unique qui sera utilisée comme base de données d'entités pour tous les composants du produit.

Création de la base de données d'entité

Vous devez créer une base de données pour que le pipeline stocke des identités, des entités, des relations et des alertes, mais aussi pour qu'il stocke des informations de configuration sur la console de configuration et des informations de contrôle de l'application.

Pourquoi et quand exécuter cette tâche

Pour obtenir des instructions sur la création de nouvelles bases de données, reportez-vous à la documentation de votre base de données.

Utilisez des MAJUSCULES pour les noms des bases de données.

Configuration de l'authentification client

L'authentification client permet aux utilisateurs de se connecter à la base de données des entités sans avoir à fournir un nom d'utilisateur et un mot de passe supplémentaires dans le fichier `.ini` du pipeline.

Pourquoi et quand exécuter cette tâche

L'authentification client est également connue sous le nom d'"authentification sécurisée de la base de données du SE". Elle permet d'établir une connexion à l'aide du nom d'utilisateur actuellement connecté. Ce schéma d'authentification confirme que le système d'exploitation a déjà correctement authentifié l'utilisateur. L'authentification client peut être utilisée sur des plateformes de base de données DB2, Oracle et Microsoft SQL. Les processus des pipelines et d'IBM WebSphere doivent être exécutés par l'utilisateur du système d'exploitation qui peut accéder à la base de données d'entités en mode sécurisé. Si plusieurs utilisateurs doivent exécuter ces processus, veuillez contacter le Support IBM pour plus de détails.

Configuration de l'authentification client pour les bases de données DB2

Configurez DB2 afin qu'il utilise l'authentification client.

Procédure

1. Définissez les options de configuration suivantes pour le serveur global :
   a. Définissez l'option **`authentication`** sur la valeur `client`.
   b. Définissez l'option **`trust_allclnts`** sur la valeur `yes`.
   c. Définissez l'option **`trust-clntauth`** sur la valeur `server`.
2. Créez un catalogue des bases de données du produit à l'aide du paramètre **`authentication client`** de la commande **`db2 catalog database`**.
3. Synchronisez les noms d'utilisateur du système d'exploitation et de la base de données DB2.
4. Veillez à disposer du pilote DB2 JDBC Type 2 en plus du pilote DB2 JDBC Type 4 standard. Il doit se trouver dans le fichier `db2java.zip`.
5. Activez l'authentification sécurisée lors de l'installation du produit.

Configuration de l'authentification client pour les bases de données Oracle

Configurez Oracle afin qu'il utilise l'authentification client.

Procédure

1. Définissez les options de configuration suivantes pour le serveur global :
   a. Définissez l'option **os_authent_prefix** sur la valeur OPS$.
   b. Définissez l'option **remote_os_authent** sur la valeur TRUE.
2. Créez des utilisateurs de base de données Oracle afin que l'utilisateur puisse utiliser des méthode d'authentification externe et de base de données. Exemple de syntaxe :

```
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. Veillez à disposer du pilote Oracle JDBC Type 2 en plus du pilote Oracle JDBC Type 4 standard. Pour Oracle, il doit se trouver dans le fichier ojdbc16.zip.
4. Activez l'authentification sécurisée lors de l'installation du produit. Donnez un nom d'utilisateur doté du préfixe OPS$ lorsque des justificatifs d'identité de base de données vous sont demandés dans le programme d'installation du produit.

Configuration de l'authentification client pour les bases de données Microsoft SQL Server

Configurez Microsoft SQL Server afin qu'il utilise l'authentification client.

Procédure

1. Vérifiez que le système DSN utilise l'authentification Windows NT et non pas l'authentification SQL Server. Sinon, créez un nouveau nom DSN système à l'aide de l'authentification Windows NT.
2. Vérifiez l'existence de l'utilisateur administrateur de la base de données dans Microsoft SQL Server Enterprise Manager. Octroyez au moins un droit d'accès public et db_owner pour la base de données à l'administrateur pour chaque base de données du produit. Définissez la base de données des entités comme base de données par défaut.
3. Veillez à disposer du pilote JDBC ODBC Bridge Type 1.
4. Créez un utilisateur de base de données (système non d'exploitation) qui bénéficie d'un accès à la base de données d'entités.
5. Activez l'authentification sécurisée lors de l'installation du produit. Utilisez l'utilisateur de base de données (système non d'exploitation) lorsqu'il vous est demandé des justificatifs d'identité de base de données dans le programme d'installation du produit.

Ajustement de la taille du cache d'instruction Oracle

Les administrateurs de bases de données Oracle doivent ajuster de manière adaptée la taille du cache d'instruction.

Pourquoi et quand exécuter cette tâche

Le produit peut utiliser les instructions de manière intensive, c'est-à-dire que le cache d'instruction Oracle peut donc devenir rapidement volumineux et dépasser les paramètres par défaut de la base de données Oracle. Pour plus d'informations sur la définition de la taille et le réglage de ces paramètres, reportez-vous à votre documentation Oracle.

Procédure

Configurez les paramètres suivants au niveau du serveur à l'aide de la commande Oracle **ALTER SYSTEM SET** :

SESSION_CACHED_CURSORS
La valeur recommandée pour ce paramètre est d'environ 20 curseurs simultanés par pipeline ou unité d'exécution de pipelines pour un traitement en parallèle.

OPEN_CURSORS
La valeur recommandée pour ce paramètre est d'environ 20 curseurs simultanés par pipeline ou unité d'exécution de pipelines pour un traitement en parallèle.

CURSOR_SHARING
Ce paramètre a une grande incidence sur les performances. Il doit être configuré en prenant en compte le fait que le produit utilise souvent des variables liées et que l'application bénéficiera d'un partage des curseurs.

Chapitre 4. Administration

Les tâches d'administration incluent la configuration et la gestion des paramètres système pour les interfaces utilisateur, ainsi que la mise à jour des paramètres de configuration globaux. Les administrateurs utilisent la console de configuration pour effectuer les tâches administratives.

Administration de la console

Pour utilisateur efficacement la console, vous devez configurer les navigateurs, établir des comptes pour les utilisateurs concernés et gérer l'accès à la console.

Console de configuration

La console de configuration fournit une interface orientée tâche pour vous aider à effectuer plus facilement certaines des tâches les plus essentielles à la prise en main d'Identity Insight.

La console de configuration est hébergée par IBM WebSphere Liberty.

Gestion de la configuration du système

La console de configuration permet de configurer la plupart des paramètres système et des options dans un ensemble d'interfaces simplifiées et rationalisées. La console écrit ensuite les changements dans la base de données de configuration. Les modifications qui sont apportées directement à la base de données de configuration ne sont pas prises en charge. Elles entraînent le plus souvent un mauvais fonctionnement du produit.

Rôles et responsabilités de l'utilisateur

Les rôles utilisateur permettent de catégoriser les tâches typiques qui doivent être exécutées pour correctement déployer et utiliser IBM InfoSphere Identity Insight. De nombreux types d'utilisateurs peuvent utiliser IBM InfoSphere Identity Insight pour des raisons variées, à savoir qu'ils endossent les responsabilités d'un ou plusieurs rôles au moment d'utiliser le produit.

Vous pouvez définir des groupes d'utilisateurs en fonction des différents rôles et responsabilités de chaque utilisateur.

Les rôles utilisateur les plus courants sont les suivants :

Analyste
Analyse les données et vérifie les entités, les relations et les alertes. L'analyste définit les résultats les plus pertinents et s'assure qu'ils sont bien renvoyés par le système. Il travaille en étroite collaboration avec l'opérateur et l'administrateur d'application.

Opérateur
Charge les données dans le système, exécute les pipelines et vérifie que le système fonctionne correctement, rédigeant le cas échéant des rapports sur la qualité des données chargées. L'opérateur vérifie également les résultats, les exceptions et les événements. Il travaille en étroite collaboration avec l'analyste, l'administrateur de sources de données et l'administrateur d'application.

Administrateur de sources de données
Prépare les données avant leur chargement dans le système, ce qui consiste à les convertir en fichier UMF et à valider ce fichier. L'administrateur de sources de données travaille en étroite collaboration avec les opérateurs, les administrateurs d'application et les administrateurs de base de données.

Administrateur d'application
Procède à la configuration de l'application, notamment celle des données, des modèles d'entités et des règles. L'administrateur d'application travaille en étroite collaboration avec les administrateurs de sources de données et les opérateurs pour définir le modèle d'entité et coordonne les modifications de configuration avec l'administrateur de base de données, l'administrateur de sources de données et les opérateurs. Il assure également la coordination et consulte les administrateurs système généraux, s'ils existent.

Administrateur de base de données
Vérifie que la base de données est correctement configurée et réglée pour pouvoir être utilisée avec l'application. L'administrateur de base de données travaille en étroite collaboration avec l'opérateur, l'administrateur de sources de données et l'administrateur d'application.

Architecte système
Evalue les configurations matérielle et logicielle requises pour la planification du déploiement de l'application. L'architecte système travaille en étroite collaboration avec le responsable de l'installation, l'administrateur de base de données, l'administrateur de sources de données et l'administrateur d'application pour assurer un déploiement qui correspond à la vision, aux stratégies et aux objectifs prévus et qui s'intègre à vos processus métier tout en offrant les résultats attendus.

Responsable de l'installation
Gère l'installation et la configuration initiale de l'application. Le responsable de l'installation configure les utilisateurs initiaux dans le système. Il est très souvent aidé par IBM Professional Services pour définir ces responsabilités.

Programmeur
Conçoit et développe des interfaces graphiques ou en personnalise pour les diverses fonctions, de telle sorte que le déploiement de l'application s'intègre à votre environnement de façon transparente. Le programmeur travaille en étroite collaboration avec l'architecte système et l'administrateur d'application, souvent pour envoyer des alertes aux personnes concernées, de la façon la plus appropriée pour votre environnement.

Architecte de la sécurité
Vérifie que l'équipe du projet respecte et implémente un système sécurisé. L'architecte de la sécurité travaille en étroite collaboration avec l'architecte système, le responsable de l'installation et l'administrateur de base de données.

Paramètres de navigateur optimaux pour utiliser la console de configuration

La console de configuration est une application Web qui nécessite des paramètres spécifiques pour que votre navigateur puisse y accéder.

Utilisez les paramètres de navigateur suivants pour un affichage optimal de la console de configuration :

Tableau 27. Paramètres de navigateur optimaux

Paramètre	Valeur	Description
Résolution	800 x 600 minimum ; 1024 x 768 ou supérieure recommandée	
Taille du texte	Moyen	
JavaScript	Activé	
Cookies	Activé	Vous devez activer au moins les cookies des sessions primaires.
Sécurité - site Web approuvé	Adresse HTTP de la console de configuration	Assurez-vous que l'adresse HTTP de la console de configuration figure dans la liste des sites Web approuvés.
Sécurité - options de téléchargement	Activé	Assurez-vous que toutes les options de téléchargement des sites Web approuvés sont activées.
Bloqueurs de fenêtres spontanées	Autoriser les fenêtres spontanées à partir de l'adresse HTTP de la console de configuration	Assurez-vous que l'adresse HTTP de la console de configuration figure dans la liste des sites Web autorisant les fenêtres spontanées.

Connexion à la console de configuration

La connexion à la console de configuration permet d'afficher et de modifier les paramètres de configuration du système.

Avant de commencer

Pour que vous puissiez vous connecter, il faut que votre administrateur système vous ait créé un compte à cet effet.

Procédure

1. Ouvrez la console de configuration :
   a. Ouvrez le navigateur dans lequel vous voulez exécuter la console de configuration.
   b. Entrez l'URL pour la console de configuration avec la syntaxe suivante : `http://<nomserveur>/console/`.
   c. Appuyez sur la touche **Entrée**.
2. Dans la fenêtre **Connexion**, entrez votre nom d'utilisateur et votre mot de passe.
3. Facultatif : Si vous êtes un administrateur système et devez modifier la configuration système actuelle, sélectionnez l'option **Editer la configuration**. Si vous modifiez la configuration système en cours, vous devez normalement arrêter tous les pipelines, afin d'éviter le traitement des nouvelles données tant que les changements de configuration ne sont pas appliqués.
4. Cliquez sur le bouton **Connexion**.

Que faire ensuite

Si vos nom d'utilisateur et mot de passe concordent avec ceux établis pour la console de configuration, cette dernière s'ouvre. Sinon, une erreur se produit et vous devez vous reconnecter après vous être renseigné sur les nom et mot de passe corrects.

Déconnexion de la console de configuration

Vous pouvez vous déconnecter de la session actuelle de console de configuration sans quitter l'application. En l'absence d'activité pendant 60 minutes, la console de configuration déconnecte automatiquement l'utilisateur actuel.

Procédure

Cliquez sur **Déconnexion** dans le coin supérieur droit d'une fenêtre de console de configuration.

Que faire ensuite

Vous êtes désormais déconnecté de la console de configuration et devrez vous y reconnecter pour continuer de l'utiliser.

Comptes utilisateur de la console de configuration

Pour la connexion à la console de configuration, l'administrateur système crée un compte qu'il vous attribue. Les comptes utilisateur comportent un nom et un mot de passe, que vous pouvez modifier.

Vous ne pouvez vous connecter plusieurs fois avec le même compte utilisateur. Si vous partagez un compte utilisateur avec d'autres personnes, vous ne pouvez vous connecter à la console de configuration simultanément. Si vous tentez de vous connecter au moyen d'un compte que qu'une autre personne est déjà en train d'utiliser, sa session se clôt et la vôtre commence.

L'administrateur système peut créer des comptes utilisateur supplémentaires à tout moment. Il peut en outre redémarrer la console de configuration afin d'imposer un dépassement de délai.

Gestion de l'accès à la console de configuration

Il faut que l'accès soit accordé à chaque utilisateur de la console de configuration et qu'il s'y connecte au moyen d'un nom d'utilisateur et d'un mot de passe. Vous pouvez gérer les noms et mots de passe au moyen du fichier spécifique à l'application fourni par la console de configuration. Si vous utilisateurs disposent de comptes de système de gestion de base de données relationnelle (RDBMS) qui leur permettent d'accéder à la base de données d'entités, vous pouvez aussi, à l'aide de ces comptes et des outils d'administration de bases de données, gérer l'accès des utilisateurs à la console de configuration. Ces noms et mots de passe se distinguent de ceux configurés pour accéder au visualiseur ; ce ne sont pas forcément les mêmes que ceux du visualiseur.

Gestion de l'accès à la console de configuration au moyen des informations de connexion à la base de données

Vous pouvez gérer l'accès à la console de configuration au moyen des mêmes ID utilisateur et mot de passe que la base de données d'entités.

Avant de commencer

Assurez-vous que personne n'est connecté à la console de configuration afin d'empêcher les conflits de configuration.

Procédure

1. Lancez l'utilitaire de configuration en accédant au répertoire `<emplacement installation>/installer/util/` et en tapant l'une des commandes suivantes :
   a. Pour Windows, tapez `eacfg.bat –i –l ../logs/`.
   b. Pour Unix, tapez `eacfg –i –l ../logs/`.
2. Dans la panneau de navigation, cliquez sur **Paramètres de la console de configuration**.
3. Cochez la case **Modifier l'authentification de la console de configuration**.
4. Cliquez sur le bouton radio **Authentification SQL** .
5. Cliquez sur **OK**.
6. A l'aide de vos outils d'administration de bases de données, indiquez les informations de connexion à la console de configuration (et à la base de données d'entités).

Gestion de l'accès à la console de configuration à l'aide de l'utilitaire gestionnaire de mot de passe

Vous pouvez gérer l'accès à la console de configuration au moyen de l'utilitaire gestionnaire de mot de passe.

Avant de commencer

Assurez-vous que personne n'est connecté à la console de configuration.

Procédure

1. Lancez l'utilitaire de configuration en accédant au répertoire `<emplacement installation>/installer/util/` et en tapant l'une des commandes suivantes :
   a. Pour Windows, tapez `eacfg.bat –i –l ../logs/`.
   b. Pour Unix, tapez `eacfg –i –l ../logs/`.
2. Dans la panneau de navigation, cliquez sur **Paramètres de la console de configuration**.
3. Cochez la case **Modifier l'authentification de la console de configuration**.
4. Cliquez sur le bouton radio **Authentification des fichiers**.
5. Cliquez sur **OK**.

Résultats

Vous pouvez désormais vous servir de l'utilitaire gestionnaire de mot de passe (pwdmgr.jar), situé dans le répertoire srd-home/console, pour ajouter ou supprimer des utilisateurs ou réinitialiser des mots de passe dans le fichier console_password.properties.

Consultation de la liste des utilisateurs et de leur statut :

Vous pouvez consulter la liste des utilisateurs et leur état au moyen de la commande de gestionnaire de mot de passe.

Procédure

1. Dans une fenêtre de commande, accédez au répertoire \srd-home\console.
2. Tapez la commande suivante : `pwdmgr console-passwords.properties console-principals.properties -l`

Exemple

Par exemple, si vous tapez la commande `pwdmgr console-passwords.properties console-principals.properties -l`, il se peut que l'exemple de résultat suivant s'affiche :

```
admin (super utilisateur)
julie (super utilisateur)
alain (super utilisateur)
josé (super utilisateur) *** JAMAIS CONNECTE ***
```

Si vous avez récemment réinitialisé un mot de passe, un message vous informe que l'utilisateur ne s'est pas encore connecté à la console de configuration avec le nouveau mot de passe.

Ajout d'un nouvel utilisateur :

Si vous gérez l'accès à la console de configuration, dans le fichier console-passwords.properties, vous pouvez ajouter un nouvel utilisateur au moyen de la commande de gestionnaire de mot de passe.

Procédure

1. Dans une fenêtre de commande, accédez au répertoire \srd-home\console.
2. Tapez la commande suivante, `pwdmgr console-passwords.properties console-principals.properties -a nom_utilisateur`, sachant que*nom_utilisateur* est le nom d'utilisateur à ajouter.

Que faire ensuite

Un utilisateur est ajouté, son mot de passe par défaut étant le nom d'utilisateur que vous avez saisi. Le nouvel utilisateur peut désormais se connecter à la console de configuration.

Suppression d'un utilisateur existant :

Si vous gérez l'accès à la console de configuration, dans le fichier console-passwords.properties, vous pouvez supprimer un utilisateur existant au moyen de la commande de gestionnaire de mot de passe.

Avant de commencer

Veillez à exécuter la commande à partir du répertoire `\srd-home\console\`. Veillez également à ce que l'utilisateur que vous supprimez existe. Si vous tentez de supprimer un utilisateur inconnu, vous recevez un message d'erreur.

Procédure

1. Dans une fenêtre de commande, accédez au répertoire \srd-home\console.
2. Tapez la commande suivante, `pwdmgr console-passwords.properties console-principals.properties -d nom_utilisateur`, sachant que*nom_utilisateur* est le nom d'utilisateur à supprimer.

Que faire ensuite

L'utilisateur que vous venez de supprimer ne peut plus se connecter à la console de configuration.

Réinitialisation d'un mot de passe :

Quand des utilisateurs oublient leur mot de passe pour le compte de la console de configuration ou qu'un mot de passe doit être modifié pour des raisons de sécurité, les administrateurs système peuvent les réinitialiser avec la commande de gestionnaire de mots de passe.

Avant de commencer

Assurez-vous d'exécuter la commande dans le répertoire `\srd-home\console\`.

Procédure

1. Dans une fenêtre de commande, allez au répertoire `\srd-home\console`.
2. Entrez la commande `pwdmgr console-passwords.properties console-principals.properties -r username`, où *username* est le nom d'utilisateur de la personne dont vous voulez réinitialiser le mot de passe.

Que faire ensuite

Le mot de passe de l'utilisateur que vous avez indiqué est désormais réinitialisé comme étant son nom d'utilisateur. A la prochaine connexion d'utilisateurs à la console de configuration après réinitialisation de leur mot de passe, le système affiche une invite pour réinitialiser le mot de passe. Une fois que vous avez réinitialisé un mot de passe, vous devez suggérer à l'utilisateur concerné de se connecter et de changer dès que possible son mot de passe pour minimiser les risques ou problèmes de sécurité.

Commande de gestionnaire de mot de passe :

La commande de gestionnaire de mot de passe permet de gérer l'accès à la console de configuration au moyen d'un fichier de propriétés. Vous pouvez ajouter, supprimer et répertorier les utilisateurs, ainsi qu'en réinitialiser le mot de passe.

La syntaxe de la commande de gestionnaire de mot de passe est la suivante :
`pwdmgr -option paramètre`

Pour utiliser une commande du gestionnaire de mot de passe, exécutez la commande à partir du répertoire `\srd-home\console\`.

Options et paramètres

Chaque option et paramètre de la commande de gestionnaire de mot de passe doit être indiqué commande distincte. Si vous n'indiquez pas une option, l'aide de la commande s'affiche.

-a *nom_utilisateur*
Ajoute un utilisateur à la fois.

Le nom d'utilisateur que vous indiquez est la valeur par défaut du mot de passe initial. L'utilisateur est invité à modifier ce mot de passe lors de la première connexion à la console.

Si vous ajoutez un utilisateur déjà existant, vous recevez un message d'erreur.

-d *nom_utilisateur*
Supprime un utilisateur à la fois.

Si vous tentez de supprimer un utilisateur inconnu, vous recevez un message d'erreur. Vous pouvez afficher la liste des utilisateurs à l'aide de l'option de liste afin de vous assurer que l'un d'eux a bien été supprimé.

-l
Affiche la liste de tous les utilisateurs et leur état.

-r *nom_utilisateur*
Réinitialise, comme mot de passe de l'utilisateur que vous avez indiqué, l'ID de cet utilisateur. Par exemple, julie/tournesol est réinitialisé en julie/julie.

Deux fichiers fonctionnent avec la commande de gestionnaire de mot de passe :

- console-passwords.properties - Ce fichier consigne tous les noms d'utilisateur et la synthèse de message des mots de passe.
- console-principals.properties - Ce fichier est réservé à l'usage de la création future de différents niveaux d'utilisateurs. Actuellement, tous les utilisateurs sont considérés de la console de configuration comme des superutilisateurs et peuvent accéder à tous les espaces de la console.

Ces fichiers se trouvent dans le répertoire srd-home. Toutefois, ne les modifiez pas manuellement. Ils permettent au produit de suivre les connexions des utilisateurs et sont des paramètres obligatoires dans certaines autres commandes.

Exemple de commandes du gestionnaire de mot de passe

Pour ajouter une nouvelle utilisatrice dont le nom de connexion et le mot de passe par défaut sont tous deux "julie", tapez la commande `pwdmgr -a julie`

Pour supprimer l'utilisatrice existante nommée julie et le mot de passe correspondant, tapez la commande `pwdmgr -d judy`

Pour afficher la liste des utilisateurs actuels et leur type d'état, tapez la commande `pwdmgr -l`

Par exemple, si vous tapez la commande `pwdmgr -l`, il se peut que l'exemple de résultat suivant s'affiche :

```
admin (super utilisateur)
julie (super utilisateur)
alain (super utilisateur)
josé (super utilisateur) *** JAMAIS CONNECTE ***
```

Si vous avez récemment réinitialisé un mot de passe, un message vous informe que l'utilisateur ne s'est pas encore connecté à la console de configuration avec le nouveau mot de passe.

Pour réinitialiser son ID comme mot de passe d'un utilisateur, tapez la commande commande `pwdmgr -r` *username*

Par exemple, si vous tapez la commande `pwdmgr -r julie`, le mot de passe de l'utilisatrice existante nommée julie est réinitialisé sur le mot de passe par défaut "julie". Si le nom de connexion et le mot de passe étaient julie/tournesol, ils sont désormais réinitialisés en julie/julie.

Rubriques d'aide

Fenêtre de connexion de la console de configuration

Cette fenêtre vous permet de vous connecter à la console de configuration.

ID utilisateur
Saisissez votre ID utilisateur de console de configuration.

Mot de passe
Saisissez votre mot de passe de console de configuration.

Editer la configuration
Cochez cette case pour utiliser le mode édition.

Connexion
Cliquez ici pour soumettre vos ID et mot de passe afin d'accéder à la console de configuration.

Effacer
Cliquez ici pour effacer l'ID et le mot de passe saisis et décocher la case Editer la configuration.

Exécution de rapports depuis la console de configuration

La console de configuration permet de générer des rapports présentant des récapitulatif des statistiques de pipeline par source de données ou un rapport répertoriant les paramètres de configuration système en cours, notamment la configuration de la résolution d'entité. Les rapports générés s'affichent dans l'application Web BIRT (Business Intelligence Reporting Tool) Report Viewer. Veillez à désactiver les logiciels de blocage d'incrustation car ils risquent de bloquer l'affichage du rapport dans l'application de visualisation.

Consultation des rapports statistiques

Lorsqu'il traite les données, le produit suit les statistiques de performances et les données des fichiers source entrants chargés dans le système. Ces informations sont récapitulées dans deux rapports : le rapport récapitulatif de source de données et le rapport récapitulatif de chargement.

Pourquoi et quand exécuter cette tâche

Les statistiques de ces rapports vous permettent de vérifier rapidement que le produit traite la totalité des enregistrements entrants, de prendre des décisions quant aux performances du système, d'évaluer la qualité des données entrantes et d'afficher le nombre de nouvelles identités, entités, relations et alertes résultant du traitement des fichiers de données.

Procédure

1. Dans la console de configuration, sélectionnez **Etat** > **Rapports**.
2. Obligatoire : Dans la liste **Rapport**, choisissez un rapport de statistiques :
   - **Etat récapitulatif de source de données** - Ce rapport procure un récapitulatif statistique rapide, par source de données, sur les enregistrements chargés et traités. Il permet de voir le nombre total de fiches chargées par fichier de source de données, le nombre total de nouvelles fiches d'identité traitées par fichier de source de données, ainsi que le nombre total de nouvelles entités en fonction des données figurant dans ce fichier de source de données. Le rapport récapitulatif de source de données trié par date de chargement, ID de chargement, source de données et fichier de source de données.

- **Rapport récapitulatif de chargement** - Il résume les statistiques et les caractéristiques de qualité pour une ou plusieurs sources de données. Il vous permet de voir les informations sur les performances de chargement, la qualité du fichier de source de données et des récapitulatifs des valeurs employées pour résoudre des entités, détecter des relations et générer des alertes. Ce rapport peut vous aider à évaluer la qualité des données chargées depuis une source de données déterminée. Des données de qualité inférieure peuvent indiquer que les données dans cette source demandent un nettoyage supplémentaire, soit avant d'être chargées dans le produit, soit pendant la résolution d'entité en appliquant des règles DQM (gestion de la qualité des données) spécifiques aux données. Le récapitulatif de chargement est trié par ID de chargement.

3. Dans la zone **Date de début**, tapez la date de début du rapport, au format `mm/jj/aaaa`. Par défaut, cette zone contient la date actuelle.

   Elle peut être laissée vide, auquel cas le produit signale toutes les données respectant d'autres critères indiqués, à commencer par la date du jour.
4. Dans la zone **Date de fin**, tapez la date de fin du rapport, au format `mm/jj/aaaa`. Par défaut, cette zone contient la date actuelle.

   Elle peut être laissée vide, auquel cas le produit signale toutes les données remplissant d'autres critères indiqués, à commencer par la date du jour.
5. Facultatif : Dans **Code de source de données**, entrez un code de source de données déterminé sur lequel doit porter le rapport. Le code de source de données saisi doit concorder exactement avec un code de source de données configuré.

   Elle peut être laissée vide, auquel cas le produit signale toutes les données remplissant d'autres critères indiqués.
6. Obligatoire : Cliquez sur **Exécuter le rapport** pour générer le rapport sélectionné.

Résultats

Le produit génère le rapport statistique sélectionné en fonction de tous les critères indiqués et affiche le rapport dans une fenêtre de navigateur distincte appelée **BIRT Report Viewer**. S'il n'y a pas de données à afficher en fonction des critères sélectionnés, la fenêtre **BIRT Report Viewer** affiche le nom du rapport, la date et l'heure de sa génération et **Page 1/1** dans la partie supérieure. La section des données est vierge.

Que faire ensuite

Utilisez les informations statistiques de ce rapport pour vous aider à ajuster le produit ou le fichier de données.

Etat récapitulatif de source de données

L'état récapitulatif de source de données procure un récapitulatif statistique rapide, par source de données, sur les enregistrements chargés dans le système pour traitement. Grâce à ce rapport, vous pouvez voir le nombre total de fiches traitées par ID de chargement. Sur le total de ces fiches chargées, le rapport montre que le nombre de fiches représentant de nouvelles identités ou nouvelles entités, et calcule le pourcentage de fiches qui sont des entités nouvellement créées.

Statistiques par chargement dans la source de données

Date de chargement
: Affiche la date à laquelle ce fichier de source de données a été chargé

ID de chargement
Affiche le numéro d'ID de chargement affecté par le système.

Source de données
Affiche le code et la description de la source de données (séparés par un tiret) du fichier de source de données qui a été chargé.

Enregistrements UMF chargés
Indique le nombre total de fiches d'identité de ce fichier de source de données qui a été chargé.

Nouvelles identités
Indique le nombre total de nouvelles identités découvertes dans le fichier de données qui a été chargé. (Ce nombre indique une identité qui n'a pas été préalablement traitée par le système.)

% de nouvelles identités
Indique le pourcentage du total des fiches chargées (Nouvelles identités divisées par les fiches UMF chargées) qui représentent de nouvelles identités.

Nouvelles entités
Indique le nombre total de nouvelles entités créées à partir de ce chargement de données.

% de nouvelles entités
Indique le pourcentage du total des fiches chargées (nouvelles entités divisées par les entités chargées) qui représentent de nouvelles entités.

Diagrammes statistiques par source de données

Enregistrements chargés par source de données
Affiche un histogramme qui montre graphiquement le nombre de fiches, provenant de chaque source de données, qui ont été chargés dans le système, en se basant sur les autres critères du rapport spécifiés. Vous pouvez ainsi voir quelles sources de données ont apporté le plus ou le moins d'enregistrements et comparer ces résultats à vos estimations de chiffres de charge.

- L'axe vertical montre les sources de données par code.
- L'axe horizontal montre le nombre d'enregistrements chargés.

Si le nombre d'enregistrements chargés d'une source de données particulière est moindre qu'escompté, vous pouvez inspecter les fichiers de cette source (vous pouvez également envisager de lancer un état récapitulatif de chargement afin de connaître la qualité des données des fichiers chargés de cette source ; la qualité des données se répercute directement sur le nombre d'enregistrements chargés).

Nouvelles entités par source de données
Affiche un histogramme qui montre graphiquement les sources de données qui ont généré le plus grand nombre de nouvelles entités, en se basant sur les autres critères du rapport spécifiés.

- L'axe vertical montre les sources de données par code.
- L'axe horizontal montre le nombre de nouvelles entités créées.

Rapport récapitulatif de chargement

Le rapport Récapitulatif de chargement récapitule les statistiques et les caractéristiques de qualité par source de données. Il contient des informations sur les fichiers sources de données. Utilisez ce rapport pour déterminer les statistiques de chargement, le nombre de résolutions d'entité et d'alertes générées par ce

chargement, les informations générales sur la qualité des données des données chargées, un récapitulatif des actions concernant les fiches UMF par chargement, et toutes les exceptions UMF générées par chargement. Le rapport est trié par ID de chargement.

Pour chaque chargement, le rapport décompose les statistiques en sections :

- Récapitulatif de chargement
- Récapitulatif d'alerte de rôle
- Récapitulatif des relations
- Récapitulatif qualitatif
- Récapitulatif des documents UMF
- Récapitulatif des exceptions

Récapitulatif de chargement

Utilisez cette section pour vous aider à déterminer le temps qui a été nécessaire au traitement d'un fichier spécifique, et vous donner une idée générale de l'utilité de ce fichier de source de données dans la résolution d'entité et la détection de relation.

Date et heure de démarrage
Indique la date et l'heure du début de chargement des données.

Date et heure de fin
Indique la date et l'heure de fin du chargement du fichier de source de données.

Nombre d'enregistrements UMF
Indique le nombre total de fiches chargées depuis ce fichier de source de données dans l'intervalle **Date et heure de début** et **Date et heure de fin**.

La valeur de la **Date et heure de fin** moins la valeur de la **Date et heure de début** correspond au nombre de minutes nécessaires au chargement de ce fichier de source de données, ce qui vous donne une idée des performances du système. Cela peut également indiquer qu'un fichier de source de données plus volumineux doit être scindé en fichiers plus petits pour accélérer le traitement.

Nouvelles identités
Indique le nombre total de nouvelles identités chargées dans l'intervalle **Date de début** et **Date de fin**.

% de nouvelles identités
Indique le pourcentage de nouvelles identités sur le total des identités de ce chargement de données (identités nouvelles dans la base de données d'entités).

Nouvelles entités
Indique le nombre total d'entités nouvellement créées dans l'intervalle **Date de début** et **Date de fin**.

% de nouvelles entités
Indique, sur le total d'entités, le pourcentage d'entités nouvellement créées suite à ce chargement de source de données.

Le nombre de nouvelles identités et de nouvelles entités peut vous procurer une idée générale de l'intérêt global de cette source de données en termes de résolution d'entité et de détection de relation. Si ces chiffres sont

faibles et restent faibles sur le long terme, il se peut que cette source de données ne soit pas utile pour atteindre les objectifs de résolution d'entité de votre entreprise.

Récapitulatif d'alerte de rôle

Utilisez cette section pour consulter les règles et scores de résolution communs aux relations détectées qui ont débouché sur des alertes de rôle. Chaque ligne représente le nombre d'alertes de rôle qui ont été générées, selon les critères mentionnés.

Règle de résolution
Affiche le nom de la règle de résolution utilisée pour évaluer l'identité et l'entité pendant la résolution d'entité et la détection de relation.

Description d'alerte
Affiche le nom de la règle d'alerte de rôle qui a déclenché l'alerte de rôle.

Gravité
Affiche un indicateur défini par l'utilisateur, servant à mesurer la priorité ou l'importance de cette alerte de rôle.

Score de résolution
Affiche un score de résolution (0-100) pour la règle de résolution donnée à l'identité et à l'entité impliquées dans l'alerte de rôle. Ce score indique le degré de ressemblance entre l'identité et l'entité. Un score de 100 signifie que l'enregistrement d'identité a été résolu sous la forme de l'entité.

Nombres d'alertes
Indique le nombre total d'alertes de rôle générées sur la base de la description de la règle d'alerte de rôle, la règle de résolution et le score de résolution.

Récapitulatif des relations

Cette section permet de consulter les attributs communs aux relations détectées qui n'ont pas déclenché d'alerte de rôle. Chaque ligne représente le nombre de relations qui ont été détectées, selon les critères mentionnés.

Règle de résolution
Affiche le nom de la règle de résolution utilisée pour évaluer les fiches d'identité entrantes et les entités existantes pendant la résolution d'entité et la détection de relation.

Score de résolution
Affiche un score de résolution (0-100) pour la règle de résolution donnée à l'identité et à l'entité pendant la résolution d'entité. Ce score indique le degré de ressemblance entre l'identité et l'entité. Un score de 100 signifie que l'enregistrement d'identité a été résolu sous la forme de l'entité.

Score de relation
Affiche un score de relation (0-100) pour la règle de résolution donnée à l'identité et à l'entité pendant la résolution de relation. Ce score indique le degré de relation entre l'identité et l'entité.

Plus le score de relation est élevé, plus l'identité et l'entité sont étroitement apparentées, selon les attributs concordants.

Nombre de relations
Indique le nombre total de relations détectées sur la base de cette règle de résolution, du score de résolution et du score de relation.

Récapitulatif qualitatif

Consultez les informations de cette section pour évaluer la qualité des données de chaque fichier source. Cette section indique la qualité par type d'attribut au sein d'un type de segment UMF et de document UMF. En consultant le récapitulatif qualitatif avec celui des exceptions UMF, vous pouvez savoir quels fichiers sources de données posent des problèmes de qualité ou d'UMF défectueux qu'il importe de régler. Vous pouvez généralement remédier à ces problèmes via la configuration ETL ou DQM/de source de données avant de traiter le fichier de source de données.

Dans certains cas, cette section peut révéler qu'une source de données est de qualité si médiocre qu'il ne faudrait plus l'utiliser pour la résolution d'entité.

Type de document
Affiche le nom du type de document UMF qui contient le type de données mentionné dans le Type de données. Cette valeur est généralement UMF_ENTITY.

Nom de la table
Affiche le nom de la table de base de données qui conserve les données provenant de segments UMF ayant le même nom. Par exemple, les données provenant du segment NUMBER sont stockées dans la table NUMS.

Type de données
Indique le type de données, tel que mentionné dans les balises UMF de type d'attribut des fiches entrantes. Ce type correspond à un segment UMF figurant dans le nom de table. Par exemple, si le nom de table est *ADDRESS* et que le type de données mentionné est *H*, les informations qualitatives évaluent le type d'adresse *Domicile*.

Si vous ne reconnaissez pas un type de données, vous pouvez indiquer que le fichier de source de données n'est pas correctement mappé à la combinaison de documents, segments et balises UMF. Vérifiez dans la section de récapitulatif des exceptions si un segment UMF et une balise UMF concordants ont provoqué des exceptions de segment. Si le problème provient d'un UMF invalide, les chiffres du Pourcentage inutilisable de la section Récapitulatif qualitatif et le Nombre d'exceptions de segment dans la section des exceptions UMF sont généralement concordants.

Nombre d'enregistrements
Indique le nombre total de fiches d'identité entrantes pour le Type de document, le Nom de table et le Type de données spécifiés.

Nombre générique
Indique le nombre total de fiches d'identité entrantes avec le Type de document, le Nom de table et le Type de données spécifiés dont les valeurs sont considérées comme génériques.

Pourcentage inutilisable
Indique le nombre total de fiches d'identité entrantes avec le Type de document, le Nom de table et le Type de données spécifiés qui sont considérées comme inutilisables. Ce nombre peut révéler un problème de saisie de données ou de transformation ETL dans le fichier de source de données.

Pourcentage utilisable
Indique le pourcentage de fiches d'identité entrantes avec le Type de document, le Nom de table (de ce segment UMF) et le Type de données

spécifiés comme utilisables pour la résolution d'entité et la détection de relation. (Nombre de fiches moins le Nombre générique moins le Pourcentage inutilisable) divisé par le Nombre de fiches équivaut au Pourcentage utilisable.

Pourcentage d'identité
Indique le pourcentage de fiches d'identité entrantes qui contenaient le type de document, le nom de table et le type de données spécifiés.

Récapitulatif d'attribut

Cette section permet de consulter dans le fichier de source de données les attributs qui ont contribué à détecter les relations et à déclencher des alertes de rôle. Chaque attribut est associé à un segment UMF spécifique, et cette section montre le nombre de relations détectées et d'alertes de rôle déclenchées, selon les données présentes dans le segment UMF entrant.

Nom du segment
Affiche le nom du segment UMF qui correspond directement à un attribut.

Type de données
Mentionne le type d'attribut (ou type de données), au sein du segment UMF, qui correspond à la description de la précision. Il se peut que le rapport mentionne soit un type d'attribut particulier, soit *TOUS*, ce qui indique tous les types d'attribut du segment UMF.

Description de précision
Décrit le seuil de concordance entre un attribut d'une entité entrante et un attribut d'une entité existante.

Alertes de rôle
Indique le nombre total d'alertes de rôle générées sur ce segment UMF, ce type de données, et cette description de précision.

Relations
Indique le nombre total de relations détectées sur ce segment UMF, ce type de données et cette description de précision

Récapitulatif des documents UMF

Vous pouvez utiliser cette section pour valider le nombre total de fiches entrantes dans un fichier de source de données, en fonction de l'action qui doit être effectuée sur la fiche. Vous pouvez réconcilier ces nombres en Nombre d'enregistrements dans la section Récapitulatif de chargement.

Type de document
Affiche le nom du type de document UMF. Cette valeur est généralement UMF_ENTITY.

Action
Indique l'action à appliquer à l'enregistrement d'identité entrant. La liste suivante répertorie les actions les plus couramment utilisées :

- *A* : ajout
- *C* : modification
- *D* : suppression

Dans le cadre du processus ETL (extraction, transformation et chargement), les enregistrements d'identité sont généralement étiquetés au moyen du format UMF afin d'indiquer quelle action effectuer sur chacun au cours du traitement par le système.

Nombre d'enregistrements UMF
Indique le nombre total de fiches traitées pour chaque type d'action dans un type de document.

Pourcentage
Indique le pourcentage du total des fiches chargées représenté par le Nombre de fiches. (la somme ne doit pas dépasser 100%).

Récapitulatif des exceptions

Ces informations aident à repérer les enregistrements d'identité défectueux, tels que ceux dont le format UMF est syntaxiquement incorrect. L'exception décrit le problème, tandis que le nom de table et l'élément indiquent les segments et enregistrements défectueux. Le comptage montre combien d'enregistrements du fichier comportaient ce format UMF incorrect.

Type de document
Affiche le nom du type de document UMF. Cette valeur est généralement UMF_ENTITY.

Action
Indique le type d'action pour la fiche d'identité entrante :

- *A* : ajout
- *C* : modification
- *D* : suppression

Dans le cadre du processus ETL (extraction, transformation et chargement), les enregistrements d'identité sont généralement étiquetés au moyen du format UMF afin d'indiquer quelle action effectuer sur chacun au cours du traitement par le système.

Segment
Affiche le nom du segment UMF sur lequel l'exception s'est produite.

Balise UMF
Affiche la valeur de la balise UMF qui a provoqué l'exception UMF.

Exception
Affiche l'ID de message ou autre code d'exception indiquant le type d'exception UMF qui s'est produite et donne des informations sur la manière de résoudre cette exception. Cette information est également disponible dans la table UMF_EXCEPT.

Nombre d'exceptions de segment
Indique le nombre total de ce type d'exception UMF.

Vérifiez le pourcentage inutilisable à la section Récapitulatif qualitatif pour savoir si un type de données concordant est signalé comme étant de qualité médiocre ou inutilisable. Si le problème provient d'un format UMF incorrect, le nombre Pourcentage inutilisable de la section Récapitulatif qualitatif et le nombre d'exceptions de segment de la section Exceptions UMF concordent généralement pour le même segment UMF et les mêmes balises UMF.

Exécution du rapport de configuration

Le rapport de configuration offre une vue unifiée de tous les paramètres système que vous pouvez configurer à l'aide de la console de configuration. Reportez-vous à ce rapport pour connaître les paramètres de configuration système en cours

avant de modifier la configuration du produit en cours, pour la résolution d'une erreur de configuration ou pour la comparaison de différents paramètres de configuration.

Procédure

1. Dans la console de configuration, cliquez sur **Configurer** > **Rapports**.
2. Dans **Rapport**, sélectionnez **Rapport de configuration**.
3. Cliquez sur **Exécuter le rapport**.

Résultats

Le produit génère le rapport statistique sélectionné en fonction de tous les critères indiqués et affiche le rapport dans une fenêtre de navigateur distincte appelée **BIRT Report Viewer**. S'il n'y a pas de données à afficher en fonction des critères sélectionnés, la fenêtre **BIRT Report Viewer** affiche le nom du rapport, la date et l'heure de sa génération et **Page 1/1** dans la partie supérieure. La section des données est vierge.

Rapport de configuration

Le rapport de configuration offre une vue unifiée des paramètres système configurés à l'aide de la console de configuration. Ce rapport permet de consulter ou imprimer la configuration système actuelle avant de la modifier, quand vous remédiez à un problème de configuration ou quand vous devez comparer différents paramètres de configuration.

La rapport répertorie les paramètres de configuration actuels par catégorie :

Sources de données
: Permet de consulter les paramètres de configuration des sources de données, dont l'ID de source de données, le code de source de données, le code de rôle associé à la source de données, la configuration de résolution d'entité associée à la source de données ainsi que l'état actuel du code de source de données (actif ou inactif).

  Pour configurer des sources de données, sélectionnez **Configurer** > **Sources** > **Sources de données**.

Types de numéro
: Permet de consulter les paramètres de configuration des types de numéro, dont l'ID de type de numéro, le type de numéro, la longueur minimum et maximum du type de numéro, les éventuels masques associés au type de numéro, les informations sur la façon dont le type de numéro est appliqué dans la résolution d'entité, et permet de savoir si le type de numéro est actif ou inactif.

  Pour configurer des types de numéros, sélectionnez **Configurer** > **Sources** > **Numéros**.

Type de caractéristiques
: Permet de consulter les paramètres de configuration des types de caractéristique, dont l'ID de type de caractéristique, le nom du type de caractéristique, la type de données associé à la caractéristique (tel que caractère ou date), les éventuels masques associés au type de numéro, les informations sur la façon dont le type de caractéristique est appliqué dans la résolution d'entité, et permet de savoir si le type de caractéristique est actif ou inactif.

Pour configurer des types de caractéristiques, sélectionnez **Configurer** > **Sources** > **Caractéristiques**.

Plugin
Permet de consulter les paramètres de configuration pour personnaliser les attributs et le score, dont l'ID, le nom, le type, la version et le nom abrégé de bibliothèque du plug-in.

Pour configurer des plug-in afin de personnaliser les attributs et le score, sélectionnez **Configurer** > **Général** > **Plug-in**.

Types d'événement
Permet de consulter les paramètres de configuration pour les types d'événement, dont l'unité de mesure associée à la valeur pour cet événement. Les types d'événement figurent dans le gestionnaire d'événements.

Pour configurer des types d'événement, sélectionnez **Configurer** > **Sources** > **Types d'événement**.

Règles de gestion de la qualité des données (DQM)
Permet de consulter la liste des règles de gestion de la qualité des données (DQM) et paramètres associés configurés pour une balise UMF précise au sein d'un segment UMF, notamment à quels segment UMF et nom de balise UMF la règle DQM est associée, l'ordre où la règle DQM y est appliquée, et les paramètres associés à la règle DQM sur ce segment et cette balise UMF ; permet en outre de savoir si cette règle DQM corrige les données entrantes de ce segment et de cette balise UMF, et si la règle DQM est actuellement activée sur ce segment et cette balise UMF.

Pour configurer un segment UMF et une balise UMF afin d'utiliser des règles DQM, sélectionnez **Configurer** > **UMF** > **Règles DQM**.

Mappage de charge
Permet de consulter les informations de configuration sur la façon dont les données UMF sont transposées dans les tables et colonnes correspondantes de la base de données d'entité, en indiquant le nom du segment UMF, le chemin de données UMF, le nom de la table de la base de données d'entité, les nom et type de zone au sein de cette table, ainsi que le type de données de cette zone ; indique également si le mappage est activé.

Pour transposer des données d'un segment UMF à une table dans la base de données d'entité, sélectionnez **Configurer** > **UMF** > **Mappe de données**.

Règles de résolution d'entité
Permet de consulter les paramètres de configuration de chaque règle de résolution d'entité, dont son ID, l'ordre de la règle, les scores de résolution et de relation minimums et de savoir si la règle incorpore les discordances.

Pour configurer les règles de résolution d'entité, sélectionnez **Configurer** > **Résolution** > **Règles de résolution**.

Concordance/discordance de résolution d'entité
Permet de consulter les paramètres des scores qui contribuent au processus de concordance et discordance de la résolution d'entité, y compris l'ID de résolution d'entité et l'ID de configuration associés, la priorité de chaque score, la description et le nom d'attribut de chaque score, ainsi que la valeur numérique du score.

Pour configurer les paramètres de concordance et discordance de résolution d'entité, sélectionnez **Configurer** > **Résolution** > **Concordances & discordances**.

Caractéristiques de la résolution d'entité
Permet de consulter les types de caractéristique qui sont configurés avec des pondérations de concordance et discordance appliquées au cours de la résolution d'entité, notamment la priorité, la pondération de concordance et la pondération de discordance.

Pour configurer des pondérations de concordance et de discordance pour des types de caractéristiques, sélectionnez **Configurer** > **Résolution** > **Caractéristiques**.

Codes de rôle
Permet de consulter la liste des codes de rôle configurés et les paramètres associés, dont l'ID et la description du code de rôle, la classe du code de rôle et son état actuel (actif ou inactif).

Pour configure des codes de rôle, sélectionnez **Configurer** > **Relations** > **Rôles**.

Règles d'alerte de rôle
Permet de consulter la liste des règles d'alerte de rôle configurées et les paramètres associés, dont l'ID et la description de la règle, sa gravité, son seuil d'alerte minimum, et les ID de code des deux rôles qui déclenchent cette règle.

Pour configurer des règles d'alerte de rôle, sélectionnez **Configurer** > **Relations** > **Règles d'alerte de rôle**.

Configuration du gestionnaire de noms
Permet de consulter les paramètres configurés pour la fonction du gestionnaire de noms qui augmente la précision du nom pendant la résolution d'entité.

Pour configurer les paramètres du gestionnaire de noms, sélectionnez **Configurer** > **Résolution** > **Configuration de correspondance du gestionnaire de noms**.

Configuration de la séparation
Permet de consulter les paramètres pour la fonction de degrés de séparation du pipeline qui peut détecter des relations à un, deux ou plusieurs degrés de séparation.

Pour configurer les paramètres pour les degrés de séparation, sélectionnez **Configurer** > **Relations** > **Configuration de la séparation**.

Séquences système
Permet de consulter les paramètres de configuration pour les numéros de séquences qui indiquent comment le système charge et traite des données. Les numéros de séquences système contribuent de deux façons aux performances de chargement du système. En premier lieu car elles permettent à chaque pipeline d'émettre une requête qui prend un ensemble séquentiel de numéros et les conserve dans le cache jusqu'à leur utilisation. En outre, les numéros de séquences empêchent plusieurs pipelines qui génèrent des ID système d'employer le même ID dans plusieurs fiches.

Par exemple, chaque fois que le pipeline crée une entité pendant le traitement de résolution d'entité, le système génère un ID entité unique. Avec les séquences système, le pipeline peut envoyer une requête et demander les 1000 numéros d'ID entité disponibles suivants. Pour les 1000 entités suivantes créées, le pipeline peut utiliser les numéros d'ID entité disponibles stockés en mémoire. L'autre méthode (plus lente) consiste, pour

chaque pipeline, à envoyer une requête à la base de données d'entité en demandant un nouvel ID entité pour chaque entité créée.

Pour configurer des séquences système, sélectionnez **Configurer** > **UMF** > **Charger la séquence**

Seuils génériques
Permet de consulter les paramètres de seuils génériques configurés par attribut, dont le nom et le type d'attribut ainsi que le seuil qui détermine quand une certaine valeur de cette attribut devient générique.

Pour configurer des seuils génériques par type d'attribut, sélectionnez **Configurer** > **UMF** > **Seuil générique**.

Dictionnaire de table
Permet de consulter les paramètres de dictionnaire par table de base de données d'entité, dont le nom de la table, sa description et son type.

Pour configurer le dictionnaire de table, sélectionnez **Configurer** > **UMF** > **Dictionnaire**.

Tables de recherche
Permet de consulter les paramètres de la liste de tables que le système utilise comme tables de recherche au cours du traitement, notamment le nom de la table, le nom de zone clé et le nom de zone d'ID ; indique également s'il faut charger la table en mémoire au cours du traitement.

Pour configurer les tables que le système utilise comme tables de recherche, sélectionnez **Configurer** > **UMF** > **Recherche**.

Configuration de correspondance
Permet de consulter les paramètres de chaque configuration de résolution présente sur votre système, dont les nom et ID de la configuration, le type de correspondance et le nom de segment UMF.

Pour configurer des configurations de correspondance, sélectionnez **Configurer** > **Résolution** > **Générateur de candidats**.

Types de document
Permet de consulter les paramètres des documents d'entrée UMF, dont le type de document, s'il faut effectuer la gestion de la qualité des données sur ce type de document, s'il faut charger les données traitées par ce type de document dans la base de données de résolution d'entité, ainsi que le niveau de résolution d'entité à effectuer sur ce type de document UMF d'entrée.

Pour configurer des documents d'entrée UMF, sélectionnez **Configurer** > **UMF** > **Documents d'entrée**.

Format de sortie UMF
Permet de consulter les paramètres de format pour les documents de sortie UMF, dont l'ID format et le code, le sens du routage et savoir si le paramètre de format de sortie est activé.

Pour configurer des formats pour des documents de sortie UMF, sélectionnez **Configurer** > **UMF** > **Documents de sortie**.

Types d'événement GEM
Permet de consulter les paramètres de format pour les événements du gestionnaire d'événements, dont l'ID, le type, la description, la catégorie, l'unité de mesure et la date et l'heure de création.

Pour configurer des types d'événement, sélectionnez **Configurer** > **Sources** > **Type d'événement**.

Paramètres système
Permet de consulter la liste des réglages des paramètres système, par groupe, dont la valeur et la valeur par défaut du paramètre, ainsi que son type et sa valeur de validation.

Pour configurer des paramètres système, sélectionnez **Configurer** > **Général** > **Paramètres système**.

Codes d'activité de l'application
Permet de consulter la liste des codes d'activité configurés pour Visualizer par type d'activité (alerte de rôle, alerte d'attribut ou alerte d'événement), dont le code d'activité, les états valides pour celui-ci, et savoir si ce code est actif ou inactif.

Pour configurer les codes d'activité utilisés dans Visualizer, sélectionnez **Configurer** > **Visualizer** > **Codes d'activité**.

Groupes d'utilisateurs
Permet de consulter les paramètres des groupes d'utilisateurs configurés pour le visualiseur, dont les noms d'utilisateurs du visualiseur associés, les date et heure de création du groupe, et si ce dernier est actif ou inactif.

Pour configurer les codes d'activité utilisés dans Visualizer, sélectionnez **Configurer** > **Visualizer** > **Codes**, puis **ANALYZER_GROUP**.

Groupes d'alertes de rôle
Permet de consulter les paramètres des groupes d'alertes de rôle configurés, dont les groupes d'applications attribués, l'ID et la description de la règle d'alerte de rôle associée, les date et heure de création du groupe d'alertes de rôle, et si ce dernier est actif ou inactif.

Pour configure des groupes d'alertes de rôle utilisés dans Visualizer, sélectionnez **Configurer** > **Relations** > **Règles d'alerte de rôle**, puis modifiez le contenu de la zone **Groupe d'alertes**.

Utilisateurs
Permet de consulter les paramètres des utilisateurs configurés pour se connecter au visualiseur, dont les noms de connexion, et de savoir s'il faut authentifier l'utilisateur du visualiseur à l'aide des accréditations de la base de données d'entités, et si cet utilisateur est actif ou inactif.

Pour configurer les utilisateurs, sélectionnez **Configurer** > **Visualizer** > **Utilisateurs de Visualizer**.

Exportation de rapports

Le composant BIRT Report Viewer permet d'exporter les données du rapport de la console de configuration dans d'autres applications, telles que Microsoft Excel, Microsoft PowerPoint, Microsoft Word ou Adobe Acrobat. Vous pouvez exporter l'ensemble ou une partie d'un rapport.

Exportation des rapports de la console de configuration

Si vous souhaitez exporter l'intégralité d'un rapport (données et format) dans une autre application, telle que Microsoft PowerPoint, ou dans un autre format, tel qu'Adobe Acrobat PDF, utilisez l'option **Export reports** dans BIRT Report Viewer. L'exportation de rapports complets fonctionne bien pour les rapports de plusieurs pages et lorsque vous ne souhaitez pas manipuler les données à l'issue de l'exportation du rapport.

Pourquoi et quand exécuter cette tâche

L'ouverture d'un rapport de la console de configuration exporté dans un fichier *.doc de Microsoft Word requiert Microsoft Word version 2003 ou suivante.

Si vous souhaitez apporter des modifications ou des ajouts mineurs au rapport exporté, exportez le rapport dans Microsoft Word ou Microsoft Excel. Ces applications conservent le formatage du rapport mais les données sont généralement affichées dans des colonnes ou des tables pour permettre leur manipulation. Le rapport exporté étant un fichier en lecture seule, vous devez l'enregistrer sous un nouveau nom pour enregistrer les modifications.

Procédure

1. Après avoir généré le rapport, cliquez sur **Export report** dans la fenêtre **BIRT Report Viewer**. L'icône Exporter le rapport est la quatrième icône à partir de la gauche de la barre d'outils BIRT Report Viewer.
2. Dans la section **Export Report**, sélectionnez le format ou l'application dans laquelle exporter les données :
   - **PDF**
   - **PowerPoint**
   - **Word**
   - **PostScript**
   - **Excel**
3. Sélectionnez les pages ou la plage de pages à exporter.
4. Facultatif : Sélectionnez la taille du rapport généré : Cette option est disponible uniquement si vous avez sélectionné l'option PDF, PowerPoint ou PostScript.
   - **Auto**: Chaque page du rapport devient une page distincte.
   - **Actual size**: Toutes les pages du rapport sont regroupées au sein d'une longue page unique.
   - **Fit to whole page** : La taille de toutes les pages du rapport sont réduites pour tenir dans un tiers d'une page. Si vous avez sélectionné l'option PowerPoint, le rapport est inséré sous forme d'image dans la page pour vous permettre de redimensionner l'image.
5. Cliquez sur **OK**.

Résultats

Si vous avez exporté le rapport dans PDF ou PostScript, le fichier obtenu est généralement placé dans le dossier où les fichiers sont téléchargés sur le client. Par exemple, C:\Documents and Settings\Administrator\My Documents\Downloads.

Si vous avez exporté le rapport dans PowerPoint, Word, ou Excel, les données sont exportées dans un fichier en lecture seule appelé *nom_rapport.extension_application_sélectionnée*.

- *nom_rapport* est le nom du rapport de la console de configuration que vous avez exporté.
- *extension_application_sélectionnée* est l'extension de format de fichier appropriée pour l'application sélectionnée.

Par exemple, si vous avez exporté le rapport récapitulatif par chargement dans Word, le nom de fichier est généralement appelé LoadSummary.doc. Une boîte de dialogue s'affiche pour vous permettre d'ouvrir le fichier dans l'application sélectionnée ou enregistrer le fichier.

Exportation des données de rapports de la console de configuration

Si vous souhaitez exporter les données des rapports dans un fichier CSV (Comma Separated Values) pour les afficher et les manipuler dans une autre application, telle que Microsoft Excel, utilisez l'option **Export data** dans le composant BIRT Report Viewer. Vous pouvez sélectionner une section du rapport, les zones à exporter et le format des données exportées.

Pourquoi et quand exécuter cette tâche

Le composant BIRT Report Viewer exporte une seule section de données d'un rapport à la fois, ce qui signifie que l'afficheur crée un ensemble de résultats distinct pour chaque section du rapport. Les données exportées sont des données brutes sans formatage.

Si vous souhaitez exporter l'ensemble du rapport, utilisez l'option **Export report** à la place. Toutefois, cette option exporte le formatage des données et du rapport et vous empêche de manipuler les données après l'exportation.

Procédure

1. Une fois le rapport généré, cliquez sur l'icône **Export data** dans BIRT Report Viewer. L'icône **Export data** est la troisième icône à partir de la gauche dans la barre d'outils de BIRT Report Viewer.
2. Obligatoire : Dans la section **Available results sets** de **Export Data**, sélectionnez la section du rapport que vous souhaitez exporter. Les noms des sections du rapport s'affichent par élément, par exemple ELEMENT_2041. Vous pouvez généralement identifier la section que vous sélectionnez en examinant les noms de colonne répertoriées dans **Available Columns**.
3. Obligatoire : Dans la zone **Available Columns**, sélectionnez les colonnes à exporter. Les noms de colonne applicables à la section du rapport sélectionnée dans la zone **Available results sets** s'affichent dans la zone **Selected Columns**. Vous ne souhaitez peut-être pas afficher les données de toutes les colonnes disponibles pour cette section du rapport.
4. Facultatif : Définissez l'ordre des colonnes dans la zone **Selected Columns**. Cette option permet de réorganiser les données par colonne avant d'exporter les données.
5. Facultatif : Dans la zone **Separator**, sélectionnez un séparateur si vous souhaitez utiliser un type de séparateur différent de la valeur par défaut **Comma** :
   - **Semi-colon**
   - **Colon**
   - **Vertical line**
   - **Tabulation**
6. Cliquez sur **OK**. Dans la boîte de dialogue qui s'affiche, indiquez si vous souhaitez ouvrir les données exportées ou enregistrer le fichier. Microsoft Excel est l'application utilisée par défaut pour ouvrir le fichier mais vous pouvez sélectionner n'importe quelle application capable d'exporter un fichier CSV.

Résultats

Les données sont exportées dans un fichier généralement appelé *nomrapport*.csv, où *nomrapport* est le nom du rapport de la console de configuration dont vous avez exporté les données.

Administration du visualiseur

Pour utiliser efficacement Visualizer, vous devez configurer les navigateurs, établir les comptes pour les utilisateurs appropriés et gérer l'accès à Visualizer.

Visualizer

Le Visualizer est une interface utilisateur graphique que les analystes et les investigateurs utilisent pour analyser les résultats des alertes, des relations et des résolutions d'entités.

Le Visualizer est hébergé par une version intégrée d'IBM WebSphere Application Server. Pour configurer le Visualizer , utilisez la console de configuration et les **Préférences** du menu **Fichier**.

Les utilisateurs du Visualizer peuvent réaliser plusieurs tâches d'analyse :

Analyse et définition d'alertes
Les alertes générées par le processus de résolution d'entité représentent les relations ou les résolutions d'entités qui peuvent concerner directement une entreprise. Généralement, les analystes consultent les alertes et décident le cas échéant de l'action à entreprendre, en fonction des informations de l'alerte. Il existe trois types d'alertes : les alertes de rôle, les alertes d'attribut et les alertes d'événements.

Le Visualizer affiche les alertes, offrant aux analystes à la fois un texte et un graphique relatifs à ces alertes ainsi qu'aux entités directement concernées. Les analystes peuvent explorer les détails en aval, puis définir l'état de l'alerte en conséquence.

Création et gestion des générateurs d'alertes d'attribut
Le Visualizer permet aux analystes de créer et gérer des recherches permanentes dans la fonction du générateur d'alertes d'attribut, mais aussi de gérer l'affichage et la réception des alertes d'attribut. Les analystes peuvent créer des générateurs d'alertes d'attribut basés sur des données d'attributs afin de localiser les identités résolues en entités en fonction de ces données d'attributs. Ils peuvent également créer un générateur d'alertes d'attribut afin de rechercher de façon permanente une entité spécifique dans la base de données de l'entité.

Recherche d'entités
Les utilisateurs du Visualizer peuvent également rechercher des entités pour une analyse approfondie à l'aide de plusieurs méthodes :

- Par attribut
- Par compte de source de données
- Par ID d'entité
- Par résolution (dans quelle mesure les critères saisis correspondent aux identités et aux entités dans la base de données de l'entité, en fonction de seuils de score de résolution minimum)

Ajout d'entités et de relations divulguées
Le Visualizer permet aux analystes d'ajouter des fiches pour la résolution d'entités et la détection de relations. Ils peuvent ajouter une seule fiche d'entité ou charger un fichier UMF contenant quelques milliers de fiches d'identités. Comme pour l'ajout de fiches d'identités via un programme d'acquisition, les fiches ajoutées via le Visualizer sont traitées par un pipeline pour la résolution d'entités et la détection de relations. Les

résultats de ce traitement sont transcrits dans la base de données des entités et toute alerte est publiée dans le Visualizer .

Les analystes peuvent également divulguer les relations entre des entités (par identité), lorsqu'un lien existe entre des identités. L'association d'entités basées sur des contacts d'urgence ou de références répertoriées sur une application d'emploi est un exemple de relation divulguée. L'entité a révélé ces relations sur l'application.

Génération et impression de rapports
Le Visualizer contient également plusieurs rapports que les analystes peuvent consulter et imprimer afin de gérer et d'effectuer un suivi du travail accompli avec le Visualizer .

Rôles et responsabilités de l'utilisateur

Les rôles utilisateur permettent de catégoriser les tâches typiques qui doivent être exécutées pour correctement déployer et utiliser IBM InfoSphere Identity Insight. De nombreux types d'utilisateurs peuvent utiliser IBM InfoSphere Identity Insight pour des raisons variées, à savoir qu'ils endossent les responsabilités d'un ou plusieurs rôles au moment d'utiliser le produit.

Vous pouvez définir des groupes d'utilisateurs en fonction des différents rôles et responsabilités de chaque utilisateur.

Les rôles utilisateur les plus courants sont les suivants :

Analyste
Analyse les données et vérifie les entités, les relations et les alertes. L'analyste définit les résultats les plus pertinents et s'assure qu'ils sont bien renvoyés par le système. Il travaille en étroite collaboration avec l'opérateur et l'administrateur d'application.

Opérateur
Charge les données dans le système, exécute les pipelines et vérifie que le système fonctionne correctement, rédigeant le cas échéant des rapports sur la qualité des données chargées. L'opérateur vérifie également les résultats, les exceptions et les événements. Il travaille en étroite collaboration avec l'analyste, l'administrateur de sources de données et l'administrateur d'application.

Administrateur de sources de données
Prépare les données avant leur chargement dans le système, ce qui consiste à les convertir en fichier UMF et à valider ce fichier. L'administrateur de sources de données travaille en étroite collaboration avec les opérateurs, les administrateurs d'application et les administrateurs de base de données.

Administrateur d'application
Procède à la configuration de l'application, notamment celle des données, des modèles d'entités et des règles. L'administrateur d'application travaille en étroite collaboration avec les administrateurs de sources de données et les opérateurs pour définir le modèle d'entité et coordonne les modifications de configuration avec l'administrateur de base de données, l'administrateur de sources de données et les opérateurs. Il assure également la coordination et consulte les administrateurs système généraux, s'ils existent.

Administrateur de base de données
Vérifie que la base de données est correctement configurée et réglée pour pouvoir être utilisée avec l'application. L'administrateur de base de

données travaille en étroite collaboration avec l'opérateur, l'administrateur de sources de données et l'administrateur d'application.

Architecte système
Evalue les configurations matérielle et logicielle requises pour la planification du déploiement de l'application. L'architecte système travaille en étroite collaboration avec le responsable de l'installation, l'administrateur de base de données, l'administrateur de sources de données et l'administrateur d'application pour assurer un déploiement qui correspond à la vision, aux stratégies et aux objectifs prévus et qui s'intègre à vos processus métier tout en offrant les résultats attendus.

Responsable de l'installation
Gère l'installation et la configuration initiale de l'application. Le responsable de l'installation configure les utilisateurs initiaux dans le système. Il est très souvent aidé par IBM Professional Services pour définir ces responsabilités.

Programmeur
Conçoit et développe des interfaces graphiques ou en personnalise pour les diverses fonctions, de telle sorte que le déploiement de l'application s'intègre à votre environnement de façon transparente. Le programmeur travaille en étroite collaboration avec l'architecte système et l'administrateur d'application, souvent pour envoyer des alertes aux personnes concernées, de la façon la plus appropriée pour votre environnement.

Architecte de la sécurité
Vérifie que l'équipe du projet respecte et implémente un système sécurisé. L'architecte de la sécurité travaille en étroite collaboration avec l'architecte système, le responsable de l'installation et l'administrateur de base de données.

Paramètres de navigateur optimaux pour Visualizer

Visualizer est une application Java, accessible via le Web, qui fonctionnera de façon optimale si vous configurez des paramètres spécifiques de votre navigateur.

Pour un affichage optimal de Visualizer, utilisez les paramètres suivants du navigateur :

Tableau 28. Paramètres de navigateur optimaux pour Visualizer

Paramètre	Valeur	Description
Taille du texte	Moyen	
JavaScript	Activé	
Cookies	Activé	Les cookies des sessions primaires doivent au moins être activés.
Sécurité - site Web approuvé	Adresse HTTP de Visualizer	Assurez-vous que l'adresse HTTP de Visualizer figure dans la liste des sites Web approuvés.
Sécurité - options de téléchargement	Activé	Assurez-vous que toutes les options de téléchargement des sites Web approuvés sont activées.

Logiciels de blocage d'incrustation	Autoriser les fenêtres spontanées à partir de l'adresse HTTP de Visualizer	Vérifiez que l'adresse HTTP de Visualizer figure dans la liste des sites Web autorisant les fenêtres spontanées.

Connexion au Visualizer

Avant de vous connecter au Visualizer, vous devez avoir un compte utilisateur Visualizer (nom d'utilisateur et mot de passe). Votre administrateur système peut vous fournir ces informations.

Procédure

1. Effectuez l'une des opérations suivantes :
   - Cliquez deux fois sur l'icône Visualizer sur votre bureau.
   - Ouvrez votre navigateur Internet et entrez l'adresse URL de Visualizer dans la barre d'adresse.

   L'URL de lancement du Visualizer est la suivante :

   `http://server:install_port`

   Par exemple, `http://localhost:13510`. Une fois Visualizer installé, la valeur *port_installation* par défaut est 13510, mais le numéro de port est modifiable. Contactez votre administrateur système si vous n'êtes pas sûr du nom de serveur ou du numéro de port.
2. Connectez-vous en entrant votre nom d'utilisateur et votre mot de passe.

   Remarque : Ces deux zones sont sensibles à la casse. A la première connexion, utilisez le mot de passe attribué par votre administrateur système. Une fois connecté, modifiez votre mot de passe Visualizer pour garantir la sécurité de votre compte Visualizer.
3. Cliquez sur **Ouvrir une session**.

Fermeture du visualiseur

Lorsque vous en avez terminé avec Visualizer, fermez-le. En fermant le Visualizer, vous vous déconnectez également. Si vous faites une pause et que vous voulez simplement sécuriser votre poste de travail pendant quelques minutes, vous pouvez verrouiller le Visualizer.

Procédure

Pour fermer le Visualizer et vous déconnecter :

- Sélectionnez **Fichier** > **Quitter**,
- Ou appuyez sur **Ctrl** + **Q**.

Gestion de l'accès au visualiseur

Pour pouvoir se connecter au visualiseur, il faut d'abord que ses utilisateurs possèdent un compte enregistré. Ces comptes ne sont pas les mêmes que ceux de la console de configuration, mais sont au contraire spécifiquement autorisés à utiliser le visualiseur.

Création d'utilisateurs de Visualizer

Pour accéder à Visualizer et l'utiliser, un administrateur système doit créer un compte pour l'utilisateur dans la console de configuration.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Visualizer**.
3. Cliquez sur l'onglet **Utilisateurs de Visualizer**.
4. Cliquez sur le bouton **Nouveau**.
5. Dans la liste déroulante **Nom de connexion à la base de données**, sélectionnez l'une des valeurs suivantes :
   - Cliquez sur **Oui** si l'utilisateur possède un compte qui lui accorde l'accès à la base de données d'entité et que vous voulez employer les informations de connexion à cette base de données.
   - Cliquez sur **Non** si vous utilisez les informations de connexion du fichier par défaut. Dans ce cas, un administrateur système choisit le premier mot de passe employé par l'utilisateur pour se connecter à Visualizer et peut réinitialiser les mots de passe Visualizer sur demande.
6. Dans la zone **Nom d'utilisateur**, entrez le nom d'utilisateur que vous voulez ajouter. Si vous avez sélectionné**Oui** dans la liste déroulante **Connexion à la base de données**, ce nom d'utilisateur doit correspondre à celui de la base de données d'entité pour cet utilisateur.
7. Dans la zone **Mot de passe** :
   a. Si vous avez sélectionné **Oui** dans la liste déroulante **Nom de connexion à la base de données**, cette valeur doit correspondre au mot de passe stocké dans les informations de connexion à la base de données.
   b. Si vous avez sélectionné **Non** dans la liste déroulante **Nom de connexion à la base de données**, tapez le mot de passe initial de l'utilisateur.

      Remarque : Pour des raisons de sécurité, encouragez vos utilisateurs de Visualizer à changer leur mot de passe initial après la première connexion.
8. Facultatif : Dans la zone **Groupe** de la liste déroulante, sélectionnez le groupe d'analystes auquel appartient cette personne.
9. Cliquez sur le bouton **Enregistrer**.

Que faire ensuite

L'utilisateur peut alors utiliser immédiatement ce nom d'utilisateur et ce mot de passe pour se connecter à Visualizer.

Désactivation d'utilisateurs de Visualizer

Vous pouvez désactiver des comptes Visualizer d'utilisateurs qui n'ont plus besoin d'accéder à Visualizer.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Visualizer**.
3. Cliquez sur l'onglet **Utilisateurs de Visualizer**.
4. Cliquez sur le nom d'utilisateur dont vous voulez désactiver le compte.
5. Dans la liste déroulante **Etat**, sélectionnez **Inactif**.
6. Cliquez sur le bouton **Enregistrer**.

Résultats

L'utilisateur désactivé ne peut plus se connecter à Visualizer.

Réinitialisation des mots de passe Visualizer

Si les utilisateurs de Visualizer oublient leur mot de passe et que leurs informations de connexion sont configurées dans la console de configuration et non via l'option sous-jacente de connexion à la base de données, vous pouvez réinitialiser leur mot de passe dans la console de configuration. Sinon, vous devez réinitialiser son mot de passe au moyen de la configuration de connexion de la base de données sous-jacente.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Visualizer**.
3. Cliquez sur l'onglet **Utilisateurs de Visualizer**.
4. Cliquez sur le nom de l'utilisateur dont vous voulez modifier le mot de passe.
5. Dans la zone **Mot de passe**, attribuez un nouveau mot de passe à cet utilisateur.

   Remarque : Pour des raisons de sécurité, encouragez les utilisateurs à changer leur mot de passe après s'être connectés, afin d'être les seuls à le connaître.
6. Cliquez sur le bouton **Enregistrer**.

Que faire ensuite

L'utilisateur peut immédiatement utiliser ce nouveau mot de passe pour se connecter à Visualizer. Pour des raisons de sécurité, une fois des mots de passe réinitialisés, encouragez les utilisateurs à changer leur mot de passe une fois connectés.

Création de groupes d'utilisateurs du visualiseur

Les alertes sont attribuées à des groupes d'analystes dans le visualiseur. Si vous ajoutez un nouveau groupe d'analystes à un projet, vous pouvez créer un nouveau groupe à l'aide de la console de configuration.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Codes**.
4. Dans la liste déroulante **Type**, cliquez sur **ANALYZER_GROUP**.
5. Cliquez sur le bouton **Nouveau**.
6. Dans la zone **Code**, tapez le nom du groupe d'analystes.
7. Dans la liste déroulante **Etat**, sélectionnez **Actif**.
8. Cliquez sur le bouton **Enregistrer**.

Rubriques d'aide

Utilisateurs du Visualizer - onglet Général :

Cet onglet permet d'ajouter de nouveaux utilisateurs de Visualizer ou de modifier des mots de passe existants d'un utilisateur.

Nom de connexion à la base de données
: Sélectionnez une option pour déterminer si vous devez utiliser les informations de connexion à la base de données d'entités sous-jacentes (nom et mot de passe) pour accéder à Visualizer.

- Oui - N'utilisez ce réglage que si cet utilisateur de Visualizer possède déjà un compte qui lui octroie l'accès à la base de données d'entité. Si vous sélectionnez cette option, utilisez le nom d'utilisateur et le mot de passe de connexion à la base de données d'entité comme nom d'utilisateur et mot de passe pour Visualizer. (S'ils ne correspondent pas, l'utilisateur de Visualizer ne peut pas se connecter.)
- Non - Utilisez les informations de connexion entrées dans cet onglet.

Nom d'utilisateur
Tapez le nom de cet utilisateur de Visualizer. S'il se sert d'une connexion à la base de données, son nom doit correspondre à celui pour la base de données d'entité.

Mot de passe
Tapez le nouveau mot de passe pour cet utilisateur de Visualizer. S'il se sert d'une connexion à la base de données, son mot de passe doit correspondre exactement à celui pour la base de données.

Groupe
Sélectionnez le groupe de Visualizer auquel cet utilisateur appartient. Ce groupe détermine les alertes et les notifications que l'utilisateur voit dans la fenêtre **Récapitulatif des alertes** de Visualizer. (Par exemple, si votre organisation possède un groupe Security Visualizer et un groupe Reservation, les utilisateurs de chacun d'eux peuvent voir des types différents d'alertes dans Visualizer.).

Etat Sélectionnez un état pour indiquer si cet utilisateur de Visualizer est actif (capable de se connecter à Visualizer) ou non.

Configuration de codes d'activité pour le visualiseur

Le visualiseur est doté de plusieurs codes d'activité par défaut destinés à la gestion des alertes. Vous pouvez ajouter de nouveaux codes d'activité et en supprimer via la console de configuration.

Création de codes d'activité pour les recherches

Le visualiseur est doté de codes d'activité pour les alertes de résultat de recherche. Si vous devez superviser des activités supplémentaires concernant la gestion des alertes, vous pouvez ajouter de nouveaux codes d'activité à la console de configuration.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Visualizer**.
3. Cliquez sur l'onglet **Codes d'activité**.
4. Dans la liste déroulante **Type d'activité**, cliquez sur **SEARCH**.
5. Cliquez sur le bouton **Nouveau**.
6. Dans la zone **Code d'activité**, tapez le nom du code d'activité.
7. Dans la liste déroulante **Code d'état d'activité**, sélectionnez le code d'état d'activité reconnu en interne auquel le nouveau code d'activité correspond.
8. Dans la liste déroulante **Etat**, sélectionnez **Actif**.
9. Cliquez sur le bouton **Enregistrer**.

Suppression de codes d'activité pour les recherches

Le visualiseur est doté de codes d'activité pour les alertes de résultat de recherche. Si vous devez supprimer des codes d'activité concernant la gestion des alertes, vous pouvez le faire à l'aide de la console de configuration.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Visualizer**.
3. Cliquez sur l'onglet **Codes d'activité**.
4. Dans la liste déroulante **Type d'activité**, cliquez sur **SEARCH**.
5. Cochez la case du code d'activité à supprimer.
6. Cliquez sur le bouton **Supprimer**. Une fenêtre de confirmation apparaît.
7. Cliquez sur **OK**.

Création de codes d'activité pour les alertes de rôle

Le visualiseur est doté de codes d'activité pour les alertes de rôle. Si vous devez superviser des activités supplémentaires concernant la gestion des alertes, vous pouvez ajouter de nouveaux codes d'activité à la console de configuration.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Visualizer**.
3. Cliquez sur l'onglet **Codes d'activité**.
4. Dans la liste déroulante **Type d'activité**, cliquez sur **CONFLIT**.
5. Cliquez sur le bouton **Nouveau**.
6. Dans la zone **Code d'activité**, tapez le nom du code d'activité.
7. Dans la liste déroulante **Code d'état d'activité**, sélectionnez le code d'état d'activité reconnu en interne auquel le nouveau code d'activité correspond.
8. Dans la liste déroulante **Etat**, sélectionnez **Actif**.
9. Cliquez sur le bouton **Enregistrer**.

Suppression de codes d'activité pour les alertes de rôle

Le visualiseur est doté de codes d'activité pour les alertes de rôle. Si vous devez supprimer des codes d'activité concernant la gestion des alertes, vous pouvez le faire à l'aide de la console de configuration.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Visualizer**.
3. Cliquez sur l'onglet **Codes d'activité**.
4. Dans la liste déroulante **Type d'activité**, cliquez sur **CONFLIT**.
5. Cochez la case du code d'activité à supprimer.
6. Cliquez sur le bouton **Supprimer**. Une fenêtre de confirmation apparaît.
7. Cliquez sur **OK**.

Création de codes d'activité pour des alertes d'événement

Visualizer fournit des codes d'activité pour des alertes d'événement générées via le traitement d'événements, si le gestionnaire d'événements est activé sur votre système. Les codes d'activité d'événements vous permettent de faire le suivi d'activités supplémentaires liées à la gestion des alertes d'événement. Le système

fournit trois codes d'activité d'événements prédéfinis, mais vous pouvez ajouter des nouveaux codes d'activité pour des alertes d'événement à l'aide de la console de configuration.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Visualizer**.
3. Cliquez sur l'onglet **Codes d'activité**.
4. Dans la liste déroulante **Type d'activité**, sélectionnez **EVENT**.
5. Cliquez sur le bouton **Nouveau**.
6. Dans la zone **Code d'activité**, entrez un nom unique pour le nouveau code d'activité.
7. Dans la liste déroulante **Code d'état d'activité**, sélectionnez le code d'état d'activité reconnu en interne auquel le nouveau code d'activité correspond.
8. Dans la liste déroulante **Etat**, sélectionnez **Actif** afin que ce code d'activité soit disponible dans Visualizer.
9. Cliquez sur le bouton **Enregistrer**.

Codes d'activité prédéfinis pour des alertes d'événement :

Les codes d'activité d'événements sont utilisés par les analystes dans Visualizer pour des alertes d'événement. Le système inclut trois codes d'activité prédéfinis pour des événements après exécution des scripts SQL du groupe de correctifs v4.2 post-installation.

Les codes d'activité suivants sont inclus dans l'ensemble prédéfini de codes d'activité d'alertes d'événement :

ATTRIBUE
Lorsque des analystes s'attribuent une alerte d'événement ou l'attribuent à un autre groupe, le système prend par défaut le code d'activité ASSIGNED.

FERME
Lorsque des analystes ferment une alerte d'événement, le système prend par défaut le code d'activité CLOSED.

EN ATTENTE
Avant les alertes d'événement de dispositions d'un analyste, le système leur attribue automatiquement l'activité EN ATTENTE ; l'alerte d'événement est alors ouverte pour tout analyste dans le groupe affecté pour révision ou disposition.

Modification de codes d'activité pour des alertes d'événement

Vous pouvez modifier des codes d'activité existants pour des alertes d'événement de disposition dans Visualizer. Vous ne pouvez pas renommer un code d'activité existant, mais vous pouvez en changer la description associée, le code d'état de l'activité ou son état.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Visualizer**.
3. Cliquez sur l'onglet **Codes d'activité**.
4. Dans la liste déroulante **Type d'activité**, sélectionnez **EVENT**.
5. Cliquez sur le code d'activité que vous voulez modifier.

6. Dans l'onglet **Général**, effectuez les changements. Par exemple, si vous voulez configurer un code d'activité sans l'afficher pour sélection dans Visualizer, sélectionnez l'état **Inactif**. De cette façon, il est inutile de supprimer le code d'activité pour l'activer ultérieurement.
7. Cliquez sur le bouton **OK**.

Suppression de codes d'activité pour des alertes d'événement

Visualizer fournit des codes d'activité pour les alertes d'événement de disposition. Si vous devez supprimer des codes d'activité liés à la gestion d'alertes d'événement, vous pouvez supprimer des codes d'activité existants à l'aide de la console de configuration, dont des codes d'activité d'alertes d'événement prédéfinis. La suppression du code d'activité rend celui-ci indisponible dans Visualizer lors de la gestion des alertes d'événement.

Pourquoi et quand exécuter cette tâche

Si vous voulez uniquement modifier des informations pour le code d'activité, vous pouvez changer celui-ci sans le supprimer ou le recréer.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Visualizer**.
3. Cliquez sur l'onglet **Codes d'activité**.
4. Dans la liste déroulante **Type d'activité**, sélectionnez **EVENT**.
5. Cochez la case à côté des codes d'activité que vous voulez supprimer.
6. Cliquez sur le bouton **Supprimer**. Une fenêtre de confirmation apparaît.
7. Cliquez sur le bouton **OK**.

Codes d'activités du Visualizer - onglet Général

Les codes d'activités sont utilisés par des analystes dans Visualizer pour des alertes de rôle, des alertes d'événement et des recherches.

Type d'activité
Renseigné par le système. Sélectionnez le type d'activité pour afficher, ajouter ou supprimer des codes d'activités :
- **CONFLICT** utilisé pour les alertes de rôle
- **EVENT** utilisé pour les alertes d'événement
- **SEARCH** utilisé pour les recherches dans Visualizer

Code d'activité
Entrez le nom unique pour ce code d'activité.

Description
Tapez la description de ce code d'activité.

Code d'état d'activité
Sélectionnez le code d'état interne auquel ce code d'activité correspond :
- **Ouvert**
- **Attribué**
- **Fermé**
- **Filtré**

Etat Indique si ce code d'activité est actif. Par exemple, vous pouvez configurer

un code d'activité avant d'implémenter le code dans Visualizer en désactivant le code d'activité. Au moment d'implémenter le code d'activité, modifiez-le pour l'activer.

Administration des paramètres de configuration du système

La configuration système peut être modifiée à l'aide des processus suivants :

Chapitre 5. Configuration des données du système

Pour utiliser efficacement IBM InfoSphere Identity Insight, vous devez au préalable configurer la base de données d'entités, la résolution d'entité, et les paramètres système.

Configuration des données dans le système

Pour utiliser IBM InfoSphere Identity Insight, vous devez au préalable configurer la base de données d'entités pour qu'elle fonctionne avec vos données sources.

Configuration de types de caractéristique

Vous pouvez configurer des types de caractéristique pour les données qu'il est impossible de classer comme nom, nombre, adresse ou adresse électronique. Quand de nouvelles données sont ajoutées à une source de données et que vous souhaitez les classer comme caractéristique dont le type n'est pas encore configuré dans le système, vous devez créer un type de caractéristique pour ces nouvelles données.

Caractéristiques

Les caractéristiques sont des traits ou propriétés définis par l'utilisateur et associés à une identité qui ne s'exprime habituellement pas sous forme de nom, de numéro, d'adresse ni d'adresse électronique.

Cet attribut permet d'enrichir le produit en définissant des attributs d'entité personnalisables, significatifs pour leurs sources de données.

Type de caractéristiques :

Les types de caractéristique organisent et identifient les données qui sont stockées dans la base de données d'entités. La date de naissance et le sexe constituent des exemples de types de caractéristique par défaut préconfigurés dans la base de données d'entités.

Si vous possédez des données qui ne sont pas définies par l'un des types de caractéristique par défaut, vous devez créer un nouveau type de caractéristique pour ces données.

Exemple

Le groupe bancaire SBN a récemment ajouté une nouvelle catégorie de données sur ses types de clients. Les données parviennent au noeud d'acquisition au moyen des balises UMF suivantes :

```
<attribute>
 <attr_type>cust_type</attr_type>
 <attr_value>merchant</attr_value>
</attribute>
```

Dans cet exemple, vous devez configurer un nouveau type de caractéristique appelé cust_type.

Types de caractéristique créés par le système :

Si un message UMF est traité avec un type de caractéristique qui n'est pas configuré, le système crée automatiquement un nouveau type.

La valeur du message UMF est enregistrée dans la base de données au moyen du nouveau type de caractéristique, et une exception UMF est transcrite.

Quand le système crée automatiquement une nouvelle caractéristique, il en résulte dans la base de données une fiche incomplète ne contenant que :

- Les informations sur le nouveau **type** basées sur le message UM.
- La valeur de **Etat** créée par le système.

Consultation des types de caractéristique

Les types de caractéristique servent aux données qu'il est impossible de classer comme nom, nombre, adresse ou adresse électronique. Il est conseillé de consulter les types de caractéristique existants si vous envisagez d'en ajouter un nouveau.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Caractéristiques**.
4. Sélectionnez le type de caractéristique à consulter.

Création d'un type de caractéristique

Dans le système, les caractéristiques des entités sont organisées par type.

Avant de commencer

Avant de créer un nouveau type de caractéristique, examinez les données de caractéristiques entrantes pour déterminer s'il est possible de les décrire précisément au moyen d'un type de caractéristique existant.

Pourquoi et quand exécuter cette tâche

Pour utiliser efficacement de nouvelles données de caractéristiques, vous devez configurer un nouveau type de caractéristique à l'aide de la console de configuration. Si vous créez un nouveau type de caractéristique dont la valeur de type de données est DATE, il vous sera proposé de créer une nouvelle règle DQM pour valider le nouveau type de caractéristique.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Caractéristiques**.
4. Cliquez sur le bouton **Nouveau**.
5. Dans l'onglet **Général**, indiquez le type, la description, le type de données, la classe, l'utilisation de la résolution, l'état, le paramètre d'historique et le niveau d'affichage de ce type de caractéristique.
6. Cliquez sur le bouton **Enregistrer**. Si vous créez un nouveau type de caractéristique dont la valeur de type de données est DATE, et que vous choisissez de créer une nouvelle règle DQM pour valider le nouveau type de

caractéristique, vous serez redirigé sur la page de création de règle DQM avec des valeurs pré-remplies selon le nouveau type de caractéristique.

Résultats

Le système peut désormais traiter les données dans un fichier UMF qui est indiqué pour <CHARACTERISTIC_TYPE>.

Suppression de types de caractéristique

Vous pouvez supprimer un type de caractéristique existant une fois que la base de données d'entités ne s'en sert plus.

Pourquoi et quand exécuter cette tâche

Si vous avez créé une règle DQM pour accompagner le type de caractéristique, il est souhaitable de la supprimer également.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Caractéristiques**.
4. Cochez la case du type de caractéristique à supprimer.
5. Cliquez sur le bouton **Supprimer**.

Rubriques d'aide

Caractéristiques - onglet Général :

L'onglet **Général** permet de désigner les détails du type de caractéristique.

Type Tapez le nom du type de caractéristique que vous souhaitez créer.

Description
Tapez la description du type de caractéristique que vous souhaitez créer.

Type de données
Dans la liste déroulante, sélectionnez le type de données du type de caractéristique que vous souhaitez créer.

CAR Sélectionnez ce type de zone pour indiquer le type de données du type de caractéristique sous forme de caractères.

CLOB Sélectionnez ce type de zone pour indiquer le type de données du type de caractéristique sous forme d'objet CLOB.

CLOB doit être utilisé pour les types de caractéristique comprenant un grand nombre de données.

Remarque : La définition du type de données sur CLOB peut avoir un impact négatif sur les performances. Utilisez VARCHAR (LVARCHAR for Informix) si possible afin de réduire l'impact éventuel sur les performances.

DATE Sélectionnez ce type de zone pour indiquer le type de données du type de caractéristique sous forme de date.

`Créer une règle DQM`
Si vous créez un nouveau type de caractéristique dont la valeur de type de données est DATE, il vous sera proposé de

créer une nouvelle règle DQM pour valider le nouveau type de caractéristique. Vous serez redirigé sur la page de création de règle DQM avec des valeurs pré-remplies en fonction du nouveau type de caractéristique.

VARCHAR
Sélectionnez ce type de zone pour indiquer le type de données du type de caractéristique sous forme de caractères variables.

Classe Dans la liste déroulante, sélectionnez la classe du type de caractéristique que vous souhaitez créer.

LC Sélectionnez ce type de zone pour désigner le type de caractéristique comme caractéristique physique.

Exemple : la taille ou le poids.

SC Sélectionnez ce type de zone pour désigner le type de caractéristique comme caractéristique système.

Exemple : une préférence de siège sur un vol ou le solde de points d'un membre de programme de fidélité.

Utilisation de la résolution
Dans la liste déroulante, indiquez si cette caractéristique doit servir à la résolution d'entité.

Aucun
Sélectionnez ce type de zone pour indiquer que la valeur de caractéristique ne servira pas à la résolution d'entité.

Concordance/discordance
Sélectionnez ce type de zone pour indiquer que la valeur de caractéristique servira à la résolution d'entité.

Candidats
Sélectionnez ce type de zone pour indiquer que la valeur de caractéristique servira à élaborer la liste de candidats et à augmenter le score d'un candidat.

Candidats/pas de score
Sélectionnez ce type de zone pour indiquer que la valeur de caractéristique servira à élaborer la liste de candidats, mais qu'elle n'augmentera pas le score d'un candidat.

Etat Dans la liste déroulante, sélectionnez **Actif** pour indiquer que cette caractéristique est active. Sinon, sélectionnez **Inactif**.

Conserver l'historique
Dans la liste déroulante, sélectionnez **Oui** pour consigner l'état historique de la valeur du type de caractéristique. A n'utiliser qu'avec les types de caractéristique dont la valeur ne change pas fréquemment. Sinon, sélectionnez **Non**.

Niveau d'affichage
Dans la liste déroulante, indiquez si cette caractéristique doit servir pour les graphiques et rapports.

Aucun
Sélectionnez ce type de zone pour exclure la valeur de ce type de caractéristique dans les graphiques et rapports.

Tous Sélectionnez ce type de zone pour inclure la valeur de ce type de caractéristique dans tous les graphiques et rapports.

Configuration de types de numéros

Vous pouvez configurer des types de numéros pour les données qui peuvent être classées comme numéros. Quand de nouvelles données sont ajoutées à une source de données et que vous souhaitez les classer comme numéro qui n'est pas encore configuré dans le système, vous devez créer un type de numéro pour ces nouvelles données.

Numéros

Les numéros sont des traits ou propriétés, définis par l'utilisateur, et associés à une identité qui peut se classer sous forme de numéro.

Types de numéros

Les types de numéros organisent et identifient les données de numéros qui sont stockées dans la base de données d'entités. Le numéro de téléphone et le numéro de sécurité sociale constituent des exemples de types de numéros par défaut préconfigurés dans la base de données d'entités.

Si vous possédez des données qui ne sont pas définies par l'un des types de numéros par défaut, vous devez créer un nouveau type de numéro pour ces données.

Exemple

Le groupe bancaire SBN possède des données qui incluent les numéros de compte chèque de la clientèle. Il souhaite ajouter ces nouvelles données à la base de données d'entités. Les données parviennent au noeud d'acquisition au moyen des balises UMF suivantes :

```
<number>
 <num_type>ca</num_type>
 <num_value>41510155060</num_value>
</number>
```

Dans cet exemple, vous devez configurer un nouveau type de numéro appelé ca.

Consultation des types de numéros

Les types de numéros servent aux données qui peuvent être classées comme numéros. Il est conseillé de consulter les types de numéros existants si vous comptez en ajouter un nouveau.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Numéros**.
4. Sélectionnez le type de numéro à consulter.

Création de types de numéros

Lorsque de nouvelles données sont ajoutées à un système source et que vous souhaitez les classer comme numéro dont le type n'est pas encore configuré, vous devez créer un nouveau type de numéro.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Numéros**.

4. Effectuez l'une des opérations suivantes :
   - Pour créer un nouveau type de numéro, cliquez sur le bouton **Nouveau**.
   - Pour créer un type de numéro basé sur un type de numéro existant, sélectionnez-en un dans la liste, puis cliquez sur le bouton **Cloner**.
5. Dans l'onglet **Général**, indiquez le type, la description, la classe, l'utilisation de la résolution, l'état, le paramètre d'historique, la pondération de concordance de lieu, la pondération de discordance de lieu et autres informations de configuration du type de numéro.
6. Dans l'onglet **Format**, indiquez la longueur minimale, la longueur maximale, le masque, le remplissage de masque, le caractère de remplissage, la longueur de hachage et autres informations de configuration du type de numéro.
7. Cliquez sur le bouton **Enregistrer**.

Suppression de types de numéros

Vous pouvez supprimer un type de numéro existant une fois que le système ne s'en sert plus.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Numéros**.
4. Sélectionnez un type de numéro dans la liste, puis cliquez sur le bouton **Supprimer**.

Rubriques d'aide

Numéros - onglet Général :

L'onglet **Général** permet de désigner les détails du type de numéro.

Type Tapez le nom du type de numéro que vous souhaitez créer.

Description
Tapez la description du type de numéro que vous souhaitez créer.

Classe Dans la liste déroulante, sélectionnez la classe du type de numéro que vous souhaitez créer.

CC Sélectionnez ce type de zone pour désigner le type de numéro comme carte de crédit.

MISC Sélectionnez ce type de zone pour désigner le type de numéro comme divers.

Exemple : un numéro d'abonné sur une compagnie aérienne.

AUTRE
Sélectionnez ce type de zone pour désigner le type de numéro comme autre.

Exemple : un numéro inconnu dans une source de données.

PHONE
Sélectionnez ce type de zone pour désigner le type de numéro comme numéro de téléphone.

PID Sélectionnez ce type de zone pour désigner le type de numéro comme numéro d'identification personnel.

Exemple : un numéro de permis de conduire ou de sécurité sociale.

SYSID

Sélectionnez ce type de zone pour désigner le type de numéro comme numéro d'identification système.

Exemple : une adresse IP.

Utilisation de la résolution

Dans la liste déroulante, indiquez si ce type de numéro doit servir à la résolution d'entité.

Aucun

Sélectionnez ce type de zone pour indiquer que la valeur de numéro ne servira pas à la résolution d'entité.

Candidats

Sélectionnez ce type de zone pour indiquer que la valeur de numéro servira à élaborer la liste de candidats et à augmenter le score d'un candidat.

Etat Dans la liste déroulante, sélectionnez **Actif** pour indiquer que ce numéro est actif. Sinon, sélectionnez **Inactif**.

Conserver l'historique

Dans la liste déroulante, sélectionnez **Oui** pour consigner l'état historique de la valeur du type de numéro. A n'utiliser qu'avec les types de numéro dont la valeur ne change pas fréquemment. Sinon, sélectionnez **Non**.

Niveau d'affichage

Dans la liste déroulante, indiquez si ce numéro doit servir pour les graphiques et rapports.

Aucun

Sélectionnez ce type de zone pour exclure la valeur de ce type de numéro dans les graphiques et rapports.

Tous Sélectionnez ce type de zone pour inclure la valeur de ce type de numéro dans tous les graphiques et rapports.

Configuration des données de nom

Les données de nom sont les données stockées dans le segment <NAME> d'un document UMF entrant. Au cours de la procédure de résolution des entités, les données de nom sont analysées, comparées aux données de nom d'entités existantes dans la base de données d'entités et associées à un score déterminé par le niveau de concordance des données de nom.

Hachage de nom optimisé avec IBM Global Name Recognition Name Hasher

La fonction Name Hasher utilise la technologie IBM Global Name Recognition pour améliorer le hachage de nom en créant des variantes de hachage pour chaque nom entrant. Les variantes de hachage de nom permettent à la procédure de résolution d'entité d'utiliser une concordance de nom partielle pendant l'analyse du nom et la définition du score.

Les scénarios suivants décrivent les avantages présentés par la fonction Name Hasher :

- Lorsque la concordance d'une grande partie des données ne peut être établie que sur le segment <NAME>
- Lorsque la concordance d'une grande partie des données ne peut être établie que sur le segment <NAME> et que les données ne sont pas conformes à la notation du prénom, du deuxième prénom et du nom de famille de culture anglo-saxonne.

L'utilisation de la fonction Name Hasher avec l'algorithme de calcul du score du gestionnaire de noms permet de classer les noms en fonction de la culture et de comparer et d'évaluer avec précision les noms de la liste de candidats dans un contexte culturel.

La fonction Name Hasher n'est pas activée par défaut. Vous pouvez utiliser la console de configuration pour activer la fonction Name Hasher et les fonctions DQM associées.

Avertissement : Contactez IBM Services ou le service de support IBM si vous mettez à niveau la fonction Name Hasher à partir des versions 8.0 ou 4.2 du produit et si vous activez Name Hasher pour la première fois. Dans les deux cas, sans l'assistance d'IBM Services ou du service de support technique d'IBM, la résolution d'entité échoue lors de la comparaison des nouvelles données aux données existantes de la base de données d'entités.

Activation de la fonction IBM Global Name Recognition Name Hasher :

L'activation de la fonction IBM Global Name Recognition Name Hasher pour le traitement de la qualité des données du segment UMF `<NAME>` peut améliorer l'analyse syntaxique des noms, la classification par culture et la génération du hachage de nom.

Avant de commencer

Si vous activez la fonction Name Hasher pour la première fois sur une installation existante, contactez IBM Services ou le service de support technique IBM. L'ensemble des données existantes de toutes les sources de données doivent être rechargées pour éviter l'échec de la résolution d'entité des nouvelles données avec les données existantes dans la base de données d'entités.

Pourquoi et quand exécuter cette tâche

Les instructions suivantes récapitulent les tâches à effectuer pour activer la fonction Name Hasher. Toutes les étapes sont effectuées à l'aide de la console de configuration. Cliquez sur le lien pour obtenir les instructions pas-à-pas de chaque tâche.

Procédure

1. Activez la fonction DQM 282 pour créer des hachages de nom. Cette fonction active la fonction Name Hasher au sein de pipelines. Si vous avez utilisé la fonction Name Hasher avant la version 8.0 Fix Pack 2, reportez-vous aux instructions de migration vers la fonction Name Hasher mise à niveau. Vous souhaitez peut-être réutiliser certains des paramètres utilisés par DQM 282.
2. Activez la fonction DQM 610 pour que le hachage de nom crée des attributs de hachage de nom composite.
3. Configurez le générateur de candidats par défaut avec nom uniquement pour le hachage de nom amélioré.
4. Configurez chaque source de données pour le hachage de nom amélioré.
5. Désactivez l'analyse syntaxique de nom complet dans la fonction DQM 252. La fonction Name Hasher crée des variantes de hachage de nom pour toutes les parties du nom, pas uniquement pour le nom complet.
6. Configurez la règle DQM 255 pour le hachage de nom amélioré. En effectuant cette tâche, vous conservez la fonction de normalisation des noms de DQM 255 mais vous désactivez le hachage de nom standard pour utiliser le hachage de

nom amélioré de la fonction Name Hasher. Vous devez également vous assurer que le contrôle de la validation du pipeline qui vérifie que la fonction DQM 255 est activée, n'échoue pas et n'arrête pas les pipelines.

7. Activez la fonction DQM 260 pour le segment UMF <NAME>. Cette fonction DQM affecte des cultures de noms à des données de nom entrantes. La fonction Name Hasher requiert l'option de culture de nom pour appliquer une expertise multiculturelle au hachage de nom amélioré. Assurez-vous que le gestionnaire de noms est activé. (En général, le gestionnaire de noms est activé.) Si vous activez la règle DQM 260 et que le gestionnaire de noms n'est pas activé, la règle DQM 260 échoue et les pipelines s'arrêtent.
8. Définissez les paramètres système de la fonction Name Hasher. En effectuant cette opération, vous configurez les paramètres système nécessaires pour les pipelines utilisés lors du hachage de nom amélioré.

Configuration des paramètres système pour le hachage de nom amélioré :

Pour permettre à la fonction Name Hasher de s'exécuter correctement lors de la résolution d'entité, la valeur par défaut du paramètre système MM HASHLESS_NAMES_ARE_GENERIC doit être désactivée. En désactivant cette valeur, la fonction Name Hasher s'applique à toutes les données de nom entrantes.

Désactivation de l'analyse syntaxique du nom complet pour le hachage de nom amélioré :

Pour permettre à la fonction Name Hasher de fonctionner correctement, vous devez désactiver la règle DQM 252 existante sur le segment <NAME>.

Configuration de la règle DQM 255 pour la fonction IBM Global Name Recognition Name Hasher :

Pour permettre à Name Hasher de fonctionner correctement, vous devez configurer la valeur du paramètre **Exclusion UMF** dans la fonction DQM 255.

Pourquoi et quand exécuter cette tâche

- Désactivez la fonctionnalité d'analyse et de hachage de nom standard de la règle DQM 255 en faveur de l'analyse et du hachage étendus fournis par le hachage de nom
- Vérifiez que la règle DQM 255 est activée, pour satisfaire le contrôle de validation du pipeline qui nécessite que la règle DQM 255 soit activée

Configuration des générateurs de candidats pour le hachage de nom amélioré :

Pour permettre à Name Hasher de fonctionner correctement, vérifiez que la configuration du générateur de candidats **Par défaut avec nom uniquement** contient un type de concordance **Caractéristique**.

Configuration des sources de données pour le hachage de nom amélioré :

Si vous utilisez la fonction de hachage de nom amélioré, vous devez configurer chaque source de données pour permettre la génération d'une liste de candidats d'attributs de nom en définissant la configuration du générateur de candidat **Par défaut avec nom uniquement**.

Création des attributs de hachage de nom composite :

La fonction DQM 610 génère des attributs à partir de différentes valeurs plus petites incluses dans le document UMF entrant. Name Hasher utilise la fonction DQM 610 pour créer des hachages de noms composites et les stocker sous forme d'attributs dans des segments UMF <NAME> et <ATTRIBUTE>.

Pourquoi et quand exécuter cette tâche

Les attributs de hachage de nom composite obtenus incluent toujours <ATTR_TYPE> de GNR_HASH. En créant ces attributs de hachage de nom, la résolution d'entité peut utiliser la concordance de nom partielle lors de l'analyse du nom et du calcul du score. La fonction de concordance de nom partielle étend la plage d'entrées d'identité et d'entité concordantes possibles.

Migration d'une version mise à niveau d'IBM Global Name Recognition Name Hasher :

Si votre produit utilisait la fonction Name Hasher avant la version 8.0 Fix Pack 2, effectuez les opérations ci-dessous en plus des tâches standard nécessaires pour passer à la dernière version de la fonction Name Hasher.

Procédure

1. Effectuez une mise à niveau standard du produit à l'aide du programme d'installation.
2. Dans la console de configuration, désactivez la fonction DQM 660 pour le segment UMF `<NAME>`. Copiez ou notez les valeurs en cours des paramètres **`maxVariants`** et **`variantScoreThreshold`** inclus avec le paramètre HTTP URL. Avant la version 8.0 Fix Pack 2, la fonction de hachage de nom amélioré utilisait un servlet Name Hasher qui s'exécutait sur un serveur d'applications Web. Dans la version 8.0 Fix Pack 2 et suivante, la fonction Name Hasher est intégrée au pipeline. En désactivant la fonction DQM 660 du segment `<NAME>`, vous désactivez le servlet Name Hasher existant.
3. Dans la console de configuration, activez la règle DQM 282 (variantes de hachage de nom) sur le segment `<NAME>` UMF et collez ou configurez manuellement les valeurs de paramètre de fonction suivantes :

   `maxVariants`
   Associez ce paramètre à la valeur déjà utilisée avec le paramètre **`maxVariants`** de la fonction DQM 660.

   `variantScoreThreshold`
   Associez ce paramètre à la valeur déjà utilisée avec le paramètre **`variantScoreThreshold`** de la fonction DQM 660.

   Remarque : Si la fonction DQM 660 ne contient pas de valeurs pour ces paramètres dans l'adresse URL, utilisez les valeurs par défaut de la fonction DQM 282.
   En effectuant cette opération, vous activez la fonction Name Hasher dans le pipeline.
4. Dans la console de configuration, configurez les paramètres système de la fonction Name Hasher. En effectuant cette opération, vous configurez globalement les paramètres que le pipeline utilise dans la fonction Name Hasher.

Analyse de nom secondaire

La création d'analyses secondaires pour un nom complet entrant améliore la fiabilité du score d'un nom et les fonctions de concordance lors de la résolution d'entités.

L'analyse syntaxique et la décomposition des noms en est l'une des premières étapes de la procédure de concordance de noms. Des analyses de noms secondaires correspondent à des variantes possibles du nom. En générant des analyses de noms secondaires pour des données de nom entrantes, vous augmentez la fiabilité de l'analyse et du score du nom entrant.

Utilisez la fonction DQM 289 pour générer des analyses de noms secondaires. Par défaut, cette fonction n'est pas activée. Pour générer des analyses de noms secondaires, vous devez configurer la fonction DQM 289 sur le segment <NAME> dans la console de configuration.

Il est possible qu'il n'y ait pas d'analyse secondaire pour certains noms. Si une analyse secondaire existe pour le nom et que celle-ci est différente de l'analyse de nom principale, la fonction DQM génère un second segment <NAME> incluant l'analyse secondaire.

Par exemple, examinons les données de nom entrantes suivantes :

