Informatica

Informatica® MDM Multidomain Edition
10.2

Guide d'implémentation d'Informatica Data Director

Informatica MDM Multidomain Edition Guide d'implémentation d'Informatica Data Director
10.2
Octobre 2016

Date de publication: 2019-05-27

Sommaire

Préface **11**

Ressources Informatica 11

Informatica Network 11

Base de connaissances Informatica 12

Documentation Informatica 12

Matrices de disponibilité de produit Informatica 12

Informatica Velocity 12

Informatica Marketplace 12

Support client international Informatica 12

Chapitre 1: Introduction **14**

Présentation 14

Prérequis 15

Chapitre 2: Concepts IDD **16**

Application IDD 16

Gestionnaire de configuration IDD 16

Fichiers de configuration IDD 16

outil d'approvisionnement 17

Zones de sujet et groupes de zones de sujet 17

Domaines 17

Groupes de domaines 18

Relations à l'intérieur des domaines 18

Utilisation de la fonction Informatica MDM Hub 20

Framework d'intégration des services 20

Authentification des utilisateurs (connexion unique) 21

Objets de base 21

Caches et option d'effacement de cache 21

Chemins de correspondance 22

Recherche 22

Fonctions de nettoyage 23

Approbation 24

Flux de travail et tâches 24

Gestionnaire de hiérarchies 25

GAS et sécurité 25

Historique 26

Tables de recherche 26

Chronologie 27

Règles de chronologie 28

Signets 28

Vue des données. 29
Vue de hiérarchie. 29
Tâche. 30
Recherche. 30

Chapitre 3: Processus d'implémentation. 31

Présentation de processus d'implémentation. 31
Avant de commencer. 31
Processus de configuration 32
Étape 1. Création de l'application IDD. 32
Étape 2. Configuration des groupes de domaines. 33
Étape 3. Configuration des domaines. 33
Étape 4. Configuration du nettoyage et de la validation. 35
Étape 5. Configuration de la recherche. 36
Étape 6. Configurer le processus de correspondance. 37
Étape 7. Configurer les flux de travail MDM. 38
Étape 8. Configuration de la sécurité. 38
Étape 9. Configurer les rapports. 39
Étape 10. Configuration des extensions de l'interface utilisateur. 39
Étape 11. Localisation de l'application. 40

Chapitre 4: Gestionnaire de configuration IDD. 41

Présentation du gestionnaire de configuration IDD. 41
Démarrage du gestionnaire de configuration Informatica Data Director. 42
Page d'Accueil. 42
Liaison ORS. 43
Ajout d'une application IDD. 43
Importation d'une configuration d'application IDD. 44
Validation, état de l'application et déploiement 44
Validation. 45
État de l'application. 45
Déploiement. 46
Édition de l'application. 47
Bases de données ORS logiques. 47
Délai d'expiration de session. 48
Domaines. 48
Importer un modèle d'importation de données. 52
Package Fournisseur de connexion personnalisé. 52
Chargement du package Fournisseur de connexion personnalisé. 53
Bibliothèques tierces. 54
Implémentation du fournisseur de connexion personnalisé. 54
Création de la bibliothèque de fournisseurs de connexion. 58
Configuration de l'authentification de la connexion unique SalesForce (WebLogic). 58

Configuration de l'authentification de la connexion unique SalesForce (WebSphere). 58
Exemple d'implémentation du fournisseur de connexion d'authentification unique Google. . . . 59
Configuration de l'authentification de la connexion unique Google. 61

Chapitre 5: Configuration manuelle d'IDD. 62

Présentation de la configuration manuelle d'IDD. 62
Outils XML. 63
Utilisation du fichier XML de configuration IDD 63
Zone de sujet. 65
Colonne de recherche. 65
Afficher les champs secondaires d'un objet de base dans l'onglet enfant. 67
Affichage du parent d'un objet principal dans un onglet enfant. 68
Développement d'un domaine enfant par défaut dans la vue de données 69
Création de référence frère 69
Petits-enfants. 70
Liens de domaines. 70
Regroupement logique de menus. 71
Personnalisation des libellés de colonnes. 71
Configurer le style d'édition de la case à cocher. 71
Configuration du gestionnaire de hiérarchies. 72
Ajouter des relations. 73
Optimisation du rendu. 74
Types de relations du gestionnaire de hiérarchies. 74
Filtre du gestionnaire de hiérarchies. 74
Activation de relations inactives. 74
Enregistrements de la table de relations de la vue de hiérarchie. 74
Vue de l'entité. 75
Personnalisations. 76
Extensions de l'interface utilisateur. 76
Onglets de niveau supérieur de l'espace de travail 77
Onglets de niveau supérieur personnalisés. 77
Démarrez un espace de travail. 77
Onglets enfants personnalisés. 80
Actions personnalisées. 82
Sécurité pour les extensions personnalisées. 85
Sorties utilisateur. 86
Sorties utilisateur et framework Entity 360. 86
Opérations de sorties utilisateur. 86
Création de sorties utilisateur. 91
Configuration d'une sortie utilisateur. 92
Messages des sorties utilisateur. 92
Dépannage. 93
Localisation. 93

Configuration de la langue d'affichage par défaut de la page de connexion et du gestionnaire de configuration. . . . 94
Pages d'erreur personnalisées. . . . 95
Configuration d'une page d'erreur personnalisée. . . . 95
Aide en ligne. . . . 96
Guide de l'utilisateur d'Informatica Data Director. . . . 96
Aide personnalisée. . . . 98

Chapitre 6: Génération de rapport. . . . 100

Présentation de la génération de rapport. . . . 100
Modèles de rapport. . . . 100
Mesures de rapport. . . . 101
Mesures de système source. . . . 101
Mesures de composition des références croisées. . . . 101
Tendances de croissance du domaine. . . . 102
Configuration de la connexion à la base de données du magasin de données. . . . 102
Configuration des paramètres de rapport. . . . 103
Mini-Data Warehouse. . . . 103
Remplissage du magasin de données avec des données de rapport. . . . 104
Activation de la génération de rapport sur le serveur Hub MDM. . . . 104
Configuration d'Informatica Data Director pour afficher les rapports. . . . 104
Définition de rapport. . . . 104
Paramètres de rapport. . . . 105
Paramètres de rapport dynamiques. . . . 105
Exemple de définition de rapport. . . . 106
Configuration d'un accès aux rapports pour un rôle. . . . 106

Chapitre 7: Propriétés globales d'IDD. . . . 107

Références de propriétés globales Informatica Data Director. . . . 107
Mise à jour des propriétés globales. . . . 114

Annexe A: Exigences de plateforme et de dimensionnement. . . . 117

Dimensionnement du serveur de base de données. . . . 117
Dimensionnement du serveur d'applications 117
Dimensionnement du client et du réseau. . . . 117
Configuration requise pour le navigateur. . . . 118

Annexe B: Composants de l'application. . . . 119

Référence sur les composants de l'application. . . . 119

Annexe C: Configuration de la sécurité IDD. . . . 120

Référence sur la configuration de la sécurité IDD. . . . 120

Annexe D: Sécurité des données. 127
Présentation de la sécurité des données. 127
Sécurité des données à l'aide de filtres. 127
Paramètres de sécurité des données. 128
Exemple de configuration d'un objet parent pour la sécurité des données. 128
Exemple de configuration d'un objet petit-enfant pour la sécurité des données. 129
Appliquer la sécurité des données. 130
Sécurité des données dans la recherche de données. 130
Sécurité des données dans les données d'entité. 130
Sécurité des données dans les données hiérarchiques. 134
Sécurité des données dans les données d'historique. 135
Sécurité des données pour les liens profonds. 135

Annexe E: Exemple de configuration de la sécurité basée sur les rôles. 137
Présentation d'un exemple de configuration de la sécurité basée sur les rôles. 137
Concepts clés. 137
IDD, Gestionnaire d'accès de sécurité (GAS) et Services Integration Framework (SIF). 137
Outils de configuration de la sécurité IDD 138
Lectures connexes. 138
Sécurité des objets et des tâches. 138
Conseils pour la conception de la sécurité pour une utilisation dans IDD. 138
Autres considérations. 139
Tâches de configuration de la sécurité IDD. 139
Configuration d'objets de conception dans la Console Hub. 140
Configuration des utilisateurs de l'application IDD (outils Utilisateurs). 140
Configuration de ressources sécurisées (Outil Ressources sécurisées) 141
Création et configuration d'une nouvelle application IDD (gestionnaire de configuration IDD). 141
Affichage des ressources personnalisées (Outil Ressources sécurisées). 141
Configuration des rôles et privilèges de ressource (outil Rôles). 142
Affectation de rôles aux utilisateurs (outil Utilisateurs et Groupes). 146
Ce que des échantillons d'utilisateurs d'IDD pourront voir et faire. 146

Annexe F: Masquage des données. 147
Présentation du masquage des données. 147
Expressions. 147
Échantillons de modèles. 148
Exemple de définition de masque. 148

Annexe G: Moteur de flux de travail Siperian BPM. 149
Siperian BPM est déconseillé. 149
Migrer de Siperian BPM à ActiveVOS. 150
Mettre à jour la configuration d'IDD pour l'adaptateur de flux de travail Siperian. 150

Configurer l'attribution des tâches. . . . 151
Configurer le moteur de flux de travail principal. . . . 151
Flux de travail et tâches. . . . 152
Diagramme des composants de configuration des tâches et des flux de travail. . . . 153
Description des composants de configuration des tâches et des flux de travail. . . . 153
Configuration des tâches. . . . 154
Types de tâches. . . . 154
Types de tâches - Échantillon XML. . . . 155
Attributs TaskType et balises. . . . 156
nom. . . . 156
displayName. . . . 157
creationType. . . . 157
displayType. . . . 158
dataUpdateType. . . . 158
pendingBVT. . . . 158
defaultApproval. . . . 159
Balise de description. . . . 159
Balise d'action. . . . 159
Balise de tâche cible. . . . 159
Personnalisation des types de tâches. . . . 159
Types d'actions. . . . 160
Types d'actions - Échantillon XML. . . . 160
Attributs et balises ActionType 161
nom. . . . 161
displayName. . . . 161
Balise de description. . . . 161
manualReassign. . . . 162
closeTaskView. . . . 162
cancelTask. . . . 162
Balise Class. . . . 162
Configuration de la sécurité des tâches. . . . 162
Affectation des tâches. . . . 163
Configuration de l'affectation des tâches. . . . 163
Interface utilisateur de configuration de l'affectation des tâches. . . . 164
Affectation automatique des tâches. . . . 164
Personnalisation de l'attribution automatique des tâches. . . . 165
Affectation manuelle des tâches. . . . 165
Personnalisation de l'attribution des tâches. . . . 165
Modification des tâches affectées. . . . 165
Notification des tâches. . . . 166
Configuration du courriel de notification des tâches. . . . 166
Configuration du gestionnaire d'utilisateurs dans la Console Hub. . . . 166

Rapports et scores de gestion des tâches. 167
Sécurité des données dans les données de tâche. 168
Tâche de révision. 168
Ouvrir des tâches de révision avec un rôle unique. 168
Ouvrir des tâches de révision avec plusieurs rôles. 169
Filtrer un enregistrement enfant dans la vue de tâche. 170
Ouvrir des tâches de fusion / annulation de fusion. 170
Affectation de tâches compatibles avec les données. 170

Annexe H: Codes de paramètres régionaux. 171

Codes de langue. 171
Codes de pays. 176

Annexe I: Dépannage. 186

Présentation du dépannage. 186
Contrôle de la configuration de votre GAS. 186
Contrôle de la configuration de votre fonction de nettoyage. 187
Les métadonnées d'Informatica Data Director n'ont pas été mises à jour. 187
Informatica Data Director s'interrompt lorsque vous basculez d'une entité à une autre. 187
La configuration d'Informatica Data Director n'est pas valide. 188
Lenteur des performances de correspondance. 188

Annexe J: Glossaire. 189

Index. 198

Préface

Le *Guide d'implémentation Informatica Data Director d'Informatica MDM Multidomain Edition* décrit les configurations d'Informatica Data Director qui s'appuient sur des domaines.

Il contient les informations suivantes :

- Les concepts relatifs aux domaines qui facilitent l'utilisation d'Informatica Data Director (IDD) avec Informatica MDM Hub
- Le processus d'implémentation des applications IDD, notamment les tâches de configuration spécifiques
- Les étapes de configuration des domaines qui nécessitent le gestionnaire de configuration IDD
- Des informations sur la configuration manuelle d'IDD
- Des informations supplémentaires, telles que les conditions requises pour la plateforme et le dimensionnement, les composants d'application IDD, la configuration de la sécurité, les codes des paramètres régionaux et le dépannage.

Ce document est destiné aux clients, partenaires et aux consultants de Services professionnels d'Informatica comme guide d'implémentation pratique pour tous les déploiements d'IDD.

Pour plus d'informations sur la configuration des entités d'entreprise ou du framework Entity 360, consultez le *Guide de l'outil d'approvisionnement d'Informatica MDM Multidomain Edition*.

Ressources Informatica

Informatica Network

Informatica Network héberge le support client international Informatica, la base de connaissances Informatica et d'autres ressources de produits. Vous pouvez accéder à Informatica Network à l'adresse https://network.informatica.com.

En tant que membre, vous pouvez :

- Accéder à toutes les ressources Informatica d'un emplacement.
- Rechercher des ressources de produits dans la base de connaissances, notamment la documentation, les FAQ et les meilleurs pratiques.
- Afficher les informations de disponibilité de produit.
- Vérifier votre cas de support.
- Rechercher votre réseau de groupe d'utilisateurs local Informatica et collaborer avec vos pairs.

Base de connaissances Informatica

La base de connaissances Informatica Network vous permet de rechercher les ressources de produits telles que la documentation, les articles de procédures pratiques, les meilleures pratiques et les matrices de disponibilité de produit (PAM).

Pour accéder à la base de connaissances, visitez le site https://kb.informatica.com. N'hésitez pas à contacter l'équipe Base de connaissances Informatica par courriel à l'adresse KB_Feedback@informatica.com pour lui faire part de vos questions, commentaires et suggestions concernant la base de connaissances.

Documentation Informatica

Pour obtenir la dernière documentation relative à votre produit, parcourez la base de connaissances Informatica à l'adresse https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx.

N'hésitez pas à contacter l'équipe Documentation d'Informatica par courriel à l'adresse infa_documentation@informatica.com pour lui faire part de vos questions, commentaires ou suggestions concernant cette documentation.

Matrices de disponibilité de produit Informatica

Les matrices de disponibilité de produit (PAM) indiquent les versions des systèmes d'exploitation, les bases de données et les autres types de sources et cibles de données pris en charge par une version d'un produit. Si vous êtes un membre d'Informatica Network, vous pouvez accéder aux PAM à l'adresse https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity est un ensemble de conseils et de meilleures pratiques développé par les services professionnels d'Informatica. Développé à partir de l'expérience concrète de centaines de projets de gestion de données, Informatica Velocity représente le savoir collectif de nos consultants, qui ont travaillé avec des entreprises du monde entier pour planifier, développer, déployer et tenir à jour des solutions de gestion des données efficaces.

Si vous êtes membre d'Informatica Network, vous pouvez accéder aux ressources d'Informatica Velocity à l'adresse http://velocity.informatica.com.

Si vous avez des questions, des commentaires et des suggestions sur Informatica Velocity, contactez le support des services professionnels d'Informatica à l'adresse ips@informatica.com.

Informatica Marketplace

Informatica Marketplace est un forum dans lequel vous pouvez trouver des solutions qui permettent d'augmenter, d'étendre ou d'améliorer vos implémentations Informatica. L'utilisation d'une des centaines de solutions créées par les développeurs et partenaires Informatica vous permettra d'améliorer votre productivité et d'accélérer le temps d'implémentation de vos projets. Vous pouvez accéder à Informatica Marketplace à l'adresse https://marketplace.informatica.com.

Support client international Informatica

Vous pouvez contacter un centre de support international par téléphone ou via le support en ligne sur Informatica Network.

Pour trouver le numéro de téléphone du support client international Informatica, visitez le site Web Informatica à l'adresse http://www.informatica.com/us/services-and-training/support-services/global-support-centers.

Si vous êtes un membre d'Informatica Network, vous pouvez utiliser le support en ligne à l'adresse http://network.informatica.com.

CHAPITRE 1

Introduction

Ce chapitre comprend les rubriques suivantes :

- Présentation, 14
- Prérequis, 15

Présentation

Attention: Ce guide explique comment créer une application Informatica Data Director (IDD) héritée et basée sur un modèle de domaine. Pour obtenir des instructions sur la manière de créer une application IDD actuelle en fonction du modèle d'entité d'entreprise, consultez plutôt le *Guide de l'outil d'approvisionnement d'Informatica MDM Multidomain Edition*.

Informatica Data Director (IDD) est une application de gouvernance des données qui active des solutions de données principales qui sont efficaces pour toutes les parties prenantes de l'équation de gouvernance des données, telles que :

- Utilisateurs professionnels
- Gestionnaires des données
- Responsables IT

Informatica Data Director est hautement configurable, avec une interface facile d'utilisation basée sur le modèle de données de votre organisation. Informatica Data Director pour Informatica MDM Hub permet aux utilisateurs professionnels d'exécuter les fonctions décrites dans la table suivante de manière efficace :

Fonctionnalité	Description
Créer	Créer des données principales de grande qualité, en travaillant individuellement ou de manière collaborative au sein de votre entreprise.
Gérer	Gérer les doublons, résoudre les correspondances, approuver et gérer les mises à jour de vos données principales, créer des tâches et les attribuer aux utilisateurs des données.
Consommer	Rechercher toutes les données principales depuis un emplacement centralisé, afficher les détails des données principales.
Surveiller	Suivre le lignage et l'historique, auditer la conformité des données principales, personnaliser votre tableau de bord.

Prérequis

Ce document nécessite d'être familiarisé avec l'architecture Informatica MDM Hub et de comprendre tous les principes des composants de la solution Informatica MDM Hub dans votre déploiement qui seront utilisés par des applications IDD.

Pour en savoir plus, consultez la documentation du produit Informatica MDM Hub.

CHAPITRE 2

Concepts IDD

Ce chapitre comprend les rubriques suivantes :

- Application IDD , 16
- Gestionnaire de configuration IDD, 16
- Fichiers de configuration IDD, 16
- outil d'approvisionnement, 17
- Zones de sujet et groupes de zones de sujet, 17
- Utilisation de la fonction Informatica MDM Hub , 20
- Signets, 28

Application IDD

Une application IDD est l'unité principale de configuration et de déploiement pour les implémentations IDD. Une application IDD est ce que les utilisateurs professionnels observent quand ils lancent IDD et s'y connectent.

Gestionnaire de configuration IDD

Le gestionnaire de configuration IDD est un utilitaire basé sur le Web, qui sert à ajouter, modifier et gérer des applications IDD.

LIENS CONNEXES :

- “Gestionnaire de configuration IDD” à la page 41

Fichiers de configuration IDD

Une application IDD comporte un ensemble de fichiers de configuration : un fichier de configuration IDD (XML), des ensembles de ressources, des ensembles de messages d'internationalisation, une aide en ligne et d'autres fichiers auxiliaires. Vous pouvez charger ou modifier des applications IDD dans le gestionnaire de configuration IDD, ou les exporter et les éditer manuellement.

LIENS CONNEXES :

- "Composants de l'application" à la page 119

outil d'approvisionnement

Vous pouvez utiliser l'outil d'approvisionnement pour définir des modèles, des tâches et des transformations d'entités d'entreprise et concevoir l'interface utilisateur d'Informatica Data Director.

Informatica Data Director requiert une configuration d'entité commerciale pour les fonctionnalités basées sur le framework Entity 360, telles que le gestionnaire des tâches et la vue Entité. Informatica Data Director nécessite également une configuration de domaine pour les fonctionnalités telles que la vue Hiérarchie, la vue XREF et la page Comparaison de correspondances pour la fusion.

Ce guide présente la configuration de domaine pour Informatica Data Director. Pour plus d'informations sur la configuration du framework Entity 360 et des entités commerciales, consultez le *Guide de l'outil d'approvisionnement d'Informatica MDM Multidomain Edition*.

Zones de sujet et groupes de zones de sujet

Dans une application IDD, les données sont organisées autour de zones de sujet et regroupées en groupes de zones de sujet.

Domaines

Le *domaine* est un concept d'organisation de base pour l'application Informatica Data Director.

Les termes ou concepts suivants se rapportent également au domaine (ou s'en approchent) : objet d'entreprise et entité hiérarchique. Informatica Data Director utilise la définition du domaine pour déterminer la manière de traiter chaque relation de clé étrangère dans un stockage de référence opérationnelle.

Le Stockage Hub conserve les métadonnées détaillées sur les tables et relations définies dans un ORS. Les métadonnées comprennent les relations entre les tables d'objet de base qui peuvent représenter :

- des références aux tables de recherche
- des liens entre un parent et les données enfants associées
- des liens associatifs entre les tables (ne représentant pas une relation de propriété)

Le Stockage Hub fournit certaines des métadonnées qui permettent à Informatica Data Director de comprendre le mode de traitement des relations. Par exemple, l'indicateur de recherche de l'objet de base indique à Informatica Data Director à quel moment traiter une table liée en tant que recherche avec une liste déroulante pré-remplie qui sera visible des utilisateurs dans l'application Informatica Data Director.

Pour les autres relations, une application Informatica Data Director peut nécessiter d'autres informations pour bien les comprendre et savoir si elles doivent être interprétées comme relations entre les tables d'un domaine ou comme relations entre les domaines. Le gestionnaire de configuration Informatica Data Director s'utilise pour indiquer ces informations supplémentaires aux applications Informatica Data Director. Vous ne pouvez pas utiliser d'alias pour un domaine basé sur une relation de gestionnaire de hiérarchies.

Un domaine représente un ensemble de données qui doit être traité comme une unité d'un point de vue commercial. Un domaine comprend :

- Un seul enregistrement racine dans un objet de base
- Un certain nombre d'enregistrements enfants et petits-enfants (par le biais des relations un à plusieurs et plusieurs à plusieurs).

Groupes de domaines

Un *groupe de domaines* est un ensemble d'une ou de plusieurs domaines qui ont le même objet de base à leur racine (appelé également l'*objet principal*).

Par exemple, un ORS utilisant un modèle Partie (un seul objet de base représentant différents types d'entités) comprend un groupe de domaines avec plusieurs domaines.

Remarque: Un objet de base ne peut être associé qu'à un seul groupe de domaines.

Relations à l'intérieur des domaines

Dans une application IDD, les relations au sein des domaines sont basées sur les relations configurées entre les objets de base dans le Stockage Hub (à l'aide du gestionnaire de schéma dans la Console Hub).

Le gestionnaire de configuration IDD fait référence aux *composants de chemin de correspondance* configurés, qui sont basés sur les relations de clés étrangères.

Relations enfant un à plusieurs

Pour une relation un à plusieurs, l'enregistrement enfant a une clé étrangère directe avec l'objet principal. IDD prend en charge deux types de relations un à plusieurs.

La table suivante décrit les types de relations enfant un à plusieurs :

Relation	Description
Un à plusieurs	La liste des enregistrements enfant est affichée dans un onglet au-dessous des données principales.
Un à un logique	Un seul enregistrement enfant est prévu pour chaque objet principal. Les données sont affichées dans le formulaire avec l'objet principal. S'il existe plusieurs enfants (par exemple en raison de la fusion de deux enregistrements d'objets principaux), l'application IDD permet de résoudre ce problème.

Relations enfants plusieurs à plusieurs

Pour les relations plusieurs à plusieurs, l'enregistrement enfant est associé à l'objet principal par le biais d'une table de relations.

IDD prend en charge deux types de relations plusieurs à plusieurs. La table suivante décrit les types de relations enfants plusieurs à plusieurs :

Relation	Description
Partie de	L'enregistrement enfant appartient à l'objet principal, aucun autre domaine ne doit référencer cet enfant. Lors de l'ajout d'un enfant, la relation et les enregistrements enfants sont ajoutés. Lors de l'édition d'un enfant, si un autre domaine y fait référence, une copie de l'enfant est créée. Les données référencées par l'autre enfant restent inchangées.
Référence	L'enfant est un autre domaine. Lors de l'ajout d'un enfant, seul un enregistrement de relation est ajouté. L'utilisateur de l'application IDD doit rechercher l'enfant de domaine à associer. Pour éditer les données de l'enfant, le domaine de l'enfant doit être ouvert. L'enfant peut être lié par une relation du Base Object standard ou par un relation du Base Object du gestionnaire de hiérarchies.

Relations petits-enfants un à plusieurs

Pour des relations un à plusieurs, l'enregistrement petit-enfant a une clé étrangère directe avec l'objet enfant. IDD prend en charge deux types de relations un à plusieurs : si l'enfant est de type plusieurs à plusieurs, la clé étrangère peut être vers (voir les exemples de modèles de données ci-dessous) :

- La relation enfant
- L'enregistrement des relations

Relation	Description
Un à plusieurs	La liste des enregistrements petits-enfants est affichée dans un onglet au-dessous des données enfants.

Relations petits-enfants plusieurs à plusieurs

Pour les relations plusieurs à plusieurs, l'enregistrement petit-enfant est associé à un objet enfant par le biais d'une table de relations.

IDD prend en charge deux types de relations plusieurs à plusieurs : si l'enfant est de type plusieurs à plusieurs, la clé étrangère peut être sur (voir les exemples de modèles de données ci-dessous) :

- Enregistrement enfant
- Enregistrement de relations.

Le tableau suivant décrit les types de relations petits-enfants plusieurs à plusieurs :

Relation	Description
Partie de	L'enregistrement petit-enfant appartient à l'objet principal, aucun autre domaine ne doit référencer ce petit-enfant. Lors de l'ajout d'un petit-enfant, la relation et les enregistrements petits-enfants sont ajoutés. Lors de l'édition d'un petit-enfant, si un autre domaine y fait référence, une copie du petit-enfant est créée. Les données référencées par l'autre enfant restent inchangées.
Référence	Le petit-enfant est un autre domaine. Lors de l'ajout d'un petit-enfant, seul un enregistrement de relation est ajouté. L'utilisateur de l'application IDD doit rechercher le petit-enfant de domaine à référencer. Pour éditer les données du petit-enfant, le domaine de ce petit-enfant doit être ouvert. Le petit-enfant peut être lié par une relation du Base Object standard ou par un relation du Base Object du gestionnaire de hiérarchies.

Remarque: Lors de la configuration du chemin de correspondance pour les petits-enfants dans le gestionnaire de schéma de la Console Hub, assurez-vous que **Contrôler l'enfant absent** est désactivé. L'application IDD ne fonctionne pas correctement si **Contrôler l'enfant absent** est activé.

Références de fratries

Une référence de fratrie est une relation d'un enregistrement dans un domaine vers un enregistrement enfant dans ce domaine.

Pour un modèle de données, un client pourrait inclure les enregistrements enfants d'adresse et de numéro de téléphone, le numéro de téléphone ayant une clé étrangère pour l'associer à une adresse spécifique. IDD peut être configuré pour prendre en charge ce type de relation.

Lors de l'ajout et de l'édition de la clé d'adresse sur le numéro de téléphone, l'utilisateur de l'application IDD reçoit une liste d'adresses contenant uniquement les enfants de cette partie.

Liens connexes :

- "Configuration manuelle d'IDD" à la page 62

Enregistrements parents

Un enregistrement qui est un parent de l'objet principal peut être inclus dans le domaine.

Il apparaît dans un onglet enfant. Comme il n'y a toujours qu'un enregistrement dans cet onglet, il apparaît toujours dans une vue de formulaire. Ces données sont en lecture seule. IDD n'autorise pas l'édition de ces données ni de la relation avec ces données.

Utilisation de la fonction Informatica MDM Hub

Framework d'intégration des services

Toutes les interactions entre une application IDD et un ORS passent par des appels API du Framework d'intégration des services (SIF).

Il n'y a pas d'accès direct à la base de données d'ORS (avec une exception : les graphes peuvent être configurés pour utiliser une source de données de serveur d'applications pour obtenir les données de

rapport). Le gestionnaire de configuration IDD utilise SIF pour accéder aux métadonnées relatives à un ORS, mais utilise une source de données pour accéder directement à la table CMX_SYSTEM.C_REPOS_DS_CONFIG.

Certains des appels de l'API SIF IDD sont asynchrones car IDD est une application multi-utilisateurs. Pour permettre la prise en charge des appels SIF asynchrones, le verrouillage au niveau des lignes doit être activé pour l'ORS auquel est liée l'application IDD. Pour plus d'informations, consultez la section sur le verrouillage au niveau des lignes dans le *Guide de configuration d'Informatica MDM Multidomain Edition* .

Utilisation d'un serveur Web

Avant de mettre en place un serveur Web qui fasse office de proxy inverse, configurez le format de l'URL du service qu'IDD génère pour les appels SIF. Configurez la propriété referer.url dans le fichier `cmxserver.properties` pour spécifier le format de l'URL du service.

Ajoutez le texte suivant au fichier `cmxserver.properties` pour configurer le format de l'URL du service :

```
referer.url=http://<hôte local>:<numéro de port>
```

Authentification des utilisateurs (connexion unique)

Par défaut, IDD authentifie les utilisateurs avec un appel SIF au serveur Hub. Pour la procédure d'authentification, l'implémentation MDM Hub exige que vous configuriez les utilisateurs pour la base de données principale. Pour plus d'informations sur la configuration des utilisateurs d'Informatica MDM Hub, consultez le *Guide de sécurité d'Informatica MDM Multidomain Edition*.

Par ailleurs, IDD propose un mécanisme pour l'installation d'un fournisseur de connexion externe. Il s'agit d'un plug-in qui identifie des utilisateurs par rapport à des fournisseurs d'identité externes (prise en charge de l'identification unique SSO). Le fournisseur de connexion côté IDD fonctionne avec le fournisseur de sécurité du Hub (module de connexion). Pour plus d'informations sur les fichiers de fournisseurs, consultez le *Guide de sécurité d'Informatica MDM Multidomain Edition*.

Objets de base

La sécurité au niveau des colonnes est configurée dans le gestionnaire d'accès de sécurité (GAS) en définissant l'accès basés sur les rôles aux objets de base et à leurs colonnes, ce qui offre un contrôle précis de l'accès des utilisateurs aux données.

IDD référence directement les objets de base pour toutes les opérations `GET` et `PUT`. IDD utilise des packages uniquement pour afficher des résultats de recherche.

Caches et option d'effacement de cache

Informatica Data Director conserve un cache de métadonnées de MDM Hub qui décrit les objets de base, les colonnes, les relations et d'autres détails. Si vous modifiez les métadonnées de MDM Hub, cliquez sur **Effacer le cache** dans le gestionnaire de configuration IDD avant d'exporter une application IDD.

L'option Effacer le cache du gestionnaire de configuration IDD efface le cache de l'application IDD sélectionnée. Dans un environnement Microsoft SQL Server, Informatica vous recommande d'effacer le cache lorsque vous apportez des modifications aux métadonnées ORS via la console Hub. Par exemple, si vous ajoutez une relation à un objet de base dans la console Hub et qu'ensuite vous enregistrez et validez les modifications, vous pouvez redéployer l'application IDD pour que les modifications deviennent effectives. Cependant, vous devez effacer le cache avant d'exporter l'application IDD pour voir la nouvelle relation dans le fichier MetadataBundle.properties.

Vous pouvez également redémarrer le serveur d'applications pour effacer le cache.

IDD conserve également les caches des attributions et des définitions de rôles du GAS et des valeurs de recherche. IDD actualise les caches à un rythme que vous pouvez configurer via les propriétés globales d'IDD.

Chemins de correspondance

Les objets enfant dans IDD sont définis à l'aide de chemins de correspondance, qui sont configurés à l'aide du gestionnaire de schéma dans la Console Hub.

Avant le lancement d'IDD, les chemins de correspondance avaient été utilisés strictement pour définir des colonnes de correspondance et des règles de correspondance. La définition du chemin de correspondance fonctionne tout aussi bien pour définir les relations enfants dans IDD.

Pour ajouter un enfant à un domaine, il sera nécessaire de créer un nouveau chemin de correspondance pour cet enfant s'il n'en existe pas encore. La définition d'un tel chemin de correspondance n'implique pas une surcharge de performances supplémentaire.

Les chemins de correspondance peuvent aussi être utilisés pour activer la recherche sur les tables liées qui ne font pas partie d'un domaine. Par exemple, supposez que vous avez une Partie liée à un Produit. Le Produit ne ferait pas partie du domaine Partie. Toutefois, un chemin de correspondance peut être défini de la Partie au Produit. Avec ce chemin de correspondance, un utilisateur de l'application IDD pourrait rechercher un Partie d'après les attributs d'un Produit lié.

Recherche

La recherche de données dans un domaine peut être basée sur l'une des API de recherche SIF suivantes : searchQuery et searchMatch.

Dans les deux cas, un package d'affichage est utilisé pour afficher les résultats de la recherche.

De base - Recherche basée sur SQL

La recherche de base utilise l'API searchQuery.

Une recherche peut être basée sur des données dans :

- Enregistrement d'objet principal
- Un de ses enregistrements enfants (objet primaire)
- Tout enregistrement lié via un composant de chemin de correspondance

Vous pouvez réaliser une recherche de base sensible à la casse lorsque vous exécutez une requête de données. La recherche de base trouve des résultats à l'aide de comparaisons de chaînes et modèles de chaînes.

Étendue - Recherche basée sur les correspondances

La recherche étendue n'est pas sensible à la casse et utilise l'API **searchMatch** avec matchType=NONE.

Elle sert aux recherches, et n'utilise donc pas un ensemble de règles de correspondance prédéfini. Toute donnée dans le domaine contribuant à une colonne de correspondance peut être utilisée comme critère de recherche. Une application IDD exige des utilisateurs qu'ils entrent des critères dans la clé de correspondance approximative avant de pouvoir exécuter la recherche.

Recherche avancée

La recherche avancée permet aux utilisateurs de l'application IDD de créer des requêtes complexes en définissant des expressions de type SQL WHERE et un texte de requête de forme libre.

Vous pouvez réaliser une recherche avancée sensible à la casse lorsque vous exécutez une requête de données. La recherche avancée permet aux utilisateurs de l'application IDD de spécifier des conditions de recherche qui vont au-delà des capacités disponibles dans les recherches de base et étendues.

Fonctions de nettoyage

IDD utilise l'API **PUT** plutôt que **cleansePut**.

IDD peut toutefois appeler l'API de **nettoyage** pour chaque enregistrement d'objet de base avant son enregistrement. Ce processus est appelé parfois *fonction de nettoyage intégrée*. La fonction de nettoyage peut effectuer un nettoyage régulier des données ainsi qu'une standardisation et des validations personnalisées des données. Chaque fonction de nettoyage configurée est appelée avant tout enregistrement des données.

- Dans la vue des données, le nettoyage est appelé lors d'un clic sur le bouton **Appliquer** d'un formulaire d'édition.
- Dans la vue de hiérarchie, le nettoyage est appelé lors d'un clic sur le bouton **OK** d'une boîte de dialogue d'ajout/édition de relation.

Nettoyage et standardisation

Le gestionnaire de configuration IDD fournit un moyen direct pour connecter les enregistrements d'objet de base aux entrées et sorties d'une fonction de nettoyage.

Les données de l'enregistrement d'objet de base sont mises à jour avec les sorties provenant de la fonction de nettoyage.

Remarque: Seules les colonnes de l'objet de base sélectionnées dans la mise en page pour la configuration du domaine peuvent servir d'entrées ou de sorties de la fonction de nettoyage.

Validation

Une fonction de nettoyage permet d'effectuer la validation de données personnalisée.

Les résultats de validation sont traités si la fonction de nettoyage comprend un paramètre de sortie validationStatus.

- Si le paramètre validationStatus n'est pas défini, il n'existe aucune erreur de validation et le processus peut se poursuivre.
- En cas d'erreurs de validation, le paramètre validationStatus comprend une série de messages de validation décrivant le nom inputParameter et un message. Dans l'IU de l'application IDD, chaque erreur de validation est associée à une valeur d'entrée dans une colonne d'entrée spécifique.

Remarque: Le Kit de ressources contient le modèle ValidationCleanseLib, qui fournit un exemple de bibliothèque de nettoyage avec des fonctions qui exécutent la validation dans une application IDD.

Fonctions de nettoyage renvoyant NULL

Lorsque la sortie d'une fonction de nettoyage est une valeur Null, l'API de **nettoyage** ne renvoie aucune information sur ce champ.

Il est supposé que la fonction ne modifie pas ce champ. Si l'objectif est que la fonction de nettoyage écrase une valeur avec NULL, les options dépendent du type de données, et les éléments suivants sont requis :

- Chaîne - La fonction peut être modifiée pour renvoyer une chaîne vide.
- Date ou numérique - Une sortie utilisateur doit être implémentée pour modifier les données. Les méthodes beforeEverything() ou beforeSave() du système de traitement Save peuvent être utilisées.

Liens connexes :

- "Sorties utilisateur" à la page 86

Approbation

Une application Informatica Data Director est configurée pour utiliser un système source unique pour toutes ses opérations.

Les données entrées et mises à jour via une application Informatica Data Director suivent toutes les règles d'approbation standard, comme décrit dans l'aide en ligne de la console d'administration ou la section *Guide de configuration d'Informatica MDM Multidomain Edition*. Les données entrées dans une application Informatica Data Director sont appliquées à l'enregistrement de l'objet de base en fonction des règles d'approbation et de validation configurées dans Informatica MDM Hub pour ce système source. Lorsque vous affichez les données de références croisées, vous pouvez promouvoir la valeur d'un attribut à partir d'un enregistrement de références croisées pour les colonnes dont l'approbation est activée. Ceci entraîne un remplacement d'approbation pour cet attribut.

Flux de travail et tâches

Une application IDD peut utiliser des flux de travail et des tâches pour prendre en charge un processus d'approbation de modification pour les enregistrements dont l'état est activé dans le Stockage Hub.

Par exemple, supposons qu'un gestionnaire des finances veuille vérifier toutes les modifications apportées aux informations bancaires du client avant que la modification puisse être acceptée comme données principales. Vous pouvez configurer une application IDD de sorte que, lorsqu'une personne du service des finances utilise l'application pour mettre à jour des informations, une tâche de vérification des modifications en attente est automatiquement attribuée au gestionnaire des finances afin qu'il les approuve ou les rejette. Un processus d'approbation des modifications garantit que seuls les enregistrements approuvés contribuent aux enregistrements Meilleure version de la vérité (MVV).

Une application IDD coordonne les activités de tâche dans la boîte de réception des tâches IDD, dans un outil de gestion des processus d'entreprise et dans les tables dont l'état est activé dans le stockage Hub. Pour inclure la prise en charge de flux de travail dans votre application, consultez "Étape 7. Configurer les flux de travail MDM" à la page 38.

Tâches et actions

Une *tâche* est une étape d'un processus de workflow.

Pour toute tâche, une ou plusieurs *actions* peuvent être effectuées. Les tâches et leurs actions associées peuvent être configurées dans le cadre d'une application IDD.

Données de traitement

Les *données de traitement* sont des données d'entreprise qui passent par des états différents (ACTIVE, PENDING ou DELETED) lors de l'avancement dans un workflow.

IDD fournit la prise en charge des données de traitement à l'aide de la fonctionnalité de gestion d'état de Informatica MDM Hub et des fonctions de gestion des tâches.

Les données peuvent être ajoutées ou mises à jour et « Soumises pour approbation » plutôt qu'enregistrées. Les modifications de données sont stockées en tant que modifications à l'état PENDING. Les données ne sont pas appliquées à l'objet de base. Une tâche est créée pour qu'un autre utilisateur approuve cette modification. Une fois approuvées, les données à l'état PENDING sont promues vers ACTIVE, puis appliquées à l'objet de base.

Gestionnaire de hiérarchies

Si le gestionnaire de hiérarchies est configuré pour un ORS, vous pouvez configurer une application IDD pour fonctionner avec cette configuration.

Configurez l'application IDD d'après les règles suivantes :

- Toute entité du gestionnaire de hiérarchies utilisée par une application IDD doit être configurée comme domaine dans le gestionnaire de configuration IDD. Le gestionnaire de hiérarchies sert à modéliser les relations entre les domaines.
- Une application IDD fonctionne par rapport à une seule configuration du gestionnaire de hiérarchies (association profils/sandbox). IDD utilise la configuration du contrôle d'accès au GAS plutôt que des configurations du gestionnaire de hiérarchies différentes pour gérer le contrôle d'accès des utilisateurs. La configuration du gestionnaire de hiérarchies utilisée par une application IDD doit inclure tous les types de relations et d'entités du gestionnaire de hiérarchies à utiliser dans l'application IDD.

GAS et sécurité

IDD utilise le système précis de contrôle d'accès du GAS, tel qu'il est configuré dans la Console Hub.

Pour plus d'informations, consultez le *Guide de sécurité d'Informatica MDM Multidomain Edition*.

Liens connexes :

- "Configuration de la sécurité IDD" à la page 120

Sécurité des objets et des colonnes

Le GAS fournit pour les objets de conception et colonnes définis dans un ORS des privilèges de sécurité basés sur les rôles.

Une application IDD utilise cette configuration de sécurité de sorte que les données affichées et les opérations disponibles pour un utilisateur individuel dépendent du ou des rôles affectés à ce compte utilisateur. Les utilisateurs de l'application IDD voient uniquement les données et fonctionnalités auxquelles ils ont accès. Par exemple, si un utilisateur n'a pas d'accès READ à une table HISTORY d'un objet de base, dans l'application IDD, la commande Historique pour ce domaine n'est pas disponible pour lui.

Remarque: Un utilisateur de Hub avec accès Administrateur (configuré dans l'outil Utilisateurs de la Console Hub) est un superutilisateur pour IDD et bénéficie de privilèges complets sur tous les objets.

Sécurité des données

Le GAS ne propose pas une sécurité des données au niveau de la ligne (qui limite l'affichage par les utilisateurs de certains enregistrements d'après le contenu de ces enregistrements).

Toutefois, IDD propose un mécanisme simple de sécurité des données. Pour chaque domaine, des *filtres de sécurité* peuvent être définis dans le fichier de configuration IDD. Un filtre de sécurité spécifie une condition de filtre, qu'IDD applique à toute donnée à laquelle accèdent les utilisateurs affectés à un rôle spécifique. Par exemple, un filtre de sécurité peut spécifier `COUNTRY_CODE = 'US'`, qui peut être appliqué aux utilisateurs ayant le rôle de gestionnaire des données US. Chaque filtre peut s'appliquer à plusieurs rôles. Tout nombre de filtres peut être créé pour un domaine pour tout nombre de rôles.

Masquage des données

IDD fournit un mécanisme de masquage des informations suivant les rôles de sécurité.

Vous pouvez définir un masque pour chaque champ dans une mise en page de colonne. Le masque peut être spécifié pour un rôle unique, pour un ensemble de rôles ou pour tous les rôles autres qu'administrateur. Lorsque vous spécifiez un masque, tout ou partie de la valeur est remplacée par un astérisque (*).

Liens connexes :

- "Masquage des données" à la page 147

Historique

IDD propose une vue des domaines de l'historique des modifications pour chaque enregistrement.

Cette fonctionnalité nécessite l'activation de l'historique sur l'objet de base. Si l'historique n'est pas activé pour un objet de base, la Vue de l'historique n'est pas disponible pour le domaine associé dans l'application IDD. IDD montre une vue de l'horaire des événements pour l'enregistrement et ses enregistrements enfants. Il est également possible d'afficher une vue des données à un moment précis.

Tables de recherche

Une table de recherche, également appelée recherche, est une table qui stocke une liste de valeurs prédéfinies dans une table relationnelle ou un fichier. IDD interroge la table de recherche pour récupérer une valeur basée sur celle de la source d'entrée et sur la condition de recherche. IDD renseigne ensuite une liste déroulante de valeurs parmi lesquelles l'utilisateur de l'application IDD peut choisir. Par exemple, si vous entrez une valeur dans le champ Pays, IDD répertorie les pays stockés dans la table de recherche d'objet de base LU_COUNTRY.

Vous pouvez définir les valeurs de recherche des manières suivantes :

- Dans une table d'objet de base de recherche physique avec une clé étrangère entre l'objet de base et l'objet de base de recherche. IDD utilise des métadonnées relatives à la clé étrangère pour renseigner les valeurs de recherche.
- Dans une table d'objet de base de recherche physique sans clé étrangère entre l'objet de base et l'objet de base de recherche. La configuration IDD décrit la relation de clé étrangère qui renseigne les valeurs de recherche.
- Dans une liste statique de valeurs dans la configuration IDD.

Pour les recherches définies dans une table physique, la colonne LOOKUP_IND de C_REPOS_TABLE indique si la table contient des valeurs de recherche ou des données classiques. Activez l'indicateur de recherche via l'outil Schéma de la console Hub. Par défaut, l'indicateur de recherche est désactivé lorsque vous créez un objet de base. Lorsque vous activez l'indicateur de recherche, MDM Hub considère l'objet de base comme

étant une recherche. Pour plus d'informations sur l'outil Schéma, consultez le *Guide de configuration d'Informatica MDM Multidomain Edition*.

Remarque: Lorsque vous créez une recherche, utilisez un nom d'affichage unique. IDD ne peut pas distinguer différentes tables de recherche qui partagent le même nom d'affichage.

Lorsqu'IDD reconnaît qu'une colonne dispose d'une clé étrangère pour une autre table, il détermine si la table associée est une table de recherche. Si la table associée est une table de recherche, IDD crée une liste déroulante dans l'application IDD pour cette colonne, remplie de valeurs émanant de la table de recherche. La colonne dans la table de recherche utilisée dépend du champ **Nom d'affichage de recherche** configuré pour la relation dans l'outil Schéma.

Liens connexes :

- "Colonne de recherche" à la page 65

Recherches dépendantes

Une recherche dépendante est une table de recherche qui dépend d'une autre.

Un exemple typique de table de recherche dépendante est une table de recherche de type et une table de recherche de sous-type. La liste des valeurs qui s'affichent dans le champ de sous-type dépend de la valeur sélectionnée dans le champ de type dans IDD. Par exemple, vous avez sélectionné États-Unis dans un champ Pays. Lorsque vous entrez une valeur dans un champ État, IDD répertorie les états américains stockés dans la recherche dépendante LU_STATE.

Chronologie

La chronologie vous permet d'afficher et de gérer les événements de modification des données des entités métier et leurs relations. Vous pouvez définir les événements de modification des données ou les versions des entités métier et leurs relations selon leurs périodes efficaces.

Les modifications de données se produisent au fil du temps et sont indépendantes de leur relation à d'autres données. Les modifications apportées aux données entraînent la création d'une période d'efficacité ou la mise à jour d'une période d'efficacité passée, présente ou future. La fonction de chronologie vous permet de suivre ces modifications de données sur une période donnée.

Par exemple, John Smith vivait à Los Angeles du 31 janvier 2008 au 20 octobre 2010. Il vit maintenant à San Francisco depuis le 21 octobre 2010. Il va habiter à Las Vegas à partir du 25 novembre 2014. Utilisez la fonction de chronologie pour suivre les modifications passées, présentes et futures apportées à des données telles que l'adresse de John Smith.

Remarque: Vous pouvez spécifier une période efficace dans le format de date. Le système utilise les paramètres régionaux de la base de données pour les dates.

Les fonctionnalités de chronologie fournissent une visibilité à deux dimensions aux données, en fonction de la période d'efficacité et de l'historique. La période d'efficacité d'un enregistrement est définie par la date de début réelle et la date de fin réelle d'un enregistrement d'objet de base. L'historique est une date issue de l'historique d'un enregistrement dont vous devez afficher la valeur. Vous pouvez gérer les événements de données d'entités métier (telles que l'adresse d'un client, son numéro de téléphone et ses relations) en activant la chronologie pour les objets de base appropriés. Pour activer la chronologie d'un objet de base enfant, vous devez tout d'abord activer la chronologie pour l'objet de base parent. MDM Hub utilise les tables de références (XREF) qui sont associées aux objets de base dont la chronologie est activée pour maintenir les périodes efficaces pour les enregistrements de l'objet de base.

Remarque: Vous devez activer la chronologie pour chaque objet de base dans la console Hub, sauf pour l'objet de base de la relation enfant activé par le gestionnaire de hiérarchies.

Pour plus d'informations, consultez le *Guide de configuration d'Informatica MDM Multidomain Edition*

Règles de chronologie

Lorsque vous définissez et maintenez les informations de chronologie, le Hub MDM applique les règles de chronologie.

Vous devez connaître les règles que le Hub MDM applique pour gérer les chronologies des entités métier et des relations. À n'importe quel point dans le temps, le Hub MDM ne considère qu'une seule version d'un enregistrement comme étant efficace, en fonction des dates réelles de début et de fin. Lorsque vous utilisez les processus de lots, les Framework d'intégration des services ou Informatica Data Director pour modifier les données, le Hub MDM conserve les données efficaces courantes. En outre, lorsque plusieurs systèmes contribuent à un enregistrement d'objet de base, le Hub MDM applique les règles pour mettre à jour la version de l'enregistrement, basé sur les enregistrements de contribution efficaces.

Vous pouvez également utiliser les sorties utilisateur pour définir et appliquer des règles personnalisées pour gérer les chronologies et les dates efficaces.

Pour plus d'informations, consultez le *Guide de configuration d'Informatica MDM Multidomain Edition*

Signets

Les signets sont des URL qui permettent d'ouvrir une application IDD et d'afficher une vue, une tâche ou une recherche.

Remarque: les signets sont disponibles pour les applications IDD qui utilisent le modèle de domaine.

L'URL spécifie quelle application IDD appeler, quelle partie de l'application ouvrir et quelle entité afficher. Des signets peuvent être utilisés pour appeler IDD depuis une application externe (par exemple, Informatica MDM Data Control, ou IDC), ou depuis un navigateur. Un utilisateur peut partager une URL de signet avec un autre utilisateur. Lorsqu'un utilisateur ouvre l'URL dans un navigateur, il doit se connecter à l'application IDD pour afficher la vue.

Dans une application IDD, vous pouvez créer des liens vers des commandes Afficher le signet sur les pages. Ces commandes fournissent l'URL pour l'entité en cours. Des signets sont disponibles pour les fonctionnalités suivantes : Vue des données, Vue de hiérarchie, tâches et recherches.

Le format de l'URL est :

```
http://<host>[:<port>]/bdd/?deeplink=<operation>;<iddAppName>/
<subjectAreaID>;<param1>[;<param2>]
```

Où :

Variable	Description
host	Nom de la machine qui héberge Informatica MDM Hub.
port	Facultatif. Numéro de port
operation	Une des valeurs suivantes : - openrecord;dv - ouvre une entité dans la Vue des données - openrecord;hm - ouvre une entité dans la Vue de hiérarchie - opentask - ouvre une fenêtre de tâche - recherche - ouvre une fenêtre de recherche
iddAppName	Nom de l'application IDD.

Variable	Description
subjectAreaID	Identifie le domaine. Utilise le format suivant : `subjectAreaGroupName/SubjectAreaName`
param1	Définit les données à afficher et dépend de l'opération.
param2	Facultatif. Dépend de l'opération.

Remarque: Tout caractère non autorisé dans une URL doit subir un double codage. Le double codage (exécuter deux fois le processus de codage) est requis pour permettre aux serveurs Web d'accepter des requêtes contenant des barres obliques (/ et \) dans leurs paramètres. Les requêtes contenant des barres obliques à codage simple utilisées dans les paramètres sont rejetées par les serveurs Web. Seules les valeurs de paramètres doivent subir un double codage.

Vue des données

L'opération *openrecord;dv* est utilisée pour ouvrir une vue des données.

L'élément *subjectAreaID* identifie le domaine, et *param1* identifie l'enregistrement. Comme avec les API SIF, un enregistrement peut être identifié par rowid ou par nom de système et clé source. Lors de l'utilisation de la clé source, veillez à inclure dans la valeur tout espace de début ou de fin.

Par ailleurs, la variable *param2* peut être utilisée pour spécifier les valeurs *xref*, *historique*, *doublons* pour ouvrir la Vue Données avec les écrans **Références croisées**, **Historique** ou **Recherche des doublons**.

