IBM Cúram Social Program Management
Version 6.0.5

Guide de configuration du système Cúram

Note
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations de la section «Remarques», à la page 27

Dernière révision : Mars 2014

Cette édition s'applique à IBM Cúram Social Program Management version 6.0.5 et à toutes les versions ultérieures, sauf indication contraire dans les nouvelles éditions.

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

Table des matières

Figures

Tableaux

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Guide de configuration du système Cúram

Un large éventail de fonctions dans l'application Cúram peuvent être configurées administrativement. Les éléments suivants peuvent être configurés : propriétés d'application, requêtes de sélection d'audit de dossier, modèles de communication, traitements par lots, paramètres de sécurité, rapports de veille commerciale, systèmes cible, services d'interopérabilité de gestion de contenu.

Introduction

Objet

L'objectif de ce guide est de donner un aperçu des options de configuration permettant aux administrateurs système de gérer les différentes composantes de l'application. Afin de bien comprendre les services d'administration de l'application, il est recommandé de lire également le `Guide d'administration des localisations Cúram` et le `Guide d'administration des organisations Cúram`.

L'administration système inclut une fonctionnalité permettant de gérer un large éventail d'éléments ayant une incidence sur le fonctionnement de l'application. L'administration système requiert une certaine aisance avec les termes techniques, étant donné que certains composants de l'administration système ne peuvent être créés que lors du développement de l'application. Exemple : l'exécution des traitements par lots se fait à partir du module d'administration système. Cependant, les traitements par lots eux-mêmes ne peuvent être conçus et implémentés que dans le cadre de son développement.

D'autres composants peuvent être gérés dans l'interface d'administration système, mais doivent être référencés dans l'application dans le cadre du développement de l'application, notamment les tables de codes et les tables de taux.

Afin de mieux comprendre ces concepts, il est recommandé de lire ce guide dans son intégralité.

Public concerné

Ce guide est destiné aux analystes métier et aux administrateurs système de l'organisation. Ces derniers doivent donc avoir une solide connaissance des exigences métier de l'organisation. La lecture de ce document exige une solide connaissance de l'application. Dans sa globalité, ce document ne nécessite pas de grandes connaissances techniques. Néanmoins, plusieurs aspects de l'administration système font référence à l'application, et certains termes seraient plus faciles à comprendre pour un lecteur disposant de meilleures connaissances techniques.

Conditions préalables

Le lecteur doit être familier avec les concepts de base de la Gestion Sociale d'Entreprise (SEM - Social Enterprise Management), et notamment avec les tâches administratives nécessaires pour gérer une entreprise de l'économie sociale, comme la gestion des utilisateurs système, la sécurité utilisateur et la hiérarchie de reporting de l'organisation.

Chapitres contenus dans ce guide

Voici une liste des différents chapitres de ce guide :

Configuration de l'application
Ce chapitre détaille plusieurs options de configuration, dont la configuration des propriétés de l'application, des tables de codes, des langues régionales et des pseudonymes des participants.

Configuration des requêtes de sélection des audits de dossier
Ce chapitre couvre la configuration des requêtes de sélection des audits de dossier.

Configuration des modèles de communication
Ce chapitre donne un aperçu des différentes options permettant de configurer les modèles de communication.

Configuration de la sécurité
Ce chapitre donne un aperçu des différentes options permettant de configurer l'administration de la sécurité.

Configuration des traitements par lots
Ce chapitre donne un aperçu des différentes options permettant de configurer les traitements par lots.

Configuration des rapports de Business Intelligence et du visualiseur
Ce chapitre donne un aperçu des différentes options permettant de configurer au niveau système le visualiseur de rapports de Business Intelligence.

Configuration d'un système cible
Ce chapitre donne un aperçu des options de base de l'interface d'administration système permettant de configurer des systèmes cibles.