```
<UMF_ENTITY>
 <NAME>
  <NAME_TYPE>M</NAME_TYPE>
  <FULL_NAME>ALLEN CRAIG</FULL_NAME>
 </NAME>
....
</UMF_ENTITY>
```

Dans cet exemple, le nom complet peut avoir au moins deux analyses syntaxiques différentes. "Allen" et "Craig" peuvent être à la fois des prénoms et des noms de famille. En générant des analyses secondaires de ce nom, le processus de résolution d'entité peut analyser et évaluer le nom en se référant à une plus grand nombre d'entités dans la base de données d'entités.

Si la fonction DQM 289 est configurée sur la balise UMF <FULL_NAME> du segment<NAME>, une analyse de nom secondaire est créée et ajoutée à l'enregistrement UMF lors du traitement du nom. L'enregistrement obtenu s'apparente à l'enregistrement suivant :

```
<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>
```

Le premier segment <NAME> contient l'analyse du nom principale et la valeur <NAME_TYPE> d'origine. Le second segment <NAME> contient l'analyse secondaire générée, indiquée par la valeur <NAME_TYPE> ALT. (Cet exemple suppose que le type de nom de l'analyse secondaire correspond à la valeur par défaut.)

Configuration des noms pour créer des analyses syntaxiques de noms secondaires :

Vous pouvez configurer des noms pour créer des analyses syntaxiques de noms secondaires, qui peuvent être utilisées pour générer plusieurs hachages de noms. Si vous utilisez la fonction IBM Global Name Recognition Name Hasher, la création d'analyses syntaxiques de noms secondaires peut améliorer les fonctions de concordance partielle de noms pour faciliter la résolution d'entité des données de noms.

Avant de commencer

- Vérifiez que le gestionnaire de noms est activé et que le chemin des fichiers de support est défini dans les paramètres système. Si vous activez cette fonction DQM sans indiquer les fichiers de support du gestionnaire de noms, le pipeline consigne une erreur et s'arrête.
- Lorsque vous activez la fonction DQM pour bénéficier de l'analyse syntaxique des noms secondaires, vous modifiez la configuration système. Comme pour toute modification de configuration, veillez à arrêter les pipelines actifs avant de changer la configuration. Redémarrez les pipelines pour les réinitialiser avec les modifications de configuration.

Pourquoi et quand exécuter cette tâche

- Pour les nouvelles installations de la version 8.0 Fix Pack 2 ou suivante, cette fonction DQM est déjà configurée et active.
- Pour les versions mises à niveau à partir de la version 8.0 Fix Pack 2 ou suivante, cette fonction DMQ est configurée mais est inactive. Pour utiliser des analyses de noms secondaires, faites passer la fonction DQM existante à l'état **Actif**.

Procédure

1. Dans la console de configuration, sélectionnez **Configurer** > **UMF** > **Règles DQM**.
2. Sélectionnez `NAME` dans la liste **Segment**.
3. Sélectionnez le nom de la balise UMF indiquant **289 - Alternate Name Parsing** dans la section **Function**.
4. Dans la zone **Statut**, vérifiez que l'option `Actif` est sélectionnée.
5. Dans l'onglet **Paramètres**, vérifiez ou définissez les valeurs de paramètre suivantes :
   - **Parse Score Threshold** : Indiquez une valeur comprise entre 0 et 100. Plus le score est élevé, plus le nombre d'analyses syntaxiques secondaires créées est faible. Cette valeur définit le seuil de score de fiabilité minimal que l'analyseur syntaxique de noms va utiliser pour déterminer si une analyse syntaxique secondaire doit être créée pour le nom entrant. Si aucune analyse secondaire ayant un score de fiabilité supérieur n'est trouvée, ou si l'analyse entrante initialement fournie a déjà un score supérieur au seuil, alors aucune analyse secondaire n'est créée.
   - **Alternate Name Type**: Entrez la valeur de `NAME_TYPE` pour indiquer que ce nom est une analyse syntaxique secondaire. Cette valeur est la balise UMF ajoutée au segment `<NAME>` pour chaque analyse syntaxique de nom secondaire créée. Par défaut, la valeur correspond à `ALT`. Pour garantir l'attribution complète de la résolution d'entité, associez pas cette valeur à une entrée `NAME_TYPE` entrante existante dans la console de configuration. N'associez pas cette valeur à **`M`** ou **`A`**.

6. Cliquez sur **Enregistrer**.

Détermination du sexe

Lorsque vous traitez les données de nom entrantes, le sexe associé au nom d'une personne peut être un facteur déterminant pour établir la concordance de deux entités. Le sexe ajoute un poids de concordance ou de discordance au score si deux identités correspondent à la même entité.

La fonction DQM 258 identifie de manière dynamique le sexe du segment <NAME> dans un enregistrement UMF entrant, crée une caractéristique de sexe et ajoute la caractéristique de sexe à l'enregistrement UMF entrant. La caractéristique de sexe est ajoutée à l'aide du segment <ATTRIBUTE>.

- Si l'enregistrement UMF entrant contient déjà une caractéristique de sexe dans ses données, la fonction DMQ 258 n'en génère pas d'autre.
- Si l'enregistrement UMF contient plusieurs segments <NAME>, la fonction DQM 258 crée une seule caractéristique de sexe pour l'ensemble de l'enregistrement d'entrée. Dans ce cas, la génération de plusieurs attributs de sexe peut créer des entrées redondantes ou conflictuelles.

Pour déterminer le sexe d'un nom de manière dynamique, vérifiez qu'au moins une balise UMF du segment <NAME> est configurée pour utiliser la fonction DQM 258.

- Pour les nouvelles installations de la version 8.0 Fix Pack 2 ou suivante, cette fonction DQM est déjà configurée et active.
- Pour les versions mises à niveau à partir de la version 8.0 Fix Pack 2 ou suivante, cette fonction DMQ est configurée mais est inactive. Si vous souhaitez utiliser cette fonction de sexe améliorée, vous devez la faire passer à l'état **Actif**. Si vous avez déjà affecté un sexe à l'aide du paramètre **Caractéristique de genre** de la fonction DQM 255, redéfinissez la valeur de ce paramètre en indiquant NONE. Vous pouvez continuer à utiliser DQM 255 avec toutes les balises UMF <NAME> pour normaliser les noms.

Vous pouvez également être amené à vérifier les configurations suivantes dans la console de configuration :

- Vérifiez que la caractéristique de sexe est configurée en tant que concordance ou discordance dans la résolution d'entité par source de données. Vous pouvez afficher ou configurer ce paramètre dans la zone **Utilisation de la résolution** disponible en sélectionnant **Configurer** > **Sources** > **Caractéristiques**.
- Vérifiez que la caractéristique est configurée avec les valeurs d'ajustement appropriées pour la résolution d'entité. Vous pouvez afficher ou configurer ce paramètre en sélectionnant **Configurer** > **Résolution** > **Caractéristiques**. Vérifiez les valeurs du poids de concordance ou de discordance affectées à la caractéristique de sexe pour vous assurer qu'elles répondent aux besoins de l'entreprise.

.

Examinez l'exemple de segment <NAME> suivant dans l'enregistrement UMF entrant :

```
<UMF_ENTITY>
 <NAME>
  <NAME_TYPE>M</NAME_TYPE>
  <LAST_NAME>RASUL</LAST_NAME>
```

```
  <FIRST_NAME>KARIM</FIRST_NAME>
 </NAME>
.....
</UMF_ENTITY>
```

Si DQM 258 est activé pour la balise UMF <FIRST_NAME> du segment <NAME>, l'enregistrement UMF entrant s'apparente à l'enregistrement suivant après l'analyse et la création du sexe :

```
<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>
```

Configuration des noms pour affecter un sexe :

Vous pouvez améliorer la résolution d'entité en affectant un sexe en fonction du nom. Vous pouvez définir des scores de concordance et de discordance en déterminant si les entités comparées sont de même sexe. Vous pouvez configurer des noms pour affecter un sexe de manière dynamique et ajouter la caractéristique Sexe aux enregistrements UMF entrants.

Avant de commencer

- Vérifiez que le gestionnaire de noms est activé et que le chemin des fichiers de support du gestionnaire de noms est défini dans les paramètres système. Si vous activez cette fonction DQM sans indiquer les fichiers de support du gestionnaire de noms, le pipeline consigne une erreur et s'arrête.
- Lorsque vous activez la fonction de sexe de cette fonction DQM, vous modifiez la configuration système. Comme pour toute modification de configuration, veillez à arrêter les pipelines actifs avant de changer la configuration. Redémarrez les pipelines pour les réinitialiser avec les modifications de configuration.

Pourquoi et quand exécuter cette tâche

- Pour les nouvelles installations de la version 8.0 Fix Pack 2 ou suivante, cette fonction DQM est déjà configurée et active.
- Pour les versions mises à niveau à partir de la version 8.0 Fix Pack 2 ou suivante, cette fonction DMQ est configurée mais est inactive. Pour utiliser cette fonction de sexe améliorée, faites passer la fonction DQM existante à l'état **Actif**. Si vous avez déjà affecté un sexe à l'aide du paramètre **Caractéristique de genre** de la fonction DQM 255, redéfinissez la valeur de ce paramètre en indiquant NONE. Vous pouvez continuer à utiliser DQM 255 avec toutes les balises UMF <NAME> pour normaliser les noms.

Procédure

1. Dans la console de configuration, sélectionnez **Configurer** > **UMF** > **Règles DQM**.
2. Sélectionnez **NAME** dans la liste **Segment**.
3. Sélectionnez le nom de balise UMF **FIRST_NAME** qui répertorie également **258 - Name Genderizer** comme **Fonction**. Cette configuration évalue uniquement le

prénom dans l'enregistrement entrant pour les noms de personne. Si la fonction de classement des noms du gestionnaire de noms est activée, vous devez indiquer l'ensemble du nom dans la balise UMF LAST_NAME du segment NAME.

4. Dans la zone **Statut**, vérifiez que l'option **Actif** est sélectionnée.
5. Dans la zone **Filtre de règle**, vérifiez que la valeur NAME_TYPE=M a été indiquée. Cette valeur permet de s'assurer que seul le nom principal de chaque enregistrement d'entrée est évalué pour affecter le sexe.
6. Dans l'onglet **Paramètres**, vérifiez que la valeur de l'option **Niveau de fiabilité de genre minimum** est comprise entre 0 et 100. Le score par défaut est 90, ce qui signifie que ce sexe n'est pas affecté sauf s'il y a un niveau de confiance de 90 % pour l'affectation de sexe. Réduisez ce score avec précaution car un score minimum inférieur à 90 peut avoir une incidence sur la résolution d'entité lors de la concordance ou la discordance du sexe.
7. Cliquez sur **Enregistrer**.

Classement des noms

Si le paramètre système **NAMESIFTER** du gestionnaire de noms est activé, le produit classe les noms par type. En classant les noms par type, la résolution d'entité peut appliquer les ressources linguistiques et les données de référence appropriées lors de l'analyse, du calcul du score et de la concordance du nom :

Les noms sont classés par nom de personne ou nom de société.

Noms de personne
: Un nom de personne ne contient pas d'indicateurs suggérant qu'il appartient à une autre catégorie. (Par exemple : "Linda K. Smith".) Les noms classés en tant que noms de personne sont soumis à une analyse syntaxique et décomposés. Les parties du nom décomposé sont classées par culture pour renforcer la précision du processus d'analyse et de définition du score.

Noms de société
: Un nom de société ou d'organisation contient un type d'indicateur signalant qu'il ne s'agit pas d'un nom de personne. (Par exemple, "Smith & Company".) Les noms classés en tant que noms de société sont automatiquement associés à la culture "Société".

Noms inconnus
: Un nom classé comme "Inconnu" contient un élément qui peut être mal orthographié ou une structure qui n'apparaît pas habituellement dans des noms de personne ou de société. (Par exemple "SMI".)

Classement des noms par type :

L'un des paramètres système de Name Manager (**NAMESIFTER**) permet de classer les noms par type. Les types de nom les plus courants sont les noms de personne et les noms de société. Le classement des noms peut apporter plus de précision à l'analyse de noms et au calcul du score de la procédure de résolution d'entité.

Classement des noms de personne par culture :

La fonction DQM 260 a été créée pour déterminer la culture du nom et ajouter cette valeur au segment UMF <NAME>. Par défaut, la configuration du segment <NAME> comprend une règle DQM 260 appliquée à la balise UMF <LAST_NAME> . Utilisez les instructions suivantes pour ajouter la règle DQM 260 à une autre balise UMF dans le segment <NAME> ou mettre à jour la règle existante sur la balise UMF<LAST_NAME>.

Présentation du gestionnaire de noms

Gestionnaire de noms

Le gestionnaire de noms améliore la précision de reconnaissance des noms afin de résoudre des problèmes complexes tels que les translittérations multiples, erreurs typographiques intraculturelles, variantes orthographiques intra et interculturelles, ainsi que les noms contenant des désignations patronymiques ou honorifiques. Il utilise les bibliothèques du composant IBM InfoSphere Global Name Recognition, qui contiennent une base de connaissances de plus de 1000000000 noms multiculturels et des informations linguistiques uniques pour ajouter des fonctions de concordance de noms en fonction d'une culture spécifique.

Le gestionnaire de noms calcule le score des noms en utilisant la procédure suivante :

- Classement des noms par type (personne ou société)
- Analyse syntaxique et décomposition des noms de personne en différentes parties
- Classement des noms par culture (prise en charge de plus de 20 cultures, notamment la culture afghane, arabe, farsi, han, japonaise, coréenne, thaïlandaise, vietnamienne et yoruban)
- Normalise les noms de personne (si le nom est classé en tant que culture anglo-saxonne, arabe, chinoise, française, allemande, hispanique, indienne, coréenne, russe ou thaïlandaise).

Configuration du gestionnaire de noms

Par défaut, le calcul du score du gestionnaire de noms est déjà activé et configuré lorsque vous installez IBM InfoSphere Identity Insight. Toutefois, vous pouvez utiliser la console de configuration pour vérifier ou modifier les paramètres de configuration du gestionnaire de noms, notamment les paramètres suivants :

- Les paramètres système du gestionnaire de noms, notamment le chemin de support des bibliothèques du composant du gestionnaire de noms (paramètres globaux que le pipeline utilise pour effectuer une résolution d'entités)
- Les seuils du score de nom du gestionnaire de noms utilisé lors la recherche de concordance de noms (concordance et discordance)

Configuration des paramètres système du gestionnaire de noms :

Par défaut, les paramètres système utilisés pour calculer le score des noms du gestionnaire de noms sont configurés lors de l'installation du produit. Toutefois, vous pouvez les mettre à jour, si nécessaire. Par exemple, vous pouvez être amené à modifier l'emplacement des bibliothèques de support du gestionnaire de noms.

Pourquoi et quand exécuter cette tâche

Vous pouvez définir le chemin des bibliothèques de support du gestionnaire de noms et activer le classement des noms par type à l'aide des paramètres système du gestionnaire de noms. Vous pouvez également définir le paramètre système **CROSSCHECKCULTURE** pour configurer le traitement des noms entre différentes cultures de noms.

Procédure

1. Dans la console de configuration, sélectionnez **Configurer** > **Général** > **Paramètres système**.

2. Dans la liste **Groupe de paramètres**, sélectionnez le groupe de paramètres **NAMEMANAGER**.
3. Dans la sous-fenêtre gauche, sélectionnez le paramètre système du gestionnaire de noms à configurer :

Paramètres système du gestionnaire de noms	Description
SUPPORTPATH	Indique l'emplacement des fichiers de support du gestionnaire de noms. La valeur par défaut est ./data, à savoir le chemin relatif du répertoire principal du produit. Si les fichiers de support sont déplacés dans un autre emplacement lors de l'installation, modifiez cette valeur en indiquant le chemin absolu du nouvel emplacement.
NAMESIFTER	Indique si la fonction de classement par type de nom (noms de personne ou de société) est activée. Pour activer le classement des noms par type (fonction Name Sifter), entrez `1` (valeur par défaut de la nouvelle installation) dans la zone **Valeur courante** Pour désactiver le classement des noms par type (fonction Name Sifter), entrez `0` (valeur par défaut de la mise à niveau) dans la zone **Valeur courante**
CROSSCHECKCULTURE	Indique si vous souhaitez effectuer le calcul du score entre des cultures de noms à l'aide du gestionnaire de noms lorsque les cultures de noms sont différentes. Pour vérifier uniquement la culture du nom entrant avant d'évaluer le score des deux noms, entrez `0` dans la zone **Valeur courante**. Pour vérifier les valeurs de culture de nom avant de calculer le score (valeur de la nouvelle installation), entrez `1` dans la zone **Valeur courante**.

Avertissement : Le paramètre système **CROSSCHECKCULTURE** détermine comment la résolution d'entité traite l'évaluation des noms par culture dans les pipelines. Avant de modifier la valeur en cours du paramètre système, adressez-vous à IBM Services ou au service de support IBM.

4. Cliquez sur **Enregistrer**.

Configuration du seuil de concordance et de discordance du gestionnaire de noms :

Vous pouvez définir les seuils de score des noms que le gestionnaire de noms utilisent lors de la résolution d'entité par règle de résolution. Une fois que la liste de candidats est générée, la résolution d'entité compare à ces seuils le score du nom du gestionnaire de noms en fonction des parties du nom et de la culture

déterminée pour chaque partie. Si le score du gestionnaire de noms est supérieur ou égal au seuil configuré pour la partie du nom, les noms sont considérés comme concordants.

Pourquoi et quand exécuter cette tâche

Important : Par défaut, les seuils de calcul du score des parties d'un nom du gestionnaire de noms sont configurés pour des résultats et des performances optimales. La modification des valeurs par défaut est une tâche de configuration avancée car ces valeurs peuvent avoir un effet négatif sur la résolution d'entité pour les règles incluant un calcul du score des noms. Avant de modifier les valeurs par défaut, adressez-vous à IBM Services ou au service de support IBM.

Procédure

1. Dans la console de configuration, sélectionnez **Configurer** > **Résolution** > **Règles de résolution**
2. Sélectionnez la configuration de la résolution dans la liste **Configurations de résolution**.
3. Sélectionnez la règle de résolution.
4. Cliquez sur **Seuils de concordance/discordance**.
5. Dans le **Gestionnaire de noms**, entrez le score minimum pour chaque seuil de partie de nom, basé sur un score compris entre 0.0 et 1.0. Plus le score est élevé, plus les parties du nom doivent être exactes pour être considérées comme concordantes. En général, un score inférieur à 0,7 ne permet pas d'établir de concordance pour les parties du nom.

calcul du score d'un nom à l'aide du gestionnaire de noms :

L'algorithme du gestionnaire de noms calcule le score des données de nom entrantes en décomposant le nom en différentes parties, puis en déterminant la culture de chaque partie. Il calcule ensuite le score de chaque partie et les scores obtenus sont utilisés lors de la résolution d'entités.

L'algorithme du gestionnaire de noms fonctionne indépendamment des algorithmes du composant Name Comparator mais vous devez quand même sélectionner NC1 ou NC2. Pendant le processus de résolution d'entité, le score des noms est tout d'abord calculé selon les algorithmes de comparateur de nom sélectionné. Si le score indique une concordance parfaite, la procédure de résolution d'entité ignore le calcul du score effectué par le gestionnaire de noms car la concordance parfaite du nom respecte la partie régissant le score dans la règle de résolution. En revanche, s'il n'y a pas de concordance parfaite pour le nom entrant, la procédure de résolution d'entité calcule le score à l'aide de l'algorithme du gestionnaire de noms.

L'algorithme analyse et décompose le nom en différentes parties (prénom, nom et nom complet), puis détermine la culture pour chaque partie du nom. L'algorithme affecte un score à chaque partie du nom et compare ces scores aux seuils configurés dans le gestionnaire de noms pour déterminer le niveau de concordance des noms. Plus le seuil du score défini est élevé, plus les parties du nom provenant des données de nom entrantes doivent être proches des parties du nom de l'entité existante dans la base de données d'entités.

Sélection des cultures pour le calcul du score des noms de la fonction Name Manager :

Vous pouvez configurer les méthodes de calcul du score des noms utilisées par culture pendant la procédure de calcul du score de la résolution d'entité. Le gestionnaire de noms peut uniquement déterminer la culture de nom et calculer le score des noms pour les cultures configurées pour utiliser la concordance de noms du gestionnaire de noms.

Pourquoi et quand exécuter cette tâche

Par défaut, chaque culture prise en charge est déjà configurée en fonction des meilleures pratiques pour le calcul du score de noms standard. La modification des valeurs par défaut est une tâche avancée qui peut avoir un effet négatif sur la résolution d'entité pour les règles incluant un calcul du score des noms. Adressez-vous à IBM Services ou au service de support technique avant de modifier les valeurs de configuration par défaut.

Procédure

1. Dans la console de configuration, sélectionnez **Configurer** > **Résolution** > **Correspondance du gestionnaire de noms**.
2. Sélectionnez une culture de la fonction Name Manager.
3. Dans la section **Utiliser la correspondance de noms de Name Manager**, sélectionnez `Oui`
4. Cliquez sur **Enregistrer**.

Configuration de règles DQM

Vous pouvez configurer des règles DQM chargées de réparer ou nettoyer les données qui ne satisfont pas aux normes de qualité minimum. Les règles DQM sont appliquées à une balise UMF précise, dans un segment UMF précis.

Pourquoi et quand exécuter cette tâche

Les règles de résolution peuvent être visualisées et modifiées à l'aide de la console, dans l'onglet **Règles DQM**.

règles DQM

Les règles sont des fonctions configurées de réparation, nettoyage et standardisation, définies par le système, appliquées aux valeurs de données d'identité entrantes, dans un ordre précis.

Les règles DQM, qui définissent comment le système traite les données entrantes, sont conçues pour formater convenablement les numéros, repérer et corriger les coquilles ou erreurs de transposition, ainsi que repérer et rectifier les inexactitudes délibérées introduites par les personnes soucieuses de dissimuler leur identité. Elles peuvent accomplir toute une palette d'opérations de réparation, nettoyage et standardisation sur les valeurs de données d'identité entrantes.

Pour configurer une règle DQM, il faut d'abord sélectionner un segment UMF (par exemple NAME) et une balise UMF particuliers (par exemple NAME_TYPE), puis la fonction DQM, définie par le système, à appliquer aux données entrantes, et enfin désigner les paramètres associés à cette fonction, dont les éventuelles valeurs par défaut que le système doit appliquer. Etant donné que le produit permet de désigner plusieurs règles pour chaque segment UMF sélectionné, il faut également choisir l'ordre dans lequel les appliquer.

Consultation des règles DQM

Les règles DQM réparent ou nettoient les données qui ne satisfont pas aux normes de qualité minimum.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Règles DQM**.
4. Dans la liste déroulante **Segment**, sélectionnez le segment UMF qui contient les règles DQM à consulter.

Création de règles DQM

Vous pouvez créer des règles DQM chargées de réparer ou nettoyer les données qui ne satisfont pas aux normes de qualité minimum.

Pourquoi et quand exécuter cette tâche

Les règles DQM sont appliquées à une balise UMF précise, dans un segment UMF précis. Il est également possible de cloner des règles DQM comme base d'une nouvelle règle.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Règles DQM**.
4. Dans la liste déroulante **Segment**, sélectionnez le segment UMF pour lequel créer une règle DQM.
5. Effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle règle DQM, cliquez sur le bouton **Nouveau**.
   - Pour créer une règle DQM basée sur une règle DQM existante, sélectionnez-en une dans la liste, puis cliquez sur le bouton **Cloner**.
6. Dans l'onglet **Général**, indiquez le nom de balise UMF d'ordre, la fonction, la règle de filtrage, l'exclusion UMF, la valeur corrigible, l'état et autres informations de configuration sur la règle DQM.
7. Dans l'onglet **Paramètres**, désignez les paramètres de la règle DQM.
8. Cliquez sur le bouton **Enregistrer**.
9. Validez la règle DQM.

Suppression de règles DQM

Une fois qu'une règle DQM n'est plus nécessaire, il convient de l'effacer.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Règles DQM**.
4. Dans la liste déroulante **Segment**, sélectionnez le segment UMF pour lequel supprimer une règle DQM.
5. Cochez les cases des règles DQM à supprimer.
6. Cliquez sur le bouton **Supprimer**.

Validation de règles DQM

Quand vous ajoutez ou modifiez une règle DQM, il convient de la valider avant de l'appliquer aux données source.

Pourquoi et quand exécuter cette tâche

La fonction de validation sert à valider toutes les règles, les unes par rapport aux autres, d'un segment entier. La validation qui peut être effectuée sur une règle individuelle est automatiquement effectuée lorsque vous enregistrez la règle.

Quand vous vous connectez à la console de configuration, une vérification de validation automatique a lieu afin de savoir si les règles DQM sont valides. Si une erreur est décelée, un message d'en-tête s'affiche en haut de l'écran de la console de configuration. Cliquez sur le lien **Corriger les erreurs** pour ouvrir une nouvelle fenêtre décrivant les erreurs.

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Règles DQM**.
4. Dans la liste déroulante **Segment**, sélectionnez le segment UMF pour lequel valider une règle DQM. Si aucun segment n'est sélectionné, la validation s'applique à tous les segments.
5. Cliquez sur le bouton **Valider**.

Désactivation des règles DQM

Vous pouvez désactiver une règle DQM devenu superflue.

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Règles DQM**.
4. Dans la liste déroulante **Segment**, sélectionnez le segment UMF qui contient la règle DQM à désactiver.
5. Cliquez sur la règle DQM à désactiver.
6. Dans l'onglet **Général**, définissez la zone d'état sur **Inactif**.
7. Cliquez sur le bouton **Enregistrer**.

Rubriques d'aide

Règles DQM - onglet Général :

L'onglet **Général** permet d'indiquer les détails de la règle DQM.

Segment
Tapez le nom du segment UMF où appliquer la règle DQM. Cette zone est généralement en lecture seule. Le seul moment où il est possible de la modifier est lorsque la liste déroulante **Segment** a été laissée vide à la création d'une nouvelle règle DQM. Le nom des segments doit être saisi en majuscules.

Ordre Tapez le numéro d'ordre dans lequel la règle DQM sera appliquée.

Nom de balise UMF
Tapez le nom de la balise UMF où appliquer la règle DQM. Le nom des balises UMF doit être saisi en majuscules.

Fonction
Dans la liste déroulante, sélectionnez la fonction DQM sur laquelle vous souhaitez baser la régle DQM.

Description de la fonction
La zone de description de fonction est une zone en lecture seule qui décrit l'effet de la règle DQM.

Filtre de règle
Si vous souhaitez que la règle DQM ne s'applique que si la balise UMF contient une valeur particulière, saisissez une équation qui inclue le nom de balise UMF et la valeur nécessaire à l'exécution de la règle DQM.

Exemple : `NAME_TYPE=m`
Cet exemple de paramètre n'applique la règle DQM que si la valeur de la balise UMF `NAME_TYPE` est `m`.

Exclure UMF
Si vous souhaitez que la règle DQM ne s'applique pas à certains documents d'entrée UMF, saisissez dans une liste délimitée par des virgules les documents d'entrée UMF pour lesquels cette règle ne doit pas s'exécuter.

Exemple : `UMF_QUERY, UMF_DISCLOSED RELATION`
Cet exemple de paramètre n'applique la règle DQM aux documents d'entrée UMF ni `UMF_QUERY` ni `UMF_DISCLOSED_RELATION`.

Corrigible
Dans la liste déroulante, sélectionnez **Oui** pour ajuster les valeurs non valides et insuffisantes. Sinon, sélectionnez **Non**.

Les paramètres de chaque règle DQM déterminent le mode de correction des valeurs de données insuffisantes.

Etat Dans la liste déroulante, sélectionnez **Actif** pour indiquer que cette règle DQM est active. Sinon, sélectionnez **Inactif**.

Configuration des codes de recherche

Les codes de recherche sont des valeurs par défaut utilisées par diverses fonction de l'application.

Les codes de recherche sont classés par types. La règle DQM 190 peut servir soit à confirmer que des codes de recherche entrants relèvent d'un type de code défini, soit, facultativement, à les ajouter au type de code concerné s'ils en sont absents.

Consultation des codes de consultation

Les codes de recherche sont des valeurs par défaut utilisées par diverses fonction de l'application.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Codes**.
4. Dans la liste déroulante **Type**, sélectionnez le type de valeurs de code de recherche à consulter.

Création de codes de recherche

Les codes de recherche sont des valeurs par défaut utilisées par diverses fonction de l'application.

Pourquoi et quand exécuter cette tâche

Vous pouvez soit créer un nouveau code de recherche, soit en créer un basé sur un code de recherche existant.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Codes**.
4. Dans la liste déroulante **Type**, sélectionnez le type de valeurs de code de recherche à créer. Pour créer un type de code entièrement nouveau, laissez la valeur telle quelle.
5. Effectuez l'une des opérations suivantes :
   - Pour créer un nouveau code de recherche, cliquez sur le bouton **Nouveau**.
   - Pour créer un code de recherche basé sur un code de recherche existant, sélectionnez-en un dans la liste, puis cliquez sur le bouton **Cloner**.
6. Dans l'onglet **Général**, indiquez le type (cette zone sera en lecture seule si elle a déjà été indiquée dans la liste déroulante **Type**), le code, la description, l'état et autres informations de configuration de ce code de recherche.

Suppression de codes de recherche

Vous pouvez supprimer les codes de recherche, créés par des utilisateurs, dont le système ne se sert plus.

Pourquoi et quand exécuter cette tâche

Veillez à ne supprimer aucun code de recherche par défaut du système car ils sont indispensables à divers composants du produit.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Codes**.
4. Dans la liste déroulante **Type**, sélectionnez le type de valeurs de code de recherche à supprimer.
5. Sélectionnez un code de recherche dans la liste, puis cliquez sur le bouton **Supprimer**.

Désactivation de codes de recherche

Vous pouvez désactiver un code de recherche devenu superflu.

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Codes**.
4. Dans la liste déroulante **Type**, sélectionnez le type de valeurs de code de recherche à désactiver.

5. Sélectionnez un code de recherche dans la liste.
6. Dans l'onglet **Général**, définissez la zone d'état sur **Inactif**.
7. Cliquez sur le bouton **Enregistrer**.

Rubriques d'aide

Codes de recherche - onglet Général :

L'onglet **Général** permet d'indiquer les détails du code de recherche.

Type Tapez le type de code de recherche dans lequel regrouper le code de recherche. Une fois renseignée, cette zone sera en lecture seule. Elle ne peut être modifiée que si la liste déroulante **Type** est restée non spécifiée lors de la création d'un nouveau code de recherche.

Code Tapez la valeur qui doit être disponible comme valeur par défaut du code de recherche. Il s'agit généralement d'une valeur qui est effectivement appliquée dans les balises UMF et stockée dans les tables de base de données. Lors de la modification de codes de recherche existants, cette zone sera en lecture seule.

Description
Tapez la description du code de recherche.

Etat Dans la liste déroulante, sélectionnez **Actif** pour indiquer que ce code de recherche est actif. Sinon, sélectionnez **Inactif**.

Codes de recherche - champ Type :

La zone **Type** permet d'indiquer le type sous lequel regrouper le code de recherche.

ADDR_STAT
Ce type de code de recherche est utilisé pour les valeurs d'état d'adresse. Ces valeurs peuvent servir à associer à des adresses particulières des renseignements tels que s'il s'agit ou non d'une adresse joignable.

ADDR_TYPE
Classifications des adresses, définies par l'utilisateur. Il s'agit des valeurs admises par la balise UMF `ADDR_TYPE`.

ANALYZER_GROUP
Ce type de code de recherche est utilisé pour les règles d'alerte de rôle et le visualiseur. Tout nouveau code de recherche dont le type est ANALYZER_GROUP constitue une option disponible de la liste déroulante **Groupe d'alertes** de l'onglet **Configurer** > **Relations** > **Règles d'alerte de rôle** > **Général** ainsi que de la liste déroulante **Groupe** de l'onglet **Configurer** > **Visualiseur** > **Utilisateurs de Visualizer** > **Général**.

ATTR_CLASS
Classifications des types de caractéristique, définies par l'utilisateur. Les valeurs saisies ici apparaîtront comme options de la liste déroulante **Classe**, dans l'onglet **Configurer** > **Sources** > **Caractéristiques** > **Général**. Les caractéristiques qui utilisent le code de recherche LINK pour leur classe d'attribut peuvent s'afficher sous forme de lien HTML dans le visualiseur si la valeur de la caractéristique respecte ce format :

Texte d'affichage du lien=URL

ATTR_MATCH_LEVEL
Ce type de code de recherche est obsolète.

CONF_LEVEL
Ce type de code de recherche est obsolète.

DENSITY_LOG_LEVEL
Ce type de code de recherche est obsolète.

DOC_TYPE
Ce type de code de recherche est obsolète.

DSRC_ACTION
Ce type de code de recherche ne doit pas être modifié car il sert au système.

EX_CLASS
Ce type de code de recherche ne doit pas être modifié car il sert au système.

EX_SEVERITY
Ce type de code de recherche ne doit pas être modifié car il sert au système.

LOG_LEVEL
Ce type de code de recherche ne doit pas être modifié car il sert au système.

ER_LEVEL
Ce type de code de recherche ne doit pas être modifié car il sert au système.

ER_LOG_LEVEL
Ce type de code de recherche ne doit pas être modifié car il sert au système.

LDR_MESSAGE_TYPE
Ce type de code de recherche est obsolète.

MM_STAT
Ce type de code de recherche est obsolète.

NAME_TYPE
Ce type de code de recherche sert à stocker les classifications de nom définies par l'utilisateur. Il s'agit des valeurs admises par la balise UMF `NAME_TYPE`.

NS-FGEN
Ce type de code de recherche ne doit pas être modifié car il sert au système.

NS-LGEN
Ce type de code de recherche ne doit pas être modifié car il sert au système.

NS-PREFIX
Ce type de code de recherche ne doit pas être modifié car il sert au système.

NS-SUFFIX
Ce type de code de recherche ne doit pas être modifié car il sert au système.

NUM_CLASS
Ce type de code de recherche sert à stocker les classifications de types de

numéro définies par l'utilisateur. Les valeurs saisies ici apparaîtront comme options de la liste déroulante **Classe**, dans l'onglet **Configurer** > **Sources** > **Numéros** > **Général**.

REC_STAT
Ce type de code de recherche ne doit pas être modifié car il sert au système.

SEARCH_REASON
Ce type de code de recherche est utilisé par le visualiseur dans une liste d'options déroulantes correspondant à la zone de motif de recherche d'alerte d'attribut. Vous pouvez ajouter ici votre propre liste de motifs valables d'alerte d'attribut.

SYS_DELETE_STAT
Ce type de code de recherche ne doit pas être modifié car il sert au système.

UNIQUE_FLAG
Ce type de code de recherche est obsolète.

USABILITY_LOG_LEVEL
Ce type de code de recherche ne doit pas être modifié car il sert au système.

Configuration de valeurs de données génériques

Vous pouvez configurer des valeurs de données de sorte qu'elles soient génériques si elles dépassent un nombre d'occurrences défini dans la base de données d'entités.

Valeurs génériques

Les valeurs génériques décrivent les valeurs de données qui surviennent régulièrement dans la base de données d'entités et qui, par conséquent, ne sont plus utilisées par le système pour résoudre les entités.

Les valeurs de données sont considérées comme génériques dès qu'elles dépassent un certain seuil. Le seuil désigne le nombre maximum configuré d'occurrences d'entités qui, dans la base de données, peuvent partager la même valeur de données.

Les valeurs génériques sont organisées et configurées par attribut et type d'attribut. La valeur de données générique d'un type d'attribut précis se substitue à celle de l'attribut parent. Les données standard dont la valeur peut être considérée comme générique sont les suivantes :

- Adresse
- Caractéristique
- Courrier électronique
- Nom
- Numéro

Exemple

Si le seuil générique des numéros de téléphone est fixé à 25, dès qu'une valeur de numéro de téléphone (par exemple 04-67-XX-XX-XX) est celle de plus de 25 entités, à compter de ce moment, cette valeur précise n'est plus utilisée pour résoudre les entités.

Remarque : Quand vous réfléchissez au niveau auquel fixer les seuils génériques, songez bien qu'un seuil trop élevé risque de nuire aux performances, le système finissant par être submergé sous des flots de données qui devraient être génériques. Inversement, en fixant un seuil générique trop bas, des alertes importantes risquent de ne pas se déclencher car des critères cruciaux sont considérés comme génériques.

Consultation des valeurs de données génériques

Les valeurs de données génériques sont des seuils génériques de chaque données que vous souhaitez considérer comme générique. Il est conseillé de consulter les valeurs génériques existantes quand vous ajoutez une nouvelle source de données.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Seuil générique**.

Configuration de valeurs de données génériques

Pour que les valeurs génériques soient ignorées au cours de la résolution d'entité, vous devez configurer le seuil générique de la donnée.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Seuil générique**.
4. Effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle valeur de données générique, cliquez sur le bouton **Nouveau**.
   - Pour créer une valeur de donnée générique basée sur une valeur de donnée générique existante, sélectionnez cette dernière dans la liste et cliquez sur le bouton **Cloner**.
5. Dans l'onglet **Général**, indiquez l'attribut, le type d'attribut et la valeur de seuil de la valeur générique.
6. Cliquez sur le bouton **Enregistrer**.

Suppression de valeurs de données génériques

Les valeurs de données génériques sont des seuils génériques de chaque données que vous souhaitez considérer comme générique. Il convient de supprimer les valeurs génériques existantes dès lors qu'elles ne sont plus pertinentes pour les données entrantes.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Seuil générique**.
4. Cochez la case de tout nom d'élément à supprimer.
5. Cliquez sur le bouton **Supprimer**.

Rubriques d'aide

Seuil générique - onglet Général :

L'onglet **Général** permet d'indiquer les détails de la valeur de donnée générique.

Nom de l'attribut
Dans la liste déroulante, sélectionnez l'attribut auquel vous souhaitez appliquer la valeur de donnée générique.

Type d'attribut
Dans la liste déroulante, sélectionnez le type d'attribut auquel vous souhaitez appliquer la valeur de donnée générique.

Cette liste déroulante ne proposera plusieurs options que si le **Nom de l'attribut** est défini sur Nom ou Caractéristique.

Seuil Tapez le nombre d'entités pouvant partager une valeur UMF du type configuré avant qu'il soit ne considéré comme générique.

Configuration de rôles

Vous pouvez configurer des rôles afin de classer les entités de la base de données d'entités. Les rôles peuvent être attribués aux sources de données ou aux entités. Les rôles conflictuels déclenchent des alertes.

Pourquoi et quand exécuter cette tâche

Les rôles peuvent être visualisés et modifiés à l'aide de la console, dans l'onglet **Sources de données**.

Rôles

Un rôle est une classification d'une identité qui en définit l'essence ou le but. Vous pouvez associer plusieurs rôles à une identité. A mesure que identités se résolvent en entités, ces dernières héritent de tous les rôles associés.

Les rôles servent à configurer les règles d'alertes de rôle, qui définissent les relations intéressantes et déclenchent les alertes.

Un rôle est attribué à chaque identité, de l'une de deux manières :

Par source de données entrante
Quand vous configurez une nouvelle source de données, vous y associez un rôle, ce qui aura pour effet d'attribuer ce rôle à toutes les identités contenant ce code de source de données.

Par UMF
Quand vous convertissez au format UMF (Universal Message Format) la source de données, vous pouvez attribuer des rôles directement comme élément de la fiche UMF au moyen du segment UMF <SEP_ROLES>, avec la balise UMF <ROLE_CODE>. Si vous configurez par UMF, il faudra ajouter les règles DQM et une table de consultation.

Exemples de rôles utiles : employés, fournisseurs, clients ou liste noire.

Exemple d'attribution de rôles à l'aide du format UMF

Pour attribuer le rôle d'employé à une fiche d'identité à l'aide du format UMF, il faut saisir le segment UMF <SEP_ROLES> et la balise UMF <ROLE_CODE> suivants de cette fiche :

```
<SEP_ROLES>

  <ROLE_CODE>employé</ROLE_CODE>

</SEP_ROLES>
```

Consultation des rôles

Un rôle définit la manière dont une entité est classée ou reconnue dans le système. Il est conseillé de consulter les rôles existants si vous envisagez d'en ajouter un nouveau.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Relations**.
3. Cliquez sur l'onglet **Codes de rôles**.
4. Sélectionnez le rôle à consulter.

Création de rôles

Pour défini comment des s'apparentent à d'autres entités, créez des rôles dans le système.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Relations**.
3. Cliquez sur l'onglet **Codes de rôles**.
4. Effectuez l'une des opérations suivantes :
   - Pour créer un nouveau rôle, cliquez sur le bouton **Nouveau**.
   - Pour créer un rôle basé sur un rôle existant, sélectionnez-en un dans la liste, puis cliquez sur le bouton **Cloner**.
5. Dans l'onglet **Général**, indiquez le code de rôle, la description, la classe, l'état et autres informations de configuration sur le nouveau rôle.
6. Cliquez sur le bouton **Enregistrer**.

Que faire ensuite

Vous pouvez utiliser ce rôle pour définir des règles d'alerte de rôle.

Suppression de rôles

Un rôle définit la manière dont une entité est classée ou reconnue dans le système. Il est souhaitable de supprimer un rôle existant s'il n'est plus valide.

Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas supprimer un rôle utilisé par une règle d'alerte de rôle ou par une source de données.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Relations**.
3. Cliquez sur l'onglet **Codes de rôles**.
4. Cochez la case de tout rôle à supprimer.
5. Cliquez sur le bouton **Supprimer**.

Rubriques d'aide

Rôles - onglet Général :

L'onglet **Général** permet d'indiquer les détails du rôle.

ID Tapez l'entier unique qui identifie l'ID de rôle.

Le prochain numéro inutilisé est automatiquement attribué comme valeur d'ID.

Code de rôle
Tapez une valeur unique pour identifier ce rôle.

Description
Tapez la description de ce rôle.

Classe de rôle
Tapez la classe de ce rôle.

Etat Dans la liste déroulante, sélectionnez **Actif** pour indiquer que ce rôle est actif. Sinon, sélectionnez **Inactif**.

Configuration de règles d'alerte de rôle

Vous pouvez configurer des règles d'alerte de rôle pour définir une combinaison de rôles qui, si le système la détecte, déclenche des alertes.

Pourquoi et quand exécuter cette tâche

Les règles d'alerte de rôle peuvent être visualisées et modifiées à l'aide de la console, dans l'onglet **Règles d'alerte de rôle**.

Alerte de rôle

Une alerte de rôle est définie dans le système par une règle qui représente les relations servant à déclencher les alertes.

Les règles de d'alerte de rôle définissent une combinaison de rôles qui, lorsqu'ils sont détectés dans une relation ou une entité, indiquent un conflit quelconque. Par exemple, une règle d'alerte de rôle peut signaler que dès qu'une entité dotée du rôle Employé connaît une entité ayant pour rôle Fournisseur, il existe une alerte de rôle. Cette règle d'alerte de rôle peut être décrite comme "l'employé connaît le fournisseur." Quand le système détecte des alertes de rôle dans des entités ou des relations, des alertes, qui peuvent être publiées auprès de l'entreprise et affichées dans les applications Analyst Toolkit, sont créées.

Bien que la plupart des règles d'alerte de rôle stipulent une combinaison de deux rôles différents présentant un conflit, il est également possible de définir une règle d'alerte de rôle dans laquelle une entité ayant un rôle donné connaît une autre entité du même rôle. Il se peut par exemple que vous souhaitiez être informé de toute relation entre vos clients et élaboriez une règle d'alerte de rôle qui déclenche une alerte dès qu'une entité cliente est en relation avec une autre entité cliente. Cette règle d'alerte de rôle peut être décrite comme "le client connaît le client."

Les règles d'alerte de rôle reposent sur des codes de rôle existants. Les rôles doivent être définis avant que des règles de conflit associées à ces rôles puissent être créées.

Consultation des règles d'alerte de rôle

Une règle d'alerte de rôle sert à déclencher des alertes quand une relation entre deux rôles définis est détectée. Il est conseillé de consulter les règles d'alerte de rôle existantes si vous envisagez d'en ajouter une nouvelle.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Relations**.
3. Cliquez sur l'onglet **Règles de conflit**.
4. Sélectionnez la règle d'alerte de rôle à consulter.

Configuration de règles d'alerte de rôle

Vous configurez des règles d'alerte de rôle pour déclencher des alertes de rôle ou des relations entre deux rôles ou identités.

Avant de commencer

Avant de définir une règle d'alerte de rôle, vous devez configurer les rôles que vous souhaitez utiliser dans cette règle. Par exemple, si vous souhaitez configurer une règle d'alerte de rôle dans laquelle un employé ne peut pas être un fournisseur, votre système doit contenir les rôles "Employé" et "Fournisseur".

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Relations**.
3. Cliquez sur l'onglet **Règles de conflit**.
4. Effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle règle d'alerte de rôle, cliquez sur le bouton **Nouveau**.
   - Pour créer une règle d'alerte de rôle basée sur une règle d'alerte de rôle existante, sélectionnez-en une dans la liste, puis cliquez sur le bouton **Cloner**.

   La zone **ID de règle de conflit** est automatiquement renseignée avec l'ID unique suivant. Vous pouvez le remplacer par n'importe quel numéro d'ID unique.
5. Cliquez sur le bouton **Nouveau**.
6. Dans l'onglet **Général**, indiquez l'ID, la description, la gravité, les codes de rôle, le groupe d'alertes et le seuil d'alerte minimum de cette règle d'alerte de rôle.
7. Dans l'onglet **Filtres**, facultatif, indiquez le filtre d'identité, le filtre de modification de données et l'ajustement de coefficient de recherche (uniquement affiché si la zone de filtre de modification de données est définie sur ajustement de coefficient de recherche). Si les filtres sont tous deux définis, il suffit qu'un seul soit satisfait pour qu'une alerte de rôle se déclenche.
8. Cliquez sur le bouton **Enregistrer**.

Suppression de règles d'alerte de rôle

Il convient de supprimer une règle d'alerte de rôle une fois qu'un rôle qui y est défini est sur le point d'être supprimé ou que la combinaison de rôles qu'elle renferme ne présente plus d'intérêt.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Relations**.
3. Cliquez sur l'onglet **Règles de conflit**.
4. Cochez la case de toute règle d'alerte de rôle à supprimer.
5. Cliquez sur le bouton **Supprimer**.

Rubriques d'aide

Règles d'alertes de rôle - onglet Général :

Utilisez l'onglet **Général** de la fenêtre **Règles d'alertes de rôle** pour configurer les détails des règles d'alertes de rôle. Les rôles sont associés aux sources de données. Selon la configuration de la source de données, un rôle est affecté à chaque identité provenant d'une source de données et entrant dans le système. Les règles d'alerte de rôle définissent le moment où l'alerte de rôle est générée en fonction d'un conflit entre les rôles affectés aux identités entrantes et aux identités associées à des entités dans la base de données d'entités.

ID de règle d'alerte de rôle
Le prochain numéro inutilisé est automatiquement attribué comme valeur d'ID.

Description
Tapez la description de cette règle d'alerte de rôle. Ce texte s'affiche dans Visualizer si une alerte de rôle est générée suivant cette règle d'alerte de rôle.

Gravité
Code monocaractère, défini par l'utilisateur, servant à catégoriser l'importance des alertes déclenchées par cette règle.

Faites correspondre la gravité de l'alerte de rôle à son importance. Ce code s'affiche avec les alertes de rôle générées à partir de cette règle d'alerte de rôle dans Visualizer. Les analystes l'utilisent pour identifier quelles sont les alertes à examiner en priorité. Le code monocaractère doit donc être éloquent pour les utilisateur de Visualizer. Par exemple, une règle d'alerte de rôle qui génère une alerte si un passager correspond à une personne sur un liste d'interdits de vol peut être plus importante qu'une règle d'alerte de rôle prévue pour générer une alerte si un employé connaît un client.

Voici des exemples de codes de gravité : C pour critique, N pour neutre, I pour intéressant, H pour haut ou B pour bas.

Rôle 1 Dans la liste déroulante, sélectionnez le premier rôle pour la comparaison dans cette règle d'alerte de rôle.

Les options de rôle qui s'affichent sont les rôles existants configurés. Si le rôle que vous souhaitez sélectionner ne s'affiche pas, configurez d'abord le rôle dans l'onglet **Rôles**.

Rôle 2 Dans la liste déroulante, sélectionnez le second rôle pour la comparaison dans cette règle d'alerte de rôle.

Les options de rôle qui s'affichent sont les rôles existants configurés. Si le rôle que vous souhaitez sélectionner ne s'affiche pas, configurez d'abord le rôle dans l'onglet **Rôles**.

Groupe d'alertes
Dans la liste déroulante, sélectionnez le groupe d'analyseurs Visualizer qui analysera les alertes de rôle déclenchées par cette règle d'alerte de rôle. Par exemple, vous pouvez diriger toutes les alertes de rôle de liste d'interdits de vol vers un service de sécurité et toutes les alertes de rôle employés-fournisseurs vers les ressources humaines.

Les options de groupe affichées sont les groupes d'analyseurs Visualizer actifs configurés avec le type de code `ANALYZER_GROUP`. Si le groupe que

vous souhaitez sélectionner ne s'affiche pas, configurez d'abord un nouveau code ANALYZER_GROUP dans l'onglet **Configuration - Général - Codes**.

Il s'agit d'un champ obligatoire, donc même si votre organisation n'utilise pas Visualizer, vous devez obligatoirement configurer et sélectionner un code de groupe d'alertes.

Onglet Règles d'alerte de rôle :

Si les filtres sont tous deux définis, il suffit qu'un seul soit satisfait pour qu'une alerte de rôle se déclenche.

Filtre d'identité
Dans la liste déroulante, sélectionnez un filtre afin de restreindre le déclenchement d'alerte de rôle quand de nouvelles identités sont ajoutées aux entités concernées par l'alerte de rôle.

Ce filtre n'affecte que le comportement de ré-alerte. La première fois que la règle d'alerte de rôle est satisfaite pour un ensemble d'entités donné, une alerte de rôle est toujours déclenchée. Ce filtre peut empêcher tout redéclenchement ultérieur de la même alerte de rôle lorsque des modifications sont apportées aux entités concernées.

Hors fonction
Sélectionnez ce type de zone pour désactiver la restriction d'alerte de rôle quand de nouvelles identités sont ajoutées aux entités concernées par l'alerte de rôle.

Nouvelle identité
Sélectionnez ce type de zone pour ne réalerter que quand un nouveau code de source de données est introduit parmi les identités dans les entités concernées par l'alerte de rôle.

Nouveau code de source de données
Sélectionnez ce type de zone pour réalerter quand un nouveau code de source de données est introduit parmi les identités.

Filtre de modification de données
Dans la liste déroulante, sélectionnez un filtre afin de restreindre le déclenchement d'alerte de rôle quand de nouvelles données d'attributs sont ajoutées aux entités concernées par l'alerte de rôle.

Ce filtre n'affecte que le comportement de ré-alerte. La première fois que la règle d'alerte de rôle est satisfaite pour un ensemble d'entités donné, une alerte de rôle est toujours déclenchée. Ce filtre peut empêcher tout redéclenchement ultérieur de la même alerte de rôle lorsque des modifications sont apportées aux entités concernées.

Hors fonction
Sélectionnez ce type de zone pour désactiver la restriction d'alerte de rôle quand de nouvelles données d'attributs sont ajoutées aux entités concernées par l'alerte de rôle.

Nouvelles données d'attributs
Sélectionnez ce type de zone pour ne réalerter que quand de nouvelles données d'attributs sont ajoutées aux entités concernées par l'alerte de rôle.

Ajustement du coefficient de recherche
Sélectionnez ce type de zone pour ne réalerter que quand sont ajoutées de nouvelles données d'attributs qui provoquent dans le

coefficient de recherche une modification égale ou supérieure à la valeur **Ajustement du coefficient de recherche**.

Ajustement du coefficient de recherche
Cette zone ne s'affiche que si la liste déroulante **Filtre de modification de données** est définie sur Ajustement du coefficient de recherche. Tapez une valeur d'ajustement (de -100 à 100) à appliquer quand le **Filtre de modification de données** est défini sur Ajustement du coefficient de recherche. Ceci n'autorise le redéclenchement d'alertes de rôle qu'en cas d'ajout de nouvelles données d'attributs qui provoquent dans le coefficient de recherche une modification égale ou supérieure à la valeur d'ajustement de ce coefficient. Indiquer zéro équivaut à désactiver le filtre.

Configuration de types d'entités

Vous pouvez configurer des types d'entités de façon à identifier la nature exacte de l'entité.

Pourquoi et quand exécuter cette tâche

Lorsque de nouvelles données d'entité sont ajoutées à une source de données et que vous souhaitez les classer en tant que type d'entité dont ce type n'est pas encore configuré dans le système, vous devez créer un type d'entité pour ces nouvelles données.

Les types d'entité peuvent être visualisés et modifiés à l'aide de la console, dans l'onglet **Types d'entité**.

Types d'entités

Les types d'entités sont des traits ou propriétés, définis par l'utilisateur, et associés à une entité afin d'en identifier la nature exacte.

La découverte de relation impersonnelle utilise des types d'entité pour relier des entités qui ne posséderaient pas autrement une relation à un degré.

Si par exemple vous souhaitez découvrir les relations impersonnelles au moyen d'appels téléphoniques, il faut créer un nouveau type d'entité nommé *Appel téléphonique* et ajuster votre noeud d'acquisition afin d'attribuer à chaque fiche d'appel téléphonique le type d'entité *Appel téléphonique*.

Lors de l'incorporation des fiches téléphoniques dans le pipeline, le processus de résolution de relation et d'entité détecte une relation à un degré entre l'entité *Appel téléphonique* et l'entité appelante (*Personne*). Il détecte également une relation à un degré entre le destinataire de l'appel et l'entité *Appel téléphonique*. De lui-même, le système ne détecte pas de relation à un degré entre les deux personnes.