Exemples :

```
http://<host>[:<port>]/bdd/?deeplink=openrecord;dv;test/Customer;rowid:268
http://<host>[:<port>]/bdd/?deeplink=openrecord;dv;test/Customer;
systemName:SFA,sourceKey:CST1160
http://<host>[:<port>]/bdd/?deeplink=openrecord;dv;test/Customer;rowid:268;xref
```

Les enregistrements fusionnés représentent un cas particulier. Si vous fusionnez un enregistrement avec un autre, les enregistrements fusionnés sont dotés du rowid de l'enregistrement qui est encore fonctionnel. Toutefois, vous pouvez continuer à utiliser une URL de signet qui fait référence au rowid qui n'est plus fonctionnel. Dans ce cas, l'URL est redirigée vers le rowid de l'enregistrement fusionné. Par exemple, admettons que vous fusionniez deux enregistrements dotés des rowids 1 et 2 et que l'enregistrement fusionné soit doté du rowid 1. Si vous utilisez une URL de signet et spécifiez le rowid 2, le lien est redirigé et récupère l'enregistrement fusionné doté du rowid 1.

Vue de hiérarchie

L'opération *openrecord;hm* est utilisée pour ouvrir une Vue de hiérarchie.

L'élément *subjectAreaID* identifie le domaine, et *param1* identifie l'enregistrement. L'utilisation de ces paramètres est la même qu'avec les paramètres de la Vue des données.

Exemples :

```
http://<host>[:<port>]/bdd/?deeplink=openrecord;hm;test/Customer;rowid:268
http://<host>[:<port>]/bdd/?deeplink=openrecord;hm;test/Customer;
systemName:SFA,sourceKey:CST1160
```

Tâche

L'opération *opentask* est utilisée pour ouvrir une tâche.

subjectAreaID identifie la zone de sujet et *param1* identifie la tâche, il s'agit simplement de la valeur de ROWID_TASK pour la tâche.

Exemple :

```
http://<host>[:<port>]/bdd/?deeplink=opentask;test/Customer;3162
```

Recherche

L'opération de *recherche* est utilisée pour ouvrir un onglet de recherche et exécuter une recherche.

L'élément *subjectAreaID* identifie la zone de sujet, et *param1* définit les champs et les valeurs sur le formulaire de recherche. Utilisez la commande Afficher le signet pour voir des exemples de *param1*.

CHAPITRE 3

Processus d'implémentation

Ce chapitre comprend les rubriques suivantes :

- Présentation de processus d'implémentation, 31
- Avant de commencer, 31
- Processus de configuration , 32

Présentation de processus d'implémentation

Cette section décrit le processus de niveau élevé recommandé pour la configuration des applications IDD.

Ce processus doit être utilisé comme modèle pour la création de plans d'implémentation IDD. L'objectif principal est de souligner les étapes du cycle de création/test qui fourniraient un modèle efficace pour un déploiement rapide d'IDD. Une telle approche permet d'utiliser les étapes intermédiaires du processus de configuration pour obtenir plus de réactions et valider les exigences auprès du client.

Avant de commencer

Cette section suppose les conditions préalables suivantes :

- Informatica MDM Hub, les adaptateurs de nettoyage et Serveurs de processus sont déjà configurés et opérationnels dans votre environnement. Pour en savoir plus, consultez le *Guide d'installation d'Informatica MDM Hub*.
- Les schémas d'ORS sont configurés et contiennent des données de test. La configuration de l'application IDD nécessite l'utilisation du gestionnaire de configuration IDD et de la Console Hub. La Console Hub est utilisée pour créer les éléments de configuration requis dans l'ORS cible (tels que les objets de base, packages, recherches, composants du chemin de correspondance, etc.).
- Tous les objets de base (et les métadonnées associées) requis pour une application IDD doivent être configurés comme SECURE dans l'outil Ressources sécurisées de la Console Hub.
- La configuration et le test initial doivent être réalisés avec un compte utilisateur Informatica MDM Hub avec des privilèges illimités pour les schémas d'ORS cibles. Vous pouvez utiliser le compte admin ou tout autre compte configuré avec tous les privilèges pour le groupe ALL_GLOBAL_RESOURCES.

  Remarque: ALL_GLOBAL_RESOURCES n'inclut pas les ressources personnalisées ajoutées dans l'application IDD, qui doivent être configurées individuellement.

- L'analyse et la modélisation des données pour définir les domaines et les règles d'entreprise ont été terminées.
- Si vous voulez prendre en charge les flux de travail, dans le MDM Hub, vous devez activer la gestion d'état sur l'objet de base cible des tables et décider de l'outil BPM à utiliser pour votre moteur de flux de travail. Vous devrez peut-être effectuer les étapes d'intégration pour les outils BPM autonomes. Pour plus d'informations, consultez le *Guide de configuration d'Informatica MDM Multidomain Edition*.
- Les autres zones du Stockage Hub doivent être configurées :
  - Sécurité
  - Fonctions de nettoyage (si elles sont utilisées pour contrôler les données IDD entrées par l'utilisateur dans une application IDD)
  - Gestionnaire de hiérarchies (s'il est utilisé dans une application IDD).

    Remarque: Si vous activez la gestion d'état sur n'importe quelle table de relation ou d'entité Gestionnaire de hiérarchies, vous devez également activer cette fonctionnalité sur toutes les autres.

Pour plus d'informations sur les outils de la console Hub, consultez l'aide en ligne de la console Admin ou le *Guide de configuration d'Informatica MDM Multidomain Edition*.

Processus de configuration

Suivez les processus de configuration pour apporter des modifications de configuration à Informatica Data Director.

Le processus de configuration est un processus itératif qui n'est pas une procédure linéaire ou unique. Vous pouvez gérer la plupart des configurations de l'application IDD directement dans le gestionnaire de configuration d'Informatica Data Director. Certaines étapes du processus de configuration requièrent l'édition manuelle des composants de l'application IDD.

Si vous avez modifié les métadonnées dans le stockage de référence opérationnelle, cliquez sur **Effacer le cache** pour obtenir les dernières métadonnées de MDM Hub.

Remarque: Ne déployez pas IDD lors de l'exécution d'une tâche de lots de chargement MDM Hub ou pendant qu'un autre utilisateur effectue des modifications dans la console MDM Hub. Si vous déployez IDD lors de ces activités de MDM Hub, IDD génère des erreurs de validation du stockage de référence opérationnelle.

Liens connexes :

- "Gestionnaire de configuration IDD" à la page 41

Étape 1. Création de l'application IDD

Créez l'application IDD dans le gestionnaire de configuration IDD

1. Pour les instances IDD qui portent sur plusieurs bases de données ORS, vous pouvez créer des domaines depuis différents ORS, mais le domaine enfant d'un domaine doit être du même ORS ; créez les domaines individuels séparément pour chaque ORS (dans des applications IDD séparées).
2. Exportez la configuration.
3. Intégrez les fichiers de configuration XML individuels en les fusionnant pour créer une instance IDD multi-ORS.

Envisagez les questions de configuration suivantes :

Considération	Description
Système source de l'application	La propriété la plus importante définie au niveau de l'application IDD est le système source utilisé par une application IDD pour suivre les mises à jour réalisées dans l'application IDD elle-même (telles que les éditions réalisées par les utilisateurs de l'application IDD dans une vue des données). Le système Admin est utilisé par défaut. En utilisant l'outil Systèmes et approbation dans la console Hub, vous pouvez créer un système source de l'application. Pour configurer l'approbation sur des colonnes d'objet de base d'un autre système, vous devez créer une table temporaire factice et la mapper au système source IDD. Quel que soit le système source de l'application IDD que vous utilisez, il doit être configuré pour avoir le plus haut niveau d'approbation pour garantir que les modifications appliquées par les utilisateurs de l'application IDD écrasent toute autre valeur utilisée et se terminent sur la MVV (enregistrement maître). Si ce n'est pas le cas, les résultats d'une mise à jour seront particulièrement sujets à confusion pour les utilisateurs de l'application IDD.
Configuration du gestionnaire de hiérarchies	Si vous prévoyez d'utiliser la fonctionnalité gestionnaire de hiérarchies d'IDD, vous devez définir le profil du gestionnaire de hiérarchies (à l'aide de l'outil Hiérarchies dans la Console Hub) qui sera utilisé pour configurer la fonctionnalité gestionnaire de hiérarchies IDD. La configuration du gestionnaire de hiérarchies doit être spécifiée dès le départ pour garantir que les définitions des domaines sont cohérentes avec les définitions de l'entité Gestionnaire de hiérarchies.

Étape 2. Configuration des groupes de domaines

Configurez les groupes de domaines.

- Utilisez le gestionnaire de configuration IDD pour créer tout groupe de domaines nécessaire.

  Par exemple, vous pouvez créer un groupe de domaines Client pour contenir deux domaines : Personne et Organisation.

Étape 3. Configuration des domaines

Configurez des domaines.

- Si le groupe de domaines contient plusieurs domaines, identifiez l'attribut de données de l'objet racine du domaine qui sera utilisé pour différencier les domaines.

  Par exemple, un attribut party_type distinguerait les entités de parties par type.

Étape 3.1 Configuration des zones de sujet dans la Console Hub

Configurez les zones de sujet dans la Console Hub.

1. Dans le gestionnaire de schéma, contrôlez les composants du chemin de correspondance configurés pour l'objet racine de la zone de sujet et vérifiez qu'il existe des chemins de correspondance pour chaque objet enfant à inclure dans la zone de sujet et pour les objets liés à utiliser dans les recherches.
2. Dans l'outil Packages, créez le package d'affichage de recherche qui sera utilisé pour afficher les résultats de recherche pour la zone de sujet. Ce package a pour table principale l'objet racine de la zone de sujet.

3. Dans le gestionnaire de schéma, contrôlez les dépendances des recherches de la zone de sujet.

Mécanisme de recherche	Description
Tables de recherche de code	Les tables de recherche de code doivent avoir l'indicateur de recherche défini comme TRUE (coché) dans les propriétés de l'objet de base du gestionnaire de schéma.
Recherches d'entités	Les recherches d'entités peuvent uniquement être spécifiées sur les entités configurées comme zones de sujet. Cela peut introduire des dépendances complexes entre les zones de sujet. Dans le cadre du développement itératif d'une application IDD, vous pouvez exclure les recherches d'entités de la configuration IDD initiale s'il existe des dépendances avec d'autres zones de sujet qui n'ont pas été configurées. Les champs de recherche peuvent être ajoutés une fois toutes les dépendances de zones de sujet satisfaites.

Étape 3.2 Configuration des domaines dans le gestionnaire de configuration IDD

Configurez les domaines dans le gestionnaire de configuration IDD.

1. Créez la configuration du domaine de base et testez-la en validant et en déployant l'application.

   Cette configuration inclut la définition de la mise en page (colonnes à afficher avec la taille et le type de champ pour chacun - il s'agit du minimum à configurer), les paramètres de correspondance utilisés pour les contrôles de doublons, la configuration de toute fonction de nettoyage à utiliser pour contrôler les données entrées par les utilisateurs de l'application IDD (utilisée pour le nettoyage et/ou la validation des données), la configuration du libellé du domaine et les affectations de tâches des domaines.

2. Ajoutez les enfants et petits-enfants au domaine.

   Tous les enfants et petits-enfants doivent avoir un chemin de correspondance configuré correctement vers l'objet racine du domaine (configuré dans le volet Faire correspondre/Fusionner les détails de configuration dans le gestionnaire de schéma). Lors de la création d'un nouvel enfant, le gestionnaire de configuration IDD affiche les noms des composants du chemin de correspondance plutôt que les noms des objets enfants.

   Seuls les composants du chemin de correspondance appropriés pour le type d'enfant sont affichés. Cette configuration inclut la définition de la mise en page (colonnes à afficher avec la taille et le type de champ pour chacun) et la configuration d'une fonction de nettoyage (facultative) à appliquer à l'enregistrement (utilisée pour le nettoyage et/ou la validation).

Conseil pour l'ajout d'enfants et petits-enfants

Pour simplifier le dépannage des problèmes de configuration des enfants et petits-enfants, envisagez de les ajouter un par un, puis de déployer/tester la configuration après chaque ajout (avant d'ajouter le suivant) pour isoler tout problème de configuration qui peut survenir de manière incrémentielle.

Configuration de la mise en page

La configuration de la mise en page est utilisée pour :

- Spécifier quels champs afficher depuis l'objet de base.
- Spécifier le nombre de colonnes pour les mises en page de formulaires.
- Spécifiez le format de date et heure.
- Spécifier la taille de tous les champs de l'IU (petit, moyen, grand).
- Spécifiez les champs requis - ceux qui ne peuvent pas avoir une valeur NULL (ceci est configuré dans le fichier de configuration IDD)

- Spécifiez quels champs afficher comme liens hypertextes.

  Remarque: Seul le type de données de colonne Chaîne défini dans la console Hub peut être marqué avec **Afficher comme hypertexte** dans le gestionnaire de configuration IDD. Seuls les champs avec une URL ou une adresse électronique valide seront analysés comme liens hypertextes.

Étape 3.3 Validation, déploiement et test des modifications

Dans l'application IDD, validez, déployez et testez les modifications.

1. Créez une requête pour une nouvelle recherche.
2. Vérifiez que tous les attributs appropriés sont disponibles (attributs définis dans les mises en page des objets racine et enfants).
3. Ajoutez une nouvelle entité (enregistrement) à une zone de sujet.
   a. Validez que tous les enfants peuvent être créés et que tous les champs apparaissent dans l'ordre prévu.
   b. Validez que tous les champs de recherche apparaissent correctement et ont les listes de valeurs correctes. Si des champs n'affichent pas les commandes de recherche, vous devez ajuster la configuration du champ de recherche (définissez l'indicateur de recherche comme TRUE dans le gestionnaire de schéma).

Étape 3.4 Configuration d'autres onglets enfants

Pour configurer d'autres onglets enfants du domaine, mettez à jour le fichier de configuration d'Informatica Data Director.

Vous pouvez configurer les onglets enfants des domaines **Objet principal appartenant à** et **XREF**.

Étape 4. Configuration du nettoyage et de la validation

La validation et le nettoyage sont des éléments facultatifs pour un primaryObject, one2ManyChild et many2ManyChild.

Le gestionnaire de configuration IDD ne crée pas l'élément cleanseFunction, mais lie uniquement la fonction de nettoyage aux colonnes dans l'objet de base.

Les données que l'utilisateur de l'application IDD a saisies dans les attributs de domaine sont intégrés comme entrées dans la fonction de nettoyage. L'enregistrement de l'objet de base est ensuite mis à jour par les sorties provenant de la fonction de nettoyage.

La fonction de nettoyage peut signaler des erreurs de validation si elle est configurée avec une sortie validationStatus. Si des erreurs de validation sont trouvées, l'application IDD affiche alors les erreurs à côté des champs ayant des problèmes.

1. Créez la bibliothèque de fonctions de validation comme modèle à l'aide de l'échantillon ValidationCleanseLib dans le Kit de ressources Informatica MDM Hub.
2. Utilisez l'outil Fonctions de nettoyage de la Console Hub pour déployer dans l'ORS la bibliothèque de nettoyage créée.
3. Utilisez les Fonctions de nettoyage et les outils Mappages de la Console Hub pour créer des fonctions de nettoyage et des correspondances à utiliser dans les applications IDD.
4. Utilisez le gestionnaire de configuration pour configurer ces fonctions pour leur utilisation dans une application IDD (dans la boîte de dialogue Édition du domaine).
5. Déployez et testez les fonctions de nettoyage et de validation. Vérifiez que tous les champs sont nettoyés et validés correctement.

Étape 5. Configuration de la recherche

La configuration de la recherche implique les recherches de base et étendue, ainsi que les requêtes publiques.

La recherche avancée est préconfigurée et ne comporte pas de paramètre éditable.

Étape 5.1 Configuration de la recherche de base

La recherche de base permet aux utilisateurs de l'application IDD de rechercher des instances de domaine via la création de requêtes dans le domaine.

Les résultats sont affichés à l'aide d'un package MDM Hub créé dans l'outil Packages de la console Hub. IDD utilise le nouveau mode de l'API **SearchQuery** pour afficher les résultats.

Le package de recherche doit respecter les critères suivants :

- Il est basé sur l'objet de base racine du domaine.
- Il renvoie une seule ligne de résultat pour chaque entité de domaine.
- Il contient le ROWID_OBJECT de l'objet de base racine du domaine.

Le package utilisé pour la recherche doit contenir les colonnes requises pour présenter les résultats de la recherche à l'utilisateur. Une application IDD effectue directement la recherche sur un objet de base racine et les enfants qui lui sont associés. Elle ne recherche pas dans les attributs du package d'affichage.

IDD ne supprime pas les doublons des résultats de recherche. Un package doit être construit pour renvoyer une ligne unique pour chaque entité trouvée.

1. Pour garantir qu'un package de recherche renvoie une ligne unique pour chaque entité, testez directement le package de recherche via SQL. Une méthode de test consiste à exécuter des vérifications ponctuelles sur les entités avec un nombre connu d'enfants de types différents.
2. Identifiez les attributs principaux pouvant être recherchés. Dans le gestionnaire de schéma, créez les index personnalisés appropriés pour prendre en charge ces recherches.
3. Pour tester les recherches, créez les différents types de requêtes et exécutez-les dans une application IDD. Utilisez différentes combinaisons de critères de recherche pour garantir les performances satisfaisantes de ces recherches.
4. Par ailleurs, la recherche peut être configurée pour les objets qui ne font pas partie du domaine lorsque vous utilisez l'onglet Recherche par enfant dans la configuration de la recherche. Cela vous permet de rechercher sur tout objet pour lequel il existe un chemin de correspondance depuis l'objet principal. Ces objets seront disponibles dans le Générateur de requêtes.

   La recherche par enfant vous permet de rechercher les types de données suivants :

   - Données associées qui ne font pas partie du domaine.
   - Références croisées de données dans le domaine.
   - En général, toute donnée pouvant être liée à l'objet principal par un chemin de correspondance.

Étape 5.2 Configuration de la recherche étendue

La recherche étendue utilise l'API searchMatch pour demander des recherches approximatives parmi les données.

1. Vous devez vous assurer que toutes les colonnes de correspondance requises ont été créées. Aucune configuration supplémentaire n'est requise dans une application IDD pour permettre la recherche approximative. IDD mappe automatiquement les critères de recherche fournis par l'utilisateur de l'application IDD dans les colonnes de correspondance disponibles, puis exécute la recherche.

2. Avant de tester la configuration de la recherche étendue, vérifiez que les données ont bien été traitées comme jetons, puis testez les fonctions de recherche approximative en créant les requêtes de recherche pour inclure les attributs de domaine avec des colonnes de correspondance sous-jacentes.

   Pour plus d'informations, voir « Configuration du processus de correspondance » dans le *Guide de configuration d'Informatica MDM Multidomain Edition* ou l'aide en ligne de la Console Hub, ainsi que la description de l'API searchMatch dans le *Guide de Framework d'intégration des services d'Informatica MDM Hub* ou dans le Javadoc.

3. La recherche étendue utilise l'API **searchMatch** avec matchType=NONE. Dans la configuration par défaut, toutes les colonnes de correspondance possibles sont générées à chaque requête searchMatch. IDD peut être configuré pour générer uniquement des colonnes de correspondance spécifiques. Dans l'onglet Recherche dans la boîte de dialogue du domaine, vous pouvez spécifier l'ensemble spécifique de colonnes de correspondance qui doit être généré.

   Remarque: Par défaut, dans ce mode de searchMatch, le niveau de recherche est 'Étroit'. Il s'agit du niveau le plus restrictif, mais il peut être modifié avec la configuration suivante dans cmxcleanse.properties :

   ```
   cmx.server.match.searcher_search_level=<level>
   ```

   où <*niveau*> est l'un des paramètres suivants : étroit, typique, exhaustif ou extrême. Pour plus d'informations sur les niveaux de recherche dans les propriétés des ensembles de règles de correspondance, voir « Configuration du processus de correspondance » dans le *Guide de configuration d'Informatica MDM Multidomain Edition*

Étape 5.3 Configuration des requêtes publiques

IDD permet aux administrateurs et utilisateurs experts de partager avec d'autres utilisateurs les requêtes qu'ils créent.

- Nous vous recommandons de configurer au moins une recherche utilisée le plus souvent comme publique pour chacun des domaines définies dans l'application IDD.

  Ainsi, les utilisateurs pourront naviguer rapidement parmi tous les domaines sans avoir à créer leurs propres versions de requêtes courantes.

Recherche non sensible à la casse

La Recherche étendue n'est pas sensible à la casse car elle est basée sur la capacité de correspondance d'Informatica MDM Hub.

En général, les recherches non sensibles à la casse ne sont pas disponibles pour la Recherche de base. Il existe une exception lorsque toutes les données du domaine sont déjà soit en majuscules, soit en minuscules. Dans ce scénario, l'API searchQuery peut être configurée pour convertir les termes de recherche entrants en majuscules ou en minuscules avant d'exécuter la requête. Pour plus d'informations, consultez la description de SearchQuery dans le *Guide de Framework d'intégration des services d'Informatica MDM Hub* ou le Javadoc.

Étape 6. Configurer le processus de correspondance

Configurez la manière dont le processus de correspondance identifie les enregistrements dupliqués.

Configurez le processus de correspondance dans l'onglet **Paramètres de correspondance** de la boîte de dialogue **Domaine**. Spécifiez un ensemble de règles de correspondance prédéfini et le type de correspondance. Vous pouvez également sélectionner des colonnes de correspondance.
Pour plus d'informations sur la configuration des paramètres de correspondance, consultez le *Aide en ligne sur le gestionnaire de configuration Informatica Data Director d'Informatica MDM Multidomain Edition*. Pour

plus d'informations sur les règles de correspondance et les ensembles de règles de correspondance, consultez le *Guide de configuration d'Informatica MDM Multidomain Edition*.

Étape 7. Configurer les flux de travail MDM

Vous pouvez configurer votre application Informatica Data Director (IDD) de manière à utiliser les flux de travail MDM prédéfinis qui sont déployés lorsque vous installez le ActiveVOS Server intégré.

L'étape suivante varie selon que le ActiveVOS Server est inclus dans votre environnement MDM ou non :

- Si votre environnement inclut le ActiveVOS Server, sélectionnez le flux de travail que vous souhaitez utiliser en tant que flux de travail d'approbation.
- Si votre environnement n'inclut pas le ActiveVOS Server, vous devez l'installer en utilisant le programme d'installation du serveur Hub. Pour plus d'informations, consultez le *Guide d'installation d'Informatica MDM Multidomain Edition*.

Liens connexes :

- "Flux de travail et tâches" à la page 152
- "Configuration manuelle d'IDD" à la page 62

Configuration d'un flux de travail d'approbation par défaut pour la vue Données du domaine

Lorsqu'un gestionnaire des données modifie les données principales, il peut envoyer cette mise à jour pour approbation en cliquant sur le bouton **Envoyer pour approbation**. Cette action ouvre la boîte de dialogue Créer une tâche. Le flux de travail d'approbation par défaut s'affiche dans le champ Type de tâche.

1. Dans le gestionnaire de configuration IDD, sélectionnez l'application et cliquez sur **Modifier**.
2. Cliquez sur l'onglet **Tâches**.
3. Sous Types de tâches, cliquez sur le type de tâche qui porte le nom du flux de travail d'approbation à utiliser par défaut, puis cliquez sur **Modifier**.
4. Cochez la case **Créer un type de tâche par défaut lors de l'approbation**, puis cliquez sur **OK**.

   Remarque: Si cette case est inactive, cela signifie que cette option est définie pour un autre type de tâche. Modifiez les autres types de tâches pour découvrir lequel est associé à cette option, puis décochez la case. Vous pouvez ensuite définir l'option dans le type de tâche de votre flux de travail favori.

Étape 8. Configuration de la sécurité

La sécurité des applications dans IDD est contrôlée par les règles du gestionnaire d'accès de sécurité (GAS) MDM Hub configurées dans la Console Hub.

Les comportements de l'application IDD peuvent être très sensibles à la configuration de sécurité.

1. Nous recommandons d'utiliser l'utilisateur admin (ou un utilisateur disposant de tous les privilèges sur toutes les ressources sécurisées) pour la configuration d'une application IDD et les tests fonctionnels initiaux.

   Pour plus d'informations, consultez le *Guide de sécurité d'Informatica MDM Multidomain Edition*.
2. Les filtres de sécurité au niveau des lignes peuvent être configurés pour chaque domaine. Par défaut, aucun filtre de sécurité n'est défini.

Sous l'onglet Recherche dans la boîte de dialogue du domaine, vous pouvez configurer des règles de sécurité des données.

3. Pour tout utilisateur donné d'une application IDD, il peut exister plusieurs filtres de données applicables.

   Par exemple, un utilisateur peut disposer de droits sur les enregistrements dont l'adresse correspond à l'état CA par le biais d'un rôle, et de droits sur les enregistrements dont l'adresse correspond à l'état NY par le biais d'un autre rôle.

Liens connexes :

- "Sécurité des données" à la page 127
- "Configuration de la sécurité IDD" à la page 120

Étape 9. Configurer les rapports

Une application IDD peut afficher les rapports Jaspersoft dans l'Démarrer un espace de travail.

Étape 10. Configuration des extensions de l'interface utilisateur

Configurez les extensions de l'interface utilisateur.

1. Une application IDD peut être personnalisée en intégrant un contenu externe à la page Web et en appelant des actions depuis des emplacements dans l'application IDD.

   Il est possible d'intégrer du contenu avec :

Élément	Description
Onglet de niveau supérieur	Les onglets peuvent être ajoutés aux côtés des onglets pour le Démarrer un espace de travail, les données de l'espace de travail et les tâches de l'espace de travail.
Démarrer un espace de travail	Il est possible d'ajouter un composant ou widget au Démarrer un espace de travail.
Onglet Enfant dans la vue des données	Les onglets peuvent être ajoutés comme enfants d'un domaine.

2. Des actions personnalisées peuvent être configurées afin qu'ils soient appelés depuis des options de menus à divers endroits dans une application IDD.

   Les informations contextuelles peuvent être transmises lors de l'appel de l'action externe.
   La table suivante présente des zones d'une application IDD où ces actions peuvent être configurées, avec les données contextuelles disponibles.

Zone	Données contextuelles disponibles
Domaine	rowid_object et données depuis l'objet principal
Enfant un à plusieurs	rowid_object et données depuis l'enfant

Zone	Données contextuelles disponibles
Enfant plusieurs à plusieurs	rowid_object et données depuis l'enfant
Résultats de la recherche	rowid_object des données sélectionnées dans la liste des résultats de recherche

LIENS CONNEXES :

- "Extensions de l'interface utilisateur" à la page 76

Étape 11. Localisation de l'application

Quatre ensembles de groupes de ressources contiennent les chaînes affichées dans l'application IDD.

Chaque ensemble comporte les composants suivants :

- Le fichier par défaut.
- Un fichier de langue anglaise fictif. Ce fichier peut être vide.
- Versions localisées du fichier, si nécessaire.

Par exemple, pour l'ensemble MessageBundle, on trouve le fichier par défaut MessageBundle.properties et le fichier en langue anglaise fictif MessageBundle_en.properties.

Chaque fichier de groupe de ressources est un fichier de propriétés codé UTF-8. Chaque entrée dans le fichier est une paire nom/valeur, `<nom>=<valeur>`. Exemples :

```
title=Business Data Director
locale=Locale
search=Search
```

Pour chaque entrée :

- <nom> est une valeur fixe référencée par l'application IDD et non modifiable.
- <valeur> est la partie qui peut être localisée

Pour localiser l'application :

▶ Utilisez le gestionnaire de configuration IDD pour ajouter des fichiers de groupes de ressources à une application IDD, en les incluant dans le fichier ZIP de l'application importé, ou en les important individuellement dans une application IDD existante.

LIENS CONNEXES :

- "Composants de l'application" à la page 119

CHAPITRE 4

Gestionnaire de configuration IDD

Ce chapitre comprend les rubriques suivantes :

- Présentation du gestionnaire de configuration IDD, 41
- Démarrage du gestionnaire de configuration Informatica Data Director, 42
- Page d'Accueil, 42
- Liaison ORS, 43
- Ajout d'une application IDD, 43
- Importation d'une configuration d'application IDD, 44
- Validation, état de l'application et déploiement , 44
- Édition de l'application, 47
- Package Fournisseur de connexion personnalisé, 52

Présentation du gestionnaire de configuration IDD

Le gestionnaire de configuration IDD sert à ajouter, modifier et gérer des applications IDD.

Une application IDD comporte un fichier de configuration XML, des ensembles de ressources, des fichiers d'aide et d'autres composants. Une application IDD complète peut être importée ou exportée comme fichier ZIP contenant tous ces composants.

Le gestionnaire de configuration IDD est conçu pour être utilisé pour créer et maintenir la configuration d'une application IDD. Il n'affiche pas encore toutes les options de configuration disponibles. Certaines fonctionnalités doivent être configurées manuellement en exportant et en éditant directement le fichier de configuration XML, puis en important de nouveau le fichier dans le gestionnaire de configuration IDD.

LIENS CONNEXES :

- "Composants de l'application" à la page 119
- "Configuration manuelle d'IDD" à la page 62

Démarrage du gestionnaire de configuration Informatica Data Director

Pour démarrer le gestionnaire de configuration Informatica Data Director, utilisez un navigateur Web pris en charge.

1. Ouvrez un navigateur Web pris en charge.

   Pour plus d'informations sur les navigateurs Web pris en charge, consultez la matrice de disponibilité des produits sur le portail MySupport Informatica à l'adresse https://mysupport.informatica.com/community/my-support/product-availability-matrices.

2. Dans la barre d'adresses, saisissez l'URL suivante pour accéder à la page de connexion du gestionnaire de configuration IDD :

   ```
   http://<hôte de MDM Hub>:<numéro de port>/bdd/config/
   ```

3. Entrez le nom de connexion et le mot de passe, puis cliquez sur **Connexion**.

   Vous devez vous connecter en tant qu'utilisateur disposant de tous les privilèges pour tous les objets de base. Pour plus d'informations sur la configuration des privilèges utilisateur, consultez le *Guide de sécurité d'Informatica MDM Multidomain Edition*.

Le gestionnaire de configuration Informatica Data Director démarre et la page Applications s'affiche.

Page d'Accueil

La page d'accueil IDD comporte les éléments suivants :

Élément	Description
Liste des applications	Liste des applications IDD existantes
Barre de commandes	Commandes disponibles (décrites ci-dessous)
Résumé des applications	Résumé des applications IDD existantes, y compris les propriétés suivantes : - Nom logique et nom d'affichage - État de la validation - État du déploiement - URL pour lancer l'application IDD
Types de composants	Uniquement disponible si la fonction Informatica Data Components (IDC) est sous licence pour votre implémentation d'Informatica MDM Hub. Pour plus d'informations, consultez l'aide en ligne du gestionnaire de configuration et le *Guide d'implémentation d'Informatica Data Components*.
Paramètres du fournisseur de connexion	Raccourci vers l'écran de configuration du module du fournisseur de connexion personnalisé (prise en charge de la connexion unique).

La barre de commandes IDD contient les commandes suivantes :

Commande	Description
Ajouter	Ajout d'une nouvelle application IDD.
Éditer	Édition de la configuration de l'application IDD sélectionnée.
Supprimer	Suppression de l'application IDD sélectionnée.
Exporter	Exportation d'une configuration d'application IDD (fichier ZIP).
Valider	Validation de l'application IDD sélectionnée.
État de l'application	Modifiez l'état de déploiement de l'application IDD : complet, limité ou non déployé.
Importer	Importation d'une configuration d'application IDD (voir les formats ci-dessous).
Redéployer	Suppression et redéploiement d'une application IDD.
Effacer le cache	Efface le cache IDD local pour l'application IDD sélectionnée. Ce cache conserve les métadonnées Hub et doit être effacé si les métadonnées ont subi des modifications.

L'aide en ligne est également disponible depuis toute page du gestionnaire de configuration.

Liaison ORS

Une configuration d'application IDD déclare une ou plusieurs bases de données d'ORS logique.

Une *base de données d'ORS logique* est un pointeur de configuration IDD vers une base de données d'ORS physique dans le Stockage Hub configuré dans la Console Hub. Tous les objets Informatica MDM Hub référencés dans une configuration le sont toujours dans un contexte d'ORS logique spécifique. Pour qu'une configuration de IDD soit valide, les objets qu'elle référence doivent exister dans l'ORS physique associé.

Lorsqu'une application IDD est ajoutée ou importée, les bases de données ORS logiques qu'elle déclare doivent être liées à un ORS physique enregistré auprès d'Informatica MDM Hub.

La liaison ORS est utilisée pour connecter une application IDD à un ORS et pour valider la configuration. La liaison ORS est également utilisée par le gestionnaire de configuration IDD pour obtenir des métadonnées concernant l'ORS.

Ajout d'une application IDD

La commande Ajouter permet de créer une nouvelle application IDD.

Une nouvelle application IDD est définie par son nom, son nom d'affichage, sa description et la liste des bases de données d'ORS logiques. Après l'ajout de l'application, choisissez la commande Éditer pour apporter des modifications plus détaillées à la configuration de l'application (comme l'ajout de domaines).

Importation d'une configuration d'application IDD

La commande importer permet de créer ou de mettre à jour une application IDD.

Elle fournit les trois options d'importation suivantes : deux pour l'importation d'une application complète et une pour l'importation d'un composant dans une application existante :

Option d'importation	Description
Importer la configuration IDD uniquement (XML)	Créez une application IDD en important le fichier XML de configuration IDD. Ceci peut permettre de remplacer une application IDD existante du même nom. Si c'est le cas, l'application existante est entièrement remplacée (comme si vous aviez effectué une suppression suivie d'une importation). Si une application du nom de la nouvelle application existe déjà, vous pouvez choisir d'importer l'application sous un nom différent. **Remarque:** Si vous remplacez une application IDD, vous devez reconfigurer les **privilèges de ressource** attribués à tous les rôles dans la console Hub.
Importer l'application IDD complète (ZIP)	Créez une application IDD en important un fichier .zip contenant les différents fichiers de composants, tels que fichiers XML, les ensembles de ressources et les fichiers d'aide. La taille maximale du fichier .zip que vous pouvez importer est de 20 mégaoctets. Dans les environnements IBM DB2, pour importer un fichier supérieur à 1 mégaoctet, exécutez la commande suivante afin de définir la taille maximale de fichier autorisée : `ALTER TABLE CMX_SYSTEM.C_REPOS_DS_CONFIG ALTER COLUMN BLOB_DATA SET DATA TYPE BLOB(`*`taille maximale`*`, octets);` **Remarque:** Si vous remplacez une application IDD, vous devez reconfigurer les **privilèges de ressource** attribués à tous les rôles dans la console Hub.
Importer dans l'application IDD existante	Mettez à jour une application IDD existante en important un fichier individuel. Ceci permet d'ajouter ou de remplacer les fichiers de composants de l'application IDD. **Remarque:** Vous pouvez également utiliser cette option lors de la promotion des modifications d'un environnement à un autre.

LIENS CONNEXES :

- "Composants de l'application" à la page 119

Validation, état de l'application et déploiement

Les paramètres maintenus suivants déterminent comment et si l'application IDD est déployée.

Paramètre	Description
valid_ind	Contient l'état de validation le plus récent pour l'application. L'état de validation est une valeur unique qui représente l'erreur la plus grave trouvée.
active_ind	Géré directement par l'utilisateur pour refléter l'intention de déploiement de l'application.

Validation

Une configuration d'application IDD est étroitement liée aux métadonnées dans un ORS.

La configuration contient des références aux objets dans un ORS. Les modifications effectuées dans un ORS (l'ajout, la modification ou le retrait des objets de base, des colonnes, des fonctions de nettoyage, etc.) ne sont pas automatiquement appliquées dans la configuration IDD. Pour cette raison, le processus de validation IDD est nécessaire et doit être répété périodiquement.

La validation est exécutée dans les cas suivants :

- en cas de demande par l'utilisateur dans le gestionnaire de configuration IDD
- en cas d'importation d'une configuration IDD
- avant de déployer une application au démarrage du serveur d'applications

Les niveaux de validation suivants sont disponibles.

valid_ind	Niveau de validation	Description
-1	Non validé	L'application IDD n'a pas été validée.
0	Aucune erreur	Aucun avertissement ni erreur n'a été trouvé lors de la validation.
1	Information	Fournit des informations à l'utilisateur. Aucune modification de configuration n'est requise.
2	Avertissement	Il se peut qu'une configuration nécessite un changement, mais elle ne doit entraîner aucun problème d'exécution.
3	Erreur	Une erreur de configuration doit être corrigée. Des problèmes d'exécution sont prévus.
4	Erreur critique	Identique à Erreur, mais indique un problème qui nécessite une intervention en urgence.
5	Erreur irrécupérable	Une erreur qui empêche l'exécution de l'application IDD. L'application ne sera pas déployée dans ces circonstances.

État de l'application

L'état de l'application est contrôlé par l'utilisateur dans le gestionnaire de configuration IDD.

Il stocke le déploiement prévu pour l'application IDD.

Remarque: Une application IDD peut être déployée même si la configuration contient des erreurs. Seules des erreurs irrécupérables (décrites dans la section précédente) empêchent le déploiement d'une application IDD. Ceci peut être utile pour déployer une application IDD qui contient des erreurs lors de la génération d'une

application, ce qui permet à l'implémenteur de tester des parties de la configuration tandis que d'autres sont incomplètes.

active_ind	Nom	Description
-1	Non déployé	L'application IDD n'est pas déployée. Utile quand l'application est en développement. Des modifications peuvent être effectuées et enregistrées sans temps système supplémentaire de déploiement de l'application.
0	Déploiement limité	L'application IDD est déployée, mais seuls les utilisateurs qui sont administrateurs peuvent se connecter. L'application ne s'affiche pas dans la liste des applications disponibles. Vous devez accéder à l'application à l'aide de son URL complète : `http://<hostname>[:<port>]/bdd?bdd_name=name`
1	Déploiement complet	L'application IDD est déployée pour une utilisation complète. Elle apparaît dans la liste des applications et tout utilisateur autorisé peut exécuter l'application.

Déploiement

Le déploiement est le processus d'utilisation d'une configuration IDD et de sa mise à disposition comme application.

Aucune application n'est déployée si active_ind est -1 pour cette application.

Le déploiement se produit en réponse aux événements suivants :

Événement	Description
Démarrage du serveur d'applications	Toutes les applications IDD avec active_ind différent de -1 sont validées au départ. Si le niveau de validation n'est pas Erreur irrécupérable, l'application IDD est déployée. À ce stade, seule une validation partielle est exécutée pour vérifier les erreurs irrécupérables.
Importer / Enregistrer	À chaque importation ou enregistrement d'une application IDD, elle est également déployée, sauf si son active_ind est -1.
Redéploiement	L'utilisateur redéploye une application IDD.

Édition de l'application

Dans l'écran Éditer l'application, vous pouvez afficher et modifier les détails de configuration d'une application IDD sélectionnée. IDD utilise les métadonnées de l'ORS logique pour présenter les options de configuration disponibles.

Les onglets suivants sont disponibles en bas de l'écran :

Onglet	Description
Domaines	Définit les groupes de domaines, domaines, enfants de domaines et petits-enfants de domaines de l'application IDD sélectionnée.
Tâches	Définit les tâches de l'application IDD sélectionnée. Pour plus d'informations, consultez l'aide en ligne du gestionnaire de configuration.
Contrôles	Disponible uniquement si votre implémentation d'Informatica MDM Hub dispose d'une licence pour la fonctionnalité Composants de données Informatica (IDC). Pour plus d'informations, consultez l'aide en ligne du gestionnaire de configuration et le *Guide d'implémentation de la fonction Composants de données Informatica*.

Les boutons de commande suivants sont également disponibles :

Bouton	Description
Enregistrer	Enregistre les dernières modifications apportées à la base de données. Si l'état de l'application n'est pas Non déployé (-1), l'application IDD est redéployée après l'enregistrement des modifications.
Valider	Exécute la validation dans la configuration actuelle de l'application IDD et affiche le rapport de validation.
Lier	Permet de changer la liaison ORS logique.
Générer le schéma d'entité commerciale	Génère des fichiers de configuration pour toutes les entités commerciales de l'application IDD.

Liens connexes :

- "Domaines" à la page 48

Bases de données ORS logiques

Lors de l'édition d'une configuration, la première tâche à accomplir est la configuration des bases de données d'ORS logiques.

Pour chacune de ces bases de données d'ORS, vous devez sélectionner un système source.

Si le gestionnaire de hiérarchies doit être utilisé par l'application IDD, la configuration celui-ci doit également être sélectionnée. L'icône à droite de la liste déroulante Configuration du gestionnaire de hiérarchies est utilisée pour les paramètres supplémentaires du gestionnaire de hiérarchies (tels que les sauts et paramètres de relations).

Remarque: Dans le gestionnaire de configuration IDD, dans la fenêtre **Paramètres du gestionnaire de hiérarchies**, la valeur de **Total des relations** ne doit pas excéder 2000.

Délai d'expiration de session

Dans l'écran Éditer l'application, vous pouvez définir un délai d'expiration de session pour une application IDD sélectionnée.

Pour définir le délai d'expiration de session, entrez une valeur en minutes dans le champ **Dépassement de délai de la session**. Enregistrez ensuite l'application IDD. Par défaut, une session expire après 30 minutes.

Si vous modifiez le délai d'expiration de session, toutes les sessions actives dans IDD deviennent non valides et les utilisateurs doivent se reconnecter.

Domaines

L'onglet Domaines dans la partie inférieure de l'écran propose une arborescence, qui indique comment l'application IDD est configurée.

Lorsque des éléments sont sélectionnés dans l'arborescence, les boutons Ajouter, Éditer et Supprimer sont mis à jour pour refléter les options disponibles. Les niveaux dans l'arborescence sont :

Niveau de l'arborescence	Description
Application IDD	Des groupes de domaines peuvent être ajoutés.
Groupe de domaines	Le groupe de domaines peut être édité ou supprimé. Des domaines peuvent être ajoutées. Le groupe de domaines identifie l'ORS logique auquel appartiennent les domaines enfant, et quel objet de base est la table principale pour ces domaines. Le groupe de domaines peut comporter un ou plusieurs domaines enfants, partageant toutes la même table principale. Ces domaines sont regroupés dans l'application IDD.
Domaine	Le domaine peut être édité ou supprimé. Des enfants de domaines peuvent être ajoutés. Si le groupe de domaines contient plusieurs domaines, chacun définit le type d'entité du gestionnaire de hiérarchies ou le qualificateur de sous-type qui identifie le domaine. Vous indiquez également : - le package utilisé pour afficher les résultats de la recherche - l'ensemble de règles de correspondance et le type de correspondance utilisés pour les contrôles de doublons - les colonnes de la table primaire qui font partie de ce domaine
Enfant de domaine	L'enfant du domaine peut être édité ou supprimé. Pour chaque enfant du domaine, vous devez spécifier : - le type de relations (un à plusieurs, plusieurs à plusieurs, etc.) - quel chemin de correspondance mène à la table enfant (la liste des chemins de correspondance est remplie selon la sélection du type de relation) - les colonnes de la table enfant à afficher.
Petit-enfant de domaine	Le petit-enfant du domaine peut être édité ou supprimé. Pour chaque petit-enfant du domaine, vous devez spécifier : - le type de relation (un à plusieurs, plusieurs à plusieurs, etc.) - quel chemin de correspondance mène à la table enfant (la liste des chemins de correspondance est remplie selon la sélection du type de relation) - les colonnes de la table enfant à afficher.

Propriétés des groupes de domaines

La boîte de dialogue utilisée pour ajouter et éditer un groupe de domaines permet de configurer :

- Nom et nom d'affichage. Le nom est l'identifiant interne pour ce domaine, et doit comporter uniquement des caractères alphanumériques. Les caractères spéciaux ne sont pas autorisés.
- L'ORS logique du groupe de domaines est lié à
- Table primaire pour les domaines dans le groupe :

Fonction	Description
Nom et nom d'affichage	Ils sont utilisés pour identifier le groupe de domaines. Le nom est l'identifiant interne pour ce groupe de domaines, et doit comporter uniquement des caractères alphanumériques. Les caractères spéciaux ne sont pas autorisés.
ORS logique	Configure l'ORS logique d'où proviennent les objets dans ce groupe de domaines.
Table primaire	Configure quel objet de base est la table principale ou racine pour les domaines du groupe de domaines.
Recherche uniquement	Ce paramètre est sélectionné pour un groupe de domaines comportant des données créées et maintenues en dehors d'une application IDD. Les domaines définis dans ce groupe sont visibles dans une application IDD uniquement lors de la création d'une clé étrangère à partir d'un autre domaine (la recherche permet de trouver l'enregistrement à associer).

Propriétés de domaine

La boîte de dialogue utilisée pour ajouter et éditer un domaine permet de configurer les propriétés suivantes :

- Nom et nom d'affichage : le nom est l'identificateur interne de ce domaine et doit comporter uniquement des caractères alphanumériques. Les caractères spéciaux ne sont pas autorisés. Un nom de domaine ne peut pas commencer par un chiffre.
- Type d'entité de Hierarchy Manager : cette propriété définit les types d'objets pouvant, le cas échéant, être liés.
- Package d'affichage des résultats de recherche : cette propriété est utilisée pour afficher les résultats de recherche pour ce domaine. Le package doit avoir la table principale du groupe de domaines comme table principale
- Colonnes de liens Correspondances potentielles : cette propriété définit les colonnes d'une mise en page devant être affichée comme lien hypertexte et ouvrant une entité Correspondance potentielle dans un nouvel onglet Vue des données.
- Colonne de sous-type : cette propriété spécifie la colonne utilisée pour le type de sous-filtre : code de type (catégorie) pour ce domaine. Automatiquement défini si un type d'entité de Hierarchy Manager est sélectionné.
- Valeur de sous-type : cette propriété spécifie la valeur utilisée pour le type de sous-filtre. Automatiquement défini si un type d'entité du Hierarchy Manager est sélectionné.
- Nombre de colonnes gelées : cette propriété indique le nombre de colonnes gelées dans les résultats de recherche du domaine.
- Afficher référence croisée : si cette option est sélectionnée, l'application IDD affiche un onglet enfant pour le domaine qui affiche les références croisées pour l'objet principal.

- Onglets pour configurer les paramètres suivants :

Fonction	Description
Mise en page	Configure les colonnes de l'objet de base qui sont disponibles dans l'application IDD pour l'affichage et la modification, le type de composant UI qui doit être utilisé et, dans le cas d'une recherche, si les données de la recherche sont localisées.
Paramètres de correspondance	Configure l'ensemble des règles de correspondance et le type de correspondance à utiliser pour les contrôles de doublons.
Rechercher	Configure les propriétés de la recherche.
Sécurité des données	Configure la sécurité au niveau des lignes et basée sur les rôles pour le domaine.
Data Masking	Configure le masquage des données basé sur les rôles pour les colonnes sélectionnées dans l'onglet Mise en page.
Nettoyer	Configure la fonction de nettoyage à utiliser pour le nettoyage et la validation.
Libellé	Configure la méthode de génération d'un libellé pour le domaine. Ce libellé est utilisé, par exemple, comme titre d'un onglet de la vue des données.
Attribution des tâches	Configure le mode d'attribution des tâches. Spécifie la liste des rôles et l'utilisateur pour chaque type de tâche.
Ordre des enfants	Configure l'ordre des onglets enfants pour le domaine.

Propriétés des enfants et petits-enfants de domaines

La boîte de dialogue utilisée pour ajouter et éditer un domaine permet de configurer les propriétés suivantes :

- Nom et nom d'affichage. Le nom est l'identifiant interne pour un enfant ou petit-enfant de domaine, et doit comporter uniquement des caractères alphanumériques. Les caractères spéciaux ne sont pas autorisés.
- Type Enfant - le type de relation avec le parent
- Chemin de correspondance à l'enfant - le composant de chemin de correspondance qui mène à cet objet enfant
- Onglets pour configurer les paramètres suivants :

Fonction	Description
Mise en page	Configure les colonnes de l'objet de base qui sont disponibles dans l'application IDD pour l'affichage et la modification, le type de composant UI qui doit être utilisé et, dans le cas d'une recherche, si les données de la recherche sont localisées. **Remarque:** Ce paramètre n'est pas appliqué aux filtres des enregistrements enfants. Toutes les colonnes sont disponibles pour les filtres.
Masquage des données	Configure le masquage des données basé sur les rôles pour les colonnes sélectionnées dans l'onglet Mise en page.
Nettoyer	Configure les fonctions de nettoyage à utiliser pour le nettoyage et la validation.

LIENS CONNEXES :

- "Localisation de la recherche" à la page 51
- "Étape 4. Configuration du nettoyage et de la validation" à la page 35

Localisation de la recherche

Une application Informatica Data Director remplit une liste de valeurs acceptables pour les colonnes que vous configurez comme des recherches dans le gestionnaire de schéma. Pour créer des recherches localisées, vous devez disposer d'une table de localisation. Lorsque vous créez une recherche, utilisez un nom d'affichage unique. Informatica Data Director ne peut pas différencier les recherches qui disposent de codes différents, mais partagent le même nom d'affichage.

Informatica Data Director prend également en charge la localisation des valeurs d'affichage de recherche. Vous pouvez configurer les valeurs d'affichage de recherche dans l'onglet Mise en page du gestionnaire de configuration d'Informatica Data Director pour les domaines et les enfants de domaines.

Par exemple, un stockage de référence opérationnelle (Operational Reference Store - ORS) possède les tables suivantes :

- C_PARTY
- C_LU_SALUTATION
- C_LCL_SALUTATION

La table C_PARTY possède un code de recherche de salutation configuré dans la table C_LU_SALUTATION. Pour chaque code de salutation, le nom d'affichage peut posséder une valeur localisée configurée dans la table C_LCL_SALUTATION.

Pour générer la liste de valeurs pour les paramètres régionaux d'un utilisateur spécifique, Informatica Data Director recherche d'abord un nom de recherche dans C_LCL_SALUTATION en fonction des paramètres régionaux spécifiés. S'il ne trouve pas de nom de recherche dans C_LCL_SALUTATION, il utilise le nom de recherche disponible dans la table de recherche SALUTATION_DISP.

Remarque: les codes de langue et de pays déterminent les paramètres régionaux. Les valeurs des codes de langue et de pays sont des codes ISO à deux lettres.

Dans le cadre du scénario précédent, la configuration spécifie que la colonne possède des valeurs de recherche localisées et indique la table et les colonnes utilisées. L'exemple de code XML suivant montre la configuration correspondant à l'exemple précédent :

```
<column columnUid="C_PARTY|SALUTATION_CODE"
        editStyle="FIELD"
        horizontalStyle="SMALL">
  <columnI18NLookup languageCdUid="C_LCL_SALUTATION|LANGUAGE_CODE"
                    countryCdUid="C_LCL_SALUTATION|COUNTRY_CODE"
                    lookupFKUid="C_LCL_SALUTATION|SALUTATION_CODE"
                    localizedNameUid="C_LCL_SALUTATION|LOCALIZED_STRING"/>
</column>
```

LIENS CONNEXES :

- "Tables de recherche" à la page 26
- "Codes de paramètres régionaux" à la page 171
- "Configuration manuelle d'IDD" à la page 62

Importer un modèle d'importation de données

Un développeur d'applications Informatica Data Director (IDD) peut configurer une application IDD de façon à autoriser les utilisateurs à importer des données depuis un fichier source. Le gestionnaire de données crée un modèle d'importation de données que vous importez dans la configuration de l'application IDD.

Remarque: L'importation de données est disponible pour les applications IDD qui implémentent le modèle de données de domaine et les vues IDD héritées.

Pour plus d'informations sur l'importation de données, consultez le *Guide de l'utilisateur Informatica Data Director d'Informatica MDM Multidomain Edition*.

Importation du modèle d'importation de données

Dans le gestionnaire de configuration IDD, un développeur d'application IDD importe le modèle d'importation de données dans l'application IDD. Le processus d'importation valide le modèle.

1. Connectez-vous au Gestionnaire de configuration IDD.
2. Sélectionnez l'application IDD.
3. Cliquez sur **Importer** > **Importer dans l'application IDD existante**.

   La fenêtre **Importer dans l'application IDD existante** s'ouvre.
4. Dans la liste **Type de configuration**, sélectionnez **Modèle d'importation de données**.
5. Cliquez sur **Parcourir** et sélectionnez le fichier XML qui contient le modèle d'importation de données.
6. Cliquez sur **Importer**.

   Le processus d'importation valide le modèle. La fenêtre **Résultat de validation** s'ouvre et affiche les erreurs éventuelles.
7. En cas d'erreurs de validation, corrigez-les dans le modèle puis réimportez-le.
8. Dans la fenêtre **Résultat de validation**, cliquez sur **OK**.