Configuration de l'application

Introduction

Ce chapitre détaille les différentes options de configuration dédiées au fonctionnement de l'application d'exécution, et notamment à la configuration des propriétés, des tables de codes, des langues régionales et des pseudonymes des participants.

Les propriétés de l'application permettent de configurer certaines composantes de l'application d'exécution. Elles offrent la possibilité aux administrateurs système de personnaliser l'application afin de répondre aux besoins de l'organisation, sans avoir à élaborer et redéployer l'application.

Les tables de codes contiennent des codes pour les éléments qui apparaissent dans les zones déroulantes. Elles permettent de gagner de l'espace dans la base de données de l'application. En stockant les sélections de la zone déroulante sous forme de codes plutôt que le texte complet de la sélection, il est possible d'économiser une grande quantité d'espace dans la base de données. Exemple : plutôt que de stocker l'ethnicité "Amérindien ou natif d'Alaska" dans la base de données, l'application peut stocker le code "ETH4". Les tables de codes permettent également de localiser les zones déroulantes, qui peuvent donc contenir des valeurs correspondant à la langue ou au dialecte de l'utilisateur.

Les paramètres régionaux déterminent une langue et une région géographique spécifiques. La fonction de localisation de l'application prend en charge plusieurs

langues. Chaque langue est spécifiée par un mappage régional. Exemple : l'anglais est mappé "en" dans les paramètres régionaux.

Configurer les propriétés de l'application

Les paragraphes suivants décrivent la façon dont les propriétés de l'application peuvent être configurées. Les propriétés de l'application sont des variables utilisées par le système de différentes manières. Exemple : certaines propriétés modifient les fonctionnalités offertes par le système et permettent donc à celui-ci d'être configuré de façon à répondre aux besoins de l'organisation. Les valeurs de ces variables peuvent être gérées en cours d'exécution, donnant ainsi la possibilité de modifier des fonctionnalités de manière dynamique sans passer par un cycle de développement complet. Comme exemple de variable, on peut citer la propriété qui détermine le format de date par défaut utilisé par l'application : *curam.misc.app.defaultdateformat*. La valeur de cette propriété peut être "Date_mdy_ext" ou modifiée pour "Date_dmy_ext".

Rechercher une propriété

Il est possible de rechercher des propriétés et de les filtrer par paramètres régionaux et par catégorie. Les catégories des propriétés se divisent en deux types : la catégorie Application et la catégorie Infrastructure. Elles regroupent des types de propriétés similaires afin de simplifier leur gestion. Exemple de type de catégorie de propriété : "Application - Paramètres des adresses". Cette catégorie de propriété inclut toutes les propriétés liées aux paramètres des adresses dans l'application.

Ajouter une propriété à l'application

Il est possible d'ajouter des propriétés à l'application. Les informations contenues dans chaque propriété comprennent les paramètres régionaux, sa valeur actuelle, sa valeur par défaut et sa catégorie. La valeur par défaut spécifie la valeur que la propriété affichera si elle est réinitialisée par un utilisateur. Les paramètres régionaux permettent de spécifier la langue dans la description et le nom d'affichage de la propriété (ex. : *en-US*, Anglais - États-Unis). Le nom d'affichage est le nom de la propriété affiché à l'attention de l'utilisateur. Exemple : la propriété de serveur de messagerie utilisée par l'application affiche le nom *curam.notification.notificationemailserver*. La description fournit des informations détaillées sur la fonction de la propriété. Le nom d'affichage et la description doivent être rédigés dans la langue définie dans les paramètres régionaux.

Créer une description pour une propriété : Les propriétés de l'application peuvent disposer de plusieurs descriptions multilingues. La description d'une propriété comprend les paramètres régionaux, le nom d'affichage et la description de la propriété. Les descriptions multilingues permettent aux utilisateurs de différentes régions de comprendre les propriétés de l'application. Seule une description de propriété peut être entrée pour chaque paramètre régional.