```
<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>
```

Découverte de relation impersonnelle

La découverte de relation impersonnelle est une fonction qui étend le processus de résolution de relation traditionnel afin de détecter et analyser des relations impersonnelles. Le processus de détection de relation détecte les relations entre entités en fonction des valeurs d'attribut associées à ces entités. Il importe parfois de détecter les relations entre entités en fonction des activités ou d'autres identifiants impersonnels. Ces relations entre entités en fonction des activités ou autres identifiants impersonnels sont appelées relations *impersonnelles*, les activités ou identifiants impersonnels qui apparentent des personnes étant appelés *faits relationnels*.

Les relations impersonnelles s'établissent toujours à au moins deux degrés de séparation, car le fait relationnel est en lui-même une entité. Par conséquent, pour activer la découverte de relations impersonnelles et rechercher des relations impersonnelles, configurez vos sources de données pour qu'elles utilisent la fonction Degrees of Separation qui étend l'entité et la résolution de relations afin de détecter des relations à plus de deux degrés de séparation.

Soit par exemple une transaction téléphonique où figurent des données sur les numéros de téléphone, à savoir à la fois le numéro émetteur et le numéro récepteur. Bien qu'une personne ait effectué l'appel téléphonique à destination d'une autre personne, d'après la transaction téléphonique seule, aucune donnée commune ne peut être attribuée à ces personnes. Souvent, le fait relationnel (l'appel téléphonique) est connu avant que toute autre information sur les entités apparentées (les deux personnes impliquées dans l'appel téléphonique) ne le soit. Ces faits relationnels ne pouvant être attribués à une personne, il faut les représenter en tant qu'entités distinctes qui ne sont pas des personnes, mais concernent des personnes. Toutefois, la découverte de relation impersonnelle reconnaît qu'il existe une relation entre deux personnes en conséquence l'appel téléphonique.

Le format UMF comporte une fonction de type d'entité qui permet de définir des faits relationnels comme types d'entités. Grâce à cette fonction, les faits relationnels deviennent des entités distinctes dans la base de données d'entités et peuvent servir à détecter les relations entre entités Personne. En configurant de nouveaux types d'entités, en indiquant le type d'entité adéquat dans l'UMF, et en créant de nouvelles configurations de résolution, ces faits relationnels peuvent servir à détecter automatiquement les relations impersonnelles et les conflits entre entités.

Les entités de types différents ne s'entre-résolvent jamais, ce même si les règles de résolution l'autorisent et même si les données admettent la résolution. Cela signifie qu'un type d'entité Appel téléphonique ne se résout jamais en un type d'entité Personne .

Analyst Toolkit génère des graphiques et des rapports pour les relations impersonnelles et les alertes associées tout comme pour les relations personnelles et les alertes associées.

Exemple de découverte de relation impersonnelle

Si par exemple vous souhaitez découvrir les relations impersonnelles au moyen d'appels téléphoniques, il faut créer un nouveau type d'entité nommé Appel téléphonique et ajuster votre noeud d'acquisition afin d'attribuer à chaque fiche d'appel téléphonique le type d'entité *Appel téléphonique*.

Lors de l'intégration des fiches téléphoniques au système, la résolution de relations et d'entités standard détecte une relation à un degré entre l'entité Appel téléphonique et l'entité appelante (Personne). Une relation à un degré entre la personne appelée et l'entité Appel téléphonique est également détectée. Le système, de lui-même, ne trouve aucune relation entre les personnes.

Toutefois, lorsque la fonction Degrees of Separation est configurée, elle continue d'analyser et de détecter la relation impersonnelle à deux degrés entre l'appelant et la personne appelée. Une relation impersonnelle existe, d'après les numéros de téléphone qui sont des attributs du type d'entité Appel téléphonique. La fonction Degrees of Separation analyse ensuite cette relation impersonnelle et déclenche une alerte en cas de conflit.

Consultation des types d'entité

Les types d'entité correspondent à des traits ou des propriétés définis par l'utilisateur et associés à une entité en vue d'identifier la nature exacte de celle-ci. Vous pouvez consulter les types d'entité existants si vous envisagez d'en ajouter un nouveau.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Types d'entité**.
4. Sélectionnez le type d'entité à consulter.

Création de types d'entité

Les types d'entité correspondent à des traits ou des propriétés définis par l'utilisateur et associés à une entité en vue d'identifier la nature exacte de celle-ci. Vous pouvez ajouter un nouveau type d'entité au système, et ce si vous ajoutez un nouveau type de données à votre système.

Avant de commencer

Avant de créer un type d'entité, consultez les données d'identité entrantes afin de déterminer s'il est possible de les décrire précisément au moyen d'un type d'entité existant.

Pourquoi et quand exécuter cette tâche

La découverte de relation impersonnelle utilise des types d'entité pour relier des entités qui ne posséderaient pas autrement une relation à un degré.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Types d'entité**.
4. Cliquez sur le bouton **Nouveau**.
5. Dans l'onglet **Général**, spécifiez l'ID, le type, la description, la configuration de la résolution d'entités, le collaborateur générique, le collaborateur de conflit, le type de recherche et autorisez la résolution de ce type d'entité.
6. Cliquez sur le bouton **Enregistrer**.

Résultats

Le système peut désormais affecter des types d'entité aux données et utiliser la découverte de relation impersonnelle pour relier des entités qui, autrement, ne posséderaient pas une relation à un degré.

Suppression de types d'entité

Vous pouvez supprimer un type d'entité existant lorsque celui-ci n'est plus utilisé par la base de données d'entités.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Types d'entité**.
4. Cochez la case du type de caractéristique à supprimer.
5. Cliquez sur le bouton **Supprimer**.

Rubriques d'aide

Types d'entité - onglet Général :

L'onglet **Types d'entité** permet de spécifier les détails de chaque type d'entité.

ID Tapez le numéro d'ID du type d'entité que vous souhaitez créer.

Cet ID est un code numérique qui s'incrémente automatiquement. Bien que le produit fournisse le numéro disponible suivant dans l'ordre, vous pouvez attribuer à ce code une valeur numérique unique en entrant cette valeur dans la zone ID.

Type Tapez le nom du type d'entité que vous souhaitez créer.

Par exemple, le type d'entité Phone call permet de décrire les entités correspondant à des enregistrements réels d'appels téléphoniques passés entre deux entités.

Description
Tapez la description du type d'entité que vous souhaitez créer.

Configuration de la résolution d'entité
Dans la liste déroulante, sélectionnez la configuration de résolution qui sera utilisée par ce type d'entité lors du chargement.

Les configurations de résolution sont définies dans l'écran **Configurer** > **Résolution** > **Configurations de résolution**.

Collaborateur générique
Dans la liste déroulante, sélectionnez **Oui** pour permettre aux données de ce type d'entité de devenir génériques. Sinon, sélectionnez **Non**.

Collaborateur de conflit
Dans la liste déroulante, sélectionnez **Oui** pour permettre aux données de ce type d'entité de générer des alertes de rôle. Sinon, sélectionnez **Non**.

Type de recherche
Dans la liste déroulante, sélectionnez **Oui** pour permettre aux données de ce type d'entité d'être utilisées pour les recherches. Sinon, sélectionnez **Non**.

Autoriser la résolution

Dans la liste déroulante, sélectionnez **Oui** pour permettre aux données de ce type d'entité d'être utilisées pour résoudre des entités. Sinon, sélectionnez **Non**.

Présentation de la fonction Degrees of Separation

La fonction Degrees of Separation développe les capacités de mise en correspondance de relations d'IBM Relationship Resolution.

Le comportement par défaut d'IBM InfoSphere Identity Insight consiste à identifier les relations importantes et à établir une correspondance avec des entités à un degré de séparation à partir d'une identité entrante résolue en entité. L'activation de la fonction Degrees of Separation étend ces capacités pour atteindre une gamme quasi illimitée de degrés de séparation définis par l'utilisateur à partir d'une identité entrante résolue en entité.

La fonction Degrees of Separation utilise des configurations de séparation, des rôles, des règles d'alerte de rôle et des scores relationnels pour effectuer une analyse de liens en temps réel par rapport à des ensembles de données très volumineux.

Lorsqu'une identité entrante est résolue en entité, un diagramme d'entité est généré à partir des relations à un degré détectées par IBM InfoSphere Identity. Le diagramme d'entité utilise les relations à un degré pour élaborer des chaînes relationnelles à plusieurs degrés émanant de l'entité qui résulte de la résolution d'identité entrante. Une chaîne d'alertes de rôle peut ensuite être créée en reliant les chaînes relationnelles à plusieurs degrés, chacune d'elles émanant de l'entité qui résulte de la résolution d'identité entrante. La chaîne d'alertes de rôle peut ensuite servir à rechercher une relation entre les entités situées en fin de chaque chaîne relationnelle à degrés multiples, y compris cette chaîne.

La fonction Degrees of Separation facilite la tâche en évaluant tous les chemins reliant deux entités et en utilisant le chemin le plus fiable lors de la signalisation des relations. Cette fonction peut être configurée en vue de signaler une alerte de rôle pour chaque règle d'alerte de rôle configurée par entité vers laquelle l'identité entrante a été résolue.

La configuration des degrés de séparation peut être définie dans la console à l'aide de l'onglet de **Configuration système**, valeur Degrés de séparation.

Exemple de degré de séparation

Cet exemple décrit un chemin de relation et explique comment la configuration des degrés de séparation détermine les alertes de rôle.

Exemple de degré de séparation

Une fois les données entrantes traitées, Identity Insight signale le chemin de relation suivant :

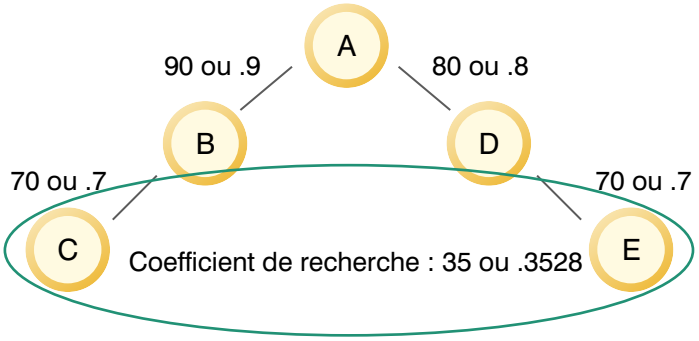
- L'entité A connaît l'entité B.
- L'entité B connaît l'entité C
- L'entité A connaît l'entité D
- L'entité D connaît l'entité E

Un *chemin de relation* est une chaîne d'entités et d'attributs qui relie une entité à une autre.

Dans le cadre du traitement des relations et des alertes de rôle, Identity Insight détermine le coefficient de recherche. Le coefficient de recherche correspond au produit des scores relationnels convertis en nombres décimaux pour chaque entité située dans la chaîne, converti en nombre entier.

Dans notre exemple, le produit calcule les scores de relation et convertit les scores en valeurs décimales :

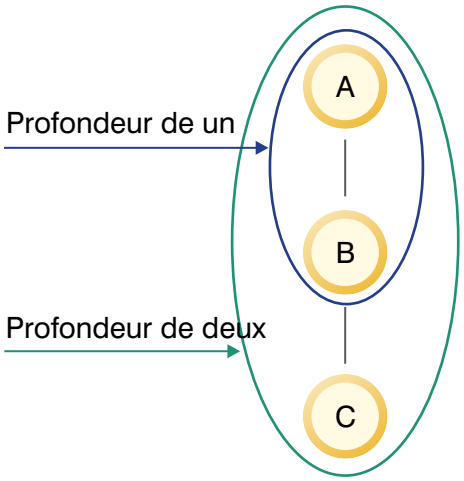
- Le score de relation de "l'entité A connaît l'entité B" est de 90. 90 est converti dans la valeur décimale 0,9
- Le score de relation de l'entité B connaît l'entité C est de 70. La valeur 70 est convertie en valeur décimale 0,7.
- Le score de relation de "l'entité A connaît l'entité D" est de 80. La valeur 80 est convertie en valeur décimale 0,8.
- Le score de relation de l'entité D connaît l'entité E est de 70. La valeur 70 est convertie en valeur décimale 0,7.



Les scores de la relation dans le chemin sont multipliés. Le résultat du calcul est un coefficient de recherche de ,3528, qui est converti en entier 35.

Le produit compare ensuite le coefficient de recherche calculé au paramètre des degrés de séparation **path strength threshold**. Si le coefficient de recherche est égal ou supérieur au seuil configuré, le produit génère des alertes de rôle. Si le coefficient de recherche est inférieur au seuil configuré, le produit ne génère pas d'alertes de rôle.

Le produit utilise ensuite le paramètre de degré de séparation **max depth** pour calculer les degrés de séparation entre les entités dans la chaîne de relation. Le paramètre max depth détermine le nombre maximal de degrés de séparation dans un chemin de relation à degrés multiples qui peuvent être pris en compte lors de la détection d'une alerte de rôle.



En règle générale, le paramètre **max depth** a pour valeur 2.

Dans cet exemple, le paramètre **max depth** a pour valeur 6. L'entité C et l'entité E ont des rôles conflictuels et sont séparées par six degrés. Une alerte de rôle est donc générée.

Affichage des configurations de séparation

Le produit permettant l'utilisation de plusieurs configurations de séparation, utilisez les instructions ci-après pour afficher les paramètres d'une configuration de séparation spécifique.

Procédure

1. Dans la console de configuration, cliquez sur **Configurer** > **Relations** > **Configuration de séparation**.
2. Sélectionnez la configuration de séparation.

Création de configuration de séparation

Vous pouvez définir des configurations de séparation pour déterminer si la résolution de relation détecte un ou plusieurs degrés de séparation entre des entités.

Procédure

1. Dans la console de configuration, cliquez sur **Configurer** > **Relations** > **Configuration de séparation**.
2. Cliquez sur **Nouveau**.
3. Dans l'onglet **Général**, définissez les paramètres de cette configuration de séparation.
4. Cliquez sur **Enregistrer**.

Edition des configurations de séparation

Vous pouvez modifier une configuration de séparation pour redéfinir les paramètres déterminant le nombre de degrés qui peuvent séparer deux entités tout en maintenant son état de relation.

Procédure

1. Dans la console de configuration, cliquez sur **Configurer** > **Relations** > **Configuration de séparation**.

2. Sélectionnez la **configuration de séparation** pour apporter vos modifications.
3. Cliquez sur **Enregistrer**.

Rubriques d'aide

Configuration de séparation - onglet Général :

Utilisez l'onglet **Général** pour indiquer les détails du configuration de séparation.

ID Saisissez l'entier unique qui identifie la configuration de séparation.

Le prochain numéro inutilisé est automatiquement attribué comme valeur d'ID.

Code Tapez une valeur unique pour identifier ce rôle.

Description
Saisissez une description pour cette configuration de séparation.

Nombre de niveaux max.
Le nombre maximal de degrés de séparation d'une chaîne de relation multidegrés dans un diagramme d'entité considéré pour la détection d'alerte de rôle.

Seuil de coefficient de recherche
Le **seuil de coefficient de recherche** calculé d'une chaîne d'alerte de rôle. Une chaîne d'alerte de rôle dont le coefficient de recherche est inférieur à ce seuil ne déclenche aucune alertes de rôle.

Le coefficient de recherche est le produit, converti en nombre entier, des conversions en décimale du score de relation de chaque entité de la chaîne d'alerte de rôle. La valeur par défaut de ce paramètre est 15.

Les degrés de séparation évaluent tous les chemins qui relient deux entités et utilisent le chemin le plus fiable pour générer des rapports sur les relations.

Configuration de documents UMF

Pour réussir à utiliser des documents UMF (Unified Messaging Format), ils doivent être connus et configurés.

Consultation des documents d'entrée UMF par défaut

Les documents d'entrée UMF sont la série de segments UMF qui structurent les données entrantes à charger, modifier ou interroger dans la base de données d'entités.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Documents d'entrée**.

Configuration de documents de sortie

Si vous vous en servez, vous devez configurer l'état activé d'un code de format de document de sortie.

Pourquoi et quand exécuter cette tâche

Données de résultat UMF de format de documents de sortie UMF.

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Documents de sortie**.
4. Cliquez sur n'importe quel lien dans la ligne qui contient le code de format de document de sortie UMF à modifier.
5. Dans la liste déroulante **Activé**, sélectionnez l'état adéquat du code de format de document de sortie UMF.
6. Cliquez sur le bouton **Enregistrer**.

Configuration de la source de données

Quand vous avez une nouvelle source de données à charger dans la base de données d'entités, vous devez la configurer.

Avant de commencer

Pour configurer une source de données, vous devez d'abord établir des rôles.

Pourquoi et quand exécuter cette tâche

Les sources de données peuvent être visualisées et modifiées à l'aide de la console, dans l'onglet **Sources de données**.

Sources de données

Les sources de données contiennent les identités que vous souhaitez traiter pour la résolution des entités et le chargement dans la base de données correspondante. Elles contiennent des données d'identification (identificateurs personnels uniques d'une identité) ainsi que d'autres types de données (autres attributs et points de données d'une identité). Les fiches d'identités de la source de données doivent être exportées au format UMF (Universal Message Format) pour que le système puisse les traiter ou pour qu'elles puissent être chargées dans la base de données des entités. Voici quelques exemples, entre autres, de sources de données : listes d'employés, de surveillance, de clients ou encore listes de fournisseurs.

Les sources de données contiennent des informations vitales, telles que celles relatives à la source d'origine (les données d'origine étant été converties au format UMF) ou la référence externe à la source de données. Ces détails font de chaque source de données un élément unique dans le système.

Lors de la résolution d'entités, si deux d'entre elles ne sont pas résolues, le système fait appel aux informations de la source de données pour définir de quelle entité proviennent les informations.

Emplacements des sources de données et systèmes source

Vous pouvez classer les sources de données entrantes en créant des emplacements source et des systèmes source et en établissant ensuite une association avec vos sources de données. Les emplacements source et les systèmes source permettent de faire la distinction entre des types de sources de données similaires.

Par exemple, si vous traitez des données de réservation et des données de ressources humaines à partir de plusieurs emplacements, un emplacement de source de données vous permet de définir l'emplacement qui contribue aux données :

- Propriété X, Données de réservation
- Propriété X, Données de ressources humaines
- Propriété Y, Données de réservation
- Propriété Y, Données de ressources humaines

Configurations par source de données

Pour optimiser les résultats des opérations de résolution d'entité et de détection de relations, configurez chaque source de données à l'aide des paramètres suivants :

Rôles Les sources de données étant des regroupement de données d'un même type, vous pouvez affecter automatiquement le même rôle à toutes les fiches d'identité d'une même source de données entrante. Par exemple, si vous associez le rôle Employé à une source de données Ressources humaines, ce rôle est automatiquement affecté à toutes les fiches entrantes de la liste des employés.

Niveaux de chargement
Vous pouvez définir si toutes les données d'une source de données entrante doivent être chargées, ou seulement les données qui permettent de résoudre une ou plusieurs entités, ou encore celles qui y sont liées.

Paramètres de résolution de relations
Vous pouvez configurer le niveau de détection de relations en fonction de la source de données. Par exemple, vous pouvez désactiver la fonction de résolution de relations d'une source de données ou sélectionner le nombre de degrés de séparation pour la détection de relations au sein de cette source de données.

Consultation des sources de données

Une source de données contient les données chargées dans la base de données d'entités. Il est conseillé de consulter les sources de données existantes si vous envisagez d'en ajouter une nouvelle.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Sources de données**.
4. Sélectionnez la source de données à consulter.

Configuration d'une source de données

Pour que le chargement de données dans la base de données d'entités réussisse, vous devez configurer le système de sorte qu'il reconnaisse chaque source de données.

Avant de commencer

Pour pouvoir charger des données dans le système, il faut que la source de données respecte le standard UMF.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Sources de données**.
4. Cliquez sur le bouton **Nouveau**.

5. Dans l'onglet **Général**, indiquez l'ID, la description et autres informations de configuration de la source de données.
6. Cliquez sur l'onglet **Résolution d'entité**.
7. Dans l'onglet **Résolution d'entité**, indiquez les informations de configuration de résolution de la source de données.
8. Cliquez sur l'onglet **Relations**.
9. Dans l'onglet **Relations**, indiquez les informations de configuration de relation de la source de données.
10. Cliquez sur le bouton **Enregistrer**.

Configuration du niveau de concordance des noms dans le gestionnaire de noms

Les données de nom pouvant varier d'une source à l'autre, vous pouvez configurer le niveau de concordance du gestionnaire de noms par source de données. Le niveau de concordance sélectionné est un paramètre de comparaison qui détermine le niveau de concordance des noms entrants de cette source de données.

Procédure

1. Dans la console de configuration, sélectionnez **Configurer** > **Sources** > **Sources de données**.
2. Sélectionnez la source de données.
3. Cliquez sur **Résolution d'entité**.
4. Dans la liste **Niveau de concordance du gestionnaire de noms**, sélectionnez le niveau de concordance. Pour la plupart des situations, utilisez la valeur **par défaut**, qui est suffisamment stricte pour obtenir des concordances de noms fiables.

Configuration des sources de données pour le hachage de nom amélioré

Si vous utilisez la fonction de hachage de nom amélioré, vous devez configurer chaque source de données pour permettre la génération d'une liste de candidats d'attributs de nom en définissant la configuration du générateur de candidat **Par défaut avec nom uniquement**.

Suppression de sources de données

Une source de données contient les données chargées dans la base de données d'entités. Il est souhaitable de supprimer une source de données soit si elle n'existe plus, soit si elle n'est plus pertinente pour la base de données d'entités.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur l'onglet **Sources de données**.
4. Cochez la case de la source de données à supprimer.
5. Cliquez sur le bouton **Supprimer**.

Création d'un emplacement de source de données

Pour créer un emplacement afin de classer une source de données, il faut que cet emplacement soit configuré dans le système.

Pourquoi et quand exécuter cette tâche

Les emplacements de source de données se créent au moyen de la console de configuration. Il s'agit d'une opération facultative qui s'emploie essentiellement si votre source de données recueille des données auprès de plusieurs emplacements physiques. Citons par exemple une base de données hôtelière qui recueille des données auprès de plusieurs établissements.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Emplacements**.
4. Cliquez sur le bouton **Nouveau**.
5. Dans l'onglet **Général**, indiquez le code d'emplacement, le nom d'emplacement, le district, la société, la latitude, la longitude, l'état et autres informations de configuration de l'emplacement de la source de données.
6. Cliquez sur le bouton **Enregistrer**.

Que faire ensuite

Vous pouvez désormais appliquer le nouvel emplacement configuré aux sources de données de votre système.

Rubriques d'aide

Sources de données - onglet Résolution d'entité :

L'onglet **Résolution d'entité** permet d'indiquer les détails de la résolution d'entité de la source de données.

Configuration de la résolution d'entité
Dans la liste, sélectionnez la configuration de résolution que cette source de données utilise lors du chargement de données.

Configuration de générateur de candidat
Dans la liste, sélectionnez la configuration de générateur de candidat utilisée pour le traitement de la résolution d'entités, lors du chargement des données à partir de cette source de données.

Valeur par défaut
Sélectionnez ce paramètre pour utiliser la configuration du générateur de candidat par défaut.

par défaut avec nom uniquement
Sélectionnez ce type de zone pour utiliser la configuration du générateur de candidat par défaut avec la concordance de nom uniquement.

Si vous souhaitez utiliser la fonction Name Hasher pour traiter les données de nom de cette source de données, sélectionnez cette configuration de générateur de candidat. (Vérifiez que les paramètres système de la fonction Name Hasher sont définis.)

Concordance de caractéristique
Dans la liste, sélectionnez **Oui** pour indiquer que des concordances de caractéristique sont traitées lors du chargement des données à partir de cette source de données. Sinon, sélectionnez **Non**.

Exécuter le détachement
Ce paramètre est généralement utilisé pour les systèmes d'hôtellerie.

Dans la liste, sélectionnez **Oui** pour indiquer que le pipeline peut établir la concordance des données sans la source de données. Si la concordance ne réussit pas, la date d'effacement est définie sur des données antérieures. Sinon, sélectionnez **Non**.

Niveau de correspondance du gestionnaire de noms
Dans la liste, sélectionnez la valeur du niveau de comparaison à utiliser lors du calcul du score des données de nom entrantes de cette source de données.

Valeur par défaut
Sélectionnez cette valeur pour utiliser le niveau de comparaison le plus courant pour la concordance de noms.

Eloignée
Sélectionnez cette valeur si vous souhaitez générer davantage de concordances de noms à partir de cette source de données. Cette valeur assouplit le niveau de concordance lors de la comparaison des noms afin que la comparaison soit moins stricte que la valeur par défaut.

Proche
Sélectionnez cette valeur si vous souhaitez générer moins de concordances de noms à partir de cette source de données. Cette valeur limite le niveau de concordance lors de la comparaison des noms afin que la comparaison soit plus stricte que la valeur par défaut.

Autoriser la non-résolution
La fonction de non résolution est un processus qui consiste à séparer les identités résolues en deux entités distinctes, en fonction de nouvelles informations provenant des données entrantes. Dans la liste, effectuez la sélection appropriée pour cette source de données :

- Sélectionnez **Oui** pour permettre à la fonction de résolution d'entité de diviser les identités en entités distinctes, lors du chargement des comptes de cette source de données.
- Sélectionnez **Non** pour empêcher à la fonction de résolution d'entité de diviser des identités en entités distinctes lors du chargement des comptes de cette source de données.

Sources de données - onglet Général :

L'onglet **Général** permet d'indiquer les détails de la source de données.

ID Tapez le numéro d'identifiant de la source de données que vous souhaitez créer.

Cet ID est un code numérique qui s'incrémente automatiquement. Bien que le produit fournisse le numéro disponible suivant dans l'ordre, vous pouvez attribuer à ce code une valeur numérique unique en entrant cette valeur dans la zone ID.

Code Tapez le code de la source de données que vous souhaitez créer.

Il s'agit de la valeur de la balise UMF `DSRC_CODE`. Le code de la source de données, qui peut être alphanumérique, sert à mieux identifier une source de données. Cette valeur, qui doit être unique, ne peut plus être modifiée une fois l'enregistrement sauvegardé.

Description
Tapez la description de la source de données que vous souhaitez créer.

Emplacement
Dans la liste déroulante, sélectionnez le code d'emplacement de la source de données que vous souhaitez créer.

Cette zone sert uniquement de référence.

Système source
Dans la liste déroulante, sélectionnez le code de système source de la source de données que vous souhaitez créer.

Cette zone sert uniquement de référence.

Etat Dans la liste déroulante, sélectionnez **Actif** pour indiquer que cette source de données est active. Sinon, sélectionnez **Inactif**.

Approuver l'action
Dans la liste déroulante, sélectionnez **Oui** pour indiquer que vous pouvez compter sur l'exactitude de la balise UMF `ACTION` issue de votre source de données. Sinon, sélectionnez **Non** pour détermine l'action en examinant la base de données d'entités. Le choix de **Non** entraîne une baisse de performance.

Pour la recherche
Dans la liste déroulante, sélectionnez **Oui** pour indiquer que cette source de données sert au chargement de recherches. Sinon, sélectionnez **Non**.

Translittération
Dans la liste déroulante, sélectionnez **Oui** pour indiquer que cette source de données doit faire l'objet d'une translittération. Cela permet la prise en charge du jeu de caractères Latin 1. Sinon, sélectionnez **Non**.

Remarque : Si vous activez le paramètre de translittération pour une source de données, vous devez également activer le paramètre de configuration de translittération pour la source de données portant l'ID 1589 (Recherche). La source de données 1589 est utilisée par le produit pour entrer des recherches dans le pipeline ; par défaut, les caractères ASCII sont employés. Le fait d'activer ce paramètre de configuration permet de s'assurer que les noms qui font partie de la recherche font également l'objet d'une translittération correcte, afin de fournir les résultats les plus précis possibles.

Sources de données - onglet Relations :

L'onglet **Relations** permet d'indiquer les détails de relation de la source de données.

Rôle Sélectionnez le code de rôle à attribuer à cette source de données.

Classe de source de données
Sélectionnez la classe de source de données appropriée de la source de données.

Chargement complet
Sélectionnez ce type de zone pour charger les données dans la base de données.

Ce réglage résout toute identité qu'il est possible de résoudre, met à jour l'entité, détecte toute relation éventuelle et déclenche les alertes définies par l'utilisateur.

Passivité complète
Sélectionnez ce type de zone pour ne pas charger les données dans la base de données.

Si vous effectuez un chargement en passivité complète, alors aucune donnée n'est stockée. Le Visualizer ne peut pas afficher l'alerte.

Chargement en cas de résolution/relation
Sélectionnez ce type de zone pour charger les données dans la base de données si elles se résolvent en, ou se rattachent à, des enregistrements existants de la base de données d'entité.

Ce réglage résout toute identité qu'il est possible de résoudre, met à jour l'entité, détecte toute relation éventuelle et déclenche les alertes définies par l'utilisateur.

Chargement en cas de résolution/relation sélective
Sélectionnez ce type de zone pour charger les données dans la base de données si elles se résolvent en, ou se rattachent à, des enregistrements existants de la base de données d'entité, uniquement si cette source de données est configurée dans la table SELECTIVE_PASSIVE_CONFIG.

Ce réglage résout toute identité qu'il est possible de résoudre, met à jour l'entité, détecte toute relation éventuelle et déclenche les alertes définies par l'utilisateur.

Chargement en cas de résolution sélective
Sélectionnez ce type de zone pour charger les données dans la base de données si elles se rattachent à des enregistrements existants de la base de données d'entité, uniquement si cette source de données est configurée dans la table SELECTIVE_PASSIVE_CONFIG.

Ce réglage résout toute identité qu'il est possible de résoudre, met à jour l'entité, détecte toute relation éventuelle et déclenche les alertes définies par l'utilisateur.

Niveau de séparation
Dans la liste déroulante, sélectionnez le niveau de séparation adéquat pour cette source de données.

Charger les données
Sélectionnez toujours ce type de zone. C'est actuellement la seule option disponible.

Configuration DoS
Dans la liste déroulante, sélectionnez la configuration de degrés de séparation adéquate pour cette source de données.

Les configurations de séparation se définissent dans l'écran **Configurer** > **Relations** > **Configuration de séparation**.

Emplacements - onglet Général :

L'onglet **Emplacements** permet d'indiquer les détails de l'emplacement de la source de données.

Code d'emplacement
Tapez le code d'emplacement à attribuer à cet emplacement de source de données.

Une valeur alphanumérique ne peut plus être modifiée une fois l'enregistrement sauvegardé.

Cette valeur est obligatoire.

Nom d'emplacement
Tapez le nom d'emplacement à attribuer à cet emplacement de source de données.

District
Tapez le district à attribuer à cet emplacement de source de données.

Cette valeur est obligatoire.

Société
Tapez le nom de société à attribuer à cet emplacement de source de données.

Latitude
Tapez la latitude de cet emplacement de source de données au format suivant :

DD:MM:SS

Longitude
Tapez la longitude de cet emplacement de source de données au format suivant :

DD:MM:SS

Etat Dans la liste déroulante, sélectionnez **Actif** pour indiquer que cet emplacement de source de données est actif. Sinon, sélectionnez **Inactif**.

Désactivation de la détection de relation

Si votre activité nécessite que vous sachiez uniquement qui est qui et non pas qui connaît qui, vous pouvez réduire le volume de traitement nécessaire à chaque fiche, et ainsi accélérer les performances globales du système, en configurant la résolution des relations pour qu'elle n'effectue que la résolution d'entité, sans détecter les relations entre entités.

Avant de commencer

Assurez-vous d'avoir sélectionné **Editer la configuration** quand vous vous êtes connecté à la session actuelle de la console de configuration.

Procédure

1. Désactivez les affectations de rôle pour chaque source de données.
   a. Cliquez sur **Configurer**.
   b. Cliquez sur **Sources**.
   c. Dans l'onglet **Sources de données**, cliquez sur la source à modifier.
   d. Cliquez sur l'onglet **Relations**.
   e. Dans la liste déroulante **Rôle**, choisissez **— Sélectionner une option —**.
   f. Dans la liste déroulante **Niveau de séparation**, choisissez **Alertes uniquement**.
   g. Cliquez sur **Enregistrer**.
2. Désactivez la règle de gestion de la qualité des données Affectations de rôle par défaut.
   a. Cliquez sur **Configurer**.

b. Cliquez sur **UMF**.
c. Dans la liste déroulante **Segment** de l'onglet **Règles DQM**, choisissez **ROOT**.
d. Cliquez dans la ligne sur un lien qui contienne la règle DQM 551, fonction Affectation de rôle par défaut.
e. Dans la liste déroulante **Etat** de l'onglet **Général**, choisissez **Inactif**.
f. Cliquez sur **Enregistrer**.

3. Supprimez toutes les règles de résolution qui ne sont pas configurées pour résoudre les entités.
   a. Cliquez sur **Configurer**.
   b. Cliquez sur **Résolution**.
   c. Cliquez sur l'onglet **Règles de résolution**.
   d. Dans la liste déroulante **Configuration de la résolution**, choisissez **DEFAULT**.
   e. Cochez la case de toute règle de résolution affichant la valeur **Non** dans la colonne **Résolution de déclencheurs**.
   f. Cliquez sur **Supprimer**.
   g. Cliquez sur **OK** pour confirmer que vous voulez supprimer les règles de résolution sélectionnées.
4. Enfin, supprimez les règles de conflit.
   a. Cliquez sur **Configurer**.
   b. Cliquez sur **Relations**.
   c. Cliquez sur l'onglet **Règles de conflit**.
   d. Cochez la case de chaque règle de conflit.
   e. Cliquez sur **Supprimer**.
   f. Cliquez sur **OK** pour confirmer que vous voulez supprimer les règles de conflit sélectionnées.

Que faire ensuite

Le système est désormais configuré pour résoudre les entités sans détecter les relations.

Configuration de types d'événements

Configurez des types d'événements pour définir et classer par catégories des événements traités par le gestionnaire d'événements. Toutefois, avant que le système traite les données entrantes contenant des types d'événements, vous devez obligatoirement activer le traitement d'événement dans les paramètres système du gestionnaire d'événements, configurer les règles métier dans l'outil de processeur d'événement complexe basé sur Eclipse et mettre en forme les données d'événement entrantes à l'aide des définitions de segment de données UMF EVENT.

Les types d'événement peuvent être visualisés et modifiés à l'aide de la console, dans l'onglet **Types d'événement**.

Types d'événements

Les types d'événements classent les événements par catégorie et définissent l'unité de mesure pour la valeur associée aux événements dans le gestionnaire d'événements. Quelques exemples de types d'événements : virement, ouverture de compte ou transaction par carte de crédit.

Les types d'événements sont requis pour le traitement d'événements car les règles métier définies par l'utilisateur, que le processeur d'événements utilise, exigent un type d'événement spécifique. Si le type d'événement n'existe pas, le processeur d'événements ne peut pas traiter l'événement en question.

Création de types d'événements

Lorsque vous souhaitez ajouter un nouveau scénario d'événements pour traiter les événements, il est possible que vous deviez créer un nouveau type d'événements pour définir les types de transactions ou d'activités inclus dans ce scénario d'événements, ainsi que l'unité de mesure associée à cette catégorie d'événements.

Avant de commencer

Le gestionnaire d'événements doit être activé pour votre système IBM InfoSphere Identity Insight.

Pourquoi et quand exécuter cette tâche

Les types d'événements sont appelés par le processeur d'événements complexes, alors qu'il traite les événements en fonction des règles métier définies par l'utilisateur. Pour qu'un type d'événements soit utilisé, vous devez au préalable créer également au moins une règle métier qui utilise ce type d'événements.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur le bouton **Type d'événements**.
4. Cliquez sur le bouton **Nouveau**.
5. Obligatoire : Sur l'onglet **Général**, indiquez le nom et la description du type d'événements, l'unité de mesure associée à ce type d'événements et le statut de ce type d'événements (actif ou inactif).
6. Facultatif : Vous pouvez également spécifier d'autres informations telles que la catégorie, la sous-catégorie et des remarques sur ce type d'événements.
7. Cliquez sur le bouton **Enregistrer**.

Edition de types d'événements

Editez un type d'événements lorsque vous souhaitez modifier la description, l'unité de mesure ou les informations complémentaires associées au type d'événements. Vous pouvez également désactiver un type d'événements afin qu'il ne soit plus utilisé. Vous ne pouvez pas modifier le nom du type d'événements.

Pourquoi et quand exécuter cette tâche

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur le bouton **Type d'événements**.
4. Sélectionnez le type d'événements que vous souhaitez éditer.
5. Sur l'onglet **Général**, effectuez les modifications.
6. Cliquez sur le bouton **Enregistrer**.

Que faire ensuite

Suppression de types d'événements

Vous pouvez supprimer un type d'événements qui n'est plus utilisé pour le traitement des événements. Si vous souhaitez conserver le type d'événements, et simplement le désactiver, vous pouvez modifier son statut au lieu de le supprimer.

Avant de commencer

Pourquoi et quand exécuter cette tâche

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Sources**.
3. Cliquez sur le bouton **Type d'événements**.
4. Cochez la case en regard du type d'événements que vous souhaitez supprimer.
5. Cliquez sur le bouton **Supprimer**.

Que faire ensuite

Rubriques d'aide

Types d'événement - onglet Général :

Cet onglet permet de définir ou d'éditer un type d'événement. Les types d'événements définissent et classent par catégories les événements et sont utilisés lors du traitement d'événement, si le gestionnaire d'événements est activé pour votre système.

Type Entrez un nom unique pour ce type d'événement. Par exemple, vous pouvez créer un type d'événement nommé `Transfert bancaire`.

Description
Entrez une description du type d'événement.

Unité de mesure
Entrez une abréviation pour l'unité de mesure de la valeur qui est associée au type d'événement. Par exemple, vous pouvez entrer `USD` pour U.S. dollars.

Etat Dans la liste déroulante, sélectionnez le statut du type d'événement, **Actif** ou **Inactif**. (Vous pouvez utiliser le statut **Inactif** pour supprimer le type d'événement du traitement d'événement, mais garder la configuration pour le type d'événement.)

Catégorie
Entrez un nom de catégorie facultatif pour le type d'événement.

Sous-catégorie
Entrez un nom de sous-catégorie en option pour le type d'événement.

En-tête de mémo 1
Entrez un en-tête de mémo 1 en option pour le type d'événement.

En-tête de mémo 2
Entrez un en-tête de mémo 2 en option pour le type d'événement.

Configuration de la résolution d'entité

La résolution d'entité est le processus qui recherche des relations dans les données. Les paramètres de configuration de la résolution d'entité sont organisés par groupes, appelés configurations de résolution. Cinq composants constituent une configuration de résolution : les règles de résolution, les confirmations & refus, les attributs, les configurations de correspondance du gestionnaire de noms et le générateur de candidat.

Résolution d'entité

La résolution d'entité désigne le processus qui résout les entités et détecte les relations. Les pipelines effectuent la résolution d'entité, à mesure qu'ils traitent les fiches d'identité entrantes, en trois phases : reconnaître, résoudre, apparenter.

Configuration des configurations de résolution

Tous les paramètres de résolution d'entité se gèrent dans une configuration de résolution, dont deux sont fournies par défaut.

Configurations de résolution

Les paramètres de résolution d'entité sont organisés par un groupe de configurations de résolution définies au moyen de la valeur Règle de résolution de chargement du système dans l'onglet **Configuration système** de la console de configuration.

L'installation par défaut de Relationship Resolution comporte deux configurations de résolution.

- **PAR DEFAUT** - paramètres de résolution par défaut appliqués dès que de nouvelles données issues d'une source définie parviennent au système.
- **RECHERCHE** - paramètres de résolution appliqués par le processus de recherche résolue dès qu'un utilisateur soumet une demande de recherche totalement résolue.

Vous pouvez créer votre propre jeu de paramètres de résolution et les identifier à l'aide d'une nouvelle configuration de résolution. Il faut pour cela d'abord cloner la configuration de résolution **PAR DEFAUT**, qui sert ensuite de point de départ de votre nouvelle configuration.

Des configurations de résolution différentes peuvent être attribuées à des sources de données spécifiques. Si vous choisissez d'appliquer plusieurs configurations de résolution sur plusieurs sources de données, vous devez tenir compte du fait que la résolution d'entité applique toujours la configuration de résolution attribuée à l'identité entrante lors du déclenchement des alertes. Ceci peut aboutir à des résultats d'alerte différents en fonction de laquelle des identités comparées est l'identité entrante et laquelle des identités existe déjà dans la base de données d'entités. Soit par exemple l'identité n°123, issue de la source de données Client et à laquelle est attribuée la configuration de résolution DEFAULT, qui contient une règle de résolution de nom et adresse dont le seuil de nom est 80, est le seul d'adresse 5. L'identité n°456, issue de la client Fournisseur, applique la configuration de résolution NEW, qui renferme la même règle de résolution, mais dont le seuil de nom est fixé à 95 et le seuil d'adresse à 7. Quand le client 123 est l'identité entrante et qu'il est comparé au fournisseur existant 456, le score de nom entre eux est calculé à 85 et le score d'adresse à 5, ce qui déclenche une alerte. Si l'ordre de traitement est inversé, le client 123 étant déjà présent dans le système et le fournisseur 456 y parvenant, ils continent à produire le même score de

résolution de 85 pour le nom et 5 pour l'adresse. Dans ce cas, il n'y aura toutefois aucune alerte car les scores de résolution ne satisfont pas les seuils de résolution de la configuration de résolution NEW, où le nom est réglé sur 95 et l'adresse sur 7.

Remarque :

L'utilisation d'une configuration de résolution d'entité autre que celle par défaut doit être effectuée et planifiée soigneusement. Les paramètres de résolution d'entité par défaut, notamment les règles de résolution et les paramètres de score, sont le fruit de centaines d'années-personne d'analyse et d'étude de données réelles. Les modifications de ces valeurs par défaut ne s'avèrent généralement nécessaires que lorsque les données ou les règles d'entreprise exigent des comportements particuliers et inhabituels de la part du système.

Consultation des configurations de résolution

Une configuration de résolution sert à désigner un ensemble de paramètres de résolution d'entité. Il est conseillé de consulter les configurations de résolution existantes si vous envisagez d'apporter des modifications à vos paramètres de résolution d'entité ou si vous souhaitez créer un nouvel ensemble de paramètres de résolution d'entité.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.

Clonage et personnalisation de la configuration de résolution par défaut

Le moyen idéal de créer une nouvelle configuration de résolution d'entité consiste à cloner (c'est-à-dire copier) la configuration de résolution par défaut, qui sert ensuite de point de départ de la nouvelle configuration. En préservant intacte la configuration par défaut, vous pouvez toujours la rétablir si nécessaire, sans avoir à réinstaller le produit.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.
3. Dans l'onglet **Configurations de résolution**, cochez la case en regard de la configuration de résolution par défaut.
4. Cliquez sur le bouton **Cloner**.
5. Dans la zone **Code** de l'onglet **Général**, tapez le nom de votre nouvelle configuration de résolution.
6. Dans la zone **Description**, tapez une nouvelle description de la configuration de résolution clonée.
7. Cliquez sur le bouton **Enregistrer**.

Que faire ensuite

Quand vous apportez des modifications aux paramètres de résolution d'entité, par exemple pour configurer des règles de résolution, les concordances et discordances ou le générateur de candidat, vous pourrez sélectionner votre nouvelle configuration de résolution.

Suppression de configurations de résolution personnalisées

Si vous n'utilisez plus une certaine configuration de résolution personnalisée, vous pouvez la supprimer. Par contre, ne supprimez pas la configuration de résolution par défaut ; en préservant intacte la configuration par défaut, vous pouvez toujours la rétablir si nécessaire, sans avoir à réinstaller le produit.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.
3. Dans l'onglet **Configurations de résolution**, cochez la case en regard de la configuration de résolution à supprimer.
4. Cliquez sur le bouton **Supprimer**.
5. Dans la fenêtre de confirmation, cliquez sur **OK** pour supprimer la configuration de résolution.

Que faire ensuite

Vous ne pouvez alors plus sélectionner cette configuration de résolution quand vous apportez des modifications aux paramètres de résolution d'entité. Par ailleurs, les paramètres de résolution d'entité concernant cette configuration de résolution ne peuvent plus être appliqués au processus de résolution d'entité.

Rubriques d'aide

Fenêtre Configurations de résolution :

Cette fenêtre vous permet de consulter la liste des configurations de résolution d'entité disponibles. Les paramètres de résolution d'entité sont organisés en groupes appelés configurations de résolution. Des configurations de résolution différentes peuvent être attribuées à des sources de données individuelles. A chaque source de données ne peut être appliquée qu'une seule configuration de résolution à la fois.

Code Nom de la configuration de résolution.

Description
Description de la configuration de résolution.

Configuration de règles de résolution

Pour définir comment des entités comparées se résolvent et sont apparentées, vous devez configurer des règles de résolution, dont des seuils de candidat et des seuils de concordance/discordance.

Pourquoi et quand exécuter cette tâche

Les règles de résolution peuvent être visualisées et modifiées à l'aide de la console, dans l'onglet **Règles de résolution**.

Règles de résolution

Les règles de résolution sont l'ensemble de critères qu'applique le système pour établir comment des entités comparées se résolvent (à savoir s'il s'agit ou non de la même entité) et se rattachent (à savoir, si elles ne se résolvent pas en une même entité, combien d'attributs elles partagent).

Quand vous définissez des règles de résolution, vous devez indiquer les seuils qui contribuent au score de résolution total, qui détermine si une identité entrante se résout en une entité existante.

- Les seuils de candidat indiquent quelles valeurs de données d'attributs sont comparées pour déterminer si une identité et une entité se résoudront en une seule entité composite. Le seuil est le score minimum auquel une valeur d'attribut particulière doit concorder entre l'identité entrante et une entité existante pour satisfaire la règle de résolution.
- Les seuils de concordance et discordance indiquent quelle pondération du score (positive ou négative) est appliquée aux valeurs de données d'attributs concordantes ou conflictuelles quand vous activez l'utilisation des discordances.

Vous pouvez également indiquer en quoi les valeurs conflictuelles des mêmes attributs affectent le score de résolution. Ces valeurs conflictuelles sont appelées discordances. Vous pouvez configurer des règles de résolution stipulant que la règle n'est pas satisfaite si les valeurs d'attributs présentent de quelconques conflits (discordances). Par ailleurs, vous pouvez moduler les seuils d'une règle de résolution afin de créer des discordances automatiques, en fonction des scores de comparaison qui ne satisfont les scores seuils désignés. Plus le score seuil fixé est élevé, plus la concordance doit être exacte pour satisfaire la règle de résolution.

Seuils de candidats

Les seuils de candidats constituent les premières parties d'une règle de résolution servant à déterminer si une identité entrante représente en fait une entité existante, ou une entité entièrement nouvelle.

Les seuils de candidats, qui se configurent à l'aide de la console, font partie intégrante d'une règle de résolution. Par exemple, si une règle de résolution possède un seuil de candidats à numéro unique, cette règle peut être décrite comme exigeant un numéro unique concordant.

Les seuils de candidats ne sont appliqués qu'aux entités existantes afin de placer cette entité dans la liste de candidats dans le cadre du processus de résolution d'entité. Le seuil effectif est le niveau minimum auquel un type de données particulier doit concorder entre une identité entrante et une entité existante pour que le processus de résolution d'entité ajoute l'entité existante à la liste de candidats.

Précision d'adresse :

La précision d'adresse désigne le barème appliqué par la résolution d'entité pour déterminer si deux adresses comparées représentent la même adresse.

La précision d'adresse se divise en neuf niveaux distincts (de 1 à 9). La plupart des adresses comportent des éléments fondamentaux qu'il est possible de comparer, notamment la rue (numéro compris), la localité, le code postal, et le code postal complémentaire. Lors de la comparaison de ces éléments, la précision d'adresse commence par un élément "rue" concordant et attribue un niveau de précision de 5. Ce niveau est ensuite modulé, à la hausse ou à la baisse, selon que les autres éléments concordent ou diffèrent. Chaque élément concordant augmente le niveau de précision de 1, chaque élément divergent le diminuant de 1. Si une valeur d'élément est présente dans une adresse alors qu'aucune n'est présente pour le même élément dans l'autre adresse, aucune modulation de la précision n'a lieu.

Par défaut, la résolution d'entité considère que les adresses comparées donnant un niveau de précision d'au moins 5 sont des adresses concordantes.

Tableau 29. Niveaux de précision d'adresse

Niveau	Description
1	1 : La rue correspond à toutes les parties, postal+4 différent. Cela signifie qu'il doit y avoir une adresse correspondant à toutes les parties, mais postal +4 est différent. Par exemple, 123 N Water St. Las Vegas, NV 89123-1234 et 123 S Water St. Las Vegas, NV 89123-5433.
2	Rue correspondante avec toutes les parties différentes. Cela signifie que seule la rue correspond, tandis que la ville, l'état, le code postal et le pays sont tous différents ou manquants. Par exemple, 123 Main St. Orlando, FL 32555 et 123 Main St. Las Vegas, NV
3	Rue correspondante avec modificateur de différence -2. Cela signifie que la rue correspond, mais que le résultat du calcul est -2. Par exemple, 123 Main St. Las Vegas, NV 89111 et 123 Main St. Las Cruces, NM.
4	Rue correspondante avec modificateur de différence -1. Cela signifie que la rue correspond, mais que le résultat du calcul est -1. Par exemple, 123 Main St. Las Vegas, NV 89111 et 123 Main St. Las Vegas, NM 54633.
5	Rue correspondante avec modificateur 0 (référence). Cela signifie que la rue correspond, mais que le résultat du calcul est 0. Par exemple, 123 Main St. Las Vegas, NV 89111 et 123 Main St.
6	Rue correspondante avec modificateur de correspondance +1. Cela signifie que la rue correspond, mais que le résultat du calcul est +1. 123 Main St. Las Vegas, NV 89111 et 123 Main St. Las Vegas
7	Rue correspondante avec modificateur de correspondance +2. Cela signifie que la rue correspond, mais que le résultat du calcul est +2. Par exemple, 123 Main St. Las Vegas, NV 89111 et 123 Main St. Las Vegas, NV.
8	Rue correspondante avec toutes les parties différentes, postal +4 manquant. Cela signifie que toutes les parties de l'adresse concordent, à part postal +4 qui n'est pas présent. Par exemple, 123 Main St. Las Vegas, NV 89111 et 123 Main St. Las Vegas, NV 89111
9	Correspondance exacte (rue avec toutes les parties). Cette sélection signifie que toutes les parties de l'adresse concordent, y compris postal +4. Par exemple, 123 Main St. Las Vegas, NV 89111-1234 et 123 Main St. Las Vegas, NV 89111-1234 **Remarque :** Cela ne fonctionne pas avec les codes postaux étrangers où les codes +4 sont inusités.

Niveau de précision 1

Chaque niveau de précision, de 1 à 9, représente un niveau de précision croissant, à l'exception du niveau 1. Ce niveau est un cas spécial dans la mesure où les informations d'adresse peuvent être identiques à l'exception de la désignation de rue North/South (Nord/Sud) ou East/West (Est/Ouest), telle que 456 North Main Street Sometown, Nevada et 456 South Main Street Sometown, Nevada. Dans ce cas, les adresses peuvent être identiques, mais le code postal+4 est assurément différent. Apparemment, ces adresses semblent devoir être converties. En fait, elles ne peuvent pas l'être, car il s'agit d'adresses différentes. Ce cas apparemment manifeste de nécessité de convertir les adresses étant en fait un net cas où il ne faut surtout pas, la valeur attribuée au niveau de précision de ce scénario est la plus basse (niveau 1) afin d'empêcher la conversion.

le niveau peut également indiquer une adresse délibérément erronée. Dans une intention de duperie, certains clients voient un intérêt à commettre systématiquement une erreur délibérée dans leur adresse. C'est pourquoi il est possible de configurer l'ordre des règles de résolution afin de considérer un niveau de précision d'adresse faible tel que le niveau 1.

Remarque : Si le niveau 1 présente un intérêt dans la résolution d'entités (par exemple si vous voulez savoir si une personne fournit des informations d'adresse incompatibles au niveau du code postal+ 4), vous devez créer une règle de résolution d'entité distincte. Cette règle doit précéder la règle de résolution par défaut qui prend en compte tous les niveaux de précision égaux et supérieurs à 5. Du fait de la complexité de la création de règles de résolution, il est recommandé de ne s'y livrer soit qu'avec l'expérience suffisante, soit avec l'aide d'IBM.

Exemples détaillés de précision d'adresse :

Les exemples suivants représentent les données comparées et les scores de précision d'adresse qui en découlent.

La première adresse représente l'adresse existante dans la base de données d'entités, et la seconde est l'adresse entrante.

Niveau 1 - La rue correspond à toutes les parties, postal+4 différent.

Cet exemple montre deux adresses qui se trouvent dans la même rue, mais qui correspondent à deux adresses différentes. L'une des adresses se trouve au nord de la rue et l'autre au sud. La seule différence entre ces deux adresses résident dans les valeurs du code ZIP+ 4.

RUE	VILLE	ETAT	CODE POSTAL
123 N Main St	Fairmount	IN	46928-1655
123 S Main St	Fairmount	IN	46928-1924

Remarque : Le niveau de précision est un cas spécial dans la mesure où les informations d'adresse sont identiques à l'exception de la désignation North/South (nord/sud) ou East/West (est/ouest). Apparemment, ces adresses peuvent être converties. En fait, elles ne peuvent pas l'être, car il s'agit d'adresses différentes. Ce cas apparemment manifeste de nécessité de convertir les adresses étant en fait un cas flagrant où il ne faut surtout pas, la valeur de ce scénario est fixée au bas de l'échelle (1) afin d'empêcher la conversion.

Niveau 2 - Rue correspondante avec toutes les parties différentes.

Cet exemple montre deux adresses ayant les mêmes informations de rue, mais des villes, un état et un code postal différents. A l'évidence, la seconde adresse est erronée (erreur éventuellement délibérée) du fait que tous les codes postaux du Nevada commence par 89.

RUE	VILLE	ETAT	CODE POSTAL
123 E Main St	Fairmount	IN	46928
123 S Main St	Las Vegas	NV	46999

Niveau 3 - Rue correspondante avec modificateur de différence -2.

Dans cet exemple, seules les informations de rue concordent. Aucune information d'état n'est fourni dans l'adresse entrante, et les informations de ville et de code postal sont incompatibles.

RUE	VILLE	ETAT	CODE POSTAL
123 E Main St	Delphi	IN	46923-1522
123 E Main St	Fairmount		46928

Niveau 4 - Rue correspondante avec modificateur de différence -1.

Cet exemple montre deux adresses ayant les mêmes informations de rue et d'état, mais des informations de ville et de code postal différentes.

RUE	VILLE	ETAT	CODE POSTAL
123 E Main St	Delphi	IN	46923-1522
123 E Main St	Fairmount	IN	46928-1924

Niveau 5 - Rue correspondante avec modificateur 0 (référence).

Dans cet exemple, seules les informations de rue sont fournies dans l'adresse entrante. Même si la correspondance ne contient pas d'informations de ville, d'état ou de code postal, elle reçoit le score de précision d'adresse de base (5). Le score de précision reflète les parties manquantes (à ne pas confondre avec des parties incompatibles du fait que les parties manquantes ne sont pas affectées d'un score).

RUE	VILLE	ETAT	CODE POSTAL
220 JEFFERSON	BUFFALO	IA	
220 Jefferson St.			

Niveau 6 - Rue correspondante avec modificateur de correspondance +1.

Cet exemple montre une adresse de domicile entrante sans état ou code postal, mais ayant des informations de rue et de ville correspondantes. Il semble que l'adresse entrante soit correcte, mais il manque des données.

RUE	VILLE	ETAT	CODE POSTAL
220 Washington	Syracuse	NY	
220 Washington Sq.	Syracuse		

Niveau 7 - Rue correspondante avec modificateur de correspondance +2.

Cet exemple montre une correspondance de rue, de ville et de code postal simple sans information d'état dans l'adresse entrante.

RUE	VILLE	ETAT	CODE POSTAL
220 JEFFERSON	BUFFALO	IA	52728
220 Jefferson St.	Buffalo		52728

Niveau 8 - Rue correspondante avec toutes les parties différentes, postal+4 manquant.

Dans cet exemple, deux adresses sont identiques, mais la standardisation d'adresse n'a pas pu les valider, car elles n'ont pas de code Zip+4.

RUE	VILLE	ETAT	CODE POSTAL
220 JEFFERSON	BUFFALO	IA	52728
220 Jefferson St.	Buffalo	IA	52728

Niveau 9 - Correspondance exacte (rue avec toutes les parties). Cette sélection signifie que toutes les parties de l'adresse concordent, y compris code postal +4.

Dans cet exemple, deux adresses correspondent au même domicile, à la même ville, au même état et au même code ZIP+ 4. Par conséquent, les adresses comparées reçoivent le score de précision d'adresse le plus élevé.

Remarque : Cela ne fonctionne pas avec les codes postaux internationaux dans lesquels les codes +4 ne sont pas utilisés.

RUE	VILLE	ETAT	CODE POSTAL
123 W Main St	Camden	IN	46917-9997
123 W Main	Camden	IN	46917-9997

Précision de nom :

La précision de nom désigne le barème appliqué par la résolution d'entité pour déterminer si deux noms comparés représentent le même nom.

Le barème de précision du nom repose sur l'utilisation de deux algorithmes possibles.

- Name Comparator 1.0
- Name Comparator 2.0

Chaque algorithme possède son propre jeu de critères de concordance de nom, disponibles pour configuration dans le cadre de la configuration des règles de résolution.

Ces algorithmes fonctionnent tous deux avec la fonction Gestionnaire de noms. Le gestionnaire de noms est une fonction configurable à part qui enrichit la concordance de nom au moyen de capacités complémentaires fondées sur des considérations culturelles uniques.

Considérations diverses sur la comparaison

Name Comparator 1.0 est le paramètre par défaut des installations mises à niveau à partir des versions 3.9.0 et antérieures. Name Comparator 2.0 est le paramètre par défaut des installations mises à niveau à partir des versions 3.9.1 et antérieures, ainsi que des nouvelles installations.

Quand vous réfléchissez à l'algorithme qui convient le mieux à vos besoins, tenez compte des avantages propres à chacun.

Name Comparator 1.0 :

- Sollicite moins l'unité centrale, d'où des performances plus rapides
- Permet de cerner plus précisément pourquoi des noms concordent

Name Comparator 2.0 :

- Gère plus efficacement les noms comportant plus de trois mots
- Repère plus efficacement les concordances entre mots désordonnés
- Applique plus efficacement la concordance floue
- Repère plus efficacement les concordances entre noms d'organismes
- Gère mieux les initiales

Name Comparator 1.0 :

Cet algorithme de concordance de nom est conçu pour traiter principalement les noms composés de deux ou trois mots. Il s'agit du paramètre de concordance de nom par défaut des mises à niveau des versions 3.9.0 et antérieures.

Name Comparator 1.0 compare deux noms, puis classe leur ressemblance selon 15 niveaux de similitude.

Tableau 30. Name Comparator 1.0 - niveaux de précision

Niveau	**Description**
1	Concordance partielle sur le prénom ou le nom uniquement EXEMPLE : John Jacob Smith = Joe Smithson
2	Concordance exacte sur le prénom ou le nom uniquement EXEMPLE : John Jacob Smith = Jonathan Henry Smith
3	Concordance de hachage proche EXEMPLE : Joe Smith = Joe Snith
4	Seuls les noms diffèrent, mais pas dans l'ordre EXEMPLE : Bob Jacob Smith = Jacob Bob Jones
5	Seuls les noms sont différents EXEMPLE : Bob Jacob Smith = Bob Jacob Jones
6	Concordance de nom standardisée avec quelques différences EXEMPLE : John Jacob Smith = Jonathan Henry Smith
7	Concordance de noms standardisée EXEMPLE : Joe W Anderson = Joseph Andersen
8	Concordance standardisée avec noms exacts, concordance de l'initiale du deuxième prénom, mais dans un ordre différent EXEMPLE : J Bob Smith = Robert J Smith
9	Concordance standardisée avec concordance exacte des noms et de l'initiale du deuxième prénom EXEMPLE : Joe W Anderson = Joseph W Anderson

Tableau 30. Name Comparator 1.0 - niveaux de précision (suite)

10	Concordance standardisée avec noms exacts, mais dans un ordre différent EXEMPLE : Bob Smith = Robert Smith
11	Concordance standardisée avec noms exacts EXEMPLE : John Jacob Smith = Johnny Jake Smith
12	Concordances de noms bruts avec concordance d'initiale de deuxième prénom, mais dans un ordre différent EXEMPLE : Joe W. Brown = Will Joe Brown
13	Concordance de noms bruts avec concordance d'initiale de deuxième prénom EXEMPLE : Joe W Anderson = Joe W Anderson
14	Concordance de noms bruts, mais dans un ordre différent EXEMPLE : John Bob Smith = Bob John Smith
15	Concordance de noms bruts EXEMPLE : Joe William Anderson = Joe William Anderson

Name Comparator 2.0 :

Cet algorithme de concordance de nom est conçu pour scinder les noms comparés : il décompose le groupe de mots de la chaîne de noms en noms individuels, ou composantes. Il compare ensuite ces composantes et attribue un score à chacune d'elles. Il s'agit du paramètre de concordance de nom par défaut des installations mises à niveau à partir des versions 3.9.1 et antérieures, ainsi que des nouvelles installations.

Name Comparator 2.0 regroupe les noms en trois catégories qu'il compare et auxquelles il attribue un score :

- Prénom (prénom et initiale – ou tous les mots à l'exception du nom)
- Nom de famille (nom)
- Nom complet (tous les mots)

Ces trois catégories d'évaluation permettent de régler la concordance de noms en fonction de règles de résolution particulières aptes à satisfaire vos impératifs de concordance. Les scores sont basés sur des entiers, de 0 à 100, 0 étant le score le plus bas et 100 le plus élevé. Plus le score est élevé dans une catégorie, plus les noms de cette catégories concordaient.

Considérations diverses sur la configuration - directives sur le calcul de score

Dès que vous remaniez ou modifiez les paramètres de concordance de nom de Name Comparator 2, suivez ces directives pour configurer plus aisément les seuils de nom des règles de résolution. Ces directives s'avèrent également pratiques au moment de l'interprétation des résultats des catégories de score de cet algorithme.

Score du nom complet

En fonction du score de 0 à 100, les directives suivantes vous aideront à déterminer le niveau de concordance du score du nom complet :

- 100 = concordance exacte

- 90 = très bonne concordance (convient à la résolution du nom et de la date de naissance)
- 80 = bonne concordance (convient à la plupart des règles de résolution)
- 70 = concordance moyenne (convient lorsque des numéros uniques sont également présents)
- Inférieur à 70 = ne convient pas à la concordance

Score du prénom
En fonction du score de 0 à 100, les directives suivantes vous aideront à déterminer le niveau de concordance du score du prénom :

- 100 = concordance exacte
- 90 = très bonne concordance (pourrait révéler une permutation prénom-nom)
- 85 = concordance acceptable minimum
- Inférieur à 85 = ne convient pas à la concordance ; peut être utile en combinaison avec le prénom ou le nom pour assurer une certaine similarité

Score du nom
En fonction du score de 0 à 100, les directives suivantes vous aideront à déterminer le niveau de concordance du score du nom :

- 100 = concordance exacte
- 90 = très bonne concordance (pourrait révéler une permutation prénom-nom)
- 85 = concordance acceptable minimum
- Inférieur à 85 = ne convient pas pour la correspondance ; peut être utile en combinaison avec le prénom ou le nom pour assurer une certaine similarité

calcul du score d'un nom à l'aide du gestionnaire de noms :

L'algorithme du gestionnaire de noms calcule le score des données de nom entrantes en décomposant le nom en différentes parties, puis en déterminant la culture de chaque partie. Il calcule ensuite le score de chaque partie et les scores obtenus sont utilisés lors de la résolution d'entités.

L'algorithme du gestionnaire de noms fonctionne indépendamment des algorithmes du composant Name Comparator mais vous devez quand même sélectionner NC1 ou NC2. Pendant le processus de résolution d'entité, le score des noms est tout d'abord calculé selon les algorithmes de comparateur de nom sélectionné. Si le score indique une concordance parfaite, la procédure de résolution d'entité ignore le calcul du score effectué par le gestionnaire de noms car la concordance parfaite du nom respecte la partie régissant le score dans la règle de résolution. En revanche, s'il n'y a pas de concordance parfaite pour le nom entrant, la procédure de résolution d'entité calcule le score à l'aide de l'algorithme du gestionnaire de noms.

L'algorithme analyse et décompose le nom en différentes parties (prénom, nom et nom complet), puis détermine la culture pour chaque partie du nom. L'algorithme affecte un score à chaque partie du nom et compare ces scores aux seuils configurés dans le gestionnaire de noms pour déterminer le niveau de concordance des noms. Plus le seuil du score défini est élevé, plus les parties du nom provenant des données de nom entrantes doivent être proches des parties du nom de l'entité existante dans la base de données d'entités.

Précision de la date de naissance :

La précision de date de naissance désigne le barème appliqué par la résolution d'entité pour déterminer si deux dates de naissance comparées représentent la même date.

Cette comparaison tient compte de diverses mesures de similitude des chaînes de dates de naissance, notamment : positions des entiers, transpositions et delta de jour, mois et année. Les mesures sont analysées pour déterminer un score de similarité compris entre 2 et 100. Vous pouvez configurer les paramètres de précision de date de naissance en fonction de quatre catégories de similitude :

- Exacte - concordance à 100 points
- Etroite - > = concordance à 90 points
- Moyenne - > = concordance à 85 points
- Vague - > = concordance à 80 points

Considérations sur les configurations

Le système est préconfiguré sur la valeur Etroite comme niveau minimum de similitude pour qu'une règle de résolution considère que deux dates de naissance comparées sont la même. La modification de cette valeur affecte le nombre de concordances et peut donc se répercuter sur le nombre de résolutions d'entité accompli par le système. Réfléchissez soigneusement avant toute modification de ce paramètre et veillez à la tester avant de la mettre en oeuvre en environnement de production.

Exemples détaillés de précision de la date de naissance :
Les exemples suivants représentent les données comparées et les scores de précision de date de naissance qui en découlent. La première date de naissance représente la date de naissance existante d'une entité de la base de données d'entités, tandis que la seconde correspond à une identité de date de naissance entrante.

Niveau de précision : exact (100 points)

Cet exemple montre deux dates exactes. L'algorithme génère une correspondance à 100 points.

DATE DE NAISSANCE	ETAT
1963/12/01	Existante
1963/12/01	Entrante

Niveau de précision : Proche (90 points)

Cet exemple montre deux dates dont le score de précision est supérieur ou égal à 90 points. L'exemple contient deux dates de naissance ayant la même année et le même jour, mais un mois de différence.

DATE DE NAISSANCE	ETAT
1963/12/01	Existante
1963/11/01	Entrante

Niveau de précision : Moyen (85 points)

Cet exemple montre deux dates dont le score de précision est supérieur ou égal à 85 points. Cet exemple contient deux dates de naissance ayant le même mois et le même jour, mais les deux derniers chiffres de l'année inversés.

DATE DE NAISSANCE	ETAT
1963/12/01	Existante
1936/12/01	Entrante

Niveau de précision : Eloigné (80 points)

Cet exemple montre deux dates dont le niveau de précision est supérieur ou égal à 80 points. L'exemple comporte deux dates de naissance dont le mois et le jour sont identiques, mais dont le troisième chiffre de l'année est incorrect (tout en restant valable comme date de naissance).

DATE DE NAISSANCE	ETAT
1963/12/01	Existante
1933/12/01	Entrante

Consultation des règles de résolution

Avant d'ajouter ou de supprimer des règles de résolution, vous pouvez consulter l'ensemble de règles de résolution actuel.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.
3. Cliquez sur l'onglet **Règles de résolution**.
4. Dans la liste déroulante **Configuration de la résolution**, sélectionnez une configuration de résolution.
5. Pour afficher le détail de règles de résolution précises, cliquez sur le lien dans la ligne où figure la règle de résolution que vous souhaitez consulter.

Création des règles de résolution

Après mûre réflexion sur vos impératifs professionnels et examen minutieux des règles de résolution existantes, il se peut que vous décidiez de créer de nouvelles règles de résolution pour vos données.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.
3. Cliquez sur l'onglet **Règles de résolution**.
4. Dans la liste déroulante **Configuration de la résolution**, sélectionnez une configuration de résolution.
5. Cliquez sur le bouton **Nouveau**.
6. Dans l'onglet **Général**, indiquez les valeurs à appliquer lors de la comparaison des données de deux entités.
7. Cliquez sur l'onglet **Seuils de candidats**.
8. Dans l'onglet **Seuils de candidats**, indiquez les valeurs de seuil des données.

9. Cliquez sur l'onglet **Seuils de concordance/discordance**.
10. Dans l'onglet **Seuils de concordance/discordance**, indiquez les valeurs de seuil des données.
11. Cliquez sur le bouton **Enregistrer**.

Suppression de règles de résolution

Pour enlever une règle de résolution de sorte qu'elle ne soit plus prise compte au cours du processus de résolution d'entité, supprimez-la

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.
3. Cliquez sur l'onglet **Règles de résolution**.
4. Dans la liste déroulante **Configuration de la résolution**, sélectionnez une configuration de résolution.
5. Cochez la case des règles de résolution à supprimer.
6. Cliquez sur le bouton **Supprimer**.
7. Dans la fenêtre de confirmation, cliquez sur **OK** pour supprimer la configuration de résolution.

Rubriques d'aide

Fenêtre Règles de résolution :

Cet écran permet de consulter les règles de résolution présentes dans une configuration de configuration. Les règles de résolution sont traitées dans l'ordre indiqué. Une fois qu'une règle de résolution est satisfaite, les scores de résolution attribués sont appliqués, et si la règle est configurée pour déclencher une résolution, l'identité entrante se résout en l'entité existante, et plus aucune autre règle de résolution d'entité n'est considérée pour cette comparaison particulière.

Ordre Ordre dans lequel les règles de résolution sont appliquées à l'identité entrante et à l'entité existante comparées

Description
Description de la règle de résolution

Niveau de fiabilité de résolution
Score de résolution appliqué à la comparaison si la règle est satisfaite

Niveau de fiabilité de relation
Score de relation appliqué à la comparaison si la règle est satisfaite

Résolution de déclencheurs
Indique si la règle résout automatiquement l'identité entrante en l'entité existante si la règle est satisfaite

Règles de résolution - onglet Général :

Cet onglet permet de configurer une nouvelle règle de résolution ou de consulter le détail d'une règle de résolution existante.

Ordre Saisissez un numéro unique indiquant l'ordre dans lequel traiter la règle.

Description
Saisissez la description de la règle.

Niveau de fiabilité de résolution
Saisissez un pourcentage de niveau de fiabilité de la ressemblance si cette règle réussit. Seul 100 % sera considéré pour la résolution.

Niveau de fiabilité de relation
Saisissez un pourcentage de niveau de fiabilité de la relation si cette règle réussit. Seul 100 % sera considéré pour la résolution.

Résolution de déclencheurs
Sélectionnez Oui pour résoudre l'identité entrante et l'entité existante si le niveau de fiabilité de résolution et de relation est de 100%.

Discordances activées
Sélectionnez "Oui" pour activer le traitement des concordances/ discordances. Sinon, aucun traitement des discordances n'aura lieu.

Discordances de caractéristiques activé
Sélectionnez "Oui" pour activer le traitement des concordances/ discordances de caractéristique. Sinon, aucun traitement des discordances de caractéristique n'aura lieu.

Règles de résolution - onglet Seuils de candidats :

Cet onglet permet soit d'indiquer les paramètres de seuils de candidats de nouvelles règles de résolution, soit de consulter les détails sur les seuils de candidats d'une règle de résolution existante. Ces paramètres définissent la **description** de règle de résolution saisie dans l'onglet Résolution **Général**.

Seuil de précision d'adresse
Sélectionnez le classement d'adresse minimum exigé pour que la règle soit considérée comme satisfaite.

Seuil d'adresse approximative
Sélectionnez le nombre minimum de concordances de valeur d'adresse approximative exigé pour que la règle soit considérée comme satisfaite.

Seuil de proximité
Sélectionnez le nombre minimum d'adresses, au sein de la zone définie dans la règle de qualité, exigé pour que la règle soit considérée comme satisfaite.

Seuil de numéro unique
Sélectionnez le nombre minimum de concordances de numéro unique exigé pour que la règle soit considérée comme satisfaite.

Seuil de numéro non unique
Sélectionnez le nombre minimum de concordances de numéro non unique exigé pour que la règle soit considérée comme satisfaite.

Seuil de caractéristique
Sélectionnez le nombre minimum de concordances de caractéristique exigé pour que la règle soit considérée comme satisfaite.

Seuil de courriel
Sélectionnez le nombre minimum de concordances de courriel exigé pour que la règle soit considérée comme satisfaite.

Seuil de données récapitulatives
Sélectionnez la somme minimum de concordances de numéro unique, autre numéro, adresse, caractéristique et courriel exigée pour que la règle soit considérée comme satisfaite.

Seuil récapitulatif
Sélectionnez la somme minimum de concordances de proximité d'adresse, adresse approximative, numéro proche et date de naissance exigée pour que la règle soit considérée comme satisfaite.

Règles de résolution - onglet Seuil de concordance/discordance :

Cet onglet permet de définir les paramètres des seuils de concordance ou discordance d'une nouvelle règle de résolution ou d'afficher les détails des seuils de concordance ou discordance d'une règle de résolution existante.

Seuil de numéro proche
Sélectionnez le nombre minimum de concordances de numéro proche exigé pour que la règle soit considérée comme satisfaite.

Seuil de date de naissance
Sélectionnez le score de concordance minimal de la date de naissance pour que la règle soit considérée comme respectée.

Paramètres de Name Comparator
Ces paramètres déterminent les critères de précision de nom de la résolution d'entité. Ces paramètres fonctionnent soit tout seuls, soit avec les paramètres de gestionnaire de noms.

Seuil de score du prénom
Entrez le seuil de score du prénom en indiquant une valeur comprise entre 0 et 100.

Seuil de score du nom
Entrez le seuil de score du nom de famille en indiquant une valeur comprise entre 0 et 100.

Seuil de score du nom complet
Entrez le seuil de score du nom complet en indiquant une valeur comprise entre 0 et 100.

Paramètres du gestionnaire de noms
Le gestionnaire de noms étend la précision des noms standard pour tenir compte d'importantes considérations culturelles. Ces paramètres s'appliquent uniquement si vous avez configuré le gestionnaire de noms.

Seuil de score du prénom
Entrez le score minimal du prénom pour que la règle soit considérée comme respectée.

Le seuil doit être une valeur de type entier comprise entre 0 et 100. Plus le score est élevé, plus la concordance est exacte. Par exemple, un score inférieur à 70 ne convient pas pour la correspondance, mais peut être utile en combinaison avec le nom ou le nom complet pour assurer une certaine similarité.

Seuil de score du nom
Entrez le score minimum de nom pour que la règle soit considérée comme respectée.

Le seuil doit être une valeur de type entier comprise entre 0 et 100. Plus le score est élevé, plus la concordance est exacte. Par exemple, un score inférieur à 70 ne convient pas pour la correspondance, mais peut être utile en combinaison avec le prénom ou le nom complet pour assurer une certaine similarité.

Seuil de score du nom complet

Entrez le score minimal du nom complet pour que la règle soit considérée comme respectée.

Le seuil doit être une valeur de type entier comprise entre 0 et 100. Plus le score est élevé, plus la concordance est exacte. Par exemple, un score inférieur à 70 ne convient pas pour la correspondance.

Personnalisation du générateur de candidat

Vous pouvez modifier les paramètres du générateur de candidat au moyen de configurations du générateur de candidat. Les modifications de la fonction de générateur de candidat s'effectuent au moyen de la console de configuration.

Générateur de candidats

La fonction de générateur de candidats définit les critères que le système applique pour ajouter une entité existante à la liste de candidats dans le cadre du processus de résolution d'entité.

Parmi les paramètres de générateur de candidats typiques figurent l'adresse, les numéros uniques, ainsi que les autres numéros. Il s'agit des types de données que le système compare afin de déterminer quelles entités existantes sont susceptibles de se résoudre en identité entrante. Dès qu'une nouvelle fiche d'identité parvient dans le système, si une entité existante comporte une valeur concordante pour n'importe lequel des types de données identifiés par le générateur de candidats, cette entité est ajoutée à la liste de candidats.

Configurations du générateur de candidats

Les paramètres du générateur de candidats sont organisés par groupes appelés configurations du générateur de candidats. Une seule configuration peut être utilisée au sein d'une configuration de résolution.

Les configurations du générateur de candidats incluses avec le produit sont les suivantes :

- **Par défaut** - ce paramètre inclut l'adresse, le numéro unique et d'autres numéros comme critères d'inclusion d'une entité dans la liste des candidats.
- **Par défaut avec nom uniquement** - ce paramètre inclut les noms comme critère d'inclusion d'une entité dans la liste des candidats. Ce paramètre est destiné à servir lorsque les données de votre entité sont susceptibles de ne contenir que des noms ou des noms et très peu d'autres types de données.

Considérations sur les configurations

Les valeurs génériques déterminent si une valeur est considérée dans le cadre du processus générateur de candidats. Une fois qu'une valeur est considérée comme générique, elle n'est plus utilisée pour générer des listes de candidats.

Les paramètres du générateur de candidats affectent directement les performances du système. Quand le système, par consultations de l'index, compare une identité entrante à chacune des entités de la base de données, il ne compare que les types de données configurés dans la fonction de générateur de candidats. Ceci permet de générer très rapidement les listes de candidats. A mesure que la base de données s'étoffe et compte de plus en plus d'entités, le volume de données que le générateur de candidats doit comparer augmente. Par exemple, si votre base de données compte 100 000 entités est que le générateur de candidats est réglé pour comparer trois types de données lors de la création de la liste de candidats, dès

qu'une nouvelle identité parvient dans le système, celui-ci peut réaliser jusqu'à 300 000 comparaisons simplement pour générer la liste de candidats. Si votre base de données compte 1 000 000 d'entités est que le générateur de candidats est réglé pour comparer trois types de données lors de la création de la liste de candidats, dès qu'une nouvelle identité parvient dans le système, celui-ci peut réaliser jusqu'à 3 000 000 comparaisons simplement pour générer la liste de candidats. Si vous n'ajoutez ne serait-ce qu'un seul critère au générateur de candidats, le système peut effectuer jusqu'à 1 000 000 comparaisons supplémentaires rien que pour établir la liste de candidats, à savoir jusqu'à 1 000 000 de comparaisons supplémentaires par fiche d'identité chargée dans le système. Si les listes de candidats sont trop volumineuses car elles prennent en compte un nombre excessif de types de données, le processus de résolution d'entité fonctionne bien plus lentement que si les paramètres du générateur ne contiennent que les types de données nécessaires à l'élaboration de listes de candidats efficaces.

Lorsque vous réfléchissez au choix entre les paramètres de configuration **Par défaut** et **Par défaut avec nom uniquement**, songez bien que si vous optez pour **Par défaut avec nom uniquement**, vous ajoutez des comparaisons dans un ordre de grandeur supérieur à celles nécessaires à la configuration **Par défaut**.

Listes de candidats

Les listes de candidats sont les listes des entités possédant le potentiel pour concorder avec la fiche d'identité entrante. La liste de candidats s'élabore en récupérant les entités qui partagent des attributs avec l'identité entrante, en fonction des attributs indiqués dans la configuration du générateur de candidats.

Le processus de résolution d'entité n'utilise les entités de la liste de candidats que pour résoudre les entités et les relations.

La résolution d'entité et la détection de relation étant déterminées en fonction d'attributs, il convient d'étudier soigneusement les attributs de vos sources de données afin de déterminer lesquels engendrent les candidats les mieux qualifiés.

Une fois la liste de candidats générée, le processus de résolution d'entité compare l'identité entrante au premier candidat de la liste, au moyen des règles de résolution configurées. Le système applique les règles de résolution, dans l'ordre, pour calculer un score de résolution qui indique quel est le degré de concordance entre les attributs de l'identité entrante et ceux de l'entité candidate. Si les attributs de l'identité entrante atteignent ou dépassent le score de résolution de cette règle, la fiche d'identité entrante est résolue dans l'entité candidate.

Si en revanche le score de résolution n'atteint pas celui fixé pour cette règle de résolution, le système passe à la règle suivante jusqu'à ce que la fiche d'identité entrante ait été résolue en une entité candidate et que toutes les règles de résolution ait été épuisées.

Si la fiche d'identité entrante n'est pas résolue en une entité existante, le système résout la fiche en une nouvelle entité et stocke cette dernière dans la base de données.

Création de configurations du générateur de candidats

A l'aide de la console de configuration, vous pouvez créer de nouveaux groupes de paramètres du générateur de candidat. Ces configurations du générateur de candidats s'avèrent commodes comme moyen simple d'appliquer une palette de paramètres de générateur de candidat configurés en ne modifiant qu'un seul paramètre.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.
3. Cliquez sur l'onglet **Générateur de candidat**.
4. Assurez-vous que la liste déroulante **Configuration de générateur de candidat** affiche **- - - Sélectionner une option - - -**, puis cliquez sur le bouton **Nouveau**.
5. Dans la zone **Configuration de générateur de candidat**, tapez le nom de la nouvelle configuration du générateur de candidat.
6. Dans la zone **Type de correspondance**, choisissez le premier type de données que vous souhaitez appliquer comme critère candidat pour la résolution.
7. Dans la zone **Nom du segment**, tapez le nom du segment UMF où se trouvent les données du type de concordance.
8. Cliquez sur le bouton **Enregistrer**.

Que faire ensuite

La configuration de générateur de candidat que vous venez de créer s'affiche désormais dans la liste déroulante **Configuration de générateur de candidat**, en vous permettant d'ajouter des critères à cette nouvelle configuration.

Ajout de critères aux configurations du générateur de candidats

Vous pouvez utiliser la console de configuration pour ajouter, aux configurations du générateur de candidats existantes, des types de données qui désignent certains types de données comme critères que le système applique pour ajouter une entité existante à la liste de candidats dans le cadre du processus de résolution d'entité.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.
3. Cliquez sur l'onglet **Générateur de candidat**.
4. Choisissez une configuration dans la liste déroulante **Configuration de générateur de candidat**.
5. Cliquez sur le bouton **Nouveau**.
6. Choisissez un type de données dans la liste déroulante **Type de correspondance**.
7. Dans la zone **Nom du segment**, tapez le nom du segment UMF où se trouvent les données du type de concordance.
8. Cliquez sur le bouton **Enregistrer**.

Que faire ensuite

Le système considérera désormais le type de données que vous venez d'indiquer lors qu'il élaborera les listes de candidats dans le cadre du processus de résolution d'entité.

Suppression de configurations du générateur de candidats

Vous pouvez supprimer une configuration du générateur de candidat à l'aide de la console de configuration. Il peut par exemple s'agir de supprimer une configuration que vous avez créée mais que vous estimez désormais inutile.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.
3. Cliquez sur l'onglet **Générateur de candidat**.
4. Choisissez une configuration dans la liste déroulante **Configuration de générateur de candidat**.
5. Cochez la case de tout type de concordance à supprimer.
6. Cliquez sur le bouton **Supprimer**. Une fenêtre de confirmation vous informe que `les enregistrements sélectionnés vont être supprimés.`
7. Cliquez sur **OK** pour confirmer la suppression de la configuration du générateur de candidat.

Que faire ensuite

L'ensemble de paramètres de générateur de candidat que vous venez de supprimer ne pourra plus servir à générer des listes de candidats dans le cadre du processus de résolution d'entité.

Rubriques d'aide

Fenêtre Générateur de candidat :

Cette fenêtre permet de consulter la liste des paramètres du générateur de candidat. Les paramètres de générateur de candidat sont regroupés par configurations.

Configuration de générateur de candidat : zone
Sélectionnez la configuration de générateur de candidat dont vous souhaitez consulter les paramètres.

Type de correspondance
Type de données qui doit concorder entre une identité entrante et une entité existante pour que cette dernière soit ajoutée à la liste de candidates à la résolution d'entité.

Nom du segment
Nom du segment UMF où se trouvent les données du type de concordance.

Séquence de correspondance
Numéro de groupe de l'ordre où les critères de liste de candidates sont comparés.

Générateur de candidat - onglet Général :

Cet onglet permet de configurer un nouveau critère de générateur de candidat ou de consulter le détail d'un critère existant.

Configuration de générateur de candidat
Configuration de générateur de candidat à laquelle ce critère appartient

Type de correspondance
Sélectionnez le type de données qui doit concorder pour que l'entité existante soit considérée comme une candidate à la résolution.

Nom du segment
Tapez le nom du segment UMF où se trouvent les données du type de

concordance : Numéro unique & autre = NUMBER; Adresse = ADDRESS; Caractéristique = ATTRIBUTE; Nom = NAME; Courriel = EMAIL_ADDR

Configuration des concordances et discordances

Vous pouvez régler les paramètres de concordance et discordance afin de modifier les scores de résolution des entités comparées.

Pourquoi et quand exécuter cette tâche

Les concordances et les discordances peuvent être visualisées et modifiées à l'aide de la console, dans l'onglet **Règles de résolution**.

Concordances et discordances

Une fois qu'une liste de candidats a été créée, et que les critères de résolution fondamentaux ont été comparés, la résolution d'entité compare des critères complémentaires afin de renforcer ou atténuer un score de résolution. Ces critères complémentaires sont les concordances et les discordances.

Les concordances et discordances comparent les types de données suivants :

- Date de naissance
- Numéro unique
- Génération
- Caractéristiques
  - Vous pouvez désigner n'importe quelle caractéristique en vue de l'utiliser dans le cadre des concordances et discordances.

La pondération de concordance est la valeur appliquée pour accorder davantage de poids au score élémentaire de la résolution de deux entités comparées. La pondération de discordance est la valeur (en général négative) appliquée pour accorder moins de poids au score élémentaire de la résolution de deux entités comparées.

Exemple

Une configuration de résolution peut avoir une valeur de concordance de date de naissance égale à +10 et une valeur de discordance égale à -20. Si la fiche entrante et une entité candidate partagent une date de naissance identique, la valeur 10 est ajoutée au score de résolution. Si les dates de naissance ne concordent pas, la valeur 20 est soustraite du score de résolution.

Remarque : Les pondérations de concordance et discordance de date de naissance s'appliquent au score de résolution attribué par une règle de résolution précise. Il ne s'agit pas de la même chose que le paramètre **`DOBConfThreshold`** configuré dans le fichier de configuration du pipeline.

Consultation des concordances et discordances de caractéristiques

Avant de créer de nouvelles concordances et discordances, vous pouvez consulter la liste actuelle des types de caractéristique utilisés lors de la résolution d'entité.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.
3. Cliquez sur l'onglet **Caractéristiques**.

4. Dans la liste déroulante **Configuration de la résolution**, sélectionnez une configuration de résolution.

Création de concordances et discordances de caractéristiques

Vous pouvez désigner n'importe quel type de caractéristique comme critère de résolution d'entité en l'ajoutant à la liste de concordances et discordances de caractéristiques.

Avant de commencer

Il faut que vous ayez configuré l'utilisation en résolution du type de caractéristique concerné par la concordance ou discordance lors de la configuration des paramètres de résolution du type de caractéristique.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.
3. Cliquez sur l'onglet **Caractéristiques**.
4. Dans la liste déroulante **Configuration de la résolution**, sélectionnez une configuration de résolution.
5. Cliquez sur le bouton **Nouveau**.
6. Dans la zone **Numéro de groupe** de l'onglet **Général**, tapez le numéro du groupe que vous voulez appliquer à cette caractéristique.
7. Dans la zone **Description**, type une description du type de caractéristique en cours de configuration.
8. Dans la liste déroulante **Type de caractéristique**, sélectionnez le type de caractéristique à configurer.
9. Dans la zone **Pondération de correspondance**, tapez la valeur (comprise entre 1 et 100) à ajouter au score de ressemblance (si les entités comparées satisfont aux critères de concordance).
10. Dans la zone **Pondération de discordance**, au moyen du signe moins (-), tapez la valeur négative (comprise entre 1 et 100) à soustraire du score de ressemblance (si les entités comparées satisfont aux critères de discordance).
11. Cliquez sur le bouton **Enregistrer**.

Suppression de concordances et discordances de caractéristiques

Pour supprimer un type de caractéristique comme critère de résolution d'entité, supprimez-le de la liste de concordances et discordances de caractéristiques.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Résolution**.
3. Cliquez sur l'onglet **Caractéristiques**.
4. Dans la liste déroulante **Configuration de la résolution**, sélectionnez une configuration de résolution.
5. Cochez la case des types de caractéristique à supprimer.
6. Cliquez sur le bouton **Supprimer**.
7. Dans la fenêtre de confirmation, cliquez sur **OK** pour supprimer la configuration de résolution.

Rubriques d'aide

Fenêtre Concordances et discordances :

Cette fenêtre permet de configurer le processus de concordance et discordance de résolution d'entité. Vous pouvez indiquer les scores de concordance et discordance à ajouter au score de résolution, ainsi que l'ordre où les concordances et discordances sont traitées. Dès qu'une concordance ou discordance est satisfaite, le score correspondant est appliqué, et aucune éventuelle concordance ni discordance restante n'est traitée. Les concordances appliquent un score positif, les discordances un score négatif.

Ordre Ordre de traitement actuel

Description
Description de la concordance ou discordance

Score Saisissez un modificateur de score positif ou négatif pour la concordance/discordance donnée.

Réordonner
Cliquez sur les flèches (vers le haut ou le bas) pour monter ou descendre d'une position la correspondance ou discordance. Le traitement s'arrêtant dès que la première concordance ou discordance est satisfaite, il est important de sélectionner l'ordre adéquat, car cela peut avoir une incidence significative sur les résultats du processus de résolution d'entité.

Fenêtres Caractéristiques :

Cette fenêtre permet de consulter la liste des caractéristiques d'entité dont les comparaisons sont configurées pour affecter le score de résolution d'entité. Ceci n'affecte le score de résolution d'entité que si le paramètre **Discordances de caractéristiques activé** de l'onglet **Règles de résolution - Général** est défini sur Oui.

Description
Nom de la caractéristique en cours de comparaison

Type de caractéristique
Nom système du type de caractéristique en cours de comparaison

Pondération de correspondance
Valeur ajoutée au processus de score de résolution d'entité si les valeurs de caractéristique comparées sont identiques

Pondération de discordance
Valeur ajoutée au processus de score de résolution d'entité si les valeurs de caractéristique comparées sont différentes

Résolution - Caractéristiques - onglet Général :

Cet onglet permet de configurer une nouvelle concordance ou discordance de caractéristique ou de consulter le détail d'une concordance ou discordance existante.

Groupe
Tapez un nombre indiquant dans quel ordre traiter la concordance ou discordance de caractéristique.

Description
Saisissez la description de la concordance ou discordance.

Type de caractéristique
Sélectionnez le type de caractéristique de la concordance ou discordance.

Pondération de correspondance
Saisissez le score à ajouter au score de résolution d'entité si les valeurs de caractéristique comparées sont identiques.

Pondération de discordance
Saisissez le score négatif à ajouter au score de résolution d'entité si les valeurs de caractéristique comparées sont différentes.

Configuration des paramètres système

Vous pouvez configurer certaines fonctions du système Identity Insight.

Configuration des paramètres système pour le calcul du score des noms

Vous pouvez configurer l'algorithme de calcul du score des noms applicable lors de la génération d'une liste de candidats dans le cadre du processus de résolution d'entité.

Procédure

1. Dans la console de configuration, sélectionnez **Configurer** > **Général** > **Paramètres système**.
2. Dans la liste **Groupe de paramètres**, sélectionnez le groupe de paramètres **NAME_MATCHING**.
3. Sélectionnez le paramètre système **ALGORITHM**.
4. Dans la zone **Valeur courante**, indiquez l'entier de l'algorithme Name Comparator à utiliser. Pour rétablir la valeur par défaut de ce paramètre système, entrez la valeur de la zone **Valeur par défaut** dans la zone **Valeur courante**.

   Remarque : Name Comparator 2 est l'algorithme de score de nom par défaut des versions de produit 3.9.1 et ultérieures.
5. Cliquez sur **Enregistrer**.

Configuration des paramètres système du gestionnaire de noms

Par défaut, les paramètres système utilisés pour calculer le score des noms du gestionnaire de noms sont configurés lors de l'installation du produit. Toutefois, vous pouvez les mettre à jour, si nécessaire. Par exemple, vous pouvez être amené à modifier l'emplacement des bibliothèques de support du gestionnaire de noms.

Pourquoi et quand exécuter cette tâche

Vous pouvez définir le chemin des bibliothèques de support du gestionnaire de noms et activer le classement des noms par type à l'aide des paramètres système du gestionnaire de noms. Vous pouvez également définir le paramètre système **CROSSCHECKCULTURE** pour configurer le traitement des noms entre différentes cultures de noms.

Procédure

1. Dans la console de configuration, sélectionnez **Configurer** > **Général** > **Paramètres système**.

2. Dans la liste **Groupe de paramètres**, sélectionnez le groupe de paramètres **NAMEMANAGER**.
3. Dans la sous-fenêtre gauche, sélectionnez le paramètre système du gestionnaire de noms à configurer :

Paramètres système du gestionnaire de noms	Description
SUPPORTPATH	Indique l'emplacement des fichiers de support du gestionnaire de noms. La valeur par défaut est ./data, à savoir le chemin relatif du répertoire principal du produit. Si les fichiers de support sont déplacés dans un autre emplacement lors de l'installation, modifiez cette valeur en indiquant le chemin absolu du nouvel emplacement.
NAMESIFTER	Indique si la fonction de classement par type de nom (noms de personne ou de société) est activée. Pour activer le classement des noms par type (fonction Name Sifter), entrez `1` (valeur par défaut de la nouvelle installation) dans la zone **Valeur courante** Pour désactiver le classement des noms par type (fonction Name Sifter), entrez `0` (valeur par défaut de la mise à niveau) dans la zone **Valeur courante**
CROSSCHECKCULTURE	Indique si vous souhaitez effectuer le calcul du score entre des cultures de noms à l'aide du gestionnaire de noms lorsque les cultures de noms sont différentes. Pour vérifier uniquement la culture du nom entrant avant d'évaluer le score des deux noms, entrez `0` dans la zone **Valeur courante**. Pour vérifier les valeurs de culture de nom avant de calculer le score (valeur de la nouvelle installation), entrez `1` dans la zone **Valeur courante**.

Avertissement : Le paramètre système **CROSSCHECKCULTURE** détermine comment la résolution d'entité traite l'évaluation des noms par culture dans les pipelines. Avant de modifier la valeur en cours du paramètre système, adressez-vous à IBM Services ou au service de support IBM.

4. Cliquez sur **Enregistrer**.

Configuration des paramètres système de la base de données

Vous pouvez configurer la taille maximum de n'importe quelle clause IN de liste de candidats créée par le pipeline au cours de la résolution d'entité.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Paramètres système**.

4. Dans la liste déroulante **Groupe de paramètres**, sélectionnez le groupe de paramètres **DB_CONFIG**.
5. Cliquez sur le paramètre système **MAX_IN_CLAUSE**.
6. Dans la zone **Valeur actuelle**, tapez le nombre maximum de caractères à inclure dans une clause IN pour générer une liste de candidats dans le cadre du processus de résolution d'entité. Les valeurs admises englobent tous les entiers de 0 à 1000. Pour rétablir la valeur par défaut de ce paramètre système, tapez dans cette zone la valeur affichée dans la zone **Valeur par défaut**.

   Remarque : Cette valeur affecte les performances de votre base de données. En fonction de la taille de votre base de données et des capacités de votre matériel, réfléchissez soigneusement à la valeur que vous attribuez à ce paramètre.
7. Cliquez sur **Enregistrer**.

Configuration des paramètres système des journaux

Vous pouvez configurer le niveau de consignation à appliquer à des tables de résolution d'entité particulières de la base de données.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Paramètres système**.
4. Dans le menu déroulant **Groupe de paramètres**, sélectionnez le paramètre système **LOG_LEVEL**.
5. Cliquez sur le nom du paramètre que vous voulez configurer.
6. Dans la zone **Valeur actuelle**, tapez le niveau de consignation à appliquer à ce code de paramètre. Les valeurs admises sont répertoriées et décrites dans la zone **Description du paramètre**. Pour rétablir la valeur par défaut de ce paramètre système, tapez dans cette zone la valeur affichée dans la zone **Valeur par défaut**.

   Remarque : Cette valeur affecte les performances de votre base de données et des composants tels que Visualizer. En fonction de la taille de votre base de données et des capacités de votre matériel, réfléchissez soigneusement à la valeur que vous attribuez à ce paramètre. Par exemple, la définition de LOG_LEVEL sur une valeur inférieure à 4 pour certaines tables peut empêcher Visualizer de fonctionner, y compris les suivantes :
   - ER_DETAIL
   - ER_ENTITY_SCORE
   - ER_ENTITY_STATE
   - ER_RELOCATION
7. Cliquez sur **Enregistrer**.

Configuration des paramètres système de concordance et discordance

Vous pouvez indiquer si vous souhaitez effectuer chaque comparaison de concordance et discordance qui est configurée. Vous pouvez aussi indiquer que ces comparaisons soient effectuées dans l'ordre configuré jusqu'à ce que l'une des concordances ou discordances soit satisfaite. La seconde option contribue à des délais de traitement plus rapides.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Paramètres système**.
4. Dans le menu déroulant **Groupe de paramètres**, sélectionnez le groupe **MM**.
5. Cliquez sur le paramètre système **MULTICONFIRMATION**.
6. Dans la zone **Valeur actuelle**, tapez 1 pour que toutes les concordances et discordances soient traitées, et que pour celles dont la condition est satisfaite, soit appliquée la somme des changements de leur score à la règle de résolution en cours de traitement. Ou alors, tapez 0 pour que les concordances et discordances soient traitées dans l'ordre indiqué, en s'arrêtant à la première dont la condition est satisfaite et en appliquant le changement de son score à la règle de résolution en cours de traitement. Pour rétablir la valeur par défaut de ce paramètre système, tapez dans cette zone la valeur affichée dans la zone **Valeur par défaut**.
7. Cliquez sur **Enregistrer**.

Configuration de paramètres système d'alertes de rôle

Vous pouvez configurer votre système de façon à signaler soit chaque alerte de conflit déclenchée par une règle de résolution d'entité pour une entité entrante, soit uniquement la plus grave de ces alertes.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Paramètres système**.
4. Dans le menu déroulant **Groupe de paramètres**, sélectionnez le groupe **MM**.
5. Cliquez sur le paramètre système **REPORT_SAME_CONFLICTS**.
6. Dans la zone **Valeur actuelle**, tapez 1 afin de signaler toutes les alertes de rôle déclenchées par chaque règle de résolution d'entité pour une entité entrante. Ou alors, tapez 0 afin de signaler uniquement l'alerte de rôle la plus grave déclenchée par chaque règle de résolution pour une entité entrante. Pour rétablir la valeur par défaut de ce paramètre système, tapez dans cette zone la valeur affichée dans la zone **Valeur par défaut**.
7. Cliquez sur **Enregistrer**.

Configuration des paramètres système de générateurs d'alertes d'attribut

Vous pouvez configurer le nombre de jours par défaut pendant lesquels un nouveau générateur d'alertes d'attribut demeurera actif avant d'expirer.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Paramètres système**.
4. Dans le menu déroulant **Groupe de paramètres**, sélectionnez **PERSISTENT_SEARCH**.
5. Cliquez sur le paramètre système **SEARCH_EXPIRATION_TIME**.
6. Dans la zone **Valeur actuelle**, indiquez le nombre de jours par défaut pendant lesquels un nouveau générateur d'alertes d'attribut demeurera actif avant

d'expirer. Les utilisateurs du visualiseur peuvent indiquer une autre date d'expiration, mais cette valeur indique le nombre par défaut de jours pendant lesquels un nouveau générateur d'alertes d'attribut sera actif.

7. Cliquez sur **Enregistrer**.

Configuration de paramètres système relatifs à la simultanéité

Si vos pipelines sont configurés en vue d'un traitement parallèle des pipelines, vous pouvez définir le nombre par défaut d'unités d'exécution de pipeline parallèles démarrant lorsque vous démarrez un pipeline.

Avant de commencer

Lorsque vous êtes connecté à la console de configuration, vous devez avoir coché la case **Editer la configuration**. Ainsi, vous pouvez ajouter, modifier et supprimer la configuration système, y compris les paramètres système.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Paramètres système**.
4. Dans le menu déroulant **Groupe de paramètres**, sélectionnez le groupe de paramètres **CONCURRENCY**.
5. Sélectionnez le paramètre système **DEFAULT_CONCURRENCY**.
6. Dans la zone Valeur actuelle, indiquez le nombre par défaut d'unités d'exécution des pipelines qui démarreront au démarrage d'un pipeline.

Configuration des paramètres système de gestion de la qualité des données

Vous pouvez configurer le délimiteur de date par défaut qu'utilise la console de configuration pour formater les dates.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Paramètres système**.
4. Dans le menu déroulant **Groupe de paramètres**, sélectionnez le groupe **DQM**.
5. Cliquez sur le paramètre système **SYSTEM_DATE_DELIMITER**.
6. Dans la zone **Valeur actuelle**, tapez **/** ou **-** pour indiquer quel délimiteur vous souhaitez que le système applique lors du formatage des dates. Pour rétablir la valeur par défaut de ce paramètre système, tapez dans cette zone la valeur affichée dans la zone **Valeur par défaut**.
7. Cliquez sur **Enregistrer**.

Configuration des paramètres système des options de produit

Vous pouvez configurer à votre guise quelles options supplémentaires activer.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Paramètres système**.

4. Dans le menu déroulant **Groupe de paramètres**, sélectionnez le groupe **CONSOLE_CONFIG**.
5. Cliquez sur le paramètre système **PRODUCT_OPTIONS**.
6. Dans la zone **Valeur actuelle**, tapez le code, fourni par IBM, qui correspond à la fonction que vous souhaitez activer. Vous devez tout mettre en majuscules. Vous pouvez tapez une liste, délimitée par des espaces, de toue les fonctions que vous souhaitez que le système active. Pour rétablir la valeur par défaut de ce paramètre système, tapez dans cette zone la valeur affichée dans la zone **Valeur par défaut**.
7. Cliquez sur **Enregistrer**.

Configuration des paramètres système du gestionnaire d'événements

Vous pouvez activer le traitement du gestionnaire d'événements et configurer les paramètres système pour le traitement des événements, dont l'identificateur URI du processeur d'événements.

Procédure

1. Dans la console de configuration, cliquez sur l'onglet **Configuration système**.
2. Dans le volet gauche, sélectionnez le paramètre système du gestionnaire d'événements à configurer :
   a. **Activation du traitement d'événement** indique si le traitement des événements par le gestionnaire d'événements est activé ou désactivé.
   b. **Délai d'attente du processeur d'événement** indique le délai (en secondes) pendant lequel le pipeline attend une réponse du processeur d'événements externes avant expiration avec une erreur. La valeur par défaut est de 60 secondes.
   c. **URI du processeur d'événement** indique l'identificateur URI devant être connecté au processeur d'événements externes. Dans **Valeur courante**, entrez l'URI, en incluant le numéro de port, même s'il s'agit du numéro de port par défaut. Par exemple : `http://hôtelocal:13510/gem`
   d. **Fenêtre d'historique d'événements** indique le nombre de jours d'historique d'événements que le pipeline envoie au processeur d'événements externes lors de l'évaluation d'un nouvel événement entrant. (Le nombre de jours par défaut est 180.)
3. Cliquez sur le bouton **Enregistrer**.

Configuration des paramètres système du visualiseur

Les paramètres système du Visualizer vous permettent d'autoriser les utilisateurs du Visualizer individuels à voir toutes les alertes, y compris celles qui sont inférieures au paramètre **Seuil d'alerte minimal** défini dans la règle d'alerte de chaque rôle. Vous pouvez modifier ce paramètre pour donner davantage de souplesse aux utilisateurs du Visualizer dans l'affichage des alertes.

Procédure

1. Dans la console de configuration, cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Paramètres système**.
4. Dans la liste déroulante **Groupe de paramètres**, sélectionnez le groupe de paramètres **VISUALIZER**.

5. Cliquez sur le paramètre système **ALLOW_ALERT_THRESHOLD_OVERRIDE**.
6. Sélectionnez l'une des options suivantes :
   - Pour permettre aux utilisateurs du Visualizer de remplacer le seuil d'alerte défini sur l'onglet **Règles d'alerte de rôle - Filtres** dans la console de configuration, entrez `1` dans le champ **Valeur courante**.
   - Pour ne pas autoriser les utilisateurs du Visualizer à remplacer le seuil d'alerte défini par le système sur l'onglet **Règles d'alerte de rôle - Filtres** dans la console de configuration, entrez `0` .
   - Pour rétablir ce paramètre système sur sa valeur par défaut, entrez la valeur affichée dans le champ **Valeur par défaut** dans le champ **Valeur courante**.
7. Cliquez sur le bouton **Enregistrer**.

Définition du chemin d'accès par défaut pour Centrifuge

Si vous utilisez le bureau Centrifuge optionnel des systèmes Centrifuges pour visualiser et afficher des graphiques d'entités, vous devez spécifier le chemin d'accès au bureau Centrifuge dans les préférences du Visualizer.

Pourquoi et quand exécuter cette tâche

Les paramètres par défaut du chemin d'accès sont configurés pour chaque client Visualizer. En spécifiant un chemin d'accès par défaut à l'aide de cette tâche, vous définissez uniquement le chemin d'accès dans le Visualizer auquel vous êtes actuellement connecté.

Procédure

1. Dans le Visualizer, cliquez sur **Fichier** > **Préférences** > **Préférences système**.
2. Sous la section **Chemins d'accès au fichier** dans **Chemin Centrifuge** :
   - Saisissez dans la zone le chemin d'accès au fichier ou l'URL (uniform resource locator) jusqu'à l'application du bureau Centrifuge.
   - Ou accédez à l'application du bureau Centrifuge et ouvrez-la.
3. Cliquez sur **Soumettre**. Un message de confirmation vous informe que vous devez redémarrer le Visualizer avant que vos modifications ne soient effectives.
4. Dans le message de confirmation, cliquez sur **OK**.
5. Fermez le Visualizer, réouvrez-le et connectez-vous de nouveau.

Résultats

Une fois le chemin d'accès configuré, le bouton **Centrifuge** s'affiche sur les écrans **Détail d'alerte de rôle** et **Récapitulatif d'entité** dans la fenêtre **Recherche**. Cliquez sur le bouton pour lancer votre application du bureau Centrifuge Desktop directement depuis le Visualizer.

Paramétrage du chemin d'accès par défaut des fichiers UMF

Si vous chargez régulièrement des fiches d'identité dans des fichiers de données UMF pour un traitement via Visualizer, le paramétrage du chemin d'accès par défaut peut vous faire gagner une étape.

Pourquoi et quand exécuter cette tâche

Les paramètres par défaut du chemin d'accès sont configurés pour chaque client Visualizer. En spécifiant un chemin d'accès par défaut à l'aide de cette tâche, vous

définissez uniquement le chemin d'accès dans le Visualizer auquel vous êtes actuellement connecté.

Procédure

1. Dans le Visualizer, sélectionnez **Fichier** > **Préférences** > **Préférences système**.
2. Dans **Chemin d'accès par défaut pour le chargement de fichier**, procédez comme suit :
   - Saisissez le chemin d'accès complet du répertoire à utiliser.
   - Ou accédez au répertoire pour le sélectionner.
3. Cliquez sur **Soumettre**. Un message de confirmation vous informe que vous devez redémarrer le Visualizer avant que vos modifications ne soient effectives.
4. Dans le message de confirmation, cliquez sur **OK**.
5. Fermez le Visualizer, réouvrez-le et connectez-vous de nouveau.

Résultats

Chaque fois que vous chargez un fichier UMF, le chemin d'accès par défaut correspond au répertoire que vous avez spécifié.

Personnalisation d'attributs et de score

IBM InfoSphere Identity Insight propose des améliorations fonctionnelles pour la configuration des données d'attribut et l'intégration des algorithmes de score. Ces modifications augmentent la taille et les types de données d'identité qui peuvent être comparées et évaluées et permet d'ajouter de nouveaux algorithmes de score dans le processus de résolution d'entité. Ces capacités sont généralement appelées personnalisation d'attributs et de score.

La technologie de résolution d'entité vous permet d'utiliser des algorithmes de correspondance d'identités et de score pour comparer et résoudre des données d'identité courantes, telles que noms, adresses, numéros de téléphone, numéros de carte de crédit, numéros d'identification fiscale et numéros de permis, et indiquer des correspondances éventuelles. Les données élémentaires qui décrivent un compte ou une entité sont appelées attribut. Les attributs peuvent inclure les caractéristiques ou traits qui décrivent une personne, un organisme, un lieu ou un élément. L'adjonction de la personnalisation d'attributs et de score vous permet d'ajouter de nouveaux types de données d'identification et d'associer des algorithmes de score qui ont été développés en tant que plug-in d'évaluation de produit. Par exemple, vous pouvez ajouter des données d'identité dérivées d'empreintes digitales, de scans de rétine ou de tests ADN, puis les comparer et les évaluer à l'aide d'un plug-in de score incluant un algorithme de comparaison approprié.

Ces améliorations d'attributs et de score augmentent le processus de résolution d'entité en vous permettant :

- d'enregistrer et de comparer des données d'attribut à l'aide de ATTR_VALUE (élargi à 8 Ko) et ATTR_LARGE_DATA pour l'enregistrement de données encore plus grandes,
- d'appliquer les algorithmes de score fournis à une gamme plus large de types d'attribut et de configurer plus facilement ces attributs avec plus de contrôle,
- d'intégrer les résultats de comparaisons et d'évaluations d'attributs personnalisés à l'aide des fonctions de rapport et d'alerte Visualizer,

- d'appliquer un modèle de plug-in pour l'ajout d'algorithmes de score créés par l'utilisateur,
- d'intégrer des plug-in de score personnalisés à l'aide de la console de configuration.

Enregistrement de données d'attributs volumineuses

Pour que le système enregistre et traite des données d'attributs plus volumineuses avec les plug-ins de score, les métadonnées doivent être converties dans le format UMF (Universal Message Format) et enregistrées dans les colonnes appropriées.

Pourquoi et quand exécuter cette tâche

Procédure

1. A l'aide du modèle d'entité que vous avez créé pour le système, analysez les données entrantes afin de vérifier leur conformité à la norme UMF. Vous devez parfaitement maîtriser les segments et balises UMF existants avant de passer à l'étape suivante.
2. Configurez l'utilitaire de ETL de manière à générer des fiches UMF conformes à votre modèle d'entité.
3. Exécutez l'utilitaire ETL.

Que faire ensuite

Une fois la conversion des données au format UMF effectuée, vous pouvez envoyer les fiches UMF vers le pipeline en vue du traitement.

Paramètres de stockage des données d'attribut volumineuses

Pour permettre au système de stocker et de traiter des données d'attribut volumineuses pour le score, les métadonnées doivent être converties au format UMF (Universal Message Format) et stockées dans les colonnes appropriées.

Utilisez les colonnes ATTR_VALUE et ATTR_LARGE_DATA pour stocker des données d'attribut volumineuses ou non structurées pour les applications d'attribut et de score personnalisées.

Colonne et nom de balise UMF	Type de données et taille	Obligatoire	Explication

ATTR_VALUE	varchar(255) (par défaut) redimensionnable jusqu'à 8k	**Oui**	Données utilisées en tant que l'un des attributs d'un processus ETL avec les plug-in de score de base. Si les données sont plus volumineuses que 8k et au format binaire, stockez les données dans le colonne ATTR_LARGE_DATA et créez un identificateur unique pour ces données dans la colonne ATTR_VALUE. L'identificateur ATTR_VALUE est utilisé pour la comparaison et le score. Par exemple, créez un hachage unidirectionnel MD5 (Message-Digest algorithm 5) qui peut être comparé et affiché dans le Visualizer et les rapports. La taille maximale de la colonne dépend de la base de données. Pour les données binaires supérieures à 255/3 qui doivent être stockées dans ATTR_VALUE, la colonne doit être redimensionnée. Pour des raisons de performance, vous devez penser à régler à nouveau le cache de la base car il est probable que très peu de lignes entrent dans le cache.

ATTR_LARGE_DATA	Objet CLOB à utiliser pour les données supérieures à 8k.	**Non**	Stockez-les sous forme de données de type caractères. Par exemple, utilisez le codage Base64 des données binaires. Utilisez cette colonne pour stocker les données d'attribut qui sont trop volumineuses pour la colonne ATTR_VALUE. ATTR_LARGE_DATA est une colonne de type CLOB (character large object) et peut gérer des données de taille illimitée. Ces données sont disponibles pour la résolution d'entité. La structure des données doit être connue de l'auteur du plug-in de comparaison personnalisé. Le Visualizer n'affichera pas ces données car le format n'est pas standard et sera différent pour des types de systèmes différents. Un objet CLOB ne fonctionnera pas aussi bien qu'une colonne varchar car un objet CLOB ne peut pas être mis en cache et nécessite une lecture de disque ; c'est pourquoi ATTR_VALUE est préférable. Si très peu de données d'attribut sont mises en cache à cause de l'augmentation de la taille de ATTR_VALUE, il peut être préférable d'utiliser seulement ATTR_LARGE_DATA pour les données inférieures à 8k afin de s'assurer que les autres attributs non volumineux, comme le sexe et la date de naissance, sont mis en cache correctement. Sur ce point, c'est à l'architecte de juger. Pensez à consulter votre administrateur de base de données. Lorsque ATTR_LARGE_DATA est utilisé, une valeur doit être affectée à ATTR_VALUE. S'il existe un moyen de créer une clé de recherche pertinente à partir des données pour ATTR_VALUE, vous devez la créer et l'affecter à ATTR_VALUE. S'il n'est pas possible de créer une clé de recherche pertinente, une valeur unique doit être affectée à ATTR_VALUE pour éviter le dysfonctionnement ou l'échec du pipeline avec la génération d'erreurs DQM. Une clé unique peut être générée automatiquement en configurant une règle DQM pour créer un hachage MD5 des données (règle 600) ou un hachage personnalisé en fonction des règles configurées (règle 615). Il est indispensable que cette valeur soit unique, en particulier si le type d'attribut doit être configuré pour des recherches persistantes car l'attribut ATTR_VALUE est utilisé pour déterminer des valeurs génériques. **Remarque :** Le plug-in 'binaryAttributeScoring' fourni ne compare pas ATTR_VALUE. Il examine et évalue uniquement le segment ATTR_LARGE_DATA.

Exemple

Voici un exemple de sortie de hachage MD5 de données binaires volumineuses :

```
<ATTRIBUTE><ATTR_TYPE>BIOMETRIC-1</ATTR_TYPE>
<ATTR_VALUE>214b21fc3e040f844a07710b1bb451a0
</ATTR_VALUE><ATTR_LARGE_DATA>
<![H4sICBRTqkgAA2Zvby50eHQAK0ktLuHlAgDkTqoPBgAAAA==]>
</ATTR_LARGE_DATA></ATTRIBUTE>
```

Il est probable que les valeurs ATTR_LARGE_DATA réelles soient bien plus volumineuses que dans cet exemple.

Configuration des caractéristiques sources de données d'attributs volumineuses

Pour configurer les caractéristiques sources de données d'attributs volumineuses, utilisez la console de configuration.

Pourquoi et quand exécuter cette tâche

La console de configuration vous permet de configurer des nouveaux types de données d'attributs pour des plug-ins de score personnalisés de la même manière que vous configurez les données des plug-ins de base.

Procédure

1. Sur l'onglet Plug-ins de la console de configuration, cliquez sur la case de sélection du plug-in personnalisé.
2. Cliquez sur l'onglet Caractéristiques.
3. Cliquez sur l'onglet Général et renseignez les champs.
4. Sélectionnez le Type de données approprié. Le type de données peut être : CHAR, DATE ou CLOB. Notez les règles à respecter pour le type de données à la rubrique «Paramètres de stockage des données d'attribut volumineuses», à la page 190.
5. Sélectionnez une classe appropriée.
6. Sélectionnez une valeur pour l'utilisation de la résolution.
7. Sélectionnez le nom du plugin de score que vous configurez.
8. Sélectionnez une valeur appropriée dans le champ Niveau d'affichage. Sélectionnez "Type uniquement sans valeur" pour que Visualizer n'affiche pas les contenus des colonnes ATTRIBUTE.ATTR_VALUE ou ATTRIBUTE.ATTR_LARGE_DATA. La colonne ATTR_VALUE n'est généralement pas utilisée lorsque la colonne CLOB est utilisée. En outre, la colonne ATTR_LARGE_DATA (CLOB) contient généralement des données codées en base 64 dont l'affichage ne serait pas pertinent ou utile dans Visualizer.
9. Cliquez sur Enregistrer.

Résultats

L'onglet Caractéristiques sous Sources affiche le nouveau type et les informations associées.

Configuration des caractéristiques de résolution de données volumineuses

Pour configurer les caractéristiques de résolution de données volumineuses et des plug-ins de score, utilisez la console de configuration.

Pourquoi et quand exécuter cette tâche

Les informations de concordance/discordance d'un nouveau type de caractéristiques sont configurées en dernier.

Procédure

1. Dans la console de configuration, cliquez sur le bouton Configurer.
2. Cliquez sur le bouton Résolution.
3. Cliquez sur l'onglet Caractéristiques.
4. Sélectionnez une configuration de résolution appropriée, telle que DEFAULT, dans le menu déroulant puis cliquez sur le bouton Nouveau.
5. Sélectionnez l'onglet Général et entrez les valeurs dans les champs affichés. Pour les descriptions des options des champs et des recommandations, reportez-vous à la section «Caractéristiques de résolution et options».
6. Cliquez sur Enregistrer.

Résultats

L'écran d'aperçu affiche un tableau récapitulatif avec les valeurs que vous avez créées pour la configuration de résolution.

Caractéristiques de résolution et options

Utilisez l'onglet général des caractéristiques de résolution pour configurer des actions et des options pour les types de données volumineuses et les plug-in de score personnalisés.

Si vous configurez un type de caractères avec une zone d'utilisation de résolution et sélectionnez une valeur "Concordance/discordance", des zones supplémentaires apparaissent de façon dynamique.

Zone	Obligatoire	Sélection et descriptions de la zone
Groupe	**Oui**	Tapez le numéro du groupe que vous souhaitez utiliser pour identifier cette caractéristique.
Description	**Oui**	Entrez une courte description de cette configuration de résolution par défaut. Si cette zone reste vide, une erreur se produit.
Type de caractéristique	**Oui**	Sélectionnez le type sur lequel vous travaillez. La liste inclut tous les types que vous avez configurés pour les sources.
Pondération de correspondance	**Oui**	Valeur de 0 à 100. Concerne le score de ressemblance.

Seuil de concordance du plug-in	**Non**	Zone de texte à format libre. Cette zone s'affiche si un type de caractéristique est défini, dont la zone d'utilisation de résolution est définie sur "Concordance/discordance", comme par exemple lorsque le type est pour un plug-in personnalisé. Si le type de caractéristique est évalué par un plug-in de score au cours de la phase de concordance et de discordance du processus de résolution d'entité, définissez une valeur de seuil de concordance. Si le score affecté par le plug-in est égal ou supérieur à cette valeur, la correspondance est considérée comme une concordance, ce qui a pour effet que la valeur de la zone de pondération de correspondance s'ajoute au score de niveau de fiabilité de résolution.
Pondération de discordance	**Oui**	Valeur de 0 à 100. Concerne le score de ressemblance.
Seuil de discordance du plug-in	**Non**	Zone de texte à format libre. Cette zone s'affiche uniquement si un type de caractéristique est défini, dont la zone d'utilisation de résolution est définie sur "Concordance/discordance", comme par exemple lorsque le type est pour un plug-in personnalisé. Si le type de caractéristique est évalué par un plug-in de score au cours de la phase de concordance et de discordance du processus de résolution d'entité, définissez ici une valeur de seuil de discordance (qui doit être interprétée par le plug-in). Si le score affecté par le plug-in est égal ou inférieur à cette valeur, la correspondance est considérée comme une discordance, ce qui a pour effet que la valeur de la zone de pondération de discordance s'ajoute au score de niveau de fiabilité de résolution.

Rapports de configuration pour la personnalisation des attributs et du score

Le rapport de configuration de la console de configuration inclut également des éléments pour la personnalisation des attributs et du score.

Les ajouts au rapport de configuration incluent :

- La section "Type de caractéristique" du rapport possède une nouvelle colonne appelée "Plug-in de score" qui affiche la valeur du type de caractéristiques du plug-in correspondant.
- Une nouvelle section de rapport de plug-in indique les fiches configurées. Les libellés d'en-tête de colonne incluent : ID, Nom, Type, Version et Nom abrégé de bibliothèque.
- La section "Caractéristiques de résolution d'entité" possède deux nouvelles colonnes qui indiquent les valeurs "Seuil de concordance du plug-in" et "Seuil de discordance du plug-in".

Configuration de plug-ins de score personnalisés

Pour configurer des plug-ins de score personnalisés, utilisez la console de configuration.

Avant de commencer

Assurez-vous que le nouveau plugin a été correctement adapté pour IBM InfoSphere Identity Insight. Pour plus d'informations, voir Développement de plug-in de score personnalisés pour IBM InfoSphere Identity Insight.

Pourquoi et quand exécuter cette tâche

La console de configuration vous permet de configurer les plug-ins de score que vous avez ajoutés à votre système.

Procédure

1. Dans la console de configuration, cliquez sur le bouton Configurer.
2. Cliquez sur le bouton Général.
3. Cliquez sur l'onglet Plug-ins.
4. Pour configurer un nouveau plug-in, cliquez sur le bouton Nouveau.
5. Pour éditer un plug-in existant, sélectionnez le plug-in que vous souhaitez configurer dans la liste de la colonne Plug-ins. Seuls les plug-ins personnalisés peuvent être édités.
6. Sur l'onglet Général, renseignez les champs :

Nom de zone	Obligatoire	Description
Plugin	**Oui**	Nom du plug-in qui sera affiché dans les options du menu “Plugin de score”.
Nom de bibliothèque court	**Oui**	Le nom dans ce champ est utilisé dans la colonne LIBRARY_NAME de la table Plugin. Le champ Nom de bibliothèque court est utilisé pour créer le nom du fichier de bibliothèque de logiciels appelé par le code du pipeline. Il est conseillé d'utiliser le même nom que celui utilisé pour le fichier de bibliothèque réel appelé par le pipeline, car certains systèmes tiennent compte de la casse. EAS est ajouté au début ou à la fin de ce nom, selon le système d'exploitation.
Version	**Oui**	Ce champ est utilisé pour suivre le numéro de version e la bibliothèque de logiciels.

7. Cliquez sur Enregistrer.

Résultats

L'onglet Plugin affiche le nom du plug-in mis à jour et les informations associées.

Développement de plug-in de score personnalisés pour IBM InfoSphere Identity Insight

IBM InfoSphere Identity Insight vous permet de créer des plug-in de score personnalisés et d'inclure des types supplémentaires de données d'attribut dans le processus de résolution d'entité.

Pour créer un plug-in de score pour IBM InfoSphere Identity Insight, vous devez obligatoirement inclure plusieurs éléments de base et générer une bibliothèque partagée. Les plug-in personnalisés doivent être installés dans un répertoire défini dans le chemin de charge de bibliothèque.

Interface de développement des plug-in de score

Les plug-in personnalisés nécessitent une interface standard.

Utilisez des objets primitifs pour éliminer une dépendance envers les versions de bibliothèque et les options de compilation. Vous pouvez ainsi utiliser des plug-in avec plusieurs versions de pipeline sans devoir régénérer le plug-in lorsque le

pipeline change les versions de bibliothèque, de compilateur ou d'autres options. Vous devez inclure les prototypes d'interface C ou C++ suivants :

```
#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

Les plug-in de score personnalisés nécessitent la fonction getVersion.

Exemple

Vous devez inclure les éléments suivants :

```
const char *getVersion();
```

return char * contient une chaîne terminée NULL décrivant la version de plug-in.

Implémentez cette fonction en stockant le numéro de version de plug-in dans une chaîne statique et renvoyez un pointeur vers le pointeur de base de la chaîne.

myPlugin.h inclut les éléments suivants :

```
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

Les plug-in personnalisés nécessitent une fonction initPlugin.

Exemple

initPlugin permet au plug-in de charger et d'enregistrer les informations de configuration dont il aura besoin pour le score. La chaîne de connexion de base de

données et le nom de fichier .ini sont fournis dans la chaîne **configInfo**. initPlugin est appelé une fois pour chaque type d'attribut utilisant un plug-in. Il s'agit d'objets partagés. Pour que le plug-in puisse être utilisé pour plusieurs types d'attribut, les informations de configuration doivent être enregistrées pour chaque type d'attribut. De cette façon, lorsque le score est appelé, il peut rechercher le type d'attribut approprié dans les informations de configuration.

```
const int initPlugin(const char *configInfo,
                     const uint configSize,
                     char *errorStr,
                     const uint maxStrSize);
```

configSize
: est la longueur de la chaîne contenue dans configInfo. L'erreur doit être au format suivant.

errorStr
: est une mémoire tampon pré-affectée destinée à copier une chaîne terminée NULL. La chaîne contient le XML décrivant les erreurs d'initialisation. L'erreur doit être au format suivant :

```
<ERROR>texte d'erreur</ERROR>
```

maxStrSize
: est la taille de la mémoire tampon pré-affectée vers laquelle pointe errorStr. La taille de la chaîne d'erreur ne peut pas dépasser cette valeur.

Voici un exemple de pseudocode d'une fonction de score :

```
const int initPlugin(const char *configInfo, const uint configSize,
char *errorStr, const uint maxStrSize)
{
  //créer une chaîne à partir de configInfo
  //faire une analyse syntaxique avec l'analyseur syntaxique XML
  //extraire DB_CONNECTION et CONFIG_FILE
  //se connecter à la base de données
  //sélectionner l'info de config dans la base de données
  //ouvrir CONFIG_FILE
  //lire l'info de config dans le fichier .ini

  //en cas d'erreur, créer une chaîne d'erreur terminée NULL et
  //strcpy dans le errorStr. Renvoyer -1.
  //s'il n'y a pas d'erreur, renvoyer 0.
}
```

initPlugin doit renvoyer -1 en cas d'erreur.

score

Les plug-in de score personnalisés nécessitent une fonction de score.

score contient les paramètres suivants :

```
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
: contient les seuils de concordance et de discordance. Ces seuils ne sont pas obligatoires.

thresholdSize
est la taille de la chaîne contenue dans thresholdStr.

inboundStr
contient l'attribut provenant de l'entité entrante en cours d'évaluation.

inboundSize
est la taille de la chaîne contenue dans inboundStr.

candidateStr
est un pointeur vers une chaîne contenant l'attribut provenant de l'entité candidate en cours d'évaluation.

candidateSize
est la taille de la chaîne contenue dans candidateStr.

result est une mémoire tampon pré-affectée destinée à copier une chaîne terminée NULL contenant du XML décrivant les résultats de score. En cas d'erreur, les résultats seront une description de l'erreur. Le format de cette chaîne de retour est défini comme suit :

```
<SCORE_RESULT>
  <MATCH_SCORE>integer 0-100</MATCH_SCORE>
  <CONFIRMATION>TRUE/FALSE</CONFIRMATION>
</SCORE_RESULT>
```

En cas d'erreur, le format des résultats est le suivant :

```
<ERROR>texte d'erreur</ERROR>
```

resultSize
est la taille de la mémoire tampon pré-affectée vers laquelle pointe le résultat. La chaîne de résultat ne peut pas dépasser cette taille. Le document de résultat étant plutôt petit, il ne devrait pas poser de problème, sauf avec les messages d'erreur particulièrement longs.

Voici un exemple de pseudocode d'une fonction de score :

```
const int score(const char *thresholdStr,
       const uint thresholdSize,
                const char *inboundStr,
       const uint inboundSize,
             const char *candidateStr,
       const uint candidateSize,
       char *result,
       const uint resultSize)
{
  //créer des chaînes à partir de  thresholdStr, inboundStr et candidateStr
  //créer des documents XML à partir de thresholdStr, inboundStr et candidateStr
  //faire une analyse syntaxique des seuils à partir du doc XML de seuil en cas d'utilisation de s
  //faire une analyse syntaxique des valeurs à partir du doc XML entrant
  //faire une analyse syntaxique des valeurs à partir du doc XML candidat

  //rechercher des erreurs éventuelles, telles que des disparités de types attr, des données incor
  //décoder les zones de données attr_value et attr_large_data si nécessaire
  //appliquer un algorithme de score aux données d'attribut
  //évaluer le score sur une plage de 0 à 100
  //déterminer la concordance ou la discordance (éventuellement à l'aide de seuils)

  //en cas d'erreur, créer une chaîne d'erreur terminée NULL et
  //strcpy dans le résultat. Renvoyer -1.
  //s'il n'y a pas d'erreur, créer un document de résultat terminé NULL et strcpy dans
  //le résultat.  Renvoyer 0.
}
```

La fonction de score doit renvoyer -1 en cas d'erreur.

Formats de données

Les plug-in de score personnalisés nécessitent un format de données défini.

Exemple

Format de données de seuil

```
<THRESHOLDS>
  <CONFIRMATION_THRESHOLD>string</CONFIRMATION_THRESHOLD>
  <DENY_THRESHOLD>string</DENY_THRESHOLD>
</THRESHOLDS>
```

Les seuils sont des chaînes à structure libre. Ils sont chargés à partir de la table MATCH_MERGE_ATTR et doivent être conformes au format attendu par le plug-in. Ce format est défini par l'auteur du plug-in et dépend du plug-in.