Package Fournisseur de connexion personnalisé

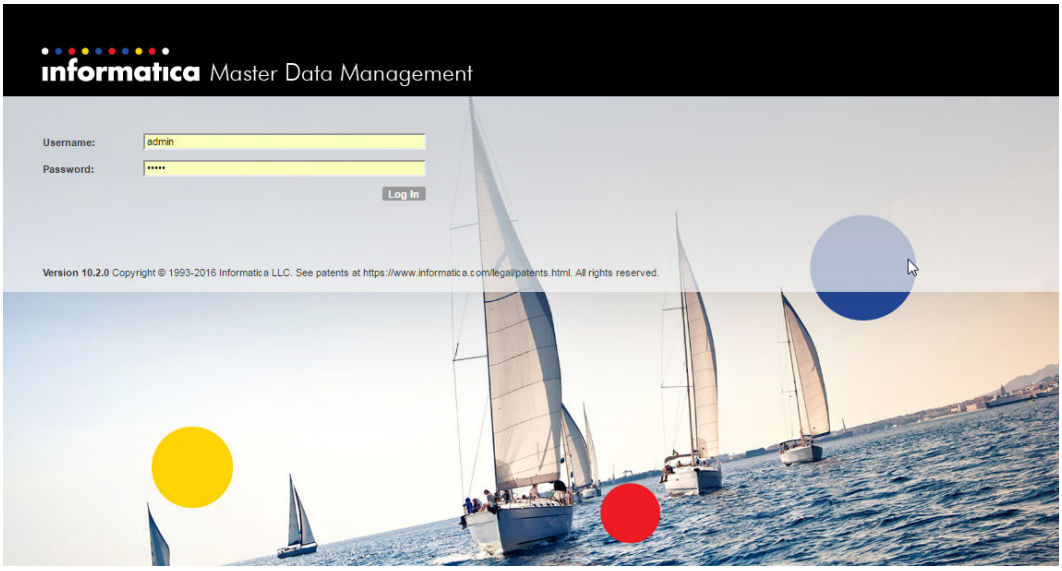
Le package Fournisseur de connexion personnalisé est un fichier d'archive contenant les classes Java. Vous pouvez utiliser le gestionnaire de configuration Informatica Data Director pour charger le fichier d'archive. Le package Fournisseur de connexion personnalisé doit se trouver dans un fichier ZIP.

Dans le framework Entity 360, le package Fournisseur de connexion personnalisé doit se trouver dans un fichier ZIP contenant les éléments suivants :

- Dossier META_INF. Ce dossier contient un fichier MANICFEST.MF dont l'entrée Connexion-Fournisseur-Classe-Nom contient un nom de classe qui implémente l'interface LoginProvider.
- Fichier JAR contenant l'implémentation Fournisseur de connexion personnalisé.
- Autres fichiers JAR contenant des dépendances de l'implémentation Fournisseur de connexion personnalisé, notamment les classes d'utilitaire, la journalisation et les bibliothèques tierces.

Vous pouvez configurer le package Fournisseur de connexion personnalisé de façon à utiliser le formulaire de connexion Informatica Data Director ou le formulaire de connexion d'un fournisseur d'identité externe tel que Google ou Salesforce.

L'image suivante montre le formulaire de connexion Informatica Data Director :



Si vous ne chargez pas de package Fournisseur de connexion personnalisé, l'implémentation Informatica Data Director authentifie les utilisateurs en fonction des justificatifs d'identité stockés dans la base de données principale MDM Hub.

Packages Fournisseur de connexion personnalisé du kit de ressources

Le kit de ressources contient des exemples de packages de fournisseur de connexion à utiliser avec l'application Informatica Data Director. Ces packages de connexion à authentification unique sont stockés en tant que fichier JAR et ZIP. Les administrateurs de base de données et les autres membres techniques d'une équipe d'implémentation MDM peuvent utiliser ces fichiers pour créer leurs propres packages Fournisseur de connexion personnalisé.

Les exemples de fichiers de packages de connexion à authentification unique se trouvent dans le répertoire suivant :

`<répertoire d'installation infamdm>/hub/resourcekit/samples/sso`

Chargement du package Fournisseur de connexion personnalisé

Pour charger le package du fournisseur de connexion personnalisé, utilisez le gestionnaire de configuration Informatica Data Director.

1. Dans le volet de navigation du gestionnaire de configuration Informatica Data Director, cliquez sur **Paramètres du fournisseur de connexion**.
2. Dans le panneau **Paramètres du fournisseur de connexion** , cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Éditer les paramètres du fournisseur de connexion**, cliquez sur **Parcourir**.
4. **Sélectionnez le fichier d'archive du fournisseur de connexion personnalisé, puis cliquez sur OK.**
5. Dans le champ Archive d'implémentation du fournisseur de connexion, entrez le nom du fichier ZIP contenant l'implémentation de la classe du fournisseur de connexion.

   Vous devez attendre la fin du chargement du fichier ZIP sur le serveur.
6. Entrez le nom de la classe qui implémente `com.siperian.bdd.security.LoginProvider` dans le champ de nom de la classe du fournisseur de connexion.

   Il s'agit du nom qualifié complet de la classe qui implémente LoginProvider.

7. Cliquez sur **OK**.

   IDD valide le fichier ZIP chargé et crée une instance de la classe du fournisseur de connexion spécifiée.

Bibliothèques tierces

Dans IDD, vous pouvez utiliser un fournisseur de connexion personnalisé avec des bibliothèques tierces. Dans le framework Entity 360, toutes les bibliothèques tierces doivent être intégrées dans le même fichier ZIP en tant que package de fournisseur de connexion personnalisé.

Implémentation du fournisseur de connexion personnalisé

La classe Fournisseur de connexion personnalisé est une classe Java qui implémente l'interface LoginProvider (`com.siperian.bdd.security.LoginProvider`) définie dans IDD. Elle assure la prise en charge du mécanisme d'authentification par connexion unique (SSO).

Le fournisseur de connexion fonctionne avec le module de connexion Hub. Toutes les données requises par le module de connexion Hub pour la vérification de l'utilisateur authentifié doivent être transmises à partir du fournisseur de connexion en tant que champ de matrice d'octets `securityPayload` de la classe `com.siperian.bdd.security.LoginCredentials`. Ce champ est transmis tel quel du fournisseur de connexion vers le module de connexion Hub et contient des informations codées spécifiques à l'implémentation sur les utilisateurs.

Fournisseur de connexion personnalisé avec formulaire de connexion externe

Si un mécanisme d'authentification particulier exige une page de connexion autre qu'IDD, l'implémentation du fournisseur de connexion personnalisé doit utiliser les méthodes d'interface indiquées et décrites dans le tableau suivant :

Nom de la méthode d'interface	Description
initialize	IDD appelle cette méthode avant toute autre méthode d'implémentation du fournisseur de connexion et transmet un ensemble de propriétés décrivant le contexte de l'exécution. Dans IDD, ces propriétés contiennent une entrée à laquelle il peut être fait référence sous le terme de LoginProvider. La propriété SSO_POST_REDIRECT_PAGE_PROPERTY contient l'URL de la page JSF qui permet d'envoyer des données dans une demande POST vers le fournisseur de connexion externe. Une implémentation du fournisseur de connexion peut utiliser cette page pour rediriger IDD vers la page de connexion externe à l'aide de la méthode POST.
isUseIDDLoginForm	Cette méthode doit renvoyer FALSE.
redirectToProviderLoginPage	Cette méthode doit former une URL vers le formulaire de connexion externe et appeler le renvoi vers cette page. Vous pouvez aussi rediriger vers la page de connexion externe à l'aide de la méthode POST.
extractLoginCredentials	IDD appelle cette méthode lorsqu'une nouvelle demande d'authentification d'utilisateur arrive. Si la demande contient des informations émanant d'un fournisseur d'identité externe, telles que des paramètres de demande et des cookies, cette méthode doit les extraire et renvoyer l'instance LoginCredentials (com.siperian.bdd.security.LoginCredentials) avec des champs correctement renseignés. Si la demande ne contient pas d'informations d'authentification, la méthode doit renvoyer NULL.

Nom de la méthode d'interface	Description
encodeComponentUrl	Cette méthode n'est pas implémentée car le nom d'utilisateur et le mot de passe sont requis par le formulaire de connexion externe qu'IDD ne reconnaît pas.
onLogout	Elle est appelée lorsqu'un utilisateur se déconnecte. Elle peut exécuter une déconnexion sur le fournisseur d'identité externe et des paramètres de nettoyage définis par la méthode requestLoginCredentials.
getLogoImageBody	Cette méthode peut renvoyer NULL.

Une fois la connexion réussie, vous êtes redirigé vers la page IDD principale ou vers la page du composant Informatica Data Controls (IDC), selon votre demande initiale.

Vous pouvez également contourner l'authentification externe à l'aide du paramètre `internal_login_form=true` dans l'URL IDD qui affiche la connexion IDD.

Par exemple,

```
http://localhost:8080/bdd?internal_login_form=true
```

Dans ce cas, le nom d'utilisateur et le mot de passe sont vérifiés par rapport à la liste des utilisateurs de MDM Hub.

Transmission des identifiants vers le lien externe

Si vous avez besoin d'intégrer des liens externes dans IDD et si les liens utilisent le même fournisseur de connexion unique (SSO) (par exemple, SalesForce.com) comme par exemple le fournisseur de connexion personnalisé installé, utilisez cette méthode pour ajouter des informations d'authentification à l'URL du lien. Si aucune information n'est ajoutée, la méthode doit renvoyer la même chaîne d'URL que celle qui lui a été transmise comme paramètre ou null.

Exemple :

Supposez que vous implémentez LoginProvider pour une utilisation avec SalesForce.com.

Vous définissez également le lien externe avec l'URL `https://na7.salesforce.com/home/home.jsp` pour afficher la page d'accueil du compte SalesForce.com intégrée à l'écran IDD.

La méthode encodeComponentUrl reçoit cette URL et la convertit de la manière suivante :

```
https://na7.salesforce.com/secur/frontdoor.jsp?sid=<SFDC_API_SESSIONID>&retUrl=https://
na7.salesforce.com/home/home.jsp
```

Après cette transformation, un Iframe de la page IDD affiche la page d'accueil requise sans redirection vers le formulaire de connexion SalesForce.

Utilisation de la page POST

IDD utilise la page POST pour rediriger les utilisateurs vers une page de connexion externe. Cette page est soumise après son chargement sur le client.

La source de la page utilise la variable prédéfinie JSF requestScope pour accéder aux paramètres décrits dans le tableau suivant :

Nom du paramètre	Utilisation
providerGateURL	Doit être une valeur de chaîne. Il définit l'URL à laquelle le formulaire sera soumis (action de formulaire).
authParameters	Il s'agit d'un mappage des paires clé – valeur. Chaque paire de valeurs est utilisée pour créer une entrée masquée. La clé d'entrée de mappage est utilisée comme nom d'entrée et la valeur comme valeur de champ d'entrée.

Dans l'exemple suivant, la variable postRedirectPageUrl est définie pendant l'appel d'une méthode d'initialisation :

```
public void redirectToProviderLoginPage(HttpServletRequest httpRequest,
                                        HttpServletResponse httpResponse,
                                        String returnUrl) throws LoginProviderException {
RequestDispatcher dispatcher =
                  httpRequest.getRequestDispatcher(postRedirectPageUrl);
httpRequest.setAttribute( PROVIDER_GATE_URL_ATTR, authReq.getOPEndpoint() );
httpRequest.setAttribute( AUTH_PARAMETERS_ATTR, authReq.getParameterMap() );
dispatcher.forward( httpRequest, httpResponse );
}
```

Pour envoyer une redirection vers la nouvelle page lors de la déconnexion, vous pouvez ajouter le code suivant à la méthode redirectToProviderLoginPage() :

```
if("gotoLogoutPage".equalsIgnoreCase(httpRequest.getParameter("logoutParam"))){
    try
        { httpResponse.sendRedirect("http://www.google.com/"); }
        catch (Exception e)
        { // TODO Auto-generated catch block e.printStackTrace(); }
}
```

La méthode onLogout() écrit le code dans la réponse, comme indiqué dans l'exemple suivant :

```
{\"logoutURL\":\"/mdm/entity360view/?logoutParam=gotoLogoutPage\",\"kerberos\":\"true\"}
```

Configuration d'Entity 360 pour l'envoi de demandes POST au service Web

Parfois, un fournisseur de connexion personnalisé utilise des services Web qui attendent une demande POST. Entity 360 inclut un servlet qui envoie des demandes POST. Pour configurer le servlet de façon à ce qu'il envoie une demande POST à un service Web tiers, entrez l'URL de destination de la demande POST dans la méthode `redirectToProviderLoginPage`.

1. Utilisez un éditeur de texte pour modifier l'implémentation du fournisseur de connexion personnalisé.
2. Copiez l'URL du servlet dans les propriétés transférées à la méthode `initialize` du fournisseur de connexion personnalisé.
3. Dans la méthode `redirectToProviderLoginPage`, créez une demande.
    a. Dans l'attribut `AuthParameters`, définissez les paramètres à l'aide des paires nom-valeur.

       Les paires nom-valeur comprennent le corps de la demande POST.

    b. Dans l'attribut `ProviderGateURL`, entrez l'URL de destination de la demande POST.

       Remarque: Assurez-vous que l'URL se termine par une barre oblique (« / »). Si ce n'est pas le cas, l'application Entity 360 génère une exception de pointeur Null.

Le code suivant affiche un exemple de demande dans l'implémentation du fournisseur de connexion personnalisé :

```
    @Override
    public void redirectToProviderLoginPage(javax.servlet.http.HttpServletRequest
request,
            javax.servlet.http.HttpServletResponse response, String originalRequest)
throws
    LoginProviderException {
        RequestDispatcher dispatcher = request.getRequestDispatcher(forwardUrl);

        Map<String, String> params = new HashMap<>();

        params.put("param1", "value1");
        params.put("param2", "value2");

        request.setAttribute("AuthParameters", params);
        request.setAttribute("ProviderGateURL", "http://external.server.com/");

        dispatcher.forward(request, response);
}
```

Fournisseur de connexion personnalisé avec formulaire de connexion IDD

Si le mécanisme d'authentification utilise le formulaire de connexion IDD pour demander le nom d'utilisateur et le mot de passe, l'implémentation du fournisseur de connexion personnalisé doit utiliser les méthodes d'interface indiquées et décrites dans le tableau suivant :

Nom de la méthode d'interface	Description
initialize	IDD appelle cette méthode avant toute autre méthode d'implémentation du fournisseur de connexion et transmet un ensemble de propriétés décrivant le contexte de l'exécution. Dans IDD, les propriétés contiennent l'entrée unique. Elle peut être référencée en tant que « LoginProvider ». SSO_POST_REDIRECT_PAGE_PROPERTY contient l'URL de la page JSF permettant l'envoi de données vers le fournisseur de connexion externe.
isUseIDDLoginForm	Cette méthode doit renvoyer TRUE.
redirectToProviderLoginPage	Cette méthode n'est pas utilisée.
extractLoginCredentials	Cette méthode extrait les justificatifs d'identité de l'utilisateur à partir d'une demande HTTP. Si la demande contient des informations d'authentification, cette méthode doit renvoyer l'instance LoginCredentials (`com.siperian.bdd.security.LoginCredentials`) contenant des champs correctement renseignés. Si la demande ne contient pas d'informations d'authentification, la méthode doit renvoyer NULL.
requestLoginCredentials	Cette méthode est appelée après qu'un utilisateur a envoyé le formulaire de connexion rempli. Elle permet d'envoyer des demandes vers un fournisseur d'identité externe pour authentifier les utilisateurs. Les instances de LoginCredentials correctement remplies sont renvoyées une fois l'authentification réussie. En cas d'échec de l'authentification, `com.siperian.bdd.security.LoginProviderException` est renvoyé.
encodeComponentUrl	Cette méthode reçoit l'URL ExternalLink et peut ajouter des paramètres d'authentification.

Nom de la méthode d'interface	Description
onLogout	Elle est appelée lorsqu'un utilisateur se déconnecte. Elle peut exécuter la déconnexion sur le fournisseur d'identité externe et les paramètres de nettoyage définis par la méthode `requestLoginCredentials`.
getLogoImageBody	Cette méthode renvoie InputStream avec le corps du fichier d'image. Vous pouvez utiliser cette méthode pour afficher le logo d'un fournisseur d'identité externe dans le formulaire de connexion IDD. Le format d'image doit être PNG, JPEG ou GIF et ne doit pas dépasser une largeur de 96 pixels et une hauteur de 32 pixels. Si cette méthode renvoie NULL, IDD utilise l'image prédéfinie pour indiquer que le formulaire de connexion est traité par le fournisseur de connexion externe.

Création de la bibliothèque de fournisseurs de connexion

La classe LoginProvider et toutes les classes IDD requises pour la compilation de l'implémentation du fournisseur de connexion personnalisé sont intégrées dans le fichier `siperian-bdd.jar`. Ce fichier est inclus dans le kit de ressources MDM, qui contient également un modèle d'implémentation de LoginProvider. Pour en savoir plus, consultez le *Guide du kit de ressources d'Informatica MDM Hub*.

Configuration de l'authentification de la connexion unique SalesForce (WebLogic)

Si vous avez besoin de configurer l'authentification SSO SalesForce pour IDD, la vérification du nom d'hôte doit être désactivée dans WebLogic. Vous pouvez désactiver la vérification du nom d'hôte à l'aide de la procédure suivante :

1. Ouvrez la Console d'administration du serveur WebLogic et connectez-vous.
2. Développez **Environnement** et sélectionnez **Serveurs**.
3. Cliquez sur le nom du serveur exécutant le Hub (par défaut, AdminServer).
4. Depuis la page Paramètres, cliquez sur l'onglet **SSL**.
5. Cliquez sur **Avancé** en bas de la page.
6. Définissez le champ Vérification du nom d'hôte sur **Aucune.**
7. Cliquez sur **Enregistrer**.
8. Redémarrez le serveur WebLogic.

Configuration de l'authentification de la connexion unique SalesForce (WebSphere)

Si vous avez besoin de configurer l'authentification SSO SalesForce pour IDD, le serveur SalesForce doit être défini comme serveur de confiance dans WebSphere. Vous devez récupérer les certificats du signataire depuis l'hôte SalesForce auquel vous essayez de vous connecter et les ajouter au magasin de confiance WebSphere, à l'aide de la procédure suivante :

1. Ouvrez la Console d'administration WebSphere et connectez-vous.
2. Développez **Sécurité** puis cliquez sur **Certificat SSL et gestion des clés** > **Gérer les configurations de sécurité d'extrémité**.
3. Développez **Sortant** et cliquez sur **HTTP**.

4. Choisissez **Ensembles de clés SSL** depuis la liste déroulante.
5. Cliquez sur **NodeDefaultTrustStore** > **Certificats des signataires**.
6. Cliquez sur **Récupérer depuis le port**.
7. Entrez les valeurs suivantes dans les champs **Hôte**, **Port** et **Alias** :
   - Hôte : `www.salesforce.com`
   - Port : `443`
   - Alias : `www.salesforce.com`
8. Cliquez sur **Récupérer des informations sur le signataire**.

   Les données du certificat sont affichées.
9. Cliquez sur **Appliquer**.
10. Répétez les étapes 6 à 9 pour les hôtes suivants :
    - na10-api.salesforce.com
    - c.na10.visual.force.com
11. Cliquez sur **Enregistrer**.
12. Redémarrez le serveur Websphere.

Exemple d'implémentation du fournisseur de connexion d'authentification unique Google

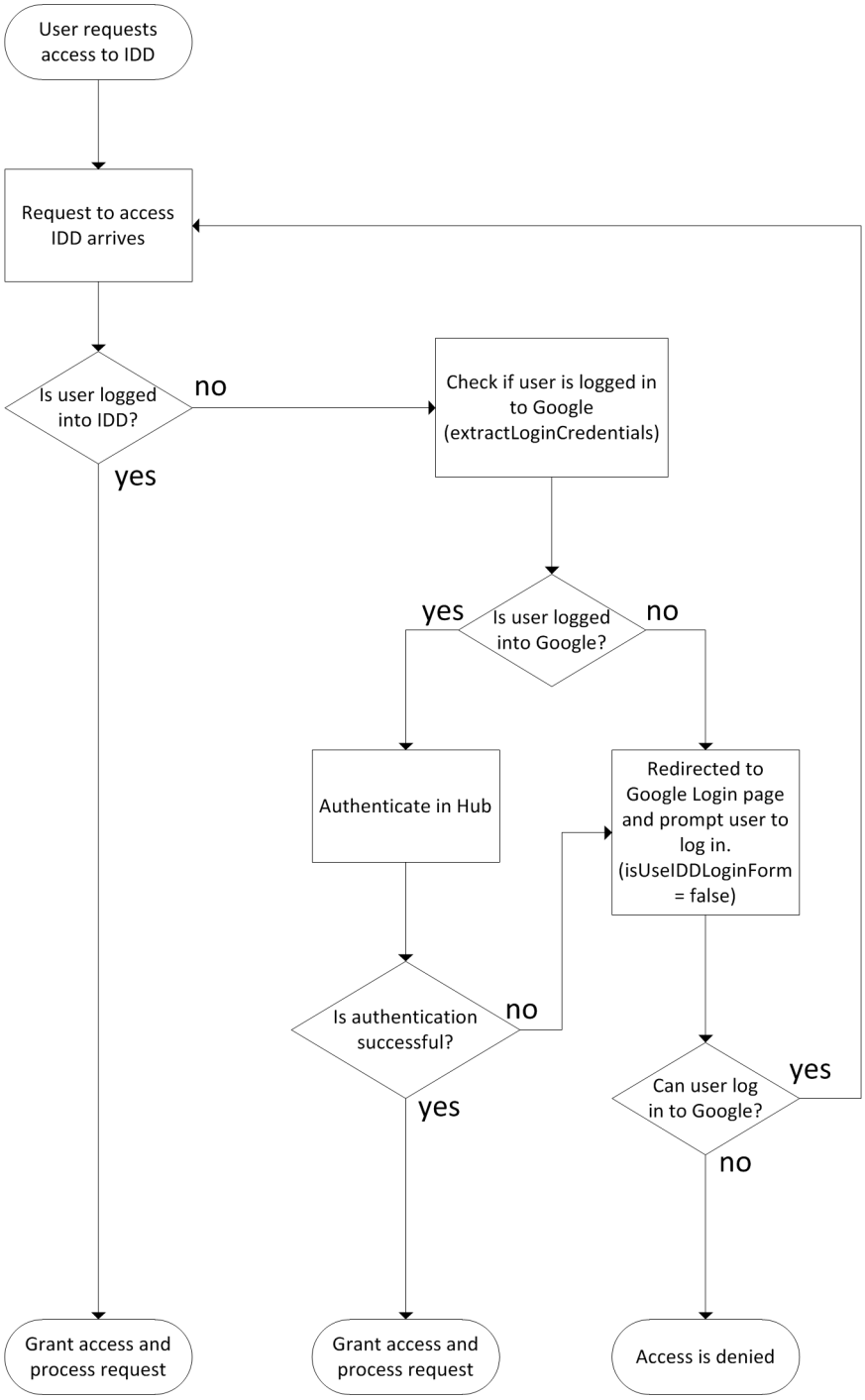
Le kit de ressources contient un exemple d'implémentation du fournisseur de connexion pour l'authentification unique (SSO) Google. L'exemple d'implémentation du fournisseur de connexion présente une manière de mettre en place l'authentification unique (SSO).

L'exemple d'implémentation du fournisseur de connexion pour l'authentification unique Google se trouve dans le fichier suivant :

```
<répertoire d'installation de MDM Hub>\hub\resourcekit\samples\sso\GoogleSSO\source\java
\com\siperian\dsapp\sso\google\GoogleLoginProvider.java
```

Lorsqu'un utilisateur demande l'accès à Informatica Data Director, le fournisseur de connexion authentifie l'utilisateur via une séquence d'événements.

L'image suivante montre la séquence d'événements qui se produit lorsque vous implémentez l'authentification unique Google à l'aide de l'exemple d'implémentation du fournisseur de connexion :



Les séquences suivantes peuvent se produire, que l'utilisateur soit connecté ou non à Informatica Data Director ou à Google :

Séquence pour les utilisateurs qui sont connectés à Informatica Data Director.

Lorsqu'un utilisateur demande l'accès à Informatica Data Director, le fournisseur de connexion vérifie si l'utilisateur est connecté. Si l'utilisateur est connecté à Informatica Data Director, le fournisseur de connexion accorde l'accès à Informatica Data Director.

Séquence pour les utilisateurs non connectés à Informatica Data Director, mais connectés à Google.

Lorsque le fournisseur de connexion détermine que l'utilisateur n'est pas connecté à Informatica Data Director, il vérifie si l'utilisateur est connecté à Google. Si l'utilisateur est connecté à Google, le fournisseur de connexion transmet les justificatifs d'identité Google de l'utilisateur vers MDM Hub. L'outil des fournisseurs de sécurité de MDM Hub authentifie les justificatifs d'identité Google. Si l'outil des fournisseurs de sécurité de MDM Hub authentifie l'utilisateur, ce dernier peut accéder à Informatica Data Director. Dans le cas contraire, le fournisseur de connexion redirige l'utilisateur vers la page de connexion Google afin qu'il indique des justificatifs d'identité différents.

Séquence pour les utilisateurs non connectés à Informatica Data Director ni à Google.

Lorsque le fournisseur de connexion détermine que l'utilisateur n'est connecté ni à Informatica Data Director ni à Google, le fournisseur de connexion redirige l'utilisateur vers le formulaire de connexion Google. Dans l'exemple d'implémentation, le fournisseur de connexion redirige l'utilisateur vers le formulaire de connexion Google au lieu du formulaire de connexion Informatica Data Director, car `isUseIDDLoginForm` est défini sur la valeur `False`. Si vous définissez `isUseIDDLoginForm` sur la valeur `True`, le fournisseur de connexion redirige l'utilisateur vers le formulaire de connexion Informatica Data Director.

Une fois l'utilisateur connecté à Google, le processus recommence (à la différence que l'utilisateur est désormais connecté à Google). L'outil des fournisseurs de sécurité de MDM Hub authentifie les justificatifs d'identité Google de l'utilisateur.

Configuration de l'authentification de la connexion unique Google

Si vous utilisez l'authentification de la connexion unique Google pour Informatica Data Director, configurez Informatica Data Director pour revenir à l'écran de connexion lorsqu'un utilisateur s'est déconnecté.

1. Ouvrez `cmxserver.properties` dans le répertoire suivant :
   - Sous UNIX : `<infamdm installation directory>/hub/server/resources`
   - Sous Windows : `<infamdm installation directory>\hub\server\resources`
2. Ajouter la propriété suivante à `cmxserver.properties` :

   ```
   cmx.bdd.redirect_to_login_after_logout=false
   ```
3. Redémarrez l'application Serveur Hub pour recharger les paramètres dans le fichier `cmxserver.properties`.

CHAPITRE 5

Configuration manuelle d'IDD

Ce chapitre comprend les rubriques suivantes :

- Présentation de la configuration manuelle d'IDD, 62
- Outils XML, 63
- Utilisation du fichier XML de configuration IDD , 63
- Zone de sujet, 65
- Configuration du gestionnaire de hiérarchies, 72
- Extensions de l'interface utilisateur, 76
- Sorties utilisateur, 86
- Localisation, 93
- Pages d'erreur personnalisées, 95
- Aide en ligne, 96

Présentation de la configuration manuelle d'IDD

Le fichier de configuration IDD (IDDConfig_fr.xml) est un document XML qui peut être modifié dans le gestionnaire de configuration IDD ou exporté et modifié manuellement.

Pour éditer la configuration pour une application IDD existante :

1. Exportez l'application IDD dans un fichier ZIP.
2. Extrayez le fichier ZIP de l'application.
3. Modifiez le fichier de configuration IDD (iddconfig.xml).
4. Importez le fichier de configuration édité directement pour remplacer celui présent dans la base de données (Importer la configuration IDD uniquement). Vous pouvez aussi zipper de nouveau l'application IDD et importer l'application complète pour remplacer tous les fichiers pour l'application (Importer l'application IDD complète).

Outils XML

Le Kit de ressources Informatica MDM Hub inclut un schéma XML (fichier XSD) pour le fichier de configuration IDD.

C'est très utile lors de l'utilisation d'éditeurs XML. Il peut vous guider dans l'édition du fichier et est surtout utilisé par l'éditeur pour vérifier que le code XML est correct dans un fichier de configuration IDD. Le fichier de configuration IDD doit réussir ce test avant d'être importé dans le gestionnaire de configuration IDD.

Lorsqu'un éditeur de texte simple peut être utilisé pour modifier la configuration IDD, de nombreux outils d'édition XML facilitent l'utilisation du code XML, y compris :

Éditeur	URL
XML Copy Editor	http://xml-copy-editor.sourceforge.net/
XML Spy	http://www.altova.com/products/xmlspy/xmlspy.html
oXygen	http://www.oxygenxml.com/

L'échantillon IDD dans le Kit de ressources contient les composants suivants, qui peuvent aider pour la configuration manuelle.

Élément du kit de ressources	Description
`siperian-bdd-config-6.xsd`	Schéma XML pour le fichier de configuration IDD. Ce fichier se trouve sous `<Dossier d'installation>\hub\resourcekit\sdk\bddXsdDoc\siperian-bdd-config-6.xsd`
Documentation HTML pour le schéma XML	Documentation de type Javadoc. Fournit les informations présentes dans le schéma XML, mais sous une forme qui facilite la navigation. **Remarque:** Consultez cette documentation pour trouver les informations les plus détaillées sur les attributs et éléments XML dans le fichier de configuration IDD.
Exemple de configuration IDD	À utiliser avec l'exemple de schéma.
Exemple de sorties utilisateur IDD	Exemple illustrant comment créer du code Java personnalisé à intégrer à IDD.
Javadocs de bibliothèque IDD	Javadocs pour les interfaces dans Siperian-bdd.jar. Utilisés pour implémenter les sorties utilisateur IDD dans Java.

Utilisation du fichier XML de configuration IDD

Un fichier XML de configuration IDD peut facilement être exécuté sur des centaines de lignes.

Le fichier n'est pas affiché entièrement ici, seulement l'extrait de code approprié. Vous trouverez un fichier de configuration complet dans le Kit de ressources, ou en l'exportant depuis le gestionnaire de configuration IDD.

L'extrait de code suivant est un exemple de groupe de domaines avec un seul domaine :

```
<subjectAreaGroup name="Customer" primaryObjectUid="C_PARTY">
        <subjectArea name="Person">
            <primaryObject hmEntityTypeUid="Person">
                <subTypeQualifier columnUid="C_PARTY|PARTY_TYPE"  filterValue="Person"/>
                <cleanseFunction
                                cleanseFunctionUid="BDD Cleanse and Validation Library|
CVPerson">
                    <cleanseInput>
                        <cleanseColumn columnUid="C_PARTY|FIRST_NAME"
parameterName="firstName"/>
                        <cleanseColumn columnUid="C_PARTY|MIDDLE_NAME"
                                       parameterName="middleName"/>
                        <cleanseColumn columnUid="C_PARTY|LAST_NAME"
parameterName="lastName"/>
                    </cleanseInput>
                    <cleanseOutput>
                        <cleanseColumn columnUid="C_PARTY|FIRST_NAME"
parameterName="firstName"/>
                        <cleanseColumn columnUid="C_PARTY|MIDDLE_NAME"
                                       parameterName="middleName"/>
                        <cleanseColumn columnUid="C_PARTY|LAST_NAME"
parameterName="lastName"/>
                        <cleanseColumn columnUid="C_PARTY|DISPLAY_NAME"
                                       parameterName="displayName"/>
                    </cleanseOutput>
                </cleanseFunction>
                <layout columnsNum="3">
                    <column columnUid="C_PARTY|NAME_PREFIX_CD" editStyle="FIELD"
                            horizontalStyle="SMALL"/>
                    <column columnUid="C_PARTY|FIRST_NAME" editStyle="FIELD"
                            horizontalStyle="MEDIUM" required="true"/>
                    <column columnUid="C_PARTY|MIDDLE_NAME" editStyle="FIELD"
                            horizontalStyle="MEDIUM"/>
                    <column columnUid="C_PARTY|LAST_NAME" editStyle="FIELD"
                            horizontalStyle="MEDIUM" required="true"/>
                    <column columnUid="C_PARTY|GENERATION_SUFFIX_CD" editStyle="FIELD"
                            horizontalStyle="SMALL"/>
                    <column columnUid="C_PARTY|BIRTHDATE" editStyle="CALENDAR"
                            horizontalStyle="MEDIUM"/>
                    <column columnUid="C_PARTY|GENDER_CD" editStyle="FIELD"
                            horizontalStyle="SMALL">
                        <columnI18NLookup languageCdUid="C_LU_GENDER_LCL|LANGUAGE_CODE"
                                          countryCdUid="C_LU_GENDER_LCL|COUNTRY_CODE"
                                          lookupFKUid="C_LU_GENDER_LCL|GENDER_CODE"
                                          localizedNameUid="C_LU_GENDER_LCL|
LOCALIZED_STRING"/>
                    </column>
                    <column columnUid="C_PARTY|TAX_ID" editStyle="FIELD"
                            horizontalStyle="MEDIUM"/>
                    <column columnUid="C_PARTY|DISPLAY_NAME" editStyle="FIELD"
                            horizontalStyle="LARGE"/>
                </layout>
                <label existsFormat="{1},{2}">
                    <column columnUid="C_PARTY|LAST_NAME"/>
                    <column columnUid="C_PARTY|FIRST_NAME"/>
                    <column columnUid="C_PARTY_ELECT_ADDR|ELECTRONIC_ADDRESS"/>
                </label>
            </primaryObject>
            <search displayPackageUid="PKG_PERSON_SEARCH">
            </search>
            <match>
                <matchRuleSet uid="C_PARTY|IDL" type="BOTH"/>
            </match>
            <taskAssignmentConfig task="UpdateWithApproval">
                <securityRole roleUid="DataSteward"/>
            </taskAssignmentConfig>
            <taskAssignmentConfig task="UpdateWithOptionalApproval" >
                <securityRole roleUid="DataSteward"/>
            </taskAssignmentConfig>
            <taskAssignmentConfig task="UpdateRejectedRecord">
```

```
            <securityRole roleUid="DataSteward"/>
        </taskAssignmentConfig>
        <taskAssignmentConfig task="ReviewNoApprove">
            <securityRole roleUid="Manager"/>
        </taskAssignmentConfig>
        <taskAssignmentConfig task="FinalReview" >
            <securityRole roleUid="SrManager"/>
        </taskAssignmentConfig>
        <taskAssignmentConfig task="Merge">
            <securityRole roleUid="DataSteward"/>
        </taskAssignmentConfig>
        <taskAssignmentConfig task="Unmerge">
            <securityRole  roleUid="DataSteward"/>
        </taskAssignmentConfig>
        <dataSecurity>
            <securityFilter columnUid="MATCH_PATH_COMPONENT.C_MT_ADDRESS|STATE_CD">
                <securityValue value='CA'>
                    <securityRole roleUid="Customer-CA"/>
                </securityValue
            </securityFilter>
        </dataSecurity>
    </subjectArea>
</subjectAreaGroup>
```

Consultez la documentation HTML pour trouver le schéma XML avec des détails sur les éléments, les attributs et les valeurs autorisées.

Zone de sujet

Les éléments décrits dans cette section peuvent nécessiter une modification manuelle directement dans le fichier IDDConfig_fr.xml.

Colonne de recherche

Une application IDD renseigne automatiquement une liste déroulante des valeurs acceptables pour les colonnes configurées dans le gestionnaire de schéma en tant que recherches.

Ceci est traité dans la gestionnaire de configuration IDD pour les colonnes qui ont une clé étrangère vers la table de recherche. Si la clé étrangère n'existe pas (par exemple, pour des raisons de performances), les informations sur la table de recherche peuvent être spécifiées dans la configuration XML.

Une recherche explicite est définie à l'aide de l'élément columnLookup, comme illustré dans l'exemple suivant.

```
<column columnUid="C_PARTY|GENDER_CD" editStyle="FIELD" horizontalStyle="SMALL">
      <columnLookup lookupFKUid="C_LU_GENDER|GENDER_CODE"
          lookupNameUid="C_LU_GENDER|GENDER_DISP"/>
   </column>
```

Dans cet exemple, la colonne C_PARTY|GENDER_CD doit être traitée comme si elle avait une clé étrangère vers la colonne C_LU_GENDER|GENDER_CODE, et la table C_LU_GENDER est traitée comme une table de recherche. L'application IDD crée une liste déroulante pour la colonne GENDER_CD, et cette liste est renseignée avec des valeurs de la table C_LU_GENDER (les valeurs affichées sont extraites de la colonne GENDER_DISP).

L'élément columnI18NLookup peut être spécifié avec le sous-élément columnLookup si la localisation des valeurs affichées est requise.

```
<column columnUid="C_PARTY|GENDER_CD" editStyle="FIELD" horizontalStyle="SMALL">
      <columnLookup lookupFKUid="C_LU_GENDER|GENDER_CODE"
         lookupNameUid="C_LU_GENDER|GENDER_DISP"/>
```

```
      <columnI18NLookup languageCdUid="C_LU_GENDER_LCL|LANGUAGE_CODE"
         countryCdUid="C_LU_GENDER_LCL|COUNTRY_CODE"
         lookupFKUid="C_LU_GENDER_LCL|GENDER_CODE"
         localizedNameUid="C_LU_GENDER_LCL|LOCALIZED_STRING"/>
   </column>
```

LIENS CONNEXES :

- "Tables de recherche" à la page 26

Tables de recherche avec colonne de sous-type

Une table de recherche unique peut être utilisée pour stocker des valeurs de recherche pour différents types de codes.

Dans ce cas, la table de recherche a une colonne de sous-type, qui identifie le type de code.

L'utilisation d'une table de recherche avec de nombreux types de recherches est configurée comme illustré dans l'exemple suivant.

```
<column columnUid="C_AUTOMOBILE|DOORS_CODE" editStyle="FIELD" horizontalStyle="SMALL">
      <columnLookup lookupFKUid="C_LU_AUTO_ATTR|CODE"
            lookupNameUid="C_LU_AUTO_ATTR|DISPLAY_NAME">
         <subTypeQualifier columnUid="C_LU_AUTO_ATTR|ATTR_TYPE">
            <filter>
               <value>Doors</value>
               <value>Style</value>
            </filter>
         </subTypeQualifier>
      </columnLookup>
   </column>
```

Dans cet exemple, la colonne C_AUTOMOBILE|DOORS_CODE est une colonne de recherche. Seules les valeurs de la table de recherche avec ATTR_TYPE="Doors" sont utilisées pour cette recherche.

La localisation de la recherche peut aussi être associée à des sous-types de recherches, comme illustré dans l'exemple suivant.

```
<column columnUid="C_AUTOMOBILE|DOORS_CODE" editStyle="FIELD" horizontalStyle="SMALL">
      <columnLookup lookupFKUid="C_LU_AUTO_ATTR|CODE"
         lookupNameUid="C_LU_AUTO_ATTR|DISPLAY_NAME">
         <subTypeQualifier columnUid="C_LU_AUTO_ATTR|ATTR_TYPE">
            <filter>
               <value>Doors</value>
               <value>Style</value>
            </filter>
         </subTypeQualifier>
      </columnLookup>
      <columnI18NLookup languageCdUid="C_LU_AUTO_ATTR_LCL|LANGUAGE_CODE"
         countryCdUid="C_LU_AUTO_ATTR_LCL|COUNTRY_CODE" lookupFKUid="C_LU_AUTO_ATTR_LCL|
CODE"
         localizedNameUid="C_LU_AUTO_ATTR_LCL|LOCALIZED_STRING">
         <subTypeQualifier columnUid="C_LU_AUTO_ATTR_LCL|ATTR_TYPE "
filterValue="Doors"/>
      </columnI18NLookup>
   </column>
```

LIENS CONNEXES :

- "Codes de langue" à la page 171

Valeurs de recherche statiques

Les valeurs pour une colonne de recherche peuvent également être définies directement dans le fichier de configuration IDD. Aucune table de recherche n'est utilisée.

L'élément columnStaticLookups est utilisé pour définir cela, comme illustré dans l'exemple suivant.

```
<column columnUid="C_PARTY|GENDER_CD" editStyle="FIELD" horizontalStyle="SMALL">
      <columnStaticLookups>
         <columnStaticLookup code="M" name="MALE"/>
         <columnStaticLookup code="F" name="FEMALE"/>
      </columnStaticLookups>
   </column>
```

Cet exemple spécifie que seules les valeurs 'M' et 'F' peuvent être stockées dans la colonne C_PARTY|GENDER_CD. Pour cette colonne, l'application IDD crée une liste déroulante remplie avec les valeurs 'MALE' et 'FEMALE'.

Les valeurs de recherche statiques peuvent aussi être localisées, comme illustré dans l'exemple suivant.

```
<column columnUid="C_PARTY|GENDER_CD" editStyle="FIELD" horizontalStyle="SMALL">
      <columnStaticLookups>
         <columnStaticLookup code="M" name="MALE"/>
         <columnStaticLookup code="F" name="FEMALE"/>
         <columnStaticLookup code="M" name="MANN" languageCode="de" countryCode="DE"/>
         <columnStaticLookup code="F" name="FRAU" languageCode="de"  countryCode="DE"/>
      </columnStaticLookups>
   </column>
```

Afficher les champs secondaires d'un objet de base dans l'onglet enfant

Pour afficher les champs secondaires depuis un objet de base (OB) dans l'onglet enfant dans IDD, utilisez le type enfant **Partie de l'objet principal** lors de la création du domaine enfant dans le gestionnaire de configuration IDD.

Vous devez configurer le fichier de configuration IDD (`IDDConfig.xml`) pour afficher les champs secondaires depuis un objet de base dans l'onglet enfant.

Pour l'exemple suivant, dans la console Hub vous devez créer un objet de base `C_EMPLOYEE` avec quatre colonnes : `EMP_ID`, `EMP_NAME`, `STATE` et `COUNTRY`, également le domaine parent `Employé` et le domaine enfant `EmpDetails`.

L'extrait de fonctions suivant affiche `EMP_NAME` (qui est un champ secondaire) dans l'onglet enfant `EmpDetails`.

```
primaryObjectUid="C_EMPLOYEE" searchOnly="false">
<subjectArea displayName="Employee" name="Employee" showXREF="false">
    <primaryObject>
        <layout columnsNum="3">
            <column columnUid="C_EMPLOYEE|EMP_ID"
                editStyle="FIELD" editable="true"
                hidden="false" horizontalStyle="MEDIUM"
                lineBreak="false"
                ns1:showInHMCompactView="false"
                required="false" xmlns:ns1="urn:siperian.dsapp.config"/>
            <column columnUid="C_EMPLOYEE|STATE"
                editStyle="FIELD" editable="true"
                hidden="false" horizontalStyle="MEDIUM"
                lineBreak="false"
                ns2:showInHMCompactView="false"
```

```
                            required="false" xmlns:ns2="urn:siperian.dsapp.config"/>
                        <column columnUid="C_EMPLOYEE|COUNTRY"
                            editStyle="FIELD" editable="true"
                            hidden="false" horizontalStyle="MEDIUM"
                            lineBreak="false"
                            ns3:showInHMCompactView="false"
                            required="false" xmlns:ns3="urn:siperian.dsapp.config"/>
                    </layout>
                    <label existsFormat="{0}"
                        existsNoAttributesFormat="{0}" newFormat="New {0}"/>
                </primaryObject>
                <poPartOfChild displayName="EmpDetails"
                    name="EmpDetails" ns4:showInHMCompactView="false"
xmlns:ns4="urn:siperian.dsapp.config">
                    <ns4:layout columnsNum="3">
                        <ns4:column columnUid="C_EMPLOYEE|EMP_NAME"
                            editStyle="FIELD" editable="true"
                            hidden="false" horizontalStyle="MEDIUM"
                            lineBreak="false"
                            ns4:showInHMCompactView="false" required="false"/>
                    </ns4:layout>
                </poPartOfChild>
                <search displayPackageUid="PKG_EMPLOYEE"/>
                <dataSecurity/>
            </subjectArea>
        </subjectAreaGroup>
```

Affichage du parent d'un objet principal dans un onglet enfant

Lorsqu'un objet principal possède un parent, vous pouvez afficher les attributs de l'objet de base parent dans un onglet enfant. Pour configurer l'affichage, vous devez modifier le fichier XML de configuration d'IDD. Vous pouvez configurer plusieurs onglets enfants (un pour chaque objet de base parent à afficher).

Dans MDM Hub, la relation entre les objets de base doit être de type un-à-un ou un-à-plusieurs. Imaginons par exemple que vous créez les objets de base C_ADDRESS et C_PARTY et que vous créez une relation entre ces objets.

1. Dans le gestionnaire de configuration IDD, créez un domaine pour l'objet principal.
   Vous pouvez par exemple créer un domaine pour C_ADDRESS.
2. Enregistrez la configuration.
3. Ouvrez le fichier XML de configuration d'IDD.
4. Après l'élément `primaryObject`, ajoutez l'élément `poParent` et définissez les champs à afficher.

   L'exemple de code suivant montre comment configurer l'élément `poParent` pour afficher trois champs de C_PARTY dans l'onglet enfant.

```
<subjectArea displayName="Address" name="Address" showXREF="false">
    <primaryObject>
  ...
    </primaryObject>
    <poParent name="Party" displayName="Party" uid="C_PARTY"
mpcUid="C_MT_PARTY_ADDRESS">
  <layout columnsNum="3">
        <column columnUid="C_PARTY|FIRST_NAME" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
        <column columnUid="C_PARTY|LAST_NAME" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
   <column columnUid="C_PARTY|PARTY_TYPE" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
  </layout>
 </poParent>
    <search displayPackageUid="PKG_ADDRESS"/>
    <dataSecurity/>
</subjectArea>
</subjectAreaGroup>
```

5. Enregistrez le fichier.

Développement d'un domaine enfant par défaut dans la vue de données

Vous pouvez configurer un domaine enfant à développer par défaut lorsque vous ouvrez un enregistrement dans la vue de données.

Définissez l'attribut `développé` sur `true` dans `BDDConfig_fr.xml` pour le domaine enfant. Lorsque vous ouvrez l'enregistrement principal, le domaine enfant apparaît développé. Les autres domaines enfants s'affichent réduits.

L'exemple de code suivant définit le domaine C_PARTY_NAME pour qu'il se développe par défaut lorsque vous ouvrez l'enregistrement principal dans la vue de données :

```
<one2ManyChild name="Names" type="ONE_2_MANY" uid="C_PARTY_NAME"
mpcUid="C_MT_PARTY_NAME" expanded="true">
    <layout columnsNum="1">
        <column columnUid="C_PARTY_NAME|NAME" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
        <column columnUid="C_PARTY_NAME|AUTOMOBILE_ID" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
    </layout>
</ one2ManyChild>
```

Création de référence frère

Vous pouvez créer une référence frère pour créer une relation d'un enregistrement dans un domaine vers un enregistrement enfant dans ce domaine. Par exemple, un client pourrait inclure les enregistrements enfants d'adresse et de numéro de téléphone, le numéro de téléphone ayant une clé étrangère pour l'associer à une adresse spécifique.

Vous devez configurer le fichier de configuration IDD (`IDDConfig.xml`) pour créer la référence frère.

L'extrait de fonctions suivant crée une référence frère pour le champ de colonne `ADDRESS_ID` dans le domaine enfant `PERSON DETAILS`.

```
<ns10:column
          columnUid="C_PERSON_DETAILS|ADDRESS_ID"
          editStyle="FIELD" editable="true"
          hidden="false" horizontalStyle="MEDIUM"
          lineBreak="false"
          ns10:showInHMCompactView="false" required="false">
       <siblingReference childName="Addresses">
          <label existsFormat=" {1}, {2} "
                    existsNoAttributesFormat="MailingAddress"
                    newFormat="New MailingAddress" taskFormat=" {1}, {2} ">
                         <column columnUid="C_ADDRESS|ADDRESS_LINE_1"/>
                         <column columnUid="C_ADDRESS|CITY_NAME"/>
          </label>
        </siblingReference>
</ns10:column>
```

Remarque: Vous devez spécifier l'attribut `ChildName` dans la balise `siblingReference` avec le nom de référence du domaine enfant disponible.

Petits-enfants

Lorsque des petits-enfants apparaissent dans une vue de table, tous les enregistrements petits-enfants sont affichés, pas uniquement ceux qui sont liés à l'enregistrement enfant sélectionné. IDD propose une option de configuration qui aide à comprendre la relation entre ces petits-enfants et l'enfant.

Un élément parentReference peut être défini pour la colonne qui est la clé étrangère de l'enregistrement enfant. Cela définit un libellé à afficher dans l'enregistrement petit-enfant qui contient des données issues de l'enfant.

Dans l'exemple ci-dessous, la colonne de clé étrangère du petit-enfant à l'enfant est configurée comme une référence parent. Cela configure un élément de libellé avec l'ensemble de colonnes à utiliser pour les libellés et l'élément existsFormat. Dans cet exemple, le libellé pour l'enregistrement enfant sera "<Numéro de téléphone>, (<Numéro de poste>)".

```
<many2ManyChild name="TestPhone" displayName="Test Phone" type="PART_OF"
        uid="C_PHONE_CHILD4" mpcUid="C_MT_PHONE_CHILD4" defaultView="form">
            <layout columnsNum="3">
                <column columnUid="C_PHONE_CHILD4_REL|PHONE_ID"
editStyle="FIELD"
                    horizontalStyle="LARGE">
                    <parentReference>
                        <label existsFormat="{0} ({1})">
                            <column columnUid="C_PARTY_PHONE|PHONE_NUM"/>
                            <column columnUid="C_PARTY_PHONE|PHONE_EXT_NUM"/>
                        </label>
                    </parentReference>
                </column>
                <column … />
            </layout>
    </many2ManyChild>
```

Liens de domaines

Un domaine peut contenir des enfants de référence plusieurs à plusieurs.

Ils présentent un domaine comme enfant d'un autre domaine. Le domaine enfant ne peut pas être édité directement. L'utilisateur de l'application IDD doit naviguer vers une vue de données distincte pour que le domaine enfant l'édite. L'élément `subjectAreaLinkColumn` est utilisé pour définir une colonne à utiliser comme liaison automatique.

Les données dans la colonne identifiée comme lien vers le domaine sont soulignées. Lorsque l'utilisateur de l'application IDD clique sur cette colonne, le domaine associé s'ouvre dans un nouvel onglet.

Qu'une colonne de lien de domaine soit configuré ou non, l'utilisateur de l'application IDD peut cliquer à l'aide du bouton droit de la souris sur l'enregistrement et sélectionner « Ouvrir dans un nouvel onglet » pour ouvrir le domaine.

```
<many2ManyChild name="Organization" displayName="Org" type="REFERENCE"
        uid="C_PARTY" subjectAreaLinkColumn=”C_PARTY_ORGANIZATION_NAME”
        mpcUid="C_MT_ORG_CHILD"  hmEntityTypeUid="Organization">
        <layout columnsNum="2">
            <column columnUid="C_PARTY|ORGANIZATION_NAME" editStyle="FIELD"
                horizontalStyle="LARGE" required="true"/>
            …
        </layout>
    </many2ManyChild>
```

Regroupement logique de menus

Si vous avez plusieurs groupes de domaines, vous pouvez les organiser ou les grouper pour créer une structure de menu logique de niveau supérieur dans l'application IDD.

Vous devez modifier le fichier de configuration IDD (`IDDConfig.xml`) pour créer des groupes logiques de groupes de domaines.

L'extrait de fonctions suivant crée un regroupement logique de groupes de domaines.

```
<sagGroups>
       <sagLogicalGroup name="Product" displayName="Product">
              <sagReference sagName="Account" />
              <sagReference sagName="AccountGroup" />
       </sagLogicalGroup>
</sagGroups>
```

Personnalisation des libellés de colonnes

Vous pouvez personnaliser les libellés de colonne dans IDD au niveau du domaine pour différencier des libellés de colonnes identiques qui sont utilisés dans plusieurs domaines ou pour modifier un libellé de colonne. Vous devez éditer le fichier `MetadataBundle.properties` pour personnaliser le libellé de colonne du domaine. Par exemple, prenez l'objet de base Party avec les domaines Personne et Entreprise. Si le libellé de colonne Tax ID est présent dans les deux domaines, vous pouvez personnaliser les libellés de colonnes pour faire une distinction entre les domaines.

Pour personnaliser les libellés de colonne d'un domaine, suivez les étapes suivantes :

1. Si vous avez modifié les métadonnées dans le stockage de référence opérationnelle, cliquez sur **Effacer le cache**.
2. Exportez l'application IDD dans un fichier ZIP.
3. Extrayez le fichier ZIP de l'application.
4. Éditez le fichier `MetadataBundle.properties`.
   Par exemple : pour modifier la colonne libellé- Tax ID en Customer Tax ID dans MetadataBundle.properties, éditez Test.Person.COLUMN.C_PARTY|TAX_ID=Customer Tax ID.
5. Dans le gestionnaire de configuration IDD, sélectionnez l'application IDD pour remplacer le fichier MetadataBundle.properties modifié.
6. Cliquez sur le bouton **Importer** et sélectionnez **Importer dans l'application IDD existante**.
7. Dans la fenêtre **Importer dans l'application IDD existante**, pour le **Type de configuration**, sélectionnez **Ensemble de métadonnées**.
8. Cliquez sur **Parcourir** pour localiser et sélectionner le fichier MetadataBundle.properties approprié.
9. Cliquez sur **Importer**.