Publier les modifications apportées à une propriété

Les modifications apportées à une propriété ne seront pas appliquées à l'application tant qu'elles ne seront pas publiées. Les propriétés de l'application ont des paramètres dynamiques qui déterminent si les modifications apportées à la propriété affecteront ou non le système après leur publication. Si une propriété est définie comme statique, les modifications publiées ne s'appliqueront qu'après le redémarrage du système, car les informations contenues dans les propriétés statiques ne peuvent pas être mises à jour quand l'application est en cours d'exécution. Comme exemple de propriété statique, on peut citer "curam.db.type=DB2", qui indique une connexion à une base de données DB2®. Cette connexion ne peut pas être désactivée quand l'application est en cours

d'exécution. Par conséquent, si la valeur est modifiée pour "curam.db.type=ORACLE", qui indique une connexion à une base de données Oracle, cette modification ne peut être appliquée qu'après le redémarrage du serveur.

Réinitialiser les propriétés par défaut

Les propriétés de l'application peuvent être réinitialisées à leur valeur par défaut. Celles qui disposent d'un paramètre dynamique seront modifiées instantanément. Les propriétés statiques seront réinitialisées à leur valeur par défaut après le redémarrage du serveur.

Configurer les tables de codes

Chaque table de codes se compose de plusieurs éléments qui représentent chacun une sélection dans une zone déroulante. Les principales informations d'une table de codes sont contenues dans ces éléments. Un élément de table de codes contient le code réel qui sera stocké dans la base de données de l'application lorsque cet élément de table de codes sera sélectionné dans une zone déroulante. Il contient également une description (texte affiché dans une zone déroulante) ainsi que les paramètres de langues qui contiennent des informations sur la localisation de l'élément de la table de codes.

Chaque table de codes possède un élément par défaut, et chaque zone déroulante est liée à un élément par défaut.

Ajouter une nouvelle table de codes à l'application

Il est possible d'ajouter de nouvelles tables de codes à l'application. Un nom unique doit être entré. Une fois la nouvelle table de codes nommée, des éléments peuvent être ajoutés. L'ordre dans lequel les éléments de la table sont affichés peut être spécifié. Les éléments peuvent être paramétrés comme sélectionnables. Si cet indicateur est défini, les éléments de table de codes apparaîtront dans la zone déroulante remplie par la table de codes parente. Il est également possible de paramétrer la langue des éléments de la table.

Les modifications apportées aux tables de codes ou à leurs éléments ne seront appliquées aux zones déroulantes de l'application que lorsqu'elles seront publiées (ou après le redémarrage du serveur).

Localiser des tables de codes

Il est possible de localiser les zones déroulantes d'une table de codes. Les zones déroulantes localisées contiennent les valeurs correspondant à la langue et au pays de l'utilisateur. La combinaison de la langue et du pays est appelée *paramètres régionaux*. Exemples de paramètres régionaux : en-US (Anglais, États-Unis), en-GB (Anglais, Royaume-Uni), es-US (Espagnol, États-Unis), etc.

L'utilisation de paramètres régionaux permet à l'application d'afficher différentes listes déroulantes pour des utilisateurs disposant de paramètres régionaux différents. Exemple : si les paramètres régionaux d'un utilisateur sont définis sur US-Spanish, la zone déroulante pour les jours de la semaine affichera les valeurs "Lunes", "Martes", "Jueves", etc. Inversement, si les paramètres régionaux d'un utilisateur sont définis sur US-English, la même zone déroulante affichera les valeurs "Monday", "Tuesday", "Wednesday", etc.

Deux paramètres d'élément de table sont localisables dans les zones déroulantes : la description (i.e. le texte qu'un utilisateur verra dans la zone déroulante) et la langue, qui fait référence aux paramètres régionaux de l'élément de la table de codes. Note : Bien que ce paramètre soit appelé "Langue" pour des raisons de

compréhension, il se rapporte en réalité aux paramètres régionaux, qui contiennent des informations à la fois sur la langue et sur le pays.