Format de données d'attribut

```
<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 peut être une chaîne vide en fonction du type d'attribut et du processus ETL. ATTR_LARGE_DATA est optionnel et doit uniquement être utilisé si les données d'un attribut sont trop volumineuses pour rentrer dans la colonne ATTR_VALUE. Ceci doit être déterminé lors de la configuration du système afin que UMF puisse être créé correctement et que les plug-in puissent être écrits pour utiliser les zones correctes.

ATTR_LARGE_DATA peut être codé pour être conforme au jeu de caractères valide de XML. Le codage Base64 est recommandé, ce qui est réalisé dans le processus ETL. Le plug-in peut nécessiter le décodage des données de ATTR_LARGE_DATA. La chaîne doit être également codée en UTF-8. Si la chaîne a été codée en base64 dans ETL, la chaîne UTF-8 sera identique à la chaîne ASCII7.

Voici un exemple de pseudocode d'une fonction de score :

```
const int score(const char *thresholdStr,
       const uint thresholdSize,
                const char *inboundStr,
       const uint inboundSize,
             const char *candidateStr,
       const uint candidateSize,
       char *result,
       const uint resultSize)
{
  //créer des chaînes à partir de  thresholdStr, inboundStr et candidateStr
  //créer des documents XML à partir de thresholdStr, inboundStr et candidateStr
  //faire une analyse syntaxique des seuils à partir du doc XML de seuil en cas d'utilisation de seu
  //faire une analyse syntaxique des valeurs à partir du doc XML entrant
  //faire une analyse syntaxique des valeurs à partir du doc XML candidat

  //rechercher des erreurs éventuelles, telles que des disparités de types attr, des données incorre
  //décoder les zones de données attr_value et attr_large_data si nécessaire
  //appliquer un algorithme de score aux données d'attribut
  //évaluer le score sur une plage de 0 à 100
  //déterminer la concordance ou la discordance (éventuellement à l'aide de seuils)

  //en cas d'erreur, créer une chaîne d'erreur terminée NULL et
```

```
  //strcpy dans le résultat. Renvoyer -1.
  //s'il n'y a pas d'erreur, créer un document de résultat terminé NULL et strcpy dans
  //le résultat.  Renvoyer 0.
}
```

La fonction de score doit renvoyer -1 en cas d'erreur.

Génération d'un objet de plugin

L'objet de plugin doit être généré dans une bibliothèque partagée.

Pourquoi et quand exécuter cette tâche

Générez l'objet dans une bibliothèque partagée (.dll sous windows, .so sous linux/unix). Toutes les bibliothèques doivent être liées d'une manière statique. Ceci empêchera les non concordances de version et les symboles non résolus possibles.

Chapitre 6. Gestion des pipelines

Les pipelines sont au coeur du système. C'est là que le traitement a lieu : où les entité sont résolues, où les relations sont détectées et où les alertes sont déclenchées. Les pipelines constituent le moyen principal par lequel les données sont chargées dans la base de données d'entité. La gestion des pipelines est une tâche opérationnelle permanente qui implique de configurer les pipelines, de démarrer et arrêter les pipelines, de superviser les pipelines, et d'acheminer les messages des pipelines à d'autres pipelines, noeuds, ou systèmes externes.

Pipelines

Les pipelines sont les composants qui effectuent la standardisation et l'uniformisation de nom et d'adresse, la gestion de la qualité des données et la résolution d'entité. Ils réalisent également la résolution des relations et génèrent des alertes en fonction de la configuration du système.

Les pipelines exécutent trois processus de base :

- Reconnaissance - impliquant l'optimisation des données entrantes via la vérification de la standardisation, du nettoyage, de l'amélioration et de la qualité
- Résolution - impliquant la résolution d'entités
- Lien - impliquant la détection de relations et la génération d'alertes

Les pipelines sont hébergés par des noeuds.

Vous pouvez configurer les pipelines pour un traitement en parallèle, de façon à ce qu'une commande pipeline génère plusieurs unités d'exécution en parallèle des pipelines, ce qui permet au système de traiter simultanément plusieurs requêtes de données. Cette fonctionnalité permet d'améliorer les performances du système, de réduire le temps de traitement des données et de limiter les contraintes de mémoire liées au matériel.

La configuration de la fonctionnalité de traitement en parallèle des pipelines s'effectue à deux endroits différents :

- Le paramètre de simultanéité globale est contrôlé par le paramètre système `Accès concurrent par défaut du pipeline` de l'onglet **Configuration système**, dans la console de configuration. La valeur indiquée ici définit le nombre d'unités d'exécution en parallèle qui sont démarrées à partir de la commande de démarrage d'un pipeline. La valeur par défaut de ce paramètre est 1, ce qui signifie que sauf modification du paramètre, une seule unité d'exécution de traitement de pipeline démarre.
- Il est possible de configurer un paramètre d'accès concurrent local (par noeud de pipeline) dans le fichier de configuration du pipeline. Si vous indiquez un paramètre d'accès concurrent et une valeur dans le fichier de configuration du pipeline par noeud de pipeline, cette valeur remplace celle du paramètre système global. Lorsque vous émettez une commande de démarrage du pipeline sur ce noeud, vous démarrez le même nombre d'unités d'exécution de pipeline en simultané que celui indiqué dans le fichier de configuration du pipeline.

Vérification de la configuration des pipelines

Le système effectue une vérification de la configuration de pipeline avant de démarrer un nouveau processus de pipeline, et ce à intervalles fréquents, pour chaque pipeline, afin d'être certain que sa configuration est valide.

Au cours de la vérification de la configuration de pipeline, le système vérifie si la configuration du pipeline est valide :

- La configuration de ce pipeline est-elle la même que la configuration présente dans la console de configuration ?
- Existe-t-il un nombre raisonnable d'enregistrements pour chaque table de configuration utilisée par le pipeline ?
- Y a-t-il des valeurs standard dans des tables de configuration spécifiques ?
- Des valeurs et identificateurs de configuration sont-ils définis dans des tables de configuration spécifiques ?

Si ces vérifications de configuration ne sont pas validées, selon la gravité de la divergence, soit le système consigne un avertissement dans les fichiers journaux, soit il arrête automatiquement le pipeline (ou ne le démarre pas) et consigne une erreur.

Noeuds de pipelines

Les noeuds de pipelines sont les machines physiques qui hébergent un ou plusieurs processus de pipelines.

Le noeud de pipeline est l'endroit où vous installez et démarrez l'exécutable des processus d'un pipeline. Vous configurez et gérez le fichier de configuration de tous les pipelines hébergés sur cette machine. Le système inscrit également les messages du pipeline dans les fichiers journaux qui se trouvent sur les noeuds du pipeline.

Les noeuds de pipelines assurent la connexion entre les processus du pipeline et les composants de l'architecture du produit suivants :

Programmes d'acquisition
Dans le cadre du processus d'extraction, transformation et chargement, les programmes d'acquisition utilisent des transports pour envoyer des données UMF aux pipelines pour traitement. Vous devez utiliser le mode de transport approprié au type de programme d'acquisition pour vous connecter aux pipelines. Par exemple, si vous utilisez l'utilitaire de fichier UMF comme programme d'acquisition, utilisez le transport Fichier.

Base de données des entités
La base de données des entités contient des informations relatives aux entités. Les pipelines accèdent à ces informations lors du traitement des fiches entrantes pour la résolution des entités et des relations. Pour que les pipelines puissent accéder à la base de données des entités, le client de base de données approprié doit être installé et configuré sur le noeud de pipeline.

Files d'attente
Si votre système fait appel à des files d'attente comme mode de transport pour l'envoi pour traitement de données aux pipelines, vous devez installer et configurer le logiciel Message Queuing approprié sur chaque noeud de pipeline.

Serveurs de nettoyage d'adresses
Si votre système utilise des produits de nettoyage d'adresses d'autres société, chaque noeud de pipeline doit être configuré de telle sorte qu'il puisse se connecter aux serveurs de nettoyage d'adresses.

Services Web
Vous devez utiliser un transport HTTP pour connecter les processus de pipeline du noeud de pipeline aux services Web.

Démarrage de pipelines

Pour qu'un pipeline puisse recevoir et traiter des données, il doit d'abord être démarré. Il est courant d'exécuter plusieurs pipelines pour augmenter le débit de données ou traiter différents types de données source. La procédure ci-après permet de démarrer un pipeline ou d'en redémarrer un étant arrêté.

Avant de commencer

- L'exécutable de pipeline doit être installé sur le noeud de pipeline hébergeant ce pipeline.
- Au moins un fichier de configuration de pipeline doit être configuré à des fins d'utilisation avec le pipeline à démarrer. Vous pouvez spécifier le fichier de configuration de pipeline à utiliser dans le cadre de la commande de démarrage du pipeline. Si vous ne spécifiez pas le nom du fichier de configuration dans le cadre de la commande de pipeline, le fichier de configuration du pipeline doit se trouver sur le noeud de pipeline et il doit correspondre au nom de l'exécutable (nom de pipeline spécifié). Par exemple, pipeline.ini.
- Les variables d'environnement de la base de données doivent être définies. Pour plus d'informations, voir Définition des variables d'environnement.
- Si vous utilisez un script pour démarrer des pipelines, vérifiez qu'il se trouve dans le même répertoire que celui depuis lequel vous avez démarré le pipeline.
- Si la valeur de paramètre système *DEFAULT_CONCURRENCY* est définie sur une valeur supérieure à 1 ou si vous avez configuré le paramètre *concurrency* dans le fichier de configuration de pipeline pour le noeud de pipeline, vous pouvez démarrer plusieurs unités d'exécution de traitement de pipeline parallèles via une seule commande de démarrage de pipeline.

Pourquoi et quand exécuter cette tâche

Un pipeline est démarré en trois étapes :

Procédure

1. Chaque pipeline doit avoir un nom unique pour son noeud de pipeline, vérifiez donc qu'il n'existe aucun autre pipeline actif ayant le même nom que celui à démarrer. (Le nom de pipeline par défaut est `pipeline`.) Pour le vérifier, tapez la commande suivante à une invite de commande : `pipeline -n nompipeline -l`

   nompipeline étant le nom à utiliser pour démarrer le nouveau pipeline. Vérifiez que ce nom correspond à celui enregistré dans la console de configuration pour ce pipeline.
2. A une invite de commande, démarrez un ou plusieurs pipelines en spécifiant les options et paramètres de commande de pipeline appropriés via ce format :

   `pipeline -option paramètre`
3. Vérifiez que la commande a fonctionné et que le pipeline est démarré et actif.

a. Si votre système s'exécute sur une plateforme Microsoft Windows et que vous utilisez l'option de pipeline de services, vous pouvez voir l'état du pipeline dans le panneau de configuration des services Microsoft Windows.
b. Si votre système s'exécute sur une plateforme UNIX et que vous utilisez l'option de pipeline de type démons, vous pouvez taper la commande suivante pour vérifier les processus en cours d'exécution :

   `ps -fu idutilisateur`

   idutilisateur étant l'identification de l'utilisateur démarrant le pipeline.
c. Ou, à une invite de commande, tapez la commande suivante :

`pipeline -nnom_pipeline -l`

nompipeline étant le nom du pipeline que vous venez de démarrer. Si le pipeline est actif, l'invite de commande renvoie `En cours d'exécution`.

Arrêt des pipelines

L'arrêt d'un pipeline signifie faire passer son état actuel d'actif et ouvert pour traiter des données à inactif et fermé aux données entrantes. Vous pouvez arrêter manuellement un seul pipeline à la fois. Suivez ces instructions pour arrêter un pipeline après avoir apporté des modifications à la configuration système (puis redémarrez le pipeline pour que les modifications de configuration prennent effet) si vous installez un correctif logiciel ou une édition de mise à niveau, ou si vous apportez des modifications de configuration au noeud qui héberge le pipeline.

Procédure

1. Assurez-vous que le pipeline à arrêter est en cours d'exécution. Pour vérifier ceci : `pipeline -n nompipeline -l` sachant que *nom_pipeline* est le nom du pipeline à arrêter. L'invite de commande renvoie `En cours d'exécution` si le pipeline est actif.
2. Sur une ligne de commande, tapez la commande d'arrêt de pipeline : `pipeline -e -n nom_pipeline` sachant que *nom_pipeline* est le nom du pipeline à arrêter.

   Remarque : Si vous avez démarré le pipeline au moyen de l'option de commande de débogage, vous pouvez l'arrêter en appuyant sur **Ctrl** + **C** sur une ligne de commande.
3. Assurez-vous que la commande a abouti et que le pipeline s'est arrêté : `pipeline -nnom_pipeline -l` sachant que *nom_pipeline* est le nom du pipeline que vous venez d'arrêter. L'invite de commande renvoie `Arrêté` si le pipeline s'est arrêté.

Configuration des pipelines

Lorsqu'un pipeline démarre, il recherche un fichier de configuration de pipeline afin d'obtenir ses variables de démarrage et les informations de configuration initiales, nécessaires au traitement des données entrantes. Par défaut, lorsqu'un pipeline est installé sur le noeud de pipeline, le système installe également un fichier de configuration de pipeline par défaut nommé pipeline.ini, qui peut être utilisé par l'ensemble des pipelines de ce noeud de pipeline. Mais certaines sections de ce fichier par défaut doivent être configurées spécifiquement en fonction des pipelines exécutés sur le noeud de pipeline, et ce afin que le pipeline dispose des connexions et de l'accès adéquats à la base de données. Ces instructions permettent de configurer le fichier de configuration du pipeline.

Avant de commencer

- Vous devez connaître le nom exact de la base de données d'entités ainsi que les informations d'identité de connexion nécessaires pour accéder à la base de données d'entités.
- Si votre système se connecte à un logiciel de correction d'adresse externe, vous devez connaître le nom de la machine hôte de ce logiciel et pouvoir sélectionner les paramètres appropriés pour ce dernier.
- Pour que les modifications apportées au fichier de configuration prennent effet, vous devez arrêter tous les pipelines s'exécutant sur ce noeud de pipeline, puis redémarrer les pipelines une fois les modifications apportées.

Pourquoi et quand exécuter cette tâche

Le fichier de configuration pipeline.ini est un fichier texte ASCII standard. Vous pouvez le modifier à l'aide de n'importe quel éditeur de texte ASCII.

Procédure

1. procédez à une copie du fichier de configuration pipeline.ini par défaut et enregistrez l'original en lieu sûr. Si vous enregistrez une copie du fichier d'origine, vous pouvez y revenir si nécessaire.
2. Ouvrez la copie du fichier de configuration pipeline.ini dans l'éditeur de texte de votre choix.
3. Mettez à jour le fichier de façon à refléter la configuration qui convient pour les pipelines s'exécutant sur ce noeud de pipeline. En général, les valeurs par défaut du fichier de configuration de pipeline par défaut conviennent ; normalement, il suffit de saisir ou de mettre à jour les informations de connexion à la base de données sous l'en-tête [SQL], et les éventuelles informations de correction d'adresse dans la section [OAC], si votre système utilise un logiciel de correction d'adresse externe.
4. Enregistrez le fichier de configuration de pipeline mis à jour Le fichier doit être enregistré dans le répertoire dans lequel réside la commande de l'exécutable de pipeline. (sinon, vous devez indiquer le nom et l'emplacement de chemin complet du fichier de configuration de pipeline à chaque fois que vous démarrez un pipeline sur ce noeud de pipeline.)

Que faire ensuite

Si vous avez arrêté tous les pipelines s'exécutant sur ce noeud avant d'avoir apporté les modifications, vous pouvez redémarrer les pipelines. Si vous n'avez pas arrêté l'ensemble des pipelines avant d'apporter ces modifications, vous devez les arrêter et les redémarrer maintenant. Les pipelines en cours d'exécution n'appliquent les modifications apportées au fichier de configuration de pipeline qu'après avoir été redémarrés. Des erreurs peuvent survenir lorsque vous modifiez des informations de configuration de pipeline sans avant auparavant arrêté les pipelines : ces erreurs concernent notamment un arrêt de pipeline en raison de valeurs de fichier de configuration de pipeline incorrectes.

Inscription de pipelines

Avant de pouvoir en superviser le statut ou les résultats d'acheminement, vous devez d'abord inscrire les pipelines dans la console de configuration. Inscrire les pipelines n'est pas la même chose qu'installer ou configurer un pipeline ; cela signifie ajouter le pipeline à l'onglet **Pipelines** de la console de configuration.

Le système se sert des informations figurant dans l'onglet **Pipelines** pour identifier précisément le pipeline. Ces informations sont exploitées par les moniteur d'application pour signaler le statut et les statistiques des pipelines supervisés ou pour acheminer les communications et résultats entre les pipelines et les autres systèmes. Le nom sous lequel vous inscrivez un pipeline est exactement le même (casse comprise) que celui à utiliser quand vous le démarrez. Si vous utilisez un autre nom ou ne respectez pas la casse du pipeline inscrit, le moniteur d'application ne pourra ni acheminer ni superviser le pipeline, faute de le reconnaître.

Une fois qu'un pipeline a été inscrit dans l'onglet **Pipelines**, vous pouvez lui configurer des règles d'acheminement dans l'onglet **Routage**, en superviser le statut et les statistiques via l'onglet **Etat du pipeline**, ou les deux. Pour superviser le statut et les statistiques d'un pipeline, lorsque vous l'inscrivez, vous devez indiquer vouloir que le système supervise le pipeline.

Une fois qu'un pipeline est inscrit, vous ne pouvez plus en modifier le nom, mais vous pouvez mettre à jour les informations le concernant. Par exemple, si le nom du noeud de pipeline change, ou si vous souhaitez lancer la supervision du statut et des statistiques du pipeline, vous pouvez modifier ces informations.

Inscription de pipelines

Il existe trois raisons d'enregistrer un pipeline : pour utiliser le contrôle d'application afin de contrôler l'état et les statistiques du pipeline et/ou pour configurer les règles de routage du pipeline. Vous pouvez soit ajouter une nouvelle inscription de pipeline, soit baser l'inscription sur un pipeline existant.

Avant de commencer

Vous devez connaître le nom unique du pipeline ainsi que le nom du noeud qui héberge le pipeline. Le pipeline ne doit pas nécessairement être déjà installé et configuré sur le noeud du pipeline avant la procédure d'inscription. Il doit en revanche être installé et configuré pour que le système puisse vérifier le pipeline ou procéder au routage.)

Pourquoi et quand exécuter cette tâche

Astuce : si vous ajoutez plusieurs pipelines qui s'exécutent tous sur le même noeud, vous pouvez enregistrer le premier pipeline, puis cloner les autres pipelines à partir du premier pipeline ajouté.

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Pipelines**.
4. Effectuez l'une des opérations suivantes :
   - Pour enregistrer un nouveau pipeline, cliquez sur le bouton **Nouveau**.
   - Pour enregistrer un nouveau pipeline basé sur un pipeline existant, cliquez sur le bouton **Cloner**.
5. Dans l'onglet **Général**, indiquez le nom unique du pipeline, sa description, le nom du noeud du pipeline et si l'état et les statistiques du pipeline doivent être vérifiés.

   Remarque :

- Le nom de pipeline que vous indiquez est le même nom que celui devant être utilisé chaque fois que vous démarrez ce pipeline. Ce nom est sensible à la casse. Lorsque vous démarrez le pipeline, vous devez donc indiquer le nom exact sous lequel vous avez enregistré le pipeline. Si vous n'indiquez pas le nom exact (ou si vous modifiez la casse), ni les règles de routage configurées pour ce pipeline, ni le contrôle d'application ne fonctionneront.
- Si vous souhaitez contrôler l'état et les statistiques de ce pipeline dans l'onglet **Etat du pipeline** de la Console de configuration, sélectionnez **Oui** dans la zone **Contrôlé**.

6. Cliquez sur le bouton **Enregistrer**.

Que faire ensuite

Si l'ajout du pipeline abouti, celui-ci s'affiche dans la liste figurant sur la gauche de l'écran. Vous pouvez à présent définir les règles de routage pour ce pipeline ou utiliser le système pour contrôler le pipeline. Gardez toutefois à l'esprit que pour un routage ou un contrôle réussi du pipeline, celui-ci doit être démarré avec le nom exact (y compris la casse) du pipeline, tel qu'enregistré dans la zone **Nom du pipeline**.

Consultation des détails sur un pipeline enregistré

Vous pouvez consulter les détails relatifs à un pipeline enregistré dans la console de configuration afin de vous assurer que les informations figurant dans l'inscription sont à jour. L'inscription de pipelines permet au système de contrôler les performances et les statistiques de ces derniers, de les acheminer, voire les deux.

Avant de commencer

- Le pipeline doit être enregistré dans la console de configuration.

Procédure

1. Cliquez sur le bouton **Etat**.
2. Cliquez sur le bouton **Etat**.
3. Cliquez sur l'onglet **Général**.
4. Cliquez sur le nom du pipeline enregistré.

Résultats

Dans la fenêtre **Détail**, consultez les détails relatifs au pipeline sélectionné.

Modification d'inscriptions de pipelines

Modifiez les informations relatives à un pipeline enregistré lorsque l'un des composants principaux de l'inscription de pipeline a été modifié, par exemple le nom du noeud de pipeline. Le nom attribué à un pipeline correspond à la seule information que vous ne pouvez pas modifier. Si vous devez modifier le nom attribué à un pipeline, vous devez soit supprimer l'inscription du pipeline et l'ajouter à nouveau avec les informations qui conviennent, soit ajouter une autre inscription de pipeline.

Pourquoi et quand exécuter cette tâche

Si le pipeline que vous souhaitez modifier est actif (c'est-à-dire, en cours de fonctionnement), il est recommandé d'arrêter de l'arrêter avant de modifier son

inscription, notamment si vous modifiez son état de supervision.

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Pipelines**.
4. Sélectionnez les pipelines à modifier, puis cliquez sur le bouton **Editer**.
5. Modifiez les informations.

   Remarque : Gardez à l'esprit que pour contrôler l'état et les statistiques du pipeline dans l'onglet **Etat du pipeline**, la zone **Contrôlé** doit être définie sur **Oui**.
6. Cliquez sur le bouton **Enregistrer**.

Résultats

Vous pouvez consulter vos modifications dans l'onglet **Pipelines**.

Que faire ensuite

Si vous avez arrêté le pipeline, redémarrez-le.

Suppression d'inscriptions de pipelines

La suppression d'une inscription de pipeline dans la console de configuration ne supprime pas physiquement le pipeline du système, mais l'enlève des onglets **Pipelines**, **Règles de routage** et **Etat du pipeline**. Ces inscriptions supprimées ne peuvent plus acheminer d'informations au moyen de règles de routage ou fournir des informations de contrôle sur l'état et les statistiques. Il n'est pas possible de modifier un nom de pipeline enregistré. Si vous devez modifier le nom d'un pipeline enregistré, vous devez soit supprimer l'inscription du pipeline et l'ajouter à nouveau avec les informations qui conviennent, soit ajouter une autre inscription de pipeline.

Pourquoi et quand exécuter cette tâche

Si le pipeline que vous souhaitez supprimer est actif (c'est-à-dire, en cours de fonctionnement) et qu'il est contrôlé par le système dans l'onglet **Etat du pipeline**, il est recommandé de l'arrêter avant de le supprimer. Il est également recommandé de consulter l'onglet **Règles de routage** afin de voir si des règles de routage sont associées à ce pipeline ; si tel est le cas, vous pouvez réacheminer ces règles vers un autre pipeline ou ajouter un nouveau pipeline utilisant ces règles de routage avant de supprimer ce pipeline.

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **Général**.
3. Cliquez sur l'onglet **Noeuds**.
4. Sélectionnez les pipelines à supprimer, puis cliquez sur le bouton **Supprimer**.

Que faire ensuite

Le pipeline que vous avez supprimé ne s'affiche plus dans les onglets **Noeuds** ou **Règles de routage**. L'état du pipeline supprimé n'est plus affiché dans l'onglet **Etat**

du pipeline. Le système n'achemine plus aucune règle de routage attribuée au pipeline supprimé dans l'onglet **Règles de routage**.

Rubriques d'aide

Onglet Pipelines

L'onglet **Pipelines** permet d'enregistrer un pipeline ou de modifier, supprimer ou consulter les pipelines enregistrés. Lorsque des pipelines sont enregistrés dans cet onglet et qu'un agent SNMP est installé et configuré sur le noeud de pipeline exécutant le pipeline enregistré, vous pouvez voir l'état, les statistiques et les performances de ce dernier dans l'onglet **Etat**. Vous pouvez également utiliser l'onglet **Règles de routage** pour configurer et acheminer les résultats d'un pipeline enregistré vers d'autres bases de données et systèmes externes.

Nom du pipeline
Répertorie le nom de chaque noeud enregistré pour le contrôle d'application dans la console de configuration, par ordre alphabétique.

Description
Fournit du texte complémentaire, qui peut décrire plus précisément ce noeud et le distinguer des autres noeuds système.

Nom d'hôte
Affiche le nom du noeud de pipeline hébergeant ce pipeline. (Si vous prévoyez de contrôler ce pipeline, il s'agit également du serveur où un agent SNMP doit être installé et en cours d'exécution.)

Contrôlé
Indique si l'état et les statistiques de ce pipeline sont contrôlés et consignés dans l'onglet **Etat** (il ne s'agit pas de la même chose que l'état actuel du pipeline ; cette colonne indique la façon dont le pipeline est actuellement enregistré).

- Oui indique que ce pipeline enregistré est contrôlé par le moniteur d'application.
- Non indique que ce pipeline n'est pas configuré pour le contrôle d'application mais qu'il l'est peut-être pour le routage.

Pipelines - Onglet Détails

Cet onglet permet d'enregistrer un pipeline ou de consulter les détails d'un pipeline enregistré existant. Vous devez enregistrer un pipeline avant de configurer les règles de routage associées dans l'onglet **Routage** ou de contrôler ses statistiques et son état dans l'onglet **Etat**.

Toutes les zones de cet onglet sont obligatoires pour enregistrer un pipeline. Une fois enregistré, vous pouvez modifier tous les paramètres d'un pipeline, à l'exception de son nom. Par exemple, si vous devez renommer le noeud de pipeline (zone **Nom d'hôte**), modifiez son nom. En revanche, si vous devez renommer un pipeline, vous devez d'abord supprimer le pipeline incorrect enregistré ici, puis ajouter à nouveau ce pipeline avec les informations correctes.

Nom du pipeline
Attribuez au pipeline un nom unique de 15 caractères maximum. Si vous voulez contrôler ou effectuer un routage vers ou depuis le pipeline, le nom doit concorder parfaitement avec celui du pipeline enregistré quand vous démarrez le pipeline, casse comprise.

La liste de gauche affiche le nom de tous les pipelines déjà enregistrés.

Description
Saisissez une description du pipeline (50 caractères maximum) afin de le différencier des autres. Utilisez par exemple cette description pour indiquer à quoi sert le système ou pour préciser le type de source de données traité par le système.

Nom d'hôte
Tapez le nom du noeud de pipeline qui exécute ce pipeline.

Contrôlé
Indiquez si le moniteur d'application fournit l'état de ce pipeline.

- **Oui** indique que vous souhaitez contrôler l'état et les statistiques de ce pipeline. Lorsqu'il a été correctement enregistré dans la console de configuration et que l'agent SNMP s'exécute sur le noeud de pipeline, l'état et les statistiques du pipeline s'affichent dans l'onglet **Etat**.
- **Non** indique que vous souhaitez enregistrer ce pipeline pour le routage et pas pour le contrôle. L'état et les statistiques de ce pipeline ne s'afficheront pas dans l'onglet **Etat**, mais vous pouvez configurer des règles de routage pour le pipeline enregistré.

Configuration des règles de routage

Les règles de routage permettent d'acheminer les résultats du traitement des pipelines ou du programme d'acquisition vers une base de données, un pipeline ou un système externe. Les règles de routage sont configurées dans l'onglet **Règles de routage** de la console de configuration, mais vous pouvez uniquement acheminer des données depuis des pipelines ou des programmes d'acquisition enregistrés au moyen du moniteur d'application. Vous pouvez configurer une nouvelle règle de routage en intégralité ou à partir d'une règle de routage existante.

Avant de commencer

- Le pipeline ou le programme d'acquisition depuis lequel vous souhaitez acheminer des données doit être enregistré auprès du moniteur d'application.
- Vous devez connaître le nom unique exact sous lequel le pipeline ou le programme d'acquisition a été enregistré.
- Vous devez connaître la méthode de transport à utiliser, ainsi que la syntaxe d'URI de transport spécifique que vous devez respecter pour l'acheminement à destination.

Procédure

1. Cliquez sur l'onglet **Configurer**.
2. Cliquez sur l'onglet **Général**.
3. Cliquez sur l'onglet **Règles de routage**.
4. Effectuez l'une des opérations suivantes :
   - Pour configurer une nouvelle règle de routage, cliquez sur le bouton **Nouveau**.
   - Pour configurer une nouvelle règle de routage à partir d'une règle existante, cochez la case en regard de la règle de routage sur laquelle baser la nouvelle règle, puis cliquez sur le bouton **Cloner**.
5. Obligatoire : dans la zone **Pipeline d'origine**, saisissez le nom enregistré du pipeline ou du programme d'application depuis lequel le routage doit s'effectuer. Le nom que vous indiquez doit être identique à celui figurant dans l'onglet **Pipelines**.

6. Obligatoire : Dans la zone **Ordonner**, saisissez un nombre, compris entre 0 et 999, indiquant l'ordre dans lequel le système doit utiliser cette règle de routage. Par défaut, cette zone est définie sur 0, qui correspond à la première règle de routage traitée pour n'importe quel pipeline ou programme d'acquisition. Le nombre figurant dans cette zone doit être unique pour ce pipeline ou programme d'acquisition, notamment s'il existe déjà plusieurs règles de routage configurées pour le pipeline ou le programme d'acquisition.

   Remarque : Dans le volet gauche de cet onglet, consultez la liste des pipelines ou des programmes d'acquisition disposant de règles de routage déjà configurées. Si ce pipeline ou noeud figure dans la liste, cherchez le nombre le plus élevé suivant les deux-points après le nom du pipeline ou du programme d'acquisition, puis saisissez le prochain numéro le plus élevé. Par exemple, si vous configurez une nouvelle règle de routage pour le pipeline PIPE08 et que PIPE08:0 figure dans la liste du volet gauche, vous devez saisir le chiffre 1 ou un chiffre plus élevé dans la zone Ordonner.
7. Obligatoire : Dans la zone **Destination**, saisissez l'URI de transport de la destination des informations acheminées. Cet élément indique au système comment acheminer les données au pipeline, à la base de données ou au système externe destinataire.

   Remarque : Pour que le routage aboutisse, le processus destinataire doit être accessible au moyen du même URI de transport spécifié. Par exemple, si la destination est un pipeline, ce dernier doit être démarré au moyen du même URI de transport.
8. Obligatoire : Dans la liste déroulante **Document**, sélectionnez le type de document UMF avec lequel indiquer le type de message à acheminer à destination.
9. Facultatif : Dans la zone **Filtre de route**, indiquez le filtre à appliquer aux informations à acheminer, et ce afin que le système achemine uniquement des informations particulières vers la destination. Les filtres constituent une fonction avancée de règles de routage. Une expression de filtrage se saisit au format `MODDIST(`*`nom_balise_UMF`*, où (*`nom_balise_UMF`* désigne le nom de la balise UMF utilisée par le système pour distribuer les enregistrements.
10. Obligatoire : Dans la liste déroulante **Activé**, sélectionnez **Oui** pour activer cette règle de routage.
11. Obligatoire : Cliquez sur le bouton **Enregistrer**.

Exemple

Que faire ensuite

Le nom du pipeline ou du programme d'acquisition s'affiche dans l'onglet **Règles de routage** et comporte les détails relatifs à la règle de routage que vous venez de configurer. Le système commence à acheminer les informations de routage du pipeline ou du programme d'acquisition vers la destination, et ce à l'aide de la règle de routage configurée.

Règles de routage

Les règles de routage ordonnent au moniteur d'application d'envoyer des messages d'un programme d'acquisition à un pipeline, ou d'un pipeline à une base de données ou à un système externe. Les règles de routage ne peuvent être configurées que pour les pipelines qui ont été inscrits auprès du moniteur

d'application, mais les résultats peuvent être acheminés vers n'importe quelle destination au moyen de la syntaxe de transport URI (Universal Resource Indicator.

Les règles de routage trouvent de nombreuses utilisations, dont voici les plus courantes :

- Equilibrer la charge de données entre un programme d'acquisition (par exemple l'utilitaire de base de données UMF) et plusieurs pipelines en vue du traitement des données.
- Diriger les résultats du traitement de pipeline (par exemple les alertes) sur un système externe ou une base de données de rapports à des fins d'investigations ou rapports plus poussés

Documents UMF et règles de routage

Les règles de routage sont configurées pour acheminer les messages au moyen de types de document UMF. Votre choix dépend des informations provenant du noeud pipeline ou de système d'où le routage doit s'effectuer. Par exemple, UMF_ALERT est un type de document UMF représentant les alertes générées par le traitement des fiches d'identité et d'entité via un pipeline. Vous pouvez acheminer n'importe quelles alertes générées depuis un pipeline particulier vers un système externe, par exemple une interface utilisée par les analystes menant les investigations sur les alertes déclenchées par le système.

Vous pouvez configurer une règle de routage chargée d'acheminer soit tous les types de document UMF, soit un type de document UMF précis, y compris type de document UMF personnalisé configuré pour votre système.

Filtres

Vous pouvez filtrer les informations qui sont acheminées vers la destination en désignant une expression de filtrage lorsque vous configurez une règle de routage. Les filtres indiquent que seules certaines informations particulières sont acheminées à destination.

Un filtre de routage s'élabore au moyen de l'expression `MODDIST(`*`nom_balise_UMF`*`)`, sachant que

`MODDIST`
: est l'expression qui indique une distribution modulaire.

`(`*`nom_balise_UMF`***`)`**
: identifie la balise UMF qui indique au système comment distribuer les fiches. A l'aide de la balise UMF identifiée, le système totalise les valeurs ASCII de tous les caractères de cette balise afin de déterminer le nombre de routes nécessaires à l'équilibrage de la charge de traitement des données.

Si vous souhaitiez acheminer toutes les fiches d'un code de source de données «source_de_données5» à une base de données de rapports distincte, vous pourriez configurer une règle de routage au moyen de l'expression de filtrage `MODDIST(datasource5)` , sachant que `source_de_données5` désigne le code de source de données.

Processus de routage

Quand une règle de routage est configurée pour un pipeline ou un programme d'acquisition, les explications ci-dessous décrivent comment le moniteur d'application effectue le processus de routage :

1. Quand le pipeline ou programme d'acquisition démarre, il envoie une demande au moniteur d'application au moyen d'un message UMF.
2. Le moniteur d'application reçoit la demande et recherche toutes les règles de routage actives concernant le pipeline ou programme d'acquisition demandeur.
3. S'il localise une règle de routage active pour le pipeline ou programme d'acquisition demandeur, il fabrique un document UMF indiquant les instructions de routage, et renvoie ce document UMF au pipeline ou programme d'acquisition demandeur.
4. Le pipeline ou programme d'acquisition demandeur interprète le message du document UMF et crée un fichier de routage portant l'extension *.RTE (* étant le nom du pipeline ou programme d'acquisition demandeur). Si le pipeline ou programme d'acquisition ne peut communiquer avec le moniteur d'application au démarrage, il cherche à consulter les instructions dans le fichier de routage.
5. Le pipeline ou programme d'acquisition demandeur ouvre les transports nécessaires pour communiquer avec la destination configurée dans la règle de routage.
   - Si le pipeline ou programme d'acquisition parvient à ouvrir le transport et à localiser la destination, il achemine les messages de document UMF adéquats vers la destination tant qu'il est allumé et qu'il traite activement les données.
   - Si le pipeline ou programme d'acquisition ne parvient pas à ouvrir le transport ou si la destination est introuvable, il s'arrête, en signalant une erreur.

Rubriques d'aide

Onglet Règles de routage

Cet onglet permet d'afficher ou de supprimer des règles de routage existantes et d'en configurer de nouvelles pour les pipelines enregistrés dans l'onglet **Pipelines**. Une fois qu'une règle de routage est configurée, elle ne peut plus être modifiée, mais uniquement supprimée.

Pipeline d'origine
Affiche le nom du noeud de pipeline qui est configuré avec une règle de routage.

Ordre Affiche l'ordre dans lequel cette règle de routage est traitée par le pipeline dans la colonne **Pipeline d'origine**. Cet ordre est utile lorsqu'il existe plusieurs règles de routage ; il est souvent défini sur 0.

Destination
Affiche l'URI de transport du pipeline, de la base de données ou du système externe.

Type de document
Affiche le type de document UMF que cette règle de routage envoie. Il s'agit du type de document correspondant aux résultats traités par le pipeline dans la colonne **Pipeline d'origine**. Cette sélection peut être soit un type de document UMF précis, soit un astérisque (*), ce qui signifie que cette règle de routage achemine tous les types de document UMF.

Activé Indique si cette règle de routage est active ou non :

- **Oui** indique qu'elle est activée. Dès que le pipeline ou noeud affiché dans la colonne **Pipeline d'origine** traite les résultats d'un type de document spécifique, le système achemine les données associées à ce type de document UMF vers la destination indiquée dans la colonne **Destination**.
- **Non** indique que la règle de routage n'est pas activée.

Onglet Détails des règles de routage

Cet onglet permet de configurer une nouvelle règle de routage ou de consulter les détails d'une règle de routage existante. Les règles de routage sont généralement configurées pour publier des types de résultats traités spécifiques depuis un pipeline vers une autre base de données ou un autre système externe. Vous ne pouvez configurer des règles de routage que pour les pipelines enregistrés dans l'onglet **Pipelines**.

Toutes les zones à l'exception de la zone **Filtre de route**, sont obligatoires pour configurer correctement une nouvelle règle de routage. Une fois configurée, une règle de routage de ne plus être modifiées ; pour la modifier, vous devez en fait la supprimer, puis l'ajouter à nouveau avec les informations correctes.

Pipeline d'origine
Saisissez le nom du pipeline d'où vous voulez acheminer le résultats. Le nom de ce pipeline doit correspondre parfaitement avec celui enregistré dans l'onglet **Pipelines**, casse comprise ; si le nom ne concorde pas, le système affiche un message d'erreur indiquant que le pipeline spécifié n'existe pas.

Ordre Entrez un nombre compris entre 0 et 999 pour indiquer l'ordre dans lequel le système applique cette règle de routage au pipeline enregistré dans la zone **Pipeline d'origine**. Par défaut, cette zone contient la valeur 0, qui signifie que le système traite cette règle en premier. Si une ou plusieurs règles de routage sont déjà configurées pour ce pipeline, entrez un nombre supérieur à l'ordre le plus élevé.

Consultez le volet de gauche pour connaître l'ordre défini pour toute règle de routage existante déjà configurée pour ce pipeline ; il est indiqué par le numéro séquentiel qui suit les deux-points après le nom du pipeline. Par exemple : PIPE08:0 indique qu'une règle de routage est déjà configurée pour le pipeline PIPE08 et qu'elle est définie pour être traitée en premier. Si vous avez configuré une nouvelle règle de routage pour PIPE08, définissez l'ordre sur 1.

Destination
Saisissez l'URI de transport vers le pipeline, la base de données ou le système externe de destination vers lequel acheminer les résultats traités. Veillez à utiliser la syntaxe adaptée au type de transport utilisé.

Liste déroulante Type de document
Dans la liste déroulante, sélectionnez le type de document UMF à acheminer depuis le pipeline enregistré vers la destination. Pour acheminer tous les résultats traités vers la destination, sélectionnez l'astérisque *.

Filtre de route
Pour indiquer que seules certaines informations doivent être acheminées vers la destination, saisissez l'expression que le système doit appliquer pour filtrer les valeurs UMF acheminées par cette règle de routage. Par exemple, pour acheminer uniquement les enregistrements d'identité ou

d'entité d'une source de données spécifique, vous pouvez taper le filtre DSRC_CODE=x, où *x* correspond au code unique de la source de données à laquelle appliquer le filtre.

Les filtres constituent une fonction avancée de règles de routage.

Liste déroulante activée

Sélectionnez une option dans la liste déroulante :

- **Oui** signifie que le moniteur d'application achemine les informations du pipeline vers la destination conformément à cette règle de routage.
- **Oui** signifie que le moniteur d'application n'achemine pas les informations du pipeline conformément à cette règle de routage.

Suppression de règles de routage

Une fois configurée, une règle de routage ne peut plus être modifiée ; vous devez en fait supprimer l'ancienne règle de routage et en configurer une nouvelle si vous devez corriger ou mettre à jour des informations. Il se peut que vous deviez également supprimer une règle de routage devenue superflue. Vous pouvez supprimer une ou plusieurs règles de routage configurées dans l'onglet **Règles de routage** de la console de configuration.

Procédure

1. Cliquez sur l'onglet **Configurer**.
2. Cliquez sur l'onglet **Général**.
3. Cliquez sur l'onglet **Règles de routage**.
4. Cochez la case en regard de chaque règle de routage configurée que vous souhaitez supprimer.
5. Cliquez sur le bouton **Supprimer**.

Que faire ensuite

Le système supprime les règles de routage sélectionnées et n'achemine plus les informations au moyen des règles de routage supprimées.

Statut et statistiques de pipeline

La supervision du statut, des statistiques et des performances d'un pipeline est importante pour le maintenir en état de fonctionner, équilibrer les charges de données et détecter les problèmes potentiels avant qu'ils ne surviennent.

Avant de pouvoir consulter le statut et les statistiques d'un pipeline, il faut que les procédures suivantes aient réussi :

1. Le pipeline est installé et configuré sur son noeud de pipeline.

Remarque : (Plateformes Windows uniquement) Si vous démarrez le pipeline en tant que service, vous pouvez afficher dans l'observateur d'événements Windows des informations de statut supplémentaires que vous ne pouvez pas visualiser ailleurs.

Informations de statut et de statistiques

Une fois qu'un pipeline commence à traiter les données, vous pouvez consulter des informations concernant l'exception UMF dans la console de configuration :

- Exceptions UMF dans l'onglet **Exceptions UMF**

Agents SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole standard qui sert à superviser les systèmes et les périphériques de réseau. Les agents SNMP sollicitent périodiquement le statut et les statistiques de chaque pipeline inscrit sur le système. Les information que l'agent SNMP recueille sur chaque pipeline inscrit s'affichent dans l'onglet **Etat du pipeline**.

Pour que les agents SNMP puissent superviser les pipelines :

- Il faut qu'un agent SNMP soit installé et configuré sur le noeud de pipeline qui exécute les pipelines à superviser.
- Chaque pipeline à superviser doit être inscrit dans la console de configuration et configuré pour la supervision.
- Il faut que l'agent SNMP soit démarré et en cours de fonctionnement sur le noeud de pipeline, en utilisant le même numéro de port que celui configuré lors de l'installation du pipeline. Ce numéro de port de l'agent SNMP s'étend à tous les systèmes et n'est pas limité à chaque noeud de pipeline. Le numéro de port SNMP par défaut est 13516, mais vous pouvez rechercher le numéro de port d'agent SNMP défini dans le fichier server.xml qui se trouve sous chaque noeud de pipeline.

Les agents SNMP sont services qu'il est donc possible d'arrêter et démarrer selon les besoins.

Exemple d'utilisation d'un agent SNMP

La société ABC supervise tous ses pipelines au moyen du moniteur d'application. Elle a ajouté un autre serveur (EAS-2) afin d'héberger trois nouveaux pipelines, dits Pipeline300, Pipeline310 et Pipeline320. Pour superviser ces pipelines, les collaborateurs de la société ABC doivent effectuer les opérations suivantes :

- Installez et configurez un agent SNMP sur le noeud de pipeline EAS-2.
- Dans la console de configuration, inscrivez chaque nouveau pipeline (Pipeline300, Pipeline310 et Pipeline320) dans l'onglet **Pipelines**.
- Démarrez l'agent SNMP sur le noeud de pipeline EAS-2. Assurez-vous que l'agent SNMP utilise le numéro de port omni-système qui a été configuré quand vous avez installé les pipelines sur ce noeud.
- Démarrez pour le traitement chaque pipeline inscrit. Veillez à taper le nom exact qui a été attribué au pipeline, car les noms de pipelines inscrits sont sensibles à la casse.

Une fois les nouveaux pipelines en cours de fonctionnement, les collaborateurs de la société ABC peuvent en superviser le statut et les statistiques via la console de configuration.

Démarrage d'agents SNMP

Pour superviser l'état et les statistiques d'un ou plusieurs pipelines dans la console de configuration, vous devez démarrer un agent SNMP sur le noeud où ces pipelines s'exécutent.

Avant de commencer

- Il faut qu'un agent SNMP soit installé et configuré sur le noeud où les pipelines s'exécutent.
- Les pipelines doivent être enregistrés dans l'onglet **Pipelines** de la console de configuration et configurés pour la supervision.

Procédure

1. A partir d'une ligne de commande sur le noeud de pipeline, à l'aide de la commande**Changer de répertoire** accédez au répertoire de base.
2. Tapez la commande suivante : **java -jar SNMPAgent**-p *numéro de port numéro de port* étant le numéro de port du système configuré lors de l'installation des pipelines pour les agents SNMP. Le numéro de port par défaut est 13516.

   Remarque : Vous trouverez le numéro de port d'agent SNMP configuré dans le fichier server.xml sur le noeud du pipeline.

Résultats

L'agent SNMP démarre.

Que faire ensuite

Dans la console de configuration, sélectionnez l'onglet**Etat du pipeline** pour vous assurer que l'agent SNMP s'exécute. Dans l'affirmative, l'agent SNMP indiquera l'état et les statistiques de tous les pipelines en fonctionnement sur ce noeud de pipeline. Il est inutile de redémarrer l'agent SNMP si vous ajoutez des pipelines tant que les fichiers .SHM se trouvent dans le même répertoire, qui est normalement celui où l'agent SNMP est démarré.

Arrêt d'agents SNMP

Arrêtez un agent SNMP sur un noeud de pipeline dès que vous devez apporter des modifications au noeud (par exemple, des mises à jour de la configuration).

Avant de commencer

Un agent SNMP doit être en cours d'exécution sur le noeud de pipeline. Il est par ailleurs recommandé d'arrêter tout pipeline s'exécutant sur ce noeud sous le contrôle du moniteur d'applications.

Procédure

Dans la fenêtre qui exécute l'agent SNMP, actionnez les touches **Ctrl** + **C**.

Que faire ensuite

- L'agent SNMP s'arrête.
- Dans la console de configuration, l'onglet **Etat du pipeline** affiche l'état ARRETE pour tous les pipelines de ce noeud.

Vérification du statut des pipelines dans la console de configuration

Il est important d'effectuer le suivi de l'état des pipelines,car en cas de panne d'un pipeline, une partie du système est arrêtée. Vous pouvez consulter rapidement l'état et les statistiques de performances les plus récents d'un pipeline à l'aide de l'onglet **Etat du pipeline** de la Console de configuration. Le contrôle d'application reçoit les informations des agents SNMP actifs, qu'il interroge avant de régénérer l'onglet **Etat du pipeline** toutes les 60 secondes.

Avant de commencer

- Un agent SNMP doit être installé et configuré sur le noeud sur lequel s'exécutent les pipelines devant faire l'objet d'un suivi.
- L'agent SNMP doit être lancé à l'aide du numéro de port omni-système configuré lors de l'installation du pipeline (également indiqué dans le fichier server.xml).
- Le pipeline doit être enregistré dans l'onglet **Pipelines** de la Console de configuration et il doit être configuré pour faire l'objet d'un suivi.
- Démarrez le pipeline en utilisant exactement le même nom et la même casse que pour le nom du pipeline enregistré dans l'onglet **Pipelines**.

Pourquoi et quand exécuter cette tâche

Si vous ne parvenez pas à consulter l'état du pipeline via la Console de configuration, vous pouvez utiliser une ligne de commande.

Procédure

1. Cliquez sur le bouton **Etat**.
2. Cliquez sur le bouton **Etat du pipeline**.
3. Recherchez le nom du pipeline à vérifier dans la colonne **Nom du pipeline** (les pipelines sont répertoriés par nom selon leur ordre alphanumérique). Recherchez ensuite les informations figurant dans les colonnes d'état et de statistiques de transactions sur la ligne correspondant au nom du pipeline.

Que faire ensuite

Vous pouvez également consulter d'autres informations sur ce pipeline en cliquant sur les différents boutons. Par exemple, si vous souhaitez savoir quand ce pipeline a été démarré pour la dernière fois, cliquez sur l'onglet **Evénements**.

Vérification de l'état des pipelines au moyen de la ligne de commande

Il est important d'effectuer le suivi de l'état des pipelines,car en cas de panne d'un pipeline, une partie du système est arrêtée. De nombreuses entreprises vérifient les pipelines via l'onglet **Etat du pipeline** de la Console de configuration. Cet onglet affiche l'état et les statistiques les plus récents sur la base d'une interrogation automatique du système toutes les 60 secondes. Vous pouvez également utiliser une ligne de commande pour vérifier l'état d'un pipeline en particulier ou de tous les pipelines d'un noeud spécifique (la vérification par ligne de commande indique uniquement l'état du pipeline, pas les statistiques de performances du pipeline.)

Avant de commencer

- Un agent SNMP doit être installé et configuré sur le noeud qui exécute le pipeline.
- Il faut que l'agent SNMP soit démarré et en cours de fonctionnement sur le noeud de pipeline, en utilisant le même numéro de port que celui configuré lors de l'installation du pipeline. Ce numéro de port de l'agent SNMP s'étend à tous les systèmes et n'est pas limité à chaque noeud de pipeline. Le numéro de port SNMP par défaut est 13516, mais vous pouvez rechercher le numéro de port d'agent SNMP défini dans le fichier server.xml qui se trouve sous chaque noeud de pipeline.

Procédure

1. A partir d'une ligne de commande du noeud de pipeline, effectuez l'une des étapes ci-après :
   - Pour vérifier l'état de tous les pipelines figurant sur ce noeud, saisissez la commande suivante : **pipeline -l**
   - Pour vérifier l'état d'un pipeline en particulier sur ce noeud de pipeline, saisissez la commande suivante : **pipeline -n nom_pipeline -l**

   où *nom_pipeline* est le nom unique du pipeline que vous souhaitez vérifier.

   Remarque : Le nom que vous saisissez doit correspondre au nom utilisé pour démarrer le pipeline.
2. Appuyez sur **Entrée**.

Résultats

Le système renvoie l'un des états suivants pour chaque pipeline :

- En cours d'exécution pour tous les pipelines actifs.
- Arrêté pour tous les pipelines inactifs.

Exemple

Par exemple, pour vérifier l'état du pipeline 08, vous devez saisir la commande suivante : **pipeline -n pipeline08 -l**

Que faire ensuite

Si l'état d'un pipeline est répertorié de façon inattendue dans la liste Arrêté, vous pouvez utiliser les rubriques de dépannage pour en découvrir la cause.

Consultation des évènements du moniteur d'application

Les événements du moniteur d'applications se produisent chaque fois qu'un message est échangé entre le moniteur d'applications et les pipelines enregistrés dans l'onglet **Pipelines** de la console de configuration. Ces messages contiennent des informations diverses, qui signalent par exemple quand un pipeline démarre ou s'arrête ou quand le système consigne des erreurs ou des avertissements, hormis pour les exceptions UMF (Universal Message Format). Ces informations peuvent vous aider à aider à remédier aux erreurs survenues sur un pipeline particulier.

Avant de commencer

- Le pipeline doit être enregistré dans l'onglet **Pipelines** de la console de configuration.
- Le pipeline doit avoir été démarré sur le noeud enregistré dans l'onglet **Pipelines** avec le nom de pipeline enregistré affiché dans l'onglet **Pipelines**.

Pourquoi et quand exécuter cette tâche

Si le pipeline est enregistré dans l'onglet **Pipelines** de la console de configuration, vous pouvez afficher les événements actuels ou historiques dans l'onglet **Evénements** de la console de configuration.

Procédure

1. Cliquez sur le bouton **Etat**.
2. Cliquez sur le bouton **Evénements**.
3. Facultatif : Dans la zone **Date de début**, entrez la date à partir de laquelle vous souhaitez consulter les événements du moniteur d'applications au format mm/jj/aaaa. Si vous laissez cette zone vide, le système affiche toutes les exceptions du moniteur d'applications qui sont conformes aux autres critères définis, à partir de la date de mise en service du système. Si vous tapez une date dans cette zone, il est inutile d'en saisir une dans la zone **Date de fin**.
4. Facultatif : Dans la zone **Date de fin**, entrez la date jusqu'à laquelle vous souhaitez consulter les événements du moniteur d'applications au format mm/jj/aaaa. Si vous laissez cette zone vide, le système affiche tous les événements du moniteur d'applications qui sont conformes aux autres critères définis, jusqu'à la date du jour. Si vous tapez une date dans cette zone, il est inutile d'en saisir une dans la zone **Date de début**.
5. Facultatif : Dans la zone **Pipeline d'origine**, tapez le nom enregistré du pipeline spécifique pour lequel vous souhaitez consulter les événements du moniteur d'applications. Si vous laissez cette zone vide, le système affiche tous les événements du moniteur d'applications qui sont conformes aux autres critères définis pour l'ensemble des pipelines (par nom enregistré).
6. Facultatif : Dans la liste déroulante **Nombre max**, sélectionnez le nombre maximal d'événements du moniteur d'applications à afficher. Le nombre d'événements conformes à tous les autres critères définis qui va être affiché par le système est inférieur ou égal à cette valeur. Si le nombre d'exceptions est plus important que cette limite, le système ne les affiche pas. S'il y a moins d'exceptions que le nombre indiqué, tous les événements du moniteur d'applications qui sont conformes à l'ensemble des autres critères définis sont affichés.
7. Obligatoire : Cliquez sur le bouton **Search**.

Exemple

Par exemple, pour afficher les 500 derniers événements du moniteur d'applications qui sont survenus aujourd'hui pour le pipeline08, vous devrez indiquer les critères suivants :

- Dans la zone **Date de début**, la date du jour.
- Dans la zone **Date de fin**, la date du jour.
- Dans la zone **Pipeline d'origine**, vous taperez `pipeline08`.
- Vous sélectionnerez **500** dans la liste déroulante **Nombre max**.

Que faire ensuite

Vous pouvez étudier plus en détail un événement du moniteur d'applications en cliquant dessus. Les informations affichées sont celles qui ont été fournies concernant l'événement lorsque celui-ci est survenu.

Consultation des exceptions UMF

Les exceptions UMF signalent des problèmes au niveau des données entrantes en cours de traitement par un pipeline. Ils surviennent quand la structure des données entrantes ne peut pas faire l'objet d'une analyse syntaxique. En général, les exceptions UMF n'étant pas comptabilisées dans le nombre limite d'erreurs de pipeline, le système consigne l'exception UMF et le traitement du pipeline se

poursuit. Ces informations peuvent vous aider à résoudre les problèmes liés aux données entrantes d'un pipeline spécifique.

Avant de commencer

- Le pipeline doit être enregistré dans l'onglet **Pipelines** de la console de configuration.
- Il faut que le pipeline ait été démarré sur le noeud enregistré dans l'onglet **Pipelines** avec le nom du pipeline enregistré tel qu'il apparaît dans l'onglet **Pipelines**.

Pourquoi et quand exécuter cette tâche

Si le pipeline est enregistré dans l'onglet **Pipelines** de la console de configuration, vous pouvez afficher les exceptions UMF actuelles ou historiques dans l'onglet **Exceptions UMF** de la console de configuration.

Procédure

1. Cliquez sur le bouton **Etat**.
2. Cliquez sur le bouton **Exceptions UMF**.
3. Facultatif : Dans la zone **Date de début**, entrez la date à partir de laquelle vous souhaitez consulter les exceptions UMF au format mm/jj/aaaa. Si vous laissez cette zone vide, le système affiche toutes les exceptions UMF répondant aux autres critères définis, à partir de la date de mise en service du système. Si vous tapez une date dans cette zone, il est inutile d'en saisir une dans la zone **Date de fin**.
4. Facultatif : Dans la zone **Date de fin**, entrez la date jusqu'à laquelle vous souhaitez consulter les exceptions UMF au format mm/jj/aaaa. Si vous laissez cette zone vide, le système affiche toutes les exceptions UMF répondant aux autres critères définis, jusqu'à la date du jour. Si vous tapez une date dans cette zone, il est inutile d'en saisir une dans la zone **Date de début**.
5. Facultatif : Dans la zone **Pipeline d'origine**, tapez le nom enregistré du pipeline spécifique pour lequel vous souhaitez consulter les exceptions UMF. Si vous laissez cette zone vide, le système affiche toutes les exceptions UMF pour l'ensemble des pipelines, par nom enregistré, répondant aux autres critères définis.
6. Facultatif : Dans la liste déroulante **Nombre max**, sélectionnez le nombre maximal d'exceptions UMF à afficher. Le système affiche un nombre inférieur ou égal à cette valeur d'exceptions UMF répondant à tous les autres critères définis. Si le nombre d'exceptions est plus important que cette limite, le système ne les affiche pas. S'il y a moins d'exceptions que le nombre indiqué, tous les événements du moniteur d'application répondant à tous les autres critères définis s'affichent.
7. Obligatoire : Cliquez sur le bouton **Search**.

Exemple

Par exemple, pour afficher les 50 dernières exceptions UMF survenues aujourd'hui pour le pipeline08, vous devrez indiquer les critères suivants :

- Dans la zone **Date de début**, la date du jour.
- Dans la zone **Date de fin**, la date du jour.
- Dans la zone **Noeud d'origine**, vous taperiez `pipeline08`.
- Dans la zone **Nombre max**, vous sélectionneriez `50`.

Que faire ensuite

Vous pouvez étudier plus en détail une exception UMF en cliquant dessus. Les informations affichées sont celles qui ont été consignées à propos de l'exception lorsque celle-ci est survenue.

Consultation des nouvelles identités

L'onglet **Nouvelles identités** de la console de configuration affiche les nouvelles identités traitées par le pipeline du système au cours des sept derniers jours. Cet onglet vous permet de vérifier les volumes de données entrantes et de vous assurer que les nombres sont conformes à la quantité de données entrantes ou au nombre de pipelines actifs. Vous pouvez en outre vérifier ponctuellement les sources de données en cours de chargement dans le pipeline afin de savoir lesquelles alimentent le système en données.

Procédure

1. Cliquez sur le bouton **Etat**.
2. Cliquez sur le bouton **Nouvelles identités**.

Résultats

Le système affiche la liste de toutes les nouvelles identités traitées au cours des sept derniers jours.

Rubriques d'aide

Onglet Etat du pipeline

Cet onglet permet de consulter l'état en cours, les statistiques et les informations de performances relatives aux pipelines enregistrés configurés pour le contrôle par le moniteur d'application et l'agent SNMP. Le système collecte l'état et les statistiques auprès de l'agent SNMP toutes les minutes et actualise l'onglet **Etat du pipeline**.

Remarque : Chaque agent SNMP s'exécutant sur chaque noeud de pipeline doit utiliser le même numéro de port sur l'ensemble du système. Ce numéro de port est configuré lors de l'installation des pipelines sur un noeud de pipeline. Le numéro de port par défaut de l'agent SNMP est 13516, mais vous pouvez rechercher le numéro de port SNMP configuré dans le fichier server.xml.

Nombre total de pipelines
Affiche le nombre total de pipelines enregistrés pour le contrôle d'application dans la console de configuration (Nombre total de pipelines = Pipelines actifs + Pipelines périmés + Pipelines arrêtés).

Pipelines actifs
Affiche le nombre total de pipelines enregistrés configurés pour le contrôle dans la console de configuration et en cours de fonctionnement.

Pipelines périmés
Affiche le nombre total de pipelines dont la configuration a été modifiée depuis le démarrage du pipeline. Ces pipelines doivent être arrêtés puis redémarrés, pour que les nouvelles modifications de configuration prennent effet.

Pipelines arrêtés
Affiche le nombre total de pipelines enregistrés configurés pour le contrôle dans la console de configuration, mais qui ne sont actuellement pas en cours de fonctionnement ou ne rapportent pas de statistiques. Chaque

pipeline arrêté est inclus dans ce total, donc si un noeud de pipeline n'est pas en cours de fonctionnement, tous les pipelines configurés pour le contrôle sur ce serveur seront comptabilités comme étant arrêtés.

TPM Affiche le nombre total moyen de transactions traitées par minute pour tous les pipelines actifs configurés pour le contrôle dans la console de configuration. Ce nombre reflète les performances globales du système ; plus il est élevé, plus chaque pipeline actif est performant. Ce nombre est actualisé et recalculé toutes les minutes, en fonction des informations envoyées par chaque agent SNMP s'exécutant sur chaque noeud de pipeline où des pipelines actifs sont en cours d'exécution (nombre total de TPM = TPM des pipelines actifs divisé par le nombre total de pipelines actifs).

TPS Affiche le nombre total moyen de transactions traitées par seconde pour tous les noeuds actifs configurés pour le contrôle dans la console de configuration. Ce nombre reflète les performances globales du système ; plus il est élevé, plus chaque noeud actif est performant. Ce nombre est actualisé et recalculé toutes les minutes, en fonction des informations envoyées par chaque agent SNMP s'exécutant sur chaque machine hôte où des noeuds actifs sont en cours d'exécution (nombre total TPS = TPS des noeuds actifs divisé par le nombre total de noeuds actifs).

Nom du pipeline
Répertorie le nom de chaque pipeline enregistré pour le contrôle dans la console de configuration, par ordre alphabétique.

Nom d'hôte
Affiche le nom du noeud de pipeline enregistré auprès de ce pipeline. Si l'état de ce pipeline s'affiche de façon inattendue comme étant `Arrêté`, vous pouvez remédier au problème à l'aide du nom du noeud de pipeline. Par exemple, si tous les pipelines d'un noeud spécifique présentent l'état `Arrêté`, il est judicieux de commencer le dépannage par le noeud de pipeline.

Etat Affiche le dernier état connu du pipeline : `Actif` (en cours de fonctionnement) ou `Arrêté` (ne fonctionnant pas). Le système met à jour les informations d'état toutes les minutes, en fonction des informations envoyées par l'agent SNMP s'exécutant sur le noeud de pipeline.

TPM Affiche le nombre moyen de transactions traitées par minute pour ce pipeline. Si le pipeline présente l'état `Arrêté`, le système affiche la mention `Non disponible`. Ce nombre reflète les performances des pipelines ; plus il est élevé, plus le pipeline est performant.

TPS Affiche le nombre moyen de transactions traitées par seconde pour ce pipeline. Si le pipeline présente l'état `Arrêté`, le système affiche la mention `Non disponible`. Ce nombre reflète les performances des pipelines ; plus il est élevé, plus le pipeline est performant.

Onglet Exceptions UMF

Cet onglet permet d'afficher les exceptions UMF consignées à partir des données chargées par les pipelines enregistrés pour le contrôle d'application. Commencez par générer un rapport à l'écran concernant les exceptions UMF à afficher. Vous pouvez ensuite sélectionner une exception UMF spécifique et l'examiner plus en détail ; ces renseignements peuvent s'avérer utiles pour résoudre les exceptions UMF dans les fichiers de données. Après avoir résolu l'une de ces erreurs, vous pouvez traiter à nouveau les enregistrements corrigés dans ce fichier en toute sécurité.

Les exceptions UMF sont des erreurs conditionnées par les données. Elles se produisent lorsque la structure de données UMF présente des problèmes au niveau d'un fichier de source de données entrant traité par un pipeline. Par défaut, les exceptions UMF ne sont pas prises en compte dans le nombre limite d'erreurs associé au pipeline (nombre défini dans le fichier de configuration du pipeline) ; à elles seules, elles n'entraînent donc généralement pas l'arrêt du pipeline. Vous trouverez une liste complète des exceptions UMF dans la table UMF_EXCEPT ou dans le fichier journal *nom_pipeline*.msg, comprenant même les exceptions UMF relatives aux pipelines non enregistrés pour le contrôle d'application.

Critères de rapport à l'écran

Ces zones permettent de définir les critères du rapport à l'écran sur les exceptions UMF. Une fois ces critères définis, cliquez sur le bouton **Rechercher** pour générer le rapport.

Date de début

Date de début du rapport sur les exceptions UMF répondant aux autres critères définis (cette zone facultative peut demeurer vide. Si tel est le cas, toutes les exceptions UMF sont affichées à compter de la date de mise en service du système, en fonction des autres critères définis).

Par défaut, cette zone utilise la date du jour. Tapez la date au format `mm/jj/aaaa`.

Date de fin

Date de fin du rapport sur les exceptions UMF répondant aux autres critères définis (cette zone facultative peut demeurer vide. Si tel est le cas, toutes les exceptions UMF sont affichées jusqu'à la date du jour, en fonction des autres critères définis).

Par défaut, cette zone utilise la date du jour. Tapez la date au format `mm/jj/aaaa`.

Noeud d'origine

Nom du pipeline enregistré pour lequel consulter les exceptions UMF (cette zone facultative peut demeurer vide. Si tel est le cas, les exceptions UMF sont affichées pour tous les pipelines enregistrés répondant aux autres critères définis).

Retenez bien que vous ne pouvez afficher dans cet onglet que les exceptions UMF associées aux pipelines enregistrés pour le contrôle d'application. Pour connaître toutes les exceptions UMF, reportez-vous à la table UMF_EXCEPT ou au fichier journal *nom_pipeline*.msg.

Code de source de données

Code exact de la source de données pour lequel consulter les exceptions UMF (cette zone facultative peut demeurer vide. Si tel est le cas, les exceptions UMF sont affichées pour toutes les sources de données répondant aux autres critères définis).

Nombre max

Liste déroulante contenant des options relatives au nombre maximal d'exceptions UMF à afficher dans le cadre des autres critères définis. Seul le nombre d'exceptions UMF défini par la limite d'affichage maximale est affiché à l'écran. Si le nombre d'exceptions UMF répondant aux critères est plus important que cette limite, le système ne les affiche pas.

Bouton Rechercher
Lorsque vous cliquez sur ce bouton, le système exécute la recherche : il localise et affiche tous les enregistrements répondant aux critères saisis.

Affichage des résultats du rapport à l'écran
Cette section de la fenêtre affiche le rapport des exceptions UMF à l'écran, en fonction des critères définis. La liste est triée par numéro d'`ID UMF`.

ID UMF
Affiche le numéro séquentiel, attribué par le système, associé à l'exception UMF. L'ID UMF est directement mappé avec la table UMF_EXCEPT, dans laquelle sont consignées les exceptions UMF.

Pipeline d'origine
Affiche le nom du pipeline qui traitait l'enregistrement lorsque l'exception UMF s'est produite.

Créé le
Affiche la date à laquelle l'exception UMF est survenue.

Document de sortie
Affiche le type de document de sortie UMF associé à cette exception UMF.

Code de source de données
Affiche le code de source de données associé au fichier de données entrant dans lequel l'exception UMF s'est produite.

Référence externe
Affiche la référence externe de l'enregistrement de données spécifique dans lequel est survenue l'exception UMF. Ces informations peuvent aider à repérer l'enregistrement devant être corrigé à l'intérieur du fichier de données.

Action
Affiche l'action associée à l'enregistrement de données entrant dans lequel l'exception UMF s'est produite (cette action est codée dans l'UMF de l'enregistrement de données).

- `A` : ajout
- `C` : modification
- `D` : suppression

Onglet Evènements

Cet onglet permet d'afficher les messages échangés entre le moniteur d'application et les pipelines enregistrés pour le suivi ou le routage. En général, ces messages sont également consignés dans des fichiers journaux système, en fonction de la façon dont votre système est configuré pour la consignation. Commencez par générer un rapport à l'écran concernant les événements du moniteur d'application à afficher. Vous pouvez ensuite sélectionner un événement spécifique et l'examiner plus en détail ; ces renseignements peuvent avoir un caractère purement informatif ou bien faciliter la résolution des erreurs ou avertissements de pipeline.

Les événements du moniteur d'application incluent généralement les messages ou erreurs échangés lors du traitement de pipeline (notamment le démarrage ou l'arrêt de pipeline), ainsi que les avertissements ou erreurs générés lors de ce traitement. Les seuls avertissements et erreurs non inclus dans cet onglet sont les exceptions UMF, qui sont des exceptions conditionnées par les données et non des exceptions ou informations de traitement.

Critères de rapport à l'écran

Ces zones permettent de spécifier les critères du rapport à l'écran relatif aux événements du moniteur d'application. Une fois ces critères définis, cliquez sur le bouton **Rechercher** pour générer le rapport. Par défaut, cet onglet affiche les événements du moniteur d'application qui se sont produits à la date du jour au niveau des pipelines enregistrés pour le suivi d'applications.

Date de début

Date de début du rapport sur les événements du moniteur d'application dans le cadre des autres critères définis (cette zone facultative peut demeurer vide. Si tel est le cas, les événements du moniteur d'application sont affichés à partir de la date de mise en service du système, en fonction des autres critères définis).

Date de fin

Date de fin du rapport sur les événements du moniteur d'application dans le cadre des autres critères définis (cette zone facultative peut demeurer vide. Si tel est le cas, les événements du moniteur d'application sont affichés jusqu'à la date du jour en fonction des autres critères définis).

Pipeline d'origine

Nom du pipeline enregistré pour lequel consulter les événements du moniteur d'application (cette zone facultative peut demeurer vide. Si tel est le cas, les événements du moniteur d'application sont affichés pour tous les pipelines enregistrés répondant aux autres critères définis).

Retenez bien que vous ne pouvez afficher dans cet onglet que les événements du moniteur d'application associés aux pipelines enregistrés pour le suivi d'application.

Nombre max

Liste déroulante contenant des options relatives au nombre maximal d'événements du moniteur d'application à afficher dans le cadre des autres critères définis. Seul le nombre d'événements d'application défini par la limite d'affichage maximale est affiché à l'écran. Si le nombre d'événements d'application répondant aux critères est plus important que cette limite, le système ne les affiche pas.

Bouton Rechercher

Lorsque vous cliquez sur ce bouton, le système exécute la recherche en localisant et en affichant tous les enregistrements du moniteur d'événements d'application répondant aux critères saisis.

Affichage des résultats du rapport à l'écran

Cette section de la fenêtre affiche le rapport des événements du moniteur d'application à l'écran, en fonction des critères saisis. La liste est triée par numéro d'ID.

ID Affiche le numéro séquentiel, attribué par le système, associé à l'événement du moniteur d'application.

Pipeline d'origine

Affiche le pipeline enregistré qui est affecté par ou impliqué dans l'événement du moniteur d'application. Il s'agit du pipeline que vous devrez peut-être dépanner.

Date/heure
Affiche l'horodatage du moment où l'événement est survenu.

Evénement
Affiche le type d'événement de moniteur d'application qui est survenu. Les colonnes **Description de l'événement** et **Niveau d'erreur** contiennent davantage d'informations sur cet événement et indiquent la gravité du type d'événement. Il existe actuellement deux types possibles d'événement de moniteur d'application :

- `NODE-INFO` est une note ou un autre type d'événement d'information qui s'est produit dans le pipeline concerné. Ce type d'événement s'affiche généralement au démarrage ou à l'arrêt du pipeline concerné.
- `NODE-ERROR` est une erreur qui est survenue dans le pipeline concerné. Consultez la colonne **Niveau d'erreur** pour savoir si cela exige une intervention immédiate. Il convient généralement d'étudier de plus près les informations relatives à cet événement du moniteur d'application ; elles peuvent faciliter la résolution du problème lié à ce pipeline.

Description de l'événement
Fournit jusqu'à 30 caractères de renseignements complémentaires sur l'événement du moniteur d'application.

Niveau d'erreur
Affiche le type de niveau d'erreur de l'événement de moniteur d'application. Il existe actuellement deux types d'événement possibles :

- `NOTE` est le niveau d'erreur associé à l'événement `NODE-INFO`. Ce type de niveau d'erreur est généralement informatif, il ne nécessite donc normalement aucune intervention de l'utilisateur.
- `ERR` est le niveau d'erreur associé à l'événement `NODE-ERROR`. Ce type de niveau d'erreur indique généralement que vous devez étudier de plus près les détails de cet événement du moniteur d'application pour résoudre l'erreur. Pour accéder aux détails complets de l'événement, il vous suffit de cliquer dessus.

Onglet Détail des évènements

Lorsque vous sélectionnez un événement spécifique du moniteur d'application dans l'onglet **Evénements**, un nouvel écran affiche les détails relatifs à cet événement. Ces détails sont directement issus des fichiers de consignation du système, à l'exception du fichier journal des exceptions UMF (ce fichier journal possède son propre onglet **Exceptions UMF**, que vous pouvez consulter). Les détails fournis peuvent vous aider à identifier et résoudre une erreur de pipeline.

ID Numéro séquentiel attribué par le système à cet événement du moniteur d'application.

Pipeline
Indique le nom du pipeline au niveau duquel cet événement du moniteur d'application est survenu.

Date/heure
Affiche l'heure et la date de cet événement CME au format `Mois, JJ, AAAA HH:MM:SS A/PM Fuseau horaire`. Ces date et heure correspondent à celles où l'événement a été consigné dans le fichier journal.

Evénement
Affiche le type d'événement du moniteur d'application :

- NODE-INFO est une note ou un autre type d'événement d'information qui s'est produit dans le pipeline concerné. Ce type d'événement s'affiche généralement au démarrage ou à l'arrêt du pipeline concerné.
- NODE-ERROR est une erreur qui est survenue dans le pipeline concerné. Consultez la colonne **Niveau d'erreur** pour savoir si cela exige une intervention immédiate. Il convient généralement d'étudier de plus près les informations relatives à cet événement ; elles peuvent faciliter la résolution du problème lié à ce pipeline.

Description de l'événement
Affiche les premiers caractères de l'événement du moniteur d'application, tel qu'il est consigné dans le fichier journal. Cette description vise à apporter des renseignements plus précis sur ce qui a déclenché le type d'événement.

Niveau d'erreur
Affiche le type de niveau d'erreur de l'événement du moniteur d'application :

- NOTE est le niveau d'erreur associé à l'événement NODE-INFO. Ce type de niveau d'erreur est généralement informatif, il ne nécessite donc normalement aucune intervention de l'utilisateur.
- ERR est le niveau d'erreur associé à l'événement NODE-ERROR. Ce type de niveau d'erreur indique généralement que vous devez étudier de plus près les détails de cet événement pour résoudre l'erreur. Pour accéder aux détails complets de l'événement, il vous suffit de cliquer dessus.

Onglet Nouveaux comptes

Cet onglet permet de consulter les charges de données des sept derniers jours. D'un simple coup d'oeil, vous pouvez savoir quelles sources de données ont soumis des fichiers en vue de leur traitement et connaître le nombre de nouvelles identités issues de ce traitement. Ces statistiques vous donnent une idée du volume de traitement, afin de voir rapidement si les volumes de données entrants cadrent avec les prévisions.

Quand vous cliquez sur cet onglet, les sept derniers jours s'affichent. S'il y a plus d'enregistrements que la page visible ne peut en afficher, utilisez la barre de défilement pour consulter les autres enregistrements. L'onglet **Nouveaux comptes** est trié par ordre alphanumérique, en fonction des codes de la source de données.

Code de source de données
Affiche le code de source de données associé à ce nouvel enregistrement d'identité. Ces informations reposent sur la balise UMF (Universal Message Format) de code de source de données présente dans le fichier entrant qui a été traité.

Remarque : Vous pouvez consulter la liste complète de tous les codes de source de données dans la console de configuration en cliquant sur les onglets **Configurer** puis **Sources**.

Description
Affiche la description de la source de données, telle qu'elle est configurée pour cette source dans la console de configuration. La description doit fournir davantage d'informations afin de faciliter l'identification de la source de données d'où proviennent ces enregistrements d'identité.

Date de chargement
Affiche la date à laquelle ce fichier de source de données a été traité et a

fourni le nombre de nouvelles identités figurant dans la colonne **Nombre d'enregistrements**. La date est exprimée au format `mois JJ, AAAA`.

Nombre d'enregistrements
Affiche le nombre total de nouvelles identités traitées à partir de ce code de source de données à la date indiquée dans la colonne **Date de chargement**. Il s'agit du nombre qui peut indiquer le volume de traitement.

Chapitre 7. Chargement de données

Pour utiliser IBM InfoSphere Identity Insight, vous devez convertir les données au format Universal Message Format (UMF) et les charger dans le système.

Ajout d'une nouvelle source de données

Quand vous avez une nouvelle source de données pour la base de données d'entités, vous devez l'ajouter.

Pourquoi et quand exécuter cette tâche

Tous les résultats sont un produit de données de qualité. L'introduction de données d'excellente qualité dans la base de données d'entités constitue donc l'une des tâches les plus cruciales, mais qui exige une analyse approfondie des données et de la configuration.

Procédure

1. Identifiez la source des données. Il est capital de savoir où s'y prendre pour résoudre les problèmes de données.
2. Analysez les métadonnées. Chaque source de données configurée dans la base de données d'entités doit mentionner un identificateur unique sur ses enregistrements, de sorte que la base de données d'entités puisse réattribuer intégralement la totalité des données à leur source originale. Recherchez la zone qui indique l'unicité des enregistrements et assurez-vous qu'ils sont vraiment uniques.
3. Utilisez un programme d'acquisition pour convertir les données depuis leur format natif au format UMF.
4. Configurez les données.
   a. Définissez un rôle pour la source de données.
   b. Configurez la source de données.
   c. Créez tous les éventuels types de numéro nécessaires.
   d. Créez tous les éventuels types de caractéristique nécessaires.
   e. Examinez la configuration de résolution, et la personnalisation si nécessaire.
   f. Configurez de nouvelles règles DQM.
   g. Validez les nouvelles règles DQM.
   h. Configurez les règles d'alerte de rôle.
5. Vérifiez les données.
   a. Vérifiez que le pipeline a démarré.
   b. Vérifiez que le pipeline a pu utiliser les transports configurés et qu'il reçoit l'UMF du programme d'acquisition.
   c. Vérifiez que le noeud d'acquisition a produit des messages XML syntaxiquement corrects en examinant le fichier `.bad`.
   d. Vérifiez qu'aucune exception UMF n'est survenue en raison d'une configuration ou d'un mappage incorrect.
   e. Vérifiez les résultats attendus en consultant les rapports récapitulatifs de source de données et de chargement.
   f. Recherchez certaines des entités résolues, à l'aide du visualiseur.

g. Le cas échéant, examinez les alertes de rôle.

Conversion de données au format UMF

Pour permettre au système de traiter les données entrantes, celles-ci doivent être converties au format UMF (Universal Message Format). Le processus de conversion au format UMF des données entrantes peut être accompli à l'aide de divers outils, tels que les utilitaires de base fournis avec le produit ou les logiciels de conversion XML standard.

Procédure

1. A l'aide du modèle d'entité que vous avez créé pour le système, analysez les données entrantes afin de vérifier leur conformité à la norme UMF. Avant de passer à l'étape suivante, vous devez posséder des connaissances suffisantes sur les segments et balises UMF existants.
2. Configurez l'utilitaire de conversion de manière à générer des fiches UMF conformes à votre modèle d'entité.
3. Exécutez l'utilitaire de conversion.

Que faire ensuite

Une fois la conversion des données au format UMF effectuée, vous pouvez envoyer les fiches UMF vers le pipeline en vue du traitement.

Programmes d'acquisition

Un programme d'acquisition contient les outils et programmes qui permettent d'obtenir des données, de les convertir au format UMF (Universal Message Format) et d'envoyer ces données converties au pipeline pour traitement.

Pour convertir des données au format UMF, vous pouvez utiliser comme programme d'acquisition soit les utilitaires fournis avec le produit, soit des outils d'extraction transformation et chargement tels que WebSphere QualityStage.

Transfert de fichiers UMF dans une file d'attente

Vous pouvez transférer des fichiers UMF dans une file d'attente à l'aide de l'utilitaire de file d'attente.

Procédure

1. Assurez-vous que les données que vous voulez envoyer sont en format large (un enregistrement par ligne).
2. Indiquez les paramètres de configuration dans le fichier de configuration.
3. Exécutez l'utilitaire de file d'attente.

Utilitaire de file d'attente

IBM fournit un utilitaire de file d'attente qui gère le transfert des données UMF vers une file d'attente à partir d'un processus ou d'un fichier.

Bien que sa tâche principale consiste à transmettre des données à des files d'attente, l'utilitaire de file d'attente vous permet également de :

- Créer des files d'attente
- Supprimer des fiches d'une file d'attente
- Afficher le statut d'une file d'attente

- Afficher les fiches d'une file d'attente

L'utilitaire de file d'attente s'attend à des données en un certain format :

- UMF format large, à savoir une ligne pour chaque fiche
- Une nouvelle ligne à la fin de chaque fiche
- Aucune nouvelle ligne dans une fiche

Vous devez utiliser l'un des gestionnaires de files d'attente suivants pour employer l'utilitaire de file d'attente.

Microsoft Windows Server x86
: Microsoft Message Queuing, composant de Microsoft Windows Server 2003 ou 2008.

  IBM Websphere MQ 6.0

Microsoft Windows Server x86_64
: Microsoft Message Queuing, composant de Microsoft Windows Server 2003 ou 2008.

  IBM Websphere MQ 7.0

Environnement d'exploitation Solaris
: IBM Websphere MQ 6.0

Linux IBM Websphere MQ 6.0

AIX IBM Websphere MQ 6.0

Quand un pipeline fonctionne en mode file d'attente, le gestionnaire de files d'attente est toujours obligatoire. Il doit être installé et en cours d'exécution. Quand un pipeline fonctionne en mode fichier, le gestionnaire de files d'attente doit être installé mais pas nécessairement en cours de fonctionnement pour les plateformes Windows et AIX. Il est inutile de l'installer ou de l'exécuter sous Solaris ou Linux.

Fichier de configuration de l'utilitaire de file d'attente

Vous pouvez utiliser un fichier de configuration pour envoyer des enregistrements à plusieurs files d'attente, avec l'utilitaire de file d'attente.

Lors de la distribution d'un ensemble de données à plusieurs files d'attente, vous devez indiquer la méthode de définition de la distribution au gestionnaire de files d'attente. L'objectif consiste à créer un mode de distribution où la première file d'attente reçoit un enregistrement, puis la suivante en reçoit un autre, et ainsi de suite, à tour de rôle.

Le fichier de configuration de l'utilitaire de file d'attente s'appelle qutil.ini et doit se trouver dans le même répertoire que le fichier exécutable de l'utilitaire de file d'attente.

Paramètres

[sectionname]
: Nom de la section. Vous pouvez désigner plusieurs groupes de paramètres de configuration au sein d'un même fichier de configuration, puis faire référence à ces paramètres dans la ligne de commande en désignant ce nom de section. Par exemple, vous pouvez appeler des sections CFG1 (configuration 1) ou CFG2 (configuration 2) et faire référence à ces sections quand vous émettez des commandes d'utilitaire de file d'attente.

MessageCountMax
Nombre maximal d'enregistrements autorisés dans chaque file d'attente à un moment donné. Dès qu'une file d'attente est pleine, l'utilitaire cesse de traiter les enregistrements.

FullCountMax
Indique le nombre total d'enregistrements qui peuvent se trouver dans la totalité des files d'attente, par opposition à une seule file d'attente. Dès que toutes les files d'attente sont pleines, l'utilitaire suspend le flot de données et attend que des enregistrements se placent dans les pipelines pour y être traités, en libérant ainsi de l'espace dans les files d'attente. Fonctionne avec FullPause.

FullPause
Nombre de millisecondes pendant lequel l'utilitaire suspend le flot de données, en permettant ainsi aux données des files d'attente d'être traitées une fois que FullCountMax est atteint.

Qout*n*=qname
Noms des files d'attente de sortie de cette section. Les noms des files d'attente de sortie peuvent être ce que bon vous semble, le paramètre devant toutefois être Qout*n*, sachant que n est un entier commençant par 0. La valeur de *n* doit être séquentielle de 0 à *n*, sachant que n est la dernière file d'attente définie. Ce format est obligatoire. Modifiez uniquement le numéro de l'identificateur Qout*n* et les noms de files d'attente (qnames).

Exemple

L'exemple suivant montre que vous avez deux ensembles d'instructions (une utilisant 2 files d'attente, l'autre en utilisant 4). Chaque file contient un maximum de 2 500 enregistrements, avec sur la totalité des files un maximum de 10 000 enregistrements. L'utilitaire de file d'attente doit se suspendre pendant 3 secondes avant toute tentative de chargement d'enregistrements supplémentaires dans une file d'attente une fois que le paramètre FullCountMax a été atteint. Ensuite, il recense les noms des 4 files d'attente à utiliser.

```
[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
```

Syntaxe de commande de l'utilitaire de file d'attente

Les commandes de l'utilitaire de file d'attente se composent d'opérations et de modificateurs.

La syntaxe élémentaire d'une commande d'utilitaire de file d'attente est la suivante :

qutil -opération *qname* **-modificateur**

qname est le nom de la file d'attente.

Opérations de commande

Les opérations définissent les diverses fonctions de l'utilitaire de file d'attente. Vous ne pouvez ajouter qu'une seule opération à une commande qutil.

-C Crée une nouvelle file d'attente.

Exige un nom unique comme nom de file d'attente.

Lettre 'C' majuscule obligatoire.

-f Copie stdin dans la file d'attente.

Nécessite un nom de file d'attente (qname).

-i Copie stdin dans plusieurs files d'attente.

Nécessite un nom de section comme défini dans le fichier qutil.ini. Indique une section du fichier qutil.ini à charger pour la distribution des messages dans plusieurs files d'attente.

-k Nombre de purges de chaque enregistrement.

Nécessite un *qname*.

Peut s'utiliser conjointement avec le modificateur -c afin de limiter le nombre d'enregistrements traités.

-p Nombre de consultations rapides de chaque enregistrement.

Ne supprime pas les enregistrements de la file d'attente.

Nécessite un *qname*.

Ecrit dans stdout.

Peut s'utiliser conjointement avec le modificateur -c afin de limiter le nombre d'enregistrements traités.

-r Nombre de lectures de chaque enregistrement.

Supprime les enregistrements de la file d'attente.

Nécessite un *qname*.

Ecrit dans stdout.

Peut s'utiliser conjointement avec le modificateur -c afin de limiter le nombre d'enregistrements traités.

-s Etat de la file d'attente.

Nécessite un *qname*.

-x Supprimer un *qname*.

Nécessite un *qname*.

Modificateurs de commande

Les modificateurs configurent des paramètres complémentaires pour une opération d'utilitaire de filed'attente. Vous pouvez utiliser plusieurs modificateurs dans une commande qutil.

-T Indique si une file d'attente est transactionnelle.

Par défaut, toutes les nouvelles files d'attente sont non transactionnelles, excepté si elles ont été définies comme transactionnelles dès leur création avec un modificateur -T.

Les files d'attente transactionnelles ne doivent pas être utilisées quand elles sont susceptibles de recevoir des informations d'acheminement issues d'un moniteur d'application.

Dans Microsoft Message Queueing, elles ne permettent pas de classer les messages par ordre de priorité ni de les traiter dans un ordre autre que celui de réception.

-c Indique qu'il faut arrêter après un nombre défini d'enregistrements traités.

Nombre entier obligatoire.

Lettre 'c' minuscule.

-l Indique le niveau de priorité de chaque enregistrement.

Nombre entier obligatoire.

Les valeurs de nombre entier valides sont les suivantes :

0-7
File d'attente de messages Microsoft
les niveaux de priorité vont de 0 à 7, où 0 est le niveau le moins élevé et 7 le niveau le plus élevé.

3 est la valeur par défaut.

0-9
IBM Websphere MQ
Les niveaux de priorité vont de 0 à 9, où 0 est le niveau le moins élevé et 9 le niveau le plus élevé.

La valeur par défaut dépend d'une propriété de file d'attente. Vous pouvez modifier cette propriété dans le gestionnaire IBM Websphere MQ.

-m Indique le gestionnaire de files d'attente.

AIX, HP-UX, Linux et Solaris uniquement

-o Indique le nombre de secondes avant l'expiration d'un message.

Nombre entier obligatoire.

-q Indique le type de file d'attente.

Microsoft Windows uniquement

Les valeurs admises sont les suivantes :

mq IBM WebSphere MQ

msmq Microsoft Message Queueing (MSMQ)

-t Indique le délai d'attente en millisecondes entre chaque enregistrement.

Nombre entier obligatoire.

Relations entre opérations et modificateurs de commande

Certains modificateurs ne sont recommandés que pour certaines opérations. La table suivante décrit la relation de chaque opération avec ses modificateurs potentiels :

Tableau 31. Relations entre opérations et modificateurs de commande de l'utilitaire de file d'attente

Opération	Modificateurs valides

Tableau 31. Relations entre opérations et modificateurs de commande de l'utilitaire de file d'attente (suite)

`-C`	`-T, -q` *EXEMPLE :* qutil -C *qname* -T -q mq
`-f`	`-c, -t, -l, -o, -q` *EXEMPLE :* qutil -f *qname* -c 50 -t 20 -l 4 -o 10 -q msmq
`-i`	AUCUN *EXEMPLE :* qutil -i configsection
`-k`	`-c` *EXEMPLE :* qutil -k *qname* -c 50
`-p`	`-c` *EXEMPLE :* qutil -p *qname* -c 50
`-r`	`-c` *EXEMPLE :* qutil -r *qname* -c 50
`-s`	AUCUN *EXEMPLE :* qutil -s *qname*
`-x`	AUCUN *EXEMPLE :* qutil -x *qname*

Conversion de fichiers UMF aux formats adéquats

L'utilitaire de formatage UMF permet de convertir les enregistrements UMF du format large au format haut, et inversement.

Utilitaire de formatage UMF

L'utilitaire de formatage UMF permet de convertir les fiches UMF du format large au format haut, et inversement. Il permet également d'extraire des données UMF définies par une balise donnée.

Les fiches UMF peuvent s'afficher soit en une seule ligne (format large), soit sous forme de série de lignes en retrait, chacune contenant un élément XML et une valeur (format haut).

Exemple : format large

```
<nom><type_nom>M</type_nom><prénom>John</prénom>
<nom_famille>Smith</nom_famille></nom>
```

Exemple : format haut

```
<nom>
 <type_nom>M</type_nom>
 <prénom>John</prénom>
 <nom_famille>Smith</nom_famille>
</nom>
```

Syntaxe de commande de l'utilitaire de formatage UMF

L'utilitaire de formatage UMF emploie diverses commandes pour formater et extraire les données.

La syntaxe élémentaire d'une commande de l'utilitaire de formatage UMF est la suivante :

```
xutil -o[switch] option
```

Paramètres

-o **Out** Envoie la sortie vers stdout. Paramètre obligatoire. Les commutateurs du paramètre sont les suivants :

- **w** Définit le format de la sortie. Tous les formats UMF d'un enregistrement se trouvent sur une ligne. Supprime tous les retours et sauts de ligne.
- **t** Définit le format de la sortie. Le format UMF d'un enregistrement se trouve sur plusieurs lignes. Insère une balise par ligne et met des onglets dans le document afin d'en faciliter la lecture.

-t **Tagname :** filtre les enregistrements en fonction d'un nom de balise. Seuls les enregistrements contenant cette balise sont envoyées à stdout. Toute erreur est envoyée à stderr.

Le paramètre tagname permet de filtrer les enregistrements. Par exemple, un fichier peut contenir des enregistrements mixtes : des entités et des activités. Il est préférable de traiter les entités avant les activités pour que ces dernières puissent avoir des entités existantes pour la concordance.

Exemples

Cette commande filtre uniquement les entités, à l'aide de mixedlist.xml comme source et entity.xml comme fichier de sortie.

```
xutil -ow -t UMF_ENTITY < mixedlist.xml > entity.xml
```

Cette commande dirige le résultat du processus d'utilitaire de formatage UMF vers un pipeline vers l'utilitaire de file d'attente.

```
xutil -ow < file.xml |qutil -f qname
```

Extension du modèle d'entité

Un modèle d'entité est un ensemble de données qui définit ce que vous considérez comme étant une entité. Suivez ces instructions pour étendre le modèle d'entité par défaut. Il ne s'agit pas d'une tâche courante, mais vous pouvez développer le modèle d'entité pour votre environnement.

Format UMF (Universal Message Format)

Le format UMF (Universal Message Format) est un dialecte XML extensible qui sert à structurer les fichiers de sources de données. Il contient des balises standard qui représentent des éléments clés des identités, des relations et des activités. Pour que les pipelines puissent traiter les données, celles-ci doivent être converties au format UMF et doivent correspondre à la spécification UMF.

Le format UMF est constitué des composants hiérarchiques suivants :

UMF, documents
Collection de segments UMF structurant les données et indiquant le type de la fiche de source de données.

Segments UMF
Partie du document UMF qui structure les données de la source de données.

Eléments UMF
Valeurs et balises XML définissant les données d'un segment UMF d'un document UMF.

La spécification UMF répertorie les types spécifiques des documents UMF, des segments UMF de chaque type de document UMF ainsi que les éléments UMF valides de chaque segment UMF.

Analyse des données de base

Pour charger vos données source dans la base de données d'entités, commencez par analyser les données source en vue de les mapper en UMF.

Procédure

1. Identifiez les données à charger dans la base de données d'entités.
2. Vérifiez que les données sont cohérentes et complètes.
3. Comparez la largeur des valeurs des éléments de segment UMF entrants avec celle des colonnes correspondantes dans leur table de base de données.
4. Identifiez les caractères invalides dans les données source.

Résultats

Les résultats de votre analyse peuvent impliquer différentes options, par exemple :

- Appliquer des règles DQM pour corriger les données comportant des caractères invalides.
- Appliquer des règles DQM afin de tronquer les données d'une largeur supérieure aux colonnes correspondantes dans leur table de base de données
- Demander aux fournisseurs de sources de données externes de procurer des données plus complètes.
- Charger uniquement les zones où figurent des données valides.

Consultation de la spécification UMF par défaut

Il est recommandé de consulter la spécification UMF par défaut afin de vous faciliter la création de votre spécification et de votre modèle d'entité UMF personnalisés. Ces éléments organisent le transfert des données depuis les sources jusqu'au balises UMF qui seront ingérées par la base de données d'entités.

Mappage de segments UMF à la base de données d'entités

Chaque fois que vos données nécessitent de nouveaux segments UMF, vous devez créer de nouveaux mappages pour les données de ces segments UMF. Sans mappage de données valide, vous ne pouvez pas charger de données dans la base de données d'entités.

Risques inhérents à la modification de la base de données d'entités

Toute modification de la base de données d'entités comportant des risques, sans expérience ou maîtrise suffisantes, il convient de s'en abstenir.

- Sans l'expérience ni la maîtrise suffisantes, il faut éviter d'ajouter des tables à la base de données d'entités

- L'ajout de champs à des tables de la base de données est un processus qui en implique bien davantage que lesdites tables. Dans la mesure du possible, il est recommandé d'utiliser les tables et champs existants pour classer les nouvelles données.
- Il ne faut pas modifier les index de tables de base de données. Toute modification des index des tables de base de données risque de provoquer des anomalies, par exemple le blocage du visualiseur.
- Il est recommandé de n'apporter de modifications à la gestion de la qualité des données qu'à condition de disposer de connaissances suffisantes ou de solliciter l'aide d'IBM.
- Utilisez toujours une base de données test pour vérifier les nouvelles configurations avant de les appliquer à votre environnement de production.

Ajout de tables à la base de données d'entités

Il se peut que vous deviez ajouter une nouvelle table de base de données quand vous ajoutez une nouvelle source de données.

Pourquoi et quand exécuter cette tâche

L'ajout de tables à la de base de données d'entités ne permet pas d'appliquer le résolution aux nouvelles données ; il s'agit uniquement d'un emplacement où stocker des données.

Il est recommandé d'utiliser une base de données test pour vérifier les nouvelles configurations avant de les appliquer à votre environnement de production.

Dans la mesure du possible, il est recommandé d'utiliser les tables et zones existantes pour classer les nouvelles données.

L'ajout d'une nouvelle table accueillera les données prévues qui ne sont pas encore configurées dans le système. In convient de créer la nouvelle table se sorte qu'elle soit cohérente avec votre modèle de données actuel.

Veillez à inclure les zones pertinentes obligatoires :

- ENTITY_ID
- DSRC_ACCT_ID
- HIST_STAT - obligatoire si vous appliquez le suivi historique séquentiel.
- SYS_CREATE_DT
- SYS_DELETE_DT
- SYS_LSTUPD_DT
- SYS_LSTUPD_US

Procédure

1. Créez la nouvelle table dans la base de données d'entités.
2. Créez le mappage de données de la nouvelle table.
3. Ajoutez de nouvelles tables de base de données au dictionnaire.
4. Définissez les mappages de données de la nouvelle table.
5. Déterminez les règles DQM adéquates à appliquer au nouveau segment et configurez ces règles via la console.
6. Vérifiez la nouvelle configuration en soumettant des données test connues à un pipeline et en vérifiant les fichiers journaux obtenus.
   a. Vérifiez si le test s'exécute sans erreurs.

b. Vérifiez si la console signale des exceptions UMF.
c. Vérifiez si les fichiers journaux `nodename.Sql.Err.log` et `nodename.err` signalent des erreurs.
d. Vérifiez si les résultats du test concordent avec les résultats escomptés.
e. Vérifiez la table UMF_LOG pour vous assurer que tous les enregistrements se chargent correctement.

Ajout de zones à des tables de la base de données d'entités :

Il se peut que vous deviez ajouter une nouvelle zone à une table de base de données d'entités existante afin d'accueillir un nouveau type de données.

Pourquoi et quand exécuter cette tâche

Il est possible d'ajouter une nouvelle zone à une table existante quand un nouveau segment UMF ne nécessite pas une table entièrement nouvelle.

L'ajout de zones à une table de base de données d'entités existante ne permet pas d'appliquer le résolution aux nouvelles données ; il s'agit uniquement d'un emplacement où stocker des données.

Il est recommandé d'utiliser une base de données test pour vérifier les nouvelles configurations avant de les appliquer à votre environnement de production.

Dans la mesure du possible, il est recommandé d'utiliser les tables et zones existantes pour classer les nouvelles données.

Procédure

1. Ajoutez la nouvelle zone dans la table de base de données appropriée.
2. Créez le mappage de données de la nouvelle zone dans la console.
3. Déterminez les règles DQM adéquates à appliquer à la nouvelle zone et configurez ces règles via la console.
4. Vérifiez la nouvelle configuration en soumettant des données test connues à un pipeline et en vérifiant les fichiers journaux obtenus.
   a. Vérifiez si le test s'exécute sans erreurs.
   b. Vérifiez si la console signale des exceptions UMF.
   c. Vérifiez si les fichiers journaux `nodename.Sql.Err.log` et `nodename.err` signalent des erreurs.
   d. Vérifiez si les résultats du test concordent avec les résultats escomptés.
   e. Vérifiez la table UMF_LOG pour vous assurer que tous les enregistrements se chargent correctement.

Ajout de nouvelles tables de base de données au dictionnaire :

Quand vos données (et UMF) nécessitent la création d'une nouvelle table de base de données, vous devez ajouter cette table au dictionnaire des tables de base de données que le système utilise. Si la table n'existe pas dans le dictionnaire, vous ne pouvez créer de mappage de données ni pour l'UMF ni pour la table.

Avant de commencer

L'utilisateur doit bénéficier de droits d'accès adéquats pour lire et stocker des données dans la table de base de données.

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Dictionnaire**.
4. Cliquez sur le bouton **Nouveau**.
5. Dans la zone **Nom de la table**, tapez le nom de la nouvelle table de base de données.

Définition de mappages de données

Vous devez créer un mappage de donnée pour les nouveaux segments et balises UMF. L'ajout de nouveaux systèmes source au produit entraîne parfois la création de nouveaux segments et balises UMF. Un mappage de données associe les données d'un UMF aux tables et colonnes correspondantes de la base de données d'entités.

Mappages de données :

Un mappage de données associe les données d'un fichier UMF aux tableaux et colonnes correspondants de la base de données d'entités.

Sans mappage de données valide, vous ne pouvez pas charger de données dans la base de données d'entités. Chaque fois que vos données nécessitent de nouveaux segments UMF, vous devez créer de nouveaux mappages pour les données de ces segments UMF.

Exemple

Le concessionnaire automobile FAS a récemment commencé a recueillir les données de compagnie d'assurance pour ses clients. Par exemple, il se peut que les données UMF d'une nouvelle compagnie d'assurance utilisent ces segments UMF :

```
<ATTRIBUTE>
<INSURANCECOMPANY>Compagnie assurances Mooninite</INSURANCECOMPANY>
</ATTRIBUTE>
```

Vous devez créer un nouveau mappage de données entre le chemin de données UMF <ATTRIBUTE><INSURANCECOMPANY> et la colonne de tableau adéquate de la base de données d'entités. La valeur XPath du chemin de données UMF est `./ATTRIBUTE/INSURANCECOMPANY/`

Consultation des mappages de données :

Un mappage de données associe les données d'un fichier UMF aux tableaux et colonnes correspondants de la base de données d'entités.

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Mappe de données**.
4. Dans la liste déroulante **Segment**, choisissez le segment UMF que vous voulez consulter.
5. Dans la liste déroulante **Table**, sélectionnez la table de segments UMF dont vous voulez consulter le mappage.

Création de mappages de données :

Un mappage de données associe des données UMF aux tables et colonnes correspondantes de la base de données d'entités. Il faut un nouveau mappage de données quand des données entrantes pourvues de nouvelles balises UMF seront traitées par le système.

Avant de commencer

Si ce mappage de données UMF mappe des données sur plusieurs tables, il faut vérifier que les tables seront insérées dans le bon ordre au cours des opérations de pipeline. Si la table n'existe pas dans le dictionnaire, vous devez l'y ajouter pour pouvoir créer un mappage de données pour l'UMF et la table.

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Mappe de données**.
4. Dans la liste déroulante **Segment**, sélectionnez le segment UMF où vous voulez ajouter un nouveau mappage de données à une table.
5. Dans la liste déroulante **Table**, sélectionnez la table de segment UMF où vous voulez ajouter un nouveau mappage de données.
6. Effectuez l'une des opérations suivantes :
   - Pour créer un nouveau mappage de données, cliquez sur le bouton **Nouveau**.
   - Pour créer un mappage de données basé sur un mappage de données existant, sélectionnez-en un dans la liste, puis cliquez sur le bouton **Cloner**.
7. S'il s'agit d'un nouveau segment, tapez le nom du segment UMF dans la zone **Segment**.
8. Sélectionnez la table de base de données voulue dans la liste déroulante **Table**.
9. Dans la zone **Colonne de table**, tapez le nom de la colonne de table de la base de données à laquelle vous souhaitez mapper le chemin de données UMF.
10. Dans la liste déroulante **Type de zone**, sélectionnez le type de zone adéquat qui représente celui de la colonne de table dans la base de données.
11. Dans la liste déroulante **Type de données**, choisissez le type de données adéquat qui représente la valeur des données.
12. Dans la zone **Chemin de données UMF**, saisissez la balise UMF.
13. Dans la liste déroulante **Méthode de mise à jour**, choisissez la méthode de mise à jour adéquate pour déterminer, entre la valeur entrante et la valeur précédemment stockée, laquelle des deux sera conservée.
14. Dans la liste déroulante de la zone **Etat**, choisissez l'état adéquat du mappage de données.
15. Cliquez sur le bouton **Enregistrer**.

Suppression de mappages de données :

Un mappage de données associe des données UMF aux tables et colonnes correspondantes de la base de données d'entités. Vous pouvez supprimer un mappage de données dont le système ne se sert plus.

Procédure

1. Cliquez sur le bouton **Configurer**.
2. Cliquez sur le bouton **UMF**.
3. Cliquez sur l'onglet **Mappe de données**.
4. Dans la liste déroulante **Segment**, sélectionnez le segment UMF où vous voulez sélectionner une table pour supprimer un mappage de données.
5. Dans la liste déroulante **Table**, sélectionnez la table de segment UMF où vous voulez supprimer un mappage de données.
6. Sélectionnez un mappage de donnée dans la liste, puis cliquez sur le bouton **Supprimer**.

Rubriques d'aide :

Mappages de données - onglet Général :

L'onglet **Général** permet d'indiquer les détails du mappage de données.

Segment
Tapez le nom du segment pour lequel vous souhaitez créer un mappage de données. Ce nom doit être saisi en majuscules.

Table Dans la liste déroulante, sélectionnez la table du mappage de données que vous souhaitez créer.

Nom de colonne de table
Tapez le nom de la colonne de table que vous souhaitez créer.

Type de colonne de table
Dans la liste déroulante, sélectionnez le type de colonne de table que vous souhaitez créer.

ID unique
La colonne de table est une clé unique s'incrémentant automatiquement qui est générée par le moteur de base de données. Une seule colonne de table peut être configurée avec cette valeur.

Clé d'entité
Si cette option est sélectionnée, la colonne de table est toujours réglée sur ENTITY_ID.

Clé d'entreprise
La colonne de table forme, avec les autres colonnes de table Clé d'entreprise désignées, une clé de recherche composite afin de déterminer l'existence du même enregistrement

Attribut
La colonne de table, qui sert simplement à stocker les données, n'a aucune incidence sur les fonctions d'insertion, de mise à jour et de suppression de la table.

Attribut de clé
La valeur de la colonne de table sert à déterminer s'il existe un enregistrement portant la même valeur. La base de données conserve une trace des modifications de ces valeurs de clé au fil du temps. Exemple : si vous souhaitez conserver une version de l'enregistrement si la valeur ADDR1 change, vous devez désigner la valeur ADDR1 comme attribut de clé.

Cette valeur n'a rien à voir avec les index.

Séquence d'historique
La colonne de table sert à déterminer quel enregistrement fourni par une certaine source est le plus récent et quels enregistrements sont historiques.

La séquence d'historique est toujours affectée à la colonne de table HIST_STAT.

Supprimer l'horodatage
La colonne de table sert à stocker les dernières date et heure où l'enregistrement a été supprimé.

Mettre à jour l'horodatage
La colonne de table sert à stocker les dernières date et heure où l'enregistrement a été mis à jour.

Type de données
Dans la liste déroulante, sélectionnez le type de données de la colonne de table.

CAR Données de type caractères (alphanumériques).

ENT Données de type entiers.

DATE Données de date. Exemple : aaaa-mm-jj ou mm-jj-aaaa.

DATE/HEURE
Données de date et heure. Exemple : aaaa-mm-jj hh:mm:ss ou mm-jj-aaaa hh:mm:ss.

Chemin de données UMF
Saisissez l'emplacement XPath de la balise UMF.

Méthode de mise à jour
Dans la liste déroulante, sélectionnez la méthode de mise à jour du mappage de données que vous souhaitez créer. La méthode de mise à jour détermine quelle valeur, entre la valeur entrante et la valeur précédemment stockée, sera conservée.

Jamais
S'il existe une valeur pour l'élément UMF dans la table de base de données, il est impossible de la mettre à jour.

Toujours
S'il existe une valeur pour l'élément UMF dans la table de base de données, il est possible de la mettre à jour.

Valeur maximum
La valeur, entrante ou stockée, la plus élevée est conservée ou mise à jour.

Limité aux types de données de colonne de table INT, DATE ou DATE/TIME.

Valeur minimum
La valeur, entrante ou stockée, la plus faible est conservée ou mise à jour.

Limité aux types de données de colonne de table INT, DATE ou DATE/TIME.

Etat Dans la liste déroulante, sélectionnez l'état du mappage de données que vous souhaitez créer.

Actif Le mappage de données est actif.

Inactif Le mappage de données est inactif.

Normalisation des adresses avec IBM InfoSphere QualityStage et AddressDoctor

La correction et la normalisation d'adresses est un processus de pipeline qui permet de corriger et de normaliser les adresses pour obtenir un traitement de résolution d'entité optimal. Cette nouvelle fonction d'IBM InfoSphere Identity Insight permet d'utiliser une solution de normalisation des données d'adresse conforme aux normes de l'industrie qui comprend AddressDoctor, IBM InfoSphere Information Server, IBM InfoSphere DataStage et IBM WebSphere QualityStage.

La prise en charge d'un module de normalisation fourni par AddressDoctor permet de supprimer les dépendances et les limitations d'autres modules, tels que WAVES (Worldwide Address Verification and Enhancement System). Le module de normalisation d'adresse du logiciel AddressDoctor peut être utilisé pour la résolution d'entité d'Identity Insight à l'aide de l'interface QS-AVI (DataStage et QualityStage Address Verification). QualityStage est un composant d'IBM Information Server.

AddressDoctor présente les avantages suivants :

- Prise en charge de plus de 240 pays et territoires.
- Meilleure couverture au niveau de la rue.
- Compatibilité avec le format Unicode et prise en charge des principaux jeux de caractères.
- Translittération.
- Statut de validation évaluant l'exactitude de l'adresse pour les livraisons.
- Formats pour les normes postales locales.

La mise en oeuvre du logiciel AddressDoctor avec l'interface QS-AVI est une tâche relativement complexe. Il est recommandé de contacter votre ingénieur commercial IBM pour obtenir l'assistance nécessaire.

Exigences du nettoyage d'adresses QS-AVI et présentation des tâches

Les étapes détaillées à suivre pour utiliser l'interface IBM QualityStage et AddressDoctor afin de nettoyer des adresses Identity Insight sont décrites dans un document technique à l'adresse ibm.com. Cette rubrique contient une présentation de la procédure, des exigences et un lien vers des informations détaillées.

Avant de commencer

Les produits suivants sont nécessaires :

- IBM InfoSphere Information Server incluant IBM InfoSphere DataStage et IBM InfoSphere QualityStage version 8.0.1
- Etapes QS-AVI Data Quality
- Base de données AddressDoctor pour le pays requis.

Pourquoi et quand exécuter cette tâche

La procédure est exécutée dans l'ordre suivant :

Procédure

1. Définissez un travail de l'étape QS-AVI dans DataStage and QualityStage Designer.
2. Importez le fichier "AddressValidateWS.dsx" dans l'étape. (Il s'agit d'un travail de nettoyage d'adresses prédéfini qui a été conçu pour l'intégration d'EAS et de QS-AVI.) Le fichier se trouve sur le disque d'installation du groupe de correctifs : `<INSTALLATION_RR>/srd-home/qsavi/AddressValidateWS.dsx`
3. Modifiez l'étape Address Verification et activez le travail DataStage pour Information Services.
4. Définissez le travail DataStage en tant que service dans la console Information Server.
5. Vérifiez le déploiement à l'aide de WISD (WebSphere Information Services Director) pour générer et examiner un document WSDL (Web Service Definition Language) de ce nouveau service.
6. Testez le service dans un environnement, tel que WebSphere Integration Developer.
7. Activez la fonction QSAVI en modifiant AddrConnection dans la section OAC du fichier pipeline.ini sous la forme suivante :

   [OAC]
   AddrConnection=qsavi://hôte:port/?timeout=ms

   hôte Est le nom d'hôte ou l'adresse IP du système Information Server.

   port Est le numéro de port. Le numéro de port par défaut est 9080.

   timeout
   Est un paramètre facultatif. Vous pouvez définir le paramètre du délai d'expiration de la connexion en externe. Le délai d'expiration de la connexion par défaut est 10000 ms (10 secondes).

Que faire ensuite

Les étapes de ce processus sont détaillées dans : Nettoyage d'adresse QS-AVI en tant que processus Web pour IBM InfoSphere Identity Insight.

identification et résolution des problèmes liés à QS-AVI

QS-AVI renvoie la chaîne ‘valstatus_qsav' qui décrit la qualité du nettoyage d'adresse et permet de résoudre les incidents associés.

Exceptions

Une exception est générée en fonction de l'état de la valeur d'indicateur :

```
// 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 renvoie également ‘resultstatus_qsav', qui décrit la probabilité du nettoyage d'adresses :

```
// 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
```

Messages d'erreur

6301E - Invalid response.

6302E - Cannot connect to InforServer server
Ce message est généré lorsque EAS ne parvient pas à se connecter à InfoServer. Il apparaît également avec la réponse ‘soapenv:Fault' d'InfoServer, qui est traitée comme une réponse non valide.

6303E - Error, failure to connect to the server : {0}", __serverName
Ce message est généré lorsque EAS ne parvient pas à se connecter au serveur InfoServer approprié.

Chapitre 8. Analyse de données

Analyst Toolkit fournit un ensemble de fonctions de développement et de personnalisation d'applications à Identity Insight. Il s'agit notamment d'un ensemble d'interfaces utilisateur et de rapports qui peuvent être modifiés selon vos besoins et référencés par d'autres applications.

Analyse de données à l'aide de Visualizer

A l'aide du Visualizer, vous pouvez effectuer plusieurs tâches d'analyse : réviser les alertes de disposition, rechercher des entités, afficher des données d'entités, afficher des graphiques d'entités et de leurs relations avec d'autres entités, créer et gérer des générateurs d'alerte d'attribut, ajouter une seule entité ou un petit fichier d'entités, divulguer des relations entre entités et imprimer des rapports.

Configuration du visualiseur

Pour utiliser efficacement Visualizer, vous devez savoir comment y accéder et comment personnaliser le mode d'affichage des informations en fonction de vos préférences.

Visualizer

Le Visualizer est une interface utilisateur graphique que les analystes et les investigateurs utilisent pour analyser les résultats des alertes, des relations et des résolutions d'entités.

Le Visualizer est hébergé par une version intégrée d'IBM WebSphere Application Server. Pour configurer le Visualizer , utilisez la console de configuration et les **Préférences** du menu **Fichier**.

Les utilisateurs du Visualizer peuvent réaliser plusieurs tâches d'analyse :

Analyse et définition d'alertes

Les alertes générées par le processus de résolution d'entité représentent les relations ou les résolutions d'entités qui peuvent concerner directement une entreprise. Généralement, les analystes consultent les alertes et décident le cas échéant de l'action à entreprendre, en fonction des informations de l'alerte. Il existe trois types d'alertes : les alertes de rôle, les alertes d'attribut et les alertes d'événements.

Le Visualizer affiche les alertes, offrant aux analystes à la fois un texte et un graphique relatifs à ces alertes ainsi qu'aux entités directement concernées. Les analystes peuvent explorer les détails en aval, puis définir l'état de l'alerte en conséquence.

Création et gestion des générateurs d'alertes d'attribut

Le Visualizer permet aux analystes de créer et gérer des recherches permanentes dans la fonction du générateur d'alertes d'attribut, mais aussi de gérer l'affichage et la réception des alertes d'attribut. Les analystes peuvent créer des générateurs d'alertes d'attribut basés sur des données d'attributs afin de localiser les identités résolues en entités en fonction de ces données d'attributs. Ils peuvent également créer un générateur d'alertes d'attribut afin de rechercher de façon permanente une entité spécifique dans la base de données de l'entité.

Recherche d'entités

Les utilisateurs du Visualizer peuvent également rechercher des entités pour une analyse approfondie à l'aide de plusieurs méthodes :

- Par attribut
- Par compte de source de données
- Par ID d'entité
- Par résolution (dans quelle mesure les critères saisis correspondent aux identités et aux entités dans la base de données de l'entité, en fonction de seuils de score de résolution minimum)

Ajout d'entités et de relations divulguées

Le Visualizer permet aux analystes d'ajouter des fiches pour la résolution d'entités et la détection de relations. Ils peuvent ajouter une seule fiche d'entité ou charger un fichier UMF contenant quelques milliers de fiches d'identités. Comme pour l'ajout de fiches d'identités via un programme d'acquisition, les fiches ajoutées via le Visualizer sont traitées par un pipeline pour la résolution d'entités et la détection de relations. Les résultats de ce traitement sont transcrits dans la base de données des entités et toute alerte est publiée dans le Visualizer .