   Connectez-vous à l'application IDD pour afficher les libellés des colonnes personnalisés.

Configurer le style d'édition de la case à cocher

Le mappage de valeurs vous permet de définir des valeurs de colonnes devant être stockées dans le Hub MDM avec le style d'édition de la case à cocher.

Le tableau suivant fournit des informations sur les styles d'édition que vous pouvez configurer pour le type de données pris en charge.

Type de données	Style d'édition
DATE	Calendrier et Calendrier long
INT et CHAR(1)	Champ, Zone de texte et Case à cocher
Autres	Champ et Zone de texte

Remarque:

- Pour une colonne de type de données CHAR(1), vous pouvez définir trois couples de valeurs que vous pouvez configurer pour une case à cocher : valeur 1/0, valeur Y/N ou valeur T/F. En fonction du couple de valeurs affecté, la valeur correspondante sera enregistrée dans l'objet de base.
- Pour une colonne de type de données INT, vous pouvez uniquement définir des couples de valeurs 0 et 1.

Pour une configuration manuelle, vous devez vous assurer que l'élément `colonne` avec `editStyle="CHECKBOX"` n'a pas plus d'un élément `valueMapping` imbriqué. L'élément `valueMapping` pour `editStyle="CHECKBOX"` doit avoir deux éléments `mappingItem` imbriqués. L'`Élément de mappage` doit aussi inclure les valeurs `sélectionnéesTrue` et `False`.

Dans l'exemple suivant, l'attribut `domainValue` est responsable de la valeur stockée dans le Hub MDM et l'attribut `sélectionné` est responsable de la présentation du contrôle case à cocher. Les valeurs `True` ou `False` sont définies respectivement pour les états de case à cocher sélectionné et non sélectionné.

```
<column columnUid="C_PARTY_PHONE|IS_VALID_IND" editStyle="CHECKBOX"
horizontalStyle="SMALL">
<valueMapping>
<mappingItem domainValue="1" selected="true"/>
<mappingItem domainValue="0" selected ="false"/>
</valueMapping>
</column>
```

Configuration du gestionnaire de hiérarchies

Les paramètres décrits ici s'appliquent à la Vue de hiérarchie IDD pour tous les types d'entités du gestionnaire de hiérarchies.

La liste XML suivante présente des exemples de tous les éléments décrits plus tard dans cette section.

```
<hmConfiguration hmConfigurationUid="Default|Master" enableAddRel="false"
            simpleNodeLimit="100">
        <hmOneHopLimits totalRels="1000"/>
        <hmManyHopLimits hops="20" relsPerEntity="50" totalRels="1000"/>
        <hmRelationshipTypes>
            <hmRelationshipType hmRelationshipUid="HM_RELATIONSHIP_TYPE.employs">
                <layout columnsNum="2">
                    <column columnUid="C_RL_PARTY|REL_NAME" editStyle="FIELD"
                        horizontalStyle="LARGE" required="true"/>
                    <column columnUid="C_RL_PARTY|REL_DESC" editStyle="FIELD"
                        horizontalStyle="MEDIUM"/>
                    <column columnUid="C_RL_PARTY|NOTE" editStyle="FIELD"
                        horizontalStyle="SMALL"/>
                </layout>
            </hmRelationshipType>
            <hmRelationshipType hmRelationshipUid="HM_RELATIONSHIP_TYPE.contains member">
```

```
                <layout columnsNum="2">
                    <column columnUid="C_RL_PARTY_GROUP|HUB_STATE_IND" editStyle="FIELD"
                        horizontalStyle="MEDIUM"/>
                </layout>
            </hmRelationshipType>
        </hmRelationshipTypes>
        <hmFilter name="filter1" displayName="Filter 1">
            <showActiveRelOnly>false</showActiveRelOnly>
            <hideUnconnectedEntities>false</hideUnconnectedEntities>
            <getParents>true</getParents>
            <getChildren>true</getChildren>
            <getUndirected>true</getUndirected>
            <getBidirectional>true</getBidirectional>
            <getUnknown>true</getUnknown>
        </hmFilter>
        <hmFilter name="filter2" displayName="Filter 2">
            <showActiveRelOnly>false</showActiveRelOnly>
            <hideUnconnectedEntities>false</hideUnconnectedEntities>
            <getParents>true</getParents>
            <getChildren>true</getChildren>
            <getUndirected>true</getUndirected>
            <getBidirectional>true</getBidirectional>
            <getUnknown>true</getUnknown>
            <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.member of account group
                </enabledRelationshipsUids>
            <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.employs</
enabledRelationshipsUids>
            <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.contains member 2
                </enabledRelationshipsUids>
            <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.customer
                </enabledRelationshipsUids>
            <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.contains member
                </enabledRelationshipsUids>
            <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.associate
                </enabledRelationshipsUids>
            <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.organization has
                </enabledRelationshipsUids>
            <enabledRelationshipsUids>HM_RELATIONSHIP_TYPE.is DNB parent of
                </enabledRelationshipsUids>
            <enabledHierarchiesUids>HM_HIERARCHY.Product</enabledHierarchiesUids>
            <enabledHierarchiesUids>HM_HIERARCHY.Customer</enabledHierarchiesUids>
            <enabledHierarchiesUids>HM_HIERARCHY.DNB</enabledHierarchiesUids>
        </hmFilter>
        <externalLinkAction callback="false" displayName="Graph Google Search"
                name="hm_google_search_action">
            <externalLink name="hm_google_search_link" type="IFRAME"
                    url="http://www.google.com/search">
                <param bddParamName="SELECTED_GRAPH_OBJECTS" name="q" />
                <param name="hl" staticValue="en" />
            </externalLink>
         </externalLinkAction>
        <externalLinkAction callback="true" displayName="Test graph callback"
                name="hm_test_callback_action">
            <externalLink name="hm_test_callback" type="IFRAME"
url="test_external_hm.html">
                <param bddParamName="USERNAME" name="username" />
                <param bddParamName="SELECTED_GRAPH_OBJECTS" name="selectedHmObjects" />
                <param bddParamName="ALL_GRAPH_OBJECTS" name="allHmObjects" />
            </externalLink>
        </externalLinkAction>
    </hmConfiguration>
```

Ajouter des relations

La Vue de hiérarchie peut être configurée pour être une vue en lecture seule.

L'utilisateur de l'application IDD peut naviguer parmi les relations, mais les relations ne peuvent pas être ajoutées ou éditées. L'attribut enableAddRel qui contrôle cela prend par défaut la valeur vrai. L'exemple ci-dessus montre comment désactiver les ajouts et éditions de relations.

Optimisation du rendu

IDD propose une riche visualisation pour les entités et relations dans la Vue de hiérarchie.

Lorsque la taille d'un graphe dans cette vue augmente pour atteindre des centaines, la durée de rendu de cette vue peut poser problème. IDD définit un seuil au-delà duquel les nœuds sont rendus de manière simplifiée, diminuant ainsi la durée de rendu. La valeur par défaut est 300, mais une configuration manuelle est possible à l'aide de l'attribut simpleNodeLimit.

Types de relations du gestionnaire de hiérarchies

Les mises en page, les fonctions de nettoyage et les sorties utilisateur peuvent être configurées pour les relations ajoutées ou éditées dans la Vue de hiérarchie.

Cette configuration est réalisée par type de relation. Il y a des colonnes standard pour chaque relation gérée automatiquement par IDD (type de hiérarchie et de relation, dates de début et de fin et références aux entités liées). La configuration avec l'élément hmRelationshipTypes spécifie tout attribut supplémentaire sur un enregistrement de relation.

Remarque: La relation de Hierarchy Manager définie comme relation de clé étrangère dans la Console Hub ne peut pas avoir de champs personnalisés ni de définition de mise en page dans IDD. Cette restriction est basée sur la nature de la relation de clé étrangère. Pour plus d'informations sur les relations de clés étrangères, consultez la section sur la configuration de relations de clés étrangères entre les objets de base dans le *Guide de configuration d'Informatica MDM Multidomain Edition*

Filtre du gestionnaire de hiérarchies

La Vue de hiérarchie comporte des filtres qui régissent l'affichage des types de hiérarchies et de relations, des directions des relations et d'autres éléments.

L'élément hmFilter sert à définir les paramètres de filtres qui peuvent être affectés comme paramètres de filtres par défaut pour une zone de sujet. Ce paramètre est utilisé tant qu'un utilisateur de l'application IDD n'a pas défini de filtre enregistré comme valeur par défaut pour cette zone de sujet.

Activation de relations inactives

Pour activer la possibilité pour l'utilisateur d'afficher les relations inactives dans Gestionnaire de hiérarchies, définissez `hmInactiveRelationshipsAvailable` sur `True`.

Pour ajouter ce paramètre à la base de données Oracle et définir le paramètre sur True, exécutez le script suivant :

```
insert into CMX_SYSTEM.C_REPOS_DS_PREF_DETAIL
(ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select 'INCTR', rowid_ds_pref, 'hmInactiveRelationshipsAvailable', 'true'
from CMX_SYSTEM.C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';
```

Enregistrements de la table de relations de la vue de hiérarchie

Définissez le nombre maximal d'enregistrements afin de limiter le nombre d'enregistrements de relations affichés par la table de relations de la vue de hiérarchie.

Le fichier `cmxserver.properties` contient le paramètre sif.api.hm.flyover.max.record.count. La valeur par défaut est 10 000.

Lorsque vous ne spécifiez pas de date effective dans la vue de hiérarchie, la table de relations affiche les enregistrements de relations effectifs et ineffectifs. De nombreux enregistrements de relations effectifs et

ineffectifs peuvent exister pour une entité donnée. Si le nombre total d'enregistrements de relations dépasse le nombre maximal d'enregistrements, Informatica Data Director affiche les enregistrements de relations les plus élevés dans l'ordre de tri. Informatica Data Director n'affiche pas les enregistrements de relations qui dépassent le nombre maximal d'enregistrements.

Lorsque vous spécifiez la date effective dans la vue de hiérarchie, la table de relations affiche toutes les relations effectives pour la date effective, indépendamment du nombre maximal d'enregistrements.

Vue de l'entité

Dans la Vue de hiérarchie, un utilisateur peut utiliser la commande Afficher les détails pour qu'une entité sélectionnée fasse apparaître une boîte de dialogue offrant une vue compacte de l'entité et de certains de ses enregistrements enfants.

Cet attribut compactViewChildrenNumber régit le nombre d'enregistrements enfants de chaque type à afficher (la valeur par défaut est 5).

Les types de colonnes et d'enfants affichés dans cette vue sont contrôlés par l'attribut showInHMCompactView sur les colonnes et objets enfants. Pour l'objet principal, showInHMCompatctView="true" doit être défini pour toute colonne à afficher. Pour les objets enfants, showInHMCompatctView="true" doit être défini pour tout objet à afficher. Si cet attribut n'est pas défini pour des colonnes de l'objet principal ou pour des enfants, seul le libellé de la zone de sujet apparaît dans cette boîte de dialogue.

```
<subjectArea name="Person">
        <primaryObject hmEntityTypeUid="Person">
            ...
            <layout columnsNum="3">
                <column columnUid="C_PARTY|NAME_PREFIX_CD" editStyle="FIELD"
                        horizontalStyle="SMALL"/>
                <column columnUid="C_PARTY|FIRST_NAME" editStyle="FIELD"
                        showInHMCompactView="true"
                        horizontalStyle="MEDIUM" required="true"/>
                <column columnUid="C_PARTY|MIDDLE_NAME" editStyle="FIELD"
                        showInHMCompactView="true"
                        horizontalStyle="MEDIUM"/>
                <column columnUid="C_PARTY|LAST_NAME" editStyle="FIELD"
                        showInHMCompactView="true"
                        horizontalStyle="MEDIUM" required="true"/>
                <column columnUid="C_PARTY|GENERATION_SUFFIX_CD" editStyle="FIELD"
                        horizontalStyle="SMALL"/>
                <column columnUid="C_PARTY|BIRTHDATE" editStyle="CALENDAR"
                        horizontalStyle="MEDIUM"/>
                </column>
            </layout>
            ...
            <one2ManyChild name="Email" type="ONE_2_ONE" uid="C_PARTY_ELECT_ADDR"
                showInHMCompactView="true"
                mpcUid="C_MT_ELECTRONIC_ADDRESS">
            </one2ManyChild>
            ...
        </primaryObject>
    </subjectArea>Subject Area settings
```

Les paramètres de l'objet principal décrits ici régissent le comportement par défaut lors de l'ouverture d'une Vue de hiérarchie avec une entité de ce type comme ancrage. Les attributs suivants peuvent être configurés.

Attribut	Description
hmManyHopLimits	Contrôle le graphe obtenu La valeur par défaut est un saut.
hmFilterName	Filtre initial à appliquer lors de l'affichage du graphe. Le nom doit être l'un des filtres définis dans les hmFilters décrits ci-dessus.
hmDefaultLayout	Mise à page à utiliser pour afficher le graphe. L'une des valeurs suivantes : hierarchy, taxonomy, tree, network, circular, explorerView.

```
<primaryObject hmEntityTypeUid="Person" hmFilter="filter1" hmDefaultLayout="tree">
        ...
        <hmManyHopLimits hops="3" relsPerEntity="50" totalRels="1000"/>
    </primaryObject>
```

Personnalisations

La Vue de hiérarchie peut être personnalisée des manières suivantes :

- Les sorties utilisateur exécutées lors de l'ajout ou de la modification de relations
- Les sorties utilisateur qui peuvent être appelées depuis le menu Plus d'actions
- Les actions personnalisées qui peuvent être appelées depuis le menu Plus d'actions et transmettre le contexte du graphe affiché

Extensions de l'interface utilisateur

Les extensions de l'interface utilisateur sont utilisées pour ajouter une fonctionnalité personnalisée à toute application IDD.

Élément	Description
uiExtensions	Peut être ajouté à la configuration pour ajouter des onglets de niveau supérieur et des extensions de l'Démarrer un espace de travail.
externalLinkChild	Peut être configuré pour ajouter des onglets enfants à un domaine.
externalLinkAction	Peut être configuré pour ajouter des actions à un domaine, à un enfant d'un domaine ou à des résultats de recherche.

Ces extensions sont appelées via une URL vers laquelle des paramètres peuvent être transmis. Ces paramètres peuvent inclure le nom d'utilisateur et le mot de passe pour l'utilisateur connecté. Ils peuvent être transmis en texte clair ou crypté via le cryptage symétrique Blowfish. Utilisez encryptionKey comme élément facultatif dans l'élément bddApplication.

```
<bddApplication xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      name="AppName"
      displayName="Application Name"
      defaultLocale="en"
      sessionTimeoutMinutes="30"
```

```
    xsi:noNamespaceSchemaLocation="./siperian-bdd-config-6.xsd">
  <encryptionKey>secretKey</encryptionKey>
  ...
</bddApplication>
```

Onglets de niveau supérieur de l'espace de travail

Par défaut, Informatica Data Director affiche trois onglets d'espace de travail de niveau supérieur : Démarrage, Données et Tâches.

Remarque: Vous ne pouvez pas désactiver les onglets par défaut Démarrage, Données et Tâches.

Il est possible de configurer des onglets supplémentaires contenant une page requise depuis une URL externe.

Onglets de niveau supérieur personnalisés

Vous pouvez ajouter des onglets de niveau supérieur personnalisés à Informatica Data Director.

Vous pouvez ajouter un onglet pour afficher un lien externe dans un iFrame. Vous ne pouvez pas utiliser iFrame sur des sites Web tels que Google et Facebook en raison de leur stratégie de confidentialité. Vérifiez que le lien externe corresponde à un site Web compatible avec iFrame.

L'exemple de code suivant ajoute une page de recherche Bing :

```
http://www.bing.com/search?q=bddUserName&hl=en

<bddApplication …>
    …
    <uiExtensions logicalOrsGroupName="CMX_ORS">
      <topLevelTab name="custom_bing_tab" displayName="Bing Search">
        <externalLink name="bing_username" type="IFRAME" url="http://www.bing.com/search"
            displayName="Bing search">
          <param name="q" bddParamName="USERNAME"/>
          <param name="hl" staticValue="en"/>
        </externalLink>
      </topLevelTab>
      …
    </uiExtensions>
    …
  </bddApplication>
```

Démarrez un espace de travail

Le Démarrer un espace de travail d'Informatica Data Director comporte trois types de composants : la liste de tâches (Mes tâches), les rapports et les composants personnalisés.

La liste des tâches est toujours disponible. Cette section décrit la configuration des composants personnalisés à l'aide de l'élément externalLink.

Par défaut, ces composants sont triés de la manière suivante liste de tâches, rapports et composants personnalisés. Leur ordre peut être modifié à l'aide de l'élément dashboardLayout décrit dans cette section. Les utilisateurs de l'application Informatica Data Director peuvent continuer à personnaliser l'ensemble des composants qu'ils verront, ainsi que l'ordre d'affichage de ces composants. Ces informations sont enregistrées dans les préférences de l'utilisateur.

Liens externes (Composants de l'espace de travail de démarrage personnalisé)

Les composants personnalisés sont définis à l'aide de l'élément externalLink.

Un élément externalLink permet l'affichage de toute page requise depuis une URL externe, ou un code HTML et JavaScript personnalisé.

L'extrait de code suivant est un exemple de composant personnaliséDémarrer un espace de travail. Deux paramètres sont transmis avec l'URL, tels que :

```
http://www.bing.com/search?q=bddUserName&hl=en
```

```
<bddApplication …>
    …
    <uiExtensions>
      …
      <dashboard>
        <externalLink name="bing_username" type="IFRAME" url="http://www.bing.com/search"
            displayName="Bing search">
          <param name="q" bddParamName="USERNAME"/>
          <param name="hl" staticValue="en"/>
        </externalLink>
        …
      </dashboard>
    </uiExtensions>
    …
  </bddApplication>
```

Paramètres de liens externes (statiques et dynamiques)

Il est possible de configurer un nombre illimité de paramètres pour l'URL spécifiée dans l'élément externalLink. Les paramètres peuvent être statiques ou dynamiques.

Paramètre	Description
Statique	Ont des valeurs prédéfinies spécifiées dans le fichier de configuration IDD. L'exemple suivant montre une définition de paramètre statique, qui utilise l'attribut staticValue : `<param name="hl" staticValue="en"/>`
Dynamique	Substitué lors de l'exécution. La définition d'un paramètre dynamique contient l'attribut bddParamName, et la valeur de cet attribut est remplacée par les données disponibles lors de l'exécution. Les paramètres dynamiques suivants sont pris en charge : - Nom de connexion de l'utilisateur de l'application IDD connecté (bddParamName="USERNAME") - Nom de connexion crypté de l'utilisateur de l'application IDD connectée(bddParamName="USERNAME_ENCRYPTED") - Mot de passe de l'utilisateur de l'application IDD connecté (bddParamName="PASSWORD") - Mot de passe crypté de l'utilisateur de l'application IDD connecté (bddParamName="PASSWORD_ENCRYPTED")

Composants des liens externes (IFRAME et IGOOGLE)

Deux types de composants externalLink sont pris en charge : IFRAME et IGOOGLE.

IFRAME

Les composants IFRAME (type= " IFRAME ") affichent une page demandée depuis une URL externe. Vous ne pouvez pas utiliser iFrame sur des sites Web tels que Google et Facebook en raison de leur stratégie de confidentialité. Vérifiez que le lien externe corresponde à un site Web compatible avec iFrame.

L'URL est construite à partir de la valeur spécifiée à l'aide de l'attribut url et des paramètres d'URL spécifiés.

L'extrait de code XML précédent définit un composant IFRAME, qui affiche une page requise à partir d'une URL générée dynamiquement. Cette URL est composée de la chaîne "http://www.bing.com/search", du paramètre statique nommé "hl", de la valeur "en", du paramètre dynamique nommé "q" et d'une valeur remplacée par le nom de l'utilisateur de l'application IDD actuellement connecté au moment de l'exécution.

Par exemple, si l'utilisateur de l'application IDD porte le nom de connexion 'admin', ce composant affiche une page requise à partir de l'URL suivante :

```
http://www.bing.com/search?q=admin&hl=en
```

IGOOGLE

Les composants IGOOGLE (type= " IGOOGLE ") sont utilisés pour intégrer le JavaScript importé depuis une URL externe (construite à partir de la valeur spécifiée à l'aide de l'attribut url et des paramètres d'URL spécifiés) et le code HTML personnalisé.

Un composant défini comme `' <externalLink name="component_name" type="IGOOGLE" url="<external URL>"/>'` ajoute un composant construit à partir d'une balise HTML unique<script> :Démarrer un espace de travail

```
<script url="external URL"/>
```

Démarrez la mise en page de l'espace de travail

Les composants du Démarrer un espace de travail sont disposés sur une grille - de haut en bas, de gauche à droite.

Par défaut, ces composants sont triés de la manière suivante liste de tâches, rapports et composants personnalisés.

Vous pouvez spécifier l'ordre par défaut à l'aide de l'élément dashboardLayout. Les utilisateurs de l'application IDD peuvent continuer à personnaliser l'ensemble des composants qu'ils verront, ainsi que l'ordre de ces composants. Il est enregistré dans les préférences de l'utilisateur.

La mise en page du Démarrer un espace de travail consiste en une grille avec *n* colonnes. Chaque élément peut occuper une ligne et une ou plusieurs cellules sur cette ligne. Il n'est pas nécessaire de placer des éléments dans toutes les cellules d'une ligne. Dans ce cas, le reste de la ligne sera vide.

L'extrait de fonctions suivant présente un exemple de mise en page de à deux colonnes Démarrer un espace de travail.

```
<dashboardLayout columns="2">
      <dashboardLayoutItem name="my_tasks" type="TASKS" columns="*"/>
                        <dashboardLayoutItem name="xref_composition"    type="REPORT" />
      <dashboardLayoutItem name="igoogle_visualization" type="EXTERNAL_LINK"/>
      <dashboardLayoutItem name="google_username" type="EXTERNAL_LINK"/>
  </dashboardLayout>
```

Chaque élément de la mise en page est représenté par l'élément dashboardLayoutItem, qui présente les attributs possibles suivants :

Paramètre	Type	Description
nom	chaîne	Identifiant d'élément unique à l'intérieur de l'élément dashboardLayout.
type	TASKS, REPORT ou EXTERNAL_LINK	Type de l'élément.
Colonnes	numéro ou "*"	Nombre de colonnes occupées par l'élément. La valeur par défaut est « 1 ». Il existe un symbole spécial "*" pour les éléments qui occupent la ligne entière.

L'ordre des éléments sur le Démarrer un espace de travail est l'ordre dans lequel ils sont spécifiés dans l'élément dashboardLayout.

Onglets enfants personnalisés

Les onglets enfants personnalisés peuvent être ajoutés à un domaine.

Ils apparaissent dans le même volet d'onglet que les onglets enfants un à plusieurs et plusieurs à plusieurs. Ils sont configurés à l'aide de l'élément externalLinkChild.

Les onglets enfants personnalisés de type externalLinkChild sont configurés pour afficher le contenu d'une page HTML requise depuis une URL externe. Voici un exemple de la définition externalLinkChild :

```
<subjectArea name="Organization" displayName="Organization">
      <primaryObject hmEntityTypeUid="Organization">
         <subTypeQualifier columnUid="C_PARTY|PARTY_TYPE" filterValue="Organization"/>
         <layout columnsNum="3">
               <column columnUid="C_PARTY|ORGANIZATION_NAME" editStyle="FIELD"
required="true"/>
         </layout>
      </primaryObject>
      <externalLinkChild name="org_name_bing_search_child" displayName="Bing Search">
         <externalLink name="org_name_bing_search_action_link" type="IFRAME"
            url="http://www.bing.com/search">
            <param name="q" bddParamName="C_PARTY|ORGANIZATION_NAME"/>
                        <param name="hl" staticValue="en"/>
         </externalLink>
      </externalLinkChild>
   </subjectArea>
```

Attributs des onglets enfants personnalisés

Les onglets enfants personnalisés sont définis à l'aide de l'élément externalLinkChild dans un domaine.

Cet élément présente les attributs suivants :

Attribut	Description
nom	Nom utilisé en interne de cet onglet d'enfant personnalisé. Il doit être unique parmi tous les onglets d'enfants personnalisés. Utilisez uniquement des caractères alphanumériques. Les caractères spéciaux ne sont pas autorisés.
displayName	Titre de l'onglet enfant. La valeur spécifiée dans la configuration XML est utilisé par défaut, mais il peut être ignoré dans le groupement des ressources.

Propriétés des liens externes

L'élément externalLinkChild doit contenir l'élément externalLink, qui définit l'URL affichée sous l'onglet enfant.

Cet élément présente les attributs suivants :

Attribut	Description
nom	Nom utilisé en interne de ce lien. Il doit être unique parmi tous les liens externes. Utilisez uniquement des caractères alphanumériques. Les caractères spéciaux ne sont pas autorisés.
type	Les liens externes définis pour les onglets enfants personnalisés doivent avoir le type "IFRAME".
url	URL affichée dans l'onglet enfant personnalisé.

Paramètres

Les paramètres peuvent être ajoutés à la fin de l'URL à l'aide de l'élément param. Les paramètres d'URL peuvent être statiques ou dynamiques.

Paramètres statiques

Les paramètres statiques ont des valeurs prédéfinies spécifiées dans la configuration.

L'exemple suivant montre une définition de paramètre statique, qui utilise l'attribut staticValue :

```
<param name="hl" staticValue="en"/>
<param name="loginName" bddParamName="USERNAME"/>
```

Paramètres dynamiques

Les valeurs des paramètres dynamiques sont remplacées lors de l'exécution.

La définition d'un paramètre dynamique contient l'attribut bddParamName, et la valeur de cet attribut est remplacée par les données suivantes disponibles lors de l'exécution :

- Nom de connexion de l'utilisateur de l'application IDD connecté (bddParamName="USERNAME")
- Nom de connexion crypté de l'utilisateur de l'application IDD connectée(bddParamName="USERNAME_ENCRYPTED")
- Nom de connexion crypté de l'utilisateur de l'application IDD connectée(bddParamName="USERNAME_ENCRYPTED")
- Mot de passe crypté de l'utilisateur de l'application IDD connecté (bddParamName="PASSWORD_ENCRYPTED")
- Colonne système 'ROWID_OBJECT' du PrimaryObject du domaine (bddParamName=" <primaryObject TableUID>|ROWID_OBJECT")
- Pour les PrimaryObjects dont la chronologie est activée, le format long en millisecondes de la date effective du domaine PrimaryObject (bddParamName="EffectiveDate")
- Données des colonnes du PrimaryObject du domaine (bddParamName=" < columnUid de la colonne PrimaryObject>")
- Données des colonnes des enfants un à un logiques du domaine (bddParamName=" < columnUid de la colonne enfant un à un de l'objet principal>")
- Vous pouvez spécifier les paramètres @LOCALHOST@ et @LOCALPORT@ dans le fichier de configuration d'Informatica Data Director. Lorsqu'une URL de rappel externalLinkAction vise une application déployée sur le même serveur que MDM Hub, vous devez spécifier le nom d'hôte local dans l'URL de façon

dynamique. Spécifiez dynamiquement le nom d'hôte local dans l'URL de sorte que la fenêtre externalLinkAction puisse interagir avec la fenêtre du navigateur Informatica Data Director sans restrictions de navigateur intersite. Le code suivant montre comment définir l'élément externalLinkAction avec le paramètre @LOCALHOST@ dans l'URL :

```
<externalLinkAction callback="false" displayName="View Lineage"
name="per_view_lineage">
<externalLink name="per_view_lineage_link" type="IFRAME" url="http://@LOCALHOST@:
10250/external_app "/>
</externalLinkAction>
```

Pour transmettre des noms d'utilisateurs et des mots de passe cryptés, vous devez définir la clé de cryptage. Vous devez définir la clé de cryptage dans le fichier de configuration IDD (IDDConfig.xml) à l'aide de l'élément `encryptionKey`.

L'exemple de code suivant montre comment définir l'élément `encryptionKey` :

```
<bddApplication xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                name="test"
                displayName="Test BDD application"
                defaultLocale="en"
                sessionTimeoutMinutes="30"
                xsi:noNamespaceSchemaLocation="siperian-bdd-config-6.xsd">
    <description>Description for test ds app configuration</description>
    <configSubVersion>2</configSubVersion>
    <encryptionKey>secretKey</encryptionKey>
...
...
                <externalLinkAction callback="true" displayName="Test callback"
name="person_test_callback_action">
                 <externalLink name="person_test_callback" type="IFRAME"
url="test_external.html">
                  <param bddParamName="SiperianRowID" name="SiperianRowID" />
                  <param bddParamName="EffectiveDate" name="date" />
                  <param bddParamName="USERNAME_ENCRYPTED" name="username" />
                  <param bddParamName="PASSWORD_ENCRYPTED" name="password" />
                  </externalLink>
                </externalLinkAction>
```

Par exemple, dans le fichier de configuration, vous pouvez définir la clé de cryptage IDD comme suit :

```
<encryptionKey>{C5869460-4830-4231-9D6E-8A073A97F099}</encryptionKey>
```

Actions personnalisées

Une *action personnalisée* est une requête HTTP appelée dans une fenêtre contextuelle de navigateur.

Les actions personnalisées peuvent être configurées pour les zones suivantes de l'application IDD :

- SubjectArea (définition d'action placée à l'intérieur de la définition SubjectArea). Ces actions personnalisées sont ajoutées dans le menu Plus d'actions du domaine (ce menu est disponible dans la Vue des données et la Vue de hiérarchie), et dans le menu contextuel affiché pour les nœuds dans la Vue de hiérarchie.
- Recherche de SubjectArea (définition d'action placée dans la définition de recherche de SubjectArea). Ces actions personnalisées sont ajoutées au menu contextuel des résultats de recherche.
- Enfants un à plusieurs et plusieurs à plusieurs (définition d'action placée à l'intérieur de la définition d'enfant). Ces actions personnalisées sont ajoutées au menu contextuel de la table enfant.
- Vue de hiérarchie (définition d'action placée à l'intérieur de la définition hmConfiguration). Ces actions personnalisées sont ajoutées au menu Plus d'actions dans la Vue de hiérarchie.

Remarque: Vous ne pouvez pas configurer les actions personnalisées en fonction des rôles utilisateur.

Les actions personnalisées sont définies à l'aide de l'élément externalLinkAction, qui présente les attributs suivants :

Attribut	Description
nom	Nom utilisé en interne de cette action personnalisée. Ce nom doit être unique parmi toutes les actions personnalisées.
displayName	Texte pour option de menu créé pour cette action personnalisée. La valeur spécifiée dans la configuration XML est utilisé par défaut, mais il peut être ignoré dans le groupement des ressources.
rappel	Cet attribut doit avoir la valeur 'vrai' pour l'action de rappel (vous trouverez ci-dessous une description des actions de rappel).
windowWidth	Largeur de la fenêtre modale qui affiche le résultat d'une action de rappel. La valeur par défaut est 700.
windowHeight	Hauteur de la fenêtre modale qui affiche le résultat d'une action de rappel. La valeur par défaut est 600.

L'élément externalLinkAction doit contenir un élément externalLink définissant l'URL de l'action personnalisée.

L'élément externalLink défini pour externalLinkAction prend en charge les mêmes paramètres que l'élément externalLink défini pour l'élément externalLinkChild. Pour plus d'informations, consultez la description de l'élément externalLink proposée sous « Onglets Enfant personnalisés » précédemment dans ce document.

Comme pour l'élément externalLink de l'onglet Enfant personnalisé, l'élément externalLink défini pour externalLinkAction prend en charge les paramètres dynamiques remplacés lors de l'exécution. Lorsque l'action est exécutée pour plusieurs enregistrements (par exemple, l'utilisateur de l'application IDD choisit dans les résultats de recherche plusieurs enregistrements et exécute une action depuis le menu contextuel de recherche) et qu'une URL d'action a un paramètre dynamique remplacé par des données des colonnes de l'enregistrement. La valeur du paramètre est construite à partir des valeurs des colonnes de tous les enregistrements sélectionnés, séparées par des virgules. Par exemple, une action est définie pour la Recherche Organisation avec la définition d'URL suivante :

```
<externalLink name="org_name_google_search_action_link" type="IFRAME"
         url="http://www.google.com/search">
      <param name="q" bddParamName="C_PARTY|ORGANIZATION_NAME"/>
      <param name="hl" staticValue="en"/>
   </externalLink>
```

Lorsque l'utilisateur de l'application IDD choisit dans les résultats de recherche trois organisations nommées 'name1', 'name2', 'name3' et exécute l'action, l'URL de l'action est la suivante :

```
http://www.google.com/search?q=name1,name2,name3&hl=en
```

Action personnalisée standard

Une action personnalisée standard ouvre une nouvelle fenêtre de navigateur affichant la page requise depuis une URL externe.

Voici un exemple d'action personnalisée définie pour SubjectArea :

```
<subjectArea name="Organization" displayName="Organization">
      <primaryObject hmEntityTypeUid="Organization">
         <subTypeQualifier columnUid="C_PARTY|PARTY_TYPE" filterValue="Organization"/>
         <layout columnsNum="3">
            <column columnUid="C_PARTY|ORGANIZATION_NAME" editStyle="FIELD"
required="true"/>
            …
```

```
         </layout>
      </primaryObject>
      <externalLinkAction name="org_name_google_search_action" displayName="Google
Search">
         <externalLink name="org_name_google_search_action_link"
               type="IFRAME" url="http://www.google.com/search">
            <param name="q" bddParamName="C_PARTY|ORGANIZATION_NAME"/>
                        <param name="hl" staticValue="en"/>
         </externalLink>
      </externalLinkChild>
      …
   </subjectArea>
```

Si l'utilisateur de l'application IDD ouvre une Organisation nommée 'Informatica' et sélectionne l'élément 'Recherche Google' dans le menu 'Plus d'actions', IDD ouvre une fenêtre affichant l'URL suivante :

```
http://www.google.com/search?q=Informatica&hl=en
```

Action personnalisée avec rappel

Une action personnalisée peut également inclure un rappel.

Ceci est utile lorsque le processus externe appelé par l'action personnalisée peut modifier des données dans la zone de sujet. Après cette modification, l'action personnalisée peut appeler le rappel pour indiquer à l'application IDD d'actualiser la zone de sujet.

IDD définit une fonction JavaScript nommée refreshObject pour actualiser la zone de sujet. Cette fonction nécessite un paramètre : l'identifiant IDD interne de l'enregistrement modifié. Pour rendre cet identifiant disponible pour les applications externes, la requête HTTP de l'action personnalisée doit le transmettre comme paramètre (dans ce cas, l'application externe peut obtenir cet identifiant d'une requête et le transmettre de nouveau à l'application IDD). Pour ajouter un identifiant d'enregistrement interne à l'URL d'une action, un paramètre d'URL dynamique avec bddParamName='SiperianRowID' doit être ajouté à la définition de l'URL (voir l'exemple d'une définition d'action de rappel plus loin dans cette section).

Lors de l'appel d'une action personnalisée de rappel, IDD ouvre une fenêtre modale contenant l'élément <iframe>, qui affiche la page HTML reçue suite à la requête HTTP de l'action. Cette page HTML permet d'appeler la fonction refreshObject à l'aide du code JavaScript suivant :

```
var modifiedRecordID = // get modified record ID from HTTP request
    var opener = window.parent.dialogArguments;
    opener.refreshObject(modifiedRecordID);
```

La fenêtre modale où apparaît le résultat de la requête de l'action est accessible depuis JavaScript comme window.parent. Par exemple, une page HTML générée en réponse à une action peut contenir la fonction JavaScript suivante, qui ferme la fenêtre modale de l'action et actualise les vues IDD :

```
function closeWindowAndRefreshBDD() {
      var modifiedRecordID = // get modified record ID from HTTP request
      var opener = window.parent.dialogArguments;
      opener.refreshObject(modifiedRecordID);
      window.parent.close();
   }
```

Remarque importante: En raison des restrictions de sécurité du navigateur, la page HTML peut appeler la fonction JavaScript définie dans l'application IDD uniquement si cette page est située dans le même domaine que l'application IDD (cette page est servie par le même serveur d'applications que celui où est déployée l'application IDD).

Voici un exemple de l'action de rappel définie pour SubjectArea :

```
<subjectArea name="Organization" displayName="Organization">
      <primaryObject hmEntityTypeUid="Organization">
         <subTypeQualifier columnUid="C_PARTY|PARTY_TYPE" filterValue="Organization"/>
         <layout columnsNum="3">
            <column columnUid="C_PARTY|ORGANIZATION_NAME" editStyle="FIELD"
required="true"/>
```

```
            …
         </layout>
      </primaryObject>
      <externalLinkAction callback="true" name="organization _callback_action"
            displayName="Org Callback">
         <externalLink      name="org_name_google_search_action_link"
               type="IFRAME" url="http://external/application/url">
            <param name="InternalID" bddParamName="SiperianRowID"/>
            <param name="organization_id" bddParamName="C_PARTY|ROWID_OBJECT"/>
         </externalLink>
      </externalLinkChild>
      …
</subjectArea>
```

Si un utilisateur d'application IDD ouvre une Organisation avec ROWID_OBJECT=1222 puis appelle cette action personnalisée, IDD ouvre une fenêtre modale affichant la page requise depuis l'URL suivante :

```
http://external/application/url?InternalID=BASE_OBJECT.C_PARTY|1222&organization_id=1222
```

Cette page peut ensuite appeler la fonction JavaScript refreshObject de l'application IDD avec le paramètre 'BASE_OBJECT.C_PARTY|1222' (il s'agit de l'identifiant interne de l'enregistrement Organisation ouvert), par lequel l'application IDD actualise toutes les vues ouvertes pour cet enregistrement.

Sécurité pour les extensions personnalisées

L'accès aux onglets enfants personnalisés et aux actions personnalisées est contrôlé via GAS.

Lors du déploiement d'une application IDD, des ressources personnalisées sont créées pour chaque onglet enfant personnalisé et chaque action personnalisée définis dans la configuration IDD. Les privilèges pour ces ressources doivent être configurés à l'aide de la Console Hub.

Onglets enfants personnalisés

Pour les onglets enfants personnalisés, les ressources sont nommées de la manière suivante :

```
CUSTOM_EXTENSION/CUSTOM_CHILD_TAB:<name>
```

où <*nom*> est le nom unique de l'onglet enfant spécifié dans la configuration.

Un onglet enfant personnalisé est visible si l'utilisateur de l'application IDD a des privilèges READ sur la ressource d'onglet correspondante.

Actions personnalisées

Pour les actions personnalisées, les ressources sont nommées de la manière suivante :

```
CUSTOM_EXTENSION/CUSTOM_ACTION:<name>
```

où <*nom*> est le nom unique de l'action spécifié dans la configuration.

Une action personnalisée est affichée et peut être exécutée si l'utilisateur de l'application IDD a le privilège EXECUTE pour la ressource d'action correspondante.

Sorties utilisateur

Les sorties utilisateur permettent d'ajouter une logique commerciale personnalisée aux opérations standard d'Informatica Data Director. Vous pouvez utiliser les sorties utilisateur dans l'espace de travail Données.

Les sorties utilisateur sont implémentées dans Java. Pour en savoir plus sur les interfaces utilisées pour implémenter les sorties utilisateur, consultez le Javadoc du fichier `siperian-bdd.jar` inclus dans le kit de ressources MDM Hub. Le kit de ressources contient également plusieurs exemples de sorties utilisateur. Ces exemples comprennent un projet Ant que vous pouvez utiliser comme modèle pour générer un fichier JAR de sortie utilisateur.

Sorties utilisateur et framework Entity 360

Les sorties utilisateur ne sont pas prises en charge dans les espaces de travail basés sur le framework Entity 360, tels que l'espace de travail **Début** et l'espace de travail d'entité.

Le framework Entity 360 vous permet d'utiliser des fonctions de nettoyage et la validation côté serveur pour remplacer certaines fonctionnalités des sorties utilisateur. Pour plus d'informations, consultez le *Guide de l'outil d'approvisionnement d'Informatica MDM Multidomain Edition*.

Remarque: pour bénéficier d'une compatibilité descendante, vous pouvez continuer à utiliser les sorties utilisateur avec l'espace de travail **Données**. Pour afficher l'espace de travail **Données**, activez la propriété `cmx.dataview.enabled` dans le fichier `cmxserver.properties`. Pour plus d'informations, consultez le *Guide de configuration d'Informatica MDM Multidomain Edition*.

Opérations de sorties utilisateur

Les sorties utilisateur disposent d'opérations et de points d'entrée définis.

Vous pouvez implémenter des sorties utilisateur pour chaque domaine afin d'ajouter une fonctionnalité personnalisée aux opérations suivantes :

- Enregistrer
- Envoyer pour approbation
- Opérations sur les tâches
- Fusionner
- Marquer comme Pas une correspondance
- Opérations personnalisées
- Relation d'enregistrement du gestionnaire de hiérarchies
- Opérations personnalisées du gestionnaire de hiérarchies
- Ouvrir

Le tableau suivant décrit les points d'entrée des sorties utilisateur disponibles pour chaque opération. Enregistrer, Envoyer pour approbation et Opérations de tâches sont des variations du processus

d'enregistrement des modifications apportées à la vue Données du domaine et fournissent le même ensemble de points d'entrée.

Opération	Point d'entrée	Description
Enregistrer, Envoyer pour approbation, Opérations de tâches	beforeValidation	**Remarque:** Ce point d'entrée n'est plus pris en charge. Utilisez à la place le point d'entrée beforeEverything.
	afterValidation	**Remarque:** Ce point d'entrée n'est plus pris en charge. Utilisez à la place le point d'entrée beforeEverything.
	beforeEverything	Appelé avant tout traitement. Utilisez ce point d'entrée pour procéder à la validation personnalisée ou à une augmentation des données dans le domaine. Informatica Data Director enregistre les modifications que la sortie utilisateur apporte aux données dans le domaine. Permet de signaler des erreurs, des avertissements et des confirmations. Permet de définir les dates de début et de fin d'une période. S'exécute en dehors de la transaction d'enregistrement.
	beforeSave	Appelé après la recherche de doublons, juste avant l'exécution de l'enregistrement composite. Utilisez ce point d'entrée pour exécuter la logique commerciale personnalisée qui augmente les données dans le domaine. Informatica Data Director enregistre les modifications que la sortie utilisateur apporte aux données dans le domaine. Permet de signaler des erreurs. S'exécute dans le cadre de la transaction d'enregistrement composite. Les demandes SIF soumises au stockage de référence opérationnelle (Operational Reference Store - ORS) font partie de cette transaction.
	afterSave	Appelé après l'enregistrement des modifications du domaine. Utilisez ce point d'entrée pour procéder à la maintenance des données qui ne font pas partie du domaine. Permet de signaler des erreurs qui annulent la transaction. S'exécute dans le cadre de la transaction d'enregistrement composite. Les demandes SIF soumises au stockage de référence opérationnelle (Operational Reference Store - ORS) font partie de cette transaction.
	afterEverything	Appelé une fois la transaction d'enregistrement terminée. Utilisez ce point d'entrée pour fournir des notifications utilisateur ou pour procéder à la maintenance des données qui ne font pas partie du domaine lorsque les modifications ne peuvent pas être exécutées dans le cadre de la transaction. Permet de signaler des avertissements. S'exécute en dehors de la transaction d'enregistrement.

Opération	Point d'entrée	Description
Fusionner	beforeEverything	Appelé avant tout traitement. Utilisez ce point d'entrée pour procéder à la validation personnalisée ou à une augmentation des données dans le domaine. Permet de signaler des erreurs, des avertissements et des confirmations. Permet de définir les dates de début et de fin d'une période. S'exécute en dehors de la transaction d'enregistrement.
	beforeMerge	Appelé juste avant l'exécution de la fusion. Utilisez ce point d'entrée pour exécuter la logique commerciale personnalisée afin de fournir des messages d'erreur ou de confirmation. Permet de signaler des erreurs. S'exécute dans le cadre de la transaction de fusion. Les demandes SIF soumises au stockage de référence opérationnelle (Operational Reference Store - ORS) font partie de cette transaction.
	afterMerge	Appelé lorsque l'opération de fusion est terminée. Utilisez ce point d'entrée pour procéder à la maintenance des données qui ne font pas partie du domaine. Permet de signaler des erreurs qui annulent la fusion. S'exécute dans le cadre de la transaction de fusion. Les demandes SIF soumises au stockage de référence opérationnelle (Operational Reference Store - ORS) font partie de cette transaction.
	afterEverything	Appelé une fois la transaction de fusion terminée. Utilisez ce point d'entrée pour fournir des notifications utilisateur ou pour procéder à la maintenance des données qui ne font pas partie du domaine lorsque les modifications ne peuvent pas être exécutées dans le cadre de la transaction. Permet de signaler des avertissements. S'exécute en dehors de la transaction.
Marquer comme Pas une correspondance	beforeEverything	Appelé avant tout traitement. Utilisez ce point d'entrée pour procéder à la validation personnalisée ou à une augmentation des données dans le domaine. Permet de signaler des erreurs, des avertissements et des confirmations. Permet de définir les dates de début et de fin d'une période. S'exécute en dehors de la transaction d'enregistrement.

Opération	Point d'entrée	Description
	beforeMarkNotAMatch	Appelé juste avant l'exécution de l'opération Pas une correspondance. Utilisez ce point d'entrée pour exécuter la logique commerciale personnalisée afin de fournir des messages d'erreur ou de confirmation. Permet de signaler des erreurs. S'exécute dans le cadre de la transaction Pas une correspondance. Les demandes SIF soumises au stockage de référence opérationnelle (Operational Reference Store - ORS) font partie de cette transaction.
	afterMarkNotAMatch	Appelé une fois l'opération Pas une correspondance terminée. Utilisez ce point d'entrée pour procéder à la maintenance des données qui ne font pas partie du domaine. Permet de signaler des erreurs qui annuleront la fusion. S'exécute dans le cadre de la transaction Pas une correspondance. Les demandes SIF soumises au stockage de référence opérationnelle (Operational Reference Store - ORS) feront partie de cette transaction.
	afterEverything	Appelé après la validation de la transaction Pas une correspondance. Utilisez ce point d'entrée pour fournir des notifications utilisateur ou pour procéder à la maintenance des données qui ne font pas partie du domaine lorsque les modifications ne peuvent pas être exécutées dans le cadre de la transaction. Permet de signaler des avertissements. S'exécute en dehors de la transaction.
Opération utilisateur	processOperation	Appelé lorsque l'utilisateur IDD appelle la sortie utilisateur de l'opération personnalisée depuis le menu Plus d'actions de la vue Données. Utilisez ce point d'entrée pour exécuter la logique commerciale personnalisée. La sortie utilisateur peut renvoyer des messages d'erreur ou d'avertissement. La vue Données est actualisée si cette sortie se termine sans erreur. Toutes les modifications apportées au domaine par la sortie utilisateur sont donc répercutées dans Informatica Data Director.
Relation d'enregistrement du gestionnaire de hiérarchies	beforeEverything	Appelé avant tout traitement. Utilisez ce point d'entrée pour procéder à la validation personnalisée ou à une augmentation de la relation. Permet de signaler des erreurs, des avertissements et des confirmations. Permet de définir les dates de début et de fin d'une période. S'exécute en dehors de la transaction d'enregistrement.

Opération	Point d'entrée	Description
	afterValidation	Appelé après l'exécution de la validation et de la fonction de nettoyage. Utilisez ce point d'entrée pour procéder à la validation personnalisée ou à une augmentation de la relation. Permet de signaler des erreurs, des avertissements et des confirmations. S'exécute en dehors de la transaction d'enregistrement.
	beforeSave	Appelé juste avant l'exécution de l'enregistrement. Utilisez ce point d'entrée pour exécuter la logique commerciale personnalisée qui augmente les données associées à la relation. Permet de signaler des erreurs. S'exécute dans le cadre de la transaction d'enregistrement. Les demandes SIF soumises au stockage de référence opérationnelle (Operational Reference Store - ORS) font partie de cette transaction.
	afterSave	Appelé après l'enregistrement des modifications de la relation. Utilisez ce point d'entrée pour procéder à la maintenance des données associées à la relation. Permet de signaler des erreurs qui annuleront l'enregistrement. S'exécute dans le cadre de la transaction d'enregistrement. Les demandes SIF soumises au stockage de référence opérationnelle (Operational Reference Store - ORS) font partie de cette transaction.
	afterEverything	Appelé une fois la transaction d'enregistrement terminée. Utilisez ce point d'entrée pour fournir des notifications utilisateur ou pour procéder à la maintenance des données associées à la relation lorsque les modifications ne peuvent pas être exécutées dans le cadre de la transaction. Permet de signaler des avertissements. S'exécute en dehors de la transaction d'enregistrement.
Opération utilisateur du gestionnaire de hiérarchies	processOperation	Appelé lorsque l'utilisateur IDD appelle la sortie utilisateur de l'opération personnalisée depuis le menu Plus d'actions de la vue Données. Utilisez ce point d'entrée pour exécuter la logique commerciale personnalisée. La sortie utilisateur peut renvoyer des messages d'erreur ou d'avertissement. La sortie utilisateur indique quelles parties du graphique doivent être actualisées suite à l'opération de la sortie utilisateur.

Opération	Point d'entrée	Description
Ouvrir	beforeOpen	Appelé avant l'exécution d'une opération ouverte. Utilisez ce point d'entrée pour marquer des colonnes comme étant en lecture seule en mode d'édition et pour remplacer les valeurs des colonnes. Permet de signaler des erreurs, des avertissements, des confirmations et des messages personnalisés. S'exécute en dehors de la transaction ouverte.
	afterOpen	Appelé une fois l'opération d'ouverture terminée. Utilisez ce point d'entrée pour envoyer différentes notifications aux données dans le domaine. Vous pouvez aussi l'utiliser pour une effectuer une vérification personnalisée des données chargées dans la base de données. Permet de signaler des erreurs, des avertissements, des confirmations et des messages personnalisés. S'exécute dans le cadre de la transaction ouverte. Les demandes SIF soumises au stockage de référence opérationnelle (Operational Reference Store - ORS) font partie de cette transaction.

Chaque sortie utilisateur comporte les données suivantes (décrites en détail dans le Javadoc) :

- les données du domaine qui fait l'objet d'opérations
- un objet SiperianClient pouvant être utilisé pour effectuer des opérations SIF sur la base de données du stockage de référence opérationnelle (Operational Reference Store - ORS), ainsi que l'identifiant du stockage de référence opérationnelle et les justificatifs d'identité de l'utilisateur à utiliser dans les demandes SIF
- données spécifiques à l'opération

Création de sorties utilisateur

Les étapes de base pour la création de sorties utilisateur pour une application IDD sont les suivantes :

1. Développer le code Java de la sortie utilisateur.
2. Compiler et créer un fichier JAR contenant les classes de sortie utilisateur.
   Utilisez `siperian-bdd.jar` depuis le kit de ressources MDM. Cette archive contient toutes les classes spécifiques à IDD et les définitions d'interface requises pour créer l'implémentation de sorties utilisateur. Pour en savoir plus, consultez le *Guide du kit de ressources de Informatica MDM Hub*.

   Remarque: Le fichier JAR doit porter le nom UserExitsImplementation.jar.
3. Utilisez le gestionnaire de configuration IDD pour importer le fichier JAR dans votre application IDD. Vous pouvez aussi inclure le fichier JAR dans un fichier ZIP de l'application IDD qui est importé.
4. Enregistrer les classes de sortie utilisateur avec la zone de sujet.
5. Déployer l'application IDD.

Configuration d'une sortie utilisateur

Les sorties utilisateur sont configurées par domaine.