Dans les environnements utilisant plusieurs paramètres régionaux, il est recommandé d'enregistrer une version régionale de chaque élément de table pour toutes les tables de codes. Exemple : une table de codes listant les jours de la semaine a été créée dans un environnement qui utilise l'anglais et l'espagnol. Cette table de codes doit contenir deux éléments avec la valeur de code "DAY1" - l'une en anglais avec la description "Monday", l'autre en espagnol avec la description "Lunes". Avoir un code de langue pour chaque jour de la semaine garantit que les utilisateurs verront tous les jours de la semaine, quelle que soit la langue affichée par l'application.

Hiérarchies des tables de codes

Les tables de codes peuvent être utilisées pour grouper d'autres tables de codes dans une hiérarchie. Une hiérarchie de table de codes peut compter un nombre illimité de tables. Elle permet de déterminer les valeurs sélectionnables dans la zone déroulante d'une table de codes à partir de la valeur sélectionnée dans la zone d'une autre table. Exemple : les valeurs disponibles au moment de sélectionner le type d'attention spéciale à enregistrer pour un participant peuvent être obtenues à partir de la catégorie ou de l'attention spéciale sélectionnée. Les hiérarchies de tables de codes peuvent être visualisées et modifiées à partir de l'interface d'administration système de l'application. Pour plus d'informations sur les hiérarchies de tables de codes, consulter le `Guide du développeur de serveur`.

Utilisation de validations configurables

Les validations sont utilisées dans toute l'application pour garder le contrôle sur les données entrées par les utilisateurs, renforcer l'intégrité des données ou empêcher la saisie de données incohérentes. Comme exemple de validation, on peut citer “La date de début du rôle Participant du dossier ne doit pas être postérieure à la date de fin du dossier - "%1d".”. Cette notification est affichée lorsqu'un utilisateur tente d'ajouter un membre à un dossier dont la date de début est postérieure à la date de fin.

Même si toutes les validations incluses à la demande sont exécutées par défaut lors du traitement, certaines ont été définies comme non requises dans la mesure où elles n'ont aucun impact sur le traitement système si elles ne sont pas exécutées. Ces validations ont été prédéfinies comme des validations configurables et peuvent être affichées par une agence.

L'application d'administration de système permet à une agence de rechercher et de désactiver des validations qui ont été identifiées comme des validations configurables. Toutes les autres validations ne peuvent pas être conservées dans l'application et sont exécutées lors du traitement.

Si une organisation doit désactiver une validation non configurable, elle devra d’abord demander au Support de rendre cette validation configurable. La validation sera alors analysée et l'on déterminera si elle peut ou non être reclassifiée en tant que validation configurable.

Activation/désactivation des validations configurables

Les validations configurables peuvent être désactivées ou activées par un administrateur. La référence unique d'une validation, par exemple, bpocaseparticipantrole.err_
caseparticipantrole_xfv_from_date_caseheader_end_date|a|, est utilisée pour

rechercher et récupérer une validation. La référence d'une validation peut être identifiée à l'aide de la documentation relative au code HTML des messages de validation, décrite dans cette section.

Pour permettre à l'application de distinguer les validations, la référence de chaque validation configurable est composée d'une combinaison de l'ID du catalogue de messages et d'une constante alphabétique utilisée pour faire la distinction entre les validations utilisées dans différents modules. De plus, une constante numérique est également ajoutée à la fin de la référence de toutes les validations utilisant le même texte de message que d'autres validations d'un module. Ces constantes sont affectées de manière arbitraire, sans aucune signification particulière donnée aux lettres ou aux chiffres utilisés.

La recherche disponible dans l'application d'administration de système n'affichera que les validations configurables dont la référence unique correspond exactement à celle entrée.

Un administrateur peut afficher des informations pour déterminer si la validation configurable est actuellement activée ou désactivée, et peut choisir de l'activer ou de la désactiver, selon les besoins. Les validations désactivées ne sont pas exécutées lors du traitement système.