Les analystes peuvent également divulguer les relations entre des entités (par identité), lorsqu'un lien existe entre des identités. L'association d'entités basées sur des contacts d'urgence ou de références répertoriées sur une application d'emploi est un exemple de relation divulguée. L'entité a révélé ces relations sur l'application.

Génération et impression de rapports

Le Visualizer contient également plusieurs rapports que les analystes peuvent consulter et imprimer afin de gérer et d'effectuer un suivi du travail accompli avec le Visualizer .

Configuration du visualiseur

Vous pouvez configurer les paramètres Visualizer pour définir le mode d'affichage des informations dans vos sessions Visualizer.

Paramétrage des options d'affichage du Visualizer :

Vous pouvez personnaliser l'affichage du Visualizer en modifiant les couleurs d'arrière-plan, la police, et autres options d'affichage dans l'onglet **Préférences de la fenêtre**.

Pourquoi et quand exécuter cette tâche

Les options d'affichage du Visualizer sont configurées pour chaque client Visualizer. A l'aide de ces instructions, vous ne pouvez modifier l'affichage que pour le client Visualizer auquel vous êtes actuellement connecté.

Procédure

1. Dans le Visualizer, cliquez sur **Fichier** > **Préférences** > **Préférences de la fenêtre**.
2. Choisissez l'aspect et la convivialité des options d'affichage à utiliser. Vous ne pouvez modifier les paramètres dans les listes déroulantes **Thème**, **Police**, et **Taille** que si vous sélectionnez l'option *Métal* dans **Aspect et convivialité**.
3. Cliquez sur **Soumettre**. Un message de confirmation vous informe que vous devez redémarrer le Visualizer avant que vos modifications ne soient effectives.
4. Cliquez sur **OK**.

5. Fermez le visualiseur. Démarrez le Visualizer et connectez-vous de nouveau.

Résultats

Le Visualizer s'affiche désormais avec les nouvelles options d'affichage de la fenêtre que vous avez sélectionnées.

Paramétrage du chemin d'accès par défaut des fichiers UMF :

Si vous chargez régulièrement des fiches d'identité dans des fichiers de données UMF pour un traitement via Visualizer, le paramétrage du chemin d'accès par défaut peut vous faire gagner une étape.

Pourquoi et quand exécuter cette tâche

Les paramètres par défaut du chemin d'accès sont configurés pour chaque client Visualizer. En spécifiant un chemin d'accès par défaut à l'aide de cette tâche, vous définissez uniquement le chemin d'accès dans le Visualizer auquel vous êtes actuellement connecté.

Procédure

1. Dans le Visualizer, sélectionnez **Fichier** > **Préférences** > **Préférences système**.
2. Dans **Chemin d'accès par défaut pour le chargement de fichier**, procédez comme suit :
   - Saisissez le chemin d'accès complet du répertoire à utiliser.
   - Ou accédez au répertoire pour le sélectionner.
3. Cliquez sur **Soumettre**. Un message de confirmation vous informe que vous devez redémarrer le Visualizer avant que vos modifications ne soient effectives.
4. Dans le message de confirmation, cliquez sur **OK**.
5. Fermez le Visualizer, réouvrez-le et connectez-vous de nouveau.

Résultats

Chaque fois que vous chargez un fichier UMF, le chemin d'accès par défaut correspond au répertoire que vous avez spécifié.

Définition du chemin d'accès par défaut pour Centrifuge :

Si vous utilisez le bureau Centrifuge optionnel des systèmes Centrifuges pour visualiser et afficher des graphiques d'entités, vous devez spécifier le chemin d'accès au bureau Centrifuge dans les préférences du Visualizer.

Pourquoi et quand exécuter cette tâche

Les paramètres par défaut du chemin d'accès sont configurés pour chaque client Visualizer. En spécifiant un chemin d'accès par défaut à l'aide de cette tâche, vous définissez uniquement le chemin d'accès dans le Visualizer auquel vous êtes actuellement connecté.

Procédure

1. Dans le Visualizer, cliquez sur **Fichier** > **Préférences** > **Préférences système**.
2. Sous la section **Chemins d'accès au fichier** dans **Chemin Centrifuge** :
   - Saisissez dans la zone le chemin d'accès au fichier ou l'URL (uniform resource locator) jusqu'à l'application du bureau Centrifuge.

- Ou accédez à l'application du bureau Centrifuge et ouvrez-la.

3. Cliquez sur **Soumettre**. Un message de confirmation vous informe que vous devez redémarrer le Visualizer avant que vos modifications ne soient effectives.
4. Dans le message de confirmation, cliquez sur **OK**.
5. Fermez le Visualizer, réouvrez-le et connectez-vous de nouveau.

Résultats

Une fois le chemin d'accès configuré, le bouton **Centrifuge** s'affiche sur les écrans **Détail d'alerte de rôle** et **Récapitulatif d'entité** dans la fenêtre **Recherche**. Cliquez sur le bouton pour lancer votre application du bureau Centrifuge Desktop directement depuis le Visualizer.

Définition des valeurs de seuil minimales pour les requêtes Visualizer :

Lorsque vous recherchez une entité à l'aide de la fonction Rechercher par résolution ou d'un générateur d'alerte d'attribut dans le Visualizer, vous sélectionnez un score de ressemblance minimal comme l'un des critères. Votre choix détermine la force de la résolution de l'entité et de la relation que le système utilise pour rechercher et renvoyer des entités. Vous pouvez modifier les valeurs par défaut d'un ou plusieurs de ces seuils dans l'onglet **Préférences système** du Visualizer.

Pourquoi et quand exécuter cette tâche

Ces paramètres sont configurés pour chaque client Visualizer. En effectuant cette tâche, vous ne modifiez que le seuil de score minimum du Visualizer auquel vous êtes actuellement connecté.

Procédure

1. Dans le Visualizer, cliquez sur **Fichier** > **Préférences** > **Préférences système**.
2. Dans la section **Valeurs de score minimum**, spécifiez le score de ressemblance le plus faible à utiliser pour déterminer quels résultats de recherche doivent être affichés. Plus le chiffre est élevé, plus les données de l'entité doivent correspondre aux critères de recherche, ce qui peut réduire le nombre de résultats renvoyés.
3. Cliquez sur **Soumettre**. Un message de confirmation vous informe que vous devez redémarrer le Visualizer avant que vos modifications ne soient effectives.
4. Dans le message de confirmation, cliquez sur **OK**.
5. Fermez le Visualizer, réouvrez-le et connectez-vous de nouveau.

Paramétrage des options par défaut du filtre de la fenêtre du Récapitulatif d'alerte :

Utilisez l'onglet **Paramétrage du filtre d'affichage d'alerte** de l'écran **Préférences système** pour personnaliser les paramètres par défaut des options de filtre de votre fenêtre **Récapitulatif d'alerte**.

Pourquoi et quand exécuter cette tâche

Ces paramètres contrôlent les valeurs par défaut suivantes dans le Visualizer :

- Le nombre maximal d'alertes à afficher dans la **Liste des alertes**
- Le score de relation minimum pour que s'affichent les alertes de rôle

- Le nombre de jours pendant lesquels s'affichent les récapitulatifs d'alerte (rétrospectivement depuis la date en cours)

Les valeurs que vous définissez ici déterminent les valeurs de filtre par défaut utilisées par votre instance de Visualizer chaque fois que vous ouvrez une nouvelle fenêtre **Récapitulatif d'alerte**.

Procédure

1. Dans le Visualizer, sélectionnez **Fichier** > **Préférences** > **Préférences système**.
2. Dans la section **Paramètres du filtre d'affichage d'alerte**, dans**Nombre maximal d'alertes à afficher dans la liste des alertes**, saisissez un nombre représentant le nombre maximal à afficher dans le tableau de la **Liste des alertes**. Le paramètre par défaut est 100, ce qui signifie que lorsque vous sélectionnez un récapitulatif d'alerte, les cent premières alertes associées s'affichent dans la **Liste des alertes**. Vous pouvez vouloir modifier le paramètre par défaut pour qu'il affiche moins d'alertes.
3. Dans **Score de relation minimum**, saisissez le score de relation le plus faible qui sera utilisé comme seuil pour l'affichage des alertes de rôle. Plus le score de relation est élevé, et plus est faible le nombre d'alertes de rôle et de récapitulatifs d'alerte de rôle qui s'affichent.
4. Dans **Nombres de jours d'affichage des alertes (y compris aujourd'hui)**, saisissez un nombre entre 1 et 99 qui indique le nombre de jours pendant lesquels l'alerte sera visible. Le nombre commence à la date en cours en progresse rétrospectivement, donc si vous saisissez 1, vous ne voyez les alertes générées que pendant la journée en cours. Si vous saisissez 10, vous ne verrez les alertes que pendant 10 jours - le jour en cours et les 9 jours précédents. La valeur par défaut est 99.
5. Facultatif : Si votre administrateur système a activé l'effacement du seuil d'alerte dans la Console de configuration, la case à cocher **Inclure les alertes de rôle filtrées** s'affiche.
   - Cochez la case **Inclure les alertes de rôle filtrées** pour afficher toutes les alertes de rôle et récapitulatifs d'alerte de rôle dans la fenêtre **Récapitulatif d'alerte** dont les scores de relation sont en dehors du seuil d'alerte minimum défini dans la règle d'alerte de rôle.
   - Décochez la case **Inclure les alertes de rôle filtrées** pour afficher uniquement les alertes de rôle et récapitulatifs d'alerte de rôle dans la fenêtre **Récapitulatif d'alerte** dont les scores de relation sont conformes au seuil d'alerte minimum.
6. Cliquez sur **Soumettre**. Un message de confirmation vous informe que vous devez redémarrer le Visualizer avant que vos modifications ne soient effectives.
7. Dans le message de confirmation, cliquez sur **OK**.
8. Fermez votre session du Visualizer, réouvrez-le et connectez-vous de nouveau.

Réglage des options de journal du visualiseur :

Vous pouvez connecter ou déconnecter le client Visualizer en configurant les options de connexion du Visualizer. Par défaut, la consignation du client Visualiseur est désactivée. En règle générale, vous activez la connexion du client Visualizer pour vous aider, vous et votre administrateur, dans le diagnostique de panne.

Pourquoi et quand exécuter cette tâche

Ces paramètres sont configurés pour chaque client Visualizer. En effectuant cette tâche, vous ne modifiez que les options de journalisation du Visualizer auquel vous êtes actuellement connecté.

Procédure

1. Dans le Visualizer, cliquez sur **Fichier** > **Préférences** > **Paramètres du journal et de la liaison**.
2. Effectuez l'une des actions suivantes sur la case à cocher **Activer la journalisation** :
   - Cochez la case à cocher pour activer la journalisation du client Visualizer.
   - Décochez la case à cocher pour désactiver la journalisation du client Visualizer.
3. Si vous avez activé la journalisation, indiquez le type de journalisation en sélectionnant une option dans **Niveau de détail du journal**. Si vous ne savez pas quel niveau sélectionner, consultez votre administrateur système. En général, dans la mesure où vous n'activez la journalisation du client Visualizer que pour faire le diagnostique de panne d'un incident, vous sélectionnez généralement le niveau débogage. Le niveau débogage consigne toute action que vous effectuez dans le Visualizer ainsi que chaque message (erreur, avertissement ou information) qui est généré. Ce niveau de journalisation remplit rapidement le fichier journal du Visualizer, ce qui signifie que vous devrez peut-être supprimer ce fichier de temps à autre.
4. Dans le **Chemin d'accès au répertoire du fichier journal** :
   - Saisissez le chemin d'accès pour enregistrer les fichiers journaux du Visualizer.
   - Ou accédez au répertoire et sélectionnez-le.
5. Cliquez sur **Soumettre**. Un message de confirmation vous informe que vous devez redémarrer le Visualizer avant que vos modifications ne soient effectives.
6. Dans le message de confirmation, cliquez sur **OK**.
7. Fermez le Visualizer, réouvrez-le et connectez-vous de nouveau.

Paramétrage des options d'hyperlien du Visualizer pour l'affichage des attributs personnalisés :

Si votre organisation comprend des liens vers des fichiers ou des images se trouvant sur d'autres systèmes dans le cadre des attributs de fiche d'identité, le Visualizer peut afficher des hyperliens vers ces fichiers. Vous cliquez sur l'hyperlien pour lancer votre navigateur Web ou votre application pour afficher le fichier ou l'image sélectionnée. Utilisez les préférences systèmes de Visualizer pour sélectionner quel navigateur ou programme ouvre les fichiers lorsque vous cliquez sur un hyperlien.

Pourquoi et quand exécuter cette tâche

Ces paramètres sont configurés pour chaque client Visualizer. En effectuant cette tâche, vous modifiez uniquement les options de l'hyperlien du Visualizer auquel vous êtes actuellement connecté.

Procédure

1. Dans le Visualizer, sélectionnez **Fichier** > **Préférences** > **Paramètres du journal et de la liaison**.

2. Sous **Paramètres de gestion des hyperliens**, sélectionnez l'une des options suivantes :
   - **Paramétrage du navigateur par défaut**
   - Ou **Utilisez le programme** et indiquez un navigateur ou un programme à utiliser pour ouvrir les hyperliens.

   Remarque : Il se peut que vous deviez seulement spécifier un navigateur Web ou un autre programme pour ouvrir des liens qui sont stockés sur des sites Web sécurisés (https://).
3. Cliquez sur **Soumettre**. Un message de confirmation vous informe que vous devez redémarrer le Visualizer avant que vos modifications ne soient effectives.
4. Dans le message de confirmation, cliquez sur **OK**.
5. Fermez le Visualizer, réouvrez-le et connectez-vous de nouveau.

Réglage des options de graphique du visualiseur :

Vous pouvez personnaliser les paramètres du graphique que vous voyez dans le Visualizer en modifiant la couleur ou l'épaisseur des lignes dans l'onglet **Préférences du graphique**.

Pourquoi et quand exécuter cette tâche

Les paramètres d'affichage du graphique du Visualizer sont configurés pour chaque client Visualizer. A l'aide de ces instructions, vous affectez uniquement les paramètres du client Visualizer auquel vous êtes actuellement connecté.

Procédure

1. Dans le Visualizer, cliquez sur **Fichier** > **Préférences** > **Préférences du graphique**.
2. Sélectionnez l'épaisseur et la couleur de la ligne à utiliser.
3. Cliquez sur **Soumettre**. Un message de confirmation vous informe que vous devez redémarrer le Visualizer avant que vos modifications ne soient effectives.
4. Dans le message de confirmation, cliquez sur **OK**.
5. Fermez le Visualizer, réouvrez-le et connectez-vous de nouveau.

Résultats

Le Visualizer affiche maintenant les graphiques avec les nouvelles options d'affichage que vous avez sélectionnées.

Rubriques d'aide :

Onglet Préférences d'affichage :

Utilisez cet onglet pour configurer la manière dont le Visualizer affiche les couleurs d'arrière-plan, les polices, et les icônes de navigation dans vos sessions du Visualizer. La configuration des préférences dans cet onglet affecte uniquement les paramètres du client Visualizer local. Si vous modifiez l'un de ces paramètres, quittez, réouvrez et reconnectez-vous au Visualizer pour voir les modifications.

Présentation

Sélectionnez un groupe préformaté des paramètres d'affichage. Les paramètres d'affichage du groupe contrôlent les sélections disponibles dans le **Thème**, la **Police**, et la **Taille**.

Remarque : La plupart des paramètres d'affichage ne vous permettent pas de sélectionner les autres zones. Actuellement, **Métal** est la seule option vous permettant de choisir d'autres paramètres d'affichage.

Le paramètre d'affichage de groupe par défaut est **Visualizer EAS**.

Thème
Choisissez une combinaison de couleur d'écran préformatée pour le paramètre d'affichage de groupe que vous avez sélectionné dans **Aspect et convivialité**.

Police Sélectionnez une police d'affichage.

Taille Sélectionnez une taille de police.

Exemple
Vous propose un aperçu de ce à quoi ressemblera l'affichage de votre Visualizer, en fonction de vos sélections.

Couleur d'arrière-plan
Cliquez sur ce bouton pour sélectionner une couleur d'arrière-plan. Cette zone n'est disponible que si vous avez sélectionné **Métal** dans la zone **Aspect et convivialité**.

Couleur du contrôle
Cliquez pour sélectionner une couleur de contour de contrôle.

Couleur du texte
Cliquez pour choisir la couleur du texte.

Onglet Préférences système :

Utilisez cet onglet pour configurer les préférences système de vos sessions de Visualizer. La configuration des préférences affecte ici uniquement les paramètres système de votre client Visualizer local. Si vous modifiez l'un de ces paramètres, quittez, réouvrez et reconnectez-vous au Visualizer pour voir les modifications.

Section Chemins de fichiers
Indiquez les chemins d'accès par défaut utilisés par le Visualizer pour charger des fichiers UMF et ouvrir l'outil de graphique Centrifuge Desktop. Si vous utilisez l'application Centrifuge Desktop pour visualiser les graphiques d'entités et les données d'entités, saisissez le chemin d'accès complet à l'application. En saisissant ici le chemin d'accès complet, vous pouvez accédez à Centrifuge directement à partir du Visualizer.

Section Valeurs de score minimum
Définissez les valeurs des seuils de score de ressemblance que vous pouvez sélectionner à partir du moment où vous créez une requête Rechercher par résolution ou un générateur d'alerte d'attribut.

Cette section contient par défaut les valeurs recommandées pour chacun de ces seuils. Ces valeurs recommandées sont des valeurs de prudence, destinées à renvoyer moins de résultats faux positifs. Vous pouvez redéfinir les valeurs afin qu'elles correspondent à vos objectifs.

En règle générale, plus la valeur d'un seuil de score minimum est élevée, et plus est faible le nombre de résultats renvoyés. Plus la valeur est faible, et plus est élevé le nombre de résultats renvoyés.

Entité Is
Saisissez le score de résolution le plus faible qui définit quand l'entité de recherche définie dans une requête Rechercher par

résolution ou un générateur d'alerte d'attribut dans la base de données d'entités représentent la même entité.

La valeur par défaut est 100. Cette valeur par défaut signifie que lorsque l'entité de recherche et une identité sont comparées, si le score de résolution est de 100, l'entité renvoyée est la même que l'entité de recherche.

Correspondance d'entité proche
Saisissez le score de résolution le plus faible qui définit quand il existe une "étroite concordance" entre l'entité de recherche définie dans une requête Rechercher par résolution ou un générateur d'alerte d'attribut et une entité dans la base de données d'entités.

La valeur par défaut est 85. Cette valeur par défaut signifie que lorsque l'entité de recherche et une entité de la base de données d'entités sont comparées, si le score de résolution minimum est égal ou supérieur à 85, mais inférieur au score **Est l'entité**, l'entité renvoyée est une concordance étroite avec l'entité de recherche.

Bonne relation
Saisissez le score le plus faible qui définit quand il existe une relation étroite ou forte entre l'entité de recherche définie dans une requête Rechercher par résolution ou un générateur d'alerte d'attribut et une entité dans la base de données d'entités. la valeur représente la force de la relation.

La valeur par défaut est 35, ce qui signifie que lorsque l'entité de recherche et une entité de la base de données d'entités sont comparées, si le score de résolution minimum est supérieur ou égal à 35, la relation entre les deux est bonne.

N'importe quelle relation
Saisissez le score le plus faible qui définit quand il existe une relation entre l'entité de recherche définie dans une requête Rechercher par résolution ou un générateur d'alerte d'attribut et une entité dans la base de données d'entités. (La valeur représente la force de la relation).

La valeur par défaut est 1, ce qui signifie que lorsque l'entité de recherche et une entité de la base de données d'entités sont comparées, si le score de résolution minimum est supérieur ou égal à 1, les deux entités ont une relation.

Section Paramètres du filtre d'affichage d'alerte
Utilisez cette section pour configurer les paramètres du filtre d'alerte par défaut qui affectent les récapitulatifs d'alerte qui s'affichent dans la fenêtre **Récapitulatif d'alerte**. Chaque fois que vous ouvrez une nouvelle fenêtre **Récapitulatif d'alerte**, le système utilise ces paramètres par défaut.

Nombre d'alertes maximal à afficher dans la liste des alertes
Saisissez un nombre qui représente le nombre maximal d'alertes à afficher dans le tableau de la **Liste des alertes** dans la fenêtre **Récapitulatif d'alerte**.

La valeur du filtre par défaut est de 100, ce qui signifie que, par défaut, seules s'affichent les 100 premières alertes de tout récapitulatif d'alerte sélectionné.

Score de relation minimum
Saisissez le score de relation le plus faible pour filtrer les

récapitulatifs d'alerte de rôle non affectée inférieurs à ce score dans l'affichage de votre fenêtre **Récapitulatif d'alerte**.

Par exemple, pour voir uniquement les récapitulatifs d'alerte de rôle pour lesquels le score de relation entre les deux entités comparées est supérieur ou égal à 50, saisissez `50` dans cette zone.

La valeur par défaut est 0, ce qui signifie que tous les récapitulatifs d'alerte de votre groupe d'analystes Visualizer et qui sont actuellement à l'état "Non affecté" s'affichent par défaut.

Nombre de jours d'affichage des alertes (y compris aujourd'hui)
Saisissez un nombre entre 1 et 99 qui indique le nombre de jours pendant lesquels les alertes seront affichées. Gardez à l'esprit que ce "jour" est une journée civile complète, qui commence à 0:00:00 et se termine à 23:59:59.

Le chiffre commence par la date en cours et remonte dans le passé. Si vous souhaitez voir des alertes générées dans les 90 derniers jours (le jour en cours et les 89 jours précédents), saisissez `90`.

La valeur par défaut est `99`, ce qui signifie que vous voyez les alertes générées aujourd'hui et 98 jours civils avant aujourd'hui.

Case à cocher Inclure les alertes de rôle filtrées
(Facultatif) Cochez cette case à cocher pour afficher toutes les alertes de rôle non affectées générées, et même les alertes inférieures au seuil d'alerte minimal, spécifié dans la configuration de la règle d'alerte de rôle. Cette case à cocher ne s'affiche que si votre administrateur système a activé cette fonction.

La sélection par défaut est effacée, ce qui signifie que seules les alertes de rôle actuellement non affectées qui satisfont ou dépassent le seuil d'alerte minimal (tel que défini dans la règle d'alerte de rôle) s'affichent dans le Visualizer.

Section Paramètres divers
Utilisez cette section pour activer les infobulles et la fenêtre de confirmation de sortie.

Activer les infobulles
Si les infobulles sont activées, chaque fois que votre curseur se déplace sur une icône de barre d'outil, ou sur une zone pour laquelle des informations supplémentaires sont disponibles, les infobulles s'affichent. Par défaut, les infobulles sont activées.

Afficher la boîte de dialogue de confirmation de sortie
Cette option détermine si le système affiche une boîte de dialogue de confirmation lorsque vous quittez le Visualizer.

- Cochez cette case à cocher pour confirmer à chaque fois votre choix de quitter le Visualizer. Le paramètre par défaut est sélectionné.
- Décochez cette case à cocher pour quitter le Visualizer sans afficher la boîte de dialogue **Confirmation de sortie** chaque fois que vous choisissez de quitter et de vous déconnecter du Visualizer.

Onglet Paramètres du journal et des liens :

Utilisez cet onglet pour configurer les paramètres de journalisation et d'hyperlien du client Visualizer. La configuration des préférences n'affecte ici que les

paramètres du client Visualizer local. Si vous modifiez l'un de ces paramètres, quittez, réouvrez et reconnectez-vous au Visualizer pour voir les modifications.

Paramètres du journal

Cochez la case à cocher pour activer la journalisation du client Visualizer, ou décochez la case à cocher pour la désactiver. En règle générale, vous n'activez la journalisation du client Visualizer que si vous travaillez avec votre administrateur système pour résoudre un message d'erreur ou un problème qui s'est produit pendant votre session du Visualizer. Par défaut, la consignation du client Visualiseur est désactivée.

Niveau de journalisation

Sélectionnez le niveau de détail de journalisation, uniquement disponible si la journalisation du client Visualizer est activée. Le niveau de détail détermine la quantité d'informations collectées dans le journal du Visualizer alors que vous l'utilisez. Consultez votre administrateur système avant de faire votre choix. En règle générale, vous activez la journalisation pour diagnostiquer une panne dans le Visualizer. C'est pourquoi vous sélectionnez généralement le niveau de débogage, qui correspond au niveau de détail de journalisation le plus élevé. Le niveau de débogage consigne chaque action et message qui se produit pendant que vous utilisez le Visualizer. Mais ce niveau de journalisation remplit également très vite le fichier journal du client Visualizer, vous devrez donc effacer le fichier journal de temps à autre. C'est la raison pour laquelle vous désactivez généralement la journalisation une fois le problème résolu.

Chemin d'accès au fichier journal

Indiquez l'emplacement du fichier et du répertoire des fichiers journaux du client Visualizer. En règle générale, vous n'avez besoin d'analyser les fichiers journaux que lorsque vous effectuez un diagnostique d'un problème ou d'un message. Les fichiers journaux peuvent se remplir d'informations très rapidement, et particulièrement au niveau de débogage. Si la journalisation du client Visualizer est activée, vous pourrez devoir occasionnellement purger les fichiers journaux afin d'éviter que ces fichiers ne deviennent trop volumineux.

Paramètres de traitement des hyperliens

Sélectionnez une option pour déterminer le programme ou le navigateur utilisé par le Visualizer pour ouvrir et afficher les hyperliens. Les fiches d'identité entrantes peuvent contenir des hyperliens, qui peuvent vous diriger vers d'autres fichiers, sites Web, ou systèmes qui contiennent des informations sur l'identité ou l'entité en rapport avec votre analyse. Les hyperliens font partie de la fiche d'identité et s'affichent en tant qu'attributs dans le récapitulatif d'entité et le graphique de résolution d'entité.

Si vous rencontrez des problèmes ou avez des questions lorsque vous cliquez sur un hyperlien, sélectionnez l'option **Utiliser le programme** et indiquez le navigateur ou le programme à utiliser pour ouvrir les hyperliens. Par exemple, si votre organisation stocke des fichiers d'empreintes digitales sur un site web sécurisé (https://), utilisez cette option pour indiquer votre navigateur web ou autre programme permettant d'ouvrir les liens qui mènent au site sécurisé des fichiers d'empreintes digitales.

Onglet Préférences de graphique :

Utilisez cet onglet pour spécifier les propriétés d'affichage des lignes qui connectent des entités dans les graphiques du Visualizer. La configuration des préférences ici affecte uniquement les paramètres du client Visualizer local. Si vous modifiez l'un de ces paramètres, quittez, réouvrez et reconnectez-vous au Visualizer pour voir les modifications.

Epaisseur du trait
Sélectionnez une épaisseur de trait. L'épaisseur de trait par défaut est de 2 pixels.

Couleur du trait
Sélectionnez une couleur de trait. La couleur de trait par défaut est un bleu moyen.

Exemple de trait
Affiche un exemple de trait du graphique, conformément à vos sélections.

Démarrage de Visualizer

Pour visualiser des entités et des données d'une base de données d'entité, vous devez d'abord démarrer Visualizer et vous connecter.

Pour lancer le Visualizer, la version système par défaut Java traite un fichier JNLP (Java Network Launch Protocol) Java Web Start que le serveur d'application produit télécharge sur le client de votre poste de travail. Le fichier JNLP est accessible de différentes manières. Mais pour pouvoir ouvrir le Visualizer, la version client requise de Java Web Start doit ouvrir le fichier JNLP.

Si plusieurs versions de Java sont installées sur votre machine cliente, il est probable que la version système par défaut de Java Web Start ne soit pas la version client requise. Vous pouvez quand même réussir à ouvrir et à exécuter le Visualizer, mais vous devez d'abord configurer votre navigateur Web pour qu'il utilise la version client requise de Java Web Start.

Remarque : La version client Java requise pour ouvrir et exécuter le Visualizer peut ne pas être la version la plus récente de Java.

Connexion au Visualizer

Avant de vous connecter au Visualizer, vous devez avoir un compte utilisateur Visualizer (nom d'utilisateur et mot de passe). Votre administrateur système peut vous fournir ces informations.

Procédure

1. Effectuez l'une des opérations suivantes :
   - Cliquez deux fois sur l'icône Visualizer sur votre bureau.
   - Ouvrez votre navigateur Internet et entrez l'adresse URL de Visualizer dans la barre d'adresse.

   L'URL de lancement du Visualizer est la suivante :

   `http://server:install_port`

   Par exemple, `http://localhost:13510`. Une fois Visualizer installé, la valeur *port_installation* par défaut est 13510, mais le numéro de port est modifiable. Contactez votre administrateur système si vous n'êtes pas sûr du nom de serveur ou du numéro de port.

2. Connectez-vous en entrant votre nom d'utilisateur et votre mot de passe.

   Remarque : Ces deux zones sont sensibles à la casse. A la première connexion, utilisez le mot de passe attribué par votre administrateur système. Une fois connecté, modifiez votre mot de passe Visualizer pour garantir la sécurité de votre compte Visualizer.
3. Cliquez sur **Ouvrir une session**.

Configuration de votre navigateur Web pour utiliser la version client requise de Java Web Start :

Si votre poste de travail contient plusieurs versions de Java et si vous rencontrez des difficultés pour ouvrir le Visualizer, configurez les préférences de votre navigateur Web afin de sélectionner la version client requise de Java Web Start. Ainsi, votre navigateur Web utilise automatiquement la version client requise de Java Web Start pour ouvrir chaque fois correctement le Visualizer.

Configuration de Microsoft Windows Internet Explorer pour utiliser la version requise de Java Web Start :

Microsoft Internet Explorer utilise les associations de fichiers par défaut définies pour le système d'exploitation Microsoft Windows afin de déterminer le mode de gestion des fichiers JNLP (Java Network Launch Protocol). En définissant ou en modifiant l'application de fichiers par défaut associée au traitement des fichiers JNLP, vous pouvez rediriger Internet Explorer afin qu'il utile la version adéquate de Java Web Start. Si plusieurs versions de Java sont installées, la modification de ce paramètre peut éviter des problèmes lors de l'ouverture du Visualizer.

Pourquoi et quand exécuter cette tâche

Cette procédure demande à Internet Explorer d'utiliser la version Java Web Start pour ouvrir toutes les applications Web. Si vous exécutez d'autres applications Web Start qui exigent des versions ultérieures de Java, utilisez plutôt l'approche de lancement direct.

Remarque : Quelques problèmes connus de Java version 1.6 sont à garder à l'esprit :

- Java version 1.6 efface parfois l'association de fichiers Windows par défaut pour les fichiers JNLP. Si vous utilisez Java version 1.6 en tant que m JVM (machine virtuelle Java) de votre système, et que ces étapes ne vous permettent pas de lancer et d'ouvrir le Visualizer, essayez d'utiliser un autre navigateur Web pour lancer le Visualizer, ou utilisez l'approche de lancement direct.
- Si votre poste de travail utilise Java version 1.6, il se peut que vous deviez configurer le JRE (environnement d'exécution Java) afin qu'il accepte les téléchargements automatiques. Si votre poste de travail rencontre ce problème, lorsque vous essaierez de démarrer le Visualizer, vous verrez un message d'erreur indiquant que l'application a demandé une version de JRE qui n'est pas installée localement.

Procédure

1. Dans le **Panneau de commande Windows**, effectuez l'une des opérations suivantes :
   - Dans la vue Catégorie, double-cliquez sur **Performance et Maintenance**. Dans la sous-fenêtre de navigation **Voir également**, situé dans le coin supérieur gauche de la fenêtre, sélectionnez **Types de fichier**.

- Dans la vue Classique, cliquez deux fois sur **Options de dossier**.

2. Dans la boîte de dialogue **Options de dossier**, cliquez sur l'onglet **Types de fichier**.
3. Dans la colonne Extensions, localisez et sélectionnez l'entrée **JNLP**. Les entrées sont classées par ordre alphabétique d'extension.

   Remarque : Si l'entrée JNLP n'existe pas, cliquez sur **Nouveau** pour créer cette entrée.
4. Cliquez sur **Modifier**.
5. Dans la boîte de dialogue **Ouvrir avec**, veillez à ce que **fichier exécutable Java WebStart** soit coché. Cliquez sur **Parcourir** pour accéder à votre répertoire Java installé.
6. Sélectionnez le fichier exécutable nommé `javaws` et cliquez sur **OK**.
7. Cliquez sur **OK** afin de fermer la boîte de dialogue **Options de dossier**. (Vous pouvez également fermer la fenêtre **Panneau de commande**.)

Résultats

Internet Explorer utilise désormais le fichier Java Web Start associé pour traiter et ouvrir correctement le Visualizer.

Configuration de Mozilla Firefox pour utiliser la version requise de Java Web Start :

En configurant ou en modifiant la manière dont Mozilla Firefox gère les fichiers JNLP (Java Network Launch Protocol), vous pouvez demander à Firefox d'utiliser automatiquement la version client Java Web Start requise afin de démarrer le Visualizer. Si plusieurs versions de Java sont installées, la modification de ce paramètre peut éviter des problèmes lors de l'ouverture du Visualizer.

Pourquoi et quand exécuter cette tâche

Cette procédure demande à Firefox d'utiliser la version Java Web Start pour ouvrir toutes les applications Web. Si vous exécutez d'autres applications Web Start qui exigent des versions ultérieures de Java, utilisez plutôt l'approche de lancement direct.

Procédure

1. Lancez Mozilla Firefox.
2. Sélectionnez **Outils** > **Options**.
3. Sélectionnez **Applications**
4. Sous **Type de contenu**, localisez l'entrée du **fichier JNLP**.

   Remarque : Si vous ne voyez pas d'entrée pour le **Fichier JNLP**, fermez la boîte de dialogue **Options**. Sur la page Visualizer Web Start, essayez de lancer le Visualizer en cliquant sur le lien **Cliquez ici pour lancer IBM Identity Insight Visualizer**. Puis recommencez à l'étape 1.
5. Sélectionnez l'entrée **fichier JNLP**.
6. Sous **Action**, sélectionnez l'option **Utiliser un autre**.
7. Dans la boîte de dialogue **Sélectionner l'application du programme d'aide**, cliquez sur **Parcourir**, accédez au répertoire où est installée la version client requise de Java, et sélectionnez le fichier exécutable `javaws`.
8. Cliquez sur **OK** afin de fermer la boîte de dialogue **Sélectionnez l'application du programme d'aide**.

9. Cliquez sur **OK** afin de fermer la boîte de dialogue **Options**.

Résultats

Mozilla Firefox utilise désormais le fichier Java Web Start sélectionné pour gérer tous les types de fichier JNLP. Le Visualizer s'ouvre correctement.

Lancement du Visualizer directement depuis un fichier exécutable Java Web Start :

Si vous souhaitez lancer le Visualizer sans modifier les paramètres Java ou autres paramètres système, vous pouvez utiliser l'approche de lancement direct. Cette approche lance le Visualizer directement depuis le fichier exécutable Java Web Start. Vous pouvez souhaiter utiliser l'approche de lancement direct si plusieurs versions de Java sont installées sur votre poste de travail et que vous utilisez d'autres applications Web Start parallèlement au Visualizer.

Avant de commencer

Localisez le chemin d'accès au fichier exécutable Java Web Start requis (`javaws`) sur votre poste de travail.

Pourquoi et quand exécuter cette tâche

Vous pouvez également créer un raccourci sur votre bureau jusqu'au fichier exécutable Java Web Start en sélectionnant le fichier `javaws` et en saisissant l'URL du Visualizer dans la zone **Cible**.

Procédure

1. Depuis votre bureau, ouvrez une fenêtre de commande DOS.
2. Dans la ligne de commande, saisissez la commande de lancement direct : URL du Visualizer *path_to_Java_installationpath_to_javaws_exe_file*>javaws.exe Par exemple, **C:/IBM/Java60/jre/bin>javaws.exe http://localhost:13510/docs/rrmdi.jnlp**

   Important : Notez l'espace entre l'extension du fichier exécutable Java Web Start et l'URL.

Résultats

Le Visualizer s'ouvre correctement.

Configuration de Java v1.6 pour l'exécution du Visualizer sur les postes de travail Microsoft Windows :

Si vous essayez de lancer le Visualizer et que vous constatez un message d'erreur indiquant que l'application a demandé une version de JRE qui n'est pas installée localement, essayez de modifier les paramètres de téléchargement automatique pour Java. Ce message d'erreur est un problème connu sur les postes de travail Microsoft Windows sur lesquels est installé Java version 1.6.

Procédure

1. Dans le **Panneau de commande Windows**, sélectionnez l'une des options suivantes :

- Pour les installations IBM de Java, sélectionnez le **Panneau de commande IBM pour Java**.
- Pour les installations Sun de Java, sélectionnez **Java**.

2. Dans l'onglet **Avancé**, développez le paramètre **Téléchargement automatique de JRE**. Si vous ne voyez pas cette option et que vous avez plusieurs versions de Java installées sur ce poste de travail, fermez le **Panneau de commande Java** et sélectionnez l'autre entrée.
3. Veillez à ce que le paramètre **Téléchargement automatique de JRE** soit réglé sur **Toujours effectuer les téléchargements automatiques** (recommandé) ou **Demander à l'utilisateur**. Le paramètre **Ne jamais effectuer de téléchargement automatique** interdit l'ouverture du Visualizer et de la Console de configuration.
4. Cliquez sur **Appliquer** .
5. Cliquez sur **OK**.
6. Fermez la fenêtre du **Panneau de commande**.

Fermeture du visualiseur

Lorsque vous en avez terminé avec Visualizer, fermez-le. En fermant le Visualizer, vous vous déconnectez également. Si vous faites une pause et que vous voulez simplement sécuriser votre poste de travail pendant quelques minutes, vous pouvez verrouiller le Visualizer.

Procédure

Pour fermer le Visualizer et vous déconnecter :

- Sélectionnez **Fichier** > **Quitter**,
- Ou appuyez sur **Ctrl** + **Q**.

Verrouillage du visualiseur

Si vous faites une courte pause ou que vous vous éloignez de votre poste de travail pendant quelques minutes, au lieu de fermer et de vous déconnecter du Visualizer, vous pouvez le verrouiller. Le verrouillage du Visualizer sécurise votre travail en agissant comme un économiseur d'écran sécurisé. Lorsque vous verrouillez le Visualizer, la fenêtre **Connexion** s'affiche. Vous réentrez dans votre session du Visualizer en saisissant votre mot de passe utilisateur.

Procédure

Pour verrouiller le Visualizer :

- Sélectionnez **Fichier** > **Verrouiller l'application**.
- Ou appuyez sur **Ctrl** + **L**.

Résultats

Votre session du Visualizer est désormais verrouillée.

Que faire ensuite

Pour réutiliser le Visualizer, saisissez votre mot de passe et cliquez sur **Déverrouiller**.

Modification de votre mot de passe de Visualiseur

La modification régulière de votre mot de passe Visualizer constitue un bon moyen de protéger la sécurité de votre compte utilisateur Visualizer.

Avant de commencer

Pour changer de mot de passe, il faut que vous soyez connecté à Visualizer.

Pourquoi et quand exécuter cette tâche

Pour les mots de passe Visualizer, il n'y a pas de nombre minimal de caractères requis. Vous pouvez utiliser toute combinaison de lettres (en majuscules ou minuscules), caractères spéciaux et chiffres. Le mot de passe est sensible à la casse. Ainsi, lorsque vous vous connectez, le mot de passe que vous saisissez doit correspondre au mot de passe de votre compte Visualizer. Par exemple, si votre mot de passe est `PASSw0rd`, et que vous essayez de vous connecter en saisissant `passw0rd`, les mots de passe ne correspondent pas et le système affiche un message d'erreur.

Procédure

1. Dans le Visualizer, cliquez sur **Fichier** > **Modifier le mot de passe**.
2. Dans **Mot de passe actuel**, saisissez le mot de passe que vous avez utilisé pour vous connecter à cette session de Visualizer. Si votre mot de passe vous a été affecté ou a été réinitialisé, il s'agit du mot de passe de votre administrateur système.
3. Dans **Nouveau mot de passe**, saisissez le nouveau mot de passe qui sera votre mot de passe Visualizer.
4. Dans **Répéter le nouveau mot de passe**, saisissez le même mot de passe que vous venez de saisir dans **Nouveau mot de passe**.
5. Cliquez sur **Modifier le mot de passe**.

Résultats

- Si les entrées dans **Nouveau mot de passe** et **Répéter le nouveau mot de passe** sont identiques, le système affiche un message indiquant que votre mot de passe a été modifié. Cliquez sur **OK**. Utilisez votre nouveau mot de passe lors de votre prochaine connexion à Visualizer
- Si les entrées ne correspondent pas, le système affiche un message d'erreur indiquant que les nouveaux mots de passe ne correspondent pas. Cliquez sur **OK**. Votre mot de passe n'est pas modifié. Pour le modifier, recommencez à partir de l'étape 2.

Analyse des alertes dans le Visualizer

L'une des tâches les plus communes que les utilisateurs du Visualizer exécutent consiste à évaluer les alertes afin de déterminer celles qui sont à réviser et celles qui sont à transférer aux autres groupes du Visualizer.

Les alertes s'affichent dans la fenêtre **Récapitulatif d'alerte** du Visualizer. Cette fenêtre représente le point de départ de l'évaluation, affectation ou transfert, et analyse des alertes.

Les alertes sont regroupées en récapitulatifs d'alerte. Les récapitulatifs d'alerte contiennent toutes les alertes du même type et ayant la même description, gravité, état, règle de résolution, score de relation, et score de résolution (ressemblance). Un récapitulatif d'alerte contient généralement plusieurs alertes spécifiques dont chacune doit être analysée et contrôlée. Une partie du contrôle comprend l'affectation d'une disposition à l'alerte, afin que vous et les autres utilisateurs du Visualizer connaissiez l'état de l'analyse et puissiez voir les commentaires indiquant vos conclusions.

N'oubliez pas que votre fenêtre **Récapitulatif d'alerte** affiche uniquement les éléments suivants :

- Les récapitulatifs d'alerte de votre groupe d'analystes Visualizer contenant les alertes non affectées
- Les alertes que vous vous êtes déjà affectées à vous-même

Vous ne voyez pas les alertes que les autres analystes de votre groupe d'analystes Visualizer se sont affectées à eux-mêmes. Vous ne voyez pas non plus les alertes assignées aux autres groupes d'analystes Visualizer.

Evaluation des récapitulatifs d'alerte

Comment déterminez-vous les alertes à vous attribuer à vous-même à des fin d'analyse ? Commencez par passer en revue les récapitulatifs d'alerte dans la fenêtre **Récapitulatif d'alerte**. Alors que vous consultez ces récapitulatifs d'alerte, comparez l'importance des informations qui constituent le récapitulatif d'alerte avec vos objectifs d'analyse. Vous pouvez devoir évaluer une ou plusieurs informations d'alerte avant de faire votre choix.

Astuces pour vous aider à hiérarchiser les récapitulatifs d'alerte :

- **Gravité de l'alerte :** Commencez par trier les récapitulatifs d'alerte par ordre de gravité. Cliquez sur l'en-tête de colonne **Gravité de l'alerte** . Ces informations peuvent être suffisantes pour vous aider à déterminer les alertes les plus critiques ou importantes pour commencer l'analyse. Par exemple, si votre organisation utilise la lettre "C" pour les alertes assorties d'une gravité critique, vous pouvez immédiatement voir les alertes critiques en regardant simplement leur gravité.
- **Description de l'alerte :** La gravité seule peut ne pas constituer une information suffisante. La description de l'alerte peut vous aider à choisir les alertes les plus importantes dans la liste de priorité, si plusieurs récapitulatifs d'alerte ont le même niveau de gravité d'alerte. Par exemple, il peut être plus important d'analyser les alertes regroupées sous la description "Aucun vol ne connaît le passager" plutôt que celles ayant la description "Le passager connaît un employé".
- **score de ressemblance et score de relation :** Plus le score est élevé, et plus il est probable qu'une relation d'intérêt existe ou que l'identité est l'entité. Dans l'exemple "Aucun vol ne connaît le passager", si les scores de ressemblance et de relation sont de 100, alors, la personne dans la liste d'interdiction de vol est le passager, et vous pouvez souhaitez prendre des mesures immédiates. Si la ressemblance est inférieure à 70 et que le score de relation est inférieur à 85, cette alerte peut encore être importante, mais non critique. Vous pouvez toujours souhaiter analyser les entités impliquées dans l'alerte, mais vous pouvez ne pas avoir besoin de prendre des mesures immédiates.

En tant qu'utilisateur Visualizer, vous connaissez les objectifs de votre organisation, et vous pouvez donc probablement ajouter vos propres facteurs personnels à utiliser lors de la hiérarchisation des alertes. Ces astuces vous permettent de commencer.

Affectation d'alertes

Dès que vous connaissez les alertes sur lesquelles vous voulez travailler, en fonction de la priorité, vous pouvez vous attribuer ces alertes. L'affectation des alertes permet à votre groupe d'analystes Visualizer de diviser et de maîtriser la liste des alertes entrantes. Lorsqu'une alerte vous est affectée, celle-ci s'affiche uniquement dans votre fenêtre Récapitulatif d'alerte, évitant ainsi tout doublon

avec un autre utilisateur Visualizer sur la même alerte. Vous pouvez immédiatement voir les alertes que vous seul recherchez actuellement.

Si, dans votre fenêtre Récapitulatif d'alerte, vous voyez une ou plusieurs alertes qui pourraient selon vous appartenir à un autre groupe d'analystes Visualizer, vous pouvez transférer ces alertes. Par exemple, vous travaillez comme agent de réservation et évaluez les alertes générées par les nouvelles réservations ou les réservations modifiées. Vous voyez une alerte répertoriée, gérée par la sécurité. Vous pouvez affecter cette alerte au groupe de Sécurité, car l'alerte est sous la juridiction de ce groupe.

Révision et disposition des alertes

Lorsque vous vous affectez une ou plusieurs alertes, vous pouvez alors procéder aux tâches de rechercher et d'analyse de ces alertes. Le Visualizer simplifie la tâche dans la fenêtre Rechercher, qui affiche dans une fenêtre toutes les informations correspondantes associées à l'alerte. Dans la fenêtre Rechercher, vous pouvez, dans le cadre de votre analyse, exécuter l'une des tâches suivantes :

- Examiner les détails d'alerte
- Consulter les récapitulatifs d'entité des entités apparentées
- Afficher l'entité ou les graphiques d'alerte associés afin de visualiser et explorer les points communs des entités ou attributs constituant l'alerte
- Ajouter des commentaires indiquant les conclusions de votre analyse
- Modifier l'état (disposition) de l'alerte au fur et à mesure des progrès de votre analyse

Alertes d'attribut

Les alertes d'attribut sont des alertes produites par les générateurs d'alertes d'attribut qui créent une requête système permanente à la recherche d'attributs ou d'identités spécifiques dans la base de données de l'entité. Chaque fois que des attributs d'entités correspondent aux critères du générateur d'alertes d'attribut, le système crée une alerte d'attribut.

Les utilisateurs du Visualizer créent leurs propres générateurs d'alertes d'attribut personnels. Si vous recherchez une identité spécifique ou n'importe quelle identité ou entité correspondant à un ensemble d'attributs spécifiques, vous pouvez créer votre propre générateur d'alertes d'attribut personnel qui recherche des correspondances jusqu'à une date d'expiration spécifiée.

Exemples d'attributs d'entité possibles dont il est souhaitable d'être informé :

- Nom et numéro unique (par exemple un numéro de carte de crédit)
- Nom et numéro de téléphone
- Adresse
- Nom et numéro non unique

Les générateurs d'alertes d'attribut sont configurés et consultables à l'aide du Visualizer . Vous êtes le seul à pouvoir accéder aux générateurs d'alertes d'attribut dont vous êtes l'auteur.

Exemple d'alerte d'attribut d'adresse

Vous surveillez l'adresse 675 Hickory Street Las Vegas, NV. Vous pouvez configurer un générateur d'alertes d'attribut afin qu'il crée une alerte d'attribut chaque fois

que cette adresse est associée à une fiche d'identité entrante qui est ajoutée à la base de données d'entités.

Alertes d'événements

Une alerte d'événement est déclenchée lorsqu'un ou plusieurs événements complexes remplissent des critères définis au cours d'un cycle de vie spécifié. Les alertes d'événement reposent sur des règles d'événement complexes et d'autres configurations incluses dans un fichier de règles d'événement (`cep.xml`). Ces alertes peuvent indiquer des situations présentant un intérêt, par exemple "Au moins deux achats de plus de 10000 dollars ont été effectués il y a une heure sur des sites situés à 200 miles l'un de l'autre".

Alertes de rôle

Une alerte de rôle identifie les situations où une ou deux entités, liées par une relation, répondent ou surpassent une règle d'alerte de rôle configurée. Les alertes de rôle se basent sur des rôles configurés et des règles d'alertes de rôle. Elles peuvent émettre un avertissement ou signaler un incident (par exemple, un client connaît un "paria") ou simplement une relation intéressante (par exemple, un client connaît un employé).

Définissez des relations *intéressantes* ou *conflictuelles* en configurant les règles d'alertes de rôle qui désignent quels rôles ne peuvent ni exister dans une seule entité, ni être liés à une seule ou plusieurs entités. Utilisez la Console de configuration pour configurer les filtres des alertes de rôle, qui déterminent si le système vous alerte de nouveau en cas de nouvelles informations (telles qu'une nouvelle identité ou un nouveau code de source de données).

Au cours de la résolution d'entité, le pipeline évalue les relations entre l'identité entrante et les entités de la liste de candidats. Une fois qu'il a établi l'existence d'une relation entre l'identité entrante et une entité candidate, le système évalue ensuite si les rôles attribués répondent ou pas à une règle d'alerte de rôle configurée. Dans l'affirmative, le système déclenche une alerte de rôle.

Une alerte de rôle identifie les données d'entité au moment où l'alerte a été créée. L'écran d'informations Alerte de rôle affiche les données de l'entité telles qu'elles se présentaient lors de la création de l'alerte de rôle. Au fil des modifications de ces données, le récapitulatif d'entité renferme les plus récentes données d'entité. Si vous souhaitez consulter les données actuelles d'une certaine entité, reportez-vous au récapitulatif.

Vous pouvez afficher les alertes de rôle et les manier dans les composants d'Analyst Toolkit (rapports Cognos, le plug-in Identity Insight pour i2, et Identity Insight Explorer).

Affichage des alertes

Vous affichez les alertes dans la fenêtre **Récapitulatif d'alerte** afin d'évaluer les alertes à analyser et à vous attribuer ou à transférer à un autre groupe d'analystes Visualizer. Vous pouvez ensuite commencer à rechercher et à disposer les alertes que vous vous êtes affecté.

Pourquoi et quand exécuter cette tâche

Les alertes qui s'affichent dans votre fenêtre **Récapitulatif d'alerte** comprennent les éléments suivants:

- Les alertes que vous vous êtes affectées à des fins d'analyse.
- Les alertes non affectées pour votre groupe d'analystes Visualizer

- Les alertes d'attribut générées par l'un de vos générateurs d'alerte d'attribut

Les récapitulatifs d'alerte non affectée sont filtrés selon les valeurs de filtre d'affichage d'alerte de la fenêtre **Récapitulatif d'alerte** qui sont configurées dans l'onglet **Préférences système** de la fenêtre **Configurer les préférences de l'écran**. Vous pouvez modifier une ou plusieurs valeurs du filtre d'affichage d'alerte dans la case du groupe **Filtres d'affichage**.

Procédure

1. Sélectionnez **Afficher** > **Récapitulatif d'alerte**.
2. Puis sélectionnez le type des alertes que vous souhaitez afficher ou sélectionnez **Afficher tous les types d'alerte**.

Résultats

Dans la fenêtre **Récapitulatif d'alerte**, vous pouvez décider des alertes avec lesquelles travailler. Vous pouvez attribuer des alertes à vous-même ou transférer des alertes à un autre groupe d'analystes Visualizer. Vous pouvez sélectionner les alertes que vous vous êtes affectées pour analyser et ajouter des commentaires sur votre analyse.

Filtrage de l'affichage des alertes dans la fenêtre Récapitulatif d'alerte

Pendant que vous passez en revue les alertes dans la fenêtre **Récapitulatif d'alerte**, vous pouvez filtrer l'affichage des récapitulatifs d'alerte en modifiant les valeurs de la zone de groupe **Filtres d'affichage**. Les filtres affectent uniquement les récapitulatifs d'alerte se trouvant actuellement à l'état "Non affecté".

Pourquoi et quand exécuter cette tâche

Les valeurs par défaut de ces filtres d'alerte sont configurées dans l'onglet **Préférences système** de la fenêtre **Configurer les préférences d'écran**. Lorsque vous modifiez les filtres d'affichage des alertes dans la fenêtre **Récapitulatif d'alerte**, vous écrasez temporairement ces valeurs par défaut. La prochaine fois que vous ouvrirez une nouvelle fenêtre **Récapitulatif d'alerte**, les filtres reviennent à leurs valeurs par défaut.

Procédure

1. Dans la fenêtre **Récapitulatif d'alerte**, ouvrez la zone de groupe **Filtres d'affichage**.
2. Effectuez vos modifications sur un ou plusieurs des filtres d'affichage d'alerte.
3. Cliquez sur**Appliquer** pour rafraîchir la fenêtre **Récapitulatif d'alerte** et appliquer les filtres d'alerte que vous avez spécifiés.

Affectation d'alertes à soi-même

En affectant une alerte à vous-même, vous assumez la responsabilité d'examiner, rechercher et de la disposition de cette alerte. Une fois que vous vous êtes affecté une alerte à vous-même, celle-ci ne s'affiche que dans votre fenêtre **Récapitulatif d'alerte**, vous permettant d'identifier plus facilement vos alertes.

Procédure

1. Dans le Visualizer, dans la fenêtre **Récapitulatif d'alerte**, dans le tableau **Récapitulatif d'alerte**, cliquez sur un récapitulatif d'alerte non affecté. Le

récapitulatif d'alerte contient une ou plusieurs alertes regroupées par type d'alerte, et qui partagent la même description, état, règle de résolution, score de ressemblance, et score de relation.

2. Dans le tableau **Liste d'alertes**, cliquez deux fois sur l'alerte à vous affecter à vous-même.
3. Dans la fenêtre **Rechercher**, cliquez sur **Définir l'état**.
4. Dans **Définir l'état**, procédez comme suit :
   a. Dans **Sélectionnez l'action que vous voulez effectuer**, sélectionnez **Définir l'état**. Un code d'activité correspondant s'affiche dans **Sélectionner un code d'activité**.
   b. Obligatoire : Dans **Sélectionner l'état**, sélectionnez **affecté**. Si vous sélectionnez un autre état, l'alerte ne vous est pas affectée.
   c. Facultatif : Pour affecter un autre code d'activité, sélectionnez-le dans **Sélectionner un code d'activité**. Si vous ne voyez pas le code d'activité que vous souhaitez sélectionner, contactez votre administrateur système pour organiser la configuration du code d'activité.
   d. Saisissez des commentaires ou notes dans la zone de texte **Commentaires**. Vous pouvez par exemple choisir de saisir des commentaires sur la raison de la modification de l'état, ou inclure des notes sur votre analyse de cette alerte.
   e. Cliquez sur **OK** pour enregistrer vos modifications.

Résultats

L'alerte illustre maintenant l'état affecté et s'affichera uniquement sur votre fenêtre **Récapitulatif d'alerte**, dès que vous aurez rafraîchi l'affichage de la fenêtre. Après avoir rafraîchi l'affichage de leur fenêtre **Récapitulatif d'alerte**, les autres analystes de votre groupe d'analystes Visualizer ne verront plus cette alerte.

Affectation d'alertes à d'autres groupes d'analystes

Si vous estimez qu'une alerte doit être affectée à un autre groupe d'analystes Visualizer, vous pouvez transférer cette alerte. Vous ne pouvez pas transférer une alerte à un utilisateur Visualizer spécifique, mais vous pouvez la transférer au groupe d'analystes Visualizer auquel appartient cet utilisateur.

Procédure

1. Dans le Visualizer, dans la fenêtre **Récapitulatif d'alerte**, dans le tableau **Récapitulatif d'alerte**, cliquez sur le récapitulatif d'alerte auquel l'alerte est associée.
2. Dans le tableau **Liste d'alertes**, cliquez deux fois sur l'alerte à transférer.
3. Dans la fenêtre **Rechercher**, cliquez sur **Définir l'état**.
4. Dans **Définir l'état**, procédez comme suit :
   a. Dans **Sélectionnez l'action que vous voulez effectuer**, sélectionnez **Transférer l'alerte**.
   b. Dans **Transférer l'alerte à**, sélectionnez le groupe d'analystes Visualizer auquel transférer l'alerte. Si vous ne voyez pas le groupe d'analystes Visualizer que vous voulez sélectionner, contactez votre administrateur système pour organiser la configuration du groupe d'analystes. Un code d'activité correspondant s'affiche dans **Sélectionner un code d'activité**.
   c. Facultatif : Pour affecter un autre code d'activité, sélectionnez-le dans **Sélectionner un code d'activité**. Si vous ne voyez pas le code d'état de

l'activité que vous souhaitez sélectionner, contactez votre administrateur système pour organiser la configuration du code d'activité.

d. Saisissez des commentaires ou notes dans la zone de texte **Commentaires**. Vous pouvez par exemple choisir de saisir des commentaires sur la raison de votre transfert de cette alerte.

e. Cliquez sur **OK** pour effectuer le transfert.

Résultats

L'alerte est maintenant transférée au groupe d'analystes Visualizer sélectionné et s'affiche dans les fenêtres **Récapitulatif d'alerte** des analystes de ce groupe d'analystes Visualizer. (Les analystes de ce groupe peuvent devoir d'abord rafraîchir l'affichage de leur fenêtre **Récapitulatif d'alerte**). Cette alerte ne s'affiche plus dans la fenêtre **Récapitulatif d'alerte** des analystes de votre groupe d'analystes Visualizer, ni dans la votre, dès lors que vous aurez rafraîchi l'affichage de la fenêtre **Récapitulatif d'alerte**.

Modification de l'état d'une alerte

Alors que vous analysez les alertes affectées à vous même ou à votre groupe d'analystes Visualizer, vous pouvez utiliser le Visualizer pour effectuer un suivi de votre recherche, des commentaires et sur le mode de disposition de l'alerte.

Pourquoi et quand exécuter cette tâche

Vous pouvez à tout moment mettre à jour l'état de l'alerte des alertes affectées à vous-même ou à votre groupe d'analystes Visualizer. Vous pouvez également ajouter à tout moment des commentaires à ces alertes. Vous ne pouvez cependant pas éditer les commentaires existants.

Procédure

1. Dans le Visualizer, dans la fenêtre **Récapitulatif d'alerte**, dans le tableau **Récapitulatif d'alerte**, cliquez sur le récapitulatif d'alerte contenant l'alerte à mettre à jour.
2. Dans la **Liste d'alertes**, cliquez deux fois sur l'alerte dont l'état doit être modifié.
3. Dans la fenêtre **Rechercher**, cliquez sur **Définir l'état**.
4. Dans **Définir l'état**, procédez comme suit :
   a. Dans **Sélectionnez l'action que vous voulez effectuer**, sélectionnez **Définir l'état**. Un code d'activité correspondant s'affiche dans **Sélectionner un code d'activité**.
   b. Facultatif : Pour affecter un autre code d'activité, sélectionnez-le dans **Sélectionner un code d'activité**. Si vous ne voyez pas le code d'état de l'activité que vous souhaitez sélectionner, contactez votre administrateur système pour organiser la configuration du code d'activité.
   c. Saisissez des commentaires ou notes dans **Commentaires**. Vous pouvez par exemple saisir des commentaires sur la raison de la modification de l'état, ou inclure des notes sur votre analyse de cette alerte.
   d. Cliquez sur **OK** pour enregistrer vos modifications.

Résultats

L'alerte reflète maintenant le nouvel état dans la fenêtre **Récapitulatif d'alerte**.

La mise à jour la plus récente d'un état ou d'un commentaire pour une alerte d'attribut s'affiche en haut de la section **Récapitulatif d'état**.

Si la modification de l'état impliquait l'affectation de l'alerte d'attribut à vous même, cette alerte d'attribut s'affichera désormais uniquement dans votre fenêtre **Récapitulatif d'alerte**, dès que vous aurez rafraîchi l'affichage. Les autres analystes de votre groupe d'analystes Visualizer ne verront plus cette alerte dans leur fenêtre **Récapitulatif d'alerte**, lorsqu'ils auront rafraîchi leur affichage.

Rubriques d'aide

Fenêtre récapitulatif d'alerte :

Utilisez cette fenêtre pour afficher les récapitulatifs d'alertes non affectées de votre groupe d'analystes Visualizer ou les alertes que vous vous êtes affectées.

Utilisez les commandes pour développer ou réduire les sections de l'écran afin de vous aider à vous concentrer sur un détail spécifique.

Afficher les alertes par type
Sélectionnez un type d'alerte à afficher ou affichez tous les types d'alerte.

Zone de groupe Afficher les filtres
Les modifications aux paramètres de filtre par défaut qui déterminent les récapitulatifs d'alerte qui s'affichent dans votre fenêtre **Récapitulatif d'alerte**. Ces filtres modifient uniquement l'affichage des récapitulatifs d'alerte actuellement non affectées et représentent uniquement une modification temporaire. Si vous fermez la fenêtre **Récapitulatif d'alerte** et que vous la réouvrez plus tard, ces paramètres reviennent aux paramètres de filtre par défaut.

Les paramètres par défaut sont des paramètres de filtre d'alerte configurés pour votre poste de travail. (Vous pouvez modifier les paramètres par défaut dans l'onglet **Préférences système** de la fenêtre **Configurer les préférences de l'écran**.)

Tableau des Récapitulatifs d'alerte
Les alertes qui partagent le même type d'alerte, la même description, gravité, état, règle de résolution, score de ressemblance, et score de relation, sont regroupées en récapitulatifs d'alerte. La colonne **Décompte** indique combien d'alertes individuelles sont regroupées dans le récapitulatif.

Vous pouvez trier le tableau en cliquant sur un en-tête de colonne de celui-ci. Le premier clic trie les valeurs de la colonne dans l'ordre croissant. Le deuxième clic trie les valeurs de la colonne dans l'ordre décroissant.

Par défaut, le tableau est trié par type d'alerte.

Type Type d'alerte représenté par le récapitulatif d'alerte.

Description
Description des alertes de ce récapitulatif.

Pour les alertes d'attribut, cette description est le numéro de dossier. Pour les alertes d'événement, cette description correspond à la description de la situation de l'événement. Pour les alertes de rôle, cette description est celle de la règle d'alerte de rôle.

Etat Etat d'activité actuel des alertes de ce récapitulatif.

Règle de résolution
Nom de la règle de résolution utilisée pour relier les entités des alertes de ce récapitulatif d'alerte.

Score de ressemblance
Score (compris entre 0 et 100) qui indique la probabilité que les identités apparentées représentent la même entité.

Score de relation
Score (compris entre 0 et 100) qui indique à quel degré les identités concernées par l'alerte sont apparentées.

Nombre
Nombre d'alertes individuelles regroupées dans ce récapitulatif d'alerte et qui satisfont les critères de la zone de groupe **Afficher les filtres** actuellement sélectionnés.

Tableau de la Liste d'alertes
Dès que vous avez sélectionné un récapitulatif d'alerte dans le tableau **Récapitulatif d'alerte**, les alertes individuelles qui font partie de ce récapitulatif s'affichent dans cette section. Le nombre d'alertes (lignes) qui s'affichent dépend du nombre total d'alertes dans le récapitulatif (ce nombre est indiqué dans la colonne **Décompte** du tableau du Récapitulatif d'alerte), et du nombre dans la zone **Maximum de lignes dans la liste des alertes** dans la zone de groupe **Afficher les filtres**. Un décompte de liste dans la barre de titre du tableau **Liste des alertes** indique comment le nombre des alertes actuellement affichées s'intègre dans le nombre total des alertes de ce récapitulatif.

Triez le tableau en cliquant sur un en-tête de colonne de celui-ci. Le premier clic trie les valeurs de la colonne dans l'ordre croissant. Le deuxième clic trie les valeurs de la colonne dans l'ordre décroissant.

Les zones qui s'affichent sont basées sur le type de récapitulatif d'alerte sélectionné.

Ecran Alerte d'attribut :

Utilisez cet écran pour définir ou modifier l'état d'analyse d'une alerte d'attribut et examiner les détails qui composent l'alerte.

Utilisez les commandes pour développer ou réduire les sections de l'écran afin de vous aider à vous concentrer sur un détail spécifique.

Etat récapitulatif
Effectue une synthèse de l'état d'analyse et de la disposition en cours de l'alerte.

Récapitulatif d'alerte
Donne la description de l'alerte ainsi que la date et l'heure auxquelles l'alerte a été générée.

Section Mise en concordance avec l'entité
Contient des détails sur les attributs mis en concordance entre les critères de recherche de votre générateur d'alerte d'attribut et les entités existantes dans la base de données d'entités. Cliquez sur un attribut spécifique pour mettre en surbrillance les informations concordantes des identités dans l'entité concordante.

Détails du générateur d'alerte d'attribut
Récapitule les critères du générateur d'alerte d'attribut qui a généré cette alerte d'attribut. Cliquez sur la source de données pour mettre tous les critères en surbrillance.

Section Entité
Affiche les informations sur l'entité qui a concordé avec les critères du générateur d'alerte d'attribut. Cliquez sur la source de données pour mettre en surbrillance les données qui sont apparues sur une fiche d'identité provenant de cette source de données.

Bouton Récapitulatif d'entité
Cliquez ici pour afficher le récapitulatif d'entité de l'entité qui a concordé. Pour approfondir votre analyse de cette alerte, vous pouvez vouloir consulter les autres identités associées à l'entité.

Ecran Alerte d'événement :

Utilisez l'écran **Alerte d'événement** pour définir ou modifier l'état d'analyse et passer en revue les détails d'une alerte d'événement. Les alertes d'événement ne s'affichent que si le Gestionnaire d'événements est activé pour votre système, si les codes d'activité des alertes d'événement sont configurés et s'il existe au moins une alerte d'événement.

Utilisez les commandes pour développer ou réduire les sections de l'écran afin de vous aider à vous concentrer sur un détail spécifique.

Etat récapitulatif
Effectue une synthèse de l'état d'analyse et de la disposition en cours de l'alerte d'événement.

Récapitulatif d'alerte
Donne la description de l'alerte d'événement ainsi que la date et l'heure auxquelles l'alerte a été générée.

Section Alerte d'événement
Donne les détails de l'événement qui composent cette alerte d'événement.

Section Entité
Donne une brève synthèse pour chaque entité impliquée dans cette alerte d'événement.

Bouton Rapport
Cliquez pour créer un rapport **Détail d'alerte d'événement**.

Ecran Alerte de rôle :

Utilisez cet écran pour afficher les détails d'une alerte de rôle et définir ou modifier l'état d'analyse de l'alerte de rôle.

Cliquez sur les commandes pour développer ou réduire les sections de l'écran afin de vous aider à vous concentrer sur un détail spécifique.

Degrees of Separation
Indique le nombre de degrés de séparation entre les entités dans cette alerte de rôle.

Etat récapitulatif
Effectue une synthèse de l'état d'analyse et de la disposition en cours de l'alerte.

Récapitulatif d'alerte
Fournit une description du récapitulatif d'alerte, du code de gravité de l'alerte, de la règle de résolution utilisée pour faire correspondre des entités au sein de l'alerte, le score de résolution qui indique le niveau de ressemblance entre les deux entités, et le score de relation qui indique la probabilité que ces deux entités se connaissent.

Onglets Détails de la concordance
Contient des détails sur les attributs mis en concordance entre les deux entités. Cliquez sur un attribut spécifique pour mettre en surbrillance les informations correspondantes provenant des identités dans l'entité correspondante.

Contient des détails sur les attributs mis en concordance entre les critères de recherche de votre générateur d'alerte d'attribut et les entités existantes dans la base de données d'entités.

Bouton Rapport
Cliquez pour créer un rapport **Détail d'alerte de rôle** pour cette alerte de rôle.

Bouton Récapitulatif d'entité
Cliquez pour afficher le récapitulatif d'entité de l'entité sélectionnée. Pour approfondir votre analyse de cette alerte, vous pouvez vouloir consulter les autres identités associées à l'entité.

Ecran Evénements d'entité :

Utilisez l'écran **Evénements d'entité** pour examiner les événements d'une entité qui se sont produits pendant un intervalle de dates spécifique. Vous accédez initialement à cet écran en cliquant sur **Afficher les événements** dans l'écran **Récapitulatif d'entité**.

Section Récapitulatif d'événement
Affiche un récapitulatif de tous les événements de cette entité avec l'intervalle de date indiqué. Par défaut, l'écran affiche tous les événements associés à l'entité, depuis la date du premier événement jusqu'à la date en cours. Modifiez l'intervalle de dates à l'aide du filtre dates de l'événement pour voir les événements d'un autre intervalle de dates.

Filtre de dates d'événement à l'écran
Filtre les événements affichés par l'intervalle de dates spécifié lorsque vous cliquez sur **Mettre à jour l'affichage**.

Date de début
Saisissez une date ou cliquez sur la commande du calendrier pour sélectionner la date de début dans l'intervalle de dates.

Si vous choisissez de saisir une date, utilisez l'un des formats de date suivants :

- `MM/jj/aaaa`, `MM-jj-aaaa`, `MM.jj.aaaa`, ou `MMjjaaaa`
- `aaaa/MM/jj`, `aaaa-MM-jj`, ou`aaaa.MM.jj`
- `janvier 3, 2008` ou `janvier 03, 2008`
- `Janvier 3, 08` ou `janvier 03, 08`
- `Jan 03, 2008` ou `Jan 3, 2008`
- `Jan 3, 08` ou `Jan 03, 08`

La zone est définie par défaut sur la première instance de date d'événement.

Date de fin
Saisissez une date ou cliquez sur la commande du calendrier pour sélectionner la date de fin dans l'intervalle de dates.

Si vous choisissez de saisir une date, utilisez l'un des formats de date suivants :

- `MM/jj/aaaa`, `MM-jj-aaaa`, `MM.jj.aaaa`, ou `MMjjaaaa`
- `aaaa/MM/jj`, `aaaa-MM-jj`, ou`aaaaa.MM.jj`
- `janvier 3, 2008` ou `janvier 03, 2008`
- `Janvier 3, 08` ou `janvier 03, 08`
- `Jan 03, 2008` ou `Jan 3, 2008`
- `Jan 3, 08` ou `Jan 03, 08`

La zone est définie par défaut sur date actuelle.

Bouton Mettre à jour l'affichage
Cliquez pour afficher les événements de cette entité dans l'intervalle de dates spécifié. Ce bouton est désactivé jusqu'à ce que vous modifiiez les dates par défaut dans les zones de date.

Bouton Rapport
Cliquez pour générer un rapport **Tous les événements** pour cette entité.

Affichage à l'écran
Cette section de l'écran récapitule les événements de cette entité pour le type d'événement dans l'intervalle de dates spécifié.

Type d'événement
Décrit le type d'événement.

Nombre
Indique le nombre total d'événements de cette entité par type d'événement, dans l'intervalle de dates spécifié. (Par exemple, si le décompte est de 4, quatre événements du même type se sont produits pour cette entité dans l'intervalle de dates spécifié.)

Valeur Indique la valeur totale des événements de cette entité par type d'événement, dans l'intervalle de dates spécifié. (Par exemple, s'il y a quatre événements, ce nombre correspond à la somme totale de la valeur pour ces quatre événements.)

Quantité
Indique le nombre total d'unités pour les événements de cette entité par type d'événement, dans l'intervalle de dates spécifié.

Unité de mesure
Décrit l'unité de mesure associée à la valeur de l'événement. L'unité de mesure est configurée par type d'événement dans la Console de configuration.

Décompte total
Indique le nombre qui représente le nombre total de tous les événements de cette entité, dans l'intervalle de dates spécifié.

Valeur totale
Indique le nombre qui représente la valeur totale de tous les événements de cette entité, dans l'intervalle de dates spécifié.

Section Détails d'événement
Sélectionnez une ligne d'événement dans la section Récapitulatif d'événement, afin de voir plus de détails sur chaque événement inclus dans ce récapitulatif de type d'événement. Si vous double-cliquez sur une ligne d'événement dans cette section, l'écran **Détails d'événement** s'affiche pour montrer des informations encore plus détaillées sur l'événement sélectionné.

Date Indique la date et l'heure de l'événement.

Source de données - Description
Décrit la source de données associée à l'événement.

ID externe
Affiche la clé unique qui identifie la fiche entrante dans la source de données d'origine de cet événement.

Référence d'événement
Fournit des informations supplémentaires sur l'événement dans la source de données d'origine, si ces informations font partie de la fiche entrante.

Valeur Affiche le montant en valeur de l'événement.

Quantité
Affiche le nombre d'unités de l'événement.

Mémo ou *Etiquette personnalisée*
Affiche des informations supplémentaires sur l'événement, telles que des notes ou commentaires, qui peuvent fournir davantage de contexte pour la transaction d'événement.

Les utilisateurs peuvent définir une étiquette personnalisée pour cette colonne, ce qui est une des options possibles lors de la configuration d'un type d'événement dans la Console de configuration. Au lieu du **Mémo**, vous pouvez souhaiter une étiquette personnalisée plus descriptive (comme par exemple,**Notes sur le virement**.

Recherche d'entités

Pour rechercher une entité dans la base de données d'entités, plusieurs méthodes de Recherche par sont à votre disposition. Si vous souhaitez être informé chaque fois que le système traite une fiche contenant un nom, une adresse, un numéro ou une adresse électronique spécifique, créez un générateur d'alerte d'attribut afin de "rechercher" automatiquement les entités.

Rechercher des entités par attribut

Lorsque vous utilisez le Visualizer, et que vous souhaitez rechercher une entité dans la base de données d'entités, vous pouvez rechercher l'entité en saisissant les critères sur les attributs associés à l'entité. Vous indiquez les critères d'attribut, et le

Visualizer crée une requête basée sur ces critères. Ce type de requête d'entité ne passe pas par le processus de résolution d'entité pour renvoyer les résultats de recherche.

Procédure

1. Dans Visualizer, effectuez l'une des opérations suivantes :
   a. Cliquez sur **Afficher** > **Rechercher par** > **Attributs**.
   b. Dans la barre d'outils, cliquez sur l'icône (Rechercher).
   c. Dans la barre d'outils, cliquez sur la flèche et sélectionnez **Attribut**.
   d. Dans la fenêtre **Rechercher par**, sélectionnez **Attribut** dans la liste déroulante **Rechercher par**.
2. Saisissez les critères pour chaque type d'attribut que vous voulez utiliser pour trouver des entités.
   a. Cliquez sur **+** pour ajouter une ligne afin de spécifier les critères pour un autre type d'attribut.
   b. Cliquez sur **-** pour supprimer l'entrée de critères de requête sélectionnée.
3. Facultatif : Cliquez sur **Afficher le récapitulatif** pour consulter un récapitulatif de la requête Rechercher par attribut. Le récapitulatif est un moyen utile de s'assurer que la requête contient les valeurs que vous souhaitez. Si tel n'est pas le cas, fermez le récapitulatif et corrigez les critères de requête.

   Deux critères de requête du même type d'attribut constituent une clause "OR". Tous les autres critères de requête se combinent sous forme de clauses "AND".

   L'ordre des critères de type d'attribut n'affecte pas les résultats.
4. Cliquez sur **Rechercher**.

Résultats

Les entités correspondant aux critères de requête s'affichent dans la fenêtre **Résultats**.

Par défaut, les résultats affichés pour les Recherches par attribut sont limités aux 1 000 premières entités concordantes. S'il existe plus de 1 000 concordances, cette information est signalée dans la fenêtre **Résultats**. (Le nombre de résultats affichés peut être configuré par votre administrateur système dans la Console de configuration, en définissant le paramètre MAX_ENTITIES_RETURNED dans les paramètres système.)

Remarque : Si votre système utilise une application de standardisation d'adresse supplémentaire, les adresses utilisant des caractères spéciaux peuvent faire l'objet d'une translittération. Par exemple, le résultat de recherche d'une adresse en Allemagne contenant un ou plusieurs umlauts dans l'adresse peut renvoyer un résultat ne contenant pas les umlauts correspondants.

Que faire ensuite

Cliquez sur une entité pour afficher le récapitulatif d'entité de l'entité sélectionnée.

Recherche d'entités par compte de source de données

Lorsque vous connaissez le numéro de compte (ou ID externe) d'une identité, et que vous souhaitez rechercher l'entité qui contient cette identité, utilisez la méthode de Recherche par compte de source de données dans le Visualizer. Vous pouvez également rechercher une entité que vous avez ajoutée via l'écran **Ajouter une entité**.

Avant de commencer

Vous devez connaître la description de la source de données ainsi que l'ID externe de l'identité (ou compte). Si vous essayez de rechercher une entité par le nom, essayez plutôt la méthode de Recherche par attribut.

Procédure

1. Dans Visualizer, effectuez l'une des opérations suivantes :
   a. Cliquez sur **Afficher** > **Rechercher par** > **Compte de source de données**.
   b. Dans la barre d'outils, cliquez sur la flèche et sélectionnez **Compte de source de données**.
   c. Dans la fenêtre **Rechercher par**, sélectionnez **Compte de source de données** dans la liste déroulante **Rechercher par**.
2. Dans **Saisir l'ID externe**, saisissez le numéro de compte de l'identité. Le compte est la manière dont l'identité est connues dans la source de données d'origine.
3. Dans **Source de données**, sélectionnez le code de source de données ainsi que la description.
4. Cliquez sur **Rechercher**.

Résultats

Si le système recherche une entité contenant une identité avec les critères d'ID externe et de source de données spécifiés, le Visualizer affiche le **Récapitulatif d'entité** de cette entité.

Recherche d'entités par ID d'entité

Lorsque vous connaissez le numéro d'ID d'entité d'une entité, utilisez la méthode de Recherche par ID d'entité du Visualizer pour localiser rapidement l'entité et afficher tout le récapitulatif de cette entité.

Avant de commencer

Vous devez connaître le numéro d'ID d'entité de l'entité que vous souhaitez rechercher. Si vous essayez de rechercher une entité par le nom, utilisez plutôt la méthode Rechercher par attribut.

Procédure

1. Dans Visualizer, effectuez l'une des opérations suivantes :
   a. Cliquez sur **Afficher** > **Rechercher par** > **ID d'entité**.
   b. Dans la barre d'outils, cliquez sur la flèche et sélectionnez **ID d'entité**.
   c. Dans la fenêtre **Rechercher par**, sélectionnez **ID d'entité** dans la liste déroulante **Rechercher par**.
2. Dans **Saisir un ID d'entité**, saisissez le numéro d'ID d'entité de l'entité à rechercher.
3. Cliquez sur **Rechercher**.

Résultats

Si le numéro d'ID d'entité correspond à une entité dans la base de données d'entités, le Visualizer affiche le récapitulatif d'entité de cette entité.

Rechercher des entités par résolution

Utilisez la Recherche par résolution pour créer une entité de recherche qui suit le processus de résolution d'entité pour voir si des identités de la base de données d'entités satisfont les critères de la requête.

Avant de commencer

La fonction Rechercher par résolution nécessite un pipeline actif disponible pour communiquer avec le serveur Visualizer. Le pipeline est le composant dans lequel se produit la résolution d'entité et de relation.

Pourquoi et quand exécuter cette tâche

Pour tirer le meilleur parti de la fonction Rechercher par résolution, il est essentiel de comprendre le fonctionnement de la résolution d'entité ainsi que sa configuration pour votre système, car la résolution d'entité est utilisée pour rechercher les résultats. Par exemple, si la résolution d'entité n'est pas configurée pour ne trouver les concordances que selon une valeur de nom, la Recherche par résolution ne renvoie aucun résultat si une recherche ne porte que sur une valeur de nom. De même, dans la mesure où la résolution d'entité ne résout pas les entités basées uniquement sur un code postal, spécifier uniquement un code postal ne renvoie pas de résultat.

La Recherche par résolution utilise les valeurs de score minimum définies dans l'onglet **Préférences système** dans le menu **Fichier**.

Procédure

1. Dans Visualizer, effectuez l'une des opérations suivantes :
   a. Cliquez sur **Afficher** > **Rechercher par** > **Résolution**.
   b. Dans la barre d'outils, cliquez sur la flèche et sélectionnez **Résolution**.
   c. Dans la fenêtre **Rechercher par**, sélectionnez **Résolution** dans la liste déroulante **Rechercher par**.
2. Saisissez autant d'attributs que vous connaissez sur l'identité.
   - Si vous saisissez quelque chose dans la section **Nom**, alors le **Nom (de famille)** est obligatoire.
   - Si vous saisissez des informations dans la section **Liste d'adresses**, l'**Adresse** est obligatoire.
   - Si vous sélectionnez un **Type** dans la section **Liste de numéros**, vous devez saisir une valeur de numéro dans la zone **Valeur**. (L'**Emplacement** est facultatif.)
   - Si vous sélectionnez un **Type** dans la section **Liste de caractéristiques**, vous devez saisir une valeur de caractéristique dans la zone **Valeur**.
   - Si vous sélectionnez un **Type** dans la section **Liste d'adresses électroniques**, vous devez saisir une valeur d'adresse électronique dans la zone **Adresse**.
3. Cliquez sur **Rechercher**.

Recherche d'entités via les générateurs d'alerte d'attribut

Lorsque vous avez une entité que vous surveillez, vous pouvez créer des générateurs d'alerte d'attribut avec les critères pour cette entité. Chaque fois que des fiches d'identité ou entités contiennent des attributs qui correspondent aux critères, le système génère une alerte d'attribut. Chaque utilisateur Visualizer crée et gère des générateurs d'alerte d'attribut personnels pour une période spécifique.

Dans la mesure où les générateurs d'alerte d'attribut sont transmis via le pipeline, le processus de résolution d'entité s'effectue sur ces demandes de recherche de la même manière que pour les données d'entité entrantes :

- Les noms et adresses sont standardisés
- Les recherches et comparaisons partielles ou floues sont effectuées afin que les entités applicables soient identifiées dans les alertes d'attribut ultérieures

Pour tirer le meilleur parti des générateurs d'alerte d'attribut, il est essentiel de comprendre le fonctionnement de la résolution d'entité ainsi que sa configuration pour votre système, car la résolution d'entité est utilisée pour rechercher vos résultats d'alerte d'attribut. Ainsi, si une résolution d'entité n'est pas configurée pour rechercher des concordances basées uniquement sur un nom, un générateur d'alerte d'attribut, configuré pour rechercher uniquement une valeur de nom ne renvoie aucun résultat. De même, dans la mesure où la résolution d'entité ne résout pas les entités basées uniquement sur un code postal, un générateur d'alerte d'attribut spécifiant uniquement un code postal ne renvoie pas de résultat.

Quand vous créez un générateur d'alerte d'attribut, respectez les consignes suivantes :

- Utilisez le **Score minimum** pour filtrer les résultats de l'alerte d'attribut. La valeur par défaut de ce champ est N'importe quelle relation. Il s'agit de l'option qui donne le plus de résultats. Choisissez un niveau plus élevé pour autoriser moins de résultats. Ces valeurs sont configurées dans les préférences système de Visualizer disponibles dans le menu **Fichier**.
- Pour les noms : Renseignez une combinaison de nom et prénom ou une combinaison de nom et deuxième prénom. Les générateurs d'alerte d'attribut n'indiquant qu'un nom, un prénom ou un deuxième prénom ne renvoient aucun résultat.
- Pour les adresses : vous devez au moins indiquer une adresse et un code postal. Les générateurs d'alerte d'attribut n'indiquant qu'une localité, un code postal, une adresse ou un pays ne renvoient aucun résultat.

Créer des générateurs d'alerte d'attribut :

Pour recevoir une alerte lorsqu'une valeur d'attribut ou une combinaison de valeurs d'attribut spécifique est traitée par le système, créez un générateur d'alerte d'attribut. Les générateurs d'alertes d'attribut continuent à générer des alertes jusqu'à la date d'expiration spécifiée.

Procédure

1. Dans Visualizer, effectuez l'une des opérations suivantes :
   a. Sélectionnez **Afficher** > **Gestionnaire du générateur d'alerte d'attribut**.
   b. Dans la barre d'outils, cliquez sur l'icône (Gestionnaire du générateur d'alerte d'attribut).
2. Dans la fenêtre **Gestionnaire du générateur d'alerte d'attribut**, cliquez sur **Créer**.
3. Utilisez les listes déroulantes et les zones pour saisir les critères spécifiques de votre nouvelle alerte d'attribut, y compris une date d'expiration. La date d'expiration par défaut est réglée sur six mois à compter de la date du jour.
4. Cliquez sur **Créer**.

Résultats

Dès que des données correspondant aux critères que vous avez spécifiées sont traitées via la résolution d'entité, une nouvelle alerte d'attribut s'affiche dans votre fenêtre **Récapitulatif des alertes**. Si les informations que vous recherchez sont actuellement dans la base de données d'entités, vous voyez une nouvelle alerte d'attribut dans la fenêtre **Récapitulatif des alertes**.

Edition des générateurs d'alerte d'attribut :

Editez un générateur actif d'alerte d'attribut lorsque vous voulez modifier le numéro de dossier, les commentaires ou la date d'expiration.

Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas modifier les attributs ou le score de résolution minimum de ces attributs. Si c'est ce que vous souhaitez faire, créez un générateur d'alerte d'attribut. Et si le nouveau générateur d'alerte d'attribut en remplace un autre, effectuez les opérations suivantes pour mettre fin au générateur d'alerte d'attribut dont vous n'avez plus besoin.

Procédure

1. Dans Visualizer, effectuez l'une des opérations suivantes :
   a. Cliquez sur **Afficher** > **Gestionnaire du générateur d'alerte d'attribut**.
   b. Dans la barre d'outils, cliquez sur (Gestionnaire du générateur d'alerte d'attribut).
2. Sélectionnez le générateur d'alerte d'attribut à éditer et cliquez sur **Créer**.
3. Dans la fenêtre **Informations sur le générateur d'alerte d'attribut**, effectuez vos modifications.
   - Vous pouvez modifier la date d'expiration, y compris définir la date à une date d'expiration antérieure pour le générateur d'alerte d'attribut.
   - Vous pouvez également mettre à jour le numéro de dossier et les commentaires.
   - Vous ne pouvez pas modifier le code raison, les attributs que vous avez sélectionnés pour le générateur d'alerte d'attribut, ni le score de résolution minimum.
4. Cliquez sur **Mettre à jour**.

Résultats

Le système consigne les modifications que vous avez effectuées sur le générateur d'alerte d'attribut. Affichez ou imprimez un rapport **Historique du générateur d'alerte d'attribut** pour voir toutes les modifications apportées à vos générateurs d'alerte d'attribut.

Rubriques d'aide :

Ecran Recherche par attribut :

Utilisez cette fenêtre pour créer une requête pour rechercher des entités dans la base de données d'entités par attribut – nom, adresse, numéros, caractéristiques, etc. Ce type de requête n'utilise généralement pas le processus de résolution d'entité pour renvoyer des résultats de requête.

Type d'attribut
Saisissez l'attribut d'entité que vous devez utiliser comme critère de la requête : nom, adresse, numéros, caractéristiques, adresses électroniques, source de données, ou date de chargement de fichier. Lorsque vous sélectionnez un type d'attribut, la fenêtre affiche les zones de critère de recherche correspondant à ce type.

L'instruction de requête que vous créez dépend des types d'attribut sélectionnés sur lesquels vous effectuez la requête :

- Dans une requête simple, les critères pour plusieurs mêmes types d'attribut créent une instruction de requête "OR". Par exemple "Bob Hayes" OR "Rob Hays".
- Dans une requête simple, les critères pour plusieurs types d'attribut créent une instruction de requête "AND". Par exemple "Bob Hayes" AND " le numéro de carte de crédit 5252-1010-5252-1010".

A l'aide de cet exemple, si vous avez saisi les deux noms suivants et une carte de crédit, l'instruction de requête ressemble à l'instruction suivante : Bob Hayes" OR "Rob Hays AND numéro de carte de crédit "5252-1010-5252-1010".

Utilisez le bouton **Afficher le récapitulatif** pour voir l'instruction de requête complète.

Zones de valeur
Saisissez les valeurs spécifiques du type d'attribut à utiliser pour rechercher les entités. Chaque type d'attribut possède son propre ensemble de zones de valeur. Si vous laissez les zones de valeur vides, le requête recherche toutes les valeurs potentielles. Cependant, lorsque vous saisissez des données dans toutes les zones de valeur, la requête s'exécute plus rapidement, et renvoie de meilleurs résultats.

- Les critères de nom sont obligatoires.
- Si vous saisissez des informations dans une zone de critère d'adresse ou d'adresse électronique, toutes les zones d'adresse sont obligatoires.
- Si vous sélectionnez un type de Nom ou de Caractéristique, la zone **Valeur** est obligatoire.

Bouton +
Ajoute une nouvelle ligne d'attribut aux critères.

Bouton -
Supprime la ligne d'attribut sélectionnée et l'entrée des critères.

Volet Recherche par attribut - Résultats
Contient les résultats de la requête Recherche par attribut, en fonction des entrées de critères. Par défaut, la zone d'affichage ne contient que les 1000 premières fiches correspondant aux critères de recherche. Toutefois, cette option peut être définie par l'administrateur système.

Les résultats s'affichent par entité et représentent les informations les plus récentes concernant chaque entité. Si vous cliquez deux fois sur une entité dans le volet de résultats, Visualizer ouvre le Récapitulatif d'entité correspondant.

ID de l'entité
Affiche l'ID de l'entité correspondant aux critères de recherche.

Nom (*décompte*)
Affiche le meilleur nom de l'entité qui correspond aux critères de recherche, et un numéro qui représente le nombre de noms associés

à cette entité. Par exemple, Bob M. Smith (4) indique qu'il y a quatre noms associés à cette entité, Bob Smith.

Adresse (*décompte*)
Affiche la meilleure adresse de l'entité qui correspond aux critères de recherche, et un numéro qui représente le nombre d'adresses associées à cette entité. Par exemple, 1024 Daisy Lane, Akron, OH 43596 (24) indique que 24 adresses sont associées à cette entité.

Type de numéro : *valeur*
Affiche les meilleurs types de numéro et valeurs de numéro de l'entité correspondant aux critères de recherche.

Type de caractéristique : *valeur*
Affiche les meilleurs types et valeurs de caractéristique de l'entité correspondant aux critères de recherche.

Relations
Affiche le nombre de relations de l'entité correspondant aux critères de recherche.

Alertes
Affiche le nombre d'alertes associées à l'entité correspondant aux critères de recherche.

Ecran Rechercher par compte de source de données :

Utilisez cette fenêtre pour rechercher une entité par les informations de compte de la source de données d'origine.

Saisir l'ID externe
Saisissez les informations sur le compte de source de données associées à l'entité dans la source de données spécifiée dans **Source de données**.

Source de données
Sélectionnez la source de données correspondant au compte spécifié dans **Saisir l'ID externe**.

Ecran Rechercher par ID d'entité :

Utilisez cette méthode Rechercher par pour trouver rapidement une entité par ID d'entité dans la base de données d'entités. Si la requête localise l'entité dans la base de données d'entités, le Visualizer affiche le Récapitulatif d'entité pour cette entité.

Fenêtre Rechercher par résolution :

Utilisez la fenêtre **Rechercher par résolution** pour créer une entité de recherche à comparer avec les identités de la base de données d'entités.

Code de source de données - Description
Sélectionnez un code de source de données ainsi qu'une description à associer aux identités trouvées par le processus Rechercher par résolution.

Score de résolution minimum
Sélectionnez le score de résolution minimal à utiliser pendant la comparaison d'identités avec les critères spécifiés pour la requête Rechercher par résolution.

Le score que vous sélectionnez détermine le nombre et le type de résultats renvoyés par la requête.

Section des critères de la Recherche par résolution
Indiquez les attributs permettant de créer l'entité de recherche qui est comparée aux identités dans la base de données d'entités. Le système renvoie des identités sur la base du score de résolution minimum que vous avez spécifié.

Liste de noms
Si vous recherchez un nom spécifique, saisissez les critères de nom dans les zones de la liste de noms. Si vous renseignez l'une des zones de nom, le **Nom** est obligatoire.

Liste d'adresses
Si vous recherchez une adresse spécifique, saisissez les critères d'adresse dans les zones de la liste d'adresses. Si vous renseignez l'une des zones d'adresse, la **Rue** est obligatoire.

Liste de numéros
Saisissez des critères de numéros spécifiques, tels qu'un numéro de passeport ou un numéro de carte de crédit dans les zones des listes de numéros. Le **Type** et la **Valeur** sont obligatoires.

Liste des caractéristiques
Saisissez les critères des caractéristiques spécifiques, telles que le sexe ou la date de naissance, dans les zones des caractéristiques. Le **Type** et la **Valeur** sont obligatoires.

Liste d'adresses électroniques
Saisissez les critères d'adresses électroniques spécifiques dans les zones de la liste d'adresses électroniques. Le **Type** et l'**Adresse** sont obligatoires.

Fenêtre du Gestionnaire de générateur d'alerte d'attribut :

Utilisez cette fenêtre pour afficher et gérer vos générateurs d'alerte d'attribut actuellement actifs. La fenêtre **Gestionnaire de générateur d'alerte d'attribut** n'affiche pas les générateurs d'alerte d'attribut arrivés à expiration.

Date d'expiration
Affiche la date à laquelle expire le générateur d'alerte d'attribut.

Date de création
Affiche la date à laquelle a été créé le générateur d'alerte d'attribut.

ID de l'entité
Indique l'ID de l'entité de recherche créée par les critères du générateur d'alerte d'attribut.

Raison
Le code raison affecté lors du processus de création du générateur d'alerte d'attribut

Score de résolution minimum
Affiche le score de résolution minimum que les entités doivent atteindre lors de la comparaison des critères d'alerte d'attribut avec les entités existantes dans la base de données d'entités avant qu'une alerte d'attribut ne soit générée pour cette entité.

Numéro du dossier
Affiche le numéro de dossier affecté pendant le processus de création du générateur d'alerte d'attribut.

Bouton Créer
Affiche la fenêtre **Créer un générateur d'alerte d'attribut**, afin que vous puissiez créer un générateur d'alerte d'attribut.

Bouton Editer
Affiche la fenêtre **Informations sur le générateur d'alerte d'attribut**, afin que vous puissiez éditer le générateur d'alerte d'attribut sélectionné. (Sélectionnez le générateur d'alerte d'attribut puis cliquez sur ce bouton.)

Fenêtre Créer un générateur d'alerte d'attribut :

Utilisez cette fenêtre pour créer un générateur d'alerte d'attribut qui utilise les critères d'attribut spécifiés pour rechercher de manière permanente des entités correspondant aux données d'attribut dans la base de données d'entités.

Code de source de données - Description
Sélectionnez un code de source de données ainsi qu'une description dans la liste déroulante à associer aux alertes d'attribut créées à partir de ce générateur d'alerte d'attribut. La sélection par défaut est généralement paramétrée sur "Rechercher".

Score de résolution minimum
Sélectionnez dans la liste déroulante le score de résolution minimum à utiliser pendant la comparaison d'identités avec les critères spécifiés pour le générateur d'alerte d'attribut.

Code raison
Sélectionnez dans la liste déroulante un code raison à associer au générateur d'alerte d'attribut.

Numéro du dossier
Saisissez un numéro de dossier facultatif pour les alertes d'attribut créées à partir de ce générateur d'alerte d'attribut.

Commentaire
Saisissez un commentaire facultatif pour les alertes d'attribut créées à partir de ce générateur d'alerte d'attribut.

Date d'expiration
Sélectionnez la date à laquelle expire ce générateur d'alerte d'attribut ou cliquez sur l'icône du calendrier et sélectionnez une date à l'aide de la commande du calendrier. La date d'expiration par défaut est réglée sur six mois à compter de la date du jour. Dans la mesure où les générateurs d'alerte d'attribut s'exécutent toujours en arrière-plan, la définition d'une date d'expiration est une bonne idée.

Section des critères d'attribut
Spécifiez les attributs que vous souhaitez pour générer une alerte d'attribut chaque fois que le système traite une fiche d'identité contenant les attributs spécifiés.

Liste de noms
Si vous recherchez un nom spécifique, saisissez les critères de nom dans les zones de la liste de noms.

Liste d'adresses
Si vous recherchez un nom spécifique, saisissez les critères de nom dans les zones de la liste d'adresses.

Liste de numéros
Si vous recherchez un numéro spécifique, tel que le numéro de

passeport ou celui d'une carte de crédit, saisissez les critères de numéro dans les zones de la liste de numéros.

Liste des caractéristiques
Si vous recherchez une caractéristique spécifique, telle que le sexe ou la date de naissance, saisissez les critères de caractéristique dans les zones de la liste de caractéristiques.

Liste d'adresses électroniques
Si vous recherchez une adresse électronique spécifique, saisissez les critères d'adresse électronique dans les zones de la liste d'adresses électroniques.

Fenêtre Informations sur le générateur d'alerte d'attribut :

Utilisez cette fenêtre pour éditer un générateur d'alerte d'attribut existant. Vous ne pouvez modifier que le numéro de dossier, la date d'expiration et les commentaires.

Code raison
(Affichage uniquement) Affiche le code raison sélectionné pour ce générateur d'alerte d'attribut.

Numéro du dossier
Affiche le numéro de dossier alphanumérique facultatif, saisi par l'utilisateur qui a créé le générateur d'alerte d'attribut.

Commentaire
Affiche tout commentaire saisi par l'utilisateur qui a créé le générateur d'alerte d'attribut.

Date d'expiration
Affiche la date d'expiration actuelle du générateur d'alerte d'attribut.

Noms utilisés
(Affichage uniquement) Si les informations sur le nom ont été saisies comme critères pour ce générateur d'alerte d'attribut, cette section répertorie toutes les informations sur le nom saisies par l'utilisateur qui a créé le générateur d'alerte d'attribut.

Adresse
(Affichage uniquement) Si les informations sur l'adresse ont été saisies comme critères pour ce générateur d'alerte d'attribut, cette section répertorie toutes les informations sur l'adresse saisies par l'utilisateur qui a créé le générateur d'alerte d'attribut.

Numéros
(Affichage uniquement) Si les informations sur les numéros ont été saisies comme critères pour ce générateur d'alerte d'attribut, cette section répertorie toutes les informations sur les numéros saisies par l'utilisateur qui a créé le générateur d'alerte d'attribut.

Autres attributs
(Affichage uniquement) Si les informations sur les caractéristiques ont été saisies comme critères pour ce générateur d'alerte d'attribut, cette section répertorie toutes les informations sur les caractéristiques saisies par l'utilisateur qui a créé le générateur d'alerte d'attribut.

Bouton Mise à jour
Cliquez pour appliquer vos modifications.

Analyse des entités

Vous pouvez utiliser le Visualizer afin de passer en revue, analyser et effectuer un graphique des entités dans la base de données d'entités.

Entités

Une entité est une collection d'une ou plusieurs identités représentant les mêmes personne, organisme, lieu ou élément. Elles sont stockées dans la base de données d'entités.

Bien que les entités soient souvent perçues comme des personnes,il peut également s'agir de choses telles que des entreprises ou des véhicules. En fait, vous pouvez utiliser la configuration extensible du système pour mapper les données de votre organisme et créer n'importe quel type d'entité à résoudre ou apparenter.

Les entités se composent généralement d'identités issues de plusieurs systèmes source différents. La résolution d'entité détermine quelles identités sont en réalité la même entité et crée une entité composite renfermant toutes les identités qui lui sont associées. Le système consigne l'historique d'attribution intégrale des fiches, en identifiant ainsi la source associée à chaque identité de l'entité composite.

Il convient de configurer le système de façon à résoudre et apparenter les entités d'une manière qui satisfasse les objectifs de votre organisme.

Récapitulatifs d'entités

Un récapitulatif d'entité est un recueil unifié de toutes les informations présentes dans la base de données sur une entité précise.

Au sein de la base de données, les entités sont organisées au moyen d'identifiants. Chaque ID d'entité possède son propre récapitulatif d'entité.

Les récapitulatifs d'entité se consultent au moyen du visualiseur. Ils peuvent contenir les types d'informations suivants :

- Références de document source
- Rôles
- Noms utilisés
- Adresses
- Numéros
- Caractéristiques
- Divulgations
- Entités associées
- Historique de conflit
- Historique des alertes d'événement
- Adresses électroniques

Consultation des récapitulatifs d'entité

Pour consulter toutes les informations sur une entité spécifique dans la base de données d'entités, affichez le récapitulatif d'entité.

Pourquoi et quand exécuter cette tâche

Vous pouvez accéder à un récapitulatif d'entité à partir de n'importe lequel des emplacements suivants de Visualizer :

- Toute fenêtre de détail d'alerte

- Toute fenêtre de graphique
- Toute fenêtre **Rechercher par :**

Procédure

- Depuis une fenêtre **Détail d'alerte de rôle**, **Détail d'alerte d'attribut**, ou **Détail d'alerte d'événement**, cliquez sur **Récapitulatif d'entité**.
- Depuis un graphique d'entité, cliquez droit sur l'icône **Entité** contenant les informations sur l'ID d'entité que vous voulez consulter et sélectionnez **Récapitulatif d'entité**.
- Dans la section **Résultats** d'une fenêtre **Rechercher par :**, cliquez deux fois sur la ligne contenant l'entité dont vous voulez consulter le récapitulatif.