Un domaine peut avoir des sorties utilisateur définies pour chaque opération de sortie utilisateur décrite précédemment dans cette section.

```
<subjectArea name="Organization" displayName="Organization">
      <primaryObject hmEntityTypeUid="Organization">
         <subTypeQualifier columnUid="C_PARTY|PARTY_TYPE" filterValue="Organization"/>
         <layout columnsNum="3">
            <column columnUid="C_PARTY|ORGANIZATION_NAME" editStyle="FIELD"
required="true"/>
            …
         </layout>
      </primaryObject>
      …
      <userExits className="com.siperian.bdd.userexits.sample.SaveHandler"/>
      <userExits className="com.siperian.bdd.userexits.sample.SendForApprovalHandler"/>
      <userExits className="com.siperian.bdd.userexits.sample.CustomActionProvider"
         actionName="Custom User Exit"/>
   </subjectArea>
```

L'extrait de code suivant est un exemple de configuration de ClassName pour les sorties utilisateur de la relation d'enregistrement du gestionnaire de hiérarchies dans le fichier IDDConfig.xml.

```
<hmRelationshipTypes>
<hmRelationshipType hmRelationshipUid="HM_RELATIONSHIP_TYPE.contains member">
<layout columnsNum="2">
<column columnUid="C_RL_PARTY_GROUP|HUB_STATE_IND" editStyle="FIELD"
horizontalStyle="MEDIUM"/>
</layout>
<userExit className="com.siperian.bdd.userexits.sample.HMRelationshipSaveHandler"/>
<userExit className="com.siperian.bdd.userexits.sample.HMRelationshipHandler"/>
</hmRelationshipType>
</hmRelationshipTypes>
```

Remarque: Vous ne pouvez pas configurer les sorties utilisateur en fonction des rôles utilisateur.

Messages des sorties utilisateur

Les sorties utilisateur peuvent renvoyer un message (tel qu'une erreur, un avertissement ou une confirmation) à afficher à l'utilisateur.

Ces messages sont traités par IDD de la même manière qu'il traite ses propres messages. Chaque message présente un code qui est une clé vers le groupe de ressources ErrorCodeBundle.properties. IDD trouve le niveau d'erreur (erreur, avertissement ou confirmation) et le texte du message dans ce groupe de ressources.

Remarque: Veillez à utiliser des codes uniques pour tout message personnalisé.

Ces chaînes de messages peuvent être localisées tout comme d'autres chaînes.

Les messages peuvent comporter des paramètres, qui sont remplacés par des données spécifiées dans la sortie utilisateur. Ces paramètres sont traités à l'aide de la classe Java MessageFormat.

Le format pour les messages dans ErrorCodeBundle.properties est :

```
error code=error level|title|main message[|secondary message]
```

où

Élément	Description
Code d'erreur	Clé unique pour le message.
Niveau d'erreur	L'une des valeurs suivantes : ERROR, WARNING ou CONFIRMATION.
Titre	Titre de la boîte de dialogue. Le titre doit décrire l'emplacement et le contexte dans lequel s'est produit le problème. En l'absence de spécification, le titre sera Informatica Data Director.
message principal	Message d'erreur principal. Ce texte doit décrire le problème du point de vue de l'utilisateur de l'application IDD, pas d'un point de vue technique interne. Par exemple, quelque chose comme `"Problème d'enregistrement xxx", pas "Erreur Put"`.
Message secondaire	Partie secondaire du message indiquant à l'utilisateur de l'application IDD que faire concernant le problème. Dans la boîte de dialogue, cette partie sera séparée du message principal par au moins une ligne vierge. Ce message ne doit pas être trop long.

Dépannage

Lorsque vous tentez de comprendre pourquoi une sortie utilisateur ne fonctionne pas correctement, utilisez les outils standard suivants.

Outil	Description
Journaux	Les exceptions générées dans la sortie utilisateur peuvent être trouvées dans les journaux Informatica MDM Hub. La sortie utilisateur peut également créer des entrées dans le journal à l'aide de log4j, comme illustré dans les modèles de sorties utilisateur.
Débogueur	Le débogueur Java peut être utilisé pour progresser dans l'exécution du code. Vous devez procéder comme vous le feriez pour déboguer toute application Java déployée dans un environnement de serveur d'applications.

Localisation

Les groupes de ressources contiennent les chaînes qui s'affichent dans une application Informatica Data Director.

Il existe quatre ensembles de groupes de ressources :

- BDDBundle
- ErrorCodeBundle
- MessagesBundle
- MetadataBundle

Chaque ensemble inclut le fichier par défaut, un fichier réservé en anglais et des versions localisées du fichier, le cas échéant.

Par exemple, l'ensemble MessagesBundle inclut le fichier par défaut `MessagesBundle.properties` et le fichier réservé en anglais `MessagesBundle_en.properties`.

Chaque fichier de groupe de ressources est un fichier de propriétés codé UTF-8. Chaque entrée dans le fichier est une paire nom/valeur, telle que <*nom*>=<*valeur*>.

- <*nom*> est une valeur fixe référencée par l'application Informatica Data Director. Vous ne pouvez pas la modifier.
- <*valeur*> est le composant que vous pouvez localiser.

Quelques exemples :

```
title=Business Data Director
locale=Locale
search=Search
```

Pour ajouter des fichiers de groupes de messages à l'application Informatica Data Director, vous pouvez les inclure dans le fichier .zip de l'application que vous importez. Vous pouvez aussi importer des fichiers de groupes de messages directement dans une application existante d'Informatica Data Director.

Remarque: Dans le fichier `MetadataBundle.properties` localisé, évitez les espaces dans les noms des types de relations et de hiérarchies du gestionnaire de hiérarchies. Informatica Data Director remplace les espaces par des traits de soulignement lorsqu'il affiche ces valeurs localisées.

Lorsque vous créez une application Informatica Data Director pour la première fois, le gestionnaire de configuration Informatica Data Director génère des groupes de ressources par défaut de chaque type. Ces groupes de ressources comportent des entrées pour tous les libellés utilisés dans l'application Informatica Data Director.

Pour modifier ou localiser ces groupes de ressources, effectuez les étapes suivantes :

1. Exportez l'application Informatica Data Director.
2. Extrayez les fichiers du fichier .zip de l'application.
3. Créez un groupe de ressources avec le suffixe de code de langue ISO approprié dans la langue sélectionnée.
4. Modifiez les libellés du groupe de ressources dans la langue sélectionnée.

   Remarque: Pour localiser les libellés des groupes de domaines, les noms des groupes de domaines et des groupes de menus logiques, utilisez le fichier `BDDBundle.properties` avec le suffixe de code de langue approprié.
5. Répétez les étapes 3 à 4 pour chaque groupe de ressources que vous voulez localiser.

Configuration de la langue d'affichage par défaut de la page de connexion et du gestionnaire de configuration

La langue de votre navigateur Web dicte la langue d'affichage de la page de connexion et du gestionnaire de configuration d'Informatica Data Director. Vous pouvez exécuter un script pour définir la langue de la page de connexion et de l'interface utilisateur du gestionnaire de configuration.

Le script ne définit pas la langue d'affichage par défaut de l'application Informatica Data Director. Vous pouvez définir la langue d'affichage de l'application Informatica Data Director dans l'option de menu Modifier la langue sous votre nom d'utilisateur. Lorsque vous définissez la langue d'affichage par défaut de la page de connexion et du gestionnaire de configuration, Informatica Data Director ignore les paramètres de langue de votre navigateur Web.

1. Exécutez le script suivant pour définir le code de langue du paramètre globalLocale :

```
INSERT
INTO CMX_SYSTEM.C_REPOS_DS_PREF_DETAIL
  (
    ROWID_DS_PREF_DETAIL,
```

```
    CREATE_DATE,
    CREATOR,
    LAST_UPDATE_DATE,
    UPDATED_BY,
    ROWID_DS_PREF,
    NAME,
    VALUE
  )
  VALUES
  (
    'MST1.5AB',
    sysdate,
    'admin',
    sysdate,
    'admin',(SELECT ROWID_DS_PREF
FROM CMX_SYSTEM.C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___'),
    'globalLocale',
    '<ISO language code>'
  );
```

Le code de langue ISO est un code à deux lettres qui représente la langue. Par exemple, le code de pays « ja » signifie japonais. Si vous ne définissez pas un code de langue ISO valide, la langue d'affichage est l'anglais.

2. Redémarrez le serveur d'application.

Pages d'erreur personnalisées

Vous pouvez configurer Informatica Data Director (IDD) pour qu'il affiche des pages d'erreur personnalisées plutôt que des messages d'erreur du serveur d'application. Par exemple, lorsqu'un utilisateur entre une URL incorrecte, vous pouvez configurer IDD pour qu'il redirige l'utilisateur vers la page de connexion ou vers une page d'erreur plus conviviale.

Pour créer des pages d'erreur personnalisées, modifiez le fichier `web.xml` et configurez la page de sorte qu'elle s'affiche lorsqu'une erreur se produit dans une session IDD.

Le fichier `web.xml` se trouve à l'emplacement suivant :

`<répertoire d'installation infamdm>/hub/server/siperian-mrm.ear/zds-gui.war`

Configuration d'une page d'erreur personnalisée

Pour créer des pages d'erreur personnalisées, modifiez le fichier `web.xml` et configurez la page qui doit s'afficher pour un code d'erreur spécifique.

1. Procédez à l'extraction des fichiers du répertoire `zds-gui.war`.

   Le répertoire contient plusieurs fichiers, dont web.xml.

2. Modifiez le fichier `web.xml` dans un éditeur de texte.
   Dans l'exemple suivant, la réponse HTTP 404 de l'application redirige l'utilisateur vers la page `error_custom.html`.

   ```
   <error-page>
   <error-code>404</error-code>
   <location>/error_custom.html</location>
   </error-page>
   ```

   Remarque: pour vous assurer que les utilisateurs accèdent à la page personnalisée, ajoutez la page `error_custom.html` au répertoire zds-gui.war.

3. Enregistrez les modifications apportées au fichier `web.xml` et redéployez l'application IDD.

Aide en ligne

Par défaut, une application Informatica Data Director (IDD) inclut l'aide du Guide de l'utilisateur. Vous pouvez également ajouter une aide personnalisée.

Aide du Guide de l'utilisateur

Le Guide de l'utilisateur décrit les tâches que vous pouvez effectuer dans une application IDD. Il vous explique par exemple comment ajouter ou fusionner des entités commerciales. Le développeur d'applications IDD peut remplacer le fichier d'aide fourni par un fichier d'aide révisé. Des versions localisées du fichier d'aide sont également disponibles. Si vous modifiez les paramètres régionaux d'une application IDD, l'aide s'affichera dans la langue définie.

Aide personnalisée

L'aide personnalisée décrit les entités commerciales ou les domaines définis dans l'application. Le développeur d'applications IDD crée l'aide personnalisée et l'ajoute à l'application.

Guide de l'utilisateur d'Informatica Data Director

Le Guide de l'utilisateur décrit les tâches que les utilisateurs professionnels peuvent effectuer dans une application Informatica Data Director (IDD). Il vous explique par exemple comment ajouter ou fusionner des entités commerciales.

Par défaut, une application IDD propose le Guide de l'utilisateur sous la forme d'un fichier d'aide en ligne. Le développeur d'applications IDD peut remplacer le fichier d'aide fourni par un fichier d'aide révisé. Les fichiers d'aide révisés sont disponibles sur le portail Mon support Informatica.

Téléchargement de fichiers d'aide révisés du Guide de l'utilisateur

Vous pouvez rechercher et télécharger des fichiers d'aide révisés du Guide de l'utilisateur sur le portail Mon support Informatica.

Remarque: l'organisation du portail Mon support évolue au fil du temps.

1. Dans un navigateur, accédez au portail Mon support Informatica.
2. Sélectionnez le produit **Master Data Management Multidomain Edition**.
3. Sélectionnez l'onglet **Documents du produit**.
4. Configurez les **filtres de document** pour rechercher des fichiers d'aide révisés pour votre version du produit.

Filtre	Description
Gamme de produits	Affiche **Master Data Management**.
Nom du produit	Affiche **MDM Multidomain Edition**.

Filtre	Description
Type de document	Sélectionne **Document du produit**.
Version du produit	Sélectionne la version du produit dans votre environnement, par exemple **10.0.0 HotFix 2**.
Catégorie	Sélectionne **Guide de l'utilisateur**.
Langue	Sélectionne la langue de l'aide (par exemple, **Anglais**).

Une liste de guides de l'utilisateur s'affiche.

5. Si l'**Aide du Guide de l'utilisateur d'Informatica Data Director** s'affiche, cela signifie qu'un fichier d'aide révisé est disponible. Cliquez sur le lien.
6. Notez le numéro de révision. Vous pouvez utiliser ce numéro pour vérifier que l'aide appropriée s'affiche.
7. Téléchargez le fichier d'aide.

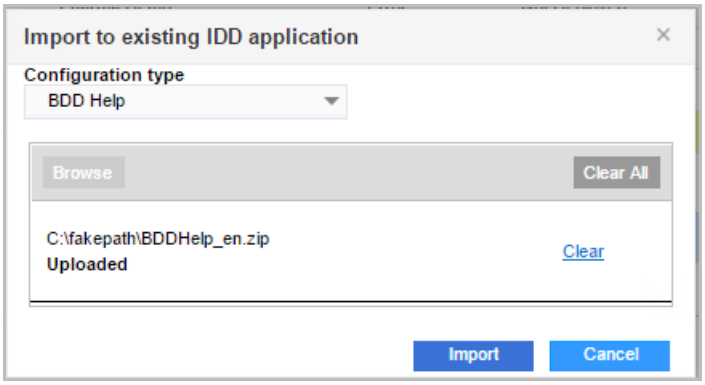
Importation d'un fichier d'aide révisé du Guide de l'utilisateur

Vous pouvez importer un fichier d'aide révisé dans vos applications IDD.

Le nom du fichier d'aide suit le format `BDDHelp_xx.zip`, où `xx` correspond à un code de langue ISO. Si vous prenez en charge plusieurs langues, importez les fichiers d'aide localisés de chaque langue. L'aide localisée s'affiche lorsqu'un utilisateur sélectionne les paramètres régionaux correspondants dans l'application IDD.

1. Connectez-vous au gestionnaire de configuration IDD.
2. Sélectionnez une application.
3. Cliquez sur **Importer** > **Importer dans l'application IDD existante**.
4. Dans la boîte de dialogue **Importer dans l'application IDD existante**, sélectionnez **Aide BDD** dans la liste **Type de configuration**.
5. Cliquez sur **Parcourir**.
6. Dans la boîte de dialogue **Ouvrir**, sélectionnez le fichier d'aide révisé et cliquez sur **Ouvrir**.

   L'image suivante montre la version anglaise du fichier d'aide prête à importer :



7. Cliquez sur **Importer**.

   Le processus d'importation met l'application à jour avec l'aide du Guide de l'utilisateur révisée.

Test de l'aide révisée

Lorsque vous importez un fichier d'aide révisé, ouvrez l'application et vérifiez que l'aide affiche le numéro de révision approprié.

1. Si l'application est ouverte, fermez-la.
2. Connectez-vous à Informatica Data Director.
3. Si vous y êtes invité, sélectionnez l'application qui contient l'aide révisée.
4. Dans le menu **Aide**, cliquez sur **Aide**.
5. Vérifiez que le numéro de révision en bas de la rubrique Bienvenue correspond au numéro du fichier d'aide que vous avez téléchargé.

Aide personnalisée

Vous pouvez créer une aide personnalisée décrivant les entités commerciales ou les domaines que vous avez définis dans l'application IDD. Après l'importation de l'aide personnalisée et le déploiement de l'application, l'élément de menu **Aide personnalisée** s'affiche dans le menu **Aide**.

Si vous prenez en charge plusieurs langues, vous pouvez créer des fichiers d'aide localisés pour chaque langue. Lorsqu'un utilisateur sélectionne les paramètres régionaux de son choix dans l'application IDD, il accède à l'aide personnalisée localisée.

Création d'un fichier d'aide personnalisée

Vous pouvez créer un fichier d'aide personnalisée pour documenter vos applications IDD. Si vous prenez en charge plusieurs langues, vous pouvez également créer des fichiers d'aide localisés pour chaque langue.

1. Créez les rubriques de l'aide personnalisée dans un outil de création HTML et générez le projet d'aide.
2. Remplacez le nom du fichier `index.htm` par `bdd_help_CSH.htm`.
3. Créez un répertoire nommé `bdd_help`.
4. Copiez les répertoires et fichiers d'aide générés dans le répertoire `bdd_help`.
5. Sélectionnez le répertoire `bdd_help` et créez un fichier .zip conservant la structure de répertoire.
6. Nommez le fichier .zip `CustomBDDHelp_xx.zip`, où `xx` correspond à un code de langue ISO à deux caractères.
7. Vérifiez que la taille du fichier `CustomBDDHelp_xx.zip` ne dépasse pas 20 Mo.

Importation d'un fichier d'aide personnalisée

Vous pouvez importer un fichier d'aide personnalisée dans des applications IDD. Si vous avez localisé l'aide personnalisée, importez également les fichiers d'aide localisés.

1. Connectez-vous au gestionnaire de configuration IDD.
2. Sélectionnez une application.
3. Cliquez sur **Modifier**.
4. Dans le panneau Éditer l'application, cochez la case **Aide personnalisée**, puis cliquez sur **Enregistrer**.

   Dans le fichier de configuration de l'application, la propriété `help` est mise à jour de manière à définir `customBddHelp` sur `true` :

   ```
   <help bddHelp="true" customBddHelp="true"/>
   ```

5. Dans l'arborescence de navigation, cliquez sur **Applications**.

   La liste des applications s'affiche.
6. Sélectionnez la même application.
7. Cliquez sur **Importer** > **Importer dans l'application IDD existante**.
8. Dans la boîte de dialogue **Importer dans l'application IDD existante**, sélectionnez **Aide BDD personnalisée** dans la liste **Type de configuration**.
9. Cliquez sur **Parcourir**.
10. Dans la boîte de dialogue **Ouvrir**, recherchez et sélectionnez le fichier `CustomBDDHelp_xx.zip` et cliquez sur **Ouvrir**.
11. Cliquez sur **Importer**.

    Le processus d'importation met l'application à jour avec le fichier d'aide personnalisée.
12. Cliquez sur **Redéployer**.

CHAPITRE 6

Génération de rapport

Ce chapitre comprend les rubriques suivantes :

- Présentation de la génération de rapport, 100
- Modèles de rapport, 100
- Mesures de rapport, 101
- Configuration de la connexion à la base de données du magasin de données, 102
- Configuration des paramètres de rapport, 103
- Mini-Data Warehouse, 103
- Activation de la génération de rapport sur le serveur Hub MDM, 104
- Configuration d'Informatica Data Director pour afficher les rapports, 104
- Configuration d'un accès aux rapports pour un rôle, 106

Présentation de la génération de rapport

Informatica Data Director affiche les rapports générés par Jaspersoft à partir des données de rapport fournies par un mini-Data Warehouse.

Un mini-Data Warehouse fournit les données représentées graphiquement par le logiciel Jaspersoft dans le Démarrer un espace de travail Informatica Data Director. Pour implémenter les rapports Jaspersoft, vous devez configurer la connexion de la base de données du mini-Data Warehouse, configurer les paramètres de rapport et configurer Informatica Data Director pour qu'il affiche les rapports.

Modèles de rapport

Vous pouvez utiliser les modèles de rapport disponibles dans le kit de ressources.

Les modèles de rapport suivants sont disponibles :

report1.jrxml

Modèle de graphique à barres.

report2.jrxml

Modèle de graphique en secteurs.

Les modèles de rapport se trouvent dans le kit de ressources aux emplacements suivants :

- Sous UNIX : `<infamdm installation directory>/hub/resourcekit/samples/BDD/jasperreports`
- Sous Windows : `<infamdm installation directory>\hub\resourcekit\samples\BDD\jasperreports`

Mesures de rapport

Vous pouvez afficher les rapports de plusieurs mesures afin de mieux connaître la composition de vos données et l'évolution de celles-ci dans le temps.

Les mesures suivantes sont disponibles :

- Mesures de système source
- Mesures de composition des références croisées
- Tendances de croissance du domaine

Mesures de système source

Les mesures de système source affichent la fréquence à laquelle chaque système source contribue aux enregistrements de références croisées.

Les administrateurs peuvent utiliser les mesures de système source pour afficher les rapports qui illustrent une distribution par participation du système source dans les enregistrements de références croisées d'un type de domaine principal. Par exemple, l'administrateur peut afficher la distribution des enregistrements avec au moins un enregistrement des références croisées participant à partir de quatre systèmes sources, tels que CRM, ERP, System et SalesForce pour le domaine Policyholder.

Utilisez`subject_area_growth_trend` en tant que nom du rapport pour configurer et remplir l'entrepôt de données pour ce rapport.

Mesures de composition des références croisées

Les mesures de composition des références croisées affichent la distribution des enregistrements de références croisées parmi les enregistrements de l'objet de base.

Les administrateurs peuvent utiliser des mesures de composition des références croisées pour générer des rapports affichant le nombre d'enregistrements de l'objet de base d'un type de domaine principal, qui consiste en un nombre spécifique d'enregistrements de références croisées. Par exemple, pour le domaine policyholder, l'administrateur peut afficher les distributions suivantes :

- Nombre d’enregistrements qui comporte un enregistrement des références croisées
- Nombre d’enregistrements qui comprend un à deux enregistrements des références croisées
- Nombre d’enregistrements qui comprend deux à trois enregistrements des références croisées
- Nombre d’enregistrements qui comprend trois à cinq enregistrements des références croisées
- Nombre d’enregistrements qui comprend cinq à dix enregistrements des références croisées
- Nombre d’enregistrements qui comprend au moins 10 enregistrements des références croisées

Utilisez`xref_composition_metric` en tant que nom du rapport pour configurer et remplir l'entrepôt de données pour ce rapport.

Tendances de croissance du domaine

Les tendances de croissance du domaine affichent l'augmentation du nombre d'enregistrements d'un domaine pour une période donnée.

Les administrateurs peuvent utiliser les tendances de croissance du domaine pour afficher les tendances de croissance d'un domaine principal. Par exemple, l'administrateur peut afficher la distribution des enregistrements MDM par type de domaine principal. Les utilisateurs peuvent ensuite afficher un domaine spécifique pour illustrer la tendance du nombre d'enregistrements pour ce type de domaine sur une période donnée.

Utilisez`subject_area_growth_trend` en tant que nom du rapport pour configurer et remplir l'entrepôt de données pour ce rapport.

Configuration de la connexion à la base de données du magasin de données

Avant de pouvoir générer des rapports ou remplir des graphes, vous devez configurer la connexion à la base de données du magasin de données.

1. Ouvrez une invite de commande.
2. Accédez au répertoire du magasin de données.
   - Sous Windows, accédez à `<répertoire d'installation infamdm>\resourcekit\data-mart`
   - Sous UNIX, accédez à `<répertoire d'installation infamdm>/resourcekit/data-mart`
3. Exécutez la commande suivante :

   ```
   java -jar populate_datamart.jar config
   ```
4. Saisissez C pour configurer la connexion de base de données.
5. Répondez aux invites décrites dans le tableau suivant :

Invite	Description
Nom de la connexion	Entrez un nom unique pour la connexion. Si le nom existe déjà, il est remplacé.
Type de connexion	Entrez le type de connexion au magasin de données. Actuellement, seul DB est pris en charge.
Fournisseur de base de données	Entrez la base de données à laquelle vous voulez vous connecter, par exemple Oracle ou IBM DB2.
Utilisateur	Entrez l'utilisateur de la base de données.
Mot de passe	Entrez le mot de passe de la base de données.
Jeton	Réservé pour un usage futur
Nom d'hôte	Entrez le nom d'hôte de la base de données.

Invite	Description
Port	Entrez le port de la base de données.
Nom de la base de données	Entrez le nom/SID de la base de données.

Configuration des paramètres de rapport

Avant de pouvoir générer des rapports, vous devez configurer les paramètres de rapport.

1. Ouvrez une invite de commande.
2. Accédez au répertoire du magasin de données.
   - Sous Windows, accédez à `<répertoire d'installation infamdm>\resourcekit\data-mart`
   - Sous UNIX, accédez à `<répertoire d'installation infamdm>/resourcekit/data-mart`
3. Exécutez la commande suivante :

   ```
   java -jar populate_datamart.jar config
   ```
4. Saisissez R pour configurer les paramètres de rapport.
5. Répondez aux invites décrites dans le tableau suivant :

Invite	Description
Nom du rapport	Nom unique du rapport. Si le nom existe déjà, il est remplacé. Vous devez indiquer l'un des noms de rapport définis dans le fichier *répertoire d'installation infamdm* >\resourcekit\data-mart\config\report-class-mapping.properties
ID de configuration du rapport	ID de configuration du rapport tel qu'il apparaît dans la table C_REPOS_RPT_CONFIG.
Nom de connexion au magasin	Nom de connexion utilisé pour se connecter au magasin de données. Spécifiez le nom du stockage de référence opérationnelle que vous utilisez pour générer les rapports.
Nom de connexion à la requête	Nom de connexion utilisé pour interroger la base de données. Spécifiez le nom du stockage de référence opérationnelle que vous utilisez pour générer les rapports.

Mini-Data Warehouse

Le mini-Data Warehouse contient les données de rapport que le logiciel de génération de rapport Jaspersoft utilise pour générer des rapports. Vous devez exécuter une commande pour remplir le mini-Data Warehouse avec les données de rapport.

Le mini-Data Warehouse est la table C_REPOS_RPT_DETAIL. Le logiciel de génération de rapport Jaspersoft utilise les données de cette table pour générer des rapports. Vous devez exécuter une commande pour remplir le mini-Data Warehouse avec les données de rapport. Vous pouvez exécuter une commande pour remplir le mini-Data Warehouse avec les données de tous les rapports ou vous pouvez spécifier un rapport.

Remplissage du magasin de données avec des données de rapport

Pour remplir le magasin de données avec les données de tous les rapports ou d'un rapport spécifique, exécutez une commande java.

1. Ouvrez une invite de commande.
2. Exécutez une commande java pour remplir le magasin de données.
   - Pour remplir le magasin de données avec les données de tous les rapports disponibles, exécutez la commande suivante :

     ```
     java -jar populate_datamart.jar
     ```
   - Pour remplir le magasin de données avec les données d'un rapport spécifique, exécutez la commande suivante :

     ```
     java -jar populate_datamart.jar exec <report name>
     ```

La table C_REPOS_RPT_DETAIL est remplie avec les données de rapport.

Activation de la génération de rapport sur le serveur Hub MDM

Pour activer la génération de rapport sur le serveur Hub MDM, copiez les fichiers .jasper dans le dossier approprié.

1. Créez un dossier intitulé `Rapports` dans le répertoire suivant :
   - Sous UNIX : *<répertoire d'installation infamdm>*/hub/server/resources
   - Sous Windows : *<répertoire d'installation infamdm>*\hub\server\resources
2. Copiez les fichiers modèles .jasper dans le dossier `Rapports`.

Configuration d'Informatica Data Director pour afficher les rapports

Modifier le fichier de configuration d'Informatica Data Director pour afficher les rapports dans Informatica Data Director.

Vous pouvez configurer les éléments reportDefinition et dashboardLayoutItem.

Définition de rapport

Les paramètres de définition de rapport associent le modèle de rapport à un stockage de référence opérationnelle et définissent le format du rapport.

Le tableau suivant décrit les attributs de `reportDefinition` :

Attribut	Description
nom	Identifiant de rapport Informatica Data Director.
displayName	Nom de rapport, tel qu'il s'affiche dans le gestionnaire de configuration Informatica Data Director.
modèle	Nom du fichier modèle *.jasper.
logicalOrsGroupName	Nom du groupe de stockages de référence opérationnelle logique défini pour l'application Informatica Data Director. Cet attribut définit la source de données du graphe standard en fonction d'un groupe de stockages de référence opérationnelle logique.
format	Format du rapport de sortie. Le format peut être `html` ou `image`.

Paramètres de rapport

Informatica Data Director envoie les paramètres de rapport au moteur de génération de rapport Jaspersoft.

Le tableau suivant décrit les attributs de `reportParam` :

Attribut	Description
Nom	Le nom du paramètre. Le modèle Jaspersoft requiert ce nom de paramètre.
Description	La description du rapport qui doit apparaître sur l'interface utilisateur. S'affiche dans l'interface utilisateur d'Informatica Data Director si l'attribut visible est `true`.
Type	Le type de données de rapport. Peut être une `date`, un `graphe` ou un `numéro`.
Valeur	La valeur associée au nom. La valeur peut être statique ou dynamique.
Visible	Détermine si le texte de la description s'affiche dans l'interface utilisateur d'Informatica Data Director. Si `true`, le paramètre est visible dans l'interface utilisateur d'Informatica Data Director. Si `false`, le paramètre est invisible dans l'interface utilisateur d'Informatica Data Director. La valeur par défaut est `false`.

Paramètres de rapport dynamiques

Vous pouvez spécifier des paramètres de rapport dynamiques pour le nom d'utilisateur et l'application Informatica Data Director ainsi que la date de début et la date de fin du rapport.

Les paramètres de rapport dynamiques commencent par « @ » et se terminent par « @ ». Informatica Data Director fournit les valeurs pour les paramètres de rapport dynamiques.

Le tableau suivant décrit les paramètres dynamiques que vous pouvez utiliser :

Nom	Type	Description
@p_user_name@	texte	Nom de l'utilisateur connecté à Informatica Data Director.
@p_bdd_name@	texte	Nom de l'application Informatica Data Director actuelle.
@p_start_date@	date	Année en cours moins 1.
@p_end_date@	date	Année en cours.

Exemple de définition de rapport

L'exemple de code suivant affiche une définition de rapport pour un rapport basé sur des mesures de composition des références croisées :

```
<bddApplication>

 <reports>
  <reportDefinition
    name=”xref_composition_metric”
    displayName=”Cross-reference Composition”
    format="image"
    template=”pie2d”
    logicalOrsGroupName=”DsUi1”>

    <reportParam name=”year” value=”2013” />
    <reportParam name=”user” value=”@p_user_name@” />

  </reportDefinition>
 </reports>

</bddApplication>
```

Configuration d'un accès aux rapports pour un rôle

Pour configurer un accès aux rapports pour un rôle, utilisez la console hub MDM afin d'autoriser le niveau d'accès aux rapports approprié pour chaque rôle.

1. Dans la console hub MDM, obtenez un verrou.
2. Dans l'espace de travail **Gestionnaire d'accès de sécurité**, sélectionnez l'outil **Rôles**.
3. Dans l'outil **Rôles**, sélectionnez le rôle dont vous voulez modifier l'accès aux rapports.
4. Sous **Ressources personnalisées**, dans l'onglet **Privilèges de ressource**, sélectionnez le nom de l'application Informatica Data Director.
5. Sous le nom de l'application Informatica Data Director, activez ou désactivez l'accès à la fonction pour la ressource **RAPPORT/affichage**. Cliquez sur **Enregistrer**.

CHAPITRE 7

Propriétés globales d'IDD

Ce chapitre comprend les rubriques suivantes :

- Références de propriétés globales Informatica Data Director, 107
- Mise à jour des propriétés globales, 114

Références de propriétés globales Informatica Data Director

La table ci-dessous liste les propriétés globales qui régissent le comportement d'exécution de toutes les applications Informatica Data Director (IDD) sur un serveur Hub unique.

La table décrit toutes les propriétés et leurs valeurs par défaut. Ces propriétés sont stockées dans la table CMX_SYSTEM.C_REPOS_DS_PREF_DETAIL. Si les propriétés ne sont pas définies, les valeurs spécifiées par défaut sont utilisées.

Important: Le serveur d'application doit être redémarré pour que les modifications des propriétés globales suivantes soient appliquées.

Propriété	Valeur par défaut	Utilisation
allowDsEmptyChildren	False	Détermine si les utilisateurs peuvent afficher les enregistrements enfants lorsque vous configurez un filtre de sécurité sur une colonne petit-enfant, alors qu'il n'existe pas d'enregistrements petits-enfants. Si cette option est définie sur la valeur `True`, les utilisateurs peuvent afficher les enregistrements enfants lorsqu'il n'existe pas d'enregistrements petits-enfants. Si cette option est définie sur la valeur `False`, les utilisateurs ne peuvent pas afficher les enregistrements enfants lorsqu'il n'existe pas d'enregistrements petits-enfants.
asyncChildLoading	False	Charge les données enfant dans la vue Données lorsque vous ouvrez explicitement l'enregistrement enfant de l'objet principal. Vous pouvez définir la valeur de propriété sur True pour charger les données enfants quand vous ouvrez l'enregistrement dans la vue Données.
credentialsAutofillDisabled	False	Pour des raisons de sécurité, si vous souhaitez contrôler l'enregistrement des justificatifs d'identité de connexion (tels que le nom utilisateur et le mot de passe) réalisé par le navigateur de l'utilisateur, vous pouvez définir cette valeur sur True.
CSVColumnSeparator	Virgule (,)	Détermine le caractère à utiliser comme séparateur de colonne lorsque vous exportez les données vers un fichier de valeurs séparées par des virgules (CSV). Vous pouvez également utiliser une tabulation, un point-virgule ou un espace comme délimiteur.
enableRememberCredentials	True	Avec la valeur True, la case Se souvenir de moi apparaît sur la page de connexion. Les utilisateurs restent connectés pendant la durée déterminée par rememberCredentialsPeriod

Propriété	Valeur par défaut	Utilisation
handleUserExitBeforeShowingDialog	False	Détermine le moment où IDD appelle la sortie utilisateur SendForApprovalHandler. Définissez cette option sur `True` afin que IDD appelle la sortie utilisateur SendForApprovalHandler lorsque l'utilisateur clique sur **Envoyer pour approbation**. Définissez cette option sur `False` pour que IDD appelle la sortie utilisateur SendForApprovalHandler lorsque l'utilisateur clique sur **OK** dans la boîte de dialogue **Envoyer pour approbation**.
HeaderBgColor	#000000	Spécifie le code de couleurs HTML de la couleur d'arrière-plan de la zone d'en-tête de l'IDD.
hmInactiveRelationshipsAvailable	False	Définissez cette option sur `True` afin que l'utilisateur puisse afficher les relations inactives dans le gestionnaire de hiérarchies.
IDD2COCSConverter.prefixCoNames	false	Lorsque la configuration d'Informatica Data Director est convertie en configuration d'entité d'entreprise, détermine si le nom de cette dernière correspond à un nom de domaine comportant un préfixe. Définissez cette propriété sur `false` pour utiliser le nom de domaine comme nom d'entité d'entreprise. Définissez-la sur `true` pour utiliser le nom de domaine précédé du nom de l'application Informatica Data Director comme nom d'entité d'entreprise.
isEffectiveDateIncluded	false	Spécifie si le champ Date d'effet doit être inclus pour les requêtes de recherche dans Informatica Data Director. Définissez cette option sur `true` pour afficher la date actuelle dans le champ Date d'effet. Définissez cette option sur `false` pour masquer le champ Date d'effet.
isFillOnGap	false	Spécifie s'il convient d'activer la propriété Éviter une discontinuité pour les opérations dans Informatica Data Director. Définissez sur `True` pour activer la propriété Éviter une discontinuité. Définissez sur `False` pour désactiver la propriété Éviter une discontinuité.

Propriété	Valeur par défaut	Utilisation
lookupCacheUpdatePeriod	300000 (5 min)	Le nombre de millisecondes pendant lequel les données de recherche peuvent être dans le cache IDD avant son rechargement.
maxCopiedChildrenNumber	10	Détermine, pour chaque type d'enfant, le nombre maximal d'enregistrements enfants copiés lorsqu'un utilisateur copie un domaine.
maxCopiedGrandChildrenNumber	10	Détermine, pour chaque type d'enfant, le nombre maximal d'enregistrements petits-enfants copiés lorsqu'un utilisateur copie un domaine.
maxImportThreads	5	Détermine le nombre maximal de threads à utiliser lors de l'importation de données.
maxParallelPromoteThreads	1	Détermine le nombre maximal de threads à utiliser lorsque vous approuvez une tâche. Lorsque maxParallelPromoteThreads est supérieur à 1 et que vous promouvez les enregistrements provenant de plusieurs objets de base, le processus de promotion s'exécute en parallèle. La valeur maximale de maxParallelPromoteThreads est égale au nombre de cœurs du processeur du serveur.
maxParallelISavedQueriesThreads	true	Détermine si les requêtes se chargent via plusieurs threads. Les requêtes multi-thread se chargent plus rapidement. Définissez sur `True` pour activer le multi-threading. Définissez cette propriété sur `False` pour désactiver le multi-threading.
maxParallelBvtThreads	1	Détermine le nombre maximal de threads à utiliser lorsque IDD charge une tâche à afficher.
maxSearchResultsExportedRows	5000	Nombre maximal de lignes de résultats de recherche qui seront exportées.
maxXrefSearchReturnCount	100	Spécifie le nombre maximal d'enregistrements de références croisées renvoyé par une demande de recherche.
needLoadChildOnOpen	False	Définissez cette propriété sur `true` pour résoudre les problèmes de faibles performances de correspondance lorsque le gestionnaire de hiérarchies est activé.

Propriété	Valeur par défaut	Utilisation
openDashboardAfterTaskClose	False	Définissez cette option sur `True` pour qu'Informatica Data Director ouvre le Démarrer un espace de travail lorsque vous avez terminé une tâche. Définissez cette option sur `False` pour qu'Informatica Data Director ouvre l'onglet précédent dans la vue Données lorsque vous avez terminé une tâche.
rememberCredentialsPeriod	24 (heures)	Durée (en heures) pendant laquelle les justificatifs d'identité de l'utilisateur restent mémorisés si la case Se souvenir de moi est cochée.
samCacheUpdatePeriod	600000 (10 min)	Détermine combien de temps (en millisecondes) les rôles SAM (ressources avec attributions de privilèges) peuvent rester dans le cache IDD avant d'être rechargés.
serverPageSize	100	Affecte la pagination des résultats de recherche et des données enfants. IDD affiche à l'utilisateur une page contenant 10 enregistrements. Toutefois, le nombre d'enregistrements obtenus depuis MDM Hub est déterminé par cette propriété. Avec le paramètre par défaut, IDD ne demandera pas de données supplémentaires avant que l'utilisateur n'arrive à la 11e page de données.
search_empty_date	False	Détermine si, lorsque vous créez un enregistrement enfant, le champ de date d'effet dans la boîte de dialogue de recherche est vide ou contient la date d'effet de la vue Données. Définissez cette option sur `True` pour que le champ de date d'effet soit vide. Définissez cette option sur `False` pour que la date d'effet de la vue Données s'affiche dans le champ de date d'effet.
searchForDuplicatesBeforeTaskDialog	False	Détermine si la boîte de dialogue **Doublons potentiels** apparaît avant ou après l'envoi d'une tâche pour approbation. Définissez cette option sur `True` pour que la boîte de dialogue **Doublons potentiels** apparaisse avant la boîte de dialogue **Créer une tâche**. Définissez cette option sur `False` pour que la boîte de dialogue **Doublons potentiels** apparaisse après que vous ayez cliqué sur **OK** dans la boîte de dialogue **Envoyer pour approbation**.

Propriété	Valeur par défaut	Utilisation
shouldDisableSearchFieldIfDependentFieldAbsence	False	Active ou désactive le champ de recherche dépendante sur le formulaire de recherche lorsque le champ de recherche parent n'est pas présent sur ledit formulaire ou s'il n'a pas de valeur. Définissez cette option sur `True` pour activer le champ de recherche dépendante sur le formulaire de recherche. Définissez cette option sur `False` pour désactiver le champ de recherche dépendante sur le formulaire de recherche.
showMatchedColumns	#DBF5EC	Indique le code de couleur HTML de la couleur qui identifie les colonnes correspondantes.
showShadowColumns	true	Spécifie si les colonnes cachées doivent s'afficher dans la vue Références croisées. Définissez sur `True` pour afficher les colonnes cachées. Définissez sur `False` pour masquer les colonnes cachées.
subjectAreaCopyDisabled	False	Détermine si les utilisateurs peuvent sélectionner Copier à partir du menu Actions d'un domaine pour copier ce domaine. Définissez cette option sur `True` afin de désactiver l'option permettant de copier un domaine. Définissez cette option sur `False` afin d'autoriser l'option permettant de copier un domaine.
table_default_width_key	-1	Détermine le pourcentage de la largeur minimale des colonnes de résultats de recherche.
tableMaxColumns	25	Détermine le nombre de colonnes visibles dans la vue de table des enregistrements enfants et petits-enfants. La valeur par défaut autorise 20 colonnes visibles et 5 colonnes masquées. Pour vous assurer d'avoir des colonnes visibles, spécifiez un nombre entier >5.

Propriété	Valeur par défaut	Utilisation
tabsExpandByDefault	s.o.	Détermine les enregistrements enfants qui sont développés par défaut dans la vue Données. Pour développer les enregistrements enfants par défaut dans la vue Données, indiquez le nom de chaque domaine entre virgules. Pour développer l'onglet **XREF** par défaut, indiquez `xref`. Pour développer l'onglet **Relations** par défaut, indiquez `hm_relationship`. Par exemple, pour développer par défaut les onglets XREF, Adresse d'expédition et Organisation, indiquez `xref, ShipAddress, Organization`. Si vous ne définissez aucune valeur pour tabsExpandedByDefault, aucun enregistrement enfant n'est développé par défaut dans la vue Données.
threadSchedulerIdleTime	5000 (secondes)	Détermine le thread planificateur du temps d'inactivité maximal.
transactionTimeout	30 (secondes)	Le nombre de secondes dont les transactions disposent pour terminer l'exécution avant l'expiration.
updateExistingPeriodByDefault	False	Détermine si la case Mettre à jour la période existante est activée par défaut. Définissez cette option sur `True` pour l'activer par défaut. Définissez cette option sur `False` pour la désactiver par défaut.
writeBOM	False	Exporte les résultats de recherche d'Informatica Data Director au format CSV à l'aide du codage UTF-8 avec une marque d'ordre d'octet. Si la recherche contient des caractères ASCII étendus, définissez writeBOM sur `True` pour voir des données valides lorsque vous ouvrez le fichier CSV.

LIENS CONNEXES :

- "Les métadonnées d'Informatica Data Director n'ont pas été mises à jour" à la page 187

Mise à jour des propriétés globales

Pour mettre à jour les propriétés globales, vous pouvez exécuter le script SQL suivant pour le schéma CMX_SYSTEM.

Le script SQL suivant, lorsqu'il est appliqué à CMX_SYSTEM, initialise les propriétés globales à l'aide de leurs valeurs par défaut. Mettez à jour le champ VALUE de ce script pour modifier ces valeurs.

```
insert into C_REPOS_DS_PREF_DETAIL
(ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
'BDDGP.1', rowid_ds_pref, ' asyncChildLoading', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
(ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
'BDDGP.2', rowid_ds_pref, 'credentialsAutofillDisabled', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
(ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
'BDDGP.3', rowid_ds_pref, 'CSVColumnSeparator', ','
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.4', rowid_ds_pref, 'enableRememberCredentials', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
(ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
'BDDGP.5', rowid_ds_pref, 'handleUserExitBeforeShowingDialog', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
    (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
    'BDDGP.6', rowid_ds_pref, 'HeaderBgColor', '#000000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
    (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
    'BDDGP.7', rowid_ds_pref, 'hmInactiveRelationshipsAvailable', 'false'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
     (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
     'BDDGP.8', rowid_ds_pref, 'IDD2COCSConverter.prefixCoNames', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.9', rowid_ds_pref, 'lookupCacheUpdatePeriod', '300000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';
```

```
insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.10', rowid_ds_pref, 'maxCopiedChildrenNumber', '10'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.11', rowid_ds_pref, 'maxCopiedGrandChildrenNumber', '10'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
    (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
    'BDDGP.12', rowid_ds_pref, 'maxImportThreads', '5'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.13', rowid_ds_pref, 'maxParallelPromoteThreads', '1'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.14', rowid_ds_pref, 'maxParallelBvtThreads', '1'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.15', rowid_ds_pref, 'maxSearchResultsExportedRows', '5000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.16', rowid_ds_pref, 'maxXrefSearchReturnCount', '100'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
     (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
     'BDDGP.17', rowid_ds_pref, 'openDashboardAfterTaskClose', 'false'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.18', rowid_ds_pref, 'rememberCredentialsPeriod', '24'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.19', rowid_ds_pref, 'samCacheUpdatePeriod', '600000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.20', rowid_ds_pref, 'search_empty_date', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.21', rowid_ds_pref, 'searchForDuplicatesBeforeTaskDialog', 'true'
```

```
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.22', rowid_ds_pref, 'serverPageSize', '100'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.23', rowid_ds_pref, 'shouldDisableSearchFieldIfDependentFieldAbsence', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.24', rowid_ds_pref, 'showMatchedColumns', '#DBF58C'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.25', rowid_ds_pref, 'subjectAreaCopyDisabled', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.26', rowid_ds_pref, 'table_default_width_key', '20'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.27', rowid_ds_pref, 'threadSchedulerIdleTime', '5000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.28', rowid_ds_pref, 'transactionTimeout', 300
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.29', rowid_ds_pref, 'updateExistingPeriodByDefault', 'true'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
   (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.30', rowid_ds_pref, 'writeBOM', 'false'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
   'BDDGP.31', rowid_ds_pref, 'isFillOnGap', 'false'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

insert into C_REPOS_DS_PREF_DETAIL
 (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE)
select
 'BDDGP.32', rowid_ds_pref, 'maxXrefSearchReturnCount', '1000'
from C_REPOS_DS_PREF where name = '___SYSTEM_PREFERENCES_ROOT___';

commit;
/
```

ANNEXE A

Exigences de plateforme et de dimensionnement

Cette annexe comprend les rubriques suivantes :

- Dimensionnement du serveur de base de données, 117
- Dimensionnement du serveur d'applications , 117
- Dimensionnement du client et du réseau, 117
- Configuration requise pour le navigateur, 118

Dimensionnement du serveur de base de données

Les déploiements IDD n'ont pas d'impact direct sur le dimensionnement du serveur de base de données.

Les exigences de la transaction IDD doivent être prises en compte lors de la définition de la section API du modèle de dimensionnement.

Dimensionnement du serveur d'applications

Une application IDD est exécutée sur le serveur d'applications et est colocalisée avec les autres composants du serveur Informatica MDM Hub.

Les serveurs d'applications doivent être dimensionnés pour autoriser 1 cœur de processeur / 1 Go de mémoire toutes les 10 sessions simultanées d'"utilisateurs lourds" IDD. L'utilisateur lourd, pour le modèle de dimensionnement, est défini comme un utilisateur de l'application IDD produisant une charge constante de 5 à 6 opérations IDD par minute.

Dimensionnement du client et du réseau

Voici les configurations minimales et recommandées pour les postes clients qui accèdent à Informatica Data Director :

Remarque: La résolution d'écran configurée pour Informatica Data Director est 1280 x 1024.

Paramètre	Valeur
CPU	Minimum : 1,6 GHz Recommandé : 2 GHz
Mémoire	Minimum : 1 Go Recommandé : 2 Go
Bande passante réseau efficace vers le serveur d'application	Minimum : 10 Mbits/s Recommandé : 100 Mbits/s

Pour obtenir plus d'informations sur les spécifications de produit et les plates-formes prises en charge, consultez la matrice de disponibilité de produits sur Informatica Network : https://network.informatica.com/community/informatica-network/product-availability-matrices/overview

Configuration requise pour le navigateur

Vous devez configurer le navigateur des machines clients pour qu'il autorise les cookies.

Désactivez le bloqueur de fenêtre pop-up si vous exécutez Informatica Data Director dans le navigateur Google chrome.

ANNEXE B

Composants de l'application

- Référence sur les composants de l'application, 119

Référence sur les composants de l'application

Une application IDD est conservée dans la base de données du système (CMX_SYSTEM.C_REPOS_DS_CONFIG) en tant que fichier ZIP contenant des fichiers de composants.

Ce fichier ZIP peut être exporté ou importé depuis et vers le gestionnaire de configuration IDD.

Nom du fichier	Utilisation
IDDConfig.xml	Fichier de configuration principal de l'application. Doit être conforme au schéma XML `siperian-bdd-config-6.xsd`.
BDDBundle.properties BDDBundle_XX.properties	Groupes de ressources avec les libellés des objets définis dans l'application IDD (tels que les domaines et les objets enfants).
MetadataBundle.properties MetadataBundle_XX.properties	Groupes de ressources avec les libellés des objets définis dans l'ORS (tels que les objets de base, les colonnes, etc.).
ErrorCodeBundle.properties ErrorCodeBundle_XX.properties	Groupes de ressources avec le texte des messages d'erreur générés par une application IDD.
MessageBundle.properties MessageBundle_XX.properties	Groupes de ressources avec le texte affiché dans l'application IDD.
BDDHelp.zip BDDHelp_XX.zip	Fichiers d'aide IDD génériques. Aide décrivant de manière générique les fonctions d'une application IDD.
CustomBDDHelp.zip CustomBDDHelp_XX.zip	Fichiers d'aide IDD personnalisés. Aide développée spécifiquement pour une application IDD donnée. Outre les instructions d'utilisation spécifiques à l'implémentation, ce fichier d'aide peut contenir des informations pertinentes telles que les procédures et stratégies d'une organisation.
logo.gif, logo.png, logo.jpg ou logo.jpeg	Substitut au logo que l'application IDD affiche en haut à gauche de l'écran. Le format du logo d'Informatica est de 147 pixels de large sur 31 pixels de haut. Pour des résultats optimaux, le logo de remplacement doit posséder des dimensions identiques.

ANNEXE C

Configuration de la sécurité IDD

- Référence sur la configuration de la sécurité IDD, 120

Référence sur la configuration de la sécurité IDD

Les tableaux suivants présentent les paramètres de configuration de la sécurité IDD. Vous pouvez définir des autorisations dans la console Hub à l'aide du gestionnaire d'accès de sécurité.

Astuce: le gestionnaire d'accès de sécurité comprend les groupes de ressources suivants : ALL_GLOBAL_RESOURCES, ALL_XREF et ALL_XREF_HISTORY. Utilisez ces groupes pour attribuer la même autorisation à toutes les ressources spécifiées. Vous pouvez par exemple cocher la case DELETE sur la ligne ALL_XREF pour définir l'autorisation DELETE sur toutes les références croisées.