Les administrateurs peuvent également accéder à une liste de toutes les validations activées en laissant la zone de recherche vide.

La section suivante décrit la documentation que l'organisation peut utiliser pour identifier les validations qui ont été contrôlées et identifiées comme des validations configurables. Cette documentation fournit également la référence unique de chaque validation pouvant être utilisée pour rechercher une validation dans l'application d'administration de système.

Utilisation de la documentation relative aux messages de validation

Afin de déterminer quelles validations correspondent à des validations configurables pouvant être désactivées, les organisations peuvent se reporter à la documentation relative aux messages de validation fournie au format HTML avec les programmes d'installation. Cette documentation est accessible une fois le programme d'installation exécuté. Elle se trouve dans un dossier 'Doc' supérieur de la base de code installée. La page d'accueil de la documentation relative aux messages de validation est accessible en sélectionnant le fichier index.html situé dans le dossier ValidationMessages/html.

Vous pouvez afficher la liste des validations référencées par chaque méthode d'une classe de façade en sélectionnant le lien "Facades A-Z Index" sur la page d'accueil de la documentation, un nom de classe de façade, puis une méthode.

Vous pouvez aussi afficher la liste des validations référencées par chaque méthode d'un écran en sélectionnant le lien "Screens A-Z Index" sur la page d'accueil de la documentation, un nom d'écran, puis une méthode.

Pour chaque validation, une référence et un texte de message de validation sont fournis. Par exemple, pour la validation utilisée afin d'éviter que la date de début d'un rôle de participant au dossier soit ultérieure à la date de fin d'un dossier, la référence de validation BPOCASEPARTICIPANTROLE.ERR_ CASEPARTICIPANTROLE_ XFV_FROM_DATE_CASEHEADER_END_DATE et le

texte du message de validation indiquant que "la date de début du rôle du participant au dossier ne doit pas être ultérieure à la date de clôture du dossier - "%1d"." sont affichés.

Pour chaque validation, la documentation indique également si la validation est configurable ou non. Toutes les validations configurables ont été contrôlées comme n'ayant aucun impact sur le traitement système si elles ne sont pas exécutées, et peuvent être désactivées par une agence. Si la validation n'est pas configurable, alors l'organisation ne peut pas la désactiver dans l'application d'administration de système et doit demander au Support si une exigence est nécessaire pour désactiver la validation.

De plus, une section Messages configurables répertorie toutes les validations configurables, y compris les façades à partir desquelles les validations sont référencées. Vous pouvez accéder à cette section en sélectionnant le lien "Configurable Messages A-Z Index" sur la page d'accueil de la documentation. L'organisation peut utiliser cette liste pour déterminer la référence de validation unique nécessaire pour rechercher et désactiver la validation dans le cadre de l'administration de système.

Par exemple, si l'organisation souhaite identifier les validations existantes et configurables dans le cadre du processus de modification des membres du dossier, elle peut sélectionner l'option "Screens A-Z Index" sur la page d'accueil de la documentation, entrer "modifyCaseMember" pour filtrer la liste des écrans, sélectionner l'écran "Case_modifyCaseMemberFromList.uim", sélectionner la référence de façade "Case.modifyCaseMember", puis afficher une liste des validations, indiquant si chaque validation est configurable ou non.

Si l'organisation identifie la validation BPOCASEPARTICIPANTROLE.ERR_ CASEPARTICIPANTROLE_XFV_FROM_DATE_CASEHEADER_FROM_DATE comme configurable, elle peut effectuer une référence croisée de celle-ci avec la liste des validations configurables pour identifier l'ID de référence unique de la validation. Cette opération est effectuée à l'aide des filtres de référence de message et de façade. Si le nom de méthode "modifyCaseMember" est saisi dans le filtre de référence de façade et que la référence de validation BPOCASEPARTICIPANTROLE.ERR_ CASEPARTICIPANTROLE_XFV_FROM_DATE_CASEHEADER_FROM_DATE est saisie dans le filtre de référence de message, une référence de validation unique de bpocaseparticipantrole.err_ caseparticipantrole_xfv_from_date_caseheader_from_date|a| s'affiche pour la validation.