Impression de récapitulatifs d'entité

Si vous souhaitez une copie papier ou une version PDF d'un récapitulatif d'entité, ou si vous voulez copier des informations d'un récapitulatif d'entité dans une autre application, telle qu'un traitement de texte ou un tableur, plusieurs méthodes d'impression existent.

Procédure

- Pour imprimer une capture d'écran de la fenêtre **Récapitulatif d'entité**, procédez comme suit :
  1. Dans la fenêtre **Récapitulatif d'entité**, cliquez sur **Imprimer**.
  2. Dans la boîte de dialogue de l'impression, indiquez vos paramètres d'impression.
  3. Cliquez sur **OK**.
- Pour imprimer le récapitulatif d'entité dans un fichier PDF, dans la fenêtre **Récapitulatif d'entité**, cliquez sur **Rapport**.
- Pour copier (imprimer) les informations du récapitulatif d'entité afin de les coller dans une autre application, procédez comme suit :
  1. Dans la fenêtre **Récapitulatif d'entité**, dans le menu **Editer**, cliquez sur **Copier l'écran dans le Presse-papier**.

     Remarque : La combinaison des touches **Ctrl** + **C** ne copie les valeurs que d'une seule zone.
  2. Collez le contenu du presse-papier dans l'application à utiliser.
  3. A l'aide de la fonction d'impression de l'application, imprimez les informations du récapitulatif d'entité.

Impression de la fenêtre actuelle

Vous pouvez imprimer n'importe quelle fenêtre du visualiseur, y compris les graphiques et récapitulatif d'entité, directement depuis cette fenêtre, à l'aide de la commande d'impression.

Procédure

1. Dans la fenêtre d'impression du Visualizer, sélectionnez **Imprimer** dans le menu **Fichier**.
2. Dans la boîte de dialogue **Imprimer**, indiquez vos paramètres d'impression.
3. Cliquez sur **OK**.

Consultation des graphiques d'entité

L'un des principaux avantages du Visualizer est que vous pouvez créer un graphique des informations sur la relation d'entité et l'alerte de rôle. Les graphiques fournissent une représentation visuelle des informations sur l'entité sélectionnée.

Pourquoi et quand exécuter cette tâche

Vous pouvez accéder à un graphique d'entité à partir de n'importe lequel des emplacements suivants de Visualizer :

- Fenêtre **Récapitulatif d'entité**
- Fenêtre **Graphique**
- Fenêtre **Détail de l'alerte d'événement**

Procédure

- Depuis une fenêtre **Récapitulatif d'entité**, cliquez sur **Graphique**.
- Depuis une fenêtre **Graphique**, cliquez droit sur l'icône **Entité** qui contient l'ID d'entité dont vous voulez consulter les informations, et sélectionnez **Afficher le graphique de l'entité**. Pour visualiser le récapitulatif d'une entité sous forme de graphique, cliquez avec le bouton droit sur l'entité et sélectionnez **Récapitulatif d'entité**.
- Depuis une fenêtre **Détail de l'alerte d'événement**, cliquez sur **Graphique**.
- Facultatif : Pour modifier l'affichage des informations dans un graphique, cliquez droit sur tout espace vierge dans le graphique, puis :
  1. Sélectionnez un réglage de **Présentation de graphique** différent afin de modifier l'agencement visuel des informations dans le graphique.
  2. Sélectionnez un réglage de **Zoom** différent pour changer de niveau de zoom.

  Chaque fois que vous modifiez les paramètres du graphique, les nouveaux paramètres sont utilisés comme paramètres par défaut pour chaque nouveau graphique que vous affichez pendant la session en cours du Visualizer.

Consultation des graphiques d'alerte de rôle

Si vous voulez visualiser une représentation graphique de la façon dont les entités qui ont été identifiées par une alerte de rôles sont apparentées, vous pouvez consulter un graphique d'alerte de rôle.

Procédure

1. Dans le Visualizer, dans la fenêtre **Récapitulatif des alertes**, cliquez deux fois sur l'alerte de rôle.
2. Dans la fenêtre **Détail de l'alerte de rôle**, cliquez sur **Graphique**.
3. Facultatif : Pour modifier la façon dont les informations s'affichent dans un graphique, cliquez avec le bouton droit sur un espace vide à l'intérieur du graphique, puis :
   a. Sélectionnez un réglage de **Présentation de graphique** différent afin de modifier l'agencement visuel des informations dans le graphique.
   b. Sélectionnez un réglage de **Zoom** différent pour changer de niveau de zoom.

   Chaque fois que vous modifiez les réglages de graphique, les nouveaux réglages sont appliqués comme réglages par défaut de tout autre graphique que vous consultez au cours de la session Visualizer actuelle.

4. Facultatif : Pour visualiser le récapitulatif d'une entité sous forme de graphique, cliquez avec le bouton droit sur l'entité et sélectionnez **Récapitulatif d'entité**.

Personnalisation des icônes de graphique

Tous les graphiques du Visualizer utilisent des icônes prédéfinies pour représenter les entités et les types d'attribut, tels que les adresses et les numéros. Vous pouvez personnaliser les icônes qui s'affichent dans les graphiques du Visualizer ou spécifier une icône à utiliser pour un nouveau type d'attribut.

Avant de commencer

Avant de personnaliser les icônes des graphiques du Visualizer, gardez à l'esprit les contraintes suivantes :

- Les icônes personnalisées résident sur le serveur d'application. Seuls les utilisateurs bénéficiant de droits d'accès administratifs au serveur d'application peuvent ajouter ou modifier des icônes de graphique personnalisées. Tous les clients Visualizer basés sur ce serveur d'application utilisent le même ensemble d'icônes. C'est pourquoi les modifications que vous effectuez affectent l'affichage des icônes des graphiques Visualizer de chacun de ces clients.
- Enregistrez les icônes personnalisées dans un dossier d'icônes séparé dans le serveur d'application. L'installation d'un nouveau fichier *.EAR pour le Visualizer supprime toutes les icônes de graphique personnalisées. Après l'installation d'une nouveau fichier *.EAR du Visualizer, vous pouvez copier les icônes de graphique personnalisées depuis le dossier des icônes dans le dossier des icônes du serveur d'application désigné.
- Les icônes doivent avoir le format .GIF. La taille recommandée de l'image est de 24 x 24 pixels.
- Les noms des icônes doivent correspondre à leur type d'attribut, uniquement en minuscules. Par exemple, si vous ajoutez un nouveau type d'attribut intitulé "Photo de preuve", le fichier doit être intitulé "photo de preuve.gif" afin que le Visualizer reconnaisse la photo de preuve personnalisée. Notez dans cet exemple, que le nom de type d'attribut et le nom du fichier d'icône contiennent des espaces.

Pourquoi et quand exécuter cette tâche

Les fichiers d'image d'icône du Visualizer sont stockés par défaut sur le serveur d'application, généralement dans un dossier intitulé `images`.

Procédure

1. Arrêter le serveur d'application.
2. Sur le serveur d'application, recherchez le dossier des icônes de graphique Visualizer par défaut. Généralement, ce dossier est situé dans *IBM Infosphere Identity Insight application server install_path*/ `was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images`.
3. Obligatoire : Créez un dossier intitulé `graphique` sous le dossier des icônes de graphique Visualizer par défaut (le dossier `/images`) pour vos fichiers d'image d'icône de graphique personnalisé.

   Remarque : Le nom du dossier doit être `graphique`.
4. Enregistrez, copiez ou déplacez chaque fichier d'image d'icône dans le nouveau dossier.

Exemple

Si vous avez créé un type d'attribut nommé FINGERPRINT_FILE et que vous souhaitez une icône de graphique personnalisée pour représenter ce type d'attribut dans les graphiques Visualizer, procédez comme suit :

1. Créez ou obtenez un fichier d'image .GIF adapté, de 24 x 24 pixels, afin de représenter le type d'attribut FINGERPRINT_FILE. Veillez à ce que le nom du fichier d'image corresponde au nom du fichier d'attribut et à ce que toutes les lettres soient en minuscules, comme dans ce nom de fichier : fingerprint_file.gif
2. Sur le serveur d'application IBM InfoSphere Identity Insight, localisez le dossier images. Pour cet exemple, le dossier d'images est situé ici : IBM-II_install/ was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images.
3. Dans le dossier des images, créez un dossier intitulé graphique. Le chemin d'accès au fichier ressemble à celui-ci : IBM-II_install/ was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images/graph
4. Copiez l'icône d'image fingerprint_file.gif dans le dossier graphique.

Que faire ensuite

Redémarrez le serveur d'application.

Rubriques d'aide

Fenêtre Récapitulatif d'entité :

Utilisez cet écran pour consulter toutes les informations détaillées connues concernant une entité, y compris les attributs des identités associées à l'entité, toutes les entités apparentées, ainsi que l'historique de toutes les alertes associées à l'entité.

Utilisez les commandes pour développer ou réduire les sections de l'écran afin de vous aider à vous concentrer sur un détail spécifique.

Informations sur la source de données
: Affiche les sources de données qui ont fourni les fiches d'identité liées à cette entité. Cliquez sur une source de données pour mettre en surbrillance les attributs qui composent la fiche de l'identité qui a été traitée depuis cette source de données. Les informations sur la source de données vous aident à tracer la fiche d'identité jusqu'à sa source d'origine.

  Lorsque des entités possèdent plusieurs identités, la surbrillance peut vous aider à distinguer une identité d'une autre ainsi que la source de données d'origine dans laquelle réside l'identité.

Rôles Affiche les rôles affectés aux identités qui relient à cette entité.

Noms Affiche les noms utilisés par les identités qui relient à cette entité.

Adresses
: Affiche les adresses connues utilisées par les identités liées à cette entité, y compris l'intervalle de dates pendant lequel chaque adresse était valide pour l'identité (si cette information est disponible).

Numéros
: Affiche les numéros connus utilisés par les identités liées à cette entité, y compris l'intervalle de dates pendant lequel chaque numéro était valide pour cette identité (si cette information est disponible).

Caractéristiques
Affiche les caractéristiques connues utilisées par les identités liées à cette entité, y compris l'intervalle de dates pendant lequel chaque caractéristique était valide pour l'identité (si cette information est disponible).

Adresses électroniques
Affiche les adresses électroniques connues utilisées par les identités liées à cette entité, y compris l'intervalle de dates pendant lequel chaque adresse électronique était valide pour l'identité (si cette information est disponible).

Divulgations
Affiche les relations divulguées qui ont été explicitement ajoutées par un analyste ou un utilisateur autorisé de Visualizer pour relier deux identités. Les divulgations créent une relation de force 100 % entre deux identité.

Entités associées
Répertorie les informations de base concernant les autres entités liées à cette entité. Sélectionnez une entité associée pour mettre en surbrillance les informations qui ont créé la relation.

Historique de conflit
Répertorie les informations de base sur les alertes de rôle associées à cette entité.

Historique des alertes d'événement
Affiche les informations concernant les alertes d'événement associées à cette entité.

Bouton Imprimer
Ouvre la boîte de dialogue d'impression, afin que vous puissiez imprimer le récapitulatif de l'entité.

Bouton Rapport
Génère un rapport **Récapitulatif d'entité**, contenant toutes les informations extraites du récapitulatif d'entité.

Ecran Graphique de relation d'entité :

Utilisez cet écran pour voir une représentation visuelle des détails de relation de l'entité sélectionnée, dont notamment les attributs d'entité, les entités apparentées, et les événements d'entité.

Zone de diagramme (Canevas)

Le corps du diagramme est désigné sous le terme de canevas. Il contient la représentation graphique des relations et montre les attributs qui relient les entités.

Cliquez sur les objets (noeuds) sur le diagramme afin de les repositionner sur le diagramme. Si un attribut d'hyperlien existe, utilisez **Ctrl** + **Clic** pour suivre le lien.

Cliquez droit sur les options du menu

Disposition du graphique
Modifie la disposition et la position actuelles des noeuds du diagramme. Chaque objet du diagramme est appelé un noeud.

Faites des essais avec les paramètres de mise en page du diagramme jusqu'à ce que vous trouviez le paramétrage qui vous convient. Ces paramètres sont purement fonctions de vos goûts et besoins lors de l'examen des relations d'entité de ce graphique.

Anneal
Sélectionnez ce paramètre pour répartir les noeuds uniformément. Le paramètre Recuit uniformise les longueurs d'arête du graphique, réduit les intersections de ligne, et empêche les noeuds de trop se rapprocher du bord du graphique.

Hiérarchique
Sélectionnez ce paramètre pour afficher les noeuds selon une hiérarchie. Le paramétrage hiérarchique fonctionne mieux sur les graphiques orientés qui ont un flux général, ou sur les graphiques qui ont des points de départ, des points d'arrivée, et un flux général entre ces points.

Organique
Sélectionnez ce paramètre pour répartir uniformément les vertices du graphique. Le paramétrage organique uniformise les longueurs d'arête et reflète la symétrie du graphique, mais ne vous permet pas d'afficher les entités apparentées.

Auto-organisation
Sélectionnez ce paramètre pour créer uniformément des groupes espacés de noeuds de graphique reliés.

Aléatoire
Sélectionnez ce paramètre pour répartir aléatoirement les noeuds du graphique.

Incliné
Sélectionnez ce paramètre pour basculer ou incliner le positionnement des noeuds du graphique de la mise en page précédemment sélectionnée.

Cercle Sélectionnez ce paramètre pour organiser les noeuds du graphique dans un cercle ayant un espacement uniforme entre les noeuds de graphique voisins.

Zoom Sélectionnez un paramètre pour modifier la taille d'affichage du canevas dans la taille d'écran actuelle.

75 % Affiche le graphique à 75% de sa taille initiale.

50 % Affiche le graphique à 50 % de sa taille originale

Afficher tous les attributs
Affiche tous les attributs affectés à cette entité.

Masquer l'attribut
Masque l'attribut sélectionné.

Afficher les entités associées
Affiche toutes les autres entités qui s'apparentent à cette entité, ainsi qu'une représentation graphique du lien de ces entités. Cette option n'est pas disponible si le paramétrage actuel de la Mise en page du graphique est **Organique**.

Récapitulatif d'entité
Ouvre la fenêtre Récapitulatif d'entité et affiche un récapitulatif détaillé de toutes les informations connues sur cette entité.

Evénements d'entité
Ouvre l'écran Evénements d'entité et affiche les informations sur les événements associés à cette entité. Cette option n'est disponible que si l'entité sélectionnée possède des événements associés.

Afficher le graphique d'entité
Ouvre la fenêtre Graphique d'entité, qui affiche une représentation visuelle des informations sur cette entité uniquement

Régler les options du graphique

Défilement du zoom
Déplacez l'indicateur de zoom pour redimensionner le canevas.

Contrainte de mise en page
Sélectionnez une contrainte de bornes de mise en page pour la taille du canevas.

Tableau des propriétés

Sélectionnez un noeud dans le graphique, et ce tableau fournit les propriétés du noeud sélectionné : Attributs ou entités.

Ecran Graphique d'alerte de rôle :

Utilisez cet écran pour voir une représentation visuelle des détails d'alerte de rôle de l'entité sélectionnée, dont notamment les attributs d'entité, les entités apparentées, et les événements d'entité.

Zone de diagramme (Canevas)

Le corps du diagramme est désigné sous le terme de canevas. Il contient la représentation diagramme des détails de l'alerte de rôle.

Cliquez sur les objets (noeuds) sur le diagramme afin de les repositionner sur le diagramme. Si un attribut d'hyperlien existe, utilisez **Ctrl** + **Clic** pour suivre le lien.

Cliquez droit sur les options du menu

Le fait de cliquer droit sur le menu vous donne le contrôle sur l'affichage du graphique et vous donne des options pour naviguer jusqu'aux fenêtres des entités apparentées.

Disposition du graphique
Modifie la disposition et la position actuelles des noeuds du diagramme. Chaque objet du diagramme est appelé un noeud.

Faites des essais avec les paramètres de mise en page du diagramme jusqu'à ce que vous trouviez le paramétrage qui vous convient. Ces paramètres sont purement fonctions de vos goûts et besoins lors de l'examen des alertes de rôle de ce diagramme.

Anneal
Sélectionnez ce paramètre pour répartir les noeuds uniformément. Le paramètre Recuit uniformise les longueurs d'arête du graphique, réduit les intersections de ligne, et empêche les noeuds de trop se rapprocher du bord du graphique.

Hiérarchique
Sélectionnez ce paramètre pour afficher les noeuds selon une hiérarchie. Le paramétrage hiérarchique fonctionne mieux sur les graphiques orientés qui ont un flux général, ou sur les graphiques qui ont des points de départ, des points d'arrivée, et un flux général entre ces points.

Organique
Sélectionnez ce paramètre pour répartir uniformément les vertices du graphique. Le paramétrage organique uniformise les longueurs d'arête et reflète la symétrie du graphique, mais ne vous permet pas d'afficher les entités apparentées.

Auto-organisation
Sélectionnez ce paramètre pour créer uniformément des groupes espacés de noeuds de graphique reliés.

Aléatoire
Sélectionnez ce paramètre pour répartir aléatoirement les noeuds du graphique.

Incliné
Sélectionnez ce paramètre pour basculer ou incliner le positionnement des noeuds du graphique de la mise en page précédemment sélectionnée.

Cercle Sélectionnez ce paramètre pour organiser les noeuds du graphique dans un cercle ayant un espacement uniforme entre les noeuds de graphique voisins.

Zoom Sélectionnez un paramètre pour modifier la taille d'affichage du canevas dans la taille d'écran actuelle.

75 % Affiche le graphique à 75% de sa taille initiale.

50 % Affiche le graphique à 50 % de sa taille originale

Afficher tous les attributs
Affiche tous les attributs affectés à cette entité.

Masquer l'attribut
Masque l'attribut sélectionné.

Afficher les entités associées
Affiche toutes les autres entités qui s'apparentent à cette entité, ainsi qu'une représentation graphique du lien de ces entités. Cette option n'est pas disponible si le paramétrage actuel de la Mise en page du graphique est **Organique**.

Récapitulatif d'entité
Ouvre la fenêtre Récapitulatif d'entité et affiche un récapitulatif détaillé de toutes les informations connues sur cette entité.

Evénements d'entité
Ouvre l'écran Evénements d'entité et affiche les informations sur les événements associés à cette entité. Cette option n'est disponible que si l'entité sélectionnée possède des événements associés.

Afficher le graphique d'entité
Ouvre la fenêtre Graphique d'entité, qui affiche une représentation visuelle des informations sur cette entité uniquement

Régler les options du graphique

Défilement du zoom
Déplacez l'indicateur de zoom pour redimensionner le canevas.

Contrainte de mise en page
Sélectionnez une contrainte de bornes de mise en page pour la taille du canevas.

Tableau des propriétés

Sélectionnez un noeud dans le graphique, et ce tableau fournit les propriétés du noeud sélectionné : Attributs ou entités.

Ajout de données à l'aide du Visualizer

Les données d'entité sont généralement chargées par le fichier de données UMF dans le système par des opérateurs système dans des processus en mode de traitement par lots ou en temps réel. Toutefois, les utilisateurs se servent du Visualizer pour ajouter manuellement une entité unique, révéler une relation entre deux entités (par identité), charger et traiter un fichier de données UMF ou valider un fichier de données UMF avant son chargement.

Avant de commencer

L'ajout données nécessite un pipeline disponible et en cours d'exécution pour traiter les données. Mais les utilisateurs du Visualizer n'ont pas besoin de démarrer ni d'exécuter leur propre pipeline. Lorsque le Visualizer ajoute des données, il les envoie automatiquement via un pipeline Visualizer désigné.

Ajout d'une seule entité

Vous pouvez ajouter une entité unique à la base de données d'entités, sans créer manuellement une fiche UMF. Vous pouvez créer une entité avec des informations aussi restreintes que le nom, mais vous devez saisir autant d'informations connues sur l'entité (adresses connues, numéros, caractéristiques ou adresses électroniques) que possible, pour une résolution d'entité et de relation optimale.

Procédure

1. Dans Visualizer, effectuez l'une des opérations suivantes :
   a. Cliquez sur **Afficher** > **Ajouter** > **Entité**.
   b. Dans la barre d'outils, cliquez sur l'icône (ajouter) et sélectionnez **Entité**.
   c. Dans la barre d'outils, cliquez sur la flèche et sélectionnez **Entité**.
   d. Dans la fenêtre **Ajouter**, dans le menu déroulant **Ajouter**, sélectionnez **Entité**.
2. Saisissez les informations relatives à l'entité à l'aide des différentes zones et listes déroulantes. Alors que vous saisissez les données, l'écran vous guide en mettant en surbrillance les zones requises en jaune. Une zone mise en surbrillance en jaune indique que, sur la base des autres sélections de cet écran, vous devez saisir les données dans toute zone mise en surbrillance en jaune.
   - Zone **Référence** : Vous devez saisir les informations dans cette zone. Les informations de référence constituent un identifiant pour l'identité. Saisissez par exemple le numéro de compte de source de données, tel qu'un compte bancaire.
   - Zones de Noms : Si vous saisissez toute partie d'un nom (prénom, deuxième prénom ou génération), le nom est obligatoire.
   - Zones d'adresse : Vous pouvez ajouter des informations dans la zone **Adresse** sans saisir la localité, l'état, le code postal ou le pays. Mais vous devez saisir des informations dans la zone **Adresse** si vous saisissez toute autre partie de l'adresse.
   - Zones Numéros, Caractéristiques, ou Adresse électronique : Si vous souhaitez saisir des informations dans l'un quelconque de ces attributs, vous devez sélectionner un type et saisir une valeur pour l'attribut.

Avertissement : Toutes les informations que vous saisissez dans cet écran font partie de l'entité que vous ajoutez. Vous n'indiquez pas de relations avec les autres entités ou les caractéristiques ou numéros partagés. Saisissez uniquement les informations qui appartiennent à l'entité que vous ajoutez, telles que les alias, ou autres noms associés à l'entité, et les adresses, numéros, caractéristiques et adresses électroniques associés à l'entité.

3. Cliquez sur **Soumettre**.

Résultats

Le Visualizer crée une fiche d'identité UMF comprenant toutes les informations que vous avez saisies pour cette entité et envoie la fiche dans le pipeline, où elle est traitée et ajoutée à la base de données d'entités.

Chargement de données à partir d'un fichier

Utilisez la fonction **Chargement de fichier** dans le Visualizer pour charger les données de plusieurs identités définies dans un fichier UMF. Le **Chargement de fichier** ne chargera que les fiches `<UMF_ENTITY>`. Lorsque vous sélectionnez un fichier UMF, le système ouvre le fichier, charge les données dans le pipeline, puis celui-ci traite les identités dans le fichier, ce qui les ajoute à la base de données d'entités et résoud toutes relations d'entités et d'identités. Les alertes se déclenchent en fonction des règles qui ont été configurées.

Pourquoi et quand exécuter cette tâche

La résolution d'entité et de relation se fait dans le composant pipeline. Pour charger et traiter des fichiers UMF via le Visualizer, un pipeline en cours d'exécution doit exister et être disponible pour communiquer avec le serveur Visualizer.

Avant de charger un fichier, vous pouvez souhaiter valider l'UMF dans le fichier, afin d'être certain que le fichier ne comporte pas d'erreurs.

Procédure

1. Dans le Visualizer, effectuez l'une des opérations suivantes :
   a. Cliquez sur **Afficher** > **UMF** > **Chargement de fichier**.
   b. Dans la barre d'outils, cliquez sur l'icône (UMF).
   c. Dans la fenêtre **UMF**, dans la zone déroulante **UMF**, sélectionnez **Chargement de fichier**.
2. Cliquez sur **Charger le fichier...** afin de sélectionner le fichier UMF à charger, puis cliquez sur **Ouvrir**. Le système charge le fichier sélectionné dans le pipeline, et ce dernier commence le traitement des données du fichier. La **Barre de progression du fichier** vous montre le temps écoulé pendant le traitement, le nombre de fiches traitées, ainsi que l'état du chargement du fichier.
   a. Pour arrêter le chargement et le traitement du fichier, cliquez sur l'icône (Arrêter).
   b. Pour mettre en pause le chargement et le traitement du fichier, cliquez sur l'icône (Pause).
   c. Pour reprendre le chargement et le traitement du fichier après la pause, cliquez sur l'icône (Continuer).

   Alors que sont chargées les données du fichier, un pipeline traite les données via la résolution d'entité et de relation. Si vous constatez une erreur, contactez votre administrateur système. L'erreur est très probablement un problème de pipeline.

Les nouvelles identités sont ajoutées à la base de données, ainsi que les entités et relations résolues. Le système génère toute alerte liée aux données, en se basant sur les règles système configurées.

3. Facultatif : Dès que le fichier est chargé et traité, cliquez sur **Afficher les résultats** pour afficher la boîte de dialogue **Résultats de chargement du fichier**, qui comprend les informations suivantes :
   - Le nombre de fiches envoyées dans le pipeline.
   - Le nombre de nouvelles entités créées dans la base de données d'entités, sur la base des données du fichier que vous avez chargé.
   - Le nombre d'exceptions UMF que le pipeline a rencontrées pendant le traitement des données dans ce fichier. (Ce nombre peut indiquer des erreurs dans le fichier UMF ou des problèmes de syntaxe qui empêchent le pipeline de traiter complètement les données).

Que faire ensuite

Si la boîte de dialogue **Résultats de chargement du fichier** indique que des exceptions UMF ont eu lieu dans le fichier que vous avez chargé, validez le fichier à l'aide de la fonction Validation de fichier UMF pour vous aider à retrouver les erreurs dans le fichier afin de pouvoir les corriger. Dès que vous avez corrigé les erreurs, rechargez les données qui contenaient les erreurs afin que le pipeline puisse traiter complètement ces données.

Validation d'un fichier UMF avant de charger les données

Si vous prévoyez d'utiliser le Visualizer pour charger et traiter les fiches des petits fichiers UMF, vous pouvez vouloir valider au préalable les données du fichier.

Pourquoi et quand exécuter cette tâche

Le processus de validation vérifie que les données correspondent aux exigences minimales pour le traitement de la résolution d'entité et de relation. Le processus de validation offre également des informations utiles sur les zones du fichier à vérifier ou à corriger avant le chargement et le traitement des données. Meilleure est la qualité des données entrées dans le système, et meilleurs sont les résultats.

Procédure

1. Dans le Visualizer, effectuez l'une des opérations suivantes :
   - Cliquez sur **Afficher** > **UMF** > **Fichier de validation UMF**.
   - Dans la barre d'outils, cliquez sur la flèche à la droite de l'icône et cliquez sur **Fichier de validation UMF**.
   - Dans la fenêtre **UMF**, dans la liste **UMF**, sélectionnez **Fichier de validation UMF**.
2. Cliquez sur **Valider le fichier...**.
3. Choisissez le fichier UMF à valider.

   Remarque : Si vous avez déjà validé un ou plusieurs fichiers UMF, et laissé la fenêtre **UMF** ouverte, les zones **Fichier à valider** et **Fichier d'erreur/avertissement** contiennent les valeurs de la dernière validation de fichier UMF.
4. Facultatif : Pour modifier le chemin d'accès au répertoire ou le nom de fichier du fichier journal du traitement de validation dans la fenêtre **Définition de validation UMF**, effectuez l'une des opérations suivantes :

- Sélectionnez le nom de répertoire et de fichier à utiliser, cliquez sur **Parcourir...**, puis cliquez sur **Ouvrir**.
- Saisissez le chemin d'accès complet ainsi que le nom de fichier du fichier journal erreur de validation et avertissement. Vous pouvez saisir le nom d'un fichier existant ou celui d'un nouveau fichier journal.

Remarque : Si vous validez plus d'un fichier UMF et que vous laissez la fenêtre **UMF** ouverte, notez que la valeur du fichier journal dans la fenêtre **Définition de validation UMF** est par défaut le même chemin d'accès et nom de fichier que le dernier fichier journal erreur de validation et avertissement. La fermeture de la fenêtre **UMF** efface les zones du chemin d'accès et du fichier journal.

5. Cliquez sur **Valider le fichier UMF** pour lancer le processus de validation. Alors que s'exécute le processus de validation, les statistiques de validation s'affichent, y compris les informations dynamiques sur le pourcentage terminé, le temps écoulé, le nombre de fiches traitées, et l'état du traitement. Vous pouvez mettre en pause ou arrêter le processus de validation à tout moment.
6. Facultatif : Lorsque vous cliquez sur **Valider le fichier UMF**, si un autre fichier journal de validation existe et possède le même emplacement et nom que celui que vous avez saisi au cours de l'étape 4, le système affiche un message d'information pour vous le signaler. Le message comprend le nom et l'emplacement du fichier. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Oui** pour utiliser le même fichier journal d'erreur de validation et avertissement. Ce choix efface le précédent fichier journal.
   - Cliquez sur **Non** pour créer ou utiliser un autre fichier journal d'erreur de validation/avertissement. Le système vous renvoie à la fenêtre **Définition de la validation UMF**, afin que vous puissiez modifier manuellement le chemin d'accès et le nom de fichier du fichier journal d'erreur de validation et avertissement.
7. Une fois le processus de validation terminé, cliquez sur **Afficher les résultats** si vous souhaitez voir un récapitulatif des résultats.

Que faire ensuite

Utilisez les informations de la fenêtre **Affichage des résultats de validation UMF** pour voir les résultats et les informations dans le fichier journal d'erreurs et d'avertissement.

Divulgation de relations entre identités

Si vous estimez que vous avez des données reliant deux identités (ou comptes), vous pouvez spécifier ce lien pour divulguer la relation à l'aide du Visualizer.

Procédure

1. Dans Visualizer, effectuez l'une des opérations suivantes :
   a. Cliquez sur **Afficher** > **Ajouter** > **Divulgation**.
   b. Dans la barre d'outils, cliquez sur la flèche à la droite de l'icône (ajouter) et sélectionnez **Divulgation**.
   c. Dans la fenêtre **Ajouter**, dans le menu déroulant **Ajouter**, sélectionnez **Divulgation**.
2. Obligatoire : Dans les zones **ID d'entité**, saisissez la valeur de l'ID d'entité des entités contenant les identités à relier.

3. Obligatoire : Cliquez sur **Consulter** pour que chaque ID d'entité récupère ses identités associées. Consultez la liste des identités récupérées pour vous assurer que vous avez saisi l'ID d'entité souhaité.
4. Pour chaque entité, sélectionnez le bouton d'option de l'identité (ou le compte de source de données) pour laquelle vous divulguez une relation.
5. Dans la zone **Description de la relation divulguée**, saisissez une description du lien entre les identités.
6. Cliquez sur **Créer**. Une fenêtre de confirmation s'affiche pour vérifier que la création de la relation divulguée a réussi.

Rubriques d'aide

Fenêtre Ajouter une entité :

Utilisez cette fenêtre pour ajouter une nouvelle entité unique à la base de données d'entités via Visualizer. Toutes les informations que vous saisissez dans cet écran deviennent des attributs de la nouvelle identité que vous venez de créer. (Vous ne créez qu'une identité à la fois.) Après avoir transmis les données que vous avez saisies pour l'identité, le système traite les données via le pipeline pour la résolution d'entité et de relation - processus pendant lequel l'identité peut être associée à une ou plusieurs entités existantes.

Code de source de données - Description
Sélectionnez la source de données à associer à l'identité que vous ajoutez. La source de données doit exister dans votre système. (Vous ne pouvez pas ajouter ici de nouvelle source de données. Si vous ne voyez pas le code de source de données ni la description que vous voulez utiliser, contactez votre administrateur système pour créer pour vous la source de données.)

Pour ajouter une identité, le code de source de données ainsi que la description sont nécessaires.

Référence
Saisissez un identifiant pour ce compte de source de données, qui est utilisé pour associer le compte avec l'identité que vous saisissez. (Des exemples de numéros de référence comprennent les numéros de dossier, les numéros de compte bancaire, ou les numéros de bonus client.)

Pour ajouter une identité, la référence est obligatoire

Liste de noms
Saisissez les noms à associer à l'identité unique que vous ajoutez. Pour ajouter une identité, les informations de nom (au moins le nom et le prénom) sont obligatoires. Vous pouvez indiquer que l'identité que vous ajoutez possède plus d'un nom en saisissant chaque nom de l'identité sur une ligne distincte. Par exemple, si vous connaissez le nom réel de l'identité ainsi qu'un ou plusieurs surnoms ("également connu sous le nom de"), vous pouvez tous les saisir sur cet écran.

Remarque : Veillez à ne saisir qu'un seul nom par ligne.

Tous les noms que vous saisissez dans cette liste sont automatiquement associés à l'identité nouvellement créée, en tant qu'attributs de cette identité. Par exemple, si vous saisissez "Robert Hays" et "Bob J. Hayes, Jr.", ces deux noms sont associés à l'identité nouvellement créée.

Liste d'adresses
Saisissez une ou plusieurs adresses associées à l'identité que vous ajoutez. Par exemple, si vous connaissez les adresses actuelles et antérieures de

l'identité, saisissez chaque adresse complète, une adresse par ligne. Toutes les adresses que vous saisissez dans cette section de la liste sont automatiquement associées à l'identité que vous ajoutez.

Les adresses ne sont pas obligatoires pour ajouter une identité. S'il n'existe pas d'adresse connue pour cette identité, vous pouvez laisser vide cette section de liste.

Adresse
En règle générale, ces informations correspondent aux informations saisies aux lignes d'adresse 1 et 2 . Par exemple, 555 Main Street Building 17 Suite 102-B

Si vous saisissez des données dans l'une des zones d'adresse, vous devez saisir les données dans la zone **Adresse**.

Date de début
Saisissez la date à laquelle les informations sur cette adresse sont devenues valides pour cette identité, si cela est connu. Par exemple, si cette identité était connue pour être à cette adresse à partir du 15 mars 1999, saisissez cette date.

Vous pouvez saisir une date de début sans date de fin.

Date de fin
Saisissez la date à laquelle les informations sur cette adresse sont devenues invalides pour cette identité, si cela est connu. Par exemple, si cette identité était connue pour quitter cette adresse à partir du 1er juin 2001, saisissez cette date.

Vous pouvez saisir une date de fin sans date de début.

Liste de numéros
Indiquez un ou plusieurs numéros associés à l'identité que vous ajoutez. Par exemple, si vous connaissez une carte de crédit utilisée par l'identité, un numéro de permis de conduire, un numéro d'identification, un numéro de passeport, et un numéro de téléphone, saisissez chaque numéro sur une ligne distincte. Tous les numéros que vous saisissez dans cette section de la liste sont automatiquement associés à l'identité que vous ajoutez.

Les numéros ne sont pas obligatoires pour ajouter une identité, alors vous pouvez laisser vide cette section de la liste. Cependant, si vous saisissez des numéros, alors, les zones **Type de numéro** et **Valeur** sont obligatoires.

Type de numéro
Sélectionnez le type de numéro dans la liste déroulante des types de numéros disponibles. Ces types de numéros doivent exister dans votre système. (Vous ne pouvez pas ajouter de nouveau type de numéro ici. Si vous ne voyez pas le type de numéro que vous voulez utiliser, contactez votre administrateur système pour le créer pour vous.)

Si vous voulez associer un numéro à l'identité que vous ajoutez, vous devez sélectionner un type de numéro.

Valeur Saisissez la valeur du numéro pour le type de numéro sélectionné. Par exemple, si vous associez un passeport avec cette identité, saisissez ici le numéro de passeport.

Si vous voulez associer un numéro à l'identité que vous ajoutez, vous devez saisir une valeur de numéro correspondant au type de numéro.

Emplacement
Saisissez le lieu associé au numéro, s'il est connu ou s'il existe. Par exemple, si vous associez un passeport à cette identité, saisissez ici le nom du pays qui a émis le passeport. Ou saisissez le nom de le lieu de délivrance d'un permis de conduire.

Date de début
Saisissez la date à laquelle ce numéro est devenu valide pour cette identité, si cela est connu. Vous pouvez saisir une date de début sans date de fin.

Date de fin
Saisissez la date à laquelle ce numéro est devenu invalide pour cette identité, si cela est connu. Par exemple, la date d'expiration d'un permis de conduire, d'un passeport ou d'une carte de crédit.

Vous pouvez saisir une date de fin sans date de début.

Liste des caractéristiques
Indiquez une ou plusieurs caractéristiques appartenant ou associées à l'identité que vous ajoutez. Par exemple, si votre système collecte des caractéristiques telles que la date de naissance, le statut marital, la couleur des yeux, ou la taille, vous pouvez saisir chaque caractéristique connue dans cette liste, à raison d'une par ligne. Toutes les caractéristiques que vous saisissez dans cette section de la liste sont automatiquement associées à l'identité que vous ajoutez.

Les caractéristiques ne sont pas obligatoires pour ajouter une identité, alors vous pouvez laisser vide cette section de la liste. Cependant, si vous saisissez des caractéristiques, alors, toutes les zones de caractéristiques sont obligatoires.

Type Sélectionnez le type de caractéristique dans la liste déroulante des types disponibles. Le type de caractéristique doit exister dans votre système. (Vous ne pouvez pas ajouter de nouveau type ici. Si vous ne voyez pas le type de caractéristique que vous voulez utiliser, contactez votre administrateur système pour le créer pour vous.)

Si vous voulez associer une caractéristique à l'identité que vous ajoutez, vous devez sélectionner un type de caractéristique.

Valeur Saisissez la valeur de la caractéristique. Si vous voulez associer une caractéristique à l'identité que vous ajoutez, vous devez saisir une valeur de caractéristique correspondant au type de caractéristique.

Date de début
Saisissez la date à laquelle cette caractéristique est devenu valide pour cette identité, si cela est connu. Vous pouvez saisir une date de début sans date de fin.

Date de fin
Saisissez la date à laquelle cette caractéristique est devenu invalide pour cette identité, si cela est connu. Vous pouvez saisir une date de fin sans date de début.

Liste d'adresses électroniques
Indiquez une ou plusieurs adresses électroniques appartenant ou associées à l'identité que vous ajoutez. Saisissez chaque adresse électronique connue dans cette liste ou une adresse électronique par ligne. Toutes les adresses électroniques que vous saisissez dans cette section de la liste sont automatiquement associées à l'identité que vous ajoutez.

Les adresses électroniques ne sont pas obligatoires pour ajouter une identité, alors vous pouvez laisser vide cette section de la liste. Cependant, si vous saisissez des données d'adresse électronique, alors, les zones **Type** et **Adresse** sont obligatoires.

Type Sélectionnez le type d'adresse électronique dans la liste déroulante des types disponibles. Le type d'adresse électronique doit exister dans votre système. (Vous ne pouvez pas ajouter de nouveau type ici. Si vous ne voyez pas le type d'adresse électronique que vous voulez utiliser, contactez votre administrateur système pour le créer pour vous.)

Si vous voulez associer une adresse électronique à l'identité que vous ajoutez, vous devez sélectionner un type.

Valeur Saisissez l'adresse électronique complète. Si vous souhaitez associer une adresse électronique à l'identité que vous ajoutez, vous devez saisir la valeur d'adresse électronique correspondant au type d'adresse électronique.

Date de début
Saisissez la date à laquelle les informations sur cette adresse électronique sont devenues valides pour cette identité, si cela est connu. Par exemple, si vous connaissez la date à laquelle ce compte d'adresse électronique a été ouvert, vous pouvez le saisir ici.

Vous pouvez saisir une date de début sans date de fin.

Date de fin
Saisissez la date à laquelle les informations sur cette adresse électronique sont devenues invalides pour cette identité, si cela est connu. Par exemple, si vous connaissez la date à laquelle ce compte d'adresse électronique a été fermé, vous pouvez le saisir ici.

Vous pouvez saisir une date de fin sans date de début.

Bouton Soumettre
Pour traiter l'identité via la résolution d'entité et de relation, et ajouter l'identité dans la base de données d'entités, après avoir saisi toutes les informations connues et pertinentes sur l'identité que vous voulez ajouter, cliquez sur **Soumettre**.

Bouton Réinitialiser
Pour effacer toutes les informations saisies dans la fenêtre sans les envoyer, cliquez sur le bouton **Réinitialiser**. L'identité n'est pas traitée via la résolution d'entité et de relation ni ajoutée dans la base de données d'entités.

Fenêtre Ajout d'une divulgation :

Utilisez cette fenêtre pour divulguer une relation entre deux identités existantes. En divulguant la relation, vous créez un lien entre les identités, et entre les entités contenant ces identités. La divulgation d'une relation indique que le lien entre ces deux identités n'a pas encore été détecté par la résolution d'entité et de relation, et que vous avez une raison spécifique pour lier manuellement les deux identités.

ID de l'entité
Saisissez le numéro d'ID d'entité de chaque identité que vous voulez relier, un dans chaque zone **ID d'entité**.

Recherche
Cliquez pour afficher les informations correspondant à l'ID d'entité que vous avez saisi. Faites-le pour les deux numéros d'ID d'entité. En examinant les informations qui s'affichent, vous pouvez vérifier que les ID d'entité correspondent aux identités que vous souhaitez relier. Ou vous pouvez corriger l'ID d'entité pour l'une ou les deux identités avant de les relier.

Boutons d'Option (à côté de chaque identité associée à chaque ID d'entité)
Sélectionnez une identité pour les deux ID d'entité. Ces ID sont les deux identités que vous souhaitez relier.

Remarque : Vous pouvez ne voir qu'une seule identité pour chaque entité, auquel cas cela signifie que cette entité ne possède actuellement qu'une identité dans le système.

Description de la relation divulguée
Saisissez une description de la manière dont sont liées les deux identités sélectionnées. Cette description fournit des informations utiles aux autres utilisateurs de Visualizer, lorsqu'ils affichent cette relation. Elle aide les utilisateurs à comprendre comment et pourquoi ces deux identités sont liées.

Créer Cliquez sur **Créer** pour divulguer la relation entre les deux identités sélectionnées. Le système envoie les informations sur les identités via le pipeline de traitement, puis met à jour les données des deux identités, ainsi que toutes les entités associées à ces identités.

Fenêtre Chargement de fichier UMF :

Utilisez cette fenêtre pour charger les données d'un fichier UMF dans la base de données d'entités via le Visualizer.

Barre d'état de chargement de fichier
Après avoir sélectionné un fichier UMF à ouvrir et à charger, cliquez sur le bouton **Charger le fichier...**, cette barre d'état montre la progression du traitement des données dans le fichier. Le système affiche des statistiques comprenant le pourcentage effectué, le temps écoulé depuis le début du traitement du fichier, ainsi que l'état du traitement du système.

bouton (Continuer)
Si vous avez mis en pause le chargement et le traitement du fichier à l'aide du bouton (Pause), cliquez sur ce bouton pour reprendre le chargement et le traitement des fiches encore non traitées du fichier. Le système continue avec la prochaine fiche du fichier sélectionné.

Bouton (Pause)
Cliquez sur ce bouton si vous voulez temporairement mettre en pause le chargement et le traitement du fichier. Le fichier reste en mémoire, et le système fait un suivi des fiches qui ont déjà été traitées. Toutes les fiches du fichier qui n'ont pas encore été traitées ne sont pas dans la base de données d'entités tant que vous continuez le chargement du fichier.

Ce bouton n'est actif que pendant que le système charge le fichier.

Bouton (Stop)
Cliquez sur ce bouton si vous souhaitez arrêter le chargement et le traitement du fichier. Le fichier est effacé de la mémoire. Toutes les fiches du fichier qui n'ont pas encore été traitées ne sont pas dans la base de données d'entités. Si vous souhaitez continuer le chargement des fiches

dans ce fichier, vous devez recharger le fichier. Pendant le rechargement du fichier, toutes les fiches qui ont déjà été traitées sont de nouveau traitées.

Ce bouton n'est actif que pendant que le système charge le fichier.

Bouton Afficher les résultats
Cliquez sur ce bouton pour afficher la boîte de dialogue **Résultats du chargement de fichier**, comprenant les informations suivantes :

- Le nombre de fiches envoyées dans le pipeline.
- Le nombre de nouvelles entités créées dans la base de données d'entités, sur la base des données du fichier que vous avez chargé.
- Le nombre d'exceptions UMF que le pipeline a rencontrées pendant le traitement des données dans ce fichier. (Ce nombre peut indiquer des erreurs dans le fichier UMF ou des problèmes de syntaxe qui empêchent le pipeline de traiter complètement les données. Contactez votre administrateur système pour corriger les exceptions UMF. Pour obtenir plus de détails, votre administrateur système peut consulter un journal des exceptions UMF.)
- Le nombre d'alertes de rôle créées, conformément aux données du fichier que vous avez chargé.

Bouton Charger le fichier...
Cliquez sur ce bouton pour charger le fichier dans le pipeline, et commencer le traitement de chaque fiche du fichier pour la résolution d'entité et de relation.

Fenêtre Fichier de validation UMF :

Utilisez cette fenêtre pour valider des données dans un fichier UMF que vous voulez charger et traiter via une résolution d'entité et de relation. En validant d'abord les données, vous pouvez corriger les erreurs potentielles ou les avertissements avant le chargement et le traitement du fichier.

Bouton Valider...
Affiche la fenêtre **Définition de la validation UMF**, dans laquelle vous sélectionnez le fichier UMF à valider, définissez le chemin d'accès et le nom de fichier de l'erreur et le fichier journal d'avertissement, et lancez le processus de validation UMF.

Si vous gardez ouverte la fenêtre **Définition de la validation UMF** et que vous validez un autre fichier UMF, lorsque vous cliquez sur **Valider...**, les zone du chemin d'accès et du fichier journal sont renseignées avec les emplacements du dernier fichier UMF validé et du fichier journal d'avertissement. Vous pouvez valider de nouveau le même fichier, ou vous pouvez sélectionner un nouveau fichier UMF à valider.

La fermeture de la fenêtre **Définition de la validation UMF** efface les zones du chemin d'accès et du fichier journal.

Exécution de rapports depuis le visualiseur

A partir du Visualizer, vous pouvez afficher et imprimer des rapports qui vous présentent des synthèses statistiques par source de données, ainsi que des rapports qui vous aident à afficher et à gérer les alertes et relations divulguées.

Consulter et imprimer des rapports dans Visualizer

Utilisez les rapports de Visualizer pour consulter des statistiques et des récapitulatifs qualitatifs sur les fichiers de source de données, vous aider à gérer vos alertes affectées, et examiner les relations divulguées, ainsi que les

informations sur les alertes d'événement ou événements. Vous pouvez afficher les rapports en ligne ou imprimer un exemplaire papier.

Pourquoi et quand exécuter cette tâche

Vous pouvez accéder à la plupart des rapports Visualizer depuis le menu **Afficher** ou depuis la barre d'outils. Mais il existe certains rapports que vous pouvez uniquement consulter et imprimer depuis un écran spécifique, tel que le rapport Récapitulatif d'entité ou le rapport Détails des événements.

Les rapports s'affichent dans votre navigateur Web sélectionné à l'aide d'Adobe Acrobat Reader. Adobe Acrobat Reader version 7.0 ou supérieure doit être installée sur votre poste de travail pour afficher et imprimer les rapports Visualizer.

Remarque : Les horodatages générés par le système et imprimées sur les rapports d'un client Visualizer sont réglés sur le fuseau horaire du serveur d'application Visualizer. Les dates s'affichent comme parfaitement réglées pour le fuseau horaire du client Visualizer lorsqu'elles s'affichent à l'écran. Par exemple, un client Visualizer EST connecté à un serveur d'application Visualizer PST affiche les date et heure générées par le système de 8:00 PM à l'écran, mais il imprime 5:00 PM sur un rapport de client Visualizer EST.

Procédure

- Pour afficher un rapport Historique du générateur d'attribut, un rapport Générateur d'attribut, un rapport Alerte d'attribut, un rapport Récapitulatif de source de données, un rapport de Divulgation, un rapport Récapitulatif de chargement, ou un rapport Etat de l'alerte de rôle, procédez comme suit :
  1. Cliquez sur **Afficher** > **Rapports**, puis sélectionnez le rapport que vous voulez afficher ou imprimer.
  2. Renseignez les critères du rapport.
  3. Cliquez sur **Exécuter le rapport** afin de générer le rapport sélectionné.
- Pour afficher un rapport Récapitulatif d'entité, dans l'écran **Récapitulatif d'entité**, cliquez sur **Rapport**.
- Pour afficher un rapport Détail d'alerte de rôle, dans l'écran **ID d'alerte de rôle**, cliquez sur **Rapport**.
- Pour afficher un rapport Détail des événements, dans l'écran **ID d'événement**, cliquez sur **Rapport**.
- Pour afficher un rapport Tous les événements, dans l'écran **Evénements d'entité**, cliquez sur **Rapport**.

Résultats

Le système génère le rapport sélectionné en fonction de l'ensemble des critères spécifiés et l'affiche dans une fenêtre distincte. Si vous souhaitez imprimer le rapport, cliquez sur le bouton de l'icône de **l'Imprimante** ou utilisez la fonction **Imprimer** de votre navigateur Web.

Rapport de l'Historique du générateur d'alerte d'attribut :

Le rapport de l'Historique du générateur d'alerte d'attribut dresse la liste des modifications apportées aux générateurs d'alerte d'attribut, telles que les modifications dans les dates d'expiration, numéros de dossier, commentaires ou état. Le rapport est trié par ID d'entité de recherche.

Entité de recherche
Affiche l'ID d'entité (et le nom, s'il est donné) tiré des critères de recherche du générateur d'alerte d'attribut.

Date et heure de création
Affiche la date et l'heure auxquelles ce générateur d'alerte d'attribut a été créé.

Section Historique
Cette section du rapport vous présente chaque mise à jour du générateur d'alerte d'attribut, en commençant par la mise à jour la plus récente (la dernière).

Commentaire
Affiche les commentaires qui ont été saisis par l'utilisateur qui a effectué la mise à jour.

Date et heure de la mise à jour
Indique la date et l'heure de la dernière modification de ce générateur d'alerte d'attribut. Si ce générateur d'alerte d'attribut n'a pas été modifié, la date et l'heure sont identiques à la **Date et heure de création**.

Date et heure d'expiration
Affiche la date et l'heure auxquelles ce générateur d'alerte d'attribut doit expirer, ou la dernière date à laquelle il générera des alertes d'attribut.

Etat Indique si le générateur d'alerte d'attribut est actif ou s'il a expiré.

Utilisateur
Affiche le nom de l'utilisateur qui a effectué cette mise à jour.

Groupe d'analystes
Indique le nom du groupe d'analystes du Visualizer auquel appartient le dernier utilisateur à avoir modifié ce générateur d'alerte d'attribut.

Score de Score de résolution
Affiche le score de résolution minimum ainsi que la description du score minimum sélectionné dans le cadre des critères du générateur d'alerte d'attribut. Ce seuil de score indique le degré de concordance nécessaire de l'attribut pour générer une alerte pour ce générateur d'alerte d'attribut. Ainsi, "Est l'entité" est la concordance la plus étroite possible, et "Toute relation" est la concordance la plus lointaine possible. Vous pouvez définir le seuil de chacun de ces scores dans l'écran **Préférences système** dans la fenêtre **Configurer les préférences d'écran**.

Code raison
Affiche le code sélectionné par l'utilisateur indiquant la raison du générateur d'alerte d'attribut.

Numéro du dossier
Affiche le numéro de dossier alphanumérique facultatif, saisi par l'utilisateur qui a créé le générateur d'alerte d'attribut.

Rapport du Générateur d'alerte d'attribut :

Utilisez le rapport du Générateur d'alerte d'attribut pour gérer les générateurs d'alerte d'attribut. En consultant ce rapport, vous pouvez voir un récapitulatif rapide de tous les générateurs d'alerte d'attribut du système, y compris la date et

l'heure auxquelles chacun d'entre eux a été créé, sa date et heure d'expiration, son état et la date et l'heure de sa dernière mise à jour. Le rapport est trié par ID d'entité de recherche.

Entité de recherche
Indique l'ID de l'entité de recherche créée par le Générateur d'alerte d'attribut.

Date et heure de création
Indique la date et l'heure auxquelles le Générateur d'alerte de rôle a été créé.

Commentaire
Affiche le texte de commentaire ajouté par un utilisateur dans le cadre du générateur d'alerte d'attribut.

Date et heure de la mise à jour
Indique la date et l'heure de la dernière modification de ce Générateur d'alerte d'attribut. Si ce générateur d'alerte d'attribut n'a pas été modifié, la date et l'heure sont identiques à la **Date et heure de création**.

Date et heure d'expiration
Indique la date et l'heure auxquelles le générateur d'alerte d'attribut doit expirer.

Etat Etat actuel de ce Générateur d'alerte d'attribut, correspondant à la date et heure de la dernière mise à jour de ce Générateur d'alerte d'attribut.

Utilisateur
Indique le dernière utilisateur qui a modifié ce Générateur d'alerte d'attribut. Si le générateur d'alerte d'attribut n'a jamais été modifié, ce nom d'utilisateur est celui de l'utilisateur qui a créé le générateur d'alerte d'attribut initial.

Groupe d'analystes
Indique le nom du groupe d'analystes auquel appartient le dernier utilisateur à avoir modifié ce générateur d'alerte d'attribut.

Score de Score de résolution
Affiche la sélection dans la liste déroulante **Score minimum** lorsque le générateur d'alerte d'attribut a été créé. Ce seuil de score indique le degré de concordance nécessaire de l'attribut pour générer une alerte pour ce générateur d'alerte d'attribut.

Le seuil de chacun de ces scores se configure dans l'onglet **Préférences système**, qui fait partie de la boîte de dialogue **Configurer les préférences d'affichage**, accessible via le menu **Fichier**.

Code raison
Code sélectionné par l'utilisateur indiquant la raison du générateur d'alerte d'attribut.

Numéro du dossier
Numéro de dossier alphanumérique facultatif, saisi par l'utilisateur qui a créé le générateur d'alerte d'attribut.

Rapport d'alerte d'attribut :

Utilisez le rapport d'alerte d'attribut pour gérer les alertes d'attribut individuelles. En consultant ce rapport, vous découvrez une liste de toutes les entités qui ont concordé avec les critères du générateur d'alerte d'attribut, ainsi que l'état et l'activité la plus récente concernant l'alerte.

Le rapport est trié par ordre croissant d'ID d'entité de recherche. S'il existe plusieurs entités concordantes par entité de recherche, celles-ci sont triées par ordre croissant d'ID d'entité.

Entité de recherche
Affiche l'ID d'entité créé par la recherche d'alerte d'attribut.

Entité correspondante
Affiche l'ID et le nom de l'entité qui a concordé avec l'entité de recherche, en se basant sur les critères du générateur d'alerte d'attribut. Si une alerte d'attribut compte plus d'une seule entité correspondante, elles s'affichent par ordre alphanumérique d'ID d'entité. Ainsi, `l'ID d'entité 37` s'affiche avant `l'ID d'entité 1003`.

Informations sur l'alerte d'attribut
Cette section du rapport affiche des informations générales sur les résultats d'une alerte.

Etat de l'alerte d'attribut
Affiche l'état actuel de cette alerte d'attribut.

Date et heure du résultat de la recherche
Affiche la date et l'heure auxquelles l'alerte d'attribut a été créée.

Etat de la recherche d'attribut
Affiche l'état actuel du générateur d'alerte d'attribut qui a généré cette alerte d'attribut.

Score de résolution minimum
Affiche le score de résolution minimum ainsi que la description du score minimum sélectionné dans le cadre des critères du générateur d'alerte d'attribut. Ce seuil de score indique le degré de concordance nécessaire entre les attributs pour générer une alerte d'attribut.

Information sur l'état de l'alerte d'attribut
Dans cette section du rapport figure l'historique de chaque état de cette alerte. Les informations sur l'état s'affichent par ordre de mise à jour de sorte que la dernière mise à jour d'état figure en premier.

Date et heure de l'état
Affiche la date et l'heure auxquelles a eu lieu la mise à jour de l'alerte d'attribut.

Utilisateur
Affiche le nom de l'utilisateur qui a mis l'alerte à jour.

Code d'activité
Affiche le code défini par l'utilisateur qui indique l'action effectuée par un utilisateur sur cette alerte d'attribut. Lorsque des utilisateurs mettent les alertes à jour, ils sélectionnent un code d'activité. Exemples de codes d'activité : Ouvert, Attribué, En attente, Fermé. Les codes d'activité sont configurés dans la Console de configuration.

Etat Affiche l'état de la disposition de cette mise à jour d'alerte, modifié à l'heure et à la date de l'état. Les états de disposition s'affichent dans l'ordre de la mise à jour, de sorte que la dernière mise à jour d'état est présentée en dernier.

Commentaire
Affiche les commentaires saisis par l'utilisateur lorsqu'il a fait la mise à jour de cette alerte.

Informations sur les entités mises en correspondance
Cette section montrent quels attributs par type et valeur de données ont concordé entre entité de recherche et entité correspondante.

Type de données
Affiche le nom de l'attribut qui a fait correspondre l'entité de recherche avec l'entité mise en concordance. Les deux valeurs de cet attribut mis en concordance s'affichent dans les colonnes Valeur de concordance et Critères de recherche.

Critères de recherche

Affiche la valeur des données appartenant à l'entité de recherche mise en concordance avec la valeur de concordance dans la colonne Entités mises en concordance.

Valeur de correspondance
Affiche la valeur de données réelle liée à l'entité correspondante, qui correspond aux mêmes type et valeur de données pour l'entité de recherche.

Description de précision
Affiche le texte qui décrit le niveau de précision des critères de recherche et de la valeur de concordance mise en concordance. Les niveaux de précision se configurent au cours de la configuration de résolution d'entité, par attribut.

Précision / Précision max
Le premier nombre est le score de précision, généré par le système, qui indique à quel degré la valeur des critères de recherche a concordé avec celle de Valeur de correspondance. Le second nombre est le score de précision maximum réalisable.

En comparant les deux nombres, vous pouvez déterminer plus précisément le proche degré de concordance entre l'entité de recherche et l'entité correspondante. Ces scores peuvent en outre vous servir à déterminer s'il faut affiner les critères de recherche d'alerte d'attribut.

Ajustement de score
Affiche le nombre associé à cet attribut qui est utilisé pour ajuster à la hausse ou à la baisse le score de résolution pendant la résolution de l'entité. Ce nombre est configuré dans le cadre de la configuration générale de la résolution de l'entité.

Etat récapitulatif de source de données :

L'état récapitulatif de source de données procure un récapitulatif statistique rapide, par source de données, sur les enregistrements chargés dans le système pour traitement. Grâce à ce rapport, vous pouvez voir le nombre total de fiches traitées par ID de chargement. Sur le total de ces fiches chargées, le rapport montre que le nombre de fiches représentant de nouvelles identités ou nouvelles entités, et calcule le pourcentage de fiches qui sont des entités nouvellement créées.

Statistiques par chargement dans la source de données

Date de chargement
Affiche la date à laquelle ce fichier de source de données a été chargé

ID de chargement
Affiche le numéro d'ID de chargement affecté par le système.

Source de données
Affiche le code et la description de la source de données (séparés par un tiret) du fichier de source de données qui a été chargé.

Enregistrements UMF chargés
Indique le nombre total de fiches d'identité de ce fichier de source de données qui a été chargé.

Nouvelles identités
Indique le nombre total de nouvelles identités découvertes dans le fichier de données qui a été chargé. (Ce nombre indique une identité qui n'a pas été préalablement traitée par le système.)

% de nouvelles identités
Indique le pourcentage du total des fiches chargées (Nouvelles identités divisées par les fiches UMF chargées) qui représentent de nouvelles identités.

Nouvelles entités
Indique le nombre total de nouvelles entités créées à partir de ce chargement de données.

% de nouvelles entités
Indique le pourcentage du total des fiches chargées (nouvelles entités divisées par les entités chargées) qui représentent de nouvelles entités.

Diagrammes statistiques par source de données

Enregistrements chargés par source de données
Affiche un histogramme qui montre graphiquement le nombre de fiches, provenant de chaque source de données, qui ont été chargés dans le système, en se basant sur les autres critères du rapport spécifiés. Vous pouvez ainsi voir quelles sources de données ont apporté le plus ou le moins d'enregistrements et comparer ces résultats à vos estimations de chiffres de charge.

- L'axe vertical montre les sources de données par code.
- L'axe horizontal montre le nombre d'enregistrements chargés.

Si le nombre d'enregistrements chargés d'une source de données particulière est moindre qu'escompté, vous pouvez inspecter les fichiers de cette source (vous pouvez également envisager de lancer un état récapitulatif de chargement afin de connaître la qualité des données des fichiers chargés de cette source ; la qualité des données se répercute directement sur le nombre d'enregistrements chargés).

Nouvelles entités par source de données
Affiche un histogramme qui montre graphiquement les sources de données qui ont généré le plus grand nombre de nouvelles entités, en se basant sur les autres critères du rapport spécifiés.

- L'axe vertical montre les sources de données par code.
- L'axe horizontal montre le nombre de nouvelles entités créées.

Rapport de divulgation :

Utilisez ce rapport pour afficher et gérer les relations divulguées entre des identités. Les relations divulguées sont des relations manuellement créées par les utilisateurs du Visualizer dans l'écran **Ajouter des divulgations** ou en intégrant la paire de balises de la relation divulguée (<DR> et </DR>) dans les fiches d'identité entrante.

Le rapport est trié par ID de relation.

ID de relation
Affiche le nombre généré par le système affecté à chaque relation divulguée une fois la relation créée.

Date et heure de création
Affiche la date et l'heure auxquelles la relation divulguée a été créée.

Description de la relation
Affiche le texte décrivant la raison de la création de la relation divulguée. Ce descriptif est saisi par l'utilisateur qui a créé la relation divulguée.

Date et heure de la mise à jour
Affiche la date et l'heure de la dernière mise à jour de cette relation divulguée.

Etat Affiche l'état de cette relation divulguée.

Date de suppression
Affiche la date et l'heure auxquelles la relation divulguée a été manuellement supprimée. Cette zone n'est renseignée avec une date et heure que si un utilisateur a déterminé que la relation n'était pas valide et a donc supprimé la relation divulguée.

Source de données
Fournit le code de source de données et la description des deux entités (pour chacune, sur des lignes séparées) désormais reliées par cette relation divulguée. Le code de source de données désigne le fichier source original.

ID externe
Fournit l'ID externe des deux entités (pour chacune, sur des lignes séparées) désormais reliées par cette relation divulguée. L'ID externe désigne généralement un numéro de compte, au sein du fichier source original, qui appartient exclusivement à l'entité.

Rapport Détail d'alerte d'événement :

Utilisez le rapport Détail d'alerte d'événement pour afficher tous les détails concernant une alerte d'événement spécifique ainsi que les entités impliquées dans l'alerte. Ce rapport est utile lorsque vous voulez un rapport papier de l'onglet **Alerte d'événement** dans la fenêtre **Rechercher**.

ID d'alerte
Affiche la description et l'ID d'alerte d'une alerte d'événement spécifique. L'ID d'alerte apparaît avant la description dans l'en-tête du rapport.

Informations sur l'alerte d'événement
Cette section affiche des informations générales pour l'alerte d'événement globale, et notamment une description de la règle d'alerte d'événement qui a déclenché cette alerte, ainsi que l'état de l'alerte d'événement.

Date et heure de l'alerte
Indique la date et l'heure auxquelles cette alerte d'événement a été créée.

ID de règle
Affiche un numéro interne généré par le système lors de la configuration initiale de la règle d'alerte d'événement. Cet ID est associé à la règle d'alerte d'événement qui a déclenché cette alerte d'événement.

Description de la règle
Texte descriptif de la règle d'alerte d'événement, défini par la personne qui a configuré la règle d'alerte d'événement.

Etat Affiche l'état actuel de cette alerte d'événement.

Détails de l'événement
Cette section donne plus d'informations sur les données de l'alerte d'événement.

Date et heure
Indique la date et l'heure auxquelles cette alerte d'événement a été créée.

Source de données
Affiche, pour chaque événement, le code et la description de la source de données d'où proviennent les données de l'événement. Cette information identifie le fichier source original.

ID externe
Affiche, pour chaque événement, l'ID externe associé au code de source de données d'où proviennent les données de l'événement. Cette information identifie souvent un numéro de compte de l'entité dans le fichier source original.

Référence d'événement
Affiche, pour chaque événement, le code unique créé par le processeur d'événement complexe pendant le traitement des données.

Quantité
Indique pour chaque événement, le nombre représentant la quantité impliquée dans cet événement. Par exemple, 1 peut signifier un virement de la valeur dans la colonne **Valeur**.

Valeur Indique pour chaque événement, la valeur totale de cet événement.

Informations sur l'entité
Pour l'entité impliquée dans l'événement, cette section donne la liste des types d'attribut et de leurs valeurs associées qui ont été impliquées dans l'événement.

Dispositions d'alerte
Cette section propose un récapitulatif des état de l'alerte d'événement.

Code d'activité
Affiche le code d'activité de l'événement sélectionné par l'utilisateur qui a modifié l'état de cette alerte d'événement.

Etat Affiche l'état (actif ou inactif) associé au code d'activité de l'événement.

Commentaires sur l'état
Affiche les commentaires des analystes concernant cette mise à jour de l'état.

Utilisateur
Indique l'ID utilisateur de l'utilisateur qui a modifié l'état de cette alerte d'événement.

Date et heure
Indique la date et l'heure de la modification de l'état.

Section Historique d'alerte d'événement de rôle
Cette section répertorie toutes les alertes de rôle dans lesquelles est impliquée cette entité responsable de cette alerte d'événement.

Section Historique d'alerte d'événement
Cette section du rapport dresse la liste de l'historique complet de l'entité impliquée dans l'alerte d'événement principale. Utilisez cette section pour voir le nombre d'alertes d'événement dans lesquelles est impliquée cette entité.

Date et heure de l'alerte
Indique la date et l'heure auxquelles cette alerte d'événement a été créée.

ID d'alerte
Affiche l'ID de cette alerte d'événement.

Description
Affiche un texte pour décrire la règle de traitement d'événement complexe qui a déclenché cette alerte d'événement.

Code d'activité
Affiche un code, défini par l'utilisateur, qui indique une action effectuée par un utilisateur sur cette alerte. Les codes d'activité sont configurés dans la Console de configuration et sont sélectionnés dans une liste déroulante du Visualizer quand une alerte est mise à jour. Certains exemples de code d'activité comprennent : Affecté, Fermé et En attente.

Etat Affiche l'état de la mise à jour de cette alerte, modifié aux date et heure de l'état. Les états s'affichent par ordre de mise à jour de sorte que la dernière mise à jour d'état figure en dernier.

Rapport Tous les événements :

Utilisez le rapport Tous les événements pour afficher tous les événements associés à une seule entité, que les événements aient ou non généré une alerte d'événement. Le rapport est utile lorsque vous voulez un rapport papier de l'écran **Evénements d'entité** dans la fenêtre **Rechercher**. Les événements qui s'affichent dans le rapport dépendent du type d'événement et de l'intervalle de dates que vous avez sélectionné dans cet écran.

Si vous n'avez pas sélectionné de type d'événement, le rapport affiche les événements de tous les types pour l'entité donnée, dans l'intervalle de dates défini. Si vous avez sélectionné un type d'événement, seuls s'affichent les événements de ce type dans l'intervalle de dates défini.

Informations de base du rapport
Cette section fournit des informations de base dans le titre du rapport, telles que l'intervalle de dates du rapport, et plus d'informations sur l'entité associée à ces événements.

Dates du rapport : Début et fin
Indique les dates de début et de fin du rapport. Seuls les événements qui ont eu lieu dans cet intervalle de dates pour cette entité s'affichent dans le rapport.

Entité associée
Indique l'ID d'entité de l'entité associée à ces événements.

Nom actuel
Indique le nom le plus courant de l'entité dans la base de données d'entités.

Adresse actuelle
Indique l'adresse la plus courante de l'entité dans la base de données d'entités.

Informations sur l'événement
Cette section donne les détails des événements associés à cette entité, par type d'événement.

Type d'événement
Décrit le type d'événement. Cette description est configurée avec le type d'événement dans la Console de configuration.

ID d'événement
Affiche le numéro généré par le système qui identifie cet événement spécifique.

Date et heure de création
Affiche la date et l'heure auxquelles l'événement s'est produit.

Source de données
Affiche le code de source de données ainsi que la description de la source de données associés à l'événement.

ID externe
Affiche la clé unique qui identifie la fiche d'identité entrante dans la source de données d'origine de cet événement.

Référence d'événement
Affiche les informations supplémentaires concernant l'événement. En règle générale il s'agit du nom du lieu où s'est produit l'événement.

Emplacement
Affiche les informations d'adresse du lieu où l'événement s'est produit.

Valeur Affiche le montant en valeur associé à l'événement.

Quantité
Affiche le nombre d'unités associées à l'événement.

Unité de mesure
Indique l'unité de mesure associée à la valeur de l'événement. L'unité de mesure est configurée par type d'événement dans la Console de configuration. L'unité de mesure vous aide à comprendre la valeur. Par exemple, si l'unité de mesure est le

dollars US et que la valeur de l'événement est 5000, vous savez que cet événement impliquait une valeur de 5000,00 $US.

Mémo ou *Etiquette personnalisée*
Affiche des informations supplémentaires sur l'événement, telles que des notes ou commentaires, qui peuvent fournir davantage de contexte pour la transaction d'événement.

Les utilisateurs peuvent définir une étiquette personnalisée pour cette colonne, ce qui est une des options possibles lors de la configuration d'un type d'événement dans la Console de configuration. Au lieu du **Mémo**, vous pouvez souhaiter une étiquette personnalisée plus descriptive. Par exemple, **Notes sur le virement**.

Mémo ou *Etiquette personnalisée* supplémentaire
Affiche plus d'informations sur l'événement, si elles sont disponibles.

Les utilisateurs peuvent définir une étiquette personnalisée pour cette colonne, ce qui est une des options possibles lors de la configuration d'un type d'événement dans la Console de configuration. Au lieu du **Mémo supplémentaire**, vous pouvez souhaiter une étiquette personnalisée plus descriptive, comme par exemple,**Commentaires de l'agent**.

Rapport récapitulatif de chargement :

Le rapport Récapitulatif de chargement récapitule les statistiques et les caractéristiques de qualité par source de données. Il contient des informations sur les fichiers sources de données. Utilisez ce rapport pour déterminer les statistiques de chargement, le nombre de résolutions d'entité et d'alertes générées par ce chargement, les informations générales sur la qualité des données des données chargées, un récapitulatif des actions concernant les fiches UMF par chargement, et toutes les exceptions UMF générées par chargement. Le rapport est trié par ID de chargement.

Pour chaque chargement, le rapport décompose les statistiques en sections :

- Récapitulatif de chargement
- Récapitulatif d'alerte de rôle
- Récapitulatif des relations
- Récapitulatif qualitatif
- Récapitulatif des documents UMF
- Récapitulatif des exceptions

Récapitulatif de chargement

Utilisez cette section pour vous aider à déterminer le temps qui a été nécessaire au traitement d'un fichier spécifique, et vous donner une idée générale de l'utilité de ce fichier de source de données dans la résolution d'entité et la détection de relation.

Date et heure de démarrage
Indique la date et l'heure du début de chargement des données.

Date et heure de fin
Indique la date et l'heure de fin du chargement du fichier de source de données.

Nombre d'enregistrements UMF
Indique le nombre total de fiches chargées depuis ce fichier de source de données dans l'intervalle **Date et heure de début** et **Date et heure de fin**.

La valeur de la **Date et heure de fin** moins la valeur de la **Date et heure de début** correspond au nombre de minutes nécessaires au chargement de ce fichier de source de données, ce qui vous donne une idée des performances du système. Cela peut également indiquer qu'un fichier de source de données plus volumineux doit être scindé en fichiers plus petits pour accélérer le traitement.

Nouvelles identités
Indique le nombre total de nouvelles identités chargées dans l'intervalle **Date de début** et **Date de fin**.

% de nouvelles identités
Indique le pourcentage de nouvelles identités sur le total des identités de ce chargement de données (identités nouvelles dans la base de données d'entités).

Nouvelles entités
Indique le nombre total d'entités nouvellement créées dans l'intervalle **Date de début** et **Date de fin**.

% de nouvelles entités
Indique, sur le total d'entités, le pourcentage d'entités nouvellement créées suite à ce chargement de source de données.

Le nombre de nouvelles identités et de nouvelles entités peut vous procurer une idée générale de l'intérêt global de cette source de données en termes de résolution d'entité et de détection de relation. Si ces chiffres sont faibles et restent faibles sur le long terme, il se peut que cette source de données ne soit pas utile pour atteindre les objectifs de résolution d'entité de votre entreprise.

Récapitulatif d'alerte de rôle

Utilisez cette section pour consulter les règles et scores de résolution communs aux relations détectées qui ont débouché sur des alertes de rôle. Chaque ligne représente le nombre d'alertes de rôle qui ont été générées, selon les critères mentionnés.

Règle de résolution
Affiche le nom de la règle de résolution utilisée pour évaluer l'identité et l'entité pendant la résolution d'entité et la détection de relation.

Description d'alerte
Affiche le nom de la règle d'alerte de rôle qui a déclenché l'alerte de rôle.

Gravité
Affiche un indicateur défini par l'utilisateur, servant à mesurer la priorité ou l'importance de cette alerte de rôle.

Score de résolution
Affiche un score de résolution (0-100) pour la règle de résolution donnée à l'identité et à l'entité impliquées dans l'alerte de rôle. Ce score indique le degré de ressemblance entre l'identité et l'entité. Un score de 100 signifie que l'enregistrement d'identité a été résolu sous la forme de l'entité.

Nombres d'alertes
Indique le nombre total d'alertes de rôle générées sur la base de la description de la règle d'alerte de rôle, la règle de résolution et le score de résolution.

Récapitulatif des relations

Cette section permet de consulter les attributs communs aux relations détectées qui n'ont pas déclenché d'alerte de rôle. Chaque ligne représente le nombre de relations qui ont été détectées, selon les critères mentionnés.

Règle de résolution
Affiche le nom de la règle de résolution utilisée pour évaluer les fiches d'identité entrantes et les entités existantes pendant la résolution d'entité et la détection de relation.

Score de résolution
Affiche un score de résolution (0-100) pour la règle de résolution donnée à l'identité et à l'entité pendant la résolution d'entité. Ce score indique le degré de ressemblance entre l'identité et l'entité. Un score de 100 signifie que l'enregistrement d'identité a été résolu sous la forme de l'entité.

Score de relation
Affiche un score de relation (0-100) pour la règle de résolution donnée à l'identité et à l'entité pendant la résolution de relation. Ce score indique le degré de relation entre l'identité et l'entité.

Plus le score de relation est élevé, plus l'identité et l'entité sont étroitement apparentées, selon les attributs concordants.

Nombre de relations
Indique le nombre total de relations détectées sur la base de cette règle de résolution, du score de résolution et du score de relation.

Récapitulatif qualitatif

Consultez les informations de cette section pour évaluer la qualité des données de chaque fichier source. Cette section indique la qualité par type d'attribut au sein d'un type de segment UMF et de document UMF. En consultant le récapitulatif qualitatif avec celui des exceptions UMF, vous pouvez savoir quels fichiers sources de données posent des problèmes de qualité ou d'UMF défectueux qu'il importe de régler. Vous pouvez généralement remédier à ces problèmes via la configuration ETL ou DQM/de source de données avant de traiter le fichier de source de données.

Dans certains cas, cette section peut révéler qu'une source de données est de qualité si médiocre qu'il ne faudrait plus l'utiliser pour la résolution d'entité.

Type de document
Affiche le nom du type de document UMF qui contient le type de données mentionné dans le Type de données. Cette valeur est généralement UMF_ENTITY.

Nom de la table
Affiche le nom de la table de base de données qui conserve les données provenant de segments UMF ayant le même nom. Par exemple, les données provenant du segment NUMBER sont stockées dans la table NUMS.

Type de données
Indique le type de données, tel que mentionné dans les balises UMF de type d'attribut des fiches entrantes. Ce type correspond à un segment UMF figurant dans le nom de table. Par exemple, si le nom de table est *ADDRESS* et que le type de données mentionné est *H*, les informations qualitatives évaluent le type d'adresse *Domicile*.

Si vous ne reconnaissez pas un type de données, vous pouvez indiquer que le fichier de source de données n'est pas correctement mappé à la combinaison de documents, segments et balises UMF. Vérifiez dans la section de récapitulatif des exceptions si un segment UMF et une balise UMF concordants ont provoqué des exceptions de segment. Si le problème provient d'un UMF invalide, les chiffres du Pourcentage inutilisable de la section Récapitulatif qualitatif et le Nombre d'exceptions de segment dans la section des exceptions UMF sont généralement concordants.

Nombre d'enregistrements
Indique le nombre total de fiches d'identité entrantes pour le Type de document, le Nom de table et le Type de données spécifiés.

Nombre générique
Indique le nombre total de fiches d'identité entrantes avec le Type de document, le Nom de table et le Type de données spécifiés dont les valeurs sont considérées comme génériques.

Pourcentage inutilisable
Indique le nombre total de fiches d'identité entrantes avec le Type de document, le Nom de table et le Type de données spécifiés qui sont considérées comme inutilisables. Ce nombre peut révéler un problème de saisie de données ou de transformation ETL dans le fichier de source de données.

Pourcentage utilisable
Indique le pourcentage de fiches d'identité entrantes avec le Type de document, le Nom de table (de ce segment UMF) et le Type de données spécifiés comme utilisables pour la résolution d'entité et la détection de relation. (Nombre de fiches moins le Nombre générique moins le Pourcentage inutilisable) divisé par le Nombre de fiches équivaut au Pourcentage utilisable.

Pourcentage d'identité
Indique le pourcentage de fiches d'identité entrantes qui contenaient le type de document, le nom de table et le type de données spécifiés.

Récapitulatif d'attribut

Cette section permet de consulter dans le fichier de source de données les attributs qui ont contribué à détecter les relations et à déclencher des alertes de rôle. Chaque attribut est associé à un segment UMF spécifique, et cette section montre le nombre de relations détectées et d'alertes de rôle déclenchées, selon les données présentes dans le segment UMF entrant.

Nom du segment
Affiche le nom du segment UMF qui correspond directement à un attribut.

Type de données
Mentionne le type d'attribut (ou type de données), au sein du segment UMF, qui correspond à la description de la précision. Il se peut que le rapport mentionne soit un type d'attribut particulier, soit *TOUS*, ce qui indique tous les types d'attribut du segment UMF.

Description de précision
Décrit le seuil de concordance entre un attribut d'une entité entrante et un attribut d'une entité existante.

Alertes de rôle
Indique le nombre total d'alertes de rôle générées sur ce segment UMF, ce type de données, et cette description de précision.

Relations
Indique le nombre total de relations détectées sur ce segment UMF, ce type de données et cette description de précision

Récapitulatif des documents UMF

Vous pouvez utiliser cette section pour valider le nombre total de fiches entrantes dans un fichier de source de données, en fonction de l'action qui doit être effectuée sur la fiche. Vous pouvez réconcilier ces nombres en Nombre d'enregistrements dans la section Récapitulatif de chargement.

Type de document
Affiche le nom du type de document UMF. Cette valeur est généralement UMF_ENTITY.

Action
Indique l'action à appliquer à l'enregistrement d'identité entrant. La liste suivante répertorie les actions les plus couramment utilisées :

- *A* : ajout
- *C* : modification
- *D* : suppression

Dans le cadre du processus ETL (extraction, transformation et chargement), les enregistrements d'identité sont généralement étiquetés au moyen du format UMF afin d'indiquer quelle action effectuer sur chacun au cours du traitement par le système.

Nombre d'enregistrements UMF
Indique le nombre total de fiches traitées pour chaque type d'action dans un type de document.

Pourcentage
Indique le pourcentage du total des fiches chargées représenté par le Nombre de fiches. (la somme ne doit pas dépasser 100%).

Récapitulatif des exceptions

Ces informations aident à repérer les enregistrements d'identité défectueux, tels que ceux dont le format UMF est syntaxiquement incorrect. L'exception décrit le problème, tandis que le nom de table et l'élément indiquent les segments et enregistrements défectueux. Le comptage montre combien d'enregistrements du fichier comportaient ce format UMF incorrect.

Type de document
Affiche le nom du type de document UMF. Cette valeur est généralement UMF_ENTITY.

Action
Indique le type d'action pour la fiche d'identité entrante :

- *A* : ajout
- *C* : modification

- *D* : suppression

Dans le cadre du processus ETL (extraction, transformation et chargement), les enregistrements d'identité sont généralement étiquetés au moyen du format UMF afin d'indiquer quelle action effectuer sur chacun au cours du traitement par le système.

Segment
Affiche le nom du segment UMF sur lequel l'exception s'est produite.

Balise UMF
Affiche la valeur de la balise UMF qui a provoqué l'exception UMF.

Exception
Affiche l'ID de message ou autre code d'exception indiquant le type d'exception UMF qui s'est produite et donne des informations sur la manière de résoudre cette exception. Cette information est également disponible dans la table UMF_EXCEPT.

Nombre d'exceptions de segment
Indique le nombre total de ce type d'exception UMF.

Vérifiez le pourcentage inutilisable à la section Récapitulatif qualitatif pour savoir si un type de données concordant est signalé comme étant de qualité médiocre ou inutilisable. Si le problème provient d'un format UMF incorrect, le nombre Pourcentage inutilisable de la section Récapitulatif qualitatif et le nombre d'exceptions de segment de la section Exceptions UMF concordent généralement pour le même segment UMF et les mêmes balises UMF.

Rapport détaillé du conflit :

Utilisez le rapport Détail d'alerte de rôle pour consulter tous les détails d'une alerte de rôle spécifique, ainsi que les entités impliquées dans l'alerte à chaque degré de séparation. Ce rapport s'avère pratique quand vous souhaitez approfondir l'analyse des entités impliquées dans chaque alerte de rôle.

Pour chaque degré de séparation, le rapport affiche les informations sur les deux entités impliquées dans l'alerte afin que vous puissiez les comparer et les confronter. Le rapport affiche ensuite les autres alertes associées à chaque entité afin que vous disposiez d'un panorama complet de chaque entité et des alertes de rôle associées. Généralement, le détail de chaque alerte de rôle s'étend sur plusieurs pages.

ID d'alerte
Description et ID d'alerte d'une alerte de rôle précise. L'ID d'alerte apparaît avant la description dans l'en-tête du rapport.

Informations sur l'alerte de rôle
Cette section affiche des informations générales pour l'alerte de rôle globale, et notamment une description de la règle d'alerte de rôle qui a déclenché cette alerte, ainsi que l'état de l'alerte de rôle.

Date et heure de l'alerte
Date et heure où cette alerte de rôle a été générée.

ID de règle
Numéro interne généré par le système lors de la configuration initiale de la règle d'alerte de rôle, cet ID est associé à la règle d'alerte de rôle qui a déclenché cette alerte de rôle.

Description de la règle
Texte descriptif de la règle d'alerte de rôle, défini par la personne qui a configuré la règle.

Gravité
Code, défini par l'utilisateur, servant à mesurer la priorité ou l'importance de cette alerte.

Etat Disposition actuelle de cette alerte de rôle

Niveau de fiabilité de relation
Score qui indique le degré de parenté des deux entités figurant dans la section Détails de la correspondance : degré *n*. Plus le score est élevé, plus elles sont étroitement apparentées. Un score de 100 indique que l'entité entrante et l'entité concordante sont la même entité.

Le score de niveau de fiabilité de relation est généré par le système, dans le cadre du processus de résolution d'entité.

Score de résolution
Score qui indique le degré de concordance de deux entités. Plus le score est élevé, plus elles concordent étroitement. Un score de 100 indique que l'entité entrante et l'entité concordante sont la même entité.

Le score de résolution est généré par le système, dans le cadre du processus de résolution d'entité.

Niveau de fiabilité de résolution
Score de résolution de base configuré dans le cadre de la résolution d'entité et qui représente le score minimum à atteindre pour résoudre l'entité entrante et l'entité concordante en une même entité. Généralement, le score de résolution et le score de niveau de fiabilité de résolution sont identiques.

Section Détails de la correspondance : degré *n*
Cette section fournit les détails de correspondance des entités impliquées dans l'alerte ainsi que les renseignements identitaires des entités respectives. Les deux entités sont représentées en tant que Entité *x* (identité entrante) et Entité *y* (identité concordante).

Pour chaque entité et chaque type de données d'attributs, le rapport indique les valeurs de données concordantes, ainsi que la source de données et l'ID externe associé aux valeur de données de chaque entité. Le rapport affiche ensuite les descriptions de la précision et les scores des attributs concordants. Si l'un des attributs concordants est Nom, il se peut que le rapport affiche également le détail sur le barème de score que la résolution d'entité a appliqué aux noms, en fonction des options de score de nom qui sont configurées pour la résolution d'entité.

Type de données
Nom de l'attribut concordant.

Valeur Valeur de données qui a concordé.

Source de données
Pour chaque entité, code et description de la source de données d'où proviennent l'attribut et la valeur de données concordants. Cette information identifie le fichier source original.

ID externe
Pour chaque entité, ID externe associé au code de source de données d'où proviennent l'attribut et la valeur de données concordants. Cette information identifie souvent un numéro de compte de l'entité dans le fichier source original.

Description de précision
Texte qui décrit le niveau de précision auquel les entités ont concordé.

Les niveaux de précision se configurent au cours de la configuration de résolution d'entité, par attribut.

Précision / Précision max
Le premier nombre correspond au score de précision généré par le système, qui indique le degré de concordance entre l'Entité *x* (identité entrante) et l'Entité *y* (identité concordante). Le second nombre est le score de précision maximum réalisable.

En comparant les deux nombres, vous pouvez déterminer plus exactement le degré de concordance entre les entités, notamment l'intérêt d'une exploration plus poussée de la concordance. Ces scores peuvent en outre vous servir à déterminer s'il faut affiner les critère de recherche d'alerte.

Ajustement de score
Le score de résolution a été modulé selon ce nombre. Ce nombre se configure au cours de la configuration de la résolution d'entité.

Détails du score de nom
Si l'un des attributs concordants est le type de données Nom, il se peut que le rapport renseigne également en détail sur le barème de score que le processus de résolution d'entité a appliqué aux concordances de nom. Pour que cette section du rapport s'affiche, il faut que l'une au moins des options de nom suivantes soit configurée dans le cadre de la résolution d'entité :

- Gestionnaire de noms
- Name Comparator 2

Nom complet
Score (0-100) qui indique le degré de concordance du nom complet des deux entités. Ce score se configure dans le cadre de la résolution d'entité.

Nom Score (0-100) qui indique le degré de concordance du nom de famille des deux entités. Ce score se configure dans le cadre de la résolution d'entité.

Prénom
Score (0-100) qui indique le degré de concordance du prénom complet des deux entités. Ce score se configure dans le cadre de la résolution d'entité.

Section Informations sur l'identité des Entités *x* et *y*
Cette section du rapport dresse la liste des informations spécifiques concernant chaque identité.

Type de données
Nom de la caractéristique. (Par exemple, Nom.)

Valeur Valeur de la caractéristique. (Par exemple, SMITH, BRUCE.)

Section Autres alertes pour l'entité *x* et *y*

Cette section du rapport affiche l'historique d'alerte de rôle de toutes les autres alertes de rôle et relations associées à la fois à l'entité entrante (entité *x*) et à l'entité concordante (entité *y*). Elle affiche également l'historique d'alerte d'événement de toutes les alertes événement associées à l'entité entrante (Entité *x*) et à l'entité concordante (Entité *y*). Ces informations peuvent offrir un tableau plus complet de chaque entité, de ses alertes et relations associées avec d'autres entités, ce qui peut vous aider dans votre analyse.

Historique de conflit

Contient les informations de l'historique d'alerte de rôle du Récapitulatif d'entité.

Date et heure de l'alerte

Date et heure auxquelles l'alerte de rôle a été créée.

ID d'alerte

Description et ID de cette alerte de rôle.

Description

Texte descriptif de la règle d'alerte de rôle qui a déclenché cette alerte.

ID de l'entité

Numéro d'ID de l'entité de cette ligne qui a concordé avec l'entité mentionnée par numéro dans Autres alertes pour l'entité *n*.

Nom Nom de l'autre entité qui a concordé avec l'entité mentionnée par numéro dans Autres alertes pour l'entité *n*.

Relations

Nombre de relations associées à l'entité apparentée.

Score de relation

Score qui indique le degré de parenté de deux entités. Plus le score est élevé, plus elles sont étroitement apparentées. Un score de 100 indique que l'entité entrante et l'entité concordante sont la même entité.

Ce score est généré par le système, dans le cadre du processus de résolution d'entité.

Code d'activité

Code, défini par l'utilisateur, qui indique une action effectuée par une personne sur cette alerte. Les codes d'activité se définissent dans la console de configuration et se sélectionnent dans une liste déroulante du visualiseur quand une alerte est mise à jour. Exemples de codes d'activité : Ouvert, Attribué, En attente, Fermé.

Etat Etat de la disposition de cette mise à jour d'alerte, modifiée aux date et heure de l'état. Les états s'affichent par ordre de mise à jour de sorte que la dernière mise à jour d'état figure en dernier.

Historique des alertes d'événement

Contient des informations provenant de l'Historique d'alerte d'événement du Récapitulatif d'entité.

Date et heure de l'alerte
Date et heure auxquelles cette alerte a été générée.

ID d'alerte
Identifiant unique généré par le système pour l'alerte d'événement.

Description
Description de l'alerte événement, depuis la configuration de l'événement dans la Console de configuration.

Rapport de l'état du conflit :

Le rapport de l'état du conflit récapitule l'état de toutes les alertes de rôle d'une heure donnée. Il permet de consulter et gérer les alertes de rôle.

Le rapport est trié par ID d'alerte de rôle et date et heure d'alerte.

ID d'alerte - description
Affiche l'ID d'alerte de rôle généré par le système, ainsi que la description de l'alerte de rôle, obtenue auprès de la règle d'alerte de rôle associée.

Date et heure de l'alerte
Indique la date et l'heure auxquelles l'alerte de rôle a été créée.

Informations sur l'entité correspondante
Cette section affiche l'historique de disposition de l'alerte, en commençant par la plus récente mise à jour de l'état.

Entité 1 et entité 2
Affiche les ID de l'Entité, et généralement, le nom complet des deux entités mises en concordance, conformément aux critères de cette alerte de rôle (par la description de l'ID d'alerte).

Code d'activité
Affiche un code, défini par l'utilisateur, qui indique une action effectuée par un utilisateur sur cette alerte. Les codes d'activité se définissent dans la console de configuration et se sélectionnent dans une liste déroulante du visualiseur quand une alerte est mise à jour. Exemples de codes d'activité : Ouvert, Attribué, En attente, Fermé.

Etat Affiche l'état de la disposition de cette mise à jour d'alerte, modifiée aux date et heure de l'état. Les états s'affichent par ordre de mise à jour de sorte que la dernière mise à jour d'état figure en dernier.

Date et heure de l'état
Indique la date et l'heure auxquelles l'état de l'alerte s'est produit.

Utilisateur
Affiche le nom de l'utilisateur qui a mis à jour l'alerte avec cet état.

Rubriques d'aide

Fenêtre de critères du rapport Historique du générateur d'alerte d'attribut :

utilisez cette fenêtre Visualizer pour spécifier les critères d'affichage du rapport de l'Historique du générateur d'alerte d'attribut. Ce rapport peut vous aider à consulter et à auditer les modifications qui ont été apportées aux générateurs d'alerte d'attribut, telles que les modifications dans les dates d'expiration, les

numéros de dossier ou l'état. Si vous voulez consulter les résultats d'un générateur d'alerte d'attribut, affichez le rapport Générateur d'alerte d'attribut.

Date de début
Saisissez la première date de la plage pour afficher les données dans le rapport sélectionné. Appliquez le format `MM/JJ/AAAA`. Par exemple, `01/01/01` correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de début** par défaut est la date d'aujourd'hui.

Date de fin
Saisissez la dernière date de la plage pour afficher les données dans le rapport sélectionné. Appliquez le format `MM/JJ/AAAA`. Par exemple, `01/01/01` correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de fin** par défaut est la date d'aujourd'hui.

Pour afficher les données d'une seule journée, utilisez la même date dans les zones **Date de début** et **Date de fin**.

Liste déroulante Etat
Sélectionnez un état spécifique ou sélectionnez **Tout** pour établir un rapport concernant tous les états des générateurs d'alerte d'attribut. Par exemple, si vous voulez consulter uniquement les modifications apportées aux générateurs d'alerte d'attribut actuellement ouverts dans l'intervalle de dates spécifié, sélectionnez **Ouvrir** dans la liste déroulante.

L'état par défaut dans la liste déroulante **Etat** est **Tout**, qui affiche les générateurs d'alerte d'attribut actifs ainsi que ceux qui ont expiré.

Liste déroulante Utilisateur
Sélectionnez une option pour voir vos générateurs d'alerte d'attribut ou ceux de toute personne appartenant à votre groupe d'utilisateurs Visualizer.

L'option par défaut est `Mes recherches`.

Bouton Exécuter le rapport
Cliquez sur ce bouton pour générer le rapport.

Fenêtre de critères du rapport du Générateur d'alerte d'attribut :

Cette fenêtre permet de définir les critères d'affichage du rapport du générateur d'alerte d'attribut dans Visualizer. Ce rapport peut être utilisé pour gérer vos générateurs d'alertes d'attribut ou les analystes de votre groupe d'utilisateurs Visualizer. Si vous voulez consulter l'historique de modification des générateurs d'alerte d'attribut, utilisez plutôt le rapport Historique de générateur d'alerte d'attribut.

Date de début
Saisissez la première date de la plage . Appliquez le format `MM/JJ/AAAA`. Par exemple, `01/01/01` correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de début** par défaut est la date d'aujourd'hui.

Date de fin
Saisissez la dernière date de la plage. Appliquez le format `MM/JJ/AAAA`. Par exemple, `01/01/01` correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de fin** par défaut est la date d'aujourd'hui.

Pour afficher les données d'une seule journée, utilisez la même date dans les zones **Date de début** et **Date de fin**.

Liste déroulante Etat
Sélectionnez un état spécifique ou sélectionnez **Tout** pour établir un rapport concernant tous les états des générateurs d'alerte d'attribut. Par exemple, si vous voulez consulter uniquement les générateurs d'alerte d'attribut actuellement actifs dans l'intervalle de dates spécifié, sélectionnez **Ouvrir**.

L'état par défaut est **Tout**, ce qui signifie que le rapport affiche les générateurs d'alerte d'attribut actifs ainsi que ceux qui ont expiré.

Liste déroulante Utilisateur
Faites une sélection :

- Pour voir uniquement vos générateurs d'alerte d'attribut, sélectionnez **Mes recherches** (la sélection par défaut).
- Pour voir tous les générateurs d'alerte d'attribut créés par les utilisateurs de votre groupe d'utilisateurs Visualizer, sélectionnez **Mon groupe**.

Bouton Exécuter le rapport
Cliquez sur ce bouton pour générer le rapport.

Fenêtre de critères du rapport Alertes d'attribut :

Utilisez cette fenêtre du Visualizer pour spécifier les critères d'affichage du rapport Alerte d'attribut, qui peut vous aider à consulter et à gérer vos alertes d'attribut.

Date de début
Saisissez la première date de la plage pour afficher les données dans le rapport sélectionné. Appliquez le format `MM/JJ/AAAA`. Par exemple, `01/01/01` correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de début** par défaut est la date d'aujourd'hui.

Date de fin
Saisissez la dernière date de la plage pour afficher les données dans le rapport sélectionné. Appliquez le format `MM/JJ/AAAA`. Par exemple, `01/01/01` correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de fin** par défaut est la date d'aujourd'hui.

Pour afficher les données d'une seule journée, utilisez la même date dans les zones **Date de début** et **Date de fin**.

Liste déroulante Etat
Sélectionnez un état spécifique ou sélectionnez **Tout** pour établir un rapport concernant toutes les alertes d'attribut. Par exemple, si vous voulez consulter uniquement les modifications apportées aux alertes d'attribut actuellement ouvertes dans l'intervalle de dates spécifié, sélectionnez **Ouvrir** dans la liste déroulante.

L'état par défaut dans la liste déroulante **Etat** est **Tout**, qui affiche les générateurs d'alerte d'attribut actifs ainsi que ceux qui ont expiré.

Liste déroulante Utilisateur
Sélectionnez un utilisateur de Visualizer par nom d'utilisateur ou sélectionnez **Tout** pour créer un rapport sur les alertes d'attribut de tous les utilisateurs du Visualizer.

Dans votre liste déroulante, votre nom d'utilisateur est l'utilisateur par défaut.

Bouton Exécuter le rapport
Cliquez sur ce bouton pour générer le rapport.

Fenêtre de critères de l'état récapitulatif de source de données :

Cette fenêtre permet de définir les critères d'affichage de l'état récapitulatif de source de données dans Visualizer. L'Etat récapitulatif de source de données affiche des données chargées dans le système par source de données. Les sources de données vous aident à savoir l'origine des données de l'identité.

Liste déroulante Source de données
Sélectionnez une source de données spécifique ou sélectionnez **[tout]** pour afficher les données provenant de toutes les sources de données.

Date de début
Saisissez la première date de la plage pour afficher les données dans le rapport sélectionné. Appliquez le format `MM/JJ/AAAA`. Par exemple, `01/01/01` correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de début** par défaut est la date d'aujourd'hui.

Date de fin
Saisissez la dernière date de la plage pour afficher les données dans le rapport sélectionné. Appliquez le format `MM/JJ/AAAA`. Par exemple, `01/01/01` correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de fin** par défaut est la date d'aujourd'hui.

Pour afficher les données d'une seule journée, utilisez la même date dans les zones **Date de début** et **Date de fin**.

Bouton Exécuter le rapport
Cliquez sur ce bouton pour générer le rapport.

Fenêtre des critères du rapport de divulgation :

Utilisez cette fenêtre du Visualizer pour spécifier les critères d'affichage du rapport de Divulgation, qui peut vous aider à consulter et à gérer les relations divulguées. Les relations divulguées ne sont pas découvertes via une résolution d'entité et de relation, mais consiste en liens manuels entre deux identités. Ces liens manuels sont généralement créés dans le Visualizer, mais ils peuvent également être créés en plaçant la paire de balises UMF de la relation divulguée (<DR> et </DR>) dans les fiches d'identité chargées et traitées par les pipelines.

Date de début
Saisissez la première date de la plage pour afficher les données dans le rapport sélectionné. Appliquez le format `MM/JJ/AAAA`. Par exemple, `01/01/01` correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de début** par défaut est la date d'aujourd'hui.

Date de fin
Saisissez la dernière date de la plage pour afficher les données dans le rapport sélectionné. Appliquez le format MM/JJ/AAAA. Par exemple, 01/01/01 correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de fin** par défaut est la date d'aujourd'hui.

Pour afficher les données d'une seule journée, utilisez la même date dans les zones **Date de début** et **Date de fin**.

Bouton Exécuter le rapport
Cliquez sur ce bouton pour générer le rapport.

Fenêtre de critères du rapport Récapitulatif de chargement :

Cette fenêtre permet de définir les critères d'affichage du rapport Récapitulatif de chargement dans Visualizer. Vous pouvez utiliser le rapport Récapitulatif de chargement pour afficher des informations générales sur la qualité des données des fichiers UMF que vous avez chargées dans le Visualizer, ainsi que des informations utiles telles que les statistiques de performance et le nombre de résolutions d'entités et alertes générées par le chargement du fichier.

Code source de données - Liste déroulante de description
Sélectionnez une source de données spécifique ou sélectionnez **[tout]** pour afficher les données chargées depuis toutes les sources de données. Ainsi, si vous avez chargé des fiches d'identité depuis plusieurs fichiers UMF à une date donnée, vous pouvez réduire les données dans le rapport à une seule source de données en sélectionnant le code source des données correspondantes.

Date de début
Saisissez la première date de la plage pour afficher les données dans le rapport sélectionné. Appliquez le format MM/JJ/AAAA. Par exemple, 01/01/01 correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de début** par défaut est la date d'aujourd'hui.

Date de fin
Saisissez la dernière date de la plage pour afficher les données dans le rapport sélectionné. Appliquez le format MM/JJ/AAAA. Par exemple, 01/01/01 correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de fin** par défaut est la date d'aujourd'hui.

Pour afficher les données d'une seule journée, utilisez la même date dans les zones **Date de début** et **Date de fin**.

Bouton Exécuter le rapport
Cliquez sur ce bouton pour générer le rapport.

Fenêtre de critères du rapport de l'état du conflit :

Utilisez cette fenêtre du Visualizer pour spécifier les critères pour générer le rapport Etat d'alerte, qui récapitule l'état des alertes de rôle dans une période donnée et qui peut être utilisé pour gérer vos alertes de rôle.

Date et heure de début
Saisissez la première date de la plage pour générer des données dans le

rapport. Appliquez le format MM/JJ/AAAA. Par exemple, 01/01/01 correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

En utilisant l'horaire militaire, saisissez la première heure dans l'intervalle de temps pour générer les données dans le rapport. Utilisez le format HH:MM. Par exemple, 09:00 représente 9H00, et 20:30 représente 20H30.

La **Date de début** et **l'Heure** par défaut est la Date d'aujourd'hui à 00:00.

Date et heure de fin
Saisissez la dernière date de la plage pour imprimer les données dans le rapport. Appliquez le format MM/JJ/AAAA. Par exemple, 01/01/01 correspond au 1er janvier 2001. Ou cliquez sur la commande du calendrier et cliquez sur la date.

La **Date de fin** et **l'Heure** par défaut est la Date d'aujourd'hui à 23:59.