Tableau 1. Général

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
Nouveau domaine de la barre d'outils	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objet de base principal et un à un logiques	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		O	O	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	O	-

Tableau 2. Vue Données

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
Création de domaine	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objet de base principal et un à un logiques	O	-	-	-	-	-
	BASE_OBJECT	NAME	-		-	O	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	O	-	-	-	-

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
Lecture de domaine	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objet de base principal et un à un logiques	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		-	O	-	-	-	-
Mise à jour de domaine	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objet de base principal et un à un logiques	-	O	O	-	-	-
	BASE_OBJECT	NAME	-		-	O	O	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	O	-
Suppression de domaine	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objet de base principal, gestion d'état activée	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		-	-	-	O	-	-
Copie de domaine	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objet de base principal et un à un logiques	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		O	O	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	O	-
Affichage des colonnes système de l'objet de base	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	L'objet de base n'est pas nouveau.	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		-	O	-	-	-	-
Création d'objet enfant	BASE_OBJECT	NAME	-	Pour les enfants un à plusieurs, seul l'objet de base lui-même est vérifié ; pour les enfants plusieurs à plusieurs, l'objet de base et sa relation sont vérifiés.	O	O	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME		-	-	-	-	O	-
Lecture d'objet enfant	BASE_OBJECT	NAME	-	-	-	O	-	-	-	-
Mise à jour d'objet enfant	BASE_OBJECT	NAME	-	Pour les enfants un à plusieurs, seul l'objet de base lui-même est vérifié ; pour les enfants plusieurs à plusieurs,	-	-	O	-	-	-

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME	l'objet de base et sa relation sont vérifiés.	-	-	-	-	O	-
Suppression d'objet enfant	BASE_OBJECT	NAME	-	Gestion d'état activée. Pour les enfants un à plusieurs, seul l'objet de base lui-même est vérifié ; pour les enfants plusieurs à plusieurs, l'objet de base et sa relation sont vérifiés.	-	-	-	O	-	-
	BASE_OBJECT	NAME	XREF	Les références croisées de l'objet enfant doivent être sélectionnées.	-	-	-	O	-	-
	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Paramètre requis lorsque vous utilisez la vue Entité.	-	O	-	-	O	-

Tableau 3. CM

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
Affichage des références croisées	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	L'objet de base n'est pas nouveau.	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		-	O	-	-	-	-

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
	BASE_OBJECT	NAME	XREF	Objet de base principal et tous les un à un logiques. Pour les enfants un à plusieurs, seul l'objet de base enfant. Pour les enfants plusieurs à plusieurs, l'objet de base enfant et sa relation.	-	O	-	-	-	-
Recherche de doublons	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		-	O	-	-	-	-
Fusionner	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	O	-	-	-	O
	BASE_OBJECT	NAME	-		-	-	-	-	-	O
Annuler la fusion	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		-	-	-	-	-	O
Affichage des données brutes	BASE_OBJECT	NAME	RAW	-	-	O	-	-	-	-

Tableau 4. Tâches

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
Envoi pour approbation (nouvel objet principal)	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objet de base principal et tous les un à un logiques, la gestion d'état est activée	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		O	O	-	-	-	-
	BASE_OBJECT	NAME	-	Objets plusieurs à plusieurs, la gestion d'état est activée	O	O	-	-	-	-

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME	Objet de base principal et tous les un à un logiques	-	-	-	-	O	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	Valeur par défaut pour approbation	O	-	-	-	-	-
Envoi pour approbation (objet principal existant)	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objet de base principal et tous les un à un logiques, la gestion d'état est activée	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		-	O	O	-	-	-
	BASE_OBJECT	NAME	-	Objets plusieurs à plusieurs, la gestion d'état est activée	-	O	O	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME	Objet de base principal et tous les un à un logiques	-	-	-	-	O	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	Valeur par défaut pour approbation	O	-	-	-	-	-
Tâche Envoyer pour approbation	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Les boutons Envoyer pour approbation et Modifier sont activés pour un enregistrement nouvellement créé. Le bouton Enregistrer est désactivé.	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		O	O	O	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ ReviewNoApprove		O	-	-	-	-	-
Ouverture de la tâche à partir de Démarrer un espace de travail	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		-	O	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA		-	-	-	-	O	-
Créer une tâche	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objet de base principal et tous les un à un logiques, la	-	O	-	-	-	-

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
	BASE_OBJECT	NAME	-	gestion d'état est activée	-	O	-	-	-	-
	BASE_OBJECT	NAME	-	Objets plusieurs à plusieurs, la gestion d'état est activée	-	-	-	-	-	-
	CLEANSE_FUNCTION	LIB_NAME	FUNCTION_NAME	Objet de base principal et tous les un à un logiques	-	-	-	-	O	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	Tout type de tâche de création	O	-	-	-	-	-
Affichage des détails de la tâche	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	O	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA	-	-	-	-	-	O	-
Fusion de la tâche	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	O	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ Merge		O	-	-	-	-	-
Annulation de la fusion de la tâche	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	O	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ Unmerge		O	-	-	-	-	-
File d'attente pour la fusion	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Le bouton File d'attente pour la fusion est activé.	-	O	O	-	-	O
	BASE_OBJECT	NAME	-		-	O	-	-	-	O
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA/ Merge		-	-	-	-	O	-
Action Exécuter la tâche	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	O	-	-	-	-
	CUSTOM_RESOURCE	BDD_NAME	TASK_TYPE:SA		-	-	-	-	O	-

Tableau 5. Vue Historique

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
Affichage de l'historique du domaine	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Persistance de l'objet de base principal,	-	O	-	-	-	-

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
				l'historique est activé pour l'objet de base principal.						
Vue Historique de l'objet principal	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Objet de base principal et tous les un à un logiques.	-	O	-	-	-	-
	BASE_OBJECT	NAME	HISTORY		-	O	-	-	-	-
	BASE_OBJECT	NAME	-	L'historique doit être activé pour l'objet de base.	-	O	-	-	-	-
Vue Historique pour l'objet de base enfant	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	Les privilèges sont pris en compte pour les relations enfants plusieurs à plusieurs.	-	O	-	-	-	-
	BASE_OBJECT	NAME	HISTORY		-	O	-	-	-	-
	BASE_OBJECT	NAME	-	L'historique doit être activé pour l'objet de base.	-	O	-	-	-	-
Affichage de l'historique des références croisées de l'objet de base	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	L'historique doit être activé pour l'objet de base.	-	O	-	-	-	-
	BASE_OBJECT	NAME	XREF_HISTORY		-	O	-	-	-	-
	BASE_OBJECT	NAME	-		-	O	-	-	-	-
Affichage de l'historique des fusions de l'objet de base	CUSTOM_RESOURCE	BDD_NAME	SUBJECT_AREA	-	-	O	-	-	-	-
	BASE_OBJECT	NAME	-		-	O	-	-	-	-

Tableau 6. Graphes

Cas d'utilisation	Groupe de ressources	Nom	Sous-nom	Exigences spéciales / commentaires	C	R	U	D	E	M
Affichage du graphe	CUSTOM_RESOURCE	BDD_NAME	CHART/ View	-	-	O	-	-	-	-

ANNEXE D

Sécurité des données

Cette annexe comprend les rubriques suivantes :

- Présentation de la sécurité des données, 127
- Appliquer la sécurité des données, 130

Présentation de la sécurité des données

La sécurité des données est la protection des données contre leur accès accidentel ou non autorisé, leur modification, leur corruption, leur destruction, leur duplication ou leur divulgation pendant les opérations telles que l'entrée, le traitement, le stockage, la transmission et la sortie et le contrôle de l'accès aux données de manière appropriée.

La sécurité des données IDD garantit que les données sont accessibles aux utilisateurs selon les critères suivants :

- Rôle utilisateur
- Configuration de la sécurité des données
- Données stockées dans le hub

Sécurité des données à l'aide de filtres

La sécurité des données dans Informatica Data Director est configurée en utilisant la boîte de dialogue **Domaine** dans le gestionnaire de configuration Informatica Data Director. Vous pouvez définir des filtres sur la colonne du domaine pour restreindre et sécuriser les données du domaine auxquelles les utilisateurs individuels peuvent accéder. Des filtres peuvent être définis sur une colonne d'objet principal, une colonne enfant et une colonne petit-enfant. Vous pouvez configurer n'importe quelle quantité de filtres pour une colonne de domaine et une colonne de groupe de domaines.

La sécurité des données Informatica Data Director prend en charge les types de valeurs suivants pour les filtres de sécurité dans le type de colonne de la table dans la base de données :

- Chaîne
- Entier
- Flottant

Remarque: La valeur de colonne de table de type Date n'est pas prise en charge par les filtres de sécurité des données d'Informatica Data Director.

Pensez aux règles et directives suivantes lors de l'utilisation des filtres :

- Chaque filtre de sécurité est défini sur les colonnes dans le domaine et consiste en une valeur de filtre à appliquer à une liste de rôles.
- Les filtres de sécurité sont basés sur des valeurs exactes et non sur des plages ou des comparaisons de caractères génériques.
- Les filtres doivent être définis sur les colonnes de correspondance pour appliquer les filtres de sécurité de manière cohérente dans les recherches de base, étendues et avancées.
- Les filtres peuvent être combinés - des combinaisons de filtres peuvent être appliquées à un utilisateur disposant de plusieurs rôles. Le résultat est que l'utilisateur a accès à toutes les données disponibles dans chaque rôle affecté à travers une union des affectations de filtres.
- Les filtres sur différentes colonnes peuvent être associés pour créer une sécurité des données multidimensionnelle.
- Plusieurs filtres sur une seule colonne pour un seul rôle. Un utilisateur a accès à une union de toutes les données qui répondent à chaque filtre.
- Filtres sur plusieurs colonnes pour un seul rôle. Un utilisateur a accès à l'intersection de toutes les données qui répondent à chaque filtre.
- Dans les environnements IBM DB2, les filtres des colonnes avec un type de données flottant ne filtrent pas au-delà de l'étendue de la colonne. Par exemple, si l'étendue de la colonne est 1 et que vous définissez le filtre sur 1.2, les valeurs qui se trouvent au-delà de l'étendue de la colonne, par exemple 1.21, sont également accessibles.

Pour plus d'informations, consultez l'*aide en ligne* du gestionnaire de configuration.

Paramètres de sécurité des données

Pour restreindre les données auxquelles les utilisateurs appartenant à un rôle particulier peuvent accéder, vous pouvez configurer les paramètres de sécurité des données dans le fichier `BDDConfig.xml`.

Vous pouvez configurer les paramètres de sécurité des données suivants :

securityFilter

Indique la colonne utilisée par Informatica Data Director (IDD) pour filtrer. L'attribut « columnUid » indique l'ID de la colonne ou le chemin de correspondance.

securityValue

Indique la valeur qui doit apparaître dans la colonne securityFilter pour que l'utilisateur soit autorisé à afficher les données d'un enregistrement.

securityRole

Indique le rôle auquel le filtre de sécurité s'applique. L'attribut « roleID » indique l'ID du rôle dont l'accès est limité par le filtre de sécurité des données.

Exemple de configuration d'un objet parent pour la sécurité des données

Vous devez configurer la sécurité dans le fichier `BDDConfig.xml` de sorte que les gestionnaires de données puissent voir le contenu qui s'applique à leur pays. Les gestionnaires de données en France doivent pouvoir

afficher les enregistrements parent dont la valeur Pays est « FR », et les gestionnaires de données au Japon, ceux dont la valeur Pays est « JA ».

Pour filtrer en fonction de l'emplacement du gestionnaire de données, créez un rôle pour chaque région dans MDM Hub. Dans cet exemple, vous attribuez le rôle « DSFrance » aux gestionnaires de données situés en France, et le rôle « DSJapan » à ceux situés au Japon.

L'extrait du fichier `BDDConfig.xml` exposé ci-dessous montre comment configurer la sécurité des données pour cet exemple :

```
<dataSecurity>
  <securityFilter columnUid="COUNTRY">
    <securityValue value="FR">
      <securityRole roleUid="DSFrance"/>
    </securityValue>
    <securityValue value="JA">
      <securityRole roleUid="DSJapan"/>
    </securityValue>
  </securityFilter>
</dataSecurity>
```

Exemple de configuration d'un objet petit-enfant pour la sécurité des données

Vous souhaitez que les gestionnaires de données situés en France puissent afficher les enregistrements enfants et petits-enfants lorsque la valeur de la colonne « Pays » de l'enregistrement petit-enfant C_MT_ADDRESS est « FR ».

Pour filtrer en fonction de l'emplacement du gestionnaire de données, créez un rôle pour les gestionnaires de données situés en France dans MDM Hub. Dans cet exemple, vous attribuez le rôle « DSFrance » aux gestionnaires de données situés en France. Utilisez le composant de chemin de correspondance de l'objet petit-enfant lorsque vous spécifiez la valeur « columnUid ».

L'extrait du fichier `BDDConfig.xml` exposé ci-dessous montre comment configurer la sécurité des données pour cet exemple :

```
<subjectArea name=”Organization”>
  <one2ManyChild name="Employee">
    <dataSecurity>
      <securityFilter columnUid="MATCH_PATH_COMPONENT.C_MT_ADDRESS|COUNTRY">
        <securityValue value="RUS">
          <securityRole roleUid="DSFrance"/>
        </securityValue>
      </securityFilter>
    </dataSecurity>
    <one2ManyChild name="Address" mpcUid="C_MT_ADDRESS">
    </one2ManyChild>
  </one2ManyChild>
</subjectArea>
```

Par défaut, les utilisateurs ne peuvent pas afficher l'enregistrement enfant si vous définissez un filtre pour une colonne petit-enfant, mais que l'enregistrement enfant n'a pas d'enregistrements petits-enfants. Pour permettre aux utilisateurs d'afficher des enregistrements enfants sans enregistrements petits-enfants, définissez la propriété globale « allowDsEmptyChildren » sur `True`.

Appliquer la sécurité des données

La sécurité des données fournit une solution de protection des données organisationnelles, telles que les données transactionnelles, historiques, dynamiques, hiérarchiques et statiques que les entreprises acquièrent, stockent, créent, suppriment et mettent à jour afin de mener des processus métier.

Dans une application IDD, la sécurité des données définie sur un domaine est appliquée sur les types de contenu suivants :

- Données de recherche
- Données d'entité
- Données hiérarchiques
- Données d'historique
- Données de tâche.

Sécurité des données dans la recherche de données

La recherche IDD permet à un utilisateur de rechercher des enregistrements par domaine et par groupe de domaines. Si un domaine possède un des filtres de sécurité des données pour l'utilisateur, les résultats de la recherche doivent contenir uniquement les enregistrements qui correspondent à la sécurité des données. La sécurité des données est appliquée à la fois pour les recherches de base et les recherches approximatives. Par exemple, lorsqu'un utilisateur effectue une recherche et a accès uniquement aux personnes en Californie (CA), le résultat de la recherche affiche uniquement les enregistrements des personnes de Californie.

Remarque:

- Si un utilisateur avec la sécurité des données effectue une recherche avec un terme de recherche, le résultat de la recherche est une intersection entre les enregistrements qui répondent à la sécurité des données et ce qui est renvoyé par la recherche.
- Si la déduplication de la recherche pour un enregistrement enfant n'est pas activée et que l'utilisateur avec la sécurité des données sur les objets principaux est supérieur à un enregistrement enfant, le résultat de la recherche aura tous les enregistrements associés à l'objet principal.
- Quand la recherche est effectuée dans un groupe de domaines, des filtres de sécurité de données différents sont utilisés.
- IDD réduit tous les doublons dans le cas où le nombre d'enregistrements trouvés est inférieur à la taille de la page du serveur configurée. Par exemple, tous les résultats sont extraits après la première requête.

Sécurité des données dans les données d'entité

IDD autorise un utilisateur à accéder à l'enregistrement de l'objet principal (objet primaire), à l'enregistrement enfant, à l'enregistrement petit-enfant et aux liens du domaine par domaine et groupe de domaines. Si un domaine comprend des filtres de sécurité des données pour un utilisateur, l'utilisateur ne peut alors accéder qu'aux enregistrements qui répondent à la sécurité des données. Les sections suivantes décrivent la manière dont la sécurité des données est appliquée pour différentes opérations dans la vue des données.

Ouvrir un enregistrement

Les filtres de sécurité des données garantissent que seuls les utilisateurs autorisés puissent ouvrir les enregistrements dans la vue des données.

Ouvrir un enregistrement en utilisant un rôle unique

Les utilisateurs avec un rôle unique peuvent ouvrir les enregistrements de l'objet principal si les conditions suivantes sont satisfaites :

- L'objet principal doit satisfaire tous les filtres de sécurité des données qui existent dans la colonne de l'objet principal.
- L'objet principal doit avoir au moins un enregistrement qui passe les restrictions de sécurité activé sur chaque onglet enfant avec la sécurité des données.

Par exemple, prenez un modèle de sécurité des données dans lequel un utilisateur a le rôle SalesManager-NY et pour lequel les filtres de sécurité suivants sont configurés :

- Filtre 1 : le code d'état est NY.
- Filtre 2 : le type de téléphone est Entreprise et Domicile.
- Filtre 3 : le code de titre de civilité est M.

À l'aide de ce modèle de sécurité des données mentionné ci-dessus, imaginez un scénario dans lequel la base de données a un enregistrement d'objet principal M. Steve Nash, qui a une adresse de facturation dans l'État de NY et un type de téléphone Professionnel. L'utilisateur avec le rôle Sales Manager- NY peut ouvrir l'enregistrement M. Steve Nash dans la vue des données, car l'objet principal satisfait le filtre 3 et ses enfants satisfont les filtres 1 et 2.

À l'aide du même modèle de sécurité des données, imaginez un scénario dans lequel la base de données a un enregistrement d'objet principal M. Carlos Booser, qui a une adresse de facturation dans l'État de NY et un type de téléphone Portable. L'utilisateur avec le rôle Sales Manager- NY ne peut pas ouvrir l'enregistrement M. Carlos Booser dans la vue des données, car il ne passe pas la restriction activée dans l'onglet enfant sur le type de téléphone.

Filtrer les enregistrements à l'aide d'un rôle unique

Les utilisateurs avec un rôle unique peuvent accéder aux détails de l'objet enfant ou petit-enfant uniquement s'il satisfait tous les filtres de sécurité des données qui existent dans la colonne enfant ou petit-enfant de l'objet principal.

Par exemple, prenez un modèle de sécurité des données dans lequel l'utilisateur a le rôle SalesManager- NY et a les filtres de sécurité suivants configurés :

- Filtre 1 : le code d'état est NY.
- Filtre 2 : le type de téléphone est Entreprise et Domicile.
- Filtre 3 : le code de titre de civilité est M.

À l'aide du modèle de sécurité des données mentionné ci-dessus, imaginez un scénario dans lequel la base de données a un enregistrement d'objet principal M. Robin Cameron, qui a une adresse de facturation dans les États de CA, TX et NY et le type de téléphone Professionnel et Fax. L'utilisateur avec le rôle Sales Manager- NY peut voir uniquement l'adresse située dans l'État de NY dans l'onglet de l'adresse de facturation et uniquement le numéro de téléphone Professionnel dans l'onglet Téléphone. Tous les autres enregistrements des deux onglets sont filtrés.

Filtrer les enregistrements à l'aide de plusieurs rôles

Par défaut, un utilisateur appartenant à plusieurs rôles peut accéder aux enregistrements enfants ou petits-enfants en combinant les filtres de sécurité des données.

Par exemple, imaginez un modèle de sécurité des données dans lequel l'utilisateur appartient aux rôles « Sales Manager NY » et « Car Sales Manager NJ » à la fois.

Le rôle « Sales Manager NY » dispose des filtres de sécurité des données suivants :

- Filtre 1 : le code d'état est NY.
- Filtre 2 : le type de téléphone est Entreprise ou Domicile.

Le rôle « Car Sales Manager NY » dispose des filtres de sécurité des données suivants :

- Filtre 1 : le code d'état est NJ.
- Filtre 2 : l'année de la voiture est 2009.

Imaginez que la base de données dispose d'un enregistrement d'objet principal sous le nom de John Smith. Les codes d'état des adresses de facturation de John sont NY, NJ et TX. Ses numéros de téléphone sont de type Entreprise et Fax. Il dispose d'une voiture fabriquée en 2009 et d'une autre fabriquée en 2001. L'utilisateur affecté aux rôles « Sales Manager NY » et « Car Sales Manager NJ » peut afficher les informations suivantes :

- L'utilisateur voit les adresses de facturation dont le code d'état est NY et celles dont le code est NJ, car le filtre de code d'état est défini pour les deux rôles.
- Si l'attribut « affectFilter » de l'élément « securityValue » est `False`, l'utilisateur voit les numéros de téléphone de tout type et les voitures fabriquées à n'importe quelle année. Informatica Data Director (IDD) n'applique pas les filtres de sécurité des données relatifs au type de téléphone ou à l'année de la voiture, car ces filtres ne sont configurés pour aucun des deux rôles.
- Si l'attribut « affectFilter » de l'élément « securityValue » est `True`, l'utilisateur voit les numéros de téléphone de type Entreprise et les voitures fabriquées en 2009. IDD applique tous les filtres de sécurité des données configurés pour chaque rôle. La valeur par défaut de l'attribut « affectFilter » est `True`.

Filtres de sécurité des données relatifs aux rôles hérités

Vous pouvez configurer des filtres de sécurité des données relatifs aux rôles hérités qui sont descendants d'un rôle parent. Pour configurer les filtres de sécurité des données relatifs aux rôles hérités, définissez l'attribut affectFilter du paramètre securityFilter dans le fichier `BDDConfig.xml`.

Par exemple, imaginez une hiérarchie de rôles dans laquelle le rôle DataSteward_NY est un descendant du rôle DataSteward. Un utilisateur appartenant au rôle DataSteward_NY appartient aussi au rôle DataSteward.

Vous souhaitez configurer un filtre de sécurité des données qui affecte uniquement les utilisateurs appartenant au rôle DataSteward_NY. Vous souhaitez que ces utilisateurs puissent voir les enregistrements dont la valeur STATE_CD est `NY`. Vous devez définir l'attribut affectFilter sur `False` afin de filtrer les données pour le rôle DataSteward_NY. Lorsque l'attribut affectFilter est `False`, Informatica Data Director filtre les données pour le rôle DataSteward_NY sans tenir compte des filtres de sécurité des données du rôle DataSteward.

L'extrait du fichier `BDDConfig.xml` exposé ci-dessous montre comment configurer les filtres de sécurité des données pour cet exemple :

```
<securityFilter columnUid="MATCH_PATH_COMPONENT.C_MT_ADDRESS|STATE_CD">
  <securityValue value="NY">
    <securityRole roleUid="DataSteward_NY"/>
  </securityValue>
  <securityValue affectFilter="false">
    <securityRole roleUid="DataSteward"/>
  </securityValue>
</securityFilter>
```

Afficher les relations

Dans IDD, une relation décrit l'affiliation entre deux entités spécifiques. Par exemple, une entité client peut posséder un lien logique vers une entité adresse.

L'onglet **Relation** dans la vue des données contient des informations sur les relations du gestionnaire de hiérarchies de l'objet principal avec d'autres entités du gestionnaire de hiérarchies. Certaines entités du gestionnaire de hiérarchies peuvent être transformées en objets principaux qui peuvent être affectés par la sécurité des données.

L'onglet **Relation** doit contenir uniquement les relations qui connectent les entités du gestionnaire de hiérarchies associées aux objets principaux se conformant aux paramètres de sécurité des données.

Fusionner des données

La fusion consiste à associer deux enregistrements ou plus, car ils sont identiques ou suffisamment similaires pour être considérés comme des doublons. Vous fusionnez des enregistrements pour consolider des données dupliquées en une seule entité (entité principale), qui représente la meilleure version de la vérité (MVV). Là où les valeurs d'attributs diffèrent, les valeurs conservées peuvent être déterminées par différents facteurs. Par exemple, les valeurs conservées peuvent être déterminées selon la configuration de l'approbation pour ces enregistrements, ou selon les valeurs fournies par un utilisateur qui a choisi de modifier la valeur de remplacement à la place.

Dans l'application IDD, la boîte de dialogue **Rechercher des candidats à la fusion** devrait afficher uniquement les enregistrements valides selon la sécurité des données du domaine de l'objet principal.

Exporter des données et exporter des profils

Tous les filtres de sécurité des données et le masquage des données sont applicables aux données exportées ainsi qu'aux données affichées à l'utilisateur.

Sauvegarder un enregistrement

Un utilisateur peut sauvegarder un enregistrement uniquement une fois la validation effectuée et tous les filtres de sécurité des données du domaine appliqués. Si un enregistrement ne respecte pas les spécifications de filtres de sécurité des données, un message d'avertissement est affiché à l'utilisateur.

Dans la boîte de dialogue du message d'avertissement, si vous choisissez **Oui**, l'objet principal est enregistré et l'onglet est fermé. Si vous choisissez **Non**, l'objet principal n'est pas encore enregistré, mais l'utilisateur peut continuer à compléter les détails de l'objet principal.

Recherche de doublons (correspondances potentielles)

Les doublons sont des entités dans lesquelles les données de certaines colonnes (telles que le nom, l'adresse ou les données de l'entreprise) sont identiques ou suffisamment similaires pour être considérées comme quasiment identiques. IDD utilise une logique de correspondance spéciale et des attributs activés pour la correspondance afin de déterminer si deux entités sont suffisamment similaires pour être considérées comme des correspondances. Les doublons sont des entités que vous prenez en compte pour une fusion.

Pour rechercher des correspondances potentielles, cliquez sur **Plus d'actions** et choisissez **Rechercher de doublons**. Si un domaine possède un filtre de sécurité des données pour l'utilisateur, les résultats de la recherche de doublons doivent contenir uniquement ces enregistrements d'objet principal qui correspondent à la sécurité des données.

Par exemple, prenez un modèle de sécurité des données dans lequel l'utilisateur a un rôle unique, SalesManager- CA et partez du principe que l'utilisateur exécute une recherche de doublons pour une

personne. Le résultat de la recherche contient les individus ayant au moins une adresse de facturation dans l'État CA et tous les autres doublons sont filtrés.

Remarque: Si un utilisateur a plus d'un rôle et exécute une recherche de doublons, l'utilisateur est autorisé à voir une union des résultats que chaque rôle permet d'afficher.

Sécurité des données dans les données hiérarchiques

Dans IDD, une hiérarchie est un ensemble de types de relations. Ce sont simplement des types de relations regroupés pour faciliter la classification et l'identification. Quand la vue du gestionnaire de hiérarchies est ouverte, elle vérifie d'abord si l'entité d'ancrage du gestionnaire de hiérarchies peut être transformée en objet principal et si elle est transformée en objet principal, elle est visible par la sécurité des données.

Ajouter des entités de gestionnaire de hiérarchies

Une entité Gestionnaire de hiérarchies peut être ajoutée au canevas à l'aide des opérations de recherche et de création.

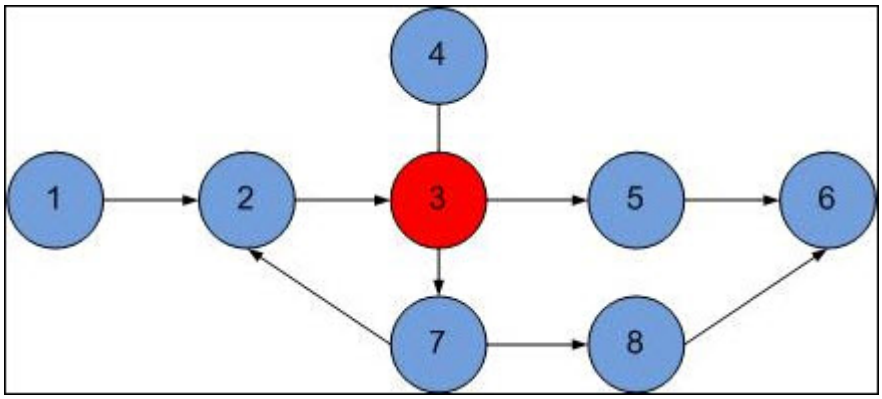
Dans les résultats de recherche de données, seuls les enregistrements qui sont autorisés par l'objet principal de la sécurité des données du domaine sont affichés. Par conséquent, avec l'option de recherche, seuls des objets valides peuvent être ajoutés.

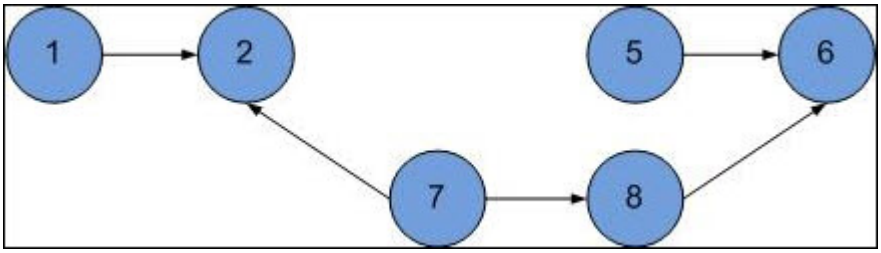
Quand un utilisateur crée une entité Gestionnaire de hiérarchies, l'utilisateur peut enregistrer l'objet primaire dans la vue des données qui n'est pas valide par la sécurité des données. Si l'utilisateur confirme l'enregistrement de l'objet primaire qui n'est pas visible par la sécurité des données, cette entité Gestionnaire de hiérarchies n'est pas ajoutée au canevas.

Constitution de graphes de gestionnaire de hiérarchies

Les entités de gestionnaire de hiérarchies peuvent être transformées en objets principaux. Les objets principaux qui ne sont pas visibles en tant que résultats de la sécurité des données ne sont pas représentés dans le graphique du gestionnaire de hiérarchies comme des entités du gestionnaire de hiérarchies. Si une entité du gestionnaire de hiérarchies n'est pas visible d'un utilisateur, le graphique du gestionnaire de hiérarchies ne doit alors pas afficher cette entité et sa sous-arborescence.

Par exemple, prenez le graphique du gestionnaire de hiérarchie suivant, où un utilisateur n'est pas autorisé à afficher l'entité 3 à cause de la sécurité des données. Dans ce cas, le graphique doit être visible à l'utilisateur sans l'entité 3 et son composant de sous-arborescence, entité 4.





Remarque: Les utilisateurs avec plusieurs rôles peuvent accéder à l'union de tous les objets qui peuvent être accessibles par chacun des rôles.

Sécurité des données dans les données d'historique

IDD vous permet d'afficher l'historique des événements de traitement des données comme les mises à jour, les suppressions et les fusions qui se sont produites pour l'entité sélectionnée. Si un objet de base correspond aux spécifications de sécurité des données, l'historique de cet objet de base est alors affiché, même si, dans le passé, il a été masqué pour des raisons de sécurité des données.

La sécurité des données dans l'historique impacte les domaines suivants :

- Historique pour les objets principaux
- Événements de l'historique
- Historique composite des objets principaux.

Ouvrir les détails d'historique

Un utilisateur peut ouvrir l'historique des données à l'aide d'un lien profond ou comme un composant d'historique dans IDC. Dans ce cas, la sécurité des données est appliquée par IDD pour garantir que l'objet principal pour lequel l'historique est construit est visible pour les utilisateurs autorisés.

Afficher les événements d'historique

Les événements dans la vue d'historique font référence à des objets de domaine objets, un objet principal ou des enfants d'un objet principal. Si l'objet principal n'est pas visible en raison de la sécurité des données, la vue d'historique n'est pas du tout affichée. Si un enregistrement enfant n'est pas visible en raison de la sécurité des données, la vue d'historique est affichée pour l'objet principal, mais les événements d'historique de l'enregistrement enfant ne sont pas ajoutés à la chronologie.

Sécurité des données pour les liens profonds

La fonctionnalité de liens profonds dans l'application IDD permet de gérer l'état de l'application en utilisant des paramètres URL. Elle permet de définir des chemins de navigation interne dans l'URL, qui peut être ouverte dans l'application IDD.

Cette fonctionnalité est également utilisée pour :

- Fournir une navigation entre composant IDC et application IDD.
- Fournir des signets à des parties spécifiques de l'application.

La sécurité des données IDD impacte les parties suivantes du lien profond :

- **Ouverture d'un enregistrement** : l'objet principal et ses données enfants sont contrôlés en fonction des paramètres de sécurité des données, avant l'affichage par un nouvel onglet des données de l'enregistrement dans la vue des données.

- **Ouverture d'une tâche** : tous les paramètres de sécurité des données mentionnés dans la section “Sécurité des données dans les données de tâche” à la page 168 sont applicables. Ces paramètres de sécurité des données déterminent si un utilisateur est capable d'ouvrir une tâche ou non.

ANNEXE E

Exemple de configuration de la sécurité basée sur les rôles

Cette annexe comprend les rubriques suivantes :

- Présentation d'un exemple de configuration de la sécurité basée sur les rôles, 137
- Concepts clés, 137
- Tâches de configuration de la sécurité IDD, 139

Présentation d'un exemple de configuration de la sécurité basée sur les rôles

Cette annexe décrit un scénario simple pour configurer l'accès basé sur des rôles aux ressources sécurisées dans Informatica Data Director (IDD).

Elle présente des concepts importants et parcourt les tâches de configuration de sécurité requises pour implémenter un modèle de scénario. Le but de cette annexe est d'apporter aux implémenteurs IDD des connaissances de base sur ce qui peut être requis pour configurer la sécurité dans leurs projets d'implémentation IDD.

Remarque: Il ne s'agit pas d'un didacticiel pratique sur la création et l'utilisation d'un modèle d'application. Il s'agit simplement d'une présentation des outils et tâches utilisés pour un scénario donné.

Concepts clés

Cette section décrit les concepts clés que vous devez comprendre avant de mettre en œuvre la sécurité pour IDD.

IDD, Gestionnaire d'accès de sécurité (GAS) et Services Integration Framework (SIF)

La plus grande partie de la fonctionnalité IDD est implémentée à l'aide d'appels SIF.

SIF nécessite la configuration du GAS, qui est très précise, pour fournir les droits et privilèges requis pour exécuter les appels SIF. La configuration du GAS implique de définir les utilisateurs, rôles, ressources

sécurisées et privilèges requis pour prendre en charge un accès basé sur les rôles aux données et opérations.

Outils de configuration de la sécurité IDD

Vous utilisez les outils suivants dans la Console Informatica MDM Hub pour configurer le GAS : Utilisateurs, Utilisateurs et groupes, Rôles et Ressources sécurisées/Groupes de ressources (y compris packages et fonctions de nettoyage).

Par ailleurs, vous utilisez le gestionnaire de configuration IDD pour lier votre configuration du GAS à des objets IDD.

Lectures connexes

La documentation Informatica suivante propose des informations de référence importantes sur la sécurité IDD, GAS et SIF :

- *Guide de sécurité d'Informatica MDM Multidomain Edition*
- *Guide de Framework d'intégration des services d'Informatica MDM Hub*, "Utilisation du Gestionnaire d'accès de sécurité avec l'API SIF"

Liens connexes :

- "Référence sur la configuration de la sécurité IDD" à la page 120

Sécurité des objets et des tâches

Il est utile d'envisager la sécurité IDD en deux grandes catégories :

- Sécurité des objets : accès aux données des zones de sujet et capacité à exécuter des opérations sur ces données (telles qu'afficher, créer, mettre à jour et fusionner) dans IDD.
- Sécurité des tâches (workflow). Accès aux tâches et actions basé sur les rôles définis dans le workflow.

Remarque: Bien que cet exemple de scénario cible uniquement la sécurité des objets, de nombreuses idées sont également applicables à la sécurité des tâches dans IDD, car la sécurité des tâches dépend également du GAS.

Liens connexes :

- "Flux de travail et tâches" à la page 24

Conseils pour la conception de la sécurité pour une utilisation dans IDD

L'implémentation de la sécurité IDD est un processus itératif et continu.

Pour débuter, vous devez comprendre les différents types d'accès aux ressources (objets et opérations) dont les utilisateurs IDD auront besoin dans votre application IDD.

Dans le GAS, le *rôle* est le mécanisme essentiel qui détermine l'étendue de l'accès d'un utilisateur aux ressources IDD. Le GAS est hautement configurable et offre un contrôle précis des ressources. Envisagez de créer un rôle distinct pour chaque combinaison unique d'accès objets/opérations, et affectez des privilèges à ce rôle. Les rôles peuvent être basés sur d'autres rôles pour créer des couches de privilèges croissantes. Une fois les utilisateurs configurés, vous les affectez au rôle le mieux adapté à leurs responsabilités professionnelles.

Cet exemple de scénario suit le principe du *moindre privilège* : les accès aux ressources sont octroyés en fonction des besoins. Par défaut, les utilisateurs n'ont aucune autorisation. Vous ne leur octroyez ensuite de manière sélective que les autorisations requises pour exécuter les opérations dont ils ont la responsabilité.

Important: La configuration du GAS doit correspondre à la configuration IDD. Quoi que vous configuriez dans l'application IDD, vous devez configurer le GAS pour fournir assez de privilèges pour prendre en charge la fonctionnalité IDD configurée.

Autres considérations

Lors de la planification de la sécurité pour votre application IDD, envisagez les problèmes suivants :

- Pour qu'IDD accède aux ressources Informatica MDM Hub, les ressources doivent être configurées comme SECURE (pas privées) dans l'outil Ressources sécurisées de la Console Hub.
- Le GAS est configuré sur la base des ORS. Lorsque vous ajoutez des utilisateurs IDD, vous devez définir le schéma IDD comme base de données par défaut pour ces utilisateurs.
- Dans l'espace de travail Données, les utilisateurs IDD ne voient généralement pas de messages d'erreur explicites concernant des privilèges insuffisants. Par exemple, une certaine ressource peut être simplement masquée pour l'utilisateur car il n'est pas configuré pour y accéder. Lors du test de votre configuration de sécurité, consultez les informations de débogage dans le journal du serveur.
- Dans l'espace de travail d'une entité, IDD affiche toutes les ressources indépendamment du rôle utilisateur. Lorsque les utilisateurs effectuent des actions pour lesquelles ils ne disposent pas des autorisations de sécurité requises, IDD affiche des messages d'erreur.
- La configuration de la sécurité est stockée à deux endroits : dans le cache du Serveur Hub et dans le cache IDD. Il existe un léger temps de latence (1 minute) pour synchroniser les modifications. Dans un environnement de développement, vous pouvez redémarrer le serveur pour actualiser le cache.

Tâches de configuration de la sécurité IDD

Cette section parcourt la série de tâches pour implémenter un modèle de scénario basé sur les rôles : fournir aux utilisateurs IDD quatre niveaux de privilèges différents (aucune autorisation, lecture seule, création et mise à jour) pour accéder à un objet de base Partie et aux ressources correspondantes.

Imaginez, par exemple, un scénario avec deux domaines tels que Partie et Organisation où le domaine Partie a une relation logique un-à-un avec le domaine Organisation. Dans la vue des données, pour modifier les attributs de l'enregistrement, vous devez posséder les privilèges CREATE et UPDATE sur les deux domaines que sont C_PARTY et C_ORGANIZATION. Si certains champs de l'objet principal ou si l'objet ayant une relation logique un-à-un avec l'objet principal sont en lecture seule, vous pouvez toujours éditer l'objet principal. Les champs qui sont en lecture seule sont visibles dans la vue des données, mais ne peuvent pas être modifiés. Si tous les champs de l'objet principal et l'objet ayant une relation logique un-à-un avec l'objet principal ont les autorisations de lecture seule, vous ne pouvez pas éditer l'objet principal dans la vue de données.

Configuration d'objets de conception dans la Console Hub

Avant de commencer, vous devez configurer tous les objets de conception dans la Console Hub qui seront utilisés par IDD.

Dans ce scénario :

- Objet de base Partie (gestionnaire de schéma)
- Packages (outil de requêtes et outil de packages), qui affectent la recherche
- Règles de correspondance (gestionnaire de schéma), qui affectent la recherche de doublons (correspondances possibles)
- Fonctions de nettoyage (outil Fonctions de nettoyage), qui affectent l'entrée de données (nettoyage en ligne des données lors de l'enregistrement)

Pour plus d'informations, consultez le *Guide de configuration d'Informatica MDM Multidomain Edition*

Remarque: Bien que ce scénario décrive uniquement la configuration d'un seul objet de base, les modèles de données des clients impliquent un réseau de relations diverses entre les objets de base. Il est important que vous configuriez toute la constellation des objets de base et les autres objets de conception auxquels accéderont des utilisateurs de l'application IDD.

Configuration des utilisateurs de l'application IDD (outils Utilisateurs)

Commencez à configurer le GAS en ajoutant des comptes utilisateur IDD à la base de données principale de votre implémentation d'Informatica MDM Hub.

Par exemple, dans la Console Hub, vous pourriez exécuter l'outil Utilisateurs et ajouter les comptes utilisateur suivants :

Compte utilisateur	A reçu un rôle qui accorde
user_1	Aucune autorisation (par défaut).
user_2	Autorisation de lecture seule sur l'objet de base Partie.
user_3	Autorisation de création sur l'objet de base Partie.
user_4	Autorisation de mise à jour sur l'objet de base Partie.

Remarque: Vérifiez que chaque utilisateur a accès à tous les Operational Record Stores (ORS) associés à l'application IDD. Vous pouvez également le faire sous l'onglet Utilisateurs affectés à la base de données dans l'outil Utilisateurs et groupes.

Configuration de ressources sécurisées (Outil Ressources sécurisées)

Pour qu'IDD ait accès à une ressource, elle doit être signalée comme SECURE dans l'outil Ressources sécurisées.

Vous devez vous assurer que tous les objets de conception configurés précédemment sont configurés comme ressources SECURE.

- Objet de base Partie, y compris les éléments suivants associés :
  - ensembles de règles de correspondance, utilisés dans IDD pour la recherche de doublons (correspondances potentielles)
  - métadonnées de contenu (HISTORY, RAW et XREF), utilisées dans IDD pour afficher l'historique des modifications, les références croisées et les enregistrements bruts
- fonctions de nettoyage utilisées pour l'entrée de données
- packages utilisés pour les résultats de recherche

Remarque:

- Envisagez de créer des groupes de ressources pour organiser des ressources accessibles d'IDD pour expédier la configuration de sécurité.
- Si vous voulez empêcher tous les utilisateurs d'IDD d'avoir accès à une ressource donnée, rendez-la PRIVATE. Par exemple, vous pourriez masquer globalement l'accès d'IDD aux enregistrements RAW de cette manière.

Création et configuration d'une nouvelle application IDD (gestionnaire de configuration IDD)

Dans le gestionnaire de configuration IDD, créez une nouvelle application IDD, puis configurez-la. Ajoutez un groupe de zones de sujet (tel qu'un groupe Partie), puis la zone de sujet Partie.

Dans ce scénario, vous spécifieriez toutes les colonnes Partie, l'ensemble de règles de correspondance Partie à utiliser pour les contrôles de doublons (à configurer comme SECURE) et une fonction de nettoyage (à configurer comme SECURE). Une fois terminé, enregistrez les modifications et déployez l'application IDD.

Remarque: Une manière de limiter l'accès des utilisateurs aux informations consiste à spécifier uniquement un sous-ensemble de colonnes pour afficher l'IUG IDD. Vous pouvez ensuite configurer des autorisations pour les rôles au niveau des colonnes, ce qui permet à certains utilisateurs de voir une colonne tandis que d'autres ne peuvent pas.

Affichage des ressources personnalisées (Outil Ressources sécurisées)

Lors du premier déploiement d'une application IDD dans le gestionnaire de configuration IDD, il ajoute automatiquement un nœud pour l'application sous le nœud Ressources personnalisées.

Lorsque vous redéployez l'application, le gestionnaire de configuration IDD ajoute/actualise tout objet de conception de prise en charge spécial comme ressource SECURE. Ces objets de prise en charge sont nécessaires pour l'intégration d'IDD avec le GAS. Après l'enregistrement des modifications du domaine et le redéploiement de l'application, ouvrez de nouveau l'outil Ressources sécurisées et notez les ressources personnalisées qui ont été ajoutées automatiquement par le fichier de configuration IDD.

Remarque: N'oubliez pas qu'il peut exister un léger retard entre le moment où vous enregistrez votre configuration de l'application et le moment où elle apparaît dans l'outil Ressources sécurisées.

Voici une brève description de ces ressources :

Ressource personnalisée	Expose la capacité à
RAPPORT/affichage	Afficher les rapports sur le Démarrer un espace de travail.
SEARCH_QUERY/Create	Créer des requêtes privées.
SEARCH_QUERY/ CreatePublic	Créer des requêtes publiques.
SUBJECT_AREA/ *BaseObject*	Accéder au domaine dans IDD. Vous verrez peut-être plusieurs ressources SUBJECT_AREA obtenir leurs données depuis le même objet de base, mais représenter différentes vues. Même si le rôle a accès à l'objet de base, vous pouvez par ailleurs limiter les privilèges sur ces ressources pour limiter les domaines SUBJECT_AREA dans lesquelles le rôle peut rechercher, qu'il peut afficher, etc.
TASK_TYPE/ *SubjectArea*:*TaskType*	Accédez à la tâche spécifiée pour le domaine associé.

Configuration des rôles et privilèges de ressource (outil Rôles)

Les rôles offrent un contrôle très précis sur les privilèges affectés aux ressources.

Pour expédier votre configuration de sécurité, vous pouvez même créer une hiérarchie de rôles en affectant des rôles aux autres rôles. Dans la Console Hub, utilisez l'outil Rôles pour configurer les autorisations requises pour les opérations IDD exécutées par ce rôle.

Création de rôles

Vous commencez par créer les rôles de votre choix, tels que :

Nom du rôle	Description
party_no_privileges_role	Valeur par défaut initiale. Aucune autorisation d'accéder à quoi que ce soit (comparable à un utilisateur sans rôle affecté). Il ne s'agit pas d'un scénario dans le monde réel - il est proposé pour montrer ce qui se produit lors de l'ajout de privilèges avec d'autres rôles.
party_read_only_role	Autorisation de lecture seule sur l'objet de base Partie.
party_create_role	Autorisation de création sur l'objet de base Partie.
party_update_role	Autorisation de mise à jour sur l'objet de base Partie.

Configuration des privilèges de ressource pour les objets de base et les objets affiliés

Ensuite, pour chaque rôle, vous configurez les privilèges de ressource pour les objets de base et les objets affiliés.

Pour configurer les autorisations pour les objets de base dans l'outil Rôles, sélectionnez le rôle à configurer, développez le nœud Objets de base, développez le nœud Partie et configurez les privilèges pour l'objet de base, les métadonnées de contenu et les ensembles de règles de correspondance.

La table suivante présente les privilèges que vous devez configurer pour ce scénario.

Nom du rôle	Privilèges de ressource
party_no_privileges_role	Aucune autorisation.
party_read_only_role	- Privilèges READ sur toutes les colonnes de l'objet de base PARTY - Privilèges READ sur un ensemble de règles de correspondance applicable - Privilèges READ sur les métadonnées de contenu (HISTORY, RAW et XREF).
party_create_role	- Privilèges READ sur toutes les colonnes de l'objet de base PARTY. - Privilèges READ sur un ensemble de règles de correspondance applicable - Privilèges READ sur les métadonnées de contenu (HISTORY, RAW et XREF) - Privilèges CREATE sur toutes les colonnes de l'objet de base PARTY (requis pour la création d'un nouvel enregistrement). - Privilèges UPDATE sur toutes les colonnes de l'objet de base PARTY (si vous voulez permettre à ce rôle de mettre à jour un enregistrement existant également).
party_update_role	- Privilèges READ sur toutes les colonnes de l'objet de base PARTY. - Privilèges READ sur un ensemble de règles de correspondance applicable - Privilèges READ sur les métadonnées de contenu (HISTORY, RAW et XREF) - Privilèges UPDATE sur toutes les colonnes de l'objet de base PARTY (requis pour enregistrer les modifications apportées à un enregistrement)

Conseils:

- Si votre objet de base a des relations avec d'autres objets de base (par exemple, relations parent-enfant, recherches de clés étrangères ou relations un à un), vous devez configurer l'accès à toutes ces ressources également. Les recherches nécessitent un accès READ, tandis que les objets de base liés nécessitent des autorisations comparables à l'objet de base du cœur).
- Vous pouvez désactiver sélectivement les privilèges READ sur certaines colonnes de sorte que les utilisateurs ne puissent pas les voir dans l'application IDD. De même, vous pouvez activer les privilèges READ et désactiver les privilèges UPDATE de sorte que les utilisateurs puissent voir les colonnes mais pas modifier des données.
- Vous devez configurer l'accès READ à un ensemble de règles de correspondance afin de trouver des doublons pour travailler.
- Vous pouvez contrôler si un rôle peut afficher l'historique (nécessite des privilèges READ sur HISTORY), afficher des références croisées (nécessite des privilèges READ sur XREF) et afficher des enregistrements bruts (nécessite des privilèges READ sur RAW).
- Sélectionnez (cochez) **Afficher uniquement les ressources pour ce rôle** pour voir rapidement quelles ressources sont affectées au rôle en cours.

Configuration des privilèges de ressource pour les packages

Les applications IDD utilisent des packages pour afficher des résultats de recherche lors de l'exécution de requêtes sous l'onglet Recherche.

Les rôles doivent être configurés pour avoir un accès READ aux packages associés à l'objet de base. Pour configurer les autorisations de packages dans l'outil Rôles, sélectionnez le rôle à configurer, développez le nœud Packages et configurez les privilèges pour les packages applicables.

Nom du rôle	Privilèges de ressource
party_no_privileges_role	Aucun privilège.
party_read_only_role	Privilèges READ sur le package Partie.
party_create_role	Privilèges READ sur le package Partie.
party_update_role	Privilèges READ sur le package Partie.

Configuration des privilèges de ressource pour les fonctions de nettoyage

Si un domaine est configuré pour utiliser une fonction de nettoyage en ligne (configurée dans le fichier de configuration IDD), le rôle doit avoir des privilèges EXECUTE sur cette fonction de nettoyage afin que cette dernière se déclenche lors de l'enregistrement.

Configuration des privilèges de ressource pour les ressources personnalisées

Ensuite, pour chaque rôle (excepté le rôle party_no_privileges_role), développez le nœud Ressources personnalisées, développez le nœud de l'application IDD et affectez les privilèges suivants :

Nom du rôle	Privilèges de ressource
party_no_privileges_role	Aucune autorisation.
party_read_only_role	- Privilèges READ sur la ressource CHART/Vue afin que les utilisateurs puissent voir les graphes dans le Démarrer un espace de travail. - Privilèges CREATE sur la ressource SEARCH_QUERY/Création et SEARCH_QUERY/CreatePublic (ou LECTURE si vous voulez que des utilisateurs exécutent des requêtes existantes uniquement et ne créent pas de nouvelles requêtes). - Privilèges READ sur la ressource SUBJECT_AREA/Party.

Nom du rôle	Privilèges de ressource
party_create_role	- Privilèges READ sur la ressource CHART/Vue afin que les utilisateurs puissent voir les graphes dans le Démarrer un espace de travail. - Privilèges READ et CREATE vers les ressources SEARCH_QUERY/Create et SEARCH_QUERY/CreatePublic. - Privilèges READ et UPDATE sur la ressource SUBJECT_AREA/Party (seulement si vous voulez autoriser le rôle à contourner le flux de travail). Normalement, les utilisateurs ont des privilèges READ et CREATE sur TASK_TYPE/Party: ReviewNoApprove, ce qui permet aux utilisateurs d'accéder au bouton **Envoyer pour approbation**. - Privilèges READ et UPDATE sur la ressource SUBJECT_AREA/Party.
party_update_role	- Privilèges READ sur la ressource CHART/Vue afin que les utilisateurs puissent voir les graphes dans le Démarrer un espace de travail. - Privilèges READ et CREATE vers les ressources SEARCH_QUERY/Create et SEARCH_QUERY/CreatePublic. - Privilèges READ et UPDATE sur la ressource SUBJECT_AREA/Party (seulement si vous voulez autoriser le rôle à contourner le flux de travail). Normalement, les utilisateurs ont des privilèges READ et UPDATE sur TASK_TYPE/Party: ReviewNoApprove, ce qui permet aux utilisateurs d'accéder au bouton **Envoyer pour approbation**.

La manière de configurer l'accès à ces ressources personnalisées affecte ce que voient les utilisateurs dans l'application IDD. Par exemple :

- Si un utilisateur n'a pas de privilèges CREATE sur SEARCH_QUERY/Create, il n'aura pas la possibilité de créer ni d'enregistrer une nouvelle requête dans IDD.
- Si un utilisateur n'a pas de privilèges CREATE sur SEARCH_QUERY/CreatePublic, il ne verra pas l'option Requête publique dans la boîte de dialogue Enregistrer la requête sous.
- En général, les utilisateurs ont besoin de privilèges READ et EXECUTE sur les tâches qui leur seront affectées. Si un utilisateur n'a pas de privilèges CREATE sur une ressource TASK_TYPE donnée, il ne pourra pas créer cette tâche dans IDD.

Conseils de configuration supplémentaires

- Si vous voulez autoriser un rôle à fusionner des données et/ou annuler des fusions de données, vous devez accorder à ce rôle des privilèges MERGE sur l'objet de base.
- Si vous voulez autoriser un rôle à ouvrir des enregistrements sous l'onglet Vue de hiérarchie, vous devez lui accorder l'accès READ à la ressource HM_PROFILE (le profil Par défaut ou une autre ressource HM_PROFILE applicable).

  Accordez également les privilèges READ, CREATE, UPDATE et/ou DELETE appropriés sur les ressources HM_RELATIONSHIP_TYPE et HM_HIERARCHY_TYPE.

  Pour ajouter une entité (Ajouter une entité), le rôle doit avoir des privilèges CREATE sur la zone de sujet. Pour ajouter une relation (Ajouter une relation), le rôle doit avoir des privilèges CREATE sur la table REL, des privilèges READ et CREATE sur HM_PROFILE et READ et CREATE sur HM_RELATIONSHIP_TYPE et HM_HIERARCHY_TYPE.

Affectation de rôles aux utilisateurs (outil Utilisateurs et Groupes)

Dans la Console Hub, utilisez l'outil Utilisateurs et Groupes pour affecter les utilisateurs IDD aux rôles que vous avez définis.

Compte utilisateur	Affecter au rôle
user_1	party_no_privileges_role
user_2	party_read_only_role
user_3	party_create_role
user_4	party_update_role

Ce que des échantillons d'utilisateurs d'IDD pourront voir et faire

Une fois que des rôles se sont vu affecter des privilèges de ressources vers des ressources SECURE et que des utilisateurs ont été affectés à des rôles, les utilisateurs peuvent se connecter à l'application IDD et voir ce à quoi ils ont accès.

Dans cet exemple, les utilisateurs pourront voir et faire :

Nom du rôle	Ce que l'utilisateur peut voir et faire
user_1 (aucun privilège)	- Sur le Démarrer un espace de travail, l'utilisateur ne peut pas voir de graphes. - Sous l'onglet Données, l'utilisateur peut voir l'onglet Recherche, mais ne peut pas afficher des requêtes publiques ni créer des requêtes. - Sous l'onglet Données, l'utilisateur peut voir différents domaines, mais il ne peut exécuter dessus aucune action.
user_2 (privilèges en lecture seule)	- Sur le Démarrer un espace de travail, l'utilisateur peut voir des graphes. - Sous l'onglet Données (onglet Recherche), l'utilisateur peut exécuter une requête, afficher des requêtes publiques et afficher les résultats de recherche (y compris tous les champs pour les enregistrements individuels), mais il ne peut pas créer ni actualiser de requête. - Sous l'onglet Données (domaine Partie), l'utilisateur ne peut pas créer un nouvel enregistrement.
user_3 (privilèges de création)	- Sur le Démarrer un espace de travail, l'utilisateur peut voir des graphes. - Sous l'onglet Données (onglet Recherche), l'utilisateur peut exécuter, créer et actualiser une requête. - Sous l'onglet Données (domaine Partie), l'utilisateur peut créer un nouvel enregistrement Partie, ajouter des données et enregistrer des modifications.
user_4 (privilèges d'actualisation)	- Sur le Démarrer un espace de travail, l'utilisateur peut voir des graphes. - Sous l'onglet Données (onglet Recherche), l'utilisateur peut exécuter, créer et actualiser une requête. - Sous l'onglet Données (domaine Partie), l'utilisateur peut éditer un enregistrement Partie existant et enregistrer des modifications, mais pas créer un nouvel enregistrement Partie.