Si plusieurs références de validation uniques sont affichées pour une combinaison particulière de références de message et de façade, l'organisation peut déterminer la référence de validation unique à désactiver en activant l'affichage de la référence dans l'application à côté du texte du message de validation qui s'affiche lorsque le processus métier est exécuté, ce qui entraîne l'appel de la validation. Cela entraîne généralement l'affichage d'une seule référence de validation, correspondant à la validation devant être désactivée. Dans le cas peu probable où plusieurs références de validation sont affichées lorsque le processus métier est exécuté, cela représente une situation dans laquelle la même validation est effectuée deux fois au cours du même processus métier, et où ces deux validations doivent être désactivées.

Notez que toutes les entrées du catalogue de messages référencées par une méthode sont affichées pour chaque méthode dans la documentation relative aux messages de validation ; ainsi, d'autres types de messages, comme les messages

d'infrastructure et les messages utilisés pour la journalisation, peuvent également être affichés avec les messages de validation. De plus, pour chaque méthode, la documentation affiche également tous les messages référencés par une méthode appelée par la méthode, ainsi, dans certains cas, des messages qui ne sont pas nécessairement appelés par l'écran utilisant la méthode sont répertoriés.

La section suivante fournit davantage d'informations sur l'activation de l'affichage de l'ID de référence de validation unique dans l'application.

Activation de l'affichage de la référence de validation unique

Les organisations peuvent également identifier la référence unique d'une validation en activant la propriété d'application curam.validationmanager.displayreference.enabled. Cette propriété d'application permet d'affiche la référence de validation unique à côté du texte du message de validation affiché dans l'application. La référence de validation unique peut ensuite être utilisée pour rechercher et désactiver/activer la validation si celle-ci est configurable. Note : Dans le cas où les validations ne sont pas contrôlées par le Responsable Validation, aucune référence ne sera affichée, même si la propriété est activée. Ces validations ne sont pas configurables.

Configurer la langue et les mappages régionaux

La langue et les mappages régionaux sont utilisés pour personnaliser la langue de l'interface utilisateur. Ils sont essentiels à beaucoup d'opérations impliquant des données culturelles et linguistiques sensibles. Les paramètres régionaux servent par exemple à générer des communications pro forma.

À chaque langue est associé un paramètre régional. Les langues disponibles pour créer un nouveau mappage régional de langue sont tirées de la liste des langues disponibles dans le système.

Configurer les pseudonymes des participants pour la recherche

Il est possible de gérer un thésaurus de pseudonymes. Ce thésaurus permet à l'organisation de définir des pseudonymes communs qui seront associés à un nom. Par exemple, un bénéficiaire dont le prénom est "James" peut également répondre au nom "Jimmy" ou "Jamie". Les pseudonymes définis peuvent être utilisés comme critères pour rechercher un bénéficiaire et/ou un bénéficiaire non enregistré. Le paramètre de recherche de pseudonyme par défaut est défini via l'interface d'administration de l'application dans les paramètres des propriétés.

Pour plus d'informations sur la recherche de bénéficiaires par pseudonyme, consulter le `Guide Cúram - Participant`.

Configuration de la vérification orthographique

Vous pouvez configurer un vérificateur orthographique à utiliser dans l'éditeur de texte enrichi. La fonction de vérification orthographique est mise à disposition par le biais d'un bouton de plug-in standard dans la barre d'outils de l'éditeur de texte enrichi. Le vérificateur orthographique vérifie l'orthographe du contenu de la zone de texte.