Pour afficher les données d'une seule journée, sélectionnez l'une des options suivantes :

- Saisissez la même date dans les zones **Date de début** et **Date de fin**.
- Saisissez 00:00 dans la zone **Heure de début**, et 23:59 dans la zone **Heure de fin**.

Intervalle de création de rapports sur les scores de relation
Si vous souhaitez affiner les résultats par score de relation, saisissez un intervalle de scores de relations dans les zones **De** et **A**.

L'intervalle par défaut s'étend de 0 à 100, ce qui correspond au score de toutes les relation.

Liste déroulante Règle d'alerte de rôle
Sélectionnez la règle d'alerte de rôle sur laquelle établir le rapport.

Liste déroulante Niveau d'alerte de rôle
Sélectionnez un niveau d'alerte de rôle spécifique ou sélectionnez **Tout** pour créer un rapport sur toutes les alertes de rôle.

Bouton Exécuter le rapport
Cliquez sur ce bouton pour générer le rapport.

Analyse des données avec Analyst Toolkit

Vous pouvez utiliser les outils et les modèles dans Identity Insight Analyst Toolkit, pour créer et personnaliser des rapports d'analyse et des informations dans un environnement d'application accessible à partir d'un navigateur.

Génération de rapports sur les données à l'aide des rapports IBM Cognos

Le composant Analyst Toolkit fournit un ensemble de rapports Cognos qui peut être utilisé pour créer des rapports Identity Insight personnalisés.

L'intégration d'IBM Cognos dans Integrity Insight offre une base permettant de personnaliser les rapports Integrity Insight de façon à ce qu'ils contiennent les informations dont vous avez besoin.

Analyst Toolkit comprend les éléments suivants pour une utilisation avec IBM Cognos :

- Les outils Cognos Business Intelligence pour le développement de requête et d'application
- La création et le déploiement d'un modèle de données Identity Insight (développé avec Cognos Framework Manager)
- Des modèles de rapport pour le récapitulatif d'entité et les informations rôle-alerte. Ces composants ont été conçus comme points de départ pour la personnalisation et le développement d'applications.

Avec la fonction de reporting et le modèle d'infrastructure Cognos, vous disposez des outils nécessaires pour créer des interfaces utilisateur et des rapports Cognos basés sur le référentiel Identity Insight. Vous pouvez utiliser les outils Cognos inclus pour créer des interfaces personnalisées et modifier les modèles fournis par EAS.

Les termes et les concepts suivants sont utilisés dans la documentation de ce produit :

Analyst Toolkit
Module Identity Insight conçu pour les composants et les exemples de modèle Cognos installés.

EntitySearcher
Navigateur de client léger qui associe le meilleur des fonctionnalités de recherche find-by-attribute et find-by-resolution dans un client doté d'un navigateur.

IBM Cognos Business Intelligence
Nom général du composant Cognos inclus dans Identity Insight.

Rapport Cognos
Spécification de la sortie XML qui peut être générée sous la forme suivante : Interface utilisateur interactive dans Cognos Viewer, un fichier PDF, un fichier XML (pour une génération personnalisée) ou un certain nombre de formats Excel (y compris CSV).

Rapport actif
Cognos 10 a introduit les rapports actifs, c'est-à-dire des rapports autonomes qui ont un aspect et un mode de fonctionnement plus proches de ceux des applications Web que les rapports Cognos standard.

Cognos Framework Manager
Outil Cognos permettant de modéliser une source de données (en général une base de données). Le modèle de données Identity Insight a été créé à l'aide de Framework Manager.

Modèle de données Cognos
Représentation logique d'une ou de plusieurs sources de données. Les auteurs de rapports Cognos utilisent le modèle de données pour créer des rapports interactifs.

Magasin de contenu Cognos
Base de données distincte utilisée par Cognos pour stocker des objets Cognos, tels que des définitions de rapport, des modèles de données et des requêtes. Le magasin de contenu n'est pas utilisé pour stocker les données Identity Insight.

Analyse de données à l'aide d'un client léger EntitySearcher

Le client léger EntitySearcher associe les meilleures fonctionnalités de recherche find-by-attribute et find-by-resolution sur un client doté d'un navigateur.

Identity Insight offre deux grandes fonctions de recherche pour rechercher des entités. La recherche find-by-resolution, parfois appelée PSearch ou recherche via des pipelines, utilise la résolution d'entité pour trouver des résultats. La recherche find-by-attribute, appelée EQ ou requête améliorée, utilise une consultation SQL plus traditionnelle.

EntitySearcher associe ces deux approches pour obtenir des résultats optimaux et éviter toute confusion au moment de choisir l'approche à utiliser. L'interface client fournit une interface find-by-attribute conviviale pour entrer des critères de recherche. Un ou les deux des types de recherche sont appelés en fonction des critères d'entrée et des résultats de chaque recherche. Les résultats des deux recherches sont compilés, dédupliqués, classés et présentés dans la grille des résultats de la recherche.

Une amélioration de la fonction de recherche permet de rechercher les entités dotées d'une date de naissance comprise dans une plage de dates indiquée. Cette recherche est effectuée lorsque la case **Expand search by** et la liste déroulante sont utilisées. Par exemple, si on prend la date 6/1/1960 et une plage de 30 jours, la plage de dates effective utilisée dans la recherche est comprise entre 5/2/1960 et 7/1/1960 [6/1/1960 moins 30 jours et 6/1/1960 plus 30 jours]. La plage inclut la date de fin.

Vous pouvez sélectionner l'option “Strict Search” ; Dans ce cas, seule l'option find-by-attribute (EQ) est utilisée. Une recherche stricte est effectuée par défaut si l'une des conditions suivantes est remplie :

- Un seul attribut est entré pour les critères de recherche.
- Il y a des éléments incomplets dans les critères de recherche de l'attribut.
- Des caractères génériques sont utilisés dans tous les critères de recherche de l'attribut. (* par exemple) ;
- Les critères de recherche de l'attribut DOB (Date of Birth) inclut une plage de dates.

L'adresse URL à utiliser pour lancer EntitySearcher est la suivante :

`http://serveur:port_d_installation/EntitySearcher/`

Pour les résultats de recherche, vous pouvez naviguer jusqu'à une version de rapport Cognos du récapitulatif d'entité Identity Insight, jusqu'à un composant graphique ou n'importe quelle cible qu'il est possible de lier en http, en demandant à l'administrateur système de configurer les valeurs URL_ENTITY_DETAIL et URL_ENTITY_GRAPH de la table de base de données COMPONENT_CONFIG.

Recherche d'entités à l'aide d'EntitySearcher :

Vous pouvez rechercher des entités en fonction des données d'attribut et déterminer le type de recherche à effectuer.

Pourquoi et quand exécuter cette tâche

Le client léger EntitySearcher associe les meilleures fonctionnalités de recherche find-by-attribute et find-by-resolution sur un client doté d'un navigateur. Une fois la recherche terminée, une interface utilisateur est disponible pour afficher les résultats de la recherche.

Procédure

1. Ouvrez EntitySearcher dans le navigateur.

   L'adresse URL à utiliser pour lancer EntitySearcher est la suivante :

   `http://serveur:port_d_installation/EntitySearcher/`

   Par exemple : `http://localhost:13510/EntitySearcher/`. La valeur par défaut de *port_installation* est 13510 mais le numéro de port peut être modifié. Si vous avez des doutes, vérifiez le nom du serveur ou le numéro de port auprès de votre administrateur système.

2. Dans la sous-fenêtre **Search Entities**, entrez les critères de recherche. Un seul attribut est affiché pour une recherche d'entité par défaut.

   a. Dans la section **Attribute list**, sélectionnez le type d'attribut pour les critères de recherche des attributs.

   b. Entrez les critères de recherche.

Option	Description
Vous avez des critères de recherche d'attributs supplémentaires.	Cliquez sur **+** à droite de l'attribut existant.
Vous n'avez pas de critères de recherche d'attributs supplémentaires.	Passez à l'étape suivante. **Remarque :** Une recherche stricte est effectuée lorsqu'un seul attribut est entré pour les critères de recherche.

3. Déterminez si vous souhaitez effectuer une recherche combinée ou uniquement une recherche stricte.

Option	Description
Effectuer une recherche combinée	Une recherche combinée est effectuée par défaut.
Effectuer une recherche stricte uniquement	Cochez la case **Strict search**. **Remarque :** Une recherche stricte est effectuée par défaut si l'une des conditions suivantes est remplie. • Un seul attribut est entré pour les critères de recherche. • Il y a des éléments incomplets dans les critères de recherche de l'attribut. • Des caractères génériques sont utilisés dans tous les critères de recherche de l'attribut. (* par exemple) ; • Les critères de recherche de l'attribut DOB (Date of Birth) inclut une plage de dates.

4. Cliquez sur **Rechercher**.

Résultats

Le panneau **Résultats de la recherche** liste les résultats de la recherche d'entités. Les résultats sont classés en fonction du score de probabilité et, éventuellement, en fonction du score de nom. Les résultats de la recherche find-by-resolution à score élevé (>86) sont présentés en premier, suivi par les résultats de la recherche find-by-attribute à score élevé. Les résultats de la recherche resolution à score faible sont répertoriés ensuite.

Que faire ensuite

Afficher le récapitulatif d'entité pour connaître le résultat d'une recherche.
A partir de la colonne **ID entité** de la ligne du résultat de la recherche de votre choix dans le sous-panneau **Résultats de la recherche**, cliquez sur la valeur **ID entité** soulignée.

Remarque : Il est possible que l'administrateur système doive configurer la valeur URL_ENTITY_DETAIL de la table de base de données COMPONENT_CONFIG pour activer cette fonctionnalité.

Afficher le diagramme d'entité pour connaître le résultat d'une recherche.
Dans le sous-panneau **Résultats de la recherche**, à partir de la colonne **ID entité** de la ligne du résultat de la recherche de votre choix, cliquez sur l'icône de création de diagramme.

Remarque : Il est possible que l'administrateur système doive configurer la valeur URL_ENTITY_GRAPH de la table de base de données COMPONENT_CONFIG pour activer cette fonctionnalité.

Exemple de rapport alerte de rôle Cognos

Le modèle de rapport d'alerte de rôle Cognos contient des informations sur les entités et sur les relations d'entité impliquées dans l'alerte, et vous pouvez le personnaliser à l'aide des outils Cognos.

Le rapport rôle-alerte utilise la technologie Active Report introduite dans Cognos 10 pour offrir des fonctions utilisateur enrichies.

Le chemin d'une alerte est présenté dans un onglet dynamique séparé, pour chaque information correspondante qui s'affiche. Les informations récapitulatives rôle-alerte sont présentées dans la partie supérieure du rapport et des clichés de l'entité (état de l'entité au moment de la génération de l'alerte) sont disponibles si l'utilisateur souhaite visualiser ce type d'informations. Une section étendue présentant les détails de concordance indique les données de score Identity Insight.

Accès aux données

Le rapport détaillé rôle-alerte utilise principalement les nouvelles vues de base de données Identity Insight. Cette approche permet un meilleur contrôle des accès aux données. Par exemple, les structures de jointure et de requête sont définies par SQL et ne sont pas traitées par le moteur Cognos. Elle fournit également une couche d'abstraction à partir des tables de données sous-jacentes, qui permet de modifier le schéma sous-jacent sans affecter directement les rapports Cognos.

Même si de nouvelles vues de base de données Identity Insight sont disponibles pour prendre en charge l'écran détaillé rôle-alerte Cognos, l'accès aux données est assuré et contrôlé par le serveur Cognos via le modèle.

Remarques techniques

Le rapport détaillé rôle-alerte de Cognos utilise la technologie Active Report. Cela signifie que le seul type de sortie pris en charge est HTML. Contrairement à un rapport Cognos standard, toutes les données utilisées par le rapport sont extraites avant l'affichage du rapport. Cette procédure permet de maintenir l'interactivité des rapports Active Report après la déconnexion du serveur Cognos. Les rapports Active Reports peuvent être distribués en tant que fichiers .MHT (MIME HTML) et sont créés à partir de la page d'accueil Cognos ou en accédant à l'adresse URL du

rapport dans un navigateur Web qui prend en charge les fichiers MHT. Le chargement global de toutes les données du rapport permet également d'éviter le rechargement de la page lorsque l'utilisateur interagit avec l'interface utilisateur.

Le rapport rôle-alerte de Cognos requiert un ID rôle-alerte en tant que paramètre. Si l'utilisateur accède au rapport directement, il doit indiquer un ID rôle-alerte. Si l'utilisateur accède au rapport configuré en tant que composant, l'ID rôle-alerte peut être transmis en tant que paramètre d'URL. Le format utilisé pour transmettre des paramètres Cognos via une adresse URL est l'ajout de la chaîne “p_” au début du nom d'invite. Dans le cas d'un rapport rôle-alerte, le paramètre attendu est **pAlertID** : La syntaxe doit donc être **p_pAlertID**. Par exemple : **&p_pAlertID=55&**.

Les vues de la base de données Identity Insight créées pour prendre en charge les composants Cognos sont nommées en utilisant le préfixe COG pour faciliter leur identification.

Firefox 3.x requiert l'installation de plug-ins supplémentaires pour permettre l'affichage de fichiers MHT.

Exemple de rapport récapitulatif d'entité Cognos

Le modèle de rapport de récapitulatif d'entité Cognos fournit toutes les informations connues sur une entité, et vous pouvez le personnaliser grâce aux outils Cognos.

Dans le rapport récapitulatif Cognos, les données d'entité sont résumées. L'utilisateur peut donc choisir quelles informations consulter.

Remarques techniques

Le récapitulatif d'entité Cognos utilise principalement des objets de requête définis par le rapport, par opposition aux vues de base de données réelles. Les requêtes virtuelles reposent sur le modèle de données Cognos et sont créées en faisant glisser les objets du modèle dans le générateur de requête des rapports et en définissant des propriétés. Le récapitulatif utilise un objet "bloc conditionnel" pour afficher la section d'informations détaillées. En raison de l'utilisation d'un bloc conditionnel pour que l'écran ait plus l'aspect d'une interface utilisateur (et non d'un rapport), les versions PDF, texte et Excel de ce rapport n'ont pas l'aspect ni le fonctionnement des données HTML générées par défaut.

Le serveur de rapport Cognos demande uniquement les informations dont il a besoin pour afficher les sections visibles du rapport. Par exemple, les informations rôle-alerte sont extraites uniquement lorsque l'utilisateur choisit d'afficher ces informations. Cette procédure permet d'obtenir des temps de chargement initiaux plus rapides et un accès aux données plus efficace mais elle a un certain coût. La page doit être rechargée lorsque la section d'informations est modifiée. Le rechargement de cette page est automatique et ne nécessite aucune interaction utilisateur mais l'utilisateur doit attendre l'actualisation de la page avant de pouvoir intervenir.

Le rapport récapitulatif Cognos requiert un ID d'entité Identity Insight comme seul paramètre. Si le rapport est exécuté à partir de la page d'accueil Cognos, l'utilisateur est invité à entrer un ID d'entité. Il est possible de lancer le rapport à partir de la page d'accueil Cognos et d'entrer un ID d'entité mais il est plus courant de l'utiliser sous la forme d'un composant intégré et de l'appeler à partir d'une autre application, telle qu'un outil de flux de travaux ou de gestion de cas.

Dans un cas d'utilisation, l'ID d'entité Identity Insight peut être transmis en tant que paramètre d'adresse URL au récapitulatif Cognos et la page invitant à entrer l'ID d'entité ne s'affiche pas.

Le format utilisé pour transmettre des paramètres Cognos via une adresse URL est l'ajout de la chaîne “p_” au début du nom d'invite. Dans le cas du rapport récapitulatif, le paramètre attendu est **pEntityID**. La syntaxe doit donc être : **p_pEntityID**. Par exemple : **&p_pEntityID=5&**.

Identification et installation des composants Cognos

Vous pouvez installer les composants IBM Cognos pour utiliser et modifier les fonctionnalités de génération de rapports IBM Identity Insight Cognos.

Avant de commencer

Vous devez installer IBM Business Intelligence Reporting avant de déployer les rapports IBM Identity Insight Cognos.

Remarque : Si une instance d'IBM Cognos Business Intelligence Reporting version 10.1.0 ou suivante est installée, vous pouvez l'utiliser pour déployer les rapports IBM Identity Insight Cognos.

Pour modifier les métadonnées des rapports, vous devez installer IBM Cognos Framework Manager.

Procédure

1. Installez IBM Business Intelligence Reporting version 10.1.0 ou suivante.
   a. Installez le composant Cognos Reporting en suivant les instructions Cognos détaillées.
2. Installez IBM Cognos Framework Manager version 10.1.0 ou suivante.
   a. Installez le composant Cognos Reporting en suivant les instructions Cognos détaillées.

Que faire ensuite

Déployez les rapports Identity Insight dans Cognos.

Déploiement de rapports Identity Insight dans Cognos :

Pour activer les rapports d'alerte de rôle et les rapports récapitulatifs d'entité IBM Identity Insight Cognos, vous devez d'abord les déployer dans IBM Cognos Business Intelligence Reporting.

Avant de commencer

Installez IBM Cognos Business Intelligence Reporting.

Procédure

1. Copiez le module de déploiement des rapports Identity Insight Cognos dans IBM Cognos Business Intelligence Reporting. Identity Insight fournit deux versions des rapports, selon que vous choisissez d'utiliser le mode de requête Dynamique ou Compatible de Cognos.

Tableau 32. Emplacements du module de déploiement des rapports Identity Insight Cognos

Copier le fichier de	Copier le fichier vers
*<répertoire installation produit>*ibm-home/cognos/deployment/IdentityInsight_v9.0_CompatibleQueryMode.zip ou *<répertoire installation produit>*/ibm-home/cognos/deployment/IdentityInsight_v9.0_DynamicQueryMode.zip	*<répertoire d'installation Cognos>*/deployment/

2. Accédez à la page de connexion Cognos dans votre navigateur. La page se trouve à l'adresse http://*<nom_serveur_ou_adresse_IP_cognos>*:*<numéro_port_cognos>*:cognos/index.html.
3. Cliquez sur **Exécutez** > **IBM Cognos Administration**.

   Remarque : Si vous souhaitez accéder à IBM Cognos Administration, vous devez disposer des droits nécessaires pour la fonction sécurisée des tâches d'administration.
4. Cliquez sur l'onglet **Configuration** et **Content Administration**. Dans la barre d'outils, cliquez sur l'icône **New Import**
5. Dans la liste des modules de déploiement disponibles, sélectionnez `IdentityInsight_v9.0_Cognos`. Lorsque le système vous invite à entrer un mot de passe, entrez `ISII4YOU`. Cliquez sur **OK**.
6. Dans le sous-panneau name and description, cliquez sur **Next**. Le sous-panneau name and description ne requiert pas de modification.
7. Dans la liste **public folders content** dans public folder content pane, cochez la case du dossier **ISII**. Cliquez sur **Suivant**.
8. Dans le sous-panneau directory content, cliquez sur **Next**. Le sous-panneau directory content ne requiert pas de modification.
9. Dans le sous-panneau general options, cliquez sur **Next**. Le sous-panneau general options ne requiert pas de modification.
10. Vérifiez le récapitulatif et cliquez sur **Next**.
11. Sélectionnez **Save and run once**. Cliquez sur **Finish** pour importer le rapport. Cliquez sur **Exécuter**. Les options d'exécution ne requièrent pas de modification.
12. Avant de fermer la boîte de dialogue, indiquez si vous souhaitez visualiser les détails de l'importation. Cliquez sur **OK**. Si le statut affiche `"Executing"`, cliquez sur **Refresh**. Lorsque le déploiement aboutit, le statut correspond à `"Succeeded"`. Cliquez sur **Fermer**.

Que faire ensuite

1. Vérifiez que les rapports sont déployés.
2. Modifiez la configuration de la base de données de déploiement des rapports Identity Insight Cognos.

Vérification du déploiement des rapports Identity Insight :

Une fois le déploiement effectué, vous devez le vérifier avant d'exécuter les rapports.

Avant de commencer

Déployez les rapports Identity Insight dans Cognos.

Procédure

1. Accédez à la page de connexion Cognos dans votre navigateur. La page se trouve à l'adresse http://<*nom_serveur_ou_adresse_IP_cognos*>:<*numéro_port_cognos*>:cognos/index.html.
2. Dans l'onglet Public Folders, vérifiez que le dossier public **ISII** existe.
3. Sélectionnez le dossier **ISII**.
4. Vérifiez qu'un seul objet de module **Identity_Insight** existe. Un objet de module apparaît sous la forme d'un dossier bleu.
5. Vérifiez que les rapports **ISII_EntityResume** et **ISII_RoleAlertDetailActive** existent.

Que faire ensuite

Modifiez la configuration de la base de données de déploiement des rapports Identity Insight Cognos.

Modification de la configuration de la base de données de déploiement des rapports Identity Insight Cognos :

Après avoir déployé et vérifié les rapports, vous devez modifier la configuration de la base de données de déploiement des rapports Identity Insight Cognos. Remarque : si vous utilisez les rapports en mode de requête dynamique, reportez-vous à la documentation Cognos pour créer une connexion JDBC à partir de Cognos (au lieu de suivre la procédure décrite ci-après).

Avant de commencer

Déployez les rapports Identity Insight dans Cognos.

Procédure

1. Accédez à la page de l'administrateur Cognos dans le navigateur.
2. Dans la partie de gauche, cliquez sur **Data Source Connection**.
3. Sélectionnez l'objet **ISII** Data Source.
4. Sélectionnez l'objet **ISII** Data Source Connection.
5. Sélectionnez l'objet **ISII** Signon.
   a. Cliquez sur **Définir les propriétés**.
   b. Dans l'onglet **Connexion**, cliquez sur **Modifier la connexion...**.
   c. Modifiez le lien pour inclure le nom d'utilisateur et le mot de passe de la base de données Identity Insight. Cliquez sur **OK**.
   d. Cliquez sur **OK**.
6. Cliquez sur **Set properties** pour l'objet Data Source Connection.
7. Dans l'onglet **Connections**, suivez les instructions indiquées pour le type de base de données Identity Insight.

Type de base de données Identity Insight	Instructions
DB2	1. Sélectionnez **IBM DB2** pour le type. 2. Cliquez sur l'icône **Edit the connection string**. 3. Modifiez la valeur du nom de la base de données DB2. Si un schéma vous est demandé, ajoutez `currentSCHEMA=<schema>;` au paramètre de la chaîne de connexion DB2. 4. Cliquez sur **Test the connection...**. 5. Cliquez sur **Tester**. 6. Vérifiez que le statut est `Succeeded`.
Oracle	1. Sélectionnez **Oracle** pour le type. 2. Cliquez sur **OK** lorsque l'avertissement `current connection string will be lost` s'affiche. 3. Cliquez sur l'icône **Edit the connection string**. 4. Modifiez la chaîne de connexion SQL*Net. 5. Cliquez sur **Test the connection...**. 6. Cliquez sur **Tester**. 7. Vérifiez que le statut est `Succeeded`.

8. Cliquez sur **Close** pour fermer le panneau test results.
9. Cliquez sur **Close** pour fermer le panneau test connections.
10. Cliquez sur **OK** pour fermer le panneau test connections.
11. Cliquez sur **OK** pour fermer le panneau set properties.

Analyse de données à l'aide de l'outil de création de diagrammes

L'outil de création de diagramme InfoSphere Identity Insight permet aux utilisateurs d'analyser des diagrammes Web qui représentent des alertes, des relations d'entité et d'autres informations d'entité Identity Insight.

Pour générer des diagrammes, l'outil de création de diagramme requiert l'exécution d'un pipeline en arrière-plan.

Les diagrammes générés par cet outil sont similaires à ceux générés avec le composant i2 Analyst Notebook. Toutefois, l'outil de création de diagramme présente l'avantage de permettre l'imbrication et le lancement des diagrammes au sein d'un outil de gestion de cas ou d'une autre application. Les utilisateurs peuvent également utiliser une adresse URL ou une page de démarrage Web pour afficher et lancer les diagrammes dans un navigateur Web. Il n'est pas nécessaire d'installer et de lancer i2 Analyst Notebook pour afficher les diagrammes créés avec cet outil.

Diagramme d'alerte

Le diagramme d'alerte généré par l'outil de création de diagramme affiche une alerte de rôle spécifique en fonction de l'ID d'alerte. Il permet de visualiser les entités liées à l'alerte de rôle et les attributs qui relient les entités.

Une alerte de rôle est lancée lorsqu'une ou plusieurs entités sont reliées via une relation qui respecte ou dépasse une règle d'alerte de rôle configurée. Les alertes de rôle reposent sur des rôles et des règles d'alerte de rôle configurés et peuvent indiquer :

- Un avertissement ou un incident, par exemple un client lié à un suspect figurant sur une liste de surveillance
- Des relations présentant un intérêt, par exemple un client qui est également fournisseur ou un employé en relation avec plusieurs clients via un numéro de téléphone

Conseils d'utilisation du diagramme d'alerte

- Si vous visualisez un indicateur d'entités associées pour une entité liée à l'alerte, utilisez l'option de menu **Afficher les entités associées restantes** en cliquant à l'aide du bouton droit de la souris pour afficher les entités associées restantes. Le diagramme est régénéré pour afficher toutes les entités associées à l'entité sélectionnée. Le diagramme lie automatiquement les entités restantes à d'autres entités du diagramme auxquelles ces entités restantes sont également associées.
- Le diagramme d'alerte affiche uniquement les attributs de chaque entité qui a contribué à l'alerte. Pour afficher tous les attributs associés à une entité

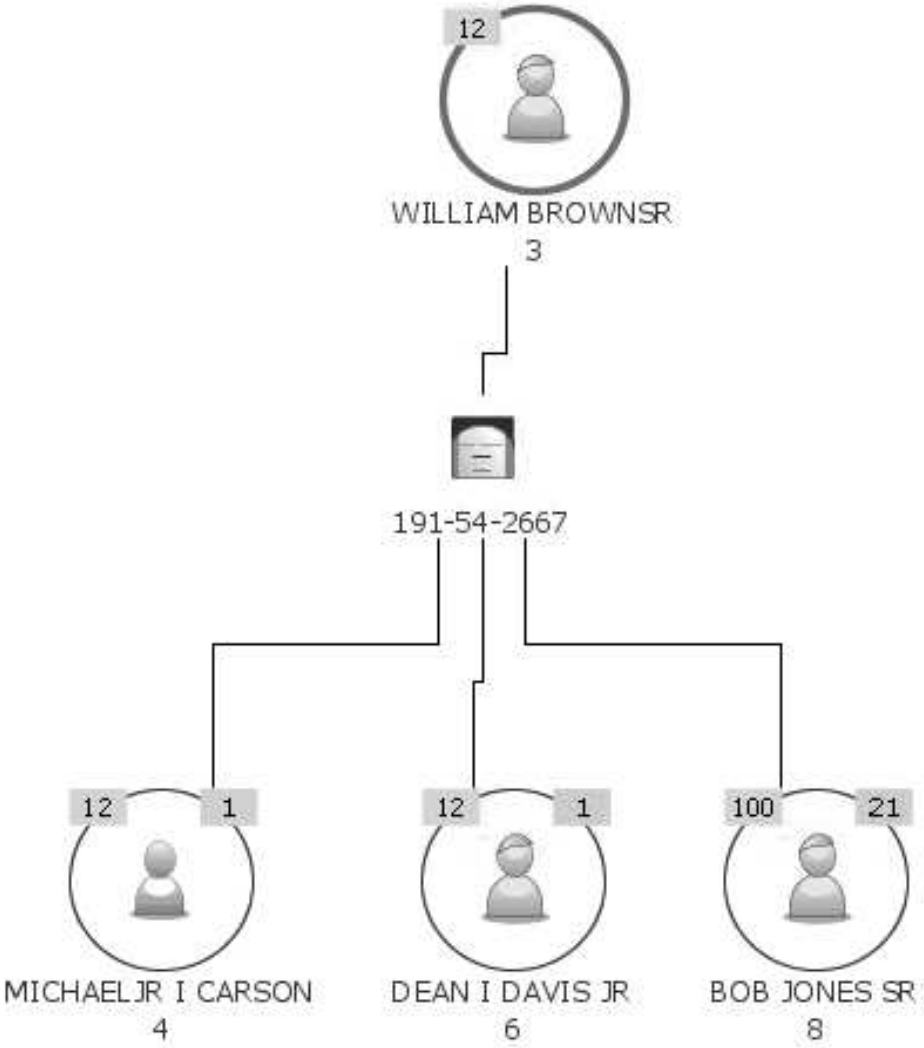
spécifique, cliquez à l'aide du bouton droit de la souris sur l'entité et sélectionnez **Afficher les attributs restants**.

- Pour afficher le récapitulatif d'une entité spécifique dans le diagramme, cliquez à l'aide du bouton droit de la souris sur l'entité et sélectionnez **Afficher la reprise**. Le récapitulatif de l'entité contient des informations supplémentaires sur l'entité, notamment les identités de cette entité et d'autres alertes liées à l'entité. Cette option, disponible en cliquant à l'aide du bouton droit de la souris, est accessible uniquement si le lien est correctement configuré et si vous avez accès au produit qui génère des récapitulatifs d'entités, par exemple Analyst Toolkit.

Diagramme d'entité

Le diagramme d'entité généré par l'outil de création de diagramme permet de visualiser les relations entre l'entité indiquée et toutes les entités associées, en fonction d'attributs partagés.

Le diagramme d'entité décrit les relations entre les entités en utilisant différentes couches d'entités et d'attributs.



Première couche - Entité principale
La première fois que vous examinez le diagramme, la première couche contient l'entité principale. L'*entité principale* est toujours l'entité que vous avez définie ou sélectionnée pour générer le diagramme d'entité. Visuellement, le trait situé autour du noeud de l'entité principale est toujours plus épais pour vous permettre de repérer l'entité principale quel que soit son emplacement dans le diagramme.

L'*entité de niveau supérieur* est l'entité affichée sur la première couche du diagramme, tout en haut. Au départ, l'entité principale représente également l'entité de niveau supérieur mais n'importe quelle entité peut devenir l'entité de niveau supérieur si vous cliquez sur le bouton droit de la souris pour sélectionner **Déplacer vers le haut**.

Deuxième couche (et couches supplémentaires paires) - Attributs partagés
La deuxième couche se compose des attributs partagés qui relient l'entité de niveau supérieur aux entités situées sur la troisième couche du diagramme. Les attributs affichés dans le diagramme indiquent à la fois le type et la valeur de l'attribut.

Si le diagramme comporte des couches supplémentaires, les couches dotées de numéros pairs contiennent toujours les attributs partagés qui relient les entités affichées au-dessous et au-dessous de cette couche d'attributs.

Troisième couche (et couches supplémentaires impaires) - Entités associées
La troisième couche du diagramme affiche les entités associées à l'entité de niveau supérieur avec un degré de séparation.

Si le diagramme comporte des couches supplémentaires, les couches impaires contiennent toujours des entités associées à la couche d'entité précédente, en fonction de la couche d'attributs partagés située entre les deux couches d'entités. Les entités affichées dans les couches d'entités suivantes sont associées à l'entité de niveau supérieur avec les degrés de séparation correspondants : Les entités de la troisième couche sont associées à l'entité de niveau supérieur avec deux degrés de séparation. Les entités de la cinquième couche sont associées à l'entité de niveau supérieur avec trois degrés de séparation, et ainsi de suite.

Conseils d'utilisation du diagramme d'entité

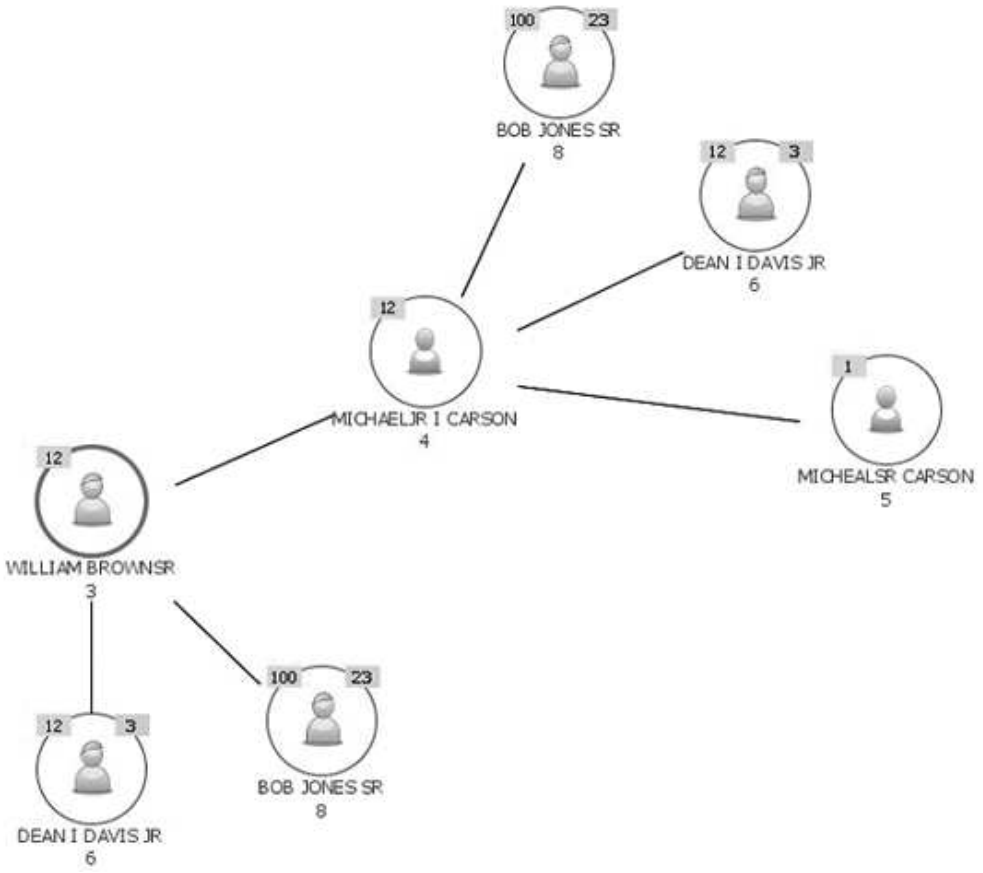
Les diagrammes d'entité peuvent contenir de nombreuses couches. Voici quelques conseils à suivre pour identifier les informations d'attribut et d'entité affichées dans un diagramme d'entité.

- Pour afficher des informations supplémentaires sur une entité :
  - Utilisez l'option de menu **Afficher les entités associées restantes**, disponible en cliquant à l'aide du bouton droit de la souris, pour explorer les relations d'une entité donnée qui ne sont pas actuellement affichées dans le diagramme.
  - Utilisez le filtre rapide **Afficher le chemin vers le haut** pour visualiser le lien reliant une entité ou un attribut à l'entité de niveau supérieur. Ce filtre masque provisoirement les entités et les attributs non associées dans le diagramme.
  - Accédez au diagramme Réseau social pour créer un diagramme qui permet d'afficher et d'examiner les relations existant entre les entités. Le diagramme Réseau social n'affiche pas les attributs partagés mais ceux-ci sont répertoriés dans l'Explorateur d'attributs. Cliquez à l'aide du bouton droit de la souris

sur l'entité à partir de laquelle vous souhaitez créer le diagramme Réseau social et sélectionnez **Créer un nouveau diagramme - Réseau social**.
  - Utilisez le filtre rapide **Afficher les entités associées uniquement** pour créer un petit diagramme Réseau social. Ce filtre rapide masque tous les attributs figurant dans le diagramme et affiche uniquement les entités liées à l'entité choisie avec un degré de séparation. (L'*entité choisie* est l'entité sur laquelle vous avez cliqué à l'aide du bouton droit de la souris pour afficher le filtre rapide.)
  - Utilisez le filtre rapide **Afficher les attributs et les entités associés uniquement** pour mettre en évidence l'entité et afficher uniquement les attributs et les entités associées à l'entité choisie.
  - Utilisez l'option de menu **Afficher la reprise**, disponible en cliquant sur le bouton droit de la souris, pour afficher le récapitulatif d'une entité du diagramme. Le récapitulatif de l'entité contient des informations supplémentaires sur l'entité, notamment les identités associées à l'entité, d'autres alertes liées à l'entité, etc. (Si le lien vers le récapitulatif d'entité n'est pas configuré, par exemple vers le récapitulatif d'entité du composant Analyst Toolkit, cette option n'apparaît pas lorsque vous affichez le menu avec le bouton droit de la souris.)
- Pour afficher le chemin entre deux entités du diagramme :
  - Utilisez le filtre rapide **Afficher le chemin vers le haut** pour visualiser le lien reliant une entité du diagramme à l'entité de niveau supérieur. Ce filtre rapide est particulièrement utile lorsque le diagramme contient plusieurs couches.
  - Utilisez l'option de menu **Déplacer vers le haut**, disponible en cliquant à l'aide du bouton droit de la souris, pour déplacer une entité vers le haut du diagramme et afficher à nouveau les attributs et les entités existants en fonction de leur lien avec la nouvelle entité de niveau supérieur. Aucune information supplémentaire n'est ajoutée au diagramme.
- Pour afficher des informations supplémentaires sur un attribut :
  - Utilisez le filtre rapide **Afficher les attributs uniquement** pour limiter les informations du diagramme à une seule entité. Le filtre permet d'afficher uniquement les attributs de l'entité sélectionnée.
  - Utilisez l'option de menu **Afficher les attributs restants**, disponible en cliquant avec le bouton droit de la souris, pour afficher tous les attributs d'une entité spécifique, y compris ceux qui ne sont pas partagés par une autre entité du diagramme en cours.
  - Utilisez l'**Explorateur d'attributs** pour sélectionner des entités du diagramme qui partagent un attribut spécifique. La valeur indiquée dans la colonne **Entités** peut vous guider. Plus la valeur de la colonne est élevée, plus le nombre d'entités partageant cet attribut dans le diagramme est élevé.
- Pour réorganiser les entités et les attributs au sein d'autres structures, cliquez à l'aide du bouton droit de la souris pour passer d'une présentation de diagramme **En couche** à **Radial**.

Diagramme Réseau social

Le diagramme Réseau social permet de visualiser les relations entre l'entité sélectionnée et toutes les entités auxquelles l'entité sélectionnée est reliée. Avec ce diagramme unique, vous pouvez déterminer qui connaît qui.



Le diagramme Réseau social présente les éléments suivants :

- Liens entité à entité : Vous pouvez afficher toutes les entités associées à l'entité principale (centrale). Toutefois, les attributs qui relient les entités n'apparaissent pas dans le diagramme mais sont accessibles en utilisant l'Explorateur d'attributs avec le diagramme.
- Ensembles de relations : Le diagramme Réseau social est unique car il affiche les entités associées au sein de groupes ou d'ensembles. Ce diagramme peut vous aider à visualiser tous les ensembles de relations auxquels une entité spécifique appartient et à rechercher des structures au sein des ensembles et des relations.

Vous pouvez développer le diagramme pour afficher toutes les entités associées d'une entité. Chaque fois que vous affichez toutes les entités associées à un entité spécifique, ce noeud d'entité devient l'entité centrale d'un nouvel ensemble de relations.

Pour garantir l'intégrité de chaque ensemble de relations, une entité peut apparaître plusieurs fois dans le diagramme au sein de différents ensembles de relations. Toutefois, elle ne s'affiche qu'une seule fois dans chaque ensemble de relations. Pour afficher tous les ensembles de relations dont l'entité fait partie, sélectionnez l'entité en cliquant sur le noeud. La partie intérieure du noeud d'entité sélectionné devient bleue dans chaque ensemble de relations dont l'entité fait partie.

Lorsqu'une entité représente l'entité centrale, l'indicateur Entités associées ne s'affiche pas car toutes les entités associées à l'entité centrale apparaissent déjà dans l'ensemble de relations. Lorsque l'entité représente l'une des entités associées dans

l'ensemble de relations et qu'elle possède d'autres relations qui ne sont pas affichées dans cet ensemble, un indicateur Entités associées s'affiche.

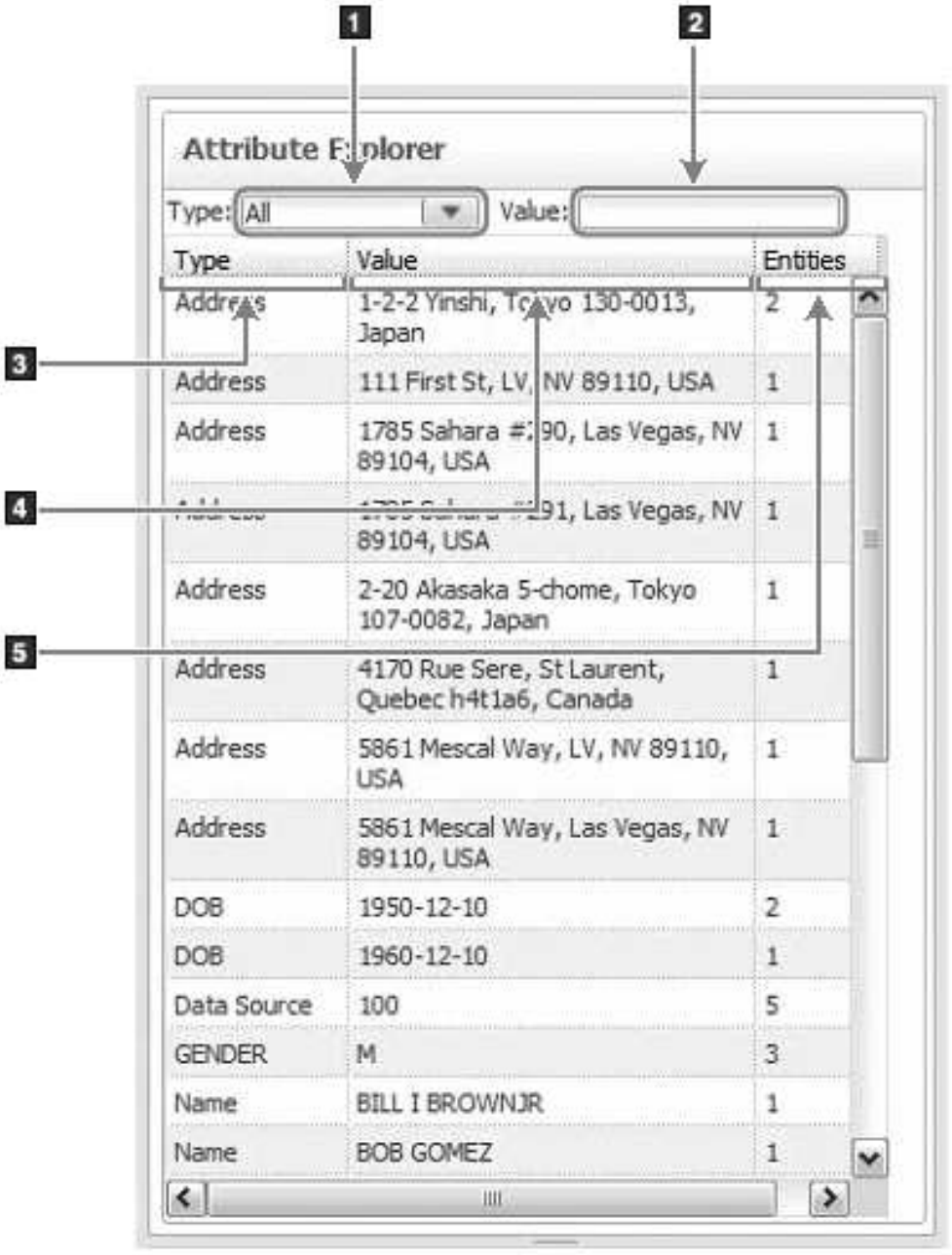
Conseils d'utilisation du diagramme Réseau social

- Utilisez l'option **Afficher les entités associées restantes**, disponible en cliquant à l'aide du bouton droit de la souris, pour développer les entités associées d'une ou de plusieurs entités dans le diagramme. Chaque extension crée un autre ensemble de relations. Recherchez les structures existant entre les ensembles.
- Si plusieurs ensembles de relations sont représentés sur le diagramme, essayez de réduire le zoom pour rechercher des structures et un contexte plus larges dans les clusters. Par exemple, si une entité spécifique apparaît dans tous les ensembles ou dans un grand nombre d'entre eux, il est possible qu'elle exerce une grande influence au sein d'une sphère spécifique. Cette entité peut également être déterminante pour connecter plusieurs ensembles de relations.
- Utilisez l'**Explorateur d'attributs** pour visualiser les attributs qui relient les entités associées. Sélectionnez la ligne d'un attribut spécifique pour mettre en évidence toutes les entités du diagramme qui partagent cet attribut. La valeur indiquée dans la colonne **Entités** peut vous indiquer les attributs partagés par la plupart des entités.

Explorateur d'attributs

Composant de l'outil de création de diagramme, l'Explorateur d'attributs est un tableau qui répertorie tous les types et les valeurs d'attribut associés à l'ensemble des entités du diagramme actuellement affiché. L'Explorateur d'attributs est automatiquement positionné à droite de la grille du diagramme.

Composants de l'Explorateur d'attributs



Numéro d'appel de l'image	Élément	Description
1	Liste déroulante Type	Sélectionnez un type d'attribut pour filtrer les données d'attribut affichées dans l'Explorateur d'attributs. Lorsque vous utilisez la liste déroulante Type, vous ne filtrez pas le diagramme. Vous filtrez uniquement les données figurant dans l'Explorateur d'attributs. Par exemple, vous pouvez sélectionner **SSN** pour filtrer les données dans l'Explorateur d'attributs et afficher uniquement les numéros de sécurité sociale. Cette liste déroulante ne contient pas forcément toutes les types d'attribut configurés pour le produit. Elle contient uniquement les types d'attribut associés aux entités actuellement affichées dans le diagramme.
2	Zone de texte Valeur	Entrez des données dans cette zone pour affiner les informations d'attribut affichées dans la table, en fonction de valeurs d'attribut. L'Explorateur d'attributs examine chaque caractère entré et renvoie la liste des valeurs d'attribut correspondant exactement à l'entrée, qu'il s'agisse d'une correspondance complète ou partielle. Par exemple, si vous entrez 123, l'Explorateur d'attributs filtre la liste d'attributs en présentant uniquement les types d'attribut incluant la chaîne 123 dans la valeur d'attribut. **Remarque :** L'Explorateur d'attributs ne reconnaît pas les caractères génériques. Quels que soient les caractères entrés dans la zone de texte, l'Explorateur d'attributs recherche une correspondance exacte et littérale de ce caractère. Ainsi, si vous entrez un caractère générique standard, tel que * (astérisque), l'Explorateur d'attributs recherche une valeur littérale correspondant au caractère *.

Numéro d'appel de l'image	Élément	Description
3	Colonne Type	Affiche les types d'attribut figurant actuellement dans le diagramme. Les éléments de la colonne correspondent aux descriptions configurées pour les types d'attribut dans la console de configuration. Par exemple, un type d'attribut Carte de crédit peut s'afficher sous la forme **CC** ou **carte de crédit**, en fonction de la manière dont il a été configuré dans la console de configuration. La colonne ne contient pas forcément tous les types d'attribut configurés pour le produit. Elle contient uniquement les types d'attribut actuellement affichés dans le diagramme.
4	Colonne Valeur	Affiche les valeurs des types d'attribut actuellement présentés dans la diagramme. Par exemple, vous pouvez visualiser la valeur **04-01-1962** qui correspond à des données d'un type d'attribut de naissance.
5	Colonne Entités	Indique le nombre d'entités affichées dans le diagramme qui partagent ce type et cette valeur d'attribut. Ces informations vous permettent d'identifier les attributs les plus souvent partagés pour continuer l'exploration.

Conseils d'utilisation de l'Explorateur d'attributs

L'Explorateur d'attributs peut vous aider dans l'analyse des diagrammes, en particulier lorsqu'ils contiennent beaucoup d'informations.

- Utilisez la colonne **Entités** pour rechercher les attributs associés à une seule entité dans le diagramme. Recherchez la valeur 1 dans la colonne. Lorsque le diagramme affiche uniquement les attributs qui relient des entités, l'Explorateur d'attributs affiche l'ensemble des attributs associés à toutes les entités dans le diagramme. Ces attributs ne relient pas l'entité à un autre noeud d'entité dans le diagramme mais ils peuvent permettre l'exploration approfondie d'une entité spécifique.
- Limitez les informations affichées dans l'Explorateur d'attributs à un seul type en sélectionnant un type dans la liste déroulante **Type**. Par exemple, si vous affichez et sélectionnez **Numéros de téléphone**, l'Explorateur d'attributs affiche uniquement les attributs de numéros de téléphone et les valeurs associées.
- Mettez en évidence toutes les entités du diagramme qui partagent le même attribut en sélectionnant un attribut (ligne de table) dans l'Explorateur d'attributs.
- Recherchez des valeurs d'attribut concordantes ou communes dans le diagramme en entrant des données dans la zone **Valeur**. Par exemple, si vous avez entré 123, l'Explorateur d'attributs peut renvoyer l'un ou l'ensemble des attributs concordants suivants :

Type	Valeur
Adresse	**123** Main Street, Anywhere, California, 1**123**4, USA
Adresse	97-**123** Rue Sere, St. Laurent, Quebec, H4T1A6, Canada
Numéro de téléphone	555-222-5**123**
Identificateur fiscal	554-**123**-3**123**

- Vous pouvez entrer plusieurs valeurs complètes ou partielles à la fois dans la zone **Valeur**. L'Explorateur d'attributs les traite comme une requête "AND". Par exemple, si vous entrez `chien chat`, l'Explorateur d'attributs recherche toutes les lignes incluant les chaînes `chien` ET `chat`. L'ordre des valeurs dans la requête n'a pas d'importance. Par exemple, si l'une des valeurs des attributs de l'Explorateur d'attributs est `ses chats et ses chiens`, cette valeur apparaît dans les résultats de la requête `chien chat`.
- Triez les informations de l'Explorateur d'attributs par colonne. Cliquez sur l'en-tête de la colonne. Une flèche s'affiche pour indiquer l'ordre de tri.

Propriétés sélectionnées

Composant de l'outil de création de diagramme, le tableau Propriétés sélectionnées affiche les propriétés du noeud d'attributs ou d'entités sélectionné dans le diagramme. Le tableau affiche uniquement les propriétés du noeud sélectionné (attribut ou entité).

- Si vous sélectionnez une entité, cette section affiche tous les attributs (types et valeurs) associés à l'entité sélectionnée.
- Si vous sélectionnez un attribut, cette section affiche toutes les entités qui partagent l'attribut sélectionné, y compris l'ID de chaque entité. La troisième colonne de cette section affiche l'ID d'identité de la source de données dont les données d'attribut proviennent.

Navigation et exploration des diagrammes de l'outil de création de diagramme

Vous pouvez naviguer et explorer les diagrammes générés dans l'outil de création de diagramme en utilisant la barre d'outils de navigation ou les options du menu contextuel de chaque diagramme.

Barre d'outils de navigation

La barre d'outils de navigation située sous le titre du diagramme contient des icônes pour une navigation standard dans le diagramme.

- Options du mode de sélection : Sélectionnez des éléments isolés dans le diagramme ou sélectionnez plusieurs éléments du diagramme à la fois (ou une zone spécifique du diagramme)
- Repositionnement du diagramme sur la grille
- Restauration de la vue par défaut du diagramme
- Options de zoom : Zoom avant ou zoom arrière

Sélection et mise en évidence

Dans les diagrammes d'alerte et d'entité, la sélection d'un noeud (à l'aide du bouton droit de la souris) entraîne la mise en évidence des attributs et des entités

associés. Le noeud sélectionné change d'aspect pour afficher un rectangle de sélection bleu en haut du noeud. La partie intérieure des noeuds mis en évidence devient bleue.

Tableau 33. Description des options de menu disponibles en cliquant avec le bouton droit de la souris dans l'outil de création de diagramme

Lorsque vous sélectionnez ce type de noeud...	**Dans ce type de diagramme...**	**Ces données sont mises en évidence...**
Attribut	Diagramme d'alerte Diagramme d'entité	Toutes les entités qui partagent cet attribut Tous les attributs associés
Entité	Diagramme d'alerte Diagramme d'entité	Toutes les entités associées à l'entité sélectionnée avec un degré de séparation Attributs à l'origine de la relation avec un degré de séparation
Entité	Diagramme Réseau social	Chaque fois que cette entité s'affiche dans le diagramme, dans chaque entité centrale auquel l'entité sélectionnée est associée. (Une entité peut s'afficher plusieurs fois dans plusieurs entités centrales de ce type de diagramme.)

Vous pouvez sélectionner plusieurs noeuds en utilisant la touche **Ctrl**. Vous pouvez également déplacer les noeuds actuellement sélectionnés en les faisant glisser dans le diagramme.

Options de menu disponibles en cliquant à l'aide du bouton droit de la souris

Sélectionnez une entité ou un attribut en plaçant le curseur dessus et en cliquant à l'aide du bouton droit de la souris.

Tableau 34. Description des options de menu disponibles en cliquant avec le bouton droit de la souris dans l'outil de création de diagramme

Cette option de menu (en cliquant avec le bouton droit de la souris)...	**Effectue l'action suivante...**	**Diagramme d'alerte**	**Diagramme d'entité**	**Diagramme Réseau social**
Zoom	Effectue un zoom avant, arrière ou adapte la taille de la grille du diagramme à l'écran.	X	X	X

Tableau 34. Description des options de menu disponibles en cliquant avec le bouton droit de la souris dans l'outil de création de diagramme (suite)

Cette option de menu (en cliquant avec le bouton droit de la souris)...	Effectue l'action suivante...	Diagramme d'alerte	Diagramme d'entité	Diagramme Réseau social
Filtres rapides (général)	Permet de vous concentrer sur les données qui vous intéressent en masquant provisoirement les données moins pertinentes. Les filtres rapides n'ajoutent pas ou ne suppriment pas de données dans le diagramme. Lorsqu'un filtre rapide est activé, la barre de titre du diagramme affiche [Quick Filter On]. Un seul filtre rapide peut être actif à la fois mais vous pouvez sélectionner un autre filtre rapide lorsque le filtrage rapide est actif. **Remarque :** Lorsqu'un filtre rapide est actif, il affiche uniquement les données du diagramme applicables à l'entité ou à l'attribut actuellement sélectionné. Par exemple, si vous sélectionnez l'entité ABC et le filtre rapide **Afficher les entités associées uniquement**, vous pouvez visualiser les entités actuellement affichées dans le diagramme et associées à ABC avec un degré de séparation.	X	X	
Filtre rapide - Afficher les attributs uniquement	Masque certaines entités pour vous permettre d'afficher les attributs associés à l'entité sur laquelle vous avez cliqué à l'aide du bouton droit de la souris.	X	X	

Tableau 34. Description des options de menu disponibles en cliquant avec le bouton droit de la souris dans l'outil de création de diagramme (suite)

Cette option de menu (en cliquant avec le bouton droit de la souris)...	**Effectue l'action suivante...**	**Diagramme d'alerte**	**Diagramme d'entité**	**Diagramme Réseau social**
Filtre rapide - Afficher les entités associées uniquement	Masque tous les attributs, y compris les attributs qui relient des entités à une autre entité, pour afficher les entités associées avec un degré de séparation à l'entité sur laquelle vous avez cliqué à l'aide du bouton droit de la souris. Ce filtre rapide permet d'obtenir la présentation d'un diagramme Réseau social à partir d'un diagramme d'alerte ou d'entité.	X	X	
Filtre rapide - Afficher les attributs et les entités associés uniquement	Masque toutes les données du diagramme, sauf les entités liées avec un degré de séparation à l'entité sur laquelle vous avez cliqué avec le bouton droit de la souris et les attributs à l'origine de la relation avec un degré de séparation. Ce filtre est particulièrement utile lorsqu'il y a beaucoup de données dans le diagramme et que vous souhaitez masquer les données en trop.	X	X	

Tableau 34. Description des options de menu disponibles en cliquant avec le bouton droit de la souris dans l'outil de création de diagramme (suite)

Cette option de menu (en cliquant avec le bouton droit de la souris)...	Effectue l'action suivante...	Diagramme d'alerte	Diagramme d'entité	Diagramme Réseau social
Filtre rapide - Afficher le chemin vers le haut	Filtre les données du diagramme pour afficher le chemin qui relie l'entité ou l'attribut à l'entité de niveau supérieur. Si vous avez cliqué sur un attribut à l'aide du bouton droit de la souris, le filtre inclut l'ensemble des entités et des attributs, ainsi que le chemin de relation de l'entité de niveau supérieur. Si vous avez cliqué sur une entité à l'aide du bouton droit de la souris, le filtre inclut l'ensemble des attributs et des entités, ainsi que le chemin de relation de l'entité de niveau supérieur.	X	X	
Filtre rapide - Désactiver le filtrage rapide	Désactive le filtre rapide en cours et affiche à nouveau les données filtrées du diagramme.	X	X	
Déplacer vers le haut	Déplace l'entité sélectionnée au sommet du diagramme pour en faire l'entité de niveau supérieur. Cette option n'ajoute pas de nouvelles données dans le diagramme ou dans l'Explorateur d'attributs. En revanche, le diagramme est régénéré pour afficher les données dans la perspective de la nouvelle entité de niveau supérieur.	X	X	

Tableau 34. Description des options de menu disponibles en cliquant avec le bouton droit de la souris dans l'outil de création de diagramme (suite)

Cette option de menu (en cliquant avec le bouton droit de la souris)...	Effectue l'action suivante...	Diagramme d'alerte	Diagramme d'entité	Diagramme Réseau social
Afficher les attributs restants	Affiche tous les attributs associés à l'entité sur laquelle vous avez cliqué à l'aide du bouton droit de la souris, même si ces attributs ne relient pas l'entité à une autre entité dans le diagramme. L'Explorateur d'attributs répertorie toujours l'ensemble des attributs associés à une entité. Cette option ne modifie donc pas les données figurant dans l'Explorateur d'attributs. L'affichage des autres attributs d'une entité peuvent fournir une autre pièce du puzzle ou vous conduire à explorer davantage une entité ou un attribut.	X	X	
Masquer les attributs restants	Supprime du diagramme les attributs qui ne relient pas les entités affichées dans le diagramme. Si tous les attributs présentés dans le diagramme relient des entités actuellement affichées dans le diagramme, cette option n'est pas disponible.	X	X	
Afficher les entités associées restantes	Affiche toutes les relations qui ne sont pas encore affichées pour l'entité sur laquelle vous avez cliqué avec le bouton droit de la souris. Les attributs à l'origine des relations sont également affichés.	X	X	X

Tableau 34. Description des options de menu disponibles en cliquant avec le bouton droit de la souris dans l'outil de création de diagramme (suite)

Cette option de menu (en cliquant avec le bouton droit de la souris)...	**Effectue l'action suivante...**	**Diagramme d'alerte**	**Diagramme d'entité**	**Diagramme Réseau social**
Créer un nouveau diagramme	Crée un diagramme correspondant au type sélectionné et incluant l'entité sur laquelle vous avez cliqué avec le bouton droit de la souris en tant qu'entité principale.	X	X	X
Disposition du graphique	Détermine la présentation du diagramme : • Mis en couche : Affiche les données du diagramme par couche en présentant des lignes d'attributs et les entités associées. Cette présentation est la présentation par défaut dans les diagrammes d'alerte et d'entité. • Radial : Affiche les données du diagramme sous la forme de noeuds et de lignes connectées réparties sur la grille du diagramme de manière aléatoire. Cette présentation peut être utile si vous souhaitez organiser les entités et les attributs vous-même.	X	X	

Tableau 34. Description des options de menu disponibles en cliquant avec le bouton droit de la souris dans l'outil de création de diagramme (suite)

Cette option de menu (en cliquant avec le bouton droit de la souris)...	Effectue l'action suivante...	Diagramme d'alerte	Diagramme d'entité	Diagramme Réseau social
Afficher la reprise	Affiche le récapitulatif de l'entité dans une nouvelle fenêtre, si le lien est configuré dans le fichier `graph.properties`. Le récapitulatif de l'entité contient des informations détaillées sur l'entité sélectionnée, notamment toutes les alertes liées à l'entité et toutes les identités associées à l'entité. Le récapitulatif est un outil d'analyse efficace, notamment lorsque vous l'utilisez avc des diagrammes de l'outil de création de diagramme. Cette option de menu, disponible lorsque vous cliquez à l'aide du bouton droit de la souris, n'est accessible que si l'URL du récapitulatif de l'entité est configuré dans le fichier `graph.properties`. Par exemple, si votre société a installé Analyst Toolkit, l'administrateur système Identity Insight peut configurer le lien afin que le récapitulatif d'entité Cognos s'affiche dans une nouvelle fenêtre du navigateur. Si ce lien n'apparaît pas, contactez l'administrateur système Identity Insight.	X	X	X

Eléments communs affichés dans les diagrammes de l'outil de création de diagramme

Les diagrammes possèdent un certain nombre d'éléments communs : icônes, indicateurs et épaisseur de trait. Ces éléments communs apportent des informations complémentaires qui peuvent vous aider à obtenir une vue plus complète du diagramme et à identifier plus facilement les sections qui vous intéressent.

Icônes Entité

Chaque noeud d'entité apparaît sous la forme d'une icône entourée d'un cercle plein.

Les entités peuvent être définies sous la forme de personnes, de sites ou de biens (sociétés, navires ou avions, par exemple). En règle générale, les entités représentent des personnes. Le noeud d'entité le plus courant est représenté par une icône de personne : Homme, Femme ou Inconnu. Le sexe indiqué par l'icône est basé sur l'une des deux affectations de sexe possibles :

- Le sexe affecté pendant l'analyse du nom de la résolution d'entité
- La valeur de l'attribut GENDER inclus dans les données de l'enregistrement d'identité entrant

Si le sexe est indéterminé, une icône d'entité générique représentant une personne s'affiche.

Le tableau ci-après affiche les icônes d'entité Personne par défaut utilisées dans les diagrammes de l'outil de création de diagramme.

Tableau 35. Exemple présentant les icônes d'entité par défaut utilisées dans les diagrammes de l'outil de création de diagramme

Cette icône...	Représente le type d'entité...
 Indicateur d'entité d'une personne Femme dans l'outil de création de diagramme	Entité (personne) Femme
 Indicateur d'entité d'une personne Homme dans l'outil de création de diagramme	Entité (personne) Homme
 Indicateur d'entité Personne de sexe inconnu dans l'outil de création de diagramme	Entité Sexe inconnu

La principale entité du diagramme d'entité ou du diagramme Réseau social comporte toujours un cercle plus épais. Quel que soit son emplacement dans le diagramme, vous pouvez toujours l'identifier en repérant le cercle plus épais.

Dans le diagramme d'alerte, toutes les entités situées dans le chemin d'alerte comportent un cercle plus épais. Quel que soit le nombre d'entités affichées dans le diagramme (par exemple si vous choisissez de limiter l'affichage aux entités associées restantes), vous pouvez toujours identifier les entités liées à l'alerte.

Icônes d'attribut

Les noeuds d'attribut sont présentés sous forme d'icônes dans les diagrammes de l'outil de création de diagramme. Chaque icône représente un type d'attribut

spécifique. Le tableau ci-après contient un exemple présentant les icônes d'attribut par défaut affichées dans les diagrammes de l'outil de création de diagramme.

Tableau 36. Exemple des icônes par défaut affichées dans l'outil de création de diagramme

Cette icône...	Représente le type d'attribut...
 Icône de l'attribut Adresse dans l'outil de création de diagramme	Adresse
 Icône de l'attribut Nom dans l'outil de création de diagramme	Nom
 Icône de l'attribut Numéro de sécurité sociale dans l'outil de création de diagramme	Numéro de sécurité sociale
 Icône de l'attribut Date de naissance dans l'outil de création de diagramme	Date de naissance
 Icône d'un autre type d'attribut dans l'outil de création de diagramme	Autre attribut (pas affecté à une icône d'attribut existante)

Vous pouvez personnaliser les icônes représentant des attributs dans les diagrammes en remplaçant l'icône d'attribut par défaut ou en ajoutant des icônes représentant les attributs propres à votre société. Voir la section «Ajout d'icônes personnalisées aux diagrammes de l'outil de création de diagramme», à la page 364 pour plus d'informations.

Indicateurs d'alerte

Chaque entité affiche un indicateur signalant le nombre d'alertes pour l'entité. L'indicateur d'alerte apparaît dans l'angle supérieur gauche du cercle plein qui entoure l'icône d'entité.

L'indicateur d'alerte possède un arrière-plan doré et le nombre d'alertes apparaît en noir. Par exemple, cet indicateur d'alerte  sur l'icône d'entité signale que cette entité comporte 25 alertes.

Indicateur d'alerte de l'outil de création de diagramme

Indicateurs d'entités associées

Les noeuds d'entité comportent également un indicateur qui signale le nombre de relations appartenant à cette entité, en fonction d'attributs partagés. Ces relations ne sont pas encore affichées comme partie intégrante de cette entité.

L'indicateur d'entités associées possède un arrière-plan bleu clair et le nombre de relations apparaît en gras, en texte noir. Par exemple, cet indicateur d'entités associées 

Indicateur d'entités associées de l'outil de création de diagramme

indique que six entités supplémentaires ayant une relation avec l'entité n'ont pas encore été affichées.

Le comportement de l'indicateur d'entités associées varie en fonction du type de diagramme :

- Dans le diagramme d'alerte : Les deux entités liées à l'alerte affichent un indicateur d'entités associées si l'entité est associée à d'autres entités qui n'apparaissent pas actuellement dans le diagramme. Vous pouvez développer le diagramme pour afficher toutes les entités associées à chaque entité affichée dans le diagramme. Dans ce cas, il n'y a plus d'indicateur d'entités associées sur les entités.
- Dans le diagramme d'entité :
  - L'entité principale n'a pas d'indicateur d'entités associées. Le diagramme affiche automatiquement toutes les entités associées à l'entité principale.
  - Les autres entités du diagramme d'entité affichent un indicateur d'entités associées si elles sont associées à d'autres entités qui ne sont pas encore affichées dans le diagramme. Vous pouvez utiliser le bouton droit de la souris pour visualiser les entités restantes de ce type d'entité afin que l'indicateur d'entités associées ne soit plus affiché.
  - Comme dans le diagramme d'alerte, vous pouvez développer le diagramme pour afficher toutes les entités associées à chaque entité figurant dans le diagramme. Dans ce cas, aucune entité n'affiche d'indicateur d'entités associées.
- Dans le diagramme Réseau social :
  - L'entité centrale (au centre de l'ensemble) ne comporte pas d'indicateur d'entités associées car le diagramme affiche automatiquement toutes les entités associées au sein de l'ensemble.
  - Les entités qui ne sont pas une entité centrale d'un ensemble de relations peuvent comporter un indicateur d'entités associées si elles sont associées à d'autres entités qui ne sont pas encore reliées au noeud concerné.
  - Si vous développez le diagramme pour inclure plusieurs ensembles de relations, il est possible qu'une entité s'affiche plusieurs fois dans le diagramme. Lorsque l'entité est l'entité centrale d'un ensemble, aucun indicateur d'entités associées ne s'affiche. En revanche, lorsque cette même entité fait partie d'un ensemble de relations mais qu'elle n'est pas l'entité centrale, l'indicateur d'entités associées s'affiche s'il y a d'autres entités associées qui ne figurent pas encore dans le diagramme pour cette entité. Vous voyez donc toujours plusieurs indicateurs d'entités associées dans le diagramme.

Indicateurs de ligne

Les lignes qui entourent les noeuds d'entité et relient les entités et les attributs peuvent fournir des informations supplémentaires :

- Les tirets qui relient les attributs indiquent une concordance d'attributs proche.
- Une ligne épaisse entourant un noeud d'entité indique l'entité principale, à savoir l'entité sélectionnée ou demandée lors de la création de ce diagramme spécifique.

Syntaxe et paramètres de l'adresse URL de l'outil de création de diagramme

Pour accéder au diagramme de l'outil de création de diagramme, vous devez créer un lien vers l'adresse URL appropriée. L'adresse URL peut être imbriquée au sein d'une application personnalisée existante (page de démarrage Web, tableau de bord ou outil de gestion de cas) ou être entrée manuellement dans un navigateur Web.

La syntaxe et les paramètres de l'adresse URL définis pour les diagrammes du composant ont la forme suivante :

`http://`*`serveur`*`:`*`port`*`/graphs/run/`*`typediagramme`*`.jsp?height=`*`nnnn`*`&width=`*`yyyy`*`&`*`identificateur=xxxx`*

serveurhôte*:*port
: Indique le nom du serveur d'applications du produit et le numéro de port d'IBM InfoSphere Identity Insight. En règle générale, le serveur d'applications du produit est le serveur WebSphere.

  Le numéro de port par défaut est 13510.

/graphs/run
: Indique les répertoires où sont stockés les fichiers de l'outil de création du diagramme. Les répertoires `/graphs/run` représentent l'emplacement par défaut où le programme d'installation du produit installe l'outil de création de diagramme.

***typedegraphique*.jsp**
: Indique le type de diagramme à créer :
  - Pour le diagramme d'alerte, entrez `role-alert.jsp`
  - Pour le diagramme d'entité, entrez `entity.jsp`
  - Pour le diagramme de réseau social, entrez `social-network.jsp`

?
: Indiquez un élément d'adresse URL.

height=*nnnn*
: Indique la hauteur de la grille du diagramme, c'est-à-dire la hauteur à utiliser pour générer le diagramme au sein de la fenêtre du navigateur Web. Entrez le nombre en pixels.

  La hauteur du diagramme est déterminée de la manière suivante :
  - Si la hauteur est indiquée dans l'adresse URL, cette valeur représente la hauteur du diagramme par défaut.
  - Si la valeur est définie dans la propriété **`defaultGraphHeight`** du fichier `graph.properties`, cette valeur représente la valeur de la hauteur du diagramme par défaut.
  - Si la hauteur du diagramme n'est pas indiquée dans l'adresse URL ou la propriété **`defaultGraphHeight`**, la hauteur du diagramme par défaut correspond à 800 pixels.

  .

Pour une grille de diagramme figurant dans une fenêtre de navigateur standard de 1024 x 768 pixels, définissez une hauteur de 450 pixels.

? Indique un sème de séparation de l'adresse URL entre les paramètres.

width=*yyyy*
Indique la largeur de la grille du diagramme, c'est-à-dire la largeur à utiliser pour générer le diagramme au sein de la fenêtre du navigateur Web. L'Explorateur d'attributs n'est pas inclus dans cette valeur car il est considéré comme un composant distinct positionné à droite de la grille du diagramme dans la fenêtre du navigateur.

La largeur du diagramme est déterminée de la manière suivante :

- Si la largeur est indiquée dans l'adresse URL, cette valeur représente la largeur du diagramme par défaut.
- Si la valeur est définie dans la propriété **defaultGraphWidth** du fichier `graph.properties`, cette valeur représente la largeur du diagramme par défaut.
- Si la largeur du diagramme n'est pas indiquée dans l'adresse URL ou la propriété **defaultGraphWidth**, la largeur du diagramme par défaut correspond à 800 pixels.

.

Pour une grille de diagramme figurant dans une fenêtre de navigateur standard de 1024 x 768 pixels, définissez une largeur de 640 pixels.

identifiant=xxxx
Indique le type d'ID (entité ou alerte) et la valeur de cette entité ou alerte. Lorsque vous utilisez l'ID d'identité, la valeur de l'ID correspond à l'ID de l'entité principale dans le diagramme d'entité ou l'entité centrale dans le diagramme Réseau social. Lorsque vous utilisez l'ID d'alerte, la valeur représente l'alerte à afficher dans le diagramme d'alerte.

- Pour le diagramme d'alerte, entrez `alertID=`*`numéro_ID_alerte_spécifique`*
- Pour les diagrammes d'entité ou de réseau social, entrez `entityID=`*`numéro_ID_entité_spécifique`*

Tâches d'administration courantes de l'outil de création de diagramme

Certaines tâches de l'outil de création de diagramme ne peuvent être effectuées que par un administrateur.

Ajout d'icônes personnalisées aux diagrammes de l'outil de création de diagramme :

L'outil de création de diagramme contient des icônes standard représentant les différents types d'attribut affichés dans les diagrammes. Vous pouvez modifier l'icône par défaut pour un ou plusieurs attributs ou ajouter des icônes pour des attributs personnalisés configurés dans le produit. Tous les diagrammes de l'outil de création de diagramme utilisent les mêmes icônes sur le serveur d'applications. Ainsi, lorsque vous personnalisez l'ensemble d'icônes d'attribut, tous les utilisateurs visualisent les mêmes icônes.

Avant de commencer

Les icônes de graphique sont créées à partir de fichiers SVG (Scalable Vector Graphics). Les fichiers SVG peuvent être créés à l'aide de différents outils de dessin

vectoriel, ou ils peuvent être téléchargés à partir de diverses sources Internet. Il est vivement recommandé de veiller à ce que les fichiers SVG utilisés pour les icônes conservent une taille raisonnablement petite (de façon à améliorer la lisibilité lorsque l'image est mise à l'échelle).

Le diagramme nécessite une définition de forme stockée au format JSON (Javascript Object Notation). La conversion du format SVG au format JSON requiert l'utilisation de deux utilitaires de commande séparés : **xlstproc** et **sed**.

Si vous utilisez un ordinateur UNIX, il est possible que vous disposiez déjà de ces outils. Si vous utilisez un ordinateur Windows, vous devrez acquérir ces outils UNIX par le biais d'un émulateur UNIX (tel que l'application gratuite Cygwin). *Remarque : si vous utilisez Cygwin, veillez à inclure les bibliothèques libxml2 et libxslt dans votre installation de façon à obtenir les utilitaires requis.*

Finalement, vous aurez besoin du fichier svg2gfx.xsl de la bibliothèque DOJO gratuite (disponible à l'adresse https://dojotoolkit.org/download). Une fois la bibliothèque DOJO téléchargée, vous trouverez le fichier svg2gfx.xsl dans le répertoire <racine intallation>/dojox/gfx/resources.

Procédure

1. Copiez le fichier svg2gfx.xsl depuis l'emplacement de DOJO dans le répertoire qui contient le ou les fichiers SVG à convertir
2. Ouvrez un terminal/une fenêtre de ligne de commande Unix et naviguez jusqu'au répertoire qui contient le ou les fichiers SVG
3. Exécutez la commande suivante : `xsltproc ./svg2gfx.xsl <votre fichier .SVG> > <nom_fichier_temp>.json`
4. Exécutez la commande suivante : `sed -e 's/,}/}/g' -e 's/,]/]/g' <nom_fichier_temp.json> > <nom final>.json`
5. Localisez votre dossier d'installation d'Identity Insight
6. Dans le dossier d'installation, naviguez jusqu'à /ibm-home/graphs
7. Créez un dossier nommé (sensible à la casse) : customImages
8. Transférez l'icône personnalisée (fichier .json) vers le dossier customImages

Exemple

Si vous avez créé un type d'attribut nommé `FLIGHT` et que vous souhaitez une icône de graphique personnalisée pour représenter ce type d'attribut dans les diagrammes de l'outil de création de diagramme, procédez comme suit :

1. Créez ou procurez-vous le fichier image approprié pour représenter le type d'attribut `FLIGHT`. Veillez à ce que le nom du fichier image corresponde au nom du type d'attribut configuré dans la Console d'administration et à ce que toutes les lettres soient en minuscules, comme dans ce nom de fichier : `flight.svg`
2. Assurez-vous que svg2gfx.xsl se trouve dans le même répertoire que `flight.svg`
3. Ouvrez un terminal/une fenêtre de ligne de commande Unix et naviguez jusqu'au répertoire qui contient `flight.svg`
4. Exécutez la commande suivante : `xsltproc ./svg2gfx.xsl flight.svg > flight_tmp.json`
5. Exécutez la commande suivante : `sed -e 's/,}/}/g' -e 's/,]/]/g' flight_tmp.json > flight.json`
6. Copiez le fichier d'icône `flight.json` dans le dossier `/customImages`.

Règles à respecter pour les icônes de diagramme personnalisées :

Vous pouvez personnaliser les icônes d'attribut qui s'affichent dans les diagrammes. Toutefois, les nouvelles icônes doivent respecter les règles définies pour les icônes de diagramme personnalisées afin que les diagrammes puissent les reconnaître et les afficher.

Règles à respecter pour les icônes personnalisées

Pour permettre aux diagrammes de reconnaître et d'afficher des icônes personnalisées, les icônes d'attribut doivent respecter les règles suivantes :

- Format de fichier : SVG (Scalable Vector Graphics)
- Nom :
  - Le nom d'icône personnalisée doit correspondre au nom du type d'attribut associé configuré dans la console de configuration.
  - Le nom d'icône personnalisée ne doit contenir que des minuscules.
- Le fichier SVG doit être converti en une définition de forme JSON (voir «Ajout d'icônes personnalisées aux diagrammes de l'outil de création de diagramme», à la page 364)

Par exemple, si vous souhaitez associer une icône d'attribut au type d'attribut FINGERPRINTS configuré dans la console de configuration, le nom du fichier d'icône doit être `fingerprints.svg`.

Exemples de nom

Pour substituer une icône de type de base existante, l'icône personnalisée doit être nommée avec l'un des noms suivants (tout en caractères minuscules) :

- address.json
- female.json
- male.json
- name.json
- undetermined_gender.json

Pour les numéros d'entité, le fichier d'icône .json doit avoir le même nom que le code de type de numéro (NUM_TYPE.NUM_TYPE dans la base de données). Exemple :

- cc.json
- dl.json
- ff.json
- ssn.json
- pp.json
- ph.json

Pour les caractéristiques d'entité, le fichier d'icône .json doit avoir le même nom que le code de type d'attribut (ATTR_TYPE.ATTR_TYPE dans la base de données). Exemple :

- dob.json
- died.json
- marital.json
- circa_dob.json

- pop.json
- nat.json
- cit.json

Création d'un lien vers le récapitulatif d'entité à partir de l'outil de création de diagramme :

Le récapitulatif d'entité contient des informations détaillées sur des entités spécifiques et est utile pour analyser les alertes et les relations d'entité. Si vous définissez les propriétés de l'adresse URL en indiquant l'application Web qui génère le récapitulatif d'entité, les utilisateurs de l'outil de création de diagramme peuvent ouvrir le récapitulatif d'entité à partir de l'un des diagrammes de l'outil.

Pourquoi et quand exécuter cette tâche

La définition d'un lien est une tâche globale. Une fois le lien défini, tous les utilisateurs qui affichent les diagrammes de l'outil de création de diagramme peuvent accéder au lien dans un menu disponible en cliquant à l'aide du bouton droit de la souris. Si les propriétés du lien ne sont pas définies, l'option **Afficher la reprise** ne s'affiche pas.

Procédure

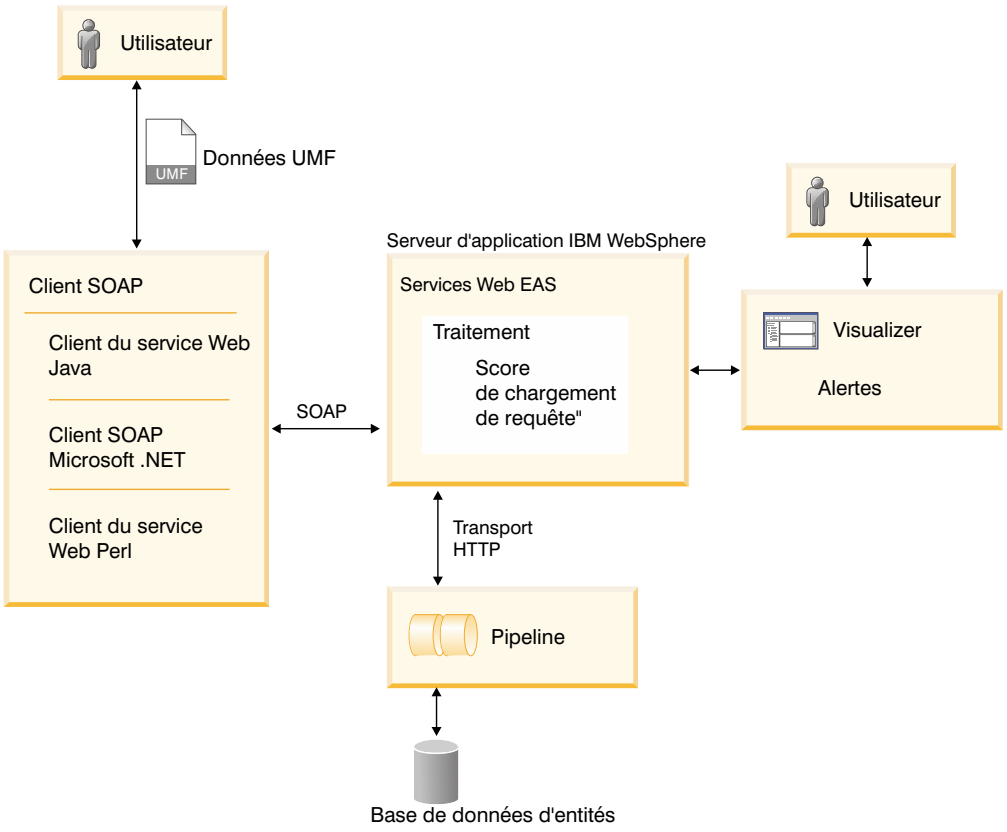
1. Demandez à l'administrateur système de mettre à jour la propriété RESUMESERVER de la table COMPONENT_CONFIG avec un lien vers le rapport Toolkit de Cognos.
   a. Remplacez la valeur de cette propriété par l'adresse URL réelle. Indiquez le serveur hôte, le nom du port et le chemin de l'application Web. Reportez-vous à l'exemple de valeur pour déterminer la forme qu'un chemin peut avoir. Par exemple, si votre société a installé et utilise Analyst Toolkit de Cognos, indiquez le chemin du récapitulatif d'entité généré par Analyst Toolkit.
   b. Vérifiez que le sème **%ISIIEntityID%** figure dans la valeur du paramètre. Ce paramètre envoie l'ID d'entité approprié à l'application Web pour générer le récapitulatif d'entité correct.
2. Facultatif : Testez le lien.

Chapitre 9. Développement

Si vous avez besoin d'utiliser des services Web dans votre environnement, IBM InfoSphere Identity fournit un service Web XML simple.

Services Web

IBM InfoSphere Identity Insight fournit un ensemble de services Web qui vous permettent de créer des applications externes pouvant charger des données UMF (Universal Message Format) pour le traitement pipeline ou la recherche d'entités dans la base de données d'entités. Pour ce faire, utilisez le mode de transport HTTP (hypertext transfer protocol) bidirectionnel, qui est une fonction standard du pipeline.



Les services Web d'IBM InfoSphere Identity Insight utilisent quatre méthodes SOAP (Simple Object Access Protocol) : traitement, recherche, chargement et notation. Ce produit prend en charge SOAP version 1.1.

Le produit comprend plusieurs composants destinés à vous aider lors de vos premières utilisation des services Web.

srd.wsdl
ce fichier contient la définition WSDL (Web services description language) des services Web du produit. Vous pouvez utiliser ce fichier avec n'importe quel toolkit ou technologie SOAP pour lancer les services Web. Pour le

trouver, démarrez WebSphere Liberty et chargez-le à partir de http://hostname:port/easws/resources/wsdl/srd.wsdl

wsutil.jar
Ce fichier est un client test de service Web fourni pour tester l'installation et la configuration de vos services Web. Cet utilitaire se trouve dans le répertoire `ibm-home/easws`.

Configuration logicielle requise par les services Web

Les services Web d'IBM InfoSphere Identity Insight exigent que certains logiciels soient installés et opérationnels.

Avant d'utiliser les services Web, vérifiez que les logiciels suivants sont installés et opérationnels :

- Les services Web d'IBM InfoSphere Identity Insight doivent être installés et en cours d'exécution.
- Le serveur intégré IBM WebSphere Application Server doit être en cours d'exécution à l'endroit où les services Web d'IBM InfoSphere Identity Insight sont déployés. Dans la plupart des cas, il s'agit du même serveur d'application que celui où la console de configuration et le visualiseur sont installés.
- Un pipeline de services Web doit être démarré et en écoute sur l'URL HTTP adéquat. Le serveur d'application tente d'envoyer les données UMF à ce pipeline de services Web via l'URL HTTP indiqué, dès qu'une demande SOAP lui parvient.

  Remarque : L'URL HTTP servant à la communication entre le serveur d'application WebSphere et le pipeline n'est *pas* le même que l'URL par les clients de services Web qui tentent d'envoyer des demandes SOAP. L'envoi de requêtes SOAP directement à l'URL HTTP du pipeline de services Web donne une erreur.

  Par exemple, si WebSphere Application Server est configuré avec la plage de ports par défaut, les numéros de port et leur utilisation sont les suivants :
  - *nnn*0 - port HTTP pour Webserver
  - *nnn*1 - port HTTPS pour Webserver
  - *nnn*2 - port d'administration HTTP
  - *nnn*3 - port d'administration HTTPS
  - *nnn*4 - port SOAP
  - *nnn*5 - Port du serveur d'application.
- Le fichier webservices.properties doit être configuré avec l'URL HTTP du pipeline en cours d'exécution, afin que le serveur intégré WebSphere Application Server sache où trouver le pipeline qui va gérer les demandes des services Web. Ce fichier se trouve généralement dans le répertoire suivant : *racine_produit*`/srd-home/easws`
- Un client de services Web compatible SOAP et WSDL, utilisé pour appeler les services Web d'IBM InfoSphere Identity Insight, doit exister. Un exemple de client, wsutil.jar, est installé avec des services Web IBM InfoSphere Identity Insight pour tester les services des éditions antérieures mais il ne s'applique pas aux services améliorés de la version 8.0, Fix Pack 2.

Démarrage de pipelines de services Web

Pour envoyer et traiter les données via un service Web, démarrez les pipelines à l'aide du transport HTTP bidirectionnel. En général, les pipelines utilisés avec les

services Web restent en fonctionnement constant en arrière-plan, à l'écoute des ports assignés aux données à traiter. Suivez ces instructions pour démarrer un pipeline de services Web.

Avant de commencer

- Assurez-vous de connaître le paramètre d'URL de pipeline configuré dans le fichier webservices.properties. Ce paramètre pointe vers le composant de services Web qui s'exécute sur le serveur intégré IBM Websphere Application Server au niveau du pipeline et doit correspondre à l'URL utilisée pour démarrer les pipelines de services Web.
- L'exécutable de pipeline doit être installé sur le noeud hébergeant ce pipeline.
- Au moins un fichier de configuration de pipeline doit être configuré à des fins d'utilisation avec le pipeline à démarrer. Vous pouvez spécifier le fichier de configuration de pipeline à utiliser dans le cadre de la commande de démarrage du pipeline. Si vous ne spécifiez pas le nom du fichier de configuration dans le cadre de la commande de pipeline, ce fichier doit impérativement se trouver sur le noeud de pipeline et utiliser le nom de fichier de configuration de pipeline par défaut, à savoir pipeline.ini.
- Si vous utilisez un script pour démarrer des pipelines, vérifiez qu'il se trouve dans le même répertoire que celui depuis lequel vous avez démarré le pipeline.
- Si vous voulez acheminer les résultats du traitement depuis ce pipeline ou contrôler les statistiques et l'état du pipeline, enregistrez ce dernier dans la console de configuration sur l'onglet **Pipelines**. Vous devez utiliser l'un des noms de pipelines déjà enregistrés pour démarrer ce pipeline pour que le contrôle ou l'acheminement aboutissent.
- Si vous utilisez le moniteur d'application pour contrôler l'état et les statistiques d'un pipeline, veillez à ce qu'un agent SNMP soit installé sur le noeud de pipeline et qu'il soit et opérationnel avant de démarrer le pipeline en question.
- Si ce pipeline achemine ses résultats vers un autre système ou une autre base de données, assurez-vous que le fichier de routage du pipeline se trouve dans le même répertoire que celui où vous démarrez le pipeline.
- Si la valeur de paramètre système *DEFAULT_CONCURRENCY* est définie sur une valeur supérieure à 1 ou si vous avez configuré le paramètre *concurrency* dans le fichier de configuration de pipeline pour le noeud de pipeline, vous pouvez démarrer plusieurs unités d'exécution de traitement de pipeline parallèles via une seule commande de démarrage de pipeline.

Pourquoi et quand exécuter cette tâche

Un pipeline est démarré en trois étapes :

Procédure

1. Vérifiez qu'il n'existe aucun autre pipeline actif sur le noeud de pipeline ayant le même nom que celui à démarrer. Chaque pipeline doit porter un nom unique sur son noeud (le nom de pipeline par défaut est `pipeline`). Pour vérifier ce point, vous pouvez procéder de deux façons :
   a. Si vous utilisez le moniteur d'application pour vérifier l'état des pipelines ou acheminer les résultats vers d'autres systèmes, consultez l'onglet **Etat du pipeline** pour savoir si un autre pipeline actif porte le même nom que celui que vous voulez utiliser.
   b. Ou, à une invite de commande, tapez la commande suivante :

   ```
   pipeline -n nompipeline -l
   ```

nompipeline étant le nom à utiliser pour démarrer le nouveau pipeline. Vérifiez que ce nom correspond à celui enregistré dans la console de configuration pour ce pipeline.

2. A une invite de commande, démarrez un ou plusieurs pipelines en spécifiant les options et paramètres de commande de pipeline appropriés via ce format :

   ```
   pipeline -option paramètre
   ```

   Remarque : Si vous utilisez Application Monitor pour ce pipeline et qu'il a été enregistré dans la console de configuration pour le contrôle ou l'acheminement, veillez à utiliser l'option `-n` dans la commande de démarrage du pipeline et indiquez le nom de pipeline enregistré. Si le nom de pipeline spécifié ne correspond pas exactement à celui enregistré (y compris la casse), l'état du pipeline ne s'affichera pas correctement sur l'onglet **Etat du pipeline** de la console de configuration et tout acheminement configuré pour ce pipeline échouera.

   Remarque : Généralement, l'option de pipeline `-s` ou `-d` est utilisée pour démarrer le pipeline en mode de service/démon ou débogage, selon le cas.

3. Vérifiez que la commande a fonctionné et que le pipeline est démarré et actif.
   a. Si vous utilisez Application Monitor et que ce pipeline a été enregistré dans la console de configuration, consultez l'onglet **Etat du pipeline**. Si le pipeline est actif, l'état affiché est `Actif`.
   b. Si votre système s'exécute sur une plateforme Microsoft Windows et que vous utilisez l'option de pipeline de services, vous pouvez voir l'état du pipeline dans le panneau de configuration des services Microsoft Windows.
   c. Si votre système s'exécute sur une plateforme UNIX et que vous utilisez l'option de pipeline de type démons, vous pouvez saisir la commande suivante pour vérifier les processus en cours d'exécution :

      ```
      ps -fu idutilisateur
      ```

      idutilisateur étant l'identification de l'utilisateur démarrant le pipeline.
   d. Ou, à une invite de commande, tapez la commande suivante :

      ```
      pipeline -nnompipeline -l
      ```

      nompipeline étant le nom du pipeline que vous venez de démarrer. Si le pipeline est actif, l'invite de commande renvoie `En cours d'exécution`.

Que faire ensuite

Cette commande de pipeline démarre le nombre d'unités d'exécution de traitement de pipeline défini par le paramètre de simultanéité du fichier de configuration de pipeline. Le nombre d'enregistrements traités simultanément est déterminé par le paramètre de simultanéité inclus dans l'option de transport HTTP.

Test des services Web

A l'aide du client test fourni, wsutil.jar, vous pouvez tester l'installation et la configuration des services Web d'IBM InfoSphere Identity Insight.

Avant de commencer

- Il faut que les services Web soient installés.
- Vérifiez que le serveur intégré WebSphere Application Server est en cours d'exécution.
- Le serveur d'applications doit disposer d'au moins un fichier de configuration de pipeline configuré pour les pipelines de services Web.

- Vérifiez que le fichier webservices.properties est configuré avec le paramètre d'URL de pipeline correct. Ce pipeline de services Web doit être en cours d'exécution.
- Créez au moins un document d'entrée UMF test à utiliser durant les tests.

Procédure

1. Sur le serveur intégré WebSphere Application Server, accédez au répertoire contenant le fichier wsutil.jar. Ce fichier se trouve généralement à l'emplacement suivant : *racine_installation*/ewas/webservice/wsutil.jar
2. Sur une ligne de commande à partir de ce répertoire, tapez la syntaxe de commande wsutil.jar de l'opération à effectuer : `java -jar wsutil.jar –-<méthode SOAP>=<URI> --input=<URL> –-output=<URI>`

Exemple de test de la méthode de chargement des services Web

La commande wsutil.jar suivante charge les enregistrements du fichier UMF «raw_entities.umf »et enregistre les résultats dans le fichier UMF «results.umf» :

```
java -jar wsutil.jar --load=http://localhost:13510/easws/services/SRDWebService
 --input=raw_entities.umf --output=results.umf
```

Fichier srd.wsdl

Pour communiquer avec les services Web d'IBM InfoSphere Identity Insight, vous devez utiliser un client de services Web. Lorsque vous installez les services Web d'IBM InfoSphere Identity Insight, le fichier srd.wsdl est également installé et contient les méthodes SRDWebService qui servent à communiquer avec les services Web d'InfoSphere Identity Insight. Vous pouvez utiliser le fichier srd.wsdl pour générer un client de services Web à utiliser avec les services Web d'IBM InfoSphere Identity Insight.

Le fichier srd.wsdl est accessible via le navigateur Web en accédant au serveur intégré WebSphere Application Server qui héberge les services Web. Généralement, ce fichier se trouve sur le serveur IBM WebSphere Application Server, à l'URL racine suivante :

`http://`*`IBM_WebSphere_Application_Server_host`*`:`*`port_installation`*`/easws/resources/wsdl/srd.wsdl`

Exemple :

`http://localhost:13510/easws/resources/wsdl/srd.wsdl`

Remarque : Assurez-vous que le serveur d'application fonctionne avant de tenter d'accéder au fichier srd.wsdl.

Vous pouvez également bâtir un client wsdl de services Web à l'aide de n'importe quelle plateforme de développement acceptant les services Web avec un kit de développement SOAP, notamment :

- Java avec IBM WebSphere Application Server
- Java avec Apache Axis
- Microsoft .NET
- Perl

Reportez vous aux instructions figurant dans la documentation de votre plateforme de développement pour créer un client de services Web au moyen d'un fichier wsdl.

Si vous créez un wsdl de client de services Web autre que le client de services Web srd.wsdl, assurez-vous que l'URL de déploiement désigne bien le client wsdl.

Méthodes SRDWebService

Le fichier srd.wsdl contient les méthodes SRDWebService qui permettent de communiquer avec les services Web d'IBM InfoSphere Identity Insight. SRDWebService contient trois méthodes : une pour charger les données dans la base de données d'entités, une pour effectuer une recherche afin d'interroger la base de données d'entités et une pour traiter les fonctionnalités de pipeline disponibles via UMF.

Méthode loadRecord

```
LoadResult loadRecord(String umfEntity)
```

L'objet LoadResult retourné par la méthode loadRecord() contient deux membres :

Membre	Description	Type
entityID	ID de l'entité renvoyée	Long
merged	Balise indiquant si l'entité a été résolue en une entité existante ou si c'en était une nouvelle	Booléen

Le paramètre umfEntity est une chaîne XML en UMF qui représente les données d'une seule entité. Consultez dans la spécification UMF les instructions sur la façon d'élaborer convenablement un enregistrement UMF_ENTITY, en veillant à définir les valeurs adéquates pour DSRC_ACCT et DSRC_REF.

Si la méthode load vous permet de traiter des documents UMF_ENTITY, elle ne renvoie pas le document de sortie UMF brut. Elle renvoie un objet LoadResult contenant l'ID d'entité et une balise indiquant s'il s'agit d'une nouvelle entrée ou si elle a été résolue avec une existante. Utilisez la méthode process à la place de cette méthode, si cela ne vous pose pas de problème d'effectuer l'analyse syntaxique du document de sortie UMF. La méthode load vous évite d'avoir à effectuer l'analyse syntaxique du document de sortie UMF résultant depuis l'opération de chargement.

Méthode basicQuery()

```
String basicQuery(String umfSearch)
```

La chaîne d'entrée de la méthode basicQuery() doit correspondre à un enregistrement UMF_SEARCH. La chaîne XML que retourne basicQuery() contient le résultat UMF_SEARCH_RESULT de la requête.

Il existe deux formes de requêtes intégrées : les requêtes récapitulatives d'ensemble de résultats et es requêtes approfondies détaillées.

Remarque : Cette méthode existe uniquement pour la compatibilité amont. Dans cette édition, cette méthode fonctionne comme la méthode process. Utilisez la méthode process à la place de la méthode basicQuery() pour toutes les nouvelles applications client.

Méthode process()

```
String process(String umfRequestDocument)
```

Utilisez la méthode process pour traiter n'importe quel document d'entrée UMF et recevoir comme résultat un document de sortie UMF. La méthode process vise à traiter toutes les demandes et réponses prises en charge par le pipeline et est la mieux adaptée pour toutes les opérations.

Cette méthode admet un paramètre String et renvoie un résultat String.

wsutil.jar

Wsutil.jar est une application Java basée sur une ligne de commande installée lors de l'installation des services Web d'IBM InfoSphere Identity Insight. Il s'agit d'un exemple de client qui vous permet d'essayer chacune des méthodes SOAP des services Web afin de tester l'installation et la configuration des services Web.

Le client test wsutil.jar doit se trouver à l'emplacement suivant :

racine_installation/ewas/webservice

Syntaxe d'utilisation de wsutil.jar

Wsutil.jar est une application Java basée sur la ligne de commande qui est fournie comme client test afin de tester l'installation et la configuration des services Web d'IBM InfoSphere Identity Insight. Pour utiliser wsutil.jar, vous devez indiquer un opérateur wsutil.jar avec les modificateurs d'entrée et de sortie correspondants.

La syntaxe de wsutil.jar dépend de l'opération de services Web que vous souhaitez tester :

```
wsutil (unix) ou wsutil.bat (win) --opérateur=URI --entrée=URI --sortie=URI
```

aide

Affiche l'aide en ligne et les informations de ligne de commande du client test wsutil.jar.

```
wsutil (unix) ou wsutil.bat (win) --help
```

load=*URI*

Désigne les fiches UMF de style de pipeline et l'URI (Uniform Resource Identifier) de l'interface des services Web d'IBM InfoSphere Identity Insight.

```
wsutil (unix) ou wsutil.bat (win) --load=URI [--xslt=URI][--
entrée=URI][--sortie=URI]
```

Cette opération charge les enregistrements UMF à partir de l'URI indiqué dans les pipelines de services Web pour le traitement de la résolution d'entité. Après le traitement, l'opération renvoie l'ID d'entité et un indicateur précisant si l'entité entrante a été fusionnée avec une entrée existante ou a entraîné la création d'une entité.

process=*URI*

Désigne les fiches UMF ou XML génériques et l'URI de l'interface des services Web d'IBM InfoSphere Identity Insight.

```
wsutil (unix) ou wsutil.bat (win) --process=URI [--xslt=URI][--
entrée=URI][--sortie=URI]
```

Utilisez cette opération pour traiter n'importe quel document d'entrée UMF et recevoir comme résultat un document de sortie UMF. La méthode process vise

à traiter toutes les demandes et réponses prises en charge par le pipeline. Elle représente généralement la méthode la mieux adaptée à toutes les opérations.

search=*URI*
Désigne les demandes et réponses UMF de style de recherche via pipeline avec l'URI de l'interface des services Web d'IBM InfoSphere Identity Insight.

`wsutil (unix) ou wsutil.bat (win) --score=URI [--xslt=URI][--entrée=URI][--sortie=URI]`

Cette opération recherche une entité spécifique dans la base de données d'entité et renvoie les informations demandées concernant cette entité, ou bien interroge la base de données d'entité afin de savoir quelles entités correspondent à un attribut donné et en renvoie la liste.

xslt=*URI*
Désigne la transformation XSLT et le fichier XML que l'opération convertira en enregistrements UMF.

`wsutil (unix) ou wsutil.bat (win) --xslt=URI][--entrée=URI][--sortie=URI]`

Cette opération permet de convertir des enregistrements XML au format UMF avant d'utiliser l'une des opérations de services Web.

modificateurs wsutil.jar

Utilisez ces modificateurs avec les opérateurs wsutil.jar pour indiquer les méthodes d'entrée et de sortie de la commande de services Web.

input=*URI*
Désigne la méthode d'entrée des enregistrements UMF. La méthode d'entrée par défaut est stdin.

output=*URI*
Désigne la méthode de sortie des enregistrements UMF. La méthode de sortie par défaut est stdout. Cette méthode permet de désigner l'emplacement et le nom du fichier dans lequel la sortie UMF va être enregistrée.

Exemple d'utilisation de wsutil.jar

La commande wsutil.jar suivante d'un système UNIX charge les fiches à partir d'un fichier, les convertit au format UMF et affiche les résultats sur la console de l'interface de ligne de commande :

```
wsutil --load=http://localhost:13510/easws/services/SRDWebService
--input=raw_entities.xml --xslt=transform.xsl
```

La commande wsutil.jar suivante d'un système Windows acquiert les demandes provenant de stdin et affiche les résultats sur la console de l'interface de ligne de commande :

```
wsutil.bat --process=http://localhost:13510/SRDWebService
```

Elaboration d'interrogations vis-à-vis de la base de données d'entités

IBM InfoSphere Identity Insight propose plusieurs manières d'interroger la base de données d'entités. Vous pouvez élaborer des recherches de pipeline de services Web afin de rechercher dans la base de données les entités concordants avec certains critères d'attributs précis. Vous pouvez également élaborer des recherches via pipeline de services Web afin d'interroger la base de données sur une entité précise.