ANNEXE F

Masquage des données

Cette annexe comprend les rubriques suivantes :

- Présentation du masquage des données, 147
- Expressions, 147
- Échantillons de modèles, 148
- Exemple de définition de masque, 148

LIENS CONNEXES :

- “Masquage des données” à la page 26

Présentation du masquage des données

Cette annexe décrit le mécanisme de masquage des données.

Ce mécanisme est utilisé pour masquer des informations critiques aux utilisateurs d'IDD non autorisés à accéder à ces informations. Pour les champs masqués, IDD remplace une partie des caractères (ou toutes les valeurs des champs) par un astérisque (*).

Le modèle de masque est décrit sous forme d'expressions régulières. Les parties d'expression devant être masquées sont placées entre parenthèses.

Expressions

Le modèle des masques est décrit sous forme d'expressions régulières.

Les parties des expressions devant être masquées sont placées entre parenthèses.

.

Un point signifie n'importe quel caractère.

.*

Un point suivi d'un astérisque signifie une séquence de caractères ou une séquence vide.

.+

Un point suivi d'un signe plus signifie un ou plusieurs caractère(s). Une séquence vide ne correspond pas à cette expression.

.{n}

Un point suivi d'un nombre entier entre accolades signifie jusqu'à n caractères.

[.]

Un point entre des crochets signifie le caractère point.

Échantillons de modèles

Les exemples suivants présentent des échantillons de modèles.

Masquer la valeur de champ complète :

```
(.+)
```

Masquer tous les caractères sauf les trois derniers :

```
(.+)…
```

Ne pas masquer les quatre premiers caractères :

```
….(.+)
```

Modèle qui masque les cinq premiers caractères, puis en laisse trois non masqués, puis masque le reste de la valeur excepté les quatre derniers caractères :

```
(.{5})…(.+)….
```

Si le modèle spécifié ne correspond pas à la valeur du champ, la valeur complète est masquée. Par exemple la chaîne « ABS » ne correspond pas au modèle `(.+)…` car il attend au moins quatre caractères (un au début devant être masqué et trois à la fin ne devant pas être masqués). Dans ce cas, « ABS » est remplacé par `"***"`.

Exemple de définition de masque

Des définitions de masques peuvent apparaître dans le fichier de configuration XML dans n'importe quelle section de mise en page.

```
<layout columnsNum="3">
   <column columnUid="C_PRODUCT|PRODUCT_NUMBER" editStyle="FIELD"
horizontalStyle="MEDIUM"
           required="true" showInHMCompactView="true">
      <dataMask value="...(.+)">
         <securityRole roleUid="Customer-CA"/>
      </dataMask>
   </column>
   <column 1columnUid="C_PRODUCT|PRODUCT_NAME" editStyle="FIELD" horizontalStyle="MEDIUM"
           Requi1red="true" showInHMCompactView="true"/>
   <column columnUid="C_PRODUCT|PRODUCT_DESC" editStyle="TEXT_AREA"
horizontalStyle="MEDIUM"/>
...
</layout>
```

L'exemple précédent présente une définition de masque pour la colonne Numéro de produit. Le masque est appliqué aux utilisateurs avec un rôle de sécurité Client-CA.

Remarque: Si aucun rôle de sécurité n'est défini pour la définition du masque de données, les masque est appliqué à tous les utilisateurs non administrateurs.

ANNEXE G

Moteur de flux de travail Siperian BPM

Cette annexe comprend les rubriques suivantes :

- Siperian BPM est déconseillé, 149
- Migrer de Siperian BPM à ActiveVOS, 150
- Flux de travail et tâches, 152
- Diagramme des composants de configuration des tâches et des flux de travail, 153
- Configuration des tâches, 154
- Types de tâches, 154
- Types de tâches - Échantillon XML, 155
- Attributs TaskType et balises, 156
- Personnalisation des types de tâches, 159
- Types d'actions, 160
- Types d'actions - Échantillon XML, 160
- Attributs et balises ActionType , 161
- Configuration de la sécurité des tâches, 162
- Affectation des tâches, 163
- Notification des tâches, 166
- Rapports et scores de gestion des tâches, 167
- Sécurité des données dans les données de tâche, 168

Siperian BPM est déconseillé

Disponible dans la version 10.0.0, le moteur de flux de travail Siperian BPM est déconseillé et sera supprimé dans la prochaine version. Auparavant, le moteur de flux de travail Siperian BPM était le moteur de flux de travail par défaut de MDM Hub.

Informatica recommande de mettre à jour les applications Informatica Data Director (IDD) pour utiliser ActiveVOS Server, le nouveau moteur de flux de travail par défaut.

Migrer de Siperian BPM à ActiveVOS

Vous pouvez migrer de l'adaptateur de flux de travail Siperian vers l'adaptateur de flux de travail ActiveVOS basé sur des entités commerciales.

Important: Informatica recommande de migrer vers l'adaptateur de flux de travail ActiveVOS basé sur des entités commerciales. L'adaptateur de flux de travail Siperian est déconseillé. Informatica continuera de prendre en charge cet adaptateur déconseillé, mais il deviendra obsolète et Informatica ne le prendra plus en charge dans ses versions ultérieures.

Définissez l'adaptateur de flux de travail ActiveVOS basé sur des entités commerciales en tant que moteur de flux de travail principal. L'adaptateur de flux de travail Siperian BPM devient l'adaptateur de flux de travail secondaire. Vous pouvez traiter des tâches avec l'adaptateur de flux de travail secondaire, mais vous devez créer des tâches avec l'adaptateur de flux de travail principal.

Utilisez la console ActiveVOS pour vous familiariser avec les processus par défaut des flux de travail ActiveVOS par défaut. Si vous ne voulez pas ajuster vos processus d'entreprise afin de les aligner avec les flux de travail ActiveVOS par défaut, vous devez acheter ActiveVOS Designer pour modifier les flux de travail.

Mettre à jour la configuration d'IDD pour l'adaptateur de flux de travail Siperian

Pour afficher les tâches de l'adaptateur de flux de travail Siperian dans le gestionnaire des tâches, mettez à jour la configuration des tâches dans le fichier de configuration d'Informatica Data Director.

1. Mettez à jour la configuration des types de tâches Siperian BPM.
   - Remplacez `defaultApproval="true"` par `defaultApproval="false"`.
   - Définissez `creationType` sur `NONE`.
2. Ajoutez la configuration des tâches pour les tâches ActiveVOS.
   L'exemple de code suivant illustre comment configurer des tâches ActiveVOS basées sur des entités commerciales dans le fichier de configuration d'Informatica Data Director :

```
<tasks includeUnassignedTasks="true">
  <!-- Task Definitions -->
    <taskType taskTypeId="BeMergeTask" name="AVOSBeMerge" displayName="Merge"
    creationType="MERGE" displayType="MERGE">
    <description>Merge two records together.</description>
  </taskType>

  <taskType taskTypeId="BeUnmergeTask" name="AVOSBeUnmerge"
    displayName="Unmerge" creationType="UNMERGE" displayType="UNMERGE">
    <description>Unmerge an XREF record from a Base Object record.
    </description>
  </taskType>

  <taskType taskTypeId="BeOneStepApprovalTask" name="AVOSBeFinalReview"
displayType="NORMAL"
    displayName="Final review" creationType="NONE" pendingBVT="true">
    <description>Update a record and require the user to go through an
    approval process before completing the task.
    </description>
  </taskType>

  <taskType name="AVOSBeNotification" displayName="Notification"
    creationType="NONE" displayType="NORMAL">
    <description>Notification step in the workflow</description>
  </taskType>

  <taskType taskTypeId="BeTwoStepApprovalTask" name="AVOSBeReviewNoApprove"
displayType="NORMAL"
```

```
    displayName="Review no approve" creationType="NONE" defaultApproval="true"
pendingBVT="true">
    <description>Update a record and require the user to go through an
    approval process before completing the task.
    </description>
  </taskType>

  <taskType taskTypeId="BeUpdateWithApprovalTask" name="AVOSBeUpdate"
    displayName="Update" creationType="CREATE" pendingBVT="true"
displayType="NORMAL">
    <description>Update a record and do not require the user to go through an
approval
    process before completing the task. The approval step is optional.
    </description>
  </taskType>
</tasks>
```

Configurer l'attribution des tâches

Pour configurer l'attribution des tâches pour l'adaptateur de flux de travail ActiveVOS en fonction des entités commerciales, utilisez le gestionnaire de configuration IDD pour configurer l'attribution des tâches pour chaque domaine. L'utilisateur peut attribuer directement la tâche ou autoriser le gestionnaire des tâches à attribuer des tâches aux utilisateurs.

1. Connectez-vous au gestionnaire de configuration Informatica Data Director.

   `http://[hôte]:[port]/bdd/config/`

2. Sélectionnez l'application à mettre à jour.
3. Cliquez sur **Modifier**.
4. Dans l'onglet Domaines, sélectionnez un domaine, puis cliquez sur **Modifier un domaine**.
5. Cliquez sur l'onglet **Attribution des tâches**, puis cliquez sur **Ajouter**.
6. Dans la boîte de dialogue Attribution des tâches, sélectionnez la tâche à configurer dans la liste des tâches.
7. Sélectionnez les rôles et les utilisateurs auxquels la tâche peut être attribuée. Cliquez sur **OK**.
8. Cliquez sur **Enregistrer**.
9. Cliquez sur **Générer le schéma d'entité commerciale**. Le gestionnaire de configuration génère la configuration d'entité commerciale et de service d'entité commerciale.
10. Dans MDM Hub, utilisez le gestionnaire de référentiel pour valider le stockage de référence opérationnelle. La validation du gestionnaire de référentiel actualise les données du référentiel mises en cache dans le serveur d'application.

Configurer le moteur de flux de travail principal

Pour configurer le moteur de flux de travail principal, ajoutez un moteur de flux de travail pour les flux de travail ActiveVOS basés sur des entités commerciales. Lorsque vous ajoutez le moteur de flux de travail ActiveVOS basé sur des entités commerciales, il devient le moteur de flux de travail principal, tandis que le moteur de flux de travail Siperian BPM devient le moteur de flux de travail secondaire. Vous ne pouvez pas créer de tâches avec le moteur de flux de travail secondaire.

Important: Si vous ajoutez un moteur de flux de travail alors que Siperian BPM est l'adaptateur de flux de travail secondaire, le moteur de flux de travail Siperian BPM est annulé dans le stockage de référence opérationnelle et les tâches sont supprimées de la boîte de réception.

1. Dans la console Hub, cliquez sur **Gestionnaire de flux de travail** dans l'espace de travail de configuration.

2. Obtenez un verrou en écriture.
3. Sélectionnez l'onglet **Moteurs de flux de travail** et cliquez sur le bouton **Ajouter**.
4. Dans la boîte de dialogue **Ajouter un flux de travail**, entrez les propriétés du moteur de flux de travail.

   Le tableau suivant décrit les propriétés du moteur de flux de travail :

Champ	Description
Moteur de flux de travail	Nom d'affichage du moteur de flux de travail
Nom d'adaptateur	Sélectionnez **BE ActiveVOS** pour l'adaptateur de flux de travail ActiveVOS en fonction des entités métier.
Hôte	Nom d'hôte de l'instance d'Informatica ActiveVOS.
Port	Nom de port de l'instance d'Informatica ActiveVOS.
Username	Nom de l'utilisateur de confiance.
Password	Mot de passe de l'utilisateur de confiance.
Protocole	Protocole de communication entre MDM Hub et ActiveVOS. Le protocole peut être HTTP ou HTTPS.

5. Cliquez sur **OK**.

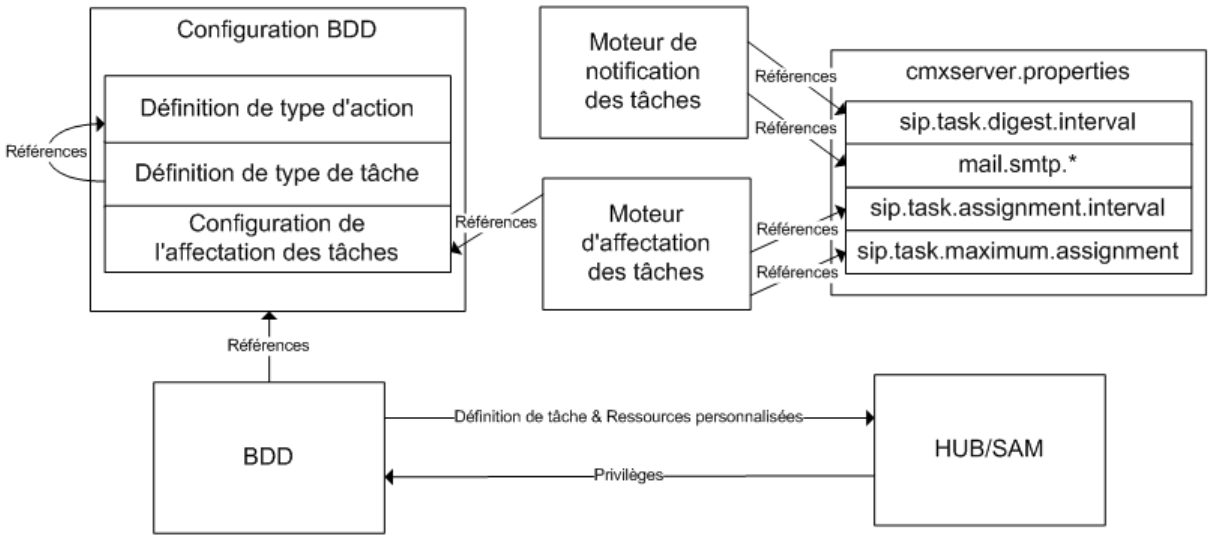
Flux de travail et tâches

Lors de l'utilisation de l'outil Siperian BPM hérité ou d'outils BPM tiers, vous devez configurer les tâches et la gestion des tâches pour votre application IDD.

Remarque: cette section ne s'applique pas à Informatica ActiveVOS, qu'il soit intégré ou autonome. La version intégrée utilise des tâches prédéfinies. La version autonome requiert que vous définissiez des tâches dans Informatica ActiveVOS.

Diagramme des composants de configuration des tâches et des flux de travail

Le diagramme suivant montre les composants de configuration des flux de travail et des tâches et leurs relations.



Description des composants de configuration des tâches et des flux de travail

Composant	Description
Définition de type d'action	Les *types d'actions* sont les blocs de construction réutilisables pour les tâches d'un flux de travail. Ils définissent la fonction d'une tâche quand une action est effectuée dans le contexte de la tâche. Ils sont réutilisables, car de nombreuses tâches fourniront des sous-ensembles d'actions similaires, qui peuvent être exécutés. **Remarque:** La Définition de type d'action peut être personnalisée seulement de manière très limitée dans cette version. Toutefois, une possibilité de personnalisation supplémentaire est prévue pour les versions futures.
Définition de type de tâche	Les *types de tâches* définissent les types de tâches qui peuvent être utilisés pour créer des flux de travail dans une application IDD. Cette section de la configuration permet de personnaliser les tâches disponibles et leur comportement général. Pour plus d'informations, voir « Types de tâches » plus loin dans ce document.
Configuration de l'affectation des tâches	Utilisé pour spécifier le comportement des mécanismes automatiques et manuels d'affectation des tâches. Elle est configurée via le gestionnaire de configuration IDD (voir "Gestionnaire de configuration IDD" précédemment dans ce document).
Moteur de notification des tâches	Exécuté dans Informatica MDM Hub et envoie des notifications par e-mail aux utilisateurs à un intervalle configuré.
Moteur d'affectation des tâches	Exécuté dans Informatica MDM Hub et affecte régulièrement toute tâche non affectée aux utilisateurs configurés.

Composant	Description
fichier cmxserver.properties	Spécifie plusieurs propriétés qui peuvent être définies pour configurer le comportement des tâches. Ces propriétés sont décrites en détails dans les sections applicables plus loin dans ce document.
IDD	L'application principale charge la configuration au démarrage (et lors du déploiement). IDD synchronise également la configuration des tâches avec le GAS en créant des métadonnées de tâches et des ressources sécurisées personnalisées dans Informatica MDM Hub.
GAS	Fournit des informations à IDD sur les privilèges accordés aux utilisateurs pour les types de tâches.

Remarque: Lors de l'utilisation de flux de travail et de tâches avec une application IDD, les possibilités des tâches ne sont disponibles que si tous les objets de base impliqués dans un domaine ont la gestion d'état activée dans le gestionnaire de schéma dans la Console Hub. C'est nécessaire car certaines tâches utilisent des enregistrements en attente, qui sont disponibles uniquement lorsque la gestion d'état est activée.

Configuration des tâches

Chaque application IDD est initialisée avec une définition de tâche et de flux de travail par défaut.

Les affectations de tâches sont configurées dans le gestionnaire de configuration IDD. Dans de nombreux cas, la définition par défaut sera adéquate. Toutefois, la configuration des affectations de tâches sera toujours requise. Chacune des sous-sections suivantes se concentre sur une partie de cette configuration.
Remarque: Par défaut, la configuration des tâches pour IDD est un processus d'approbation en deux étapes.

Types de tâches

Cette section du fichier de configuration IDD spécifie les types de tâches dans une application IDD.

Les types de tâches sont les composants de tâches les plus configurables. Cette section détermine le comportement des tâches dans Informatica MDM Hub, ainsi que le passage d'une tâche à la suivante.

La configuration par défaut d'IDD inclut sept tâches prédéfinies :

Tâches prédéfinies	Description
UpdateWithApproval	Mettre à jour un enregistrement et l'étape suivante nécessite que l'utilisateur subisse un processus d'approbation avant de terminer la tâche.
UpdateWithOptionalApproval	Mettre à jour un enregistrement et l'étape suivante ne nécessite pas que l'utilisateur subisse un processus d'approbation avant de terminer la tâche. L'étape d'approbation est facultative.

Tâches prédéfinies	Description
ReviewNoApprove	Contrôlez une modification et faites-la remonter ou rejetez-la. Cette tâche ne propose pas d'option Approuver et exige qu'au moins une autre personne contrôle également les modifications.
FinalReview	Vérifier une modification et l'approuver, la rejeter ou la remonter.
Fusionner	Fusionner des enregistrements.
Annuler la fusion	Annuler la fusion d'un enregistrement XREF depuis un enregistrement d'objet de base.
UpdateRejectedRecord	Mettre à jour un enregistrement qui a été rejeté dans un processus d'approbation.

Types de tâches - Échantillon XML

L'extrait suivant d'un fichier de configuration IDD concerne les types de tâches (et sera pris comme référence plus loin dans cette sous-section).

```
<!-- Task Definitions -->
        <taskType name="UpdateWithApproval" displayName="Update With Approval"
                  creationType="create">
            <description>Update a record and require the user to go through
                         an approval process before completing the task.
            </description>
            <action name="SubmitForApproval">
                <targetTask>ReviewNoApprove</targetTask>
            </action>
            <action name="Augment">
                <targetTask>UpdateWithApproval</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
         <taskType name="UpdateWithOptionalApproval" displayName="Update With Optional
Approval"
                   creationType="create">
            <description>Update a record and do not require the user to go through
                         an approval process before completing the task. The approval
step
                         is optional.
            </description>
            <action name="CompleteUpdate"/>
            <action name="SubmitForApproval">
                <targetTask>ReviewNoApprove</targetTask>
            </action>
            <action name="Augment">
                <targetTask>UpdateWithOptionalApproval</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
        <taskType name="ReviewNoApprove" displayName="Review" defaultApproval="true"
                  creationType="none" pendingBVT="true">
            <description>Review a change and either escalate or reject it. This task
                         does not provide an Approve option and requires at least one
                         other person to review the changes as well.
            </description>
            <action name="Reject">
                <targetTask>UpdateWithApproval</targetTask>
            </action>
            <action name="Escalate">
                <targetTask>FinalReview</targetTask>
```

```
            </action>
            <action name="Reassign">
                <targetTask>ReviewNoApprove</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
        <taskType name="FinalReview" displayName="Final Review" creationType="none"
                  pendingBVT="true">
            <description>Review a change and approve, reject or escalate it.</
description>
            <action name="Approve"/>
            <action name="Reject">
                <targetTask>UpdateWithApproval</targetTask>
            </action>
            <action name="Escalate">
                <targetTask>FinalReview</targetTask>
            </action>
            <action name="Reassign">
                <targetTask>FinalReview</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
        <taskType name="Merge" displayName="Merge" creationType="merge"
displayType=”merge”>
            <description>Merge two records together.</description>
            <action name="Reassign">
                <targetTask>Merge</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
        <taskType name="Unmerge" displayName="Unmerge" creationType="unmerge"
                  displayType=”unmerge”>
            <description>Unmerge an XREF record from a Base Object record.</description>
            <action name="Unmerge"/>
            <action name="Reassign">
                <targetTask>Unmerge</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
```

Vous pouvez personnaliser les flux de travail et les tâches en modifiant les propriétés des types de tâches. Il faut être vigilant lors de toute modification de la définition de tâche, car des erreurs à ce niveau peuvent rendre les tâches inutilisables dans une application IDD. La définition des tâches inclut les propriétés suivantes.

Attributs TaskType et balises

nom

L'attribut de nom est l'identificateur du type de tâche. N'utilisez pas d'espaces et de caractères non-ASCII pour l'attribut de nom.

L'attribut de nom est destiné à un usage interne par une application IDD et Informatica MDM Hub et il n'est donc pas nécessaire de modifier ces paramètres. Si vous présentez un nouveau type de tâche, vous pouvez spécifier n'importe quel nom vu qu'il n'aura pas d'incidence.

displayName

L'attribut displayName indique le nom de la tâche qui doit s'afficher dans une application IDD.

Toutefois, le nom réel affiché dans une application IDD est issu d'un ensemble de ressources. De ce fait, les modifications apportées à la valeur displayName peuvent ne pas être visibles dans l'application IDD déployée. Le nom d'affichage est utilisé comme valeur par défaut lorsque l'application IDD extrait le nom d'affichage localisé depuis un ensemble de ressources.

creationType

Cet attribut ne doit pas être modifié pour les tâches existantes.

Il sert à déterminer où une tâche peut être créée dans une application IDD. Les valeurs possibles sont :

creationType	Description
création	Les tâches sont créées quand l'utilisateur de l'application IDD choisit Créer une tâche dans un menu de l'application IDD. **Remarque:** Lors de la création d'une tâche à l'aide de **Plus d'actions** > **Créer la tâche**, dans la fenêtre **Créer la tâche**, seules les tâches configurées comme **CREATE** pour l'option **Type de création** seront listées dans le champ déroulant **Type**.
fusionner	Une tâche est créée quand l'utilisateur de l'application IDD choisit la commande pour créer une tâche dans la vue Correspondances potentielles. **Remarque:** Seul un type de tâche doit avoir cette désignation.
annuler la fusion	Les tâches sont créées quand l'utilisateur de l'application IDD choisit la commande pour créer une tâche dans la boîte de dialogue Références croisées **Remarque:** Seul un type de tâche doit avoir cette désignation.
aucun	Les tâches ne peuvent pas être créées par un utilisateur de l'application IDD dans l'application IDD. Cette désignation indique que ces types de tâches peuvent uniquement être créés à la suite d'un flux de travail.

Exemple: Le type de tâche FinalReview a cette désignation dans l'exemple de code précédent car ce type de tâche ne peut être créé que dans le cadre d'un flux (lorsque l'action Remonter est exécutée sur une tâche ReviewNoApprove).

displayType

Cet attribut spécifie comment une tâche doit être affichée lors de son ouverture dans la vue des données.

Les valeurs possibles sont :

displayType	Description
Normal	La tâche est ouverte dans la vue des données avec le menu des actions de tâche disponible. La vue des données présentera l'enregistrement de données associé à la tâche.
Fusionner	La tâche est ouverte dans la vue des données avec le menu des actions de tâche disponible. L'onglet enfant Correspondances potentielles est visible et sélectionné dans la vue des données. La correspondance potentielle associée à la tâche est mise en surbrillance et sélectionnée automatiquement dans l'onglet enfant Correspondances potentielles.
annuler la fusion	La tâche est ouverte dans la vue des données avec le menu des actions de tâche disponible. La boîte de dialogue Références croisées est ouverte au-dessus de la vue des données. L'enregistrement de référence croisée dont la fusion doit être annulée est sélectionné dans la boîte de dialogue.

dataUpdateType

Une des valeurs suivantes.

dataUpdateType	Description
ACTIVE	Les modifications apportées à l'enregistrement indiqué dans la vue de tâche avant d'exécuter cette action sont enregistrées dans l'état ACTIVE.
PENDING	Les modifications apportées à l'enregistrement indiqué dans la vue de tâche avant d'exécuter cette action sont enregistrées dans l'état PENDING. Cette valeur est utilisée pour tous les flux d'approbation afin d'enregistrer les modifications comme étant en attente jusqu'à ce qu'elles soient approuvées.
NONE	Les modifications apportées à l'enregistrement indiqué dans la vue de tâche avant d'exécuter cette action seront perdues. Dans ce cas, l'utilisateur de l'application IDD voit une boîte de dialogue de confirmation pour confirmer qu'il veut abandonner toute modification apportée à l'enregistrement. Les modifications peuvent être enregistrées à l'aide du bouton **Enregistrer** dans la vue des données avant d'exécuter l'action de tâche.

pendingBVT

Cet attribut spécifie si la vue de données doit inclure les valeurs de références croisées en attente lors de la construction de la vue BVT dans une application IDD.

Quand cet attribut est défini comme vrai, toute référence croisée en attente référencée par cette tâche sera incluse dans la vue BVT. Ainsi, les utilisateurs obtiennent une vue en mode « simulation » de l'enregistrement tel qu'il s'afficherait si les références croisées en attente étaient activées. Ceci est utile pour approuver les modifications en attente et pour décider si l'enregistrement obtenu est correct.

defaultApproval

Cet attribut doit être défini sur vrai pour un seul type de tâche.

Le type de tâche qui a la valeur vrai pour cet attribut est le type de tâche qui sera créé lors d'un clic sur le bouton **Envoyer pour approbation** dans la vue des données de IDD.

Remarque: Si cet attribut est défini sur vrai pour plusieurs types de tâches, des résultats inattendus sont possibles si le type de tâche est créé lors d'un clic sur le bouton **Envoyer pour approbation**.

Balise de description

Cet élément propose une brève description de l'objectif du type de tâche.

Balise d'action

Cet élément est une référence à un type d'action décrit dans la section suivante.

Balise de tâche cible

Cette balise est facultative dans chaque action de tâche.

Lorsqu'elle est définie, elle spécifie le nom du type de tâche qui représente l'étape suivante dans le workflow lors de l'exécution de l'action associée.

Exemple: Lors de l'appel de l'action Remonter sur le type de tâche ReviewNoApprove, une nouvelle tâche FinalReview est créée comme étape suivante du workflow.

Si cette balise est omise, l'action termine le processus de workflow une fois exécuté.

Exemple: L'action d'annulation de la tâche, présente dans chaque type de tâche, mettra fin au workflow.

Personnalisation des types de tâches

Les types de tâches sont hautement personnalisables.

Il est possible de créer de nouveaux types de tâches tant que les règles décrites précédemment sont respectées. Les flux existants peuvent être modifiés en modifiant les valeurs dans les balises de tâches cibles pour un type de tâche donné. L'extrait de code suivant est un exemple de processus d'approbation en deux étapes et d'un processus d'approbation en une étape.

```
<taskType creationType="NONE" dataUpdateType="ACTIVE"
            defaultApproval="false" displayName="Final Review"
            displayType="NORMAL" name="FinalReview" pendingBVT="true">
            <description>Review a change and approve, reject or escalate it.</
description>
            <action name="Approve"/>
            <action name="Reject">
                <targetTask>UpdateRejectedRecord</targetTask>
            </action>
            <action name="Escalate">
                <targetTask>FinalReview</targetTask>
            </action>
            <action name="Reassign">
                <targetTask>FinalReview</targetTask>
            </action>
            <action name="CancelTask"/>
        </taskType>
```

Types d'actions

Cette section du fichier de configuration IDD spécifie les types d'actions utilisables par chaque tâche dans une application IDD.

Chaque type de tâche définit un ensemble d'actions possibles dans le contexte de la tâche. Comme plusieurs types de tâches peuvent avoir des actions identiques ou similaires disponibles, les types d'actions sont définis en dehors du contexte d'une tâche, et sont référencés depuis la définition de type de tâche, telle qu'elle est décrite précédemment.

Lorsque vous éditez une tâche dans le gestionnaire de configuration IDD, dans la fenêtre **Configuration de tâche**, vous pouvez configurer les types d'actions et l'étape suivante pour chaque tâche. Lorsque vous travaillez avec une tâche dans l'application IDD, seuls les types d'actions sélectionnés seront affichés à l'utilisateur sous forme de bouton et le type de tâche sélectionné dans la section **Étape suivante** sera exécuté à l'étape suivante du flux de travail pour ce type d'action particulier.

Remarque: Pour un type d'action sélectionné, si la valeur dans la section **Étape suivante** est **<Vide>**, l'action ferme le processus de flux de travail une fois exécuté.

Le tableau suivant fournit la liste des types d'actions et leur description :

Types d'actions	Description
SubmitForApproval	Soumission d'une modification à l'approbation.
Augmenter	Réaffectation de la tâche à un autre utilisateur pour obtenir de l'aide.
CompleteUpdate	Validation des modifications apportées à un enregistrement d'un domaine.
Approuver	Approbation et validation des modifications apportées à un enregistrement d'un domaine.
Rejeter	Rejet des modifications et réaffectation à l'utilisateur ayant effectué les modifications.
Remonter	Réaffectation de la tâche à un autre contrôleur pour obtenir de l'aide. Ceci peut entraîner la création d'une nouvelle tâche.
Réaffecter	Réaffectation de la tâche à un autre utilisateur / rôle.
Annuler la fusion	Exécution de l'opération d'annulation de la fusion définie par la tâche.
CancelTask	Annulation de la tâche en la supprimant.

Types d'actions - Échantillon XML

L'extrait suivant d'un fichier de configuration IDD concerne les types de tâches et sera pris comme référence plus loin dans cette sous-section.

```
<!-- Action Definitions - MUST come before the task types definitions. -->
        <actionType name="SubmitForApproval" displayName="Submit For Approval">
            <description>Submit a change for approval.</description>
            <class>com.siperian.dsapp.domain.task.action.SubmitForApproval</class>
        </actionType>
        <actionType name="Augment" displayName="Augment" manualReassign="true">
            <description>Reassign the task to another user for assistance.</description>
```

```
            <class>com.siperian.dsapp.domain.task.action.Reassign</class>
        </actionType>
        <actionType name="CompleteUpdate" displayName="Complete Update">
            <description>Commit changes made to a subject area record.</description>
            <class>com.siperian.dsapp.domain.task.action.CompleteUpdate</class>
        </actionType>
        <actionType name="Approve" displayName="Approve">
            <description>Approve and commit changes made to a subject area record.</
description>
            <class>com.siperian.dsapp.domain.task.action.Approve</class>
        </actionType>
        <actionType name="Reject" displayName="Reject">
            <description>Reject changes and reassign to the user
                        who made the changes.</description>
            <class>com.siperian.dsapp.domain.task.action.Reject</class>
        </actionType>
        <actionType name="Escalate" displayName="Escalate">
            <description>Reassign the task to another reviewer for assistance.
                        This could result in a new task being created.</description>
            <class>com.siperian.dsapp.domain.task.action.Reassign</class>
        </actionType>
        <actionType name="Reassign" displayName="Reassign" manualReassign="true">
            <description>Reassign the task to another user/role.</description>
            <class>com.siperian.dsapp.domain.task.action.Reassign</class>
        </actionType>
        <actionType name="Unmerge" displayName="Unmerge">
            <description>Perform the unmerge operation defined by the task.</description>
            <class>com.siperian.dsapp.domain.task.action.Unmerge</class>
        </actionType>
        <actionType name="CancelTask" displayName="Cancel Task" cancelTask="true">
            <description>Cancel the task by deleting it.</description>
            <class>com.siperian.dsapp.domain.task.action.CancelTask</class>
</actionType>
```

Attributs et balises ActionType

nom

L'attribut de nom d'un type d'action ne doit jamais être modifié.

Il est destiné à une utilisation interne par une application IDD et Informatica MDM Hub, si bien qu'il n'y a aucun besoin de modifier ces paramètres. Si un nouveau type d'action est introduit, tout nom peut être spécifié, car il n'aura pas d'incidence.

displayName

Il s'agit du nom de l'action tel qu'il apparaît dans une application IDD.

Toutefois, le nom réel affiché dans une application IDD est issu d'un ensemble de ressources, si bien que les modifications apportées à cette valeur peuvent ne pas être visibles dans l'application IDD.

Balise de description

Cet élément propose une brève description de l'objectif du type d'action.

manualReassign

Lorsque cet attribut est défini sur vrai, l'utilisateur de l'application IDD est invité à sélectionner un utilisateur spécifique pour l'affectation de la tâche avant l'exécution de l'action.

Il est utilisé, par exemple, lors de la réaffectation manuelle d'une tâche à un autre utilisateur. S'il est défini sur faux, l'affectation des tâches pour ce type d'action est automatique.

closeTaskView

Lorsque cet attribut est défini sur vrai, l'onglet dans lequel travaillait l'utilisateur de l'application IDD lors de cette action est fermé et l'utilisateur est renvoyé à la pageDémarrer un espace de travail.

L'extrait de fonctions suivant est un exemple de type d'action.

```
<actionType cancelTask="true" closeTaskView="true"
            displayName="Cancel Task" manualReassign="false" name="CancelTask">
            <description>Cancel the task by deleting it.</description>
            <class>com.siperian.dsapp.domain.task.action.CancelTask</class>
        </actionType>
```

Remarque: Vous pouvez configurer cet attribut pour chaque type d'action à l'aide du fichier de configuration IDD (IDDConfig.xml). La valeur par défaut de cet attribut est True.

cancelTask

Lorsque cet attribut est défini sur vrai, la tâche est annulée lorsque cette action est exécutée.

Ainsi, la tâche est entièrement supprimée et non récupérable, et toute modification en attente associée à la tâche est supprimée de manière permanente.

Balise Class

Cet attribut ne doit PAS être modifié dans cette version car il spécifie la classe Java utilisée pour exécuter l'action.

Il n'existe aucun moyen d'ajouter des systèmes de traitement d'actions personnalisés dans cette version, mais cette fonctionnalité est prévue dans une version future.

Configuration de la sécurité des tâches

Lors du déploiement d'une instance d'une application IDD, ou lors du redémarrage du serveur d'applications, l'application IDD synchronise un ensemble de ressources personnalisées avec Informatica MDM Hub.

Cet ensemble de ressources personnalisées inclut une ressource personnalisée pour chaque domaine, et chaque type de tâche par domaine (d'après le fichier de configuration IDD).

Utilisez l'outil Rôles de la Console Hub pour configurer la sécurité pour les tâches en spécifiant des privilèges sur les ressources personnalisées du type de tâche.

Les privilèges suivants pour les types de tâches sont appliqués dans une application IDD :

privilège	Description
Lire	Inutilisé.
Créer	Ce privilège est requis pour qu'un utilisateur de l'application IDD crée de nouvelles tâches. Lorsque l'utilisateur choisit la commande Créer une tâche depuis la vue des données, l'application IDD affiche une boîte de dialogue contenant une liste de types de tâches possibles à créer. Cette liste contient uniquement les types de tâches pour lesquels l'utilisateur a le privilège de création. Par ailleurs, les tâches affichées dans cette liste doivent aussi être configurées correctement dans le fichier de configuration IDD en définissant l'attribut creationType sur "créer".
Mettre à jour	Inutilisé.
Supprimer	Inutilisé.
Fusionner	Inutilisé.
Exécuter	Ce privilège est requis pour qu'un utilisateur de l'application IDD consulte les détails relatifs à une tâche et apporte des modifications aux détails de la tâche (ce qui inclut ajouter des commentaires, modifier la date d'échéance et même réaffecter la tâche). Les utilisateurs de l'application IDD ayant des privilèges d'exécution sur un type de tâche sont autorisés à exécuter toutes les actions pour ce type de tâche. Cela est vrai quoi que fasse l'action lorsqu'elle est exécutée. Par exemple, s'il y a une action qui crée une nouvelle tâche, l'utilisateur peut l'exécuter même s'il n'a pas de privilège de création sur le type de tâche créé par l'action.

Important: Les privilèges pour les tâches, domaines et objets de base fonctionnent tous ensemble dans le GAS. Une configuration du GAS incorrecte peut provoquer un comportement inattendu dans une application IDD. Les tâches sont affectées par rôle ou par utilisateur (dans le gestionnaire de configuration IDD, description ci-dessous). IDD ne vérifie pas que le rôle ou l'utilisateur bénéficie de la configuration de sécurité pour autoriser les opérations sur cette tâche. L'implémenteur de l'application IDD doit réaliser une configuration correcte. Par ailleurs, pour qu'un utilisateur de l'application IDD puisse annuler une tâche, il doit disposer du privilège DELETE sur la XREF de chaque objet de base dans un domaine.

Affectation des tâches

Configuration de l'affectation des tâches

Chaque Domaine de l'application IDD peut être configuré pour utiliser un ensemble spécifique de types de tâches.

Chaque type de tâche peut ensuite être associé à un ou plusieurs rôles de sécurité ou à un nom d'utilisateur unique. Cela signifie que la tâche d'un Type de tâche spécifique peut être uniquement affectée aux utilisateurs possédant les rôles de sécurité spécifiés, ou à l'utilisateur spécifié dans la définition Affectation des tâches.

Dans le fichier de configuration XML, l'affectation des tâches peut être définie à l'aide de la balise `taskAssignmentConfig`.

Exemple :

```
<taskAssignmentConfig task="UpdateWithApproval">
                    <securityRole roleUid="DataSteward"/>
                </taskAssignmentConfig>
                <taskAssignmentConfig task="UpdateWithOptionalApproval" >
                    <securityRole roleUid="DataSteward"/>
                    <securityRole roleUid="Customer-NY"/>
                </taskAssignmentConfig>
                <taskAssignmentConfig task="UpdateRejectedRecord" user=”user1”/>
                <taskAssignmentConfig task="ReviewNoApprove">
                    <securityRole roleUid="Manager"/>
                </taskAssignmentConfig>
                <taskAssignmentConfig task="FinalReview" >
                    <securityRole roleUid="SrManager"/>
                </taskAssignmentConfig>
                <taskAssignmentConfig task="Merge">
                    <securityRole roleUid="DataSteward"/>
                </taskAssignmentConfig>
                <taskAssignmentConfig task="Unmerge">
                    <securityRole  roleUid="DataSteward"/>
                </taskAssignmentConfig>
```

Dans l'exemple précédent, les tâches `UpdateWithOptionalApproval` peuvent être affectées à des utilisateurs ayant un rôle Gestionnaire des données ou Client-NY. Les tâches de type UpdateRejectedRecord ne peuvent être affectées qu'à un utilisateur (utilisateur1).

L'élément d'affectation des tâches doit contenir la tâche `attribut` requise, avec le nom de l'un des types de tâches définis dans la configuration IDD. Il doit également contenir un ou plusieurs rôles de sécurité d'un élément enfant, ou un attribut utilisateur avec le nom d'un utilisateur, auquel peut être affectée la tâche de type particulier.

Interface utilisateur de configuration de l'affectation des tâches

Vous pouvez spécifier l'affectation des tâches à l'aide de l'onglet Affectation des tâches de la boîte de dialogue Domaine d'IDD.

Lorsque vous cliquez sur l'onglet **Affectation des tâches**, les types de tâches pouvant être utilisés avec le Domaine sont affichés. Vous pouvez sélectionner un type de tâche et cliquer sur **Ajouter** pour l'ajouter au Domaine.

Si tous les types de tâches définis dans l'instance de l'application IDD sont déjà ajoutés au Domaine, le bouton Ajouter est désactivé.

Vous pouvez modifier un type Tâche sélectionné à l'aide du bouton **Éditer**. Le bouton **Supprimer** permet de retirer un type de tâche du Domaine.

Vous devez sélectionner l'option **Affecter au rôle** pour modifier ou ajouter des rôles. Les rôles de sécurité définis dans MDM Hub (à l'aide de MDM Hub) peuvent être déplacés vers la liste Rôles sélectionnés et associés au Type de tâche pour un Domaine.

Affectation automatique des tâches

L'affectation automatique des tâches est contrôlée via un démon de serveur exécuté dans Informatica MDM Hub.

Sa fréquence d'exécution est contrôlée par la valeur de la propriété sip.task.assignment.interval dans cmxserver.properties. Par défaut, elle est définie sur 0, ce qui signifie que le démon est désactivé. Il ne doit être activé que si vous exécutez des applications IDD et exigez l'affectation des tâches. Pour activer le démon, définissez une valeur en minutes pour sip.task.assignment.interval. Avec la valeur 1, le démon sera exécuté une fois par minute. Ce démon a deux tâches :

Il affecte toute tâche qui n'a pas de propriétaire (rowid_user null) d'après la configuration de l'affectation des tâches dans l'application IDD.

Il examine toutes les entrées de la table de correspondance associées à la table principale d'un domaine configuré et crée des tâches à affecter aux utilisateurs disponibles de l'application IDD.

Un *utilisateur disponible* (a) a un nombre de tâches actuellement affectées inférieur au nombre maximum configuré, et (b) a le rôle spécifié dans la configuration de l'affectation des tâches. Vous pouvez configurer le nombre maximum de tâches à affecter automatiquement à un utilisateur de l'application IDD en spécifiant la propriété sip.task.maximum.assignment dans le fichier cmxserver.properties. Par défaut, le nombre maximum de tâches à affecter par utilisateur est de 25.

Lorsque les tâches sont affectées automatiquement, les utilisateurs de l'application IDD ayant le rôle configuré sont sélectionnés pour l'affectation de la tâche à tour de rôle jusqu'à ce qu'il n'y ait plus aucun utilisateur qui a moins de tâches affectées que le maximum autorisé. Lors de chaque exécution du démon d'affectation, il affecte toutes les tâches non affectées qu'il peut. S'il n'y a pas assez d'utilisateurs pour recevoir toutes les tâches non affectées, il peut rester des tâches non affectées après l'exécution du démon (qui seront affectées lorsque de l'espace deviendra disponible dans la file d'attente des tâches d'un utilisateur de l'application IDD cible). Lors de l'affectation automatique des tâches, l'utilisateur de l'application IDD qui reçoit une tâche spécifique ne peut pas être prévu avec certitude. Si une tâche doit être affectée à un utilisateur spécifique, il convient d'utiliser l'affectation manuelle.

Personnalisation de l'attribution automatique des tâches

L'attribution automatique des tâches peut être personnalisée via la sortie utilisateur AssignTasks.

La sortie utilisateur AssignTasks fonctionne avec l'adaptateur de flux de travail Siperian BPM.

Affectation manuelle des tâches

L'affectation manuelle des tâches est contrôlée par l'utilisateur de l'application IDD dans l'application IDD.

Lors de la création de tâches, les utilisateurs ont la possibilité de sélectionner un utilisateur cible pour la tâche. Si cela est spécifié, l'utilisateur sélectionné devient le détenteur de la nouvelle tâche créée. En l'absence de spécification, le démon d'affectation automatique affecte la tâche à l'utilisateur disponible suivant.

Personnalisation de l'attribution des tâches

L'attribution manuelle des tâches peut être personnalisée via la sortie utilisateur GetAssignableUsersForTasks.

La sortie utilisateur GetAssignableUsersForTasks fonctionne avec l'adaptateur de flux de travail Siperian BPM.

Modification des tâches affectées

Les applications IDD peuvent administrer les affectations de tâches sous l'onglet d'administration des tâches.

Si une tâche est affectée à un utilisateur absent du bureau, par exemple, un administrateur peut utiliser l'application IDD pour affecter ses tâches à un autre utilisateur.

Si un utilisateur va être indisponible pendant un certain temps, vous pouvez éviter l'affectation automatique des tâches à cet utilisateur en le retirant du rôle.

Notification des tâches

La notification des tâches est simple.

À un intervalle défini, un e-mail récapitulatif peut être envoyé aux utilisateurs qui détiennent des tâches. Le démon est exécuté dans le cadre d'Informatica MDM Hub. L'intervalle d'envoi des notifications est configurable comme un nombre spécifié d'heures dans le fichier cmxserver.properties avec la propriété sip.task.digest.interval. L'intervalle de notification par défaut est de 0 heure, ce qui signifie que les récapitulatifs sont désactivés. Pour activer les récapitulatifs, définissez une valeur en heures.

L'exemple d'e-mail récapitulatif est comme indiqué ci-dessous :

```
De : siperian_task_notification@siperian.com À : null Objet : Récapitulatif des tâches
du gestionnaire des données pour admin Mime-Version : 1.0 Content-Type : text/plain;
charset=us-ascii Content-Transfer-Encoding: 7bit Tâches terminées depuis la dernière
notification : 0 Tâches totales affectées : 17 Ce message a été envoyé par le démon de
notification des tâches du serveur Hub Siperian.
```

Remarque: Vous ne pouvez pas personnaliser le corps du résumé de l'e-mail.

Configuration du courriel de notification des tâches

Pour configurer le courriel de notification des tâches, modifiez les propriétés dans le fichier cmxserver.properties. Vous devez configurer un emplacement de serveur SMTP sortant.

La liste suivante décrit les propriétés du courriel de notification des tâches que vous pouvez configurer dans le fichier cmxserver.properties :

mail.smtp.sender

Adresse électronique de l'expéditeur. La valeur par défaut est siperian_task_notification@siperian.com.

mail.smtp.host

Nom d'hôte du serveur de messagerie.

mail.smtp.port

Numéro de port du serveur de messagerie.

mail.smtp.auth

Détermine le besoin d'authentification ou non du serveur de messagerie spécifié pour les messages sortants. Vous devez définir mail.smtp.auth sur true si vous utilisez le serveur de messagerie Informatica MDM Hub.

mail.smtp.user

Nom d'utilisateur pour le serveur de messagerie sortant. Vous devez spécifier une valeur pour mail.smtp.user si la valeur de mail.smtp.auth est true.

mail.smtp.password

Mot de passe pour le mail.smtp.user spécifié. Vous devez spécifier une valeur pour mail.smtp.password si la valeur de mail.smtp.auth est true.

Configuration du gestionnaire d'utilisateurs dans la Console Hub

Par ailleurs, afin que les utilisateurs de l'application IDD reçoivent des e-mails, le compte de messagerie entrant doit être configuré dans Informatica MDM Hub.

Dans l'outil Utilisateurs de la Console Hub, spécifiez l'adresse électronique à laquelle des notifications doivent être envoyées à l'utilisateur IDD. Un e-mail sera envoyé uniquement si des tâches sont affectées à un utilisateur de l'application IDD.

Rapports et scores de gestion des tâches

Les mesures de gestion des tâches affichent la distribution des tâches d'Informatica Data Director.

Les administrateurs peuvent utiliser les mesures de gestion des tâches pour afficher la distribution des tâches d'Informatica Data Director. Vous pouvez générer des rapports basés sur les mesures de gestion des tâches suivantes :

Tâche de domaine par date de création

Les utilisateurs peuvent afficher les tendances des dates de création pour un domaine. Utilisez`task_sa_by_create_date` en tant que nom du rapport pour configurer et remplir l'entrepôt de données pour ce rapport.

Tâche de domaine par date d'échéance

Les utilisateurs peuvent afficher des rapports basés sur le nombre d'enregistrements avec des plages de dates spécifiées par l'administrateur lors de la configuration du rapport. Utilisez`task_sa_by_due_date` en tant que nom du rapport pour configurer et remplir l'entrepôt de données pour ce rapport.

Tâche de domaine par priorité

Les utilisateurs peuvent afficher des rapports basés sur le nombre d'enregistrements avec des priorités telles que « Faible », « Moyenne » et « Élevée ». Utilisez`task_sa_by_priority` en tant que nom du rapport pour configurer et remplir l'entrepôt de données pour ce rapport.

Tâche de domaine par statut

Les utilisateurs peuvent afficher des rapports basés sur le nombre d'enregistrements avec les statuts d'échéance tels que « Ponctuel » et « En retard ». Utilisez`task_sa_by_status` en tant que nom du rapport pour configurer et remplir l'entrepôt de données pour ce rapport.

Tâche de domaine par type de tâche

Les utilisateurs peuvent afficher des rapports basés sur le nombre d'enregistrements avec les types de tâches tels que « Mise à jour avec approbation », « Fusion » et « Annuler la fusion ». Utilisez`task_sa_by_task_type` en tant que nom du rapport pour configurer et remplir l'entrepôt de données pour ce rapport.

Tâche par domaine

Les utilisateurs peuvent afficher des rapports basés sur le nombre d'enregistrements avec des domaines tels que « Personne », « Organisation » et « Produit ». Utilisez`task_by_subject_area` en tant que nom du rapport pour configurer et remplir l'entrepôt de données pour ce rapport.

Attributaire de tâche par priorité

Les utilisateurs peuvent afficher des rapports basés sur le nombre d'enregistrements d'un attributaire disposant de priorités telles que « Faible », « Moyenne » et « Élevée» Utilisez`task_assignee_by_priority` en tant que nom du rapport pour configurer et remplir l'entrepôt de données pour ce rapport.

Attributaire de tâche par statut

Les utilisateurs peuvent afficher des rapports basés sur le nombre d'enregistrements pour un attributaire qui a les statuts d'échéance tels que « Ponctuel » et « En retard ». Utilisez`task_assignee_by_status` en tant que nom du rapport pour configurer et remplir l'entrepôt de données pour ce rapport.

Sécurité des données dans les données de tâche

IDD permet aux utilisateurs autorisés de participer à des flux de travail, qui sont des modèles informatiques de travail réel impliquant une série d'opérations ou d'activités. La sécurité des données IDD impacte les parties suivantes de la tâche :

- Vérifier les autorisations d'affichage - si une tâche peut être ouverte par un utilisateur ou non. Si l'utilisateur n'est pas autorisé à ouvrir une tâche, un message d'avertissement est affiché à l'utilisateur.
- Filtrer les données enfants - quels enregistrements enfants sont vus par l'utilisateur dans la vue des données.

Remarque:

- Les filtres de sécurité des données ne sont pas appliqués sur les données XREF. Par exemple, si un utilisateur a accès aux données de l'objet principal et aux données de ses enfants alors, selon la sécurité des données, l'utilisateur est autorisé à voir toutes les références croisées contributives.
- La logique de l'application des filtres de sécurité des données dépend du type de tâche.

Tâche de révision

La principale différence entre l'ouverture des objets principaux standard et le contrôle des tâches dans la vue des données est que les filtres de sécurité ne sont pas appliqués à un état actif de l'objet principal et de ses enfants. La sécurité des données est appliquée après que la fonction d'aperçu MVV ait été exécutée sur tous les enregistrements en attente associés à la tâche.

Ouvrir des tâches de révision avec un rôle unique

Un utilisateur avec un rôle unique peut ouvrir une tâche uniquement si les conditions suivantes sont satisfaites :

- Tous les enregistrements en attente associés à la tâche doivent respecter les filtres de sécurité des données.
- S'il existe plusieurs filtres sur une colonne unique pour un rôle unique, l'utilisateur a accès à une union de toutes les données qui répondent à chaque filtre.
- S'il existe des filtres sur plusieurs colonnes pour un rôle unique, l'utilisateur a alors accès à une intersection de toutes les données qui répondent à chaque filtre.
- S'il existe des filtres de sécurité configurés sur les enregistrements enfants ou petits-enfants, alors une des conditions suivantes doit être True :
  - Un objet principal a au moins un enregistrement passant des restrictions de sécurité dans chaque onglet enfant avec la sécurité des données activée.
  - Il y a un enregistrement en attente associé à la tâche, qui appartient à l'onglet enfant, avec la sécurité des données activée et qui répond aux paramètres de sécurité des données conformément à la condition précédente.