Les organisations peuvent activer ou désactiver le vérificateur orthographique via la propriété d'application curam.spellcheck.enable. Si cette propriété d'application

est activée, le bouton du vérificateur orthographique apparaît dans la barre d'outils de l'éditeur de texte enrichi. Si elle est désactivée, le bouton du vérificateur orthographique n'apparaît pas.

Lorsque la vérification orthographique est activée, un utilisateur peut sélectionner le dictionnaire à utiliser dans la barre d'outils de l'éditeur de texte enrichi. Une agence peut utiliser la table de codes SpellcheckLocale pour activer et désactiver les dictionnaires que l'utilisateur peut sélectionner. Cette table de codes peut aussi être utilisée pour indiquer quel est le dictionnaire à présenter par défaut. La table de codes est remplie avec les valeurs d'environnement local pour les dictionnaires suivants qui sont disponibles :

- Anglais (Etats-Unis)
- Anglais (Royaume-Uni)
- Français
- Français (Canada)
- Allemand
- Italien
- Espagnol
- Portugais

Configuration des requêtes de sélection des audits de dossier

Introduction

Ce chapitre donne un aperçu des options de l'interface d'administration système permettant de configurer les audits de dossiers. Les audits de dossiers servent à examiner et à évaluer des dossiers. La liste des dossiers à auditer est générée par des requêtes de sélection. Une requête de sélection est constituée d'une instruction SQL et de critères de sélection, utilisés pour valider la requête et obtenir des informations de la base de données. Il existe deux types de requêtes de sélection : les requêtes dynamiques et les requêtes fixes.

La requête dynamique permet de générer une liste de dossiers de manière très flexible. Le coordinateur d'audit peut choisit un ou plusieurs critère(s) pour générer cette liste. Exemple : le coordinateur peut choisir de générer une liste de tous les dossiers affichant le statut "Ouvert", ou sélectionner plusieurs critères pour générer cette liste. Exemple : les critères de date de lancement et de sexe permettent d'obtenir un groupe plus spécifique de dossiers.

La requête fixe est moins flexible que la requête dynamique, en cela que les valeurs des critères constituent une partie de la requête. Le coordinateur d'audit ne peut pas entrer les paramètres d'une requête fixe. Cependant, les requêtes fixes sont réutilisables et plus faciles à exécuter, étant donné que le coordinateur n'a pas à sélectionner de critères. Exemple de requête fixe : "Tous les dossiers ouverts pour les hommes âgés de 18 à 35 ans".

Pour plus d'informations sur les requêtes de sélection et les audits de dossiers en général, consulter le `Guide Cúram - Audits de dossiers`. Pour de plus amples informations sur les requêtes de sélection et les instructions SQL, consulter le `Guide Cúram - Développement d'audits de dossiers`.

Créer et publier une requête de sélection dynamique

De nouvelles requêtes de sélection dynamique peuvent être créées par un administrateur de base de données ou un administrateur système. Une fois créées, elles sont associées à une configuration d'audit de dossier par un administrateur. Avant de pouvoir associer la nouvelle requête de sélection à une configuration d'audit de dossier, des tâches de développement seront nécessaires pour produire la nouvelle page de critères de sélection que le coordinateur d'audit utilisera. Quatre exemples de requêtes dynamiques sont fournis pour chaque type de dossier standard : Dossiers intégrés, Produits de prestations, Produits de dette et Dossier d'investigation.

À la création d'une requête de sélection dynamique, il est impératif d'attribuer des noms aux pages de recherche manuelle et de recherche aléatoire. Ce sont les pages que le coordinateur a devant lui lorsqu'il crée une liste de dossiers à auditer. L'administrateur système doit également entrer l'instruction SQL de la requête de sélection qui sera utilisée pour recherche la liste des dossiers voulus dans la base de données.