Recherches via pipeline de services Web

Intégrées aux pipelines, une interface de recherche et d'interrogation dynamiques constituent un point d'accès unique pour que les services Web puissent interroger la base de données d'entités. A l'aide de documents d'entrée UMF, il faut structurer la demande, puis envoyer le document d'entrée UMF via les service Web aux pipelines, en vue du traitement. A l'issue du traitement, le pipeline renvoie un document de sortie UMF où figurent les résultats.

Les recherches via pipeline de services Web apportent les réponses à deux types de questions :

Quelles entités de la base de données d'entités concordent avec un attribut ou jeu d'attributs particulier ? (UMF_SEARCH)

Ce type de recherche via pipeline de services Web tire pleinement parti de la résolution d'entité pour reconnaître et standardiser les critères de recherche entrants, puis faire concorder les critères de recherche avec des entités de la base de données. Cela s'appelle une interrogation récapitulative ou de l'ensemble de résultats, et renvoie la liste des entités dont des valeurs de données concordent avec la valeur d'attribut ou liste de valeurs d'attributs demandée.

Pour effectuer une interrogation récapitulative ou de l'ensemble de résultats, il faut créer un document d'entrée UMF_SEARCH contenant les critères de recherche dont se sert le pipeline pour exécuter la résolution d'entité. Le pipeline répond en renvoyant un document de sortie UMF_SEARCH_RESULT avec les résultats de l'interrogation, à savoir la liste des entités concordant avec les critères de recherche.

De quelles informations la base de données d'entités dispose-t-elle sur une entité spécifique ? (UMF_QUERY)

Ce type de recherche via pipeline de services Web se sert d'instructions et paramètres SQL pour interroger la base de données d'entités. Cela s'appelle une interrogation détaillée ou en aval, et renvoie la liste détaillées des informations sur une seule entité.

Pour effectuer une interrogation détaillée ou en aval, il faut créer un document d'entrée UMF_QUERY qui indique sur quelle entité de la base de données vous désirez des renseignements. Le pipeline répond en renvoyant un document de sortie UMF_QUERY_RESULT fournissant le détail sur l'entité concernée.

Tandis qu'ils effectuent les recherches via pipeline de services Web, les pipelines accomplissent toutes les fonctions de pipeline standard, dont la consignation.

L'entrée (demande) et la sortie (réponse) des recherches via pipeline de services Web utilisent toutes deux des documents UMF et structurent les informations en UMF.

Formats de recherche via pipeline de services Web

Ce produit contient plusieurs formats intégrés pour chacune des recherches via pipeline de services Web :

Formats UMF_SEARCH

WS_SUMMARY_TOP10
Renvoie la liste des dix entités de la base de données concordant au plus près avec les données d'attributs indiquées dans les critères de recherche

WS_SUMMARY_TOP100
Renvoie la liste des cent entités de la base de données concordant au plus près avec les données d'attributs indiquées dans les critères de recherche

WS_SUMMARY
Renvoie la liste de toutes les entités de la base de données concordant avec les données d'attributs indiquées dans les critères de recherche

UMF_QUERY formats

WS_DETAIL
Renvoie toutes les données de la base sur l'ID d'entité demandé

WS_RELATION
Renvoie la liste de toutes les entités de la base de données qui sont apparentées à un degré à l'entité d'entrée

WS_ALERT
Renvoie la liste de toutes les alertes de la base de données d'entités impliquant l'ID d'entité d'entrée

Il faut indiquer quel format prédéfini appliquer, dans la balise FORMAT_CODE, dans le document d'entrée UMF adéquat.

Considérations sur les performances

Les recherches via pipeline de services Web où figurent davantage de critères signifient généralement que le système compare à un moindre nombre d'entités dans la base de données. Cela signifie à son tour que le système renvoie les résultats plus vite que les recherches comportant moins de critères.

Elaboration d'interrogations de services Web pour rechercher une entité précise

Suivez ces instructions pour élaborer un document d'entrée UMF_QUERY destiné à rechercher une entité spécifique dans la base de données d'entités. Ce document d'entrée UMF_QUERY doit être envoyé dans un pipeline de services Web pour traitement. Une fois l'interrogation traitée par le pipeline, les services Web renvoient un document de sortie UMF_QUERY_RESULT qui contient les détails de l'entité d'entrée demandée.

Avant de commencer

Le serveur intégré WebSphere Application Server doit être en cours d'exécution et au moins un pipeline de services Web doit être démarré et en cours d'exécution pour recevoir et traiter le document d'entrée UMF_QUERY.

Pourquoi et quand exécuter cette tâche

Etant donné que la demande de recherche est un document d'entrée UMF, les critères doivent être formatés à l'aide de balises UMF valides. Vous pouvez employer n'importe quel éditeur de texte ou utilitaire qui crée des données UMF.

Procédure

1. Créez un nouveau document d'entrée UMF_QUERY.
2. Dans le segment ROOT, saisissez les balises et valeurs UMF nécessaires.
   a. Saisissez le code de source de données dans la balise DSRC_CODE. Le code de source de données par défaut pour les recherches de pipeline de services Web est 1589. Si vous utilisez un autre code de source de données que le code par défaut des recherches de pipeline de services Web, assurez-vous qu'il soit configuré pour ne pas résoudre les entités.
   b. Entrez le code de référence de source de données qui référence la transaction de message à l'origine de la demande dans la balise DSRC_REF. Le code de référence de source de données doit être pertinent, car il est renvoyé à l'application appelante.
   c. Saisissez le code de format qui indique le format de sortie des résultats à l'aide de la balise FORMAT_CODE. Les pipelines contiennent trois codes de format intégrés pour les recherches via pipeline de services Web à l'aide d'UMF_QUERY :
      - WS_DETAIL, qui renvoie toutes les données d'entité disponibles pour l'ID d'entité d'entrée ;
      - WS_RELATION, qui renvoie la liste de toutes les entités apparentées à l'ID d'entité d'entrée par une relation à un degré ;
      - la requête WS_ALERT, qui renvoie toutes les alertes de rôle dans le système impliquant l'ID d'entité d'entrée.

      Si vous utilisez un autre code de format, il doit être configuré dans la table UMF_OUTPUT_FORMAT.
   d. Dans la balise ENTITY_ID, saisissez l'ID de l'entité sur laquelle vous souhaitez renvoyer des données.
3. Indiquez tout autre critère de recherche à l'aide des autres segments UMF facultatifs <NAME>, <ADDRESS>, <EMAIL>, <ATTRIBUTE> et <NUMBER>.
4. Envoyez le document d'entrée UMF_QUERY à un pipeline de services Web.

Résultats

Un pipeline de services Web traite le document UMF_QUERY à l'aide des critères définis pour rechercher dans la base de données les entités concordant avec l'interrogation. Le pipeline traite ensuite l'interrogation, crée des fichiers de journalisation standard, puis renvoie les résultats à l'application appelante, dans un document de sortie UMF_QUERY_RESULT via les services Web.

Exemple de recherche UMF_QUERY

Cet exemple d'interrogation UMF_QUERY recherche toutes les informations sur l'ID d'entité 1223 :

Remarque : le format choisi pour cet exemple est utilisé dans un souci de lisibilité et ne respecte pas le format obligatoire d'une ligne par enregistrement UMF.

```
<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>
```

Document d'entrée UMF_QUERY

Le document d'entrée UMF_QUERY contient la série de segments UMF qui structurent les données entrantes pour rechercher dans la base de données d'entités contenant des valeurs d'attribut qui concordent avec les critères de recherche, puis renvoient la liste d'entités à l'application appelante. Il contient les critères de recherche et de demande d'une recherche via le pipeline de services Web.

Les informations d'un document d'entrée UMF_QUERY reposent sur des instruction SQL. Les résultats de cette recherche via le pipeline de services Web sont renvoyés à l'application appelante dans un document de sortie UMF_QUERY_RESULT. UMF_QUERY effectue une requête "Enhanced Query / Find by Attribute".

Ces éléments et segments UMF requis comprennent le document d'entrée UMF_QUERY :

DSRC_CODE
Balise UMF de code de source de données qui est obligatoire car elle référence et identifie l'application appelante. Dans le cadre de la consignation de pipeline normale, ce code de source de données est consigné dans la table UMF_LOG pour chaque requête UMF_QUERY traitée.

Le système est préconfiguré avec un code de source de données, 1589, qui peut s'utiliser pour toutes les recherches via pipeline de services Web. Ce code de source de données effectue le traitement de résolution d'entité sans résoudre les critères de recherche entrants avec l'entité de la base de données d'entités qui concorde avec la recherche. Vous pouvez créer votre propre code de source de données pour une application appelante particulière ; veillez simplement à ce qu'il soit configuré pour ne pas résoudre d'entités.

DSRC_REF
Balise UMF de référence de source de données qui est obligatoire car elle référence la transaction de message demandeuse et est renvoyée à l'application appelante.

FORMAT_CODE
Balise UMF qui corrèle avec un format de document de sortie UMF qui est indiqué dans la table UMF_OUTPUT_FORMAT. IBM InfoSphere Identity Insight contient trois codes de format intégrés pour les recherches via pipeline de services Web à l'aide d'UMF_QUERY :

- WS_DETAIL, qui renvoie toutes les données d'entité disponibles pour l'ID d'entité demandé ;
- WS_RELATION, qui renvoie la liste de toutes les entités apparentées à l'entité d'entrée à un degré ;
- WS_ALERT, qui renvoie toutes les alertes dans le système impliquant l'ID d'entité d'entrée.

Pour effectuer une requête amélioré (EQ) (Requête améliorée / Rechercher par attribut) via ce document d'entrée, le FORMAT_CODE suivant doit être indiqué.

Exemple ENHANCED_QUERY_RESULT :

```
<UMF_QUERY>
<FORMAT_CODE>ENHANCED_QUERY_RESULT</FORMAT_CODE>
 <ATTRIBUTE>
```

```
  <ATTR_TYPE>CIT</ATTR_TYPE>
  <ATTR_VALUE>CANADA</ATTR_VALUE>
 </ATTRIBUTE>
</UMF_QUERY>
```

ENTITY_ID
Cette balise UMF obligatoire désigne l'ID de l'entité dans la recherche. Le système renvoie une réponse qui renseigne en détail sur les données connues concernant cette entité de la base de données d'entités, selon les autres critères d'interrogation.

Vous indiquez ensuite les critères de recherche optionnels au moyen des autres segments UMF disponibles et de leurs balises valides de noms, adresses, numéros, caractéristiques et adresses électroniques.

NAME
Recherchez les attributs de nom qui définissent le nom de la personne, l'organisation, le lieu ou l'élément, tels que définis par le modèle d'entité et l'identité entrante.

NUMBER
Recherchez les attributs de numéro qui se composent de données généralement décrites sous forme de numéro, telles que le numéro de carte de crédit, numéro de téléphone et numéro de passeport.

ADDRESS
Recherchez les attributs d'adresse qui définissent une localisation de l'identité et contiennent généralement les informations d'adresse standard : numéro et nom de rue, numéro du bâtiment, code postal, localité, état et pays.

ATTRIBUTE
Recherchez les attributs de caractéristique qui définissent d'autres spécificités ou informations identitaires qui ne sont pas exprimées par les autres types d'attributs.

EMAIL
Recherchez les attributs d'adresse électronique qui définissent les adresses de messagerie Internet.

Exemple de recherche UMF_QUERY

Cet exemple de UMF_QUERY applique le code au format WS_DETAIL pour interroger la base de données d'entités et renvoyer toutes les informations recensées sur l'ID d'entité 1223 :

Remarque : le format choisi pour cet exemple est utilisé dans un souci de lisibilité et ne respecte pas le format obligatoire d'une ligne par enregistrement UMF.

```
<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>
```

Code de format WS_DETAIL :

Quand vous élaborez une recherche via pipeline de services Web pour connaître les détails concernant une entité particulière de la base de données d'entité, utilisez

le code de format intégré WS_DETAIL. Ce code de format est indiqué dans le document d'entrée UMF_QUERY qui contient les critères de la requête.

Exemple de recherche via pipeline de services Web au moyen du code de format WS_DETAIL

Cet exemple de recherche via pipeline de services Web renvoie toutes les informations de la base de données d'entités sur Joe Franklin, ID d'entité 87.

Remarque : Le format choisi pour cet exemple est utilisé dans un souci de lisibilité et ne respecte pas le format obligatoire d'une ligne par enregistrement UMF.

Pour solliciter le détail de l'ID d'entité 87 (Joe Franklin), créez un document d'entrée UMF_QUERY avec la demande :

```
<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>
```

Après avoir envoyé ce document UMF_QUERY via les services Web en vue de leur traitement par un pipeline de services Web, l'application appelante reçoit une réponse dans le document UMF_QUERY_RESULT suivant :

```
<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>
```

A partir de cette réponse, vos pouvez constater qu'il existe trois sources de données détenant des informations sur Joe Franklin : la liste de l'OFAC, une liste du FBI et la liste A9. Joe utilise deux adresses différentes, mais dans chaque cas, les mêmes numéros de téléphone et de carte de crédit.

Code de format WS_ALERT :

Quand vous élaborez une recherche via pipeline de services Web pour connaître toutes les alertes de rôle de la base de données d'entités concernant une entité précise, utilisez le code de format intégré WS_ALERT. Ce code de format est indiqué dans le document d'entrée UMF_QUERY qui contient les critères de la requête.

Exemple de recherche via pipeline de services Web au moyen du code de format WS_ALERT

Cet exemple de recherche via pipeline de services Web renvoie la liste de toutes les alertes de rôle impliquant Joe Franklin, ID d'entité ID 87.

Remarque : Le format choisi pour cet exemple est utilisé dans un souci de lisibilité et ne respecte pas le format obligatoire d'une ligne par enregistrement UMF.

Pour solliciter les alertes de rôle pour l'entité ID 87 (Joe Franklin), créez un document d'entrée UMF_QUERY avec la demande :

```
<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>
```

Après avoir envoyé ce document UMF_QUERY via les services Web en vue de leur traitement par un pipeline de services Web, l'application appelante reçoit une réponse dans le document UMF_QUERY_RESULT suivant :

```
<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>
```

A partir de cette réponse, vos pouvez constater qu'il existe deux alertes de rôle pour Joe Franklin : une où l'employée Susan Miller connaît Joe, l'autre où le fournisseur Julio Martinez connaît Joe.

Code de format WS_RELATION :

Quand vous élaborez une recherche via pipeline de services Web pour obtenir la liste de toutes les entités apparentées à un degré avec une entité particulière, utilisez le code de format intégré WS_RELATION. Ce code de format est indiqué dans le document d'entrée UMF_QUERY qui contient les critères de la requête.

Exemple de recherche via pipeline de services Web au moyen du code de format WS_RELATION

Cet exemple de recherche via pipeline de services Web renvoie la liste de toutes les entités apparentées à un degré avec Joe Franklin, ID d'entité 87.

Remarque : Le format choisi pour cet exemple est utilisé dans un souci de lisibilité et ne respecte pas le format obligatoire d'une ligne par enregistrement UMF.

```
<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>
```

Après avoir envoyé ce document UMF_QUERY via les services Web en vue de leur traitement par un pipeline de services Web, l'application appelante reçoit une réponse dans le document UMF_QUERY_RESULT suivant :

```
<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>
```

Elaboration d'interrogations de services Web pour rechercher des entités avec des attributs similaires

Suivez ces instructions pour élaborer un document d'entrée UMF_SEARCH afin de rechercher des entités dans la base de données d'entités qui concordent avec les valeurs de données des attributs spécifiés dans les critères de recherche. Envoyez ce document d'entrée UMF_SEARCH dans un pipeline de services Web pour traitement. Une fois l'interrogation traitée par le pipeline, les services Web renvoient un document de sortie UMF_SEARCH_RESULTS qui contient la liste des entités répondant aux critères de recherche.

Avant de commencer

Le serveur intégré WebSphere Application Server doit être en cours d'exécution et au moins un pipeline de services Web doit être démarré et en cours d'exécution pour recevoir et traiter le document d'entrée UMF_SEARCH.

Pourquoi et quand exécuter cette tâche

Etant donné que la demande de recherche est un document d'entrée UMF, les critères doivent être formatés à l'aide de balises UMF valides. Vous pouvez employer n'importe quel éditeur de texte ou utilitaire qui crée des données UMF.

Procédure

1. Créez un nouveau document d'entrée UMF_SEARCH.
2. Dans le segment ROOT, saisissez les balises et les valeurs UMF requises ainsi que toutes les balises et valeurs UMF facultatives que vous souhaitez utiliser pour définir les critères de recherche. Saisissez au minimum des valeurs pour les balises UMF suivantes :
   a. Saisissez le code de source de données dans la balise DSRC_CODE. Le code de source de données par défaut pour les recherches de pipeline de services Web est 1589. Si vous utilisez un autre code de source de données que le code par défaut des recherches de pipeline de services Web, assurez-vous qu'il soit configuré pour ne pas résoudre les entités.
   b. Entrez le code de référence de source de données qui référence la transaction de message à l'origine de la demande dans la balise DSRC_REF. Le code de référence de source de données doit être pertinent, car il est renvoyé à l'application appelante.
   c. Saisissez le code de format qui indique le format de sortie des résultats à l'aide de la balise FORMAT_CODE. Les pipelines contiennent trois codes de format intégrés pour les recherches via pipeline de services Web à l'aide d'UMF_SEARCH :
      - WS_SUMMARY_TOP10, qui renvoie les dix premières entités répondant aux critères de recherche ;
      - WS_SUMMARY_TOP100, qui renvoie les cent premières entités répondant aux critères de recherche ;
      - WS_SUMMARY, qui renvoie toutes les entités qui concordent avec les critères de recherche

      Si vous utilisez un autre code de format, il doit être configuré dans la table UMF_OUTPUT_FORMAT.
   d. Indiquez le score de résolution minimum dans la balise MIN_LIKE_SCORE afin de définir le score numérique le plus bas pouvant être considéré comme une correspondance entre les valeurs d'attribut des critères de recherche et les entités de la base de données contenant les mêmes attributs. Plus le score est élevé, plus la concordance doit être exacte. Un score de 100 indique une concordance exacte.
3. A l'aide des autres segments valides du document d'entrée UMF, indiquez les valeurs de données pour les attributs qui composent les critères de recherche. Ces valeurs correspondent aux attributs dont la recherche de pipeline de services Web a besoin pour élaborer la liste des entités faisant apparaître des valeurs concordantes ou similaires. Le degré de concordance dépend de la valeur de MIN_LIKE_SCORE.
4. Envoyez le document d'entrée UMF_SEARCH via les services Web.

Résultats

Un pipeline de services Web traite le document UMF_SEARCH en appliquant le processus de résolution d'entité pour rechercher des entités dans la base de données à l'aide des critères définis. Le pipeline traite ensuite l'interrogation, crée des fichiers de journalisation standard, puis renvoie les résultats à l'application appelante dans un document UMF_SEARCH_RESULTS via les services Web et au format sélectionné.

Exemple de document d'interrogation UMF_SEARCH

Cet exemple de document d'entrée UMF_SEARCH utilise le code de format WS_SUMMARY_TOP10 pour rechercher dans la base de données d'entités les dix premières entités possédant des numéros de sécurité sociale dont la valeur des données correspond exactement à la valeur 555-09-8761 :

Remarque : le format choisi pour cet exemple est utilisé dans un souci de lisibilité et ne respecte pas le format obligatoire d'une ligne par enregistrement UMF.

```
<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>
```

Document d'entrée UMF_SEARCH

Le document d'entrée UMF_SEARCH contient les critères de recherche et de demande d'une recherche via le pipeline de services Web. Il contient la série de segments UMF qui structurent les données entrantes pour rechercher dans la base de données des entités contenant des valeurs d'attribut qui concordent avec les critères de recherche, puis renvoient la liste d'entités à l'application appelante. Les résultats de cette recherche via le pipeline de services Web sont renvoyés à l'application appelante dans un document de sortie UMF_SEARCH_RESULT. UMF_SEARCH lance une procédure complète "Recherche par résolution".

Ces éléments et segments UMF requis comprennent le document d'entrée UMF_SEARCH :

DSRC_CODE

Balise UMF de code de source de données qui est obligatoire car elle référence et identifie l'application appelante. Dans le cadre de la consignation de pipeline normale, ce code de source de données est consigné dans la table UMF_LOG pour chaque requête UMF_SEARCH traitée.

Le système est préconfiguré avec un code de source de données, 1589, qui peut s'utiliser pour toutes les recherches via pipeline de services Web. Ce code de source de données effectue le traitement de résolution d'entité sans résoudre les critères de recherche entrants avec l'entité de la base de données d'entités qui concorde avec la recherche. Vous pouvez créer votre propre code de source de données pour une application appelante particulière ; veillez simplement à ce qu'il soit configuré pour ne pas résoudre d'entités.

DSRC_REF
Balise UMF de référence de source de données qui est obligatoire car elle référence la transaction de message demandeuse et est renvoyée à l'application appelante.

SRC_CREATE_DT
Balise UMF de date de création de source qui est facultative. Si cette balise contient une valeur, elle sert à la consignation.

SRC_LSTUPD_DT
Balise UMF de date de dernière mise à jour de source, qui est facultative. Si cette balise contient une valeur, elle sert à la consignation.

SRC_LSTUP_US
Balise UMF d'utilisateur de dernière mise à jour de la source, qui est facultative. Si cette balise contient une valeur, elle sert à la consignation.

MIN_LIKE_SCORE
Balise UMF de score de résolution (ou ressemblance) minimum qui est obligatoire pour établir la plus faible valeur concordante des autres segments et balises UMF indiqués. Ce score numérique détermine ce qui est considéré comme une concordance entre les valeurs d'attribut demandées et les entités de la base de données dotées des mêmes attributs. Plus le score est élevé, plus la concordance doit être exacte. Un score de 100 indique une concordance exacte.

Par exemple, si la recherche vise à trouver toutes les entités possédant un numéro de sécurité sociale précis, la balise MIN_LIKE_SCORE détermine à quel degré un numéro de sécurité sociale doit concorder avec la valeur de sécurité sociale indiquée dans la requête avant qu'une entité de la base de données soit répertoriée comme composante de l'ensemble de résultats de cette requête.

FORMAT_CODE
Balise UMF qui corrèle avec un format de document de sortie UMF qui est indiqué dans la table UMF_FORMAT_CODE. IBM InfoSphere Identity Insight contient trois codes de format intégrés pour les recherches via pipeline de services Web à l'aide d'UMF_SEARCH :

- WS_SUMMARY_TOP10, qui renvoie les dix premières entités répondant aux critères de recherche ;
- WS_SUMMARY_TOP100, qui renvoie les cent premières entités répondant aux critères de recherche ;
- WS_SUMMARY, qui renvoie toutes les entités qui concordent avec les critères de recherche

La seule différence entre ces interrogations est le nombre d'enregistrements renvoyé, désigné dans le nom de la requête.

Vous indiquez ensuite les critères de recherche optionnels au moyen des autres segments UMF disponibles et de leurs balises valides de noms, adresses, numéros, caractéristiques et adresses électroniques.

NAME
Recherchez les attributs de nom qui définissent le nom de la personne, l'organisation, le lieu ou l'élément, tels que définis par le modèle d'entité et l'identité entrante.

NUMBER
Recherchez les attributs de numéro qui se composent de données

généralement décrites sous forme de numéro, telles que le numéro de carte de crédit, numéro de téléphone et numéro de passeport.

ADDRESS
Recherchez les attributs d'adresse qui définissent une localisation de l'identité et contiennent généralement les informations d'adresse standard : numéro et nom de rue, numéro du bâtiment, code postal, localité, état et pays.

ATTRIBUTE
Recherchez les attributs de caractéristique qui définissent d'autres spécificités ou informations identitaires qui ne sont pas exprimées par les autres types d'attributs.

EMAIL
Recherchez les attributs d'adresse électronique qui définissent les adresses de messagerie Internet.

Exemple de requête UMF_SEARCH

Cet exemple de requête UMF_SEARCH renvoie les cinq premières entités de la base de données dont le numéro de sécurité sociale concorde exactement avec celui-ci : 555-09-8761. Même si le système trouve davantage d'entités, seules les cinq premières figurent dans la liste.

Remarque : le format choisi pour cet exemple est utilisé dans un souci de lisibilité et ne respecte pas le format obligatoire d'une ligne par enregistrement UMF.

```
<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>
```

Codes de format WS_SUMMARY :

IBM InfoSphere Identity Insight contient trois codes de format préconfigurés afin d'être utilisés avec le document d'entrée UMF_SUMMARY : WS_SUMMARY, WS_SUMMARY_TOP10 et WS_SUMMARY_TOP100. Ces codes de format renvoient la liste des entités qui concordent avec les critères définis dans le document d'entrée UMF_SUMMARY. La seule différence entre ces codes de format est le nombre maximal d'enregistrements renvoyé, désigné dans le nom du code de format.

Exemple de recherche via pipeline de services Web au moyen du code de format WS_SUMMARY_TOP10

Cet exemple de recherche via pipeline de services Web renvoie les dix entités de la base de données d'entités qui concordent le plus avec les critères de recherche suivants :

- Nom : Joe Franklin
- Téléphone : 415-555-3325
- Date de naissance : 2 janvier 1956

Il se sert du document d'entrée UMF_SEARCH pour indiquer ces critères qui désignent également le code de formatWS_SUMMARY_TOP10.

Remarque : Le format choisi pour cet exemple est utilisé dans un souci de lisibilité et ne respecte pas le format obligatoire d'une ligne par enregistrement UMF.

```
<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>
```

Après avoir envoyé ce document UMF_SEARCH via les services Web en vue de leur traitement par un pipeline de services Web, l'application appelante reçoit une réponse dans le document UMF_SEARCH_RESULT suivant :

```
<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>
```

Dans ce cas, il n'existe dans la base de données que trois entités concordant avec les critères de recherche, avec un score de ressemblance minimum de 80.

Chapitre 10. Dépannage et assistance

Cette section vous renseigne sur les moyens de remédier à un problème survenu avec votre logiciel IBM InfoSphere Identity Insight, notamment en vous expliquant comment effectuer une recherche dans les bases de connaissances, télécharger les correctifs et contacter l'assistance.

Présentation du dépannage

Le dépannage est une approche systématique de la résolution d'un problème. Il a pour but de déterminer pourquoi quelque chose ne fonctionne pas comme prévu, et comment remédier au problème.

La première étape du processus de dépannage consiste à décrire le problème intégralement. Sans description du problème, ni vous ni IBM ne pouvons savoir par où commencer pour en identifier la cause. Cette étape implique de vous poser des questions élémentaires, notamment :

- Quels sont les symptômes du problème ?
- Où le problème survient-il ?
- Quand le problème survient-il ?
- Dans quelles conditions le problème survient-il ?
- Le problème peut-il être reproduit ?

Les réponses à ces questions aboutissant généralement à une bonne description du problème, il s'agit du meilleur moyen de s'engager sur la voie de sa solution.

Quels sont les symptômes du problème ?

Quand vous commencez à décrire un problème, la question la plus évidente est "quel est le problème ?" Voilà qui peut paraître une question allant de soi ; toutefois, vous pouvez la décomposer en plusieurs questions plus ciblées qui concourent à un panorama plus descriptif du problème. Ces questions peuvent être les suivantes, entre autres :

- Qui, ou quoi, signale le problème ?
- Quels sont les codes et messages d'erreur ?
- Comment le système défaille-t-il ? Par exemple, est-ce une boucle, un blocage, une panne totale, une dégradation des performances, un résultat erroné ?
- Quelle est l'incidence du problème sur votre activité professionnelle ?

Où le problème survient-il ?

Déterminer où le problème trouve son origine n'est pas toujours tâche aisée, mais il s'agit de l'une des étapes les plus importantes de sa solution. Il peut exister de nombreuses strates technologiques entre les composants défaillant et ceux signalant le problème. Les réseaux, disques, et pilotes ne sont que quelques-une des composants à considérer lorsque vous vous penchez sur un problème.

Les questions suivantes peuvent vous aider à vous concentrer sur l'endroit où survient le problème afin d'isoler la couche problématique.

- Le problème est-il spécifique à une seule plateforme ou à un seul système d'exploitation ?
- Le problème est-il commun sur plusieurs serveurs ?
- L'environnement et la configuration actuels sont-ils gérés ?

Retenez bien que même si le problème est signalé par une certaine couche, cela ne signifie pas qu'il provient de cette couche. L'un des aspects de l'identification de l'endroit d'où provient un problème consiste à comprendre l'environnement où il se produit. Prenez donc le temps de décrire entièrement l'environnement problématique, système d'exploitation compris, sa version, tous les logiciels correspondants et leur version, ainsi que les informations matérielles. Vérifiez que vous tournez sur un environnement dont la configuration est compatible ; de nombreux problèmes sont imputables à des niveaux de logiciel incompatibles qui ne sont pas destinés à fonctionner ensemble ou n'ont pas été intégralement testés ensemble.

Quand le problème survient-il ?

Dressez la chronologie détaillée des évènements aboutissant à une défaillance, notamment pour les cas qui constituent des occurrences uniques. Pour cela, le moyen le plus simple consiste à procéder à rebours : commencez au moment où l'erreur a été signalée (aussi précisément que possible, même jusqu'à la milliseconde près), et remontez en amont au moyen des journaux et informations disponibles. Il n'est normalement pas utile de regarder plus loin que le premier évènement suspect que vous repérez dans un journal diagnostic ; toutefois, cela n'est pas toujours facile, et demande de la pratique. Savoir où s'arrêter de chercher s'avère particulièrement difficile lorsque plusieurs couches technologiques sont concernées, et que chacune possède ses propres informations diagnostiques.

Pour dresser une chronologie détaillée des évènements, essayez de répondre à ces questions :

- Le problème ne survient-il qu'à un certain moment du jour ou de la nuit ?
- A quelle fréquence le problème survient-il ?
- Quelle succession d'évènements aboutit au moment où le problème est signalé ?
- Le problème survient-il après une modification d'environnement, par exemple la mise à niveau ou l'installation d'un logiciel ou de matériel ?

Les réponses aux questions de ce type peuvent contribuer à vous fournir un contexte de référence dans lequel étudier le problème.

Dans quelles conditions le problème survient-il ?

Savoir quelles autres systèmes et applications fonctionnent au moment où un problème survient est un aspect important du dépannage. Ces questions et autres sur votre environnement facilitent l'identification de la cause première du problème :

- Le problème survient-il toujours lorsque la même opération est en cours d'exécution ?
- Faut-il qu'une certaine succession d'évènements ait lieu pour que le problème survienne ?
- D'autres applications défaillent-elles au même moment ?

Les réponses aux questions de ce type peuvent vous aider à cerner les circonstances où le problème survient et à recouper les corrélations. Retenez bien

que le simple fait que plusieurs problèmes soient survenus vers le même moment ne signifie pas nécessairement qu'ils soient liés.

Le problème peut-il être reproduit ?

Du point du vue du dépannage, le problème "idéal" est celui qu'il est possible de reproduire. En général, avec les problèmes reproductibles, vous disposez d'une plus large palette d'outils et procédures pour vous aider à enquêter. Par conséquent, les problèmes que vous pouvez reproduire sont souvent plus faciles à déboguer et à résoudre. Toutefois, ces problèmes peuvent présenter un inconvénient : si leur incidence sur les activités de l'entreprise est élevée, vous ne souhaitez pas les voir survenir de nouveau ! Si possible, recréez le problème en environnement test ou de développement, ce qui offre généralement davantage de souplesse et de contrôle au cours de votre investigation.

- Le problème peut-il être recréé sur un ordinateur test ?
- Plusieurs utilisateurs ou applications rencontrent-ils le même type de problème ?
- Le problème peut-il être recréé en exécutant une seule commande, une série de commandes, une application particulière ou une application autonome ?

Dépannage d'IBM InfoSphere Identity Insight

Posez-vous les questions suivantes afin de vous aider à identifier et à résoudre les problèmes qui surviennent dans IBM InfoSphere Identity Insight.

1. Au cours de l'installation, le programme d'installation vous a-t-il informé que l'installation de certains composants avait échoué ? Dans ce cas, consultez les fichiers journaux d'installation pour identifier et résoudre le problème.
2. Vos mises à jour de service sont-elles au plus récent niveau ?
3. Recevez-vous un message d'erreur ?
4. Avez-vous vérifié si, dans les fichiers journaux, figurent des messages concernant le problème ?
5. Le problème survient-il lors de l'utilisation l'un des composants suivants ?
   - Les applications Web Analyst Toolkit - voir la rubrique «Liste de vérification du dépannage des applications Web d'Analyst Toolkit», à la page 395
   - Pipelines - voir la rubrique Liste de vérifications du dépannage des pipelines
6. Avez-vous recherché dans lesbases de connaissances du produit des informations susceptibles de résoudre le problème ?
7. Si vous avez essayé chacune de ces options et que votre problème n'est toujours pas résolu, contactez l'assistance logicielle IBM.

Liste de vérifications du dépannage des pipelines

Si vous rencontrez des problèmes avec des pipelines, avant d'appeler l'assistance logicielle IBM, consultez cette liste des problèmes les plus courants .

1. Le pipeline indique l'état Arrêté ou aucun état
2. Le pipeline s'arrête
3. Les pipelines ne tiennent pas compte des modifications de configuration effectuées dans la Console de configuration
4. Les pipelines ne démarrent pas sous AIX
5. Le pipeline ne traite qu'une partie d'une fiche entrante
6. Le transport ne fonctionne pas
7. Le pipeline ne charge pas un nombre en notations scientifique ou à virgule flottante

8. Après le démarrage d'un pipeline, je reçois un message d'avertissement indiquant qu'aucune route n'est définie

1. **Le pipeline indique un état "Arrêté" ou n'indique aucun état**
   - Le noeud de pipeline a-t-il rencontré une erreur ou est-il arrêté ?
   - Le transport désigné dans la commande de pipeline utilise-t-il la syntaxe correcte ?
   - Le pipeline s'est-il arrêté ?
2. **Le pipeline s'arrête ou tombe en panne**
   - Le pipeline a-t-il rencontré trop d'erreurs lors du traitement des fichiers de données entrants ?
     - Consultez les fichiers journaux pour plus d'information sur les erreurs. Utilisez ces informations pour résoudre ce problème.
     - Vérifiez le paramètre *ErrorLimit* dans le fichier de configuration de pipeline. Vous devrez peut-être augmenter ce nombre.
   - Le pipeline est-il à court de ressources mémoire ?
   - Le problème provient-il de la base de données pour l'une des raisons suivantes :
     - Espace disque insuffisant ?
     - Connexion au pipeline perdue ?
     - Les nom d'utilisateur et mot de passe de cette base de données ont-ils changé ?
3. **Les pipelines ne tiennent pas compte des modifications de configuration effectuées dans la Console de configuration**
   - Afin que les pipelines appliquent les modifications de la configuration, ils doivent être arrêtés puis redémarrés. Lorsque les pipelines redémarrent, les modifications de configuration sont appliquées dans le cadre du processus d'initialisation du pipeline.
   - A des fins d'intégrité des données, arrêtez et redémarrez tous les pipelines en cours d'exécution après une modification de configuration.
4. **Le pipeline ne démarre pas sous AIX**
   - Avez-vous reçu un message d'erreur indiquant que le module dépendant libicuio.a était introuvable ?
     - Si c'est le cas, vérifiez que la bibliothèque se trouve dans l'un des répertoires suivants : `/usr/lib`, `/lib`, `$DB2INSTHOM/sqllib/lib`. Ou configurez la variable d'environnement `LIBPATH` afin d'inclure le répertoire *`installation_home`*`/lib` du produit.
   - Vérifiez la version et l'emplacement des bibliothèques d'exécution. Le problème peut être causé par des paramètres incorrects dans la `Mise à jour d'exécution` et l'environnement `LIBPATH`. Reportez-vous au «Guide d'installation et de configuration d'IBM InfoSphere Identity Insight» pour obtenir les informations de support les plus récentes.
5. **Le pipeline ne traite qu'une partie d'un enregistrement entrant, et non sa totalité**
   - Vérifiez si des messages UMF non valide figurent dans le fichier journal *.BAD. Ce fichier journal indique le nom du fichier de source de données entrant qui était en cours de traitement.
   - Vérifiez l'onglet **Exceptions UMF** dans la console de configuration.
6. **Le transport de pipeline ne fonctionne pas**

- Vérifiez que la syntaxe utilisée pour le transport est correcte. Par exemple, si vous spécifiez un transport de base de données, avez-vous inclus des guillemets lorsque c'était nécessaire ?
- Si le transport est une file d'attente, la file d'attente de messages existe-t-elle ?
- Si le transport est un fichier, le fichier existe-t-il ? Le fichier se trouve-t-il dans le répertoire désigné dans le transport ?

7. **Le pipeline ne charge pas un nombre en notation scientifique ou à virgule flottante**
   - Il s'agit d'un limitation connue des pipelines. Revoyez les nombres en notation scientifique ou à virgule flottante dans l'UMF afin de multiplier l'exposant afin que le nombre soit en notation numérique standard. Par exemple, `-1.267E-05` multiplié est `-0.00001267`.
8. **Après le démarrage d'un pipeline, je reçois un message d'avertissement indiquant qu'aucune route n'est définie**
   - Ce message d'avertissement est uniquement informatif. Vous pouvez l'ignorer en toute sécurité. (Ce message vous informe simplement qu'aucune route n'est définie pour ce pipeline. Les routes ne sont pas indispensables pour exécuter un pipeline.)

Liste de vérification du dépannage des applications Web d'Analyst Toolkit

Si vous rencontrez des problèmes avec des application Web, avant d'appeler le service de support logiciel IBM, consultez cette liste des problèmes les plus courants :

1. Je ne peux pas voir l'écran de connexion de la Console de configuration
2. Je ne peux pas me connecter à la Console de configuration
3. Un rapport s'ouvre dans le navigateur Web, mais il n'affiche aucune donnée
4. Je ne peux pas voir l'état d'un pipeline dans l'onglet Etat du pipeline
5. Les modifications de configuration réalisées dans la Console de configuration ne sont pas prises en compte par les pipelines.

1. **Je ne peux pas voir l'écran Connexion.**
   - Voyez-vous le message "Impossible d'afficher cette page" ?
     - L'URL de l'application Web est probablement incorrecte. Saisissez de nouveau l'URL. Si vous ne connaissez pas l'URL exacte, contactez votre administrateur système ou le support technique interne pour obtenir de l'aide.
     - Autres raisons potentielles : Le port qui connecte votre machine au serveur WebSphere Liberty peut être bloqué, ou ce dernier n'a peut-être pas démarré. Contactez votre administrateur système ou le support technique interne pour obtenir une assistance.
   - L'écran est-il vierge ?
     - Contactez votre administrateur système ou le support technique interne. Le port qui connecte votre machine au serveur WebSphere Liberty peut ne pas avoir démarré, ou le mot de passe de la base de données Indentity Insight peut avoir changé.
   - Si aucune de ces solutions ne résout le problème, contactez votre administrateur système ou le support technique interne pour obtenir une assistance.
2. **Je ne peux pas me connecter à l'application Web.**

- Vérifiez que vous saisissez le nom d'utilisateur et le mot de passe exacts. Etant donné qu'Analyst Toolkit ne verrouille pas les comptes utilisateur, quel que soit le nombre de tentatives de connexion incorrectes, essayez de nouveau de saisir votre nom d'utilisateur et votre mot de passe.
- Si vous avez oublié votre nom d'utilisateur et mot de passe, contactez votre administrateur système ou le support technique interne pour obtenir une assistance. Il faudra peut-être réinitialiser votre mot de passe.

3. **Les modifications de configuration réalisées dans la Console de configuration ne sont pas prises en compte par les pipeline.**
   - Afin que les pipelines appliquent les modifications de la configuration, ils doivent être arrêtés puis redémarrés. Lorsque les pipelines redémarrent, les modifications de configuration sont appliquées dans le cadre du processus d'initialisation du pipeline.
   - A des fins d'intégrité des données, arrêtez et redémarrez tous les pipelines en cours d'exécution après une modification de configuration.

Liste de vérifications du dépannage de Visualizer

Si vous rencontrez des problèmes avec le Visualizer, avant d'appeler le support IBM, consultez cette liste des problèmes les plus courants rencontrés lors de l'utilisation du Visualizer. Vous serez peut-être en mesure de résoudre par vous-même votre problème ou de répondre à votre question sur le Visualizer.

1. Je ne peux pas démarrer le Visualizer
2. Je ne peux pas me connecter au Visualizer
3. J'ai généré un rapport du Visualizer. Le rapport s'ouvre dans mon navigateur web, mais rien ne s'y affiche
4. Je reçois des messages d'erreur concernant le pipeline
5. Le Visualizer est 'suspendu' ou se 'bloque'
6. La fonction de recherche par attribut ne renvoie pas les résultats attendus
7. Lors de l'utilisation de la fenêtre Recherche par attribut, je reçois un message d'erreur concernant des "index insuffisants"
8. Les icônes personnalisées des graphiques du Visualizer ne s'affichent pas ou s'affichent de manière incorrecte
9. Les liens (ou hyperliens) du Visualizer ne fonctionnent pas

1. **Je ne peux pas démarrer le Visualizer**
   - Dans un premier temps, veillez à ce que la version client requise de Java soit installée sur le votre poste de travail client.
   - Si plusieurs versions de Java sont installées sur votre machine cliente, il est probable que la version système par défaut de Java Web Start ne soit pas la version requise pour s'exécuter dans le Visualizer. Gardez également à l'esprit que la version Java client devant ouvrir et exécuter le Visualizer peut ne pas être la dernière version de Java installée sur votre machine. Deux manières permettent de résoudre ce problème : Associez la version client requise de Java Web Start à votre navigateur Web ou utilisez une approche de lancement direct.
     – Visualizer est-elle la seule application Web Start que vous utilisez sur ce poste de travail client ? Si oui, configurez votre navigateur Web pour qu'il associe le type de fichier *.JNLP afin d'utiliser la version client requise de Java Web Start.
     – Parallèlement au Visualizer, exécutez-vous d'autres applications Web Start sur ce poste de travail ou souhaitez-vous éviter de faire des modifications

sur les paramètres système et Java ? Si oui, lancez directement le Visualizer depuis le fichier Java Web Start.

- Recevez-vous un message d'erreur indiquant que l'application a demandé une version de JRE qui n'est pas installée ? Si oui, configurez Java version 1.6 pour accepter les téléchargements automatiques.
- Voyez-vous la page de lancement Visualizer Web start ?
  - Oui, je vois la page de lancement Visualizer Web start, mais je vois un message indiquant que "Java Web Start est requis pour lancer le Visualizer." Je ne vois pas de lien **"Cliquez ici pour lancer IBM InfoSphere Identity Insight Visualizer"**.
    - Utilisez-vous ce poste de travail client exclusivement pour le Visualizer ? Si oui, configurez votre navigateur Web pour qu'il associe le type de fichier .JNLP afin d'utiliser la version client requise de Java Web Start.
    - Utilisez-vous ce poste de travail client pour ouvrir d'autres applications Web Start ou souhaitez-vous éviter d'apporter des modifications sur les paramètres système et Java ? Si oui, lancez directement le Visualizer depuis le fichier Java Web Start.
  - Oui, je vois la page de lancement Visualizer Web Start ainsi qu'un écran Visualizer Splash, mais je ne vois pas la fenêtre de **de connexion** du Visualizer.
    - Avez-vous cliqué sur le lien **"Cliquez ici pour lancer IBM InfoSphere Identity Insight Visualizer"** ?
      - Si oui, Java peut être en train d'ouvrir le Visualizer, ce qui peut prendre plusieurs minutes. Si le Visualizer est en cours d'ouverture, vous voyez généralement un écran Java Splash ou une fenêtre Java Web Start.
      - Dans le cas contraire, cliquez sur le lien pour lancer le Visualizer.
    - Le problème provient probablement du serveur intégré WebSphere Application Server. Le serveur d'application rencontre un problème ou une erreur et un redémarrage peut être nécessaire, ou le serveur d'application ne peut pas se connecter à la base de données produit appropriée. Contactez votre administrateur système ou le support technique interne.
  - Non, je ne vois pas la page de lancement Visualizer Web Start.
    - Si vous voyez le message "Impossible d'afficher la page", vérifiez l'URL du Visualizer. L'URL du Visualizer peut contenir une coquille ou peut être incorrecte. Saisissez de nouveau l'URL. Si vous ne connaissez pas l'URL du Visualizer, contactez votre administrateur système ou le support technique interne.
    - Si l'URL est exacte, voici quelques autres raisons potentielles pour lesquelles la page Visualizer Web Start ne s'affiche pas :
      - Le serveur WebSphere Application Server rencontre un problème ou une erreur et un redémarrage peut être nécessaire.
      - Le port qui connecte votre poste de travail client au serveur WebSphere Application Server peut être bloqué ou peut être déjà utilisé par une autre application.
- Si aucune de ces actions ne résout le problème, demandez à votre administrateur système ou au support technique interne de contacter le support logiciel IBM.

2. **Je ne peux pas me connecter au Visualizer**
   - Voyez-vous l'écran de **Connexion** du Visualizer ?

– Non, je ne vois pas l'écran de **Connexion** du Visualizer.
  - Le problème provient probablement du serveur intégré WebSphere Application Server. Le serveur d'application rencontre un problème ou une erreur (non connecté) ou le serveur d'application ne peut pas se connecter à la base de données produit appropriée. Contactez votre administrateur système ou le support technique interne pour obtenir une assistance.
– Oui, je vois l'écran de **Connexion** du Visualizer, mais je ne peux pas me connecter.
  - Vérifiez que vous saisissez les nom d'utilisateur et mot de passe correspondants à votre compte utilisateur Visualizer. Quel que soit le nombre d'échecs de tentatives de connexion, le Visualizer ne verrouille pas les comptes utilisateur. Essayez de saisir de nouveau votre nom d'utilisateur et mot de passe. Vous ne pouvez pas verrouiller votre compte.
  - Cliquez sur **Connexion**. Le bouton **Connexion** n'est pas automatiquement sélectionné. Par conséquent, si vous saisissez votre nom d'utilisateur et mot de passe et appuyez sur **Entrée**, rien ne se passe. Utilisez la souris pour cliquer sur **Connexion** ou sélectionnez **Connexion** à l'aide du clavier.

• Avez-vous oublié vos nom et mot de passe ?
  – Oui. Contactez votre administrateur système ou le support technique interne pour consulter votre nom d'utilisateur ou réinitialiser le mot de passe de votre compte Visualizer dans la Console de configuration.

3. **J'ai généré un rapport du Visualizer. Le rapport s'ouvre dans mon navigateur web, mais rien ne s'y affiche.**
   • Patientez une minute ou deux, car il se peut que le rapport soit toujours en cours de génération. Quand le système génère un rapport, il commence par afficher un écran vierge dans le navigateur. Une fois que le rapport a fini de se générer et qu'il est prêt pour l'affichage, le système l'affiche.
   • Veillez à ce qu'Adobe Acrobat Reader version 7.0 ou supérieure soit installé sur votre machine locale. Sinon, vous pouvez télécharger gratuitement la plus récente version d'Adobe Acrobat Reader sur le site Web d'Adobe.
   • Votre système est-il doté d'un pare-feu ? Si tel est le cas, vérifiez que l'hôte local et le serveur d'applications disposent de droits d'accès à travers le pare-feu.
4. **Je reçois des messages d'erreur concernant le pipeline.**
   • Examinez attentivement le message d'erreur pour plus d'informations sur la cause du problème.
   • Assurez-vous que le pipeline Visualizer est un pipeline HTTP.
   • La connexion client du Visualizer sur votre poste de travail est-elle allumée ?
     – Non.
       - «Activation de la consignation du client visualiseur», à la page 416 sur votre machine. Réglez le niveau de consignation sur débogage. Puis contactez votre administrateur système ou le support technique interne, en indiquant le texte du message d'erreur et en signalant à la personne que vous avez activé la connexion du Visualizer client. Votre administrateur système ou support technique interne peut vouloir essayer de se reconnecter au pipeline, puis examiner le fichier journal.
       - Une fois le problème résolu, désactivez la consignation du client Visualizer.

– Oui.
  - Examinez les fichiers journaux du client du Visualizer qui se trouvent dans *répertoire_installation*/logs/ewas.
  - Contactez l'administrateur système ou le support technique interne. Votre administrateur système ou support technique interne peut vouloir analyser le fichier journal du Visualizer client.

5. **Le Visualizer est 'suspendu' ou se 'bloque'.**
   - Il se peut que le port qui connecte votre machine au serveur intégré WebSphere Application Server soit bloqué ou que le serveur intégré WebSphere Application Server ne soit pas démarré. Contactez votre administrateur système ou le support technique interne.
   - Informations pour les administrateurs de bases de données, ou le support technique interne :
     – Considérez les statistiques d'exécution par rapport aux tables de base de données d'entités qui affectent le Visualizer.
     – Si tous les utilisateurs du Visualizer subissent des problèmes de type 'suspension' avec le Visualizer, vérifiez que les index de table de base de données n'ont pas été modifiés. La modification de ces index peut entraîner des résultats imprévisibles et indésirables. Si vous vous apercevez que les index ont été modifiés, contactez le service de support logiciel IBM.
6. **La fonction de Recherche par attribut ne renvoie pas les résultats attendus.**
   - Passez en revue vos critères de recherche.
     – Si vous constatez moins de résultats que prévu, un élargissement des critères peut s'avérer nécessaire.
     – Si vous constatez plus de résultats que prévu, vous devrez peut-être affiner vos critères de recherche.
     – Par défaut, le système ne renvoie pas plus de 1000 enregistrements par recherche. (Cependant, ce paramètre peut être configuré. Ce réglage est contrôlé par le paramètre MAX_ENTITIES_RETURNED dans l'onglet **Paramètres système** de la Console de configuration. Pour vérifier ou modifier ce paramètre, vous pouvez contacter votre administrateur système ou le support technique interne.)
   - Le problème est peut-être dû à la configuration des paramètres de sensibilité à la casse de la base de données. Contactez votre administrateur système ou le support technique interne afin de vérifier la configuration de la base de données concernant les paramètres de sensibilité à la casse.
     – Pour les bases de données DB2 : l'administrateur de base de données, l'administrateur système, ou le support technique interne peut devoir appliquer un script afin de prendre en charge les recherches de bases de données non sensibles à la casse. Demandez-lui de contacter le service de support technique IBM pour obtenir le script et les instructions relatives à son exécution.
     – Pour les bases de données Microsoft SQL Server : les bases de données sont peut-être définies pour être sensibles à la casse. L'administrateur de base de données, l'administrateur système ou le support technique interne devra peut-être modifier les paramètres de sensibilité à la casse de la base de données.
     – Pour les bases de données Oracle : L'administrateur de base de données, l'administrateur système, ou le support technique interne peut devoir

créer des index fonctionnels avec UPPER (des lettres majuscules) pour prendre en charge les recherches de base de données non sensibles à la casse.

7. **Lors de l'utilisation de la fenêtre Recherche par attribut, je reçois un message d'erreur concernant des "index insuffisants".**
   - Vous tentez d'effectuer une recherche sur une zone qui n'est pas indexée.
     – Essayez d'affiner la recherche en entrant des critères supplémentaires.
     – Ou contactez votre administrateur système ou le support technique interne. Selon l'incidence sur les performances du système, ce dernier peut créer un index sur cette zone. (Votre administrateur système ou le support technique interne peut également vérifier le paramètre `ENABLE_SEARCH_INDEX_CHECK` dans l'onglet **Paramètres système** de la Console de configuration. Si ce paramètre n'est pas réglé sur 1, les performances du système peuvent être affectées.)
8. **Les icônes personnalisées des graphiques du Visualizer ne s'affichent pas ou s'affichent de manière incorrecte.**
   - Les icônes peuvent ne pas se trouver dans le répertoire ou serveur d'application adéquat. Contactez votre administrateur système ou support technique interne afin de vérifier l'emplacement (indiqué par le chemin d'accès) des icônes de graphique personnalisées.
   - Les noms d'icône peuvent être en majuscules et minuscules plutôt que tout en minuscules ou peuvent ne pas correspondre à leur type d'attribut correspondant. Par exemple, si **`Preuve photo`** est le nom du type d'attribut, alors le nom de fichier de l'image doit être entièrement en minuscules et inclure un espace entre les mots `preuve` et `photo`. Le nom de fichier doit ressembler à cela :**`preuve photo.gif`**. Contactez votre administrateur système ou le support technique interne pour vérifier que le nom du fichier d'icône est correct.
   - Les icônes peuvent ne pas se trouver sous le format de fichier .GIF recommandé. Ou les icônes peuvent ne pas avoir la taille recommandée, à savoir 24-par-24 pixels. Contactez votre administrateur système ou le support technique interne pour vous assurer que l'icône est sous le bon format de fichier et utilise la taille d'image recommandée.
9. **Les liens (ou hyperliens) du Visualizer ne fonctionnent pas. Je vois un message d'erreur lorsque je clique sur un lien d'attribut.**
   - Configurez les paramètres d'hyperlien de votre poste de travail. Dans les préférences système du Visualizer, sélectionnez le navigateur web ou le programme utilisé pour ouvrir les fichiers associés aux attributs de fiche d'identité. Ce paramètre doit être configuré sur chaque poste de travail exécutant le Visualizer.
   - Après avoir configuré les paramètres d'hyperlien, veillez à fermer le Visualizer et à le redémarrer.

Santé du système

Voici quelques astuces pour les administrateurs de base de données et les administrateurs système afin de préserver la santé de votre système IBM InfoSphere Identity Insight.

Astuces de performance

Si vous constatez une dégradation des performances générales de votre système, consultez cette liste afin d'obtenir des idées sur les causes possibles :

- Réglage de la base de données : Quand a été la dernière fois qu'une personne a exécuté les statistiques de base de données par rapport aux tables IBM InfoSphere Identity Insight ?
- Très grandes entités : La base de données d'entités contient-elle de très grandes entités– des entités avec de nombreuses identités ?

Bien que cette liste ne soit pas exhaustive, elle constitue un point de départ pour valider le fait que les performances du système sont optimales.

Astuces pour le contrôle de la base de données d'entités

Voici quelques éléments spécifiques à vérifier afin de mieux contrôler la santé de la base de données d'entités :

- Réglage de la base de données : Quel est le planning d'exécution des statistiques de base de données par rapport aux tables IBM InfoSphere Identity Insight ?
- Numéros uniques : La base de données d'entités contient-elle plusieurs entités qui partagent le même numéro unique ?
- Entités : La base de données d'entités contient-elle des entités avec de nombreux numéros uniques ?
- Sur-résolution : La base de données d'entités contient-ellede très grandes entités– entités avec de nombreuses identités ?

Bien que cette liste ne soit pas exhaustive, elle fournit des astuces rapides pour le contrôle de la santé générale du système.

Tables de base de données affectant les performances du système

Si les performances du système semblent ralenties, les administrateurs de base de données peuvent exécuter des statistiques de base de données par rapport à plusieurs tables de base de données d'entités afin d'améliorer les performances du pipeline et l'expérience utilisateur de Visualizer.

Tables du pipeline

Si les performances du pipeline semblent ralenties, essayez d'exécuter les statistiques de base de données par rapport aux tables de base de données d'entités suivantes :

- DQM_NAME_DICT
- NAME
- ADDRESS
- NUMS
- ATTRIBUTES
- EMAIL_ADDR
- DSRC_ACCT
- SEP_RELATIONS
- SEP_ROLES
- ENTITY
- DISCLOSED_RELATIONS
- UMF_LOG
- UMF_EXCEPT

Tables du Visualizer

Si l'utilisateur du Visualizer se plaint que ses performances semblent ralenties, essayez d'exécuter les statistiques de base de données par rapport aux tables de base de données d'entités suivantes :

- 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

De plus, dans la mesure où le Visualizer utilise également un pipeline en arrière-plan pour effectuer plusieurs tâches du Visualizer (telles que l'ajout d'entrées, la recherche d'entités par la résolution d'entités, et la divulgation de relations), les administrateurs de base de données doivent également exécuter les statistiques de base de données par rapport aux tables de base de données répertoriées dans la section tables du pipeline.

Requête de grandes entités

Cette requête SQL recherche de grandes entités. Plus l'entité possède de fiches d'identité, plus elle devient grande. Parfois, les résultats du traitement des données d'identité entrantes peuvent entraîner une sur-résolution des fiches d'identité par le système pendant la résolution d'entité et de relation. Les grandes entités peuvent provoquer un ralentissement significatif des performances du système.

Instruction de requête SQL des grandes entités

```
select entity_id
 count(dsrc_acct) as IDENTITY_CNT
from
 DSRC_ACCT
sachant que
 sys_delete_dt is null
groupe par
 entity_id
count(dsrc_acct) > 100
order by count(dsrc_acct)desc;
```

Etape suivante ?

Dans le plug-in Identity Insight pour i2 ou l'application Explorer, utilisez l'écran **Rechercher par ID d'entité** pour consulter les ID d'entité renvoyés par les résultats de requête de grandes entités. Vérifiez l'exactitude de l'association des identités à cette entité. Pour les entités correctement construites, l'entité possède de nombreux comptes de source de données différents, alors que la majeure partie des données sont très similaires pour les noms, adresses et numéros associés. Si vous avez des questions sur la construction de l'entité, contactez vos Services ou Support IBM pour obtenir une assistance.

Exemple de résultats de requête de grandes entités

Voici un exemple de résultats à la requête de grandes entités :

ENTITY_ID	IDENTITY_CNT
3015	22
5241	41
7854	36

Requête Total de numéros uniques par entité

Cette requête renvoie des informations sur le nombre de numéros uniques associés à une entité spécifique, par ID d'entité. Vous pouvez trouver cette requête utile si chaque entité ne possède généralement qu'un seul numéro unique. Le fait de vérifier si des entités contiennent de nombreux types de numéros uniques constitue une excellente manière de contrôler les anomalies de données et de vérifier que vos règles de résolution fonctionnent comme prévu.

Instruction de requête SQL Nombre total de numéros uniques associés à une entité unique

```
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;
```

Etape suivante ?

Dans Explorer, utilisez l'écran **Rechercher par ID d'entité** afin de consulter les ID d'entité renvoyés par les résultats de requête Nombre total de numéros uniques par ID d'entité. En examinant le récapitulatif d'entité de chaque entité, vous pouvez déterminer si l'entité doit avoir plus d'un numéro unique. Dans certains cas, cette situation peut être une indication de fraude. Par exemple, aux Etats-Unis,

les numéros de sécurité sociale (SSN) sont des numéros uniques. En règle générale, chaque entité américaine ne possède qu'un seul SSN. Si cette requête révèle une entité possédant plusieurs SSN, l'étape suivante consiste probablement à effectuer une enquête et une analyse approfondies sur la raison de cette multiplicité de SSN.

Exemple de résultats de la requête Nombre total de numéros uniques par entité

Voici un exemple de résultats à la requête Nombre total de numéros uniques par entité :

ENTITY_ID	UNIQUE_NUMBER_CNT
3003	2
3030	2
3039	2

Requête Numéro unique partagé par plusieurs entités

Les numéros uniques sont des numéros, qui, généralement, appartiennent uniquement à une seule entité et ne sont pas partagés par plusieurs entités. Le fait de vérifier si plusieurs entités partagent les mêmes numéros uniques constitue une excellente manière de contrôler les anomalies de données et de vérifier que vos règles de résolution fonctionnent comme prévu. Vous pouvez utiliser la requête Numéro unique partagé par plusieurs entités afin de découvrir les entités qui partagent le même numéro unique. Indépendamment du nombre de fiches d'identité de cette entité qui contiennent le même numéro unique, la requête ne compte un numéro unique qu'une seule fois pour une seule entité.

Instruction de requête SQL Numéros uniques partagés par plusieurs entités

```
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;
```

Etape suivante ?

Dans Explorer, utilisez l'écran **Rechercher par attribut** afin de consulter chaque numéro renvoyé par la requête SQL Numéros uniques partagés par plusieurs entités. Dans l'écran **Résultats**, examinez les informations de l'entité pour chaque entité qui partage un numéro unique. Vous pouvez également consulter le récapitulatif d'entité de ces entités afin de déterminer la raison pour laquelle elles partagent le même numéro unique.

En vous basant sur le numéro unique, vous pourriez découvrir des relations intéressantes entre les entités. Vous pourriez notamment découvrir que deux entités différentes utilisent le même numéro de sécurité sociale.

Ou vous pourriez détecter un problème avec le codage UMF des numéros uniques. Vous pourriez par exemple découvrir qu'un même numéro de passeport est partagé entre deux entités, car la fiche d'identité UMF entrante n'a pas utilisé NUM_LOC pour indiquer le pays (lieu) émettant le numéro de passeport. Les numéros comme les passeports ou les permis de conduite ne sont spécifiques qu'à un lieu donné, comme un pays ou un Etat. En eux-mêmes, ces numéros ne sont peut-être pas aussi unique que vous pourriez le croire.

Exemple de résultats de la requête Numéro unique partagé par plusieurs entités

Voici un exemple des résultats à la requête Numéro unique partagé par plusieurs entités :

NUM_TYPE	NUM_VALUE	cnt
SSN (numéro de sécurité sociale)	000-00-0000	9
SSN (numéro de sécurité sociale)	111-11-1111	9
SSN (numéro de sécurité sociale)	555-55-5555	5
SSN (numéro de sécurité sociale)	611-00-6666	2
SSN (numéro de sécurité sociale)	999-99-9999	3

Recherche dans les bases de connaissances

Il est souvent possible de trouver la solution aux problèmes en effectuant une recherche dans les bases de connaissances IBM. Cette rubrique explique comment optimiser vos résultats en exploitant les ressources, outils d'assistance et méthodes disponibles.

Ressources techniques disponibles

Outre ce centre de documentation, vous disposez des ressources techniques suivantes pour vous aider répondre à vos questions et à résoudre vos problèmes :

Notes techniques d'IBM InfoSphere Identity Insight disponibles à l'adresse suivante :www.ibm.com/software/support/isa/

Recherche avec des outils d'assistance

Vous disposez des outils bureautiques suivants pour faciliter vos recherches sur l'ensemble des bases de connaissances IBM :

- **IBM Support Assistant (ISA)** est un banc d'essai de maintenabilité gratuit qui vous aide à régler les questions et problèmes éventuels que vous poseraient les logiciels IBM. Les instructions de téléchargement et installation d'ISA sont disponibles sur le site Web www.ibm.com/software/support/isa/
- La **barre d'outils d'assistance logicielle IBM** est un module de navigateur doté d'un mécanisme qui vous facilite les recherches sur les sites d'assistance IBM. Vous pouvez télécharger la barre d'outils sur www.ibm.com/software/support/toolbar/.

Astuces de recherche

Les ressources suivantes vous expliquent comment optimiser les résultats de vos recherches :

- Recherche sur le site Web d'assistance IBM
- Au moyen du moteur de recherche Google

Réception de mises à jour automatiques

- **My support**. Pour recevoir par courriel des bulletins hebdomadaires sur les correctifs et autres actualités concernant l'assistance, procédez comme suit :
  1. Rendez-vous sur le site Web d'assistance logicielle IBM, à l'adresse www.ibm.com/software/support/.
  2. Cliquez sur **My support** dans le coin supérieur droit de la page, sous **Assistance personnalisée**.
  3. Si vous êtes déjà inscrit sur My support, identifiez-vous et passez à l'étape suivante. Si vous n'êtes pas encore inscrit, cliquez sur **S'inscrire maintenant**. Renseignez le formulaire d'inscription en utilisant votre adresse électronique comme identifiant IBM et cliquez sur **Soumettre**.
  4. Cliquez sur **Modifier le profil**.
  5. Dans la **liste des produits**, sélectionnez **Logiciel**. Une deuxième liste s'affiche.
  6. Dans cette deuxième liste, sélectionnez un segment de produit, par exemple, **Gestion de systèmes**. Une troisième liste s'affiche.
  7. Dans cette troisième liste, sélectionnez un sous-segment de produit, par exemple, **Performances & disponibilité des applications**. La liste des produits pertinents s'affiche.
  8. Sélectionnez les produits dont vous souhaitez recevoir les mises à jour.
  9. Cliquez sur **Ajouter des produits**.
  10. Une fois que vous avez sélectionné tous les produits qui vous intéressent, cliquez sur **S'abonner au courrier électronique** dans l'onglet **Modifier le profil**.
  11. Sélectionnez **Veuillez m'envoyer ces documents par courriel hebdomadaire**.
  12. Au besoin, actualisez votre adresse électronique.
  13. Dans la **liste de documents**, sélectionnez **Logiciel**.
  14. Sélectionnez les types de documents sur lesquels vous souhaitez recevoir des informations.
  15. Cliquez sur **Mettre à jour**.

Généralités sur les messages

Lorsque vous recevez un message d'un composant système, vous pouvez généralement résoudre le problème en lisant l'intégralité du message, ainsi que les actions de récupération qui sont y associées.

Les identificateurs de message comptent 10 caractères, ces caractères vous renseignant davantage sur le message.

- Les trois premiers caractères identifient le produit.
  - **CWU** est l'identificateur produit d'IBM InfoSphere Identity Insight.
- Les deux caractères suivants identifient précisément, au sein du produit, le composant à l'origine du message.
  - **AE** est l'identificateur du composant pipeline.
  - **AI** est l'identificateur de composant de la console de configuration.
  - **AK** est l'identificateur du composant Gestionnaire d'événements.

  - **AL** est l'identificateur de composant des services Web.
- Les quatre caractères suivants sont le numéro de message.
- Le dernier caractère est le code du type de message, qui indique la gravité du message :
  - **E** indique un message d'erreur. Ce type de message signale un problème nécessitant une intervention immédiate sur un composant précis. Consultez dans les fichiers journaux du composant les informations qui vous aideront à résoudre l'erreur.
  - **I** indique un message d'information. Bien que ce type de message ne nécessite pas d'intervention immédiate, il est judicieux de consulter les fichiers journaux du composant pour plus d'informations.
  - **W** indique un message d'avertissement. Ce type de message signale qu'est survenue une situation susceptible de nécessiter votre attention. Consultez les fichiers journaux du composant pour plus d'informations sur la situation à l'origine de l'avertissement et sur le moyen d'y remédier.

Exemples de messages

Si vous recevez un message dont l'identificateur est CWUAE0001E, cela signale, sur un pipeline, une erreur qui a très probablement provoqué son arrêt, et donc celui du traitement. Il convient alors de consulter les fichiers journaux du pipeline afin de résoudre le problème et de pouvoir redémarrer la pipeline.

Si vous recevez un message dont l'identificateur est CWUAE325W, cela indique qu'un message d'avertissement est survenu sur le pipeline, mais que cet avertissement n'a pas empêché le pipeline de continuer à traiter les fiches entrantes. Vous pouvez vous reporter aux fichiers journaux du pipeline pour plus d'informations sur l'avertissement et déterminer quelles mesures vous êtes susceptible de devoir engager pour remédier au problème ou corriger la fiche entrante. Si ce pipeline particulier est en cours de supervision par le moniteur d'application, vous pouvez également vérifier les fenêtres de ce dernier dans la console de configuration pour plus d'informations.

Erreurs d'analyse UMF

Les erreurs d'analyse UMF surviennent quand des enregistrements d'identité UMF sont incorrectement formatés, comme lorsqu'une balise de fin manque ou que des caractères incorrects non valides figurent dans l'UMF.

Tableau 37. Erreurs d'analyse UMF

Code d'erreur UMF	Description du code	Gravité
005	Les espaces de droite ne sont pas autorisés dans la *chaîne* du nom de balise	Grave
010	Il manque la <*chaîne*> de balise de début de racine	Grave
015	</*chaîne*> de balise de fin inattendue	Grave
020	</*chaîne*> de balise de fin incorrecte. </*chaîne*> attendue	Grave
025	Document incomplet, balises de fin insuffisantes... Dernier segment : <*chaîne*>	Grave
030	Document vide	Avertissement
035	Les segments ne peuvent pas contenir de '*chaîne*' de données de balise lorsqu'ils ont des enfants	Grave

Journaux

IBM InfoSphere Identity Insight est doté de mécanismes de consignation qui transcrivent des informations dans une série de fichiers journaux. Généralement, le système se met à transcrire les informations dans les fichiers journaux dès qu'une condition préalable survient sur un composant système précis, par exemple à l'installation ou au démarrage de ce composant, lorsqu'un utilisateur accède à ce composant, ou lorsqu'une erreur se produit durant le traitement.

Les composants système suivants créent des fichiers journaux :

- Pipelines
- Applications Web d'Analyst Toolkit
- Services Web
- Gestionnaire d'événements

Fichiers journaux de pipeline

Dès que vous démarrez un pipeline, le système lance automatiquement la consignation, en fonction de la configuration de consignation actuelle du fichier de configuration de pipeline. Des fichiers journaux sont créés pour chaque pipeline, par nom de pipeline, même si vous avez démarré plusieurs pipelines au moyen du même fichier de configuration.

Types de fichiers journaux de pipeline

Par défaut, tous les fichiers journaux de pipeline sont transcrits dans le répertoire du noeud de pipeline où le pipeline a été démarré. Il existe plusieurs types différents de fichiers journaux de pipeline. Quel message est consigné dans quel fichier dépend du mode dans lequel le pipeline a été démarré (mode débogage `-d` ou mode démon/service `-s`), du type de message en cours de consignation et de la configuration de consignation actuelle.

Tableau 38. Fichiers de consignation de pipeline par type de message, nom de fichier journal et modes de consignation

Type de message	Nom de fichier journal	Action	Modes de consignation
Messages d'erreur	*nom_pipeline*.err Consigne les erreurs critiques survenues dans le pipeline.	Après avoir consulté les fichiers journaux, corrigez les erreurs ou les problèmes indiqués avec le pipeline.	Service Débogage
Messages d'erreur SQL	*nom_pipeline*.SqlErr.log Consigne les erreurs SQL survenues dans le pipeline. Ce fichier est soumis à une limite de taille de 1 mégaoctet. Dès que ce fichier atteint cette limite, le système archive automatiquement le fichier journal actuel et en crée un nouveau.	Après avoir consulté ce fichier journal, corrigez les erreurs ou problèmes de SQL indiqués.	Service Débogage

Tableau 38. Fichiers de consignation de pipeline par type de message, nom de fichier journal et modes de consignation (suite)

Type de message	Nom de fichier journal	Action	Modes de consignation
Erreurs de file d'attente	*nom_pipeline*.MQErr.log Consigne les erreurs de file d'attente.	Après avoir consulté ce fichier journal, corrigez les erreurs ou problèmes de MQ indiqués.	
Visualiseur d'événement Windows	(plateformes Microsoft Windows uniquement) Si les services sont installés sur le pipeline et qu'il a été démarré au moyen du mode service (option de pipeline `-s`), le pipeline envoie également les erreurs et les messages importants au visualiseur d'événements Windows.	Contrôlez les messages dans l'écran Visualiseur d'événements Windows et corrigez toutes les erreurs ou problèmes indiqués.	Service (plateformes Microsoft Windows uniquement)
Messages UMF erronés/non valides qui n'ont pu être traités	*nom_pipeline*.bad Consigne des informations sur les enregistrements du fichier de source de données entrant contenant un UMF syntaxiquement incorrect ou non valide. Le pipeline n'a pu traiter la portion de l'enregistrement contenant cet UMF syntaxiquement incorrect ou non valide, ce qui signifie parfois que le pipeline traite des enregistrements partiels.	Après avoir consulté ce fichier journal, corrigez les enregistrements dans le fichier de source de données entrant concerné par l'UMF erroné ou non valide. Ensuite, renvoyez les enregistrements corrigés via un pipeline pour traitement.	Service Débogage
Messages UMF qui ont généré des exceptions	*nom_pipeline*.msg Consigne les informations sur les enregistrements du fichier de source de données entrant contenant des exceptions générées durant le traitement. Le pipeline a néanmoins traité l'enregistrement. Ce type de message peut révéler un problème de qualité des données de ce fichier source.	Après avoir consulté ce fichier journal, vous pouvez encore avoir besoin de corriger les fiches dans le fichier de source de données entrant ayant généré l'exception UMF. Ensuite, renvoyez les enregistrements corrigés via un pipeline pour traitement. Vous pouvez également consulter le rapport récapitulatif de chargement ou récapitulatif de source de données pour plus d'informations.	Service Débogage

Tableau 38. Fichiers de consignation de pipeline par type de message, nom de fichier journal et modes de consignation (suite)

Type de message	Nom de fichier journal	Action	Modes de consignation
trace de débogage	Consigne les informations de trace de débogage quand un pipeline a été démarré au moyen du mode débogage (option de pipeline `-d`). Il n'y a pas de fichier journal. Le pipeline s'exécute en avant-plan avec des messages de sortie envoyés directement à l'interpréteur de commandes. Vous pouvez utiliser la fonction de réacheminement pour créer un fichier à partir de la sortie de la commande du pipeline : `pipeline -d -f my_umf.xml > mon_fichier_journal.log`		Débogage
Instructions SQL et statistiques de performances	*nom_pipeline*.SqlDebug.log Consigne les instructions SQL et les statistiques de performances à même de faciliter l'identification et la résolution des incidents et de contrôler les performances. Ce fichier est soumis à une limite de taille de 48 mégaoctets. Dès qu'un fichier atteint cette limite, le système archive automatiquement le fichier journal actuel et en crée un nouveau.		Débogage
Le pipeline s'arrête alors qu'il traite un fichier	*nom_pipeline*.cnt Alors que le pipeline traite les enregistrements entrants, il consigne le nom du fichier de source de données en cours de traitement, ainsi qu'un comptage d'enregistrements tous les 100 enregistrements du fichier traités. Si un pipeline s'arrête tandis qu'il traite un fichier de source de données entrant, ce fichier peut vous aider à déterminer les enregistrements du fichier de source de données devant être rechargés dans le pipeline pour le traitement.	Après avoir consulté ce fichier journal et remédié au problème qui arrête le pipeline, rechargez les enregistrements non traités dans le pipeline pour les traiter.	Fichier

Configurations de consignation de pipeline

IBM InfoSphere Identity Insight contient une configuration de consignation par défaut qui consigne les événements et erreurs de pipeline. Cette configuration de consignation par défaut est automatiquement appliquée, hormis si une configuration personnalisée n'est indiquée dans le fichier de configuration de pipeline.

Il existe deux manières principales de démarrer les pipelines : mode débogage (option de pipeline `-d`) ou mode service/démon (option de pipeline `-s`).

- Le mode débogage s'avère pratique pour tester et dépanner le système. Normalement, il ne s'emploie pas en environnement de production. La consignation pour mode débogage inclut davantage d'informations sur les opérations de traçage et de pipeline.
- Le mode service/démon est le mode type en environnement de production. La consignation du mode service/démon s'en tient généralement aux erreurs et problèmes qui nécessitent une intervention.

Toutes les configurations de consignation de pipeline (à la fois par défaut et personnalisées) doivent indiquer comment consigner les événements de pipeline en mode débogage et en mode service/démon. Si la configuration de consignation par défaut ne répond pas à vos besoins, vous pouvez en créer une personnalisée en ajoutant une section de consignation dans le fichier de configuration de pipeline et en utilisant les composants de configuration de pipeline pour indiquer la façon dont le système consigne les événements et les erreurs du pipeline à la fois pour le mode débogage et le mode service/démon.

Configuration par défaut de la consignation du mode débogage

```
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.*
```

Configuration par défaut de la consignation du mode service Microsoft Windows

```
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.*
```

Configuration par défaut de la consignation du mode démon UNIX

```
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.*
```

Composants de consignation de pipeline

Les composants de consignation de pipeline permettent de créer des configurations de consignation de pipeline personnalisées. Ils fournissent au système les instructions sur la façon dont il faut consigner les événements et messages de pipeline.

Programme d'écriture de journaux

Désigne quel programme d'écriture utiliser pour transcrire ou afficher le fichier journal.

fichier Transcrit les événement et messages de journal dans un nom de fichier spécifique.

Le programme d'écriture de journaux utilise les composants de consignation Chemin, Paramètre, Espace et Filtre. Exemple :

`file://chemin_absolu?paramètres [white space] filtre`

cmeadmin
Transcrit les événement et messages dans le journal cmeadmin.

Le programme d'écriture de journaux cmeadmin utilise les composants de consignation Espace et Filtre. Exemple :

`cmeadmin://[white space] filtre`

console
Transcrit les événement et messages dans la console à ligne de commande.

Le programme d'écriture du journal de la console utilise les composants de consignation Emplacement, Paramètres et Filtre. Exemple :

`console://emplacement_fichier?paramètres filtre`

journal des événements
(plateformes Microsoft Windows uniquement) Transcrit les événements et messages dans le visualiseur d'événements Microsoft Windows.

Le programme d'écriture du journal des événements utilise les composants de consignation Filtre. Exemple :

`eventlog://./filtre`

Chemin
Indique l'adresse de fichier et le nom de fichier où transcrire les renseignements de journal :

adresse de fichier
Les valeurs admises sont les suivantes :

- stdout - utilisé avec le programme d'écriture de la console
- stderr - utilisé avec le programme d'écriture de la console
- *chemin absolu* - utilisé avec le programme d'écriture de fichier

nom de fichier
Indique dans quel fichier journal du produit standard les informations doivent être consignées. L'extension du nom de fichier détermine le type de fichier journal. Les noms d'extension de fichiers journaux admises sont les suivantes :

- .err
- .bad
- .msg
- .SqlDebug.log
- .SqlErr.log
- .MQErr.log

Paramètre
Indique des paramètres de consignation facultatifs. Les valeurs admises sont les suivantes :

style=bare
Indique que la consignation n'inclut ni l'horodatage ni

d'autres informations d'en-tête. Ce paramètre est généralement inclus dans les fichiers qui consignent les messages UMF.

rotateSize=*Taille de fichier maximale*
Indique en kilo-octets la taille maximum du fichier journal. Quand le fichier dépasse la taille maximum, le système archive automatiquement le fichier journal et crée un fichier à utiliser pour la journalisation. Le système ajoute un 0 au nom du fichier archive, et le nouveau fichier prend le nom du fichier original. Ce processus continue jusqu'à ce que le système atteigne le nombre maximum de fichiers archives indiqué dans le paramètre `keep`.

keep=*Nombre maximum d'archives*
Indique le nombre maximum de fichiers archives à conserver durant la rotation de fichiers, selon le paramètre `rotateSize`. Quand le nombre maximum de fichiers est dépassé, le système écrase le plus ancien fichier journal archive avec les nouvelles informations.

Espace
Indique quel type d'espace placer dans le fichier journal. Les valeurs admises sont les suivantes :

- Espace
- Onglet

Filtre Indique les renseignements de journal à consigner. Les valeurs admises sont les suivantes :

Module
Indique le type de messages à consigner. Les valeurs admises sont les suivantes :

- $NODE_NAME : messages génériques
- sql : messages SQL
- mq - messages de file d'attente de messages
- bad_xml - messages UMF non valides ou syntaxiquement incorrects
- msg - exceptions UMF
- logger : messages du programme de consignation

Si vous voulez inclure tous les types de module, utilisez un astérisque comme caractère générique. Exemple :

```
console://stdout *.ERR
```

Gravité
Indique le niveau de gravité du message de journal. Les valeurs admises sont les suivantes :

- CRIT - message critique
- ERR - message d'erreur
- WARN - message d'avertissement
- NOTE - notifications
- INFO - messages d'information
- PERF - messages sur les performances
- DBUG - messages de débogage

Si vous voulez inclure tous les types de gravité, utilisez un astérisque comme caractère générique. Exemple :

```
console://stdout *.*
```

Si vous voulez exclure une gravité afin qu'elle ne soit pas signalée, utilisez le point d'exclamation. Exemple :

```
console://stdout mq.!DBUG
```

Configuration d'une consignation de pipeline personnalisée

IBM InfoSphere Identity Insight fournit des configurations de consignation de pipeline par défaut qui déterminent la façon dont les pipelines consignent les erreurs et les messages en mode débogage et en mode service/démon. Vous pouvez en revanche souhaiter modifier la configuration de consignation de pipeline par défaut ou créer une configuration de consignation personnalisée en vue de répondre aux besoins de votre organisation. Pour ce faire, vous devez créer deux fichiers de consignation spécifiant la configuration de consignation personnalisée, puis modifiez le fichier de configuration de pipeline afin d'utiliser ces fichier de consignation personnalisés.

Pourquoi et quand exécuter cette tâche

La consignation de pipeline s'effectue par noeud de pipeline ; par conséquent, vous devrez apporter ces modifications à chaque noeud de pipeline. Une fois créés, vous pouvez copier les fichiers de configuration standard et de débogage dans chaque noeud de pipeline. Vous pouvez copier puis coller le texte de la section [consignation] d'un fichier de configuration de pipeline à l'autre, ou vous pouvez encore copier l'intégralité de ce fichier d'un noeud de pipeline à l'autre. N'oubliez pas de régler les paramètres de connexion, en fonction des besoins.

Procédure

1. Au moyen de n'importe quel éditeur de texte, créez deux fichiers :
   a. Un fichier de configuration de débogage, utilisé afin de spécifier la consignation des pipelines s'exécutant en mode débogage
   b. Un fichier de configuration standard, utilisé afin de spécifier la consignation des pipelines s'exécutant en mode service/démon
2. Dans chaque fichier, utilisez les composants de consignation de pipeline qui conviennent afin d'indiquer au système comment se connecter dans ce mode.
3. Enregistrez chaque fichier. Il est judicieux d'enregistrer ces fichiers dans le répertoire dans lequel se trouve le fichier de configuration de pipeline.
4. Dans le fichier de configuration de pipeline, ajoutez une nouvelle section nommée `[consignation]`. Il s'agit de la section dans laquelle vous indiquerez les noms des deux fichiers de configuration de consignation que vous avez créés.
5. Dans l'en-tête de la section `[consignation]`, ajoutez les deux paramètres suivants :
   a. `DebugConfigFile=`*`nom du fichier de configuration de débogage`*
   b. `ConfigFile=`*`nom du fichier de configuration de consignation en mode service/démon`*

      Remarque : Si vous avez enregistré les fichiers de configuration de consignation dans un répertoire autre que celui dans lequel se trouve le fichier de configuration de pipeline, veillez à indiquer le chemin complet du fichier.

6. Enregistrez les modifications apportées au fichier de configuration de pipeline.

Que faire ensuite

Avant que ces modifications apportées à la consignation prennent effet, vous devrez arrêter et redémarrer tous les pipelines s'exécutant sur chaque noeud de pipeline affecté.

Fichiers journaux des applications Web d'Analyst Toolkit

Les applications Web s'appuient sur IBM WebSphere Liberty pour communiquer avec IBM InfoSphere Identity Insight et s'y connecter. Les fichiers journaux WebSphere Liberty incluent des informations sur les services Web et sur les applications Analyst Toolkit, ainsi que sur les erreurs WebSphere Liberty. Si votre système est configuré pour traiter les événements (à l'aide du gestionnaire d'événements), les erreurs d'événements sont également consignées dans les fichiers journaux des erreurs Web.

Le serveur d'applications contient deux fichiers journaux primaires qui peuvent aider à résoudre les problèmes :

- la sortie standard et les flux d'erreurs, qui sont consignés dans le fichier nommé `console.log` ;
- les messages capturés par les composants de consignation, qui sont consignés dans le fichier nommé `messages.log`. Les messages écrits dans ce fichier contiennent des informations supplémentaires, telles que l'horodatage du message et l'ID de l'unité d'exécution qui a écrit le message.

Ces fichiers journaux se trouvent dans le répertoire suivant :

répertoire_installation`/wlp/usr/servers/iiServer/logs`

Les fichiers journaux WebSphere sont configurés par un administrateur système sur le serveur d'applications.

Fichiers journaux du visualiseur

Le visualiseur est doté de deux types de fichiers journaux destinés à faciliter la résolution des incidents ou l'interprétation des messages du visualiseur : un fichier journal local pour chaque client Visualiseur, et des fichiers journaux pour le serveur d'application WebSphere qui héberge le visualiseur.

Consignation du client Visualiseur

Vous pouvez configurer le visualiseur de façon à consigner les erreurs, avertissements et message d'information qui surviennent sur votre client Visualiseur local. Chaque poste de travail comporte un client Visualiseur, si bien que vous pouvez choisir de consigner ou non les messages du visualiseur par poste de travail.

Par défaut, la consignation du client Visualiseur est désactivée. Vous activez ou désactiver la consignation du visualiseur et sélectionnez les paramètres de consignation dans la fenêtre **Configurer les préférences d'affichage** dans l'onglet **Paramètres du journal**.

Vous déterminez l'emplacement du répertoire du fichier journal du client Visualiseur quand vous activez la consignation du client Visualiseur soit en

saisissant le nom du répertoire, soit en accédant à ce répertoire. Le nom par défaut des fichiers journaux du client Visualiseur est visualizer.log. Il s'agit d'un fichier texte, consultable au moyen de n'importe quel éditeur de texte.

Les messages s'ajoutent au fichier journal existant jusqu'à ce que la taille de fichier maximum soit atteinte. La taille maximum d'un journal de client Visualiseur est d'un méga-octet.

- Si le fichier journal atteint la taille maximum, le système en crée un autre dans l'emplacement de répertoire configuré et commence à y consigner les messages.
- Dès que le second fichier journal atteint la taille maximum, le système met automatiquement en rotation la consignation de messages vers le premier fichier journal, jusqu'à ce qu'il soit plein.

Cette rotation automatique des fichiers journaux continue chaque fois que le fichier journal actuel atteint sa taille limite. A mesure que le système applique la rotation entre fichiers journaux, il écrase les messages précédent dans ce fichier journal.

Consignation de service d'application IBM WebSphere

Le Visualizer s'appuie sur le serveur WebSphere Application Server afin de communiquer avec IBM InfoSphere Identity Insight et s'y connecter. Les événements de services Web sont consignés dans les fichiers journaux du serveur d'application, de même que les événements de console de configuration, qui font eux aussi appel au serveur d'application IBM WebSphere.

Le serveur d'applications contient deux fichiers journaux primaires qui peuvent aider à résoudre les problèmes :

- Les messages système, qui sont consignés dans le fichier `SystemOut.log`.
- Les messages d'erreur système, qui sont consignés dans le fichier `SystemErr.log`.

Ces fichiers journaux se trouvent dans le répertoire suivant :

répertoire_installation`/logs/ewas`

Les fichiers journaux de WebSphere Application Server sont configurés par un administrateur système sur le serveur d'applications ou via l'utilitaire de configuration d'IBM InfoSphere Identity Insight.

Activation de la consignation du client visualiseur

Suivez ces instructions pour activer la fonction de consignation du client Visualizer et configurer les paramètres de consignation de ce dernier. Si vous apportez des modifications à la fonction de consignation ou aux paramètres du client Visualizer, vous devez redémarrer Visualizer pour qu'elles soient prises en compte.

Pourquoi et quand exécuter cette tâche

Les paramètres de consignation du client Visualizer sont configurés pour chaque client Visualizer local. Si vous suivez ces instructions pour activer la consignation, seuls les paramètres du client Visualizer de cette machine locale sont affectés.

Procédure

1. Dans le menu **Fichier**, sélectionnez **Préférences**.
2. Sélectionnez l'onglet **Paramètres du journal**.

3. Sous **Paramètres du journal**, sélectionnez la case **Activer la consignation** pour qu'une coche s'affiche dans celle-ci. (Cette case doit comporter une coche quand la consignation est activée.)
4. Sélectionnez le niveau de détail de la consignation dans la zone **Niveau de journalisation** :
   a. Sélectionnez **Erreurs** pour consigner les événements du client Visualizer à l'origine des messages d'erreur. Ce niveau de consignation est celui utilisé par défaut quand la consignation est activée. Il offre un équilibre satisfaisant entre performances et informations consignées.
   b. Sélectionnez **Avertissements** pour consigner les événements du client Visualizer à l'origine des messages d'avertissement ou d'erreur.
   c. Sélectionnez **Informations** pour consigner les événements du client Visualizer à l'origine des messages d'information, d'avertissement ou d'erreur.
   d. Sélectionnez **Débogage** pour consigner les messages de traçage de tous les événements Visualizer. Ce niveau de consignation n'est normalement défini que pour remédier à une erreur précise de Visualizer, généralement avec l'assistance technique IBM. Le niveau débogage peut générer un gros volume de messages de traçage, qui sont utiles pour résoudre les problèmes, mais risquent de réduire les performances obtenues par Visualizer pour ses opérations normales.
5. Dans la zone **Chemin d'accès au fichier journal**, saisissez le chemin d'accès complet et le nom du fichier journal du client Visualizer ou accédez à un répertoire existant.
   - Tapez le chemin d'accès complet au fichier journal du client Visualizer
   - Vous pouvez également accéder à un répertoire existant de votre machine locale pour le sélectionner comme répertoire de consignation du client Visualizer.
6. Cliquez sur le bouton **Soumettre** pour enregistrer vos modifications.
7. Redémarrez Visualizer en vous en déconnectant, puis en vous reconnectant. Les modifications des paramètres de consignation de votre client Visualizer ne prennent effet qu'après le redémarrage de Visualizer.

Désactivation de la consignation du client visualiseur

Suivez ces instructions pour désactiver la fonction de consignation du client Visualizer, notamment si vous avez activé la consignation de niveau débogage pour remédier à un problème précis de Visualizer. Bien que les fichiers journaux puissent vous aider à résoudre les problèmes, certains niveaux de consignation, tels que le niveau débogage, peuvent réduire les performances de Visualizer. Si vous apportez des modifications à la fonction de consignation ou aux paramètres du client Visualizer, vous devez redémarrer Visualizer pour qu'elles soient prises en compte.

Avant de commencer

Veillez à être connecté à une session Visualizer active.

Pourquoi et quand exécuter cette tâche

Les paramètres de consignation du client Visualizer sont configurés pour chaque client Visualizer local. Si vous suivez ces instructions pour désactiver la consignation, seuls les paramètres du client Visualizer de cette machine locale sont affectés.

Procédure

1. Dans le menu **Fichier**, sélectionnez **Préférences**.
2. Sélectionnez l'onglet **Paramètres du journal**.
3. Sous **Paramètres du journal**, sélectionnez la case **Activer la consignation** pour qu'aucune coche ne s'affiche dans celle-ci. (Cette case doit être vide quand la consignation est désactivée.) Lorsque la consignation est désactivée, les paramètres de configuration de la consignation le sont également.
4. Cliquez sur le bouton **Soumettre** pour enregistrer vos modifications.
5. Redémarrez Visualizer en vous en déconnectant, puis en vous reconnectant. Les modifications des paramètres de consignation de votre client Visualizer ne prennent effet qu'après le redémarrage de Visualizer.

Fichiers journaux du gestionnaire d'événements

Si votre système est configuré pour traiter les événements à l'aide du gestionnaire d'événements, le système crée un fichier journal qui contient des informations relatives aux événements. Les messages d'erreur issus du processeur d'événements externes sont consignés dans les fichiers journaux d'erreurs de WebSphere Liberty. Les erreurs de pipeline standard qui se sont produites lors du traitement du pipeline sont consignées dans le fichiers journaux du pipeline, en fonction de la configuration de la consignation dans le pipeline en cours.

Le serveur d'applications contient des fichiers journaux primaires qui peuvent être utilisés pour résoudre des messages et des incidents liés au gestionnaire d'événements :

- les informations sur le gestionnaire d'événements, qui sont consignées dans le fichier `gem_prog_`*`date`*`.log` ;
- les messages d'erreur du gestionnaire d'événements, qui sont consignés dans le répertoire *`répertoire_installation`*`/logs`.

Les messages sont ajoutés au programme et aux journaux de données par date d'événement. Ces fichiers journaux doivent être régulièrement contrôlés, puis archivés ou supprimés, conformément à la politique de votre entreprise.

Ces fichiers journaux se trouvent dans le répertoire suivant :

`répertoire_installation``/logs`

Traçage

Les traces sont des archives de traitement de composants ou de transactions. Les informations recueillies à partir d'une trace peuvent servir à cerner tant les problèmes que les performances. Dans IBM InfoSphere Identity Insight, les traces relèvent de la consignation du composant de débogage.

Obtention des correctifs

Il se peut qu'un correctif apte à remédier à votre problème soit disponible. Pour télécharger des correctifs, suivez la procédure ci-après.

Procédure

1. Déterminez quel correctif il vous faut. Accédez au document *Fixes by version for IBM InfoSphere Identity Insight* disponible à l'adresse suivante :http://www-1.ibm.com/support/docview.wss?rs=2216&uid=swg27008307 puis

cliquez sur l'un des correctifs pour obtenir plus de détails sur tous les correctifs de cette version spécifique (les correctifs sont classés par version, édition et modification).

2. Téléchargez le correctif. Dans la liste des correctifs, cliquez sur le lien Download information. Dans la section «Download package», cliquez sur le lien «Download Options» correspondant à votre environnement.
   - Si l'écran de contrat de licence IBM apparaît, lisez les informations et cliquez sur **I Accept** si vous acceptez le contrat et souhaitez poursuivre le téléchargement du correctif.
   - Si vous cliquez sur **I Do Not Accept**, le correctif ne se télécharge pas.

   Dans la fenêtre **File Download**, cliquez sur **Save** et enregistrez le fichier en local.
3. Appliquez le correctif. Accédez à l'emplacement où le correctif a été enregistré. Extrayez ou décompressez les fichiers contenus dans le correctif, puis suivez les instructions du fichier "readme" pour installer le correctif.

Informations sur les correctifs et mises à jour de service

Si vous rencontrez un problème avec InfoSphere Identity, vérifiez d'abord la liste des mises à jour recommandées afin de vous assurer que votre logiciel est au niveau de maintenance le plus récent. Ensuite, consultez la liste des problèmes résolus afin de savoir si IBM a déjà publié un correctif individuel afin d'y remédie.

Des correctifs individuels sont publiés aussi souvent que nécessaire afin de remédier aux imperfections du produit. Par ailleurs, deux sortes de lots de correctifs cumulatifs, appelés groupe de correctifs et groupes de mises à jour, sont publiés périodiquement pour que les utilisateurs puissent passer au niveau de maintenance le plus récent. Il convient d'installer ces lots dès que possible afin de prévenir tout problème.

Pour recevoir une notification hebdomadaire sur les correctifs et mises à jour, abonnez-vous aux mises à jour par courriel My Support.

Le tableau suivant décrit les caractéristiques de chaque type de maintenance.

Tableau 39. Caractéristiques d'un correctif, d'un groupe de correctifs et d'un groupe de mises à jour

Nom	Caractéristiques
Correctif	• Correctif individuel publié entre les mises à jour pour résoudre un problème précis, for example, PQ79582. • Une fois le correctif installé, testez toute fonction sur laquelle le composant concerné par le correctif a une incidence.

Tableau 39. Caractéristiques d'un correctif, d'un groupe de correctifs et d'un groupe de mises à jour (suite)

Nom	Caractéristiques
Groupe de correctifs	• Lot de correctifs cumulatif contenant tous les correctifs publiés depuis le groupe de correctifs ou groupe de mises à jour précédent ; un groupe de correctifs de nouveaux correctifs. • Les groupes de correctifs augmentent le niveau de modification du produit et sont donc nommés en conséquence, par exemple 4.0.2. • Un groupe de correctifs peut mettre à jour soit des composants précis, soit l'intégralité de l'image du produit. • Au cours de l'installation du groupe de correctifs, tous les correctifs installés antérieurement sont automatiquement désinstallés. • Une fois un groupe de mises à jour installé, il convient de tester par régression la totalité des fonctions critiques. • Les deux plus récents groupes de correctifs sont disponibles par téléchargement (par exemple, 4.0.2 et 4.0.1). Les groupes de correctifs antérieurs ne sont plus disponibles.
Groupe de mises à jour	• Lot de correctifs cumulatif contenant tous les correctifs publiés depuis le groupe de correctifs ou groupe de mises à jour précédent, ainsi que de nouveaux correctifs. • Outre les correctifs, un groupe de mises à jour contient généralement de nouvelles fonctions et met à jour l'intégralité de l'image du produit. • Les groupe de mises à jour augmentent le niveau de modification du produit et sont donc nommés en conséquence, par exemple 4.0.2. • Au cours de l'installation du groupe de correctifs, tous les correctifs installés antérieurement sont automatiquement désinstallés. • Une fois un groupe de mises à jour installé, il convient de tester par régression la totalité des fonctions critiques.

Mises à jour de service

Les mises à jour de service vous permettent de maintenir votre système au niveau de maintenance logicielle le plus récent.

Vous pouvez accéder aux mises à jour de services les plus récentes à la page d'assistance du produit IBM InfoSphere Identity Insight. L'adresse URL est la suivante :

```
https://www-947.ibm.com/support/entry/portal/Overview/Software/
Information_Management/InfoSphere_Identity_Insight
```

Pour déterminer le niveau de service de pipeline sur votre système :

1. A partir d'une ligne de commande sur le noeud de pipeline, entrez la commande suivante :

   ```
   pipeline
   ```

2. Cette version de pipeline se trouve sur la première ligne. Ce numéro détermine le niveau de service.

Pour déterminer le niveau de service de console de configuration sur votre système :

1. Démarrez la console de configuration.
2. Connectez-vous à la console de configuration.
3. Sélectionnez **A propos de** dans le menu principal.
4. Regardez le numéro de version figurant dans la fenêtre A propos de. Ce numéro détermine le niveau de service.

Joindre l'assistance logicielle IBM

L'assistance logicielle IBM fournit une aide en cas d'incident survenu avec ce produit.

Avant de commencer

Avant de contacter l'assistance logicielle IBM, votre société doit disposer d'un contrat de maintenance logicielle IBM en vigueur, et vous devez être autorisé à soumettre des problèmes à IBM. Pour tout renseignement sur les types de contrats de maintenance disponibles, voir la rubrique «Enhanced Support» du manuel *Software Support Handbook*, à l'adresse techsupport.services.ibm.com/guides/services.html

Pourquoi et quand exécuter cette tâche

Pour joindre l'assistance logicielle IBM au sujet d'un incident, procédez comme suit :

Procédure

1. Définissez l'incident, déterminez sa gravité et recueillez des informations sur le contexte. Pour obtenir de l'aide, voir la rubrique «Contacting IBM» du manuel *Software Support Handbook*, à l'adresse techsupport.services.ibm.com/guides/beforecontacting.html
2. Rassemblez des données de diagnostic.
3. Préparez-vous à indiquer les informations suivantes dans le rapport d'incident, afin d'aider le service d'assistance logicielle IBM :
   - Nom et version du produit
   - Nom et version de la base de données
   - Nom et version du système d'exploitation
4. Soumettez votre problème à l'assistance logicielle IBM, par l'une des méthodes suivantes :
   - En ligne : cliquez sur **Submit and track problems**, sur le site d'assistance logicielle IBM, à l'adresse http://www.ibm.com/software/support/probsub.html
   - Par téléphone : pour connaître le numéro à composer depuis votre pays, consultez la page Contacts du manuel IBM Software Support Handbook, à l'adresse techsupport.services.ibm.com/guides/contacts.html

Que faire ensuite

Si l'incident que vous soumettez concerne un défaut logiciel ou une documentation manquante ou inexacte, l'assistance logicielle IBM crée un rapport officiel d'analyse de programme (APAR). Cet APAR décrit l'incident en détail. Dans la mesure du possible, l'assistance logicielle IBM fournit un palliatif que vous pouvez utiliser

jusqu'à ce que l'APAR ait été résolu et qu'un correctif ait été diffusé. IBM publie quotidiennement les APAR résolus, sur le site Web de l'assistance logicielle, afin que les autres utilisateurs confrontés au même problème puissent bénéficier de la même solution.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. IBM InfoSphere Identity Insight Version 9.0.

Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet en attente couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Europe Middle-East Africa
Tour Descartes
La Défense 5
2, avenue Gambetta
92066 - Paris-La Défense CEDEX
France
Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

IBM World Trade Asia Corporation
Licensing 2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun autre pays dans lequel il serait contraire aux lois locales. LE PRESENT DOCUMENT EST LIVRE «EN L'ETAT». IBM DECLINE TOUTE RESPONSABILITE, EXPRESSE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE QUALITE MARCHANDE OU D'ADAPTATION A VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier sans préavis les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les informations contenues dans ces sites Web ne sont pas associées à ce produit IBM et l'utilisation de ces sites se fait à vos propres risques et périls.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange d'informations entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Europe Middle-East Africa
Tour Descartes
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
Canada

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif. Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des

noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel peut contenir des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de marketing ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquelles ils ont été écrits. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir explicitement ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

Les marques IBM ainsi que certaines marques non IBM sont assorties, lors de leur première occurrence dans les présentes informations, du symbole correspondant.

IBM, le logo IBM, ibm.com, sont des marques ou des marques déposées d'International Business Machines aux Etats-Unis et/ou dans certains autres pays. Si ces termes ainsi que d'autres de la marque IBM sont assortis, lors de leur première occurrence dans les présentes informations, d'un symbole de marque (® ou ™), ces symboles indiquent des marques déposées ou de droit commun aux Etats-Unis détenues par IBM au moment de la publication de ces informations. Ces marques peuvent également être des marques déposées ou de droit commun dans d'autres pays. Une liste en vigueur des marques IBM est disponible sur le web, dans la section "Informations sur le copyright et les marques" à l'adresse www.ibm.com/legal/copytrade.shtml.

Les termes suivants sont des marques ou des marques déposées d'autres sociétés.

Adobe, le logo Adobe, PostScript, et le logo PostScript sont des marques déposées ou des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans d'autres pays.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium, et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que toutes les marques incluant Java sont des marques d'Oracle Corporation aux Etats-Unis et/ou dans certains autres pays.

D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X

Imprimé en France

SC11-7004-00