Par exemple, prenez un modèle de sécurité des données dans lequel l'utilisateur a le rôle SalesManager- NY et a les filtres de sécurité suivants configurés :

- Filtre 1 : le code d'état est NY.
- Filtre 2 : le type de téléphone est Entreprise et Domicile.
- Filtre 3 : le code de titre de civilité est M.

À l'aide du modèle de sécurité des données mentionné ci-dessus, imaginez un scénario dans lequel la base de données a un enregistrement d'objet principal M. Florian Amadeu, qui a une adresse de facturation dans l'État de NY et un type de téléphone Fax. Un utilisateur sans restrictions de sécurité des données ajoute un nouveau numéro de téléphone Professionnel et crée une tâche **Envoyer pour approbation**. L'utilisateur avec le rôle Sales Manager- NY pourra ouvrir l'enregistrement M. Florian Amadeu dans la vue des données, car il satisfait les trois conditions ci-dessus, l'objet principal lui-même satisfait la sécurité des données (Filtre3) et a au moins un enregistrement dans chaque enfant où la sécurité des données est activée – adresse NY (enregistrement actif) et téléphone PROFESSIONNEL (enregistrement en attente).

À l'aide du même modèle de sécurité des données, imaginez un scénario dans lequel la base de données a un enregistrement d'objet principal M. Dominic Wilkins, qui a une adresse de facturation dans l'État de NY et aucun type de téléphone. Un utilisateur sans restrictions de sécurité des données ajoute un nouveau numéro de téléphone professionnel et crée une tâche **Envoyer pour approbation**. L'utilisateur avec le rôle Sales Manager- NY ne pourra pas ouvrir la tâche, car l'utilisateur n'a pas de téléphone qui satisfait le Filtre2.

Ouvrir des tâches de révision avec plusieurs rôles

L'utilisateur avec plusieurs rôles peut ouvrir la tâche uniquement si les conditions suivantes sont satisfaites.

- Tous les enregistrements en attente associés à la tâche doivent satisfaire les filtres de sécurité des données pour au moins un rôle utilisateur.
- Un utilisateur avec plusieurs rôles peut se voir appliquer des combinaisons de filtres. Le résultat est que l'utilisateur a accès à toutes les données disponibles dans chaque rôle affecté - une union des affectations de filtres.
- Si les filtres de sécurité sont configurés sur les enfants ou petits-enfants, une des conditions suivantes doit être vraie.
  - Un objet principal a au moins un enregistrement passant des restrictions de sécurité dans chaque onglet enfant avec la sécurité des données activée.
  - L'enregistrement en attente associé à la tâche a un onglet enfant avec la sécurité des données activée et correspond au paramètre de la sécurité des données comme mentionné dans la condition précédente.

Par exemple, imaginez un modèle de sécurité des données dans lequel l'utilisateur a le rôle Sales Manager-NY, possède les filtres de sécurité des données comme mentionné dans la section "Ouvrir des tâches de révision avec un rôle unique" à la page 168 et possède également le rôle CarSalesManager-NJ qui présente les filtres de sécurité suivants.

- Filtre 1 : le code d'État est NJ.
- Filtre 2 : l'année de la voiture est 2009.

En outre, l'utilisateur a un autre rôle CarSalesManager-CA qui a le filtre de sécurité suivant configuré.

- Filtre 1 : le code d'état de l'adresse est CA.
- Filtre 2 : l'année de la voiture est 2008.

À l'aide du modèle de sécurité des données mentionné ci-dessus, imaginez un scénario dans lequel la base de données a un enregistrement d'objet principal M. Derrick Rose, qui a une adresse de facturation dans l'État de CA et un type de téléphone Domicile. Un utilisateur sans restrictions de sécurité des données ajoute une nouvelle adresse de facturation dans l'état de NY et crée une tâche **Envoyer pour approbation**. L'utilisateur avec le rôle Sales Manager- NY pourra ouvrir l'enregistrement M. Derrick Rose dans la vue des données, car il satisfait les filtres de sécurité du rôle SalesManager-NY.

À l'aide du même modèle de sécurité des données mentionné ci-dessus, imaginez un scénario dans lequel la base de données a un enregistrement d'objet principal M. Tyros Thomas, qui a une adresse de facturation dans l'État de CA et une voiture fabriquée en 2008. Un utilisateur sans restrictions de sécurité des données a modifié l'adresse de facturation pour NJ et crée une tâche **Envoyer pour approbation**. L'utilisateur avec les deux rôles CarSalesManager-CA et CarSalesManager-NJ n'est pas autorisé à ouvrir la tâche, car M. Tyros

Thomas ne satisfait pas les filtres de CarSalesManager-CA et CarSalesManager-NJ avec l'enregistrement en attente pour la nouvelle adresse.

Filtrer un enregistrement enfant dans la vue de tâche

IDD applique des filtres de sécurité lors de la récupération des données pour les onglets enfants dans la vue des données. Par exemple, prenez un modèle de sécurité des données dans lequel l'utilisateur a le rôle SalesManager-CA et a le filtre de sécurité de code d'état d'adresse de facturation CA.

À l'aide du modèle de sécurité des données mentionné ci-dessus, imaginez un scénario dans lequel la base de données a un enregistrement d'objet principal, M. Blake Griffin, qui a deux adresses de facturation dans les villes de New York et Bloomfield Hills, toutes deux dans l'État de NY. L'utilisateur sans restrictions de sécurité des données modifie la valeur de l'État de Bloomfield Hills en CA, crée une adresse de facturation supplémentaire à Los Angeles (État de Californie) et crée ensuite une tâche **Envoyer pour approbation**. L'utilisateur avec le rôle Sales Manager- NY pourra ouvrir l'enregistrement de M. Blake Griffin dans la vue des données et peut voir deux adresses CA dans l'onglet **Adresse de facturation**. L'une des deux est l'ancienne adresse à NY qui est modifiée, la deuxième est la nouvelle adresse ajoutée. L'adresse à NY qui n'est pas changée est filtrée lorsque les filtres de sécurité sont appliqués sur l'aperçu MVV.

Ouvrir des tâches de fusion / annulation de fusion

IDD applique les règles suivantes pour déterminer si la tâche de fusion ou d'annulation de la fusion peut être ouverte par l'utilisateur.

- La tâche de fusion ne peut être ouverte que si tous les objets primaires devant être fusionnés correspondent aux paramètres de la sécurité des données.
- La tâche d'annulation de la fusion peut être ouverte si l'objet principal peut être ouvert selon les paramètres de sécurité des données.

Par exemple, prenez un modèle de sécurité des données dans lequel l'utilisateur a le rôle SalesManager-CA et a le filtre de sécurité de code d'État d'adresse de facturation CA.

À l'aide du modèle de sécurité des données mentionné ci-dessus, imaginez un scénario dans lequel deux personnes dans la base de données ont le même nom Kevin Durant. L'un des individus a une adresse de facturation à Los Angeles (État de Californie) et l'autre a une adresse de facturation à New York (État de NY). L'utilisateur sans restrictions de sécurité des données crée une tâche **Fusion** pour les enregistrements des deux personnes. Les utilisateurs avec le rôle SalesManager- CA ne pourront pas ouvrir la tâche, car ils n'ont pas l'autorisation requise pour ouvrir l'enregistrement d'une personne avec l'adresse de facturation dans l'État de NY et, par conséquent, ne peuvent pas effectuer une tâche entière **Fusion**.

Affectation de tâches compatibles avec les données

Lors de l'attribution d'une tâche dans la boîte de dialogue **Assigner une tâche** , IDD filtre les contrôleurs de tâche qui n'ont pas le privilège pour ouvrir la tâche. Par ailleurs, pour l'affectation automatique des tâches, le démon affecte la tâche uniquement aux utilisateurs qui ont le privilège d'ouvrir la tâche.

ANNEXE H

Codes de paramètres régionaux

Cette annexe comprend les rubriques suivantes :

- Codes de langue, 171
- Codes de pays, 176

Codes de langue

Code ISO	Langue
aa	Afar
ab	Abkhaze
af	Afrikaans
am	Amharique
ar	Arabe
as	Assamais
ay	Aymara
az	Azéri
ba	Bachkir
be	Biélorusse
bg	Bulgare
bh	Bihari
bi	Bichelamar
bn	Bengali, Bangla
bo	Tibétain

Code ISO	Langue
br	Breton
ca	Catalan
co	Corse
cs	Tchèque
cy	Gallois
da	Danois
de	Allemand
dz	Dzongkha
el	Grec
en	Anglais
eo	Esperanto
Es	Espagnol
et	Estonien
eu	Basque
fa	Perse
fi	Finnois
fj	Fidjien
fo	Féroïen
fr	Français
fy	Frison
ga	Irlandais
gd	Gaélique écossais
gl	Galicien
gn	Guarani
gu	Gujarati
ha	Haoussa
he	Hébreu (anciennement iw)

Code ISO	Langue
hi	Hindi
hr	Croate
hu	Hongrois
hy	Arménien
ia	Interlingua
id	Indonésien (anciennement in)
ie	Interlingue
ik	Inupiak
is	Islandais
it	Italien
iu	Inuktitut
ja	Japonais
jw	Javanais
ka	Géorgien
kk	Kazakh
kl	Groenlandais
km	Cambodgien
kn	Kannada
ko	Coréen
ks	Kashmiri
ku	Kurde
ky	Kirghiz
la	Latin
ln	Lingala
lo	Lao
lt	Lituanien
lv	Letton

Code ISO	Langue
mg	Malgache
mi	Maori
mk	Macédonien
ml	Malayalam
mn	Mongol
mo	Moldave
mr	Marathi
ms	Malais
mt	Maltais
my	Birman
na	Nauru
ne	Népalais
nl	Néerlandais
no	Norvégien
oc	Occitan
om	Oromo
ou	Oriya
pa	Pendjabi
pl	Polonais
ps	Pachto, Pachtoune
pt	Portugais
qu	Quechua
rm	Romanche
rn	Kirundi
ro	Roumain
ru	Russe
rw	Kinyarwanda

Code ISO	Langue
sa	Sanskrit
sd	Sindhi
sg	Sango
sh	Serbo-Croate
si	Cingalais
sk	Slovaque
sl	Slovène
sm	Samoan
sn	Shona
so	Somali
sq	Albanais
sr	Serbe
ss	Siswati
st	Sotho du Sud
su	Soudanais
sv	Suédois
sw	Swahili
ta	Tamoul
te	Télougou
tg	Tadjik
th	Thaï
ti	Tigrigna
tk	Turkmène
tl	Tagalog
tn	Tswana
to	Tongien
tr	Turc

Code ISO	Langue
ts	Tsonga
tt	Tatar
tw	Twi
ug	Ouïghour
uk	Ukrainien
ur	Ourdou
uz	Ouzbek
vi	Vietnamien
vo	Volapük
wo	Wolof
xh	Xhosa
yi	Yiddish (anciennement ji)
yo	Yoruba
za	Zhuang
zh	Chinois
zu	Zoulou

LIENS CONNEXES :

- "Tables de recherche avec colonne de sous-type" à la page 66

Codes de pays

Pays	Code à deux lettres	ISO #
ILES ALAND	AX	248
AFGHANISTAN	AF	4
ALBANIE	AL	8
ALGERIE	DZ	12

Pays	Code à deux lettres	ISO #
SAMOA AMERICAINES	AS	16
ANDORRE	AD	20
ANGOLA	AO	24
ANGUILLA	AI	660
ANTARCTIQUE	AQ	10
ANTIGUA ET BARBUDA	AG	28
ARGENTINE	AR	32
ARMENIE	AM	51
ARUBA	AW	533
AUSTRALIE	AU	36
AUTRICHE	AT	40
AZERBAIDJAN	AZ	31
BAHAMAS	BS	44
BAHREIN	BH	48
BANGLADESH	BD	50
BARBADE	BB	52
BELARUS	BY	112
BELGIQUE	BE	56
BELIZE	BZ	84
BENIN	BJ	204
BERMUDES	BM	60
BHOUTAN	BT	64
BOLIVIE	BO	68
BOSNIE HERZEGOVINE	BA	70
BOTSWANA	BW	72
ILE BOUVET	BV	74
BRESIL	BR	76

Pays	Code à deux lettres	ISO #
TERRITOIRE BRITANNIQUE DE L'OCEAN INDIEN	IO	86
BRUNEI DARUSSALAM	BN	96
BULGARIE	BG	100
BURKINA FASO	BF	854
BURUNDI	BI	108
CAMBODGE	KH	116
CAMEROUN	CM	120
CANADA	CA	124
CAP VERT	CV	132
ILES CAIMAN	KY	136
REPUBLIQUE CENTRAFRICAINE	CF	140
TCHAD	TD	148
CHILI	CL	152
CHINE	CN	156
ILE DE NOEL	CX	162
ILES COCO (KEELING)	CC	166
COLOMBIE	CO	170
COMORES	KM	174
CONGO, République Démocratique du (anciennement Zaïre)	CD	180
CONGO, République du	CG	178
ILES COOK	CK	184
COSTA RICA	CR	188
COTE D'IVOIRE	CI	384
CROATIE (nom local : Hrvatska)	HR	191
CUBA	CU	192
CHYPRE	CY	196
REPUBLIQUE TCHEQUE	CZ	203

Pays	Code à deux lettres	ISO #
DANEMARK	DK	208
DJIBOUTI	DJ	262
DOMINIQUE	DM	212
REPUBLIQUE DOMINICAINE	DO	214
EQUATEUR	EC	218
EGYPTE	EG	818
SALVADOR	SV	222
GUINEE EQUATORIALE	GQ	226
ERYTHREE	ER	232
ESTONIE	EE	233
ETHIOPIE	ET	231
ILES FALKLAND (MALVINAS)	FK	238
ILES FEROE	FO	234
FIDJI	FJ	242
FINLANDE	FI	246
FRANCE	FR	250
GUINEE FRANCAISE	GF	254
POLYNESIE FRANCAISE	PF	258
TERRITOIRES FRANCAIS DU SUD	TF	260
GABON	GA	266
GAMBIE	GM	270
GEORGIE	GE	268
ALLEMAGNE	DE	276
GHANA	GH	288
GIBRALTAR	GI	292
GRECE	GR	300
GROENLAND	GL	304

Pays	Code à deux lettres	ISO #
GRENADE	GD	308
GUADELOUPE	GP	312
GUAM	GU	316
GUATEMALA	GT	320
GUINEE	GN	324
GUINEE-BISSAU	GW	624
GUYANE	GY	328
HAITI	HT	332
ILES HEARD ET MC DONALD	Gestionnaire de hiérarchies	334
HONDURAS	HN	340
HONG KONG	HK	344
HONGRIE	HU	348
ISLANDE	IS	352
INDE	IN	356
INDONESIE	ID	360
IRAN (REPUBLIQUE ISLAMIQUE D')	IR	364
IRAQ	IQ	368
IRLANDE	IE	372
ISRAEL	IL	376
ITALIE	IT	380
JAMAIQUE	JM	388
JAPON	JP	392
JORDANIE	JO	400
KAZAKHSTAN	KZ	398
KENYA	KE	404
KIRIBATI	KI	296
COREE, REPUBLIQUE POPULAIRE DEMOCRATIQUE DE	KP	408

Pays	Code à deux lettres	ISO #
COREE, REPUBLIQUE DE	KR	410
KOWEIT	KW	414
KIRGHIZISTAN	KG	417
REPUBLIQUE DEMOCRATIQUE POPULAIRE LAO	LA	418
LETTONIE	LV	428
LIBAN	LB	422
LESOTHO	LS	426
LIBERIA	LR	430
JAMAHIRIYA ARABE LIBYENNE	LY	434
LICHTENSTEIN	LI	438
LITUANIE	LT	440
LUXEMBOURG	LU	442
MACAO	MO	446
MACEDOINE, ANCIENNE REPUBLIQUE YOUGOSLAVE DE	MK	807
MADAGASCAR	MG	450
MALAWI	MW	454
MALAISIE	MY	458
MALDIVES	MV	462
MALI	ML	466
MALTE	MT	470
ILES MARSHALL	MH	584
MARTINIQUE	MQ	474
MAURITANIE	MR	478
ILE MAURICE	MU	480
MAYOTTE	YT	175
MEXIQUE	MX	484
MICRONESIE, ETATS FEDERES DE	FM	583

Pays	Code à deux lettres	ISO #
MOLDAVIE, REPUBLIQUE DE	MD	498
MONACO	MC	492
MONGOLIE	MN	496
MONTSERRAT	MS	500
MAROC	MA	504
MOZAMBIQUE	MZ	508
MYANMAR	MM	104
NAMIBIE	NA	516
NAURU	NR	520
NEPAL	NP	524
PAYS-BAS	NL	528
ANTILLES NEERLANDAISES	AN	530
NOUVELLE CALEDONIE	NC	540
NOUVELLE ZELANDE	NZ	554
NICARAGUA	NI	558
NIGER	NE	562
NIGERIA	NG	566
NIOUE	NU	570
ILE NORFOLK	NF	574
ILES MARIANNES	MP	580
NORVEGE	NO	578
OMAN	OM	512
PAKISTAN	PK	586
PALAU	PW	585
TERRITOIRE PALESTINIEN, Occupé	PS	275
PANAMA	PA	591
PAPOUASIE NOUVELLE GUINEE	PG	598

Pays	Code à deux lettres	ISO #
PARAGUAY	PY	600
PEROU	PE	604
PHILIPPINES	PH	608
PITCAIRN	PN	612
POLOGNE	PL	616
PORTUGAL	PT	620
PORTO RICO	PR	630
QATAR	QA	634
REUNION	RE	638
ROUMANIE	RO	642
FEDERATION DE RUSSIE	RU	643
RWANDA	RW	646
SAINTE HELENE	SH	654
SAINT KITTS ET NEVIS	KN	659
SAINTE LUCIE	LC	662
SAINT PIERRE ET MIQUELON	PM	666
SAINT VINCENT ET LES GRENADINES	VC	670
SAMOA	WS	882
SAN MARIN	SM	674
SAO TOME ET PRINCIPE	ST	678
ARABIE SAOUDITE	SA	682
SENEGAL	SN	686
SERBIE ET MONTENEGRO	CS	891
SEYCHELLES	SC	690
SIERRA LEONE	SL	694
SINGAPOUR	SG	702
SLOVAQUIE	SK	703

Pays	Code à deux lettres	ISO #
SLOVENIE	SI	705
ILES SALOMON	SB	90
SOMALIE	SO	706
AFRIQUE DU SUD	ZA	710
GEORGIE DU SUD ET LES ILES SANDWICH DU SUD	GS	239
ESPAGNE	ES	724
SRI LANKA	LK	144
SOUDAN	SD	736
SURINAM	SR	740
ILES SVALBARD ET JAN MAYEN	SJ	744
SWAZILAND	SZ	748
SUEDE	SE	752
SUISSE	CH	756
REPUBLIQUE ARABE DE SYRIE	SY	760
TAIWAN	TW	158
TADJIKISTAN	TJ	762
TANZANIE, REPUBLIQUE UNIE DE	TZ	834
THAILANDE	TH	764
TIMOR ORIENTAL	TL	626
TOGO	TG	768
TOKELAU	TK	772
TONGA	TO	776
TRINITE ET TOBAGO	TT	780
TUNISIE	TN	788
TURQUIE	TR	792
TURKMENISTAN	TM	795
ILES TURKS ET CAICOS	TC	796

Pays	Code à deux lettres	ISO #
TUVALU	TV	798
OUGANDA	UG	800
UKRAINE	UA	804
EMIRATS ARABES UNIS	AE	784
ROYAUME-UNI	GB	826
ETATS-UNIS	US	840
ILES MINEURES ELOIGNEES DES ETATS-UNIS	UM	581
URUGUAY	UY	858
OUZBEKISTAN	UZ	860
VANUATU	VU	548
SAINT-SIEGE DU VATICAN	VA	336
VENEZUELA	VE	862
VIETNAM	VN	704
ILES VIERGES (BRITANNIQUES)	VG	92
ILES VIERGES (AMERICAINES)	VI	850
ILES WALLIS ET FUTUNA	WF	876
SAHARA OCCIDENTAL	EH	732
YEMEN	YE	887
ZAMBIE	ZM	894
ZIMBABWE	ZW	716

ANNEXE I

Dépannage

Cette annexe comprend les rubriques suivantes :

- Présentation du dépannage, 186
- Contrôle de la configuration de votre GAS, 186
- Contrôle de la configuration de votre fonction de nettoyage, 187
- Les métadonnées d'Informatica Data Director n'ont pas été mises à jour, 187
- Informatica Data Director s'interrompt lorsque vous basculez d'une entité à une autre, 187
- La configuration d'Informatica Data Director n'est pas valide, 188
- Lenteur des performances de correspondance, 188

Présentation du dépannage

Cette annexe décrit certains conseils sur les éléments à vérifier lorsque l'on trouve des résultats inattendus dans la configuration de l'application IDD.

Contrôle de la configuration de votre GAS

Vérifiez que le GAS a les autorisations appropriées affectées à tous les niveaux requis conformément à la documentation.

Les zones à contrôler pour CRUD incluent :

- Si des références croisées et des historiques de modifications sont requis, les boutons étant activés dans l'application IDD, le contenu des métadonnées approprié (objets XREF et HIST) correspond à des ressources SECURE et est configuré de manière appropriée.
- Requêtes/Packages - Garantissent que les ressources sont SECURE. Dans le cas contraire, une application IDD pourrait refuser l'accès à tout le domaine.

Contrôle de la configuration de votre fonction de nettoyage

Si des fonctions de nettoyage sont configurées, vérifiez que :

- Chaque fonction de nettoyage est une ressource SECURE.
- Tous les rôles exigeant un accès à la fonction de nettoyage ont une autorisation d'exécution.

Les métadonnées d'Informatica Data Director n'ont pas été mises à jour

Informatica Data Director conserve un cache de métadonnées de MDM Hub qui décrit les objets de base, les colonnes, les relations et d'autres détails. Pour effacer le cache de l'application IDD sélectionnée et forcer IDD à recharger les métadonnées, cliquez sur **Effacer le cache** dans le gestionnaire de configuration IDD.

Vous pouvez également redémarrer le serveur d'applications pour effacer le cache.

Informatica Data Director s'interrompt lorsque vous basculez d'une entité à une autre

Informatica Data Director s'interrompt lorsque vous basculez d'une entité à une autre pour les relations du gestionnaire de hiérarchies des systèmes sources pour lesquels l'écrasement de la gestion d'état n'est pas activé.

Ce problème se produit dans les environnements JBoss exécutés sous Java 1.7. Pour le résoudre, vous devez configurer le fichier `standalone-full.xml`.

1. Ouvrez le fichier `standalone-full.xml` pour effectuer la modification. Le fichier se trouve dans le répertoire suivant :
   - Sous UNIX. `<répertoire d'installation JBoss>/jboss-eap-6.1/standalone/configuration`
   - Sous Windows. `<répertoire d'installation JBoss>\jboss-eap-6.1\standalone\configuration`
2. Ajoutez le code XML suivant au fichier `standalone-full.xml` pour configurer le traitement asynchrone de la journalisation :

```
<async-handler name="ASYNC">
   <level name="INFO"/>
   <queue-length value="1024"/>
   <overflow-action value="BLOCK"/>
      <subhandlers>
         <handler name="FILE"/>
         <handler name="CONSOLE"/>
      </subhandlers>
</async-handler>
```

3. Sous <subsystem xmlns="urn:jboss:domain:logging:1.2"> dans le fichier `standalone-full.xml`, ajoutez le code XML suivant pour configurer le traitement asynchrone de la journalisation racine :

```
<root-logger>
   <level name="INFO"/>
   <handlers>
      <handler name="ASYNC"/>
   </handlers>
</root-logger>
```

4. Redémarrez le serveur d'application.

La configuration d'Informatica Data Director n'est pas valide

Si vous recevez un message d'erreur indiquant que la configuration d'Informatica Data Director n'est pas valide, validez le fichier `IDDConfig.xml` en fonction du schéma `siperian-bdd-config-6.xsd`.

Le schéma `siperian-bdd-config-6.xsd` se trouve dans le kit de ressources dans le répertoire suivant :

- Sous UNIX : `<répertoire d'installation infamdm>/hub/resourcekit/sdk/bddXsdDoc`
- Sous Windows : `<répertoire d'installation infamdm>\hub\resourcekit\sdk\bddXsdDoc`

Lenteur des performances de correspondance

Les utilisateurs de l'application IDD signalent que les performances de correspondance sont très lentes.

Activez la propriété `needLoadChildOnOpen` et redémarrez le serveur d'application.

Pour activer la propriété, exécutez les instructions SQL suivantes sur la base de données ORS :

```
insert into C_REPOS_DS_PREF_DETAIL (ROWID_DS_PREF_DETAIL, ROWID_DS_PREF, NAME, VALUE) select
'BDDGP.30', rowid_ds_pref, 'needLoadChildOnOpen', 'true' from C_REPOS_DS_PREF where name =
'___SYSTEM_PREFERENCES_ROOT___';

commit;
```

ANNEXE J

Glossaire

administrateur

Utilisateur de l'application IDD qui a la responsabilité principale de la configuration de l'application IDD.

annuler la fusion

Processus d'annulation de la fusion des enregistrements fusionnés auparavant. Pour les objets de base de style fusion uniquement.

Application IDD

Unité principale de configuration et de déploiement pour l'implémentation d'IDD. Une application IDD est ce que les utilisateurs professionnels observent quand ils lancent IDD et s'y connectent.

Approbation

L'approbation est un mécanisme de mesure du facteur de confiance associé à chaque cellule selon son système source, l'historique des modifications et d'autres règles d'entreprise. L'approbation prend en compte l'âge des données, la diminution de leur fiabilité dans le temps et la validité des données.

authentification

Processus de vérification d'identité d'un utilisateur pour s'assurer qu'il est celui qu'il prétend être. Dans une application IDD, les utilisateurs sont authentifiés par leurs justificatifs d'identité fournis—nom d'utilisateur / mot de passe, charge de sécurité ou une combinaison des deux. L'application IDD fournit un mécanisme d'authentification interne et prend également en charge l'authentification de l'utilisateur à l'aide de fournisseurs d'authentification tiers.

base de données

Ensemble de données organisées dans le Stockage Hub. Informatica MDM Hub prend en charge deux types de bases de données : une base de données principale et un stockage de référence opérationnelle (Operational Reference Store - ORS).

Base de données principale

Base de données qui contient les paramètres de configuration de l'environnement Informatica MDM Hub—comptes utilisateur, configuration de sécurité, registre ORS, paramètres de file d'attente des messages, etc. Une seule base de données principale peut être affectée à un environnement Informatica MDM Hub donné. Le nom par défaut de la base de données principale est CMX_SYSTEM.

Chemin de correspondance

Vous permet de parcourir la hiérarchie entre les enregistrements—que cette hiérarchie existe entre les objets de base (chemins inter-table) ou au sein d'un objet de base unique (chemins intra-table). Les chemins de

correspondance sont utilisés pour configurer des règles de colonne de correspondance impliquant les enregistrements correspondants soit dans des tables séparées, soit dans la même table.

clé de correspondance

Chaînes encodées qui représentent les données dans la colonne de clés de correspondances approximatives de l'objet de base. Les clés de correspondance sont constituées de valeurs de longueur fixe, compressées et codées, construites à partir d'une combinaison des mots et des chiffres d'un nom ou d'une adresse, de sorte que les variations correspondantes aient la même valeur de clé de correspondance. Les clés de correspondance sont une partie des jetons de correspondance générés durant le processus de marquage, stockés dans la table de clés de correspondance, puis utilisés durant le processus de correspondance pour identifier les candidats à la correspondance.

clé de correspondance approximative

Colonne spéciale dans l'objet de base que le gestionnaire de schéma ajoute si une colonne de correspondance utilise la stratégie de correspondance/recherche approximative. Cette colonne est le champ principal utilisé au cours de la recherche et de la correspondance pour générer des candidats de correspondance pour cet objet de base. Tous les objets de base approximatifs ont une et une seule clé de correspondance approximative.

clé étrangère

Dans une base de données relationnelle, une colonne (ou un ensemble de colonnes) dont la valeur correspond à une valeur de clé primaire dans une autre table (ou, dans de rares cas, dans la même table). La clé étrangère agit comme un pointeur vers l'autre table. Par exemple, la colonne Department_Number dans la table Employé serait une clé étrangère pointant vers la clé primaire de la table Département.

colonne de correspondance

Colonne utilisée dans une règle de correspondance à des fins de comparaison. Chaque colonne de correspondance est basée sur une ou plusieurs colonnes de l'objet de base.

Console Hub

Interface utilisateur d'Informatica MDM Hub qui comprend un ensemble d'outils pour les administrateurs et les gestionnaires des données. Chaque outil permet d'effectuer une action spécifique, ou un ensemble d'actions associées, telles que la génération du modèle de données, l'exécution de tâches de lots, la configuration du flux de données, la configuration de l'accès des applications externes aux ressources d'Informatica MDM Hub, et autres tâches de fonctionnement et de configuration système.

correspondance

Processus visant à déterminer si deux enregistrements doivent être fusionnés automatiquement ou s'ils doivent être candidats à la fusion manuelle parce qu'ils possèdent des valeurs identiques ou similaires dans les colonnes spécifiées.

correspondance approximative

Stratégie de correspondance/recherche utilisant la correspondance probabiliste, qui prend en compte les variations d'orthographe, les fautes d'orthographe possibles et d'autres différences qui peuvent différencier les enregistrements correspondants.

déduplication

Technique pour éliminer les données redondantes.

Domaine

Concept central d'organisation pour une application IDD. Un domaine représente un ensemble de données qui doit être traité comme une unité d'un point de vue commercial.

Données de traitement

Les données de traitement sont des données d'entreprise qui peuvent passer par des états différents (ACTIVE, PENDING ou DELETED) en progressant dans un flux de travail.

Données principales

Un ensemble d’entités communes, centrales—avec leurs attributs et leurs valeurs—qui sont considérées comme essentielles pour l'activité d’une entreprise et qui sont requises pour l’utilisation dans au moins deux systèmes ou processus métier. Des exemples de données principales incluent les données client, produit, employé, fournisseur et emplacement.

doublon

Un ou plusieurs enregistrements dans lesquels les données de certaines colonnes (telles que le nom, l'adresse ou les données d'entreprise) sont identiques ou quasiment identiques. Les règles de correspondance exécutées pendant le processus de correspondance déterminent si deux enregistrements sont suffisamment semblables pour être considérés comme des doublons à des fins de consolidation.

ensemble de règles de correspondance

Un ensemble logique de règles de correspondance qui permettent aux utilisateurs d’exécuter différents ensembles de règles à différents stades dans le processus de correspondance. Les ensembles de règles de correspondance comprennent un niveau de recherche qui dicte la stratégie de recherche, un certain nombre de règles de correspondance automatiques et manuelles, et en option, un filtre qui vous permet d’inclure ou d’exclure de manière sélective les enregistrements pendant les processus de correspondance. Les ensembles de règles de correspondance sont utilisés pour s’exécuter en correspondance aux règles de colonne, mais pas aux règles de correspondance de clé primaire.

entité

Une entité est un objet, une personne, un lieu, ou une chose qui a un sens et pouvant être utilisé dans votre base de données.

Entité métier

Structure imbriquée d'objets de base. Utilisez le framework Entité 360 dans Informatica Data Director pour afficher toutes les informations associées à l'objet de base racine d'une entité métier. Effectuez une recherche intelligente dans Informatica Data Director pour rechercher des données dans une entité métier.

état du système

Décrit comment les enregistrements d'objet de base sont pris en charge par Informatica MDM Hub. Les états suivants sont pris en charge : ACTIVE, PENDING et DELETED.

Fichiers auxiliaires

Les fichiers auxiliaires sont des fichiers temporaires créés dans diverses circonstances, lors de la modification ou de l'exportation d'un projet.

Filtre de sécurité

Le filtre de sécurité spécifie une condition qu'IDD applique pour restreindre et sécuriser les données de domaine auxquelles les utilisateurs individuels peuvent accéder. Des filtres peuvent être définis sur une colonne d'objet principal, une colonne enfant et une colonne petit-enfant. Vous pouvez configurer n'importe quelle quantité de filtres pour un domaine.

Flux de travail

Dans Informatica MDM Multidomain Edition, un flux de travail représente un processus d'entreprise au sein d'une organisation. Consultez la section *processus d'entreprise* à la page 195.

fonction de nettoyage

IDD vous permet d'utiliser des fonctions de nettoyage déjà définies dans MDM pour nettoyer, standardiser et valider les données d'entrée. Vous pouvez utiliser cette fonction pour la standardisation et la validation de l'adresse, ainsi que pour l'accroissement des données issues d'autres sources.

Fournisseur de connexion externe

Plug-in utilisé avec IDD pour authentifier les utilisateurs en fonction des fournisseurs d'identité externes.

Fournisseur de connexion personnalisé

Module enfichable qui authentifie les utilisateurs lors du démarrage de l'application IDD.

Framework d'intégration des services (SIF)

Partie d'Informatica MDM Hub s'interfaçant avec des programmes clients. Logiquement, il sert de niveau intermédiaire dans le modèle client/serveur. Il vous permet d’implémenter les interactions requête/réponse à l’aide de l’une des variations architecturales suivantes :

- Services Web à couplage lâche utilisant le protocole SOAP.
- Appels de procédure distante Java à couplage fort basés sur EJB (Enterprise JavaBeans) ou XML.
- Messages basés sur JMS (Java Message Service) asynchrone.
- Documents XML allant et venant via HTTP.

gestion des processus d'entreprise (BPM)

La gestion des processus d'entreprise se concentre sur l'adaptation des processus d'une organisation. Informatica MDM est doté d'un moteur de gestion des processus d'entreprise intégré, qui vous permet d'automatiser les processus de vérification et d'approbation des données principales.

gestion d’état

Le processus de gestion d'état du système d'objets de base et d'enregistrements de références croisées pour attribuer la logique de traitement à travers le flux de données. Vous pouvez affecter un état du système à des objets de base et des enregistrements de références croisées à différentes étapes du flux de données à l’aide des outils du Hub fonctionnant avec les enregistrements. De plus, vous pouvez utiliser les différents outils du Hub pour gérer votre schéma pour activer la gestion d’état pour un objet de base, ou définir des autorisations utilisateur pour contrôler qui peut modifier l’état d’un enregistrement.

La gestion d’état est limitée aux états suivants : ACTIVE, PENDING et DELETED.

Gestionnaire de configuration IDD

Utilitaire Web utilisé pour ajouter, modifier et gérer des applications IDD.

Gestionnaire de hiérarchies

Le Gestionnaire de hiérarchies permet aux utilisateurs de gérer les données de hiérarchie associées aux enregistrements gérés dans le MDM Hub. Pour plus d'informations, consultez le *Guide de configuration d'Informatica MDM Multidomain Edition* et le *Guide du gestionnaire des données d'Informatica MDM Multidomain Edition*.

Gestionnaire de schéma

Le gestionnaire de schéma est un composant utilisé au moment de la conception dans la console Hub pour définir le schéma, ainsi que les tables temporaires et les tables d'arrivée. Il permet également de définir des règles de correspondance et de fusion, de validation et de files d'attente de messages.

gestionnaire des données

Utilisateur de l'application IDD qui a la responsabilité principale pour la qualité des données.

Gestionnaire d'accès de sécurité (GAS)

Le gestionnaire d'accès de sécurité (GAS) est l'infrastructure de sécurité complète d'Informatica MDM Hub pour la protection des ressources Informatica MDM Hub contre l'accès non autorisé. Pendant l'exécution, le GAS met en application les décisions de stratégie de sécurité de votre entreprise pour votre implémentation d'Informatica MDM Hub, en gérant l'authentification et les autorisations d'accès des utilisateurs conformément à votre configuration de la sécurité.

Gouvernance des données

La gouvernance des données représente la pratique de la gestion des données en tant qu'actif dans l'entreprise. Elle implique les processus, les stratégies, les normes, les technologies et les personnes dans l'entreprise pour assurer la disponibilité de données exactes, cohérentes et opportunes pour une meilleure prise de décision et des processus métier améliorés.

Groupe de domaines

Un ensemble d'une ou plusieurs domaines qui ont le même objet de base à leur racine (aussi appelé objet principal).

groupe de ressources

Ensemble de ressources sécurisées qui simplifie l'affectation de privilèges, vous permettant d'affecter des privilèges à plusieurs ressources à la fois, et d'affecter facilement des groupes de ressources à un rôle.

groupe d'utilisateurs

Ensemble logique de comptes d'utilisateurs.

hiérarchie

Dans le gestionnaire de hiérarchies, un ensemble de types de relations. Ces types de relations ne sont ni classés suivant la place des entités dans la hiérarchie, ni forcément associés entre eux. Ce sont simplement des types de relations regroupés pour faciliter la classification et l'identification.

Kit de ressources

Le kit de ressources Informatica MDM Hub est un ensemble d'utilitaires, d'exemples et de bibliothèques qui fournissent des exemples des fonctionnalités d'Informatica MDM Hub pouvant être étendues et implémentées.

lignage

Quels systèmes et quels enregistrements de ces systèmes ont contribué aux enregistrements consolidés dans le Stockage Hub.

mappage

Définit un ensemble de transformations qui sont appliquées aux données source. Les mappages sont utilisés pendant le processus d'activation de données (ou en utilisant la requête API SiperianClient CleansePut) pour transférer des données depuis une table d'arrivée vers une table temporaire. Un mappage identifie la colonne source dans la table d'arrivée et la colonne cible à renseigner dans la table temporaire, ainsi que toute fonction de nettoyage intermédiaire utilisée pour nettoyer les données.

Masquage des données

Mécanisme de masquage des informations selon les rôles de sécurité.

meilleure version de la vérité (MVV)

Un enregistrement qui a été consolidé avec les meilleures cellules de données des enregistrements source. Parfois abrégé en MVV.

métadonnées

Données utilisées pour décrire d'autres données. Dans Informatica MDM Hub, les métadonnées sont utilisées pour décrire le schéma (modèle de données) utilisé dans votre implémentation Informatica MDM Hub, avec les paramètres de configuration connexes.

métadonnées de contenu

Données qui décrivent les données métier qui ont été traitées par Informatica MDM Hub. Les métadonnées de contenu sont stockées dans des tables de support pour un objet de base, incluant des tables de références croisées, des tables d'historique et autres. Les métadonnées de contenu sont utilisées pour aider à déterminer d'où proviennent les données de l'objet de base et la manière dont elles ont été modifiées au fil du temps.

Modèle de données

Le modèle de données est un modèle abrégé qui décrit la manière dont les données sont structurées et organisées.

nettoyage des données

Processus de standardisation du contenu et de la mise en page des données, de décomposition et d'analyse des valeurs texte en éléments identifiables, de vérification des valeurs identifiables (type codes postaux) par rapport aux bibliothèques de données, et de remplacement des valeurs incorrectes par des valeurs correctes issues des bibliothèques de données.

objet de base

Table contenant les informations sur une entité concernant votre entreprise, comme un client ou un compte.

objet de base de relation

Un objet de base de relation est un objet de base utilisé pour stocker les informations concernant les relations du gestionnaire de hiérarchies.

objet de conception

Parties des métadonnées utilisées pour définir le schéma et d'autres paramètres de configuration pour une implémentation. Les objets de conception incluent des instances des types d'objets Informatica MDM Hub suivants : objets et colonnes de base, tables d'arrivée et de staging, colonnes, index, relations, mappages, fonctions de nettoyage, requêtes et packages, paramètres d'approbation, règles de validation et de correspondance, définitions du gestionnaire d'accès de sécurité, définitions du gestionnaire de hiérarchie et autres paramètres.

objet hub

Terme générique pour divers types d'objets définis dans le Hub qui contiennent des informations sur vos entités métier. Voici quelques exemples : objets de base, tables de références croisées et n'importe quel objet dans le hub que vous pouvez associer à des métrologies de rapport.

parentReference

Un élément parentReference peut être défini dans le XML pour la colonne qui est la clé étrangère vers l'enregistrement enfant. Ceci définit un libellé à afficher dans l'enregistrement petit-enfant qui contient des données issues de l'enfant, pour aider les utilisateurs à comprendre la relation entre les petits-enfants et l'enfant

procédure stockée

Ensemble nommé d'instructions SQL (Structured Query Language) qui sont compilées et stockées sur le serveur de base de données. Les tâches de lot d'Informatica MDM Hub sont encodées dans des procédures stockées pour qu'elles puissent être exécutées à l'aide de scripts d'exécution de tâche dans un logiciel de planification de tâche (tel que Tivoli ou CA Unicenter).

processus

Consultez la section *processus d'entreprise* à la page 195.

processus d'entreprise

Un processus d'entreprise est un flux de travail qui permet d'atteindre un objectif organisationnel et de mettre en œuvre une fonction d'entreprise. Un processus d'entreprise contient les activités requises pour atteindre l'objectif et définit des chemins d'exécution via les activités. Informatica MDM Multidomain Edition dispose de processus d'entreprise ActiveVOS prédéfinis qui sont gérés par le serveur Informatica ActiveVOS. L'objectif organisationnel de ces processus est de s'assurer que le personnel autorisé, tel que les gestionnaires d'entreprise ou les gestionnaires de données, vérifie toutes les mises à jour des données principales.

processus de validation

Processus de vérification de l'exhaustivité et de l'intégrité des métadonnées qui décrivent un référentiel. Le processus de validation compare le modèle logique d'un référentiel à son schéma physique. En cas de problème, Gestionnaire de référentiels génère une liste de problèmes nécessitant une attention particulière.

Référence de fratrie

Une référence de fratrie est une relation d'un enregistrement dans un domaine vers un enregistrement enfant dans ce domaine. Par exemple, un client pourrait inclure les enregistrements enfants d'adresse et de numéro de téléphone, le numéro de téléphone ayant une clé étrangère pour l'associer à une adresse spécifique.

règle de correspondance

Définit les critères selon lesquels Informatica MDM Hub détermine si les enregistrements peuvent être des doublons. Les colonnes de correspondance sont combinées en règles de correspondance pour déterminer les conditions dans lesquelles deux enregistrements sont considérés comme étant suffisamment similaires pour fusionner. Chaque règle de correspondance indique à Informatica MDM Hub la combinaison des colonnes de correspondance dont il a besoin pour examiner les points de similitude.

Relations de domaines

Les relations de domaine définissent la façon dont les domaines sont associés entre eux. Un domaine peut avoir des domaines enfants et petits-enfants et des références de fratrie.

schéma

Modèle de données utilisé dans une implémentation Informatica MDM Hub d'un client. Informatica MDM Hub n’impose ou ne requiert aucun schéma particulier. Le schéma est indépendant des systèmes source.

Sécurité des données

La sécurité des données interdit la consultation de certains enregistrements par les utilisateurs en fonction du contenu de ces enregistrements.

Serveur de correspondance de nettoyage

Le composant d'exécution du serveur de correspondance de nettoyage est un servlet qui gère les requêtes de nettoyage. Ce servlet est déployé dans un environnement de serveur d’applications. Le servlet contient deux composants de serveur :

- un serveur de nettoyage prenant en charge les opérations de nettoyage des données
- un serveur de correspondance prenant en charge les opérations de correspondance

Le serveur de correspondance de nettoyage est multi-thread, afin que chaque instance puisse traiter plusieurs requêtes simultanément. Il peut être déployé sur divers serveurs d’applications.

Le serveur de correspondance de nettoyage s'interface avec tous les moteurs de nettoyage pris en charge, comme le moteur de nettoyage Trillium Director. Le serveur de correspondance de nettoyage et le moteur de nettoyage s'attachent à standardiser les données. Cette standardisation fonctionne en étroite collaboration avec le moteur de consolidation Informatica (anciennement dénommé moteur de fusion) pour optimiser les données pour la consolidation.

Serveur Hub

Composant d’exécution dans la couche médiane (serveur d’applications) utilisé pour des services essentiels et communs, notamment l’accès, la sécurité et la gestion de session.

service d'entité métier

Un service d'entité métier est un ensemble d'opérations qui exécutent le code MDM Hub pour créer, mettre à jour, supprimer et rechercher des enregistrements d'objets de base dans une entité métier.

sortie utilisateur

Les sorties utilisateur permettent d'ajouter une logique métier personnalisée aux opérations IDD standard.

source de données

Dans l'environnement du serveur d'applications, une source de données est une ressource JDBC qui identifie des informations sur une base de données, telles que l'emplacement du serveur de base de données, le nom de la base de données, l'identifiant utilisateur et le mot de passe de la base de données, etc. Informatica MDM Hub a besoin de ces informations pour communiquer avec un ORS.

Stockage de référence opérationnelle (Operational Reference Store - ORS)

Schéma de base de données contenant les règles de traitement des données principales, les règles de gestion de l'ensemble des objets de données principales, ainsi que les règles de traitement et la logique auxiliaire utilisées par Informatica MDM Hub pour définir la meilleure version de la vérité (MVV).

Stockage Hub

Dans une implémentation d'Informatica MDM Hub, base de données contenant la base de données principale et une ou plusieurs bases de données de stockage de référence opérationnelle (Operational Reference Store - ORS).

table de correspondance

Type de table système, associé à un objet de base, qui prend en charge le processus de correspondance. Au cours de l'exécution d'une tâche de correspondance pour un objet de base, Informatica MDM Hub remplit sa table de correspondance associée avec les valeurs ROWID_OBJECT pour chaque paire d'enregistrements correspondants, ainsi que l'identifiant pour la règle de correspondance qui a entraîné la correspondance et un indicateur de fusion automatique.

table d'historique

Type de table dans un ORS qui contient des informations d'historique sur les modifications d'une table associée. Les tables d'historique fournissent des options détaillées de suivi des modifications, notamment l'historique de fusion et d'annulation de fusion, l'historique des données prénettoyées, l'historique de l'objet de base et l'historique des références croisées.

type de correspondance

Chaque colonne de correspondance possède un type de correspondance qui détermine son attribution de jeton en préparation de la comparaison de correspondance.

type de données

Définit les caractéristiques des valeurs autorisées dans une colonne de table—caractères, nombres, dates, données binaires, etc.

valeur Null

Absence de valeur dans une colonne d'un enregistrement. Null est différent de vide ou de zéro.

INDEX

A

ActiveVOS
  migration depuis Siperian BPM 150
Affectation automatique des tâches 164
Affectation manuelle des tâches 165
Afficher les champs secondaires d'un objet de base dans l'onglet enfant 67
aide
  fichier d'aide personnalisée, création 98
  fichier d'aide personnalisée, importation 98
aide en ligne
  fichier d'aide personnalisée, création 98
  fichier d'aide personnalisée, importation 98
Ajout d'une application IDD 43
approbation
  à propos de 24
Attributs d'onglet enfant personnalisé 80
Attributs et balises ActionType 161
Attributs et balises TaskType 156
Authentification de la connexion unique
  configuration de l'authentification de la connexion unique Google 61
Authentification de la connexion unique Google
  configuration 61
Authentification des utilisateurs (identification unique SSO) 21
authentification unique
  paramètres du fournisseur de connexion 52

C

Chemins de correspondance 22
Chronologie 27
Codes de langue 171
Codes pays 176
Colonne de recherche 65
concepts d'Informatica Data Director
  Domaines 17
Concepts IDD
  Application IDD 16
  Fichiers de configuration IDD 16
  Gestionnaire de configuration IDD 16
  Groupes de domaines 18
Configuration de l'affectation des tâches 163
Configuration de l'authentification par identification unique SalesForce (WebLogic) 58
Configuration de l'authentification par identification unique SalesForce (WebSphere) 58
Configuration de la recherche
  Configurer la recherche de base 36
  Configurer la recherche étendue 36
  Configurer les requêtes publiques 37
Configuration de la sécurité 38, 120
configuration de la sécurité des données
  exemple avec un objet parent 129
  exemple avec un objet petit-enfant 129
Configuration de la sécurité des tâches 162
Configuration des domaines 33
Configuration des extensions de l'interface utilisateur 39
Configuration des groupes de domaines 33
Configuration des recherches de correspondances et de doublons dans IDD 37
Configuration du flux de travail 38
Configuration du gestionnaire de hiérarchies HM (Hierarchy Manager) 72
configuration du navigateur
  configuration requise 118
Configuration du nettoyage et de la validation 35
Configurer le style d'édition de la case à cocher 71
Configurer les rapports 39
connexions à la base de données
  magasin de données 102
Création de l'application IDD 32
Création de référence frère 69

D

délai d'expiration de session 48
Démarrez la mise en page de l'espace de travail
  à propos de 79
Déploiement 46
Description des composants de configuration des tâches et des flux de travail 153
Diagramme des composants de configuration des tâches et des flux de travail 153
Dimensionnement du client et du réseau 117
Dimensionnement du serveur d'applications 117
Dimensionnement du serveur de base de données 117

E

Effacer le cache
  à propos de 21
Extensions de l'interface utilisateur 76

F

Fichier XML de configuration IDD 63
Flux de travail et tâches 24
Fonctions de nettoyage
  Fonctions de nettoyage renvoyant NULL 24
  Nettoyage et standardisation 23
  Validation 23
Framework d'intégration des services 20

G

GAS et sécurité
  Masquage des données 26
  Sécurité des données 26
  Sécurité des objets et des colonnes 25
génération de rapport
  présentation 100
Gestionnaire de hiérarchies 25
guide de l'utilisateur
  fichier d'aide révisé, importation 96–98

H

Historique 26

I

Importation d'une configuration d'application IDD 44
importation de données
  importation du modèle 52
Informatica Data Director 14

L

Liaison ORS 43
Liens de domaines 70
liens externes
  paramètres 81
Liens externes (Composants de l'espace de travail de démarrage personnalisé) 78
Localisation de l'application 40
Localisation de la recherche 51

M

magasin de données
  configuration des connexions à la base de données 102
  configuration des paramètres de rapport 103
  remplissage 104
Masquage des données 147
mesures
  à propos de 101
  mesures de composition des références croisées 101
  mesures de gestion des tâches 167
  mesures de système source 101
  tendances de croissance du domaine 102
mesures de composition des références croisées
  à propos de 101
mesures de gestion des tâches
  à propos de 167
mesures de système source
  à propos de 101
mini-Data Warehouse
  à propos de 103
Mise à jour des propriétés globales 114
modèles de rapport
  à propos de 100
module Fournisseur de connexion personnalisé
  authentification unique 52
Module Fournisseur de connexion personnalisé
  chargement 53
moteurs de flux de travail
  ajout 151

N

Notification des tâches 166

O

Objets de base 21
onglets
  onglets personnalisés 77
onglets de niveau supérieur
  onglets 77
Onglets enfants personnalisés (domaine) 80
outil BPM
  configurer 38
Outils XML 63

P

page d'erreur personnalisée
  configuration 95
Page d'Accueil 42
paramètres
  pour les liens externes 81
paramètres de rapport
  magasin de données 103
Paramètres du fournisseur de connexion
  bibliothèques tierces 54
  Création de la bibliothèque de fournisseurs de connexion 58
  Implémentation du fournisseur de connexion personnalisé 54
paramètres dynamiques
  pour les liens externes 81
paramètres statiques
  pour les liens externes 81
Personnalisation de l'attribution automatique des tâches 165
Personnalisation des libellés de colonnes 71
Petits-enfants 70
Prérequis 15
présentation 14
Présentation de la configuration manuelle d'IDD 62
Présentation de processus d'implémentation 31
Présentation du gestionnaire de configuration IDD 41
processus de configuration
  à propos de 32
Propriétés des liens externes 81

R

rapports
  mesures 101
Recherche
  De base - Recherche basée sur SQL 22
  Recherche avancée 23
  Recherche étendue - basée sur les correspondances 22
Recherche non sensible à la casse 37
Recherches dépendantes 27
Référence sur les composants de l'application 119
Référence sur les propriétés globales d'IDD 107
Règles de chronologie 28
Regroupement logique de menus 71
Relations à l'intérieur des domaines
  Références de fratries 20
  Relations enfant un à plusieurs 18
  Relations enfants plusieurs à plusieurs 19
  Relations petits-enfants plusieurs à plusieurs 19
  Relations petits-enfants un à plusieurs 19

reportParam
  paramètres de rapport 105

S

sécurité des données
  utilisation de filtres 127
Sécurité des données 127
serveurs Web
  utilisation 21
Signets 28
Siperian BPM
  migration vers ActiveVOS 150
  note d'obsolescence 149

T

Tables de recherche 26
Tables de recherche avec colonne de sous-type 66
tendances de croissance du domaine
  à propos de 102
Types d'actions 160
Types d'actions - Échantillon XML 160
Types de tâches 154
Types de tâches - Échantillon XML 155

V

Valeurs de recherche statiques 67
Validation 45
vue de données
  développer un domaine enfant par défaut 69
Vue de hiérarchie 29
Vue des données 29