Lorsqu'une requête de sélection est créée, des critères de sélection sont enregistrés pour garantir la validité de la requête. L'administrateur système publie ensuite la requête de sélection afin qu'elle puisse être ajoutée à une configuration d'audit de dossier par un administrateur. Le coordinateur d'audit pourra alors utiliser cette requête pour générer une liste de dossiers à auditer. Les critères de sélection permettent d'obtenir une liste de dossiers.

Lors de la configuration d'un audit de dossier, l'administrateur ne doit associer qu'une seule requête dynamique prédéfinie à une configuration d'audit.

Créer et publier une requête de sélection fixe

Les requêtes fixes sont utilisées parallèlement aux requêtes dynamiques. Le coordinateur d'audit a la possibilité de choisir le type de requête qu'il souhaite utiliser pour générer la liste aléatoire de dossiers à auditer (si cela a été configuré comme tel). Il n'est pas nécessaire de spécifier les noms des pages à la création de requêtes fixes, ces dernières étant prédéfinies. Les coordinateurs d'audit n'ont pas besoin d'entrer des paramètres pour les critères de sélection de la requête. Les pages affichant les critères de sélection ne sont donc pas nécessaires.

Sinon, les requêtes fixes sont créées de la même façon que les requêtes dynamiques, avec une instruction SQL validée par les critères de sélection. Une fois la requête fixe publiée, l'administrateur peut l'associer à une configuration d'audit de dossier. Le coordinateur d'audit peut choisir n'importe quelle requête fixe configurée pour un audit de dossier. Lorsqu'elle est utilisée pour générer une liste de dossiers à auditer, elle permet au coordinateur d'obtenir une liste dans l'application en cours d'exécution.

L'administrateur peut associer une ou plusieurs requêtes fixes à une configuration d'audit de dossier.

Configuration des modèles de communication

Introduction

Ce chapitre donne un aperçu des différentes options permettant de configurer les modèles de communication. Deux types de modèle sont pris en charge :Microsoft Word et XSL. Les modèles XSL sont des feuilles de style permettant de générer des

communications pro forma. Les modèles Microsoft Word sont utilisés pour créer des communications Microsoft Word. Les modèles XSL servent à générer des communications de masse, tandis que les modèles Microsoft Word servent à communiquer des informations plus spécifiques aux clients et aux participants, et peuvent être édités individuellement selon les besoins de l'assistant social.

Pour plus d'informations sur les modèles de communication, consulter le `Guide Cúram - Communications`.

Gérer les modèles Microsoft Word

Les modèles Microsoft Word sont des modèles de document basiques offrant un certain niveau de personnalisation pour les communications client individuelles.

Ils n'exigent aucune connaissance technique spécifique et peuvent être créés dans Microsoft Word. Chaque modèle peut être recherché localement et téléchargé. Pour télécharger un modèle Microsoft Word, il est nécessaire d'entrer un nom et un ID pour le modèle en question, ainsi que des paramètres régionaux. Cela permet à l'assistant social de choisir parmi plusieurs modèles à partir des paramètres régionaux du participant concerné lorsqu'il crée une communication Microsoft Word.

Un modèle Microsoft Word compte plusieurs zones qui permettent de remplir automatiquement la communication Microsoft Word à sa création avec certaines données, comme l'adresse du correspondant. À noter : Pour remplir les zones insérées dans le modèle Microsoft Word avec les données du client, il sera nécessaire de passer par des phases de développement. Pour plus d'informations sur la façon d'insérer ces zones, reportez-vous à la section «Insérer des zones dans un modèle Microsoft Word», à la page 23.

Gérer les modèles XSL

Les modèles XSL permettent de générer des documents et des lettres pro forma imprimés par l'application à l'aide d'une combinaison de feuilles de style XML et XSL.

Les feuilles de style XSL sont utilisées pour formater les données XML en vue de l'impression. Les modèles XSL peuvent être créés à partir de n'importe quel éditeur XSL. Ils peuvent ensuite être téléchargés et archivés dans la base de données de l'application. Pour télécharger un modèle XSL, il est nécessaire d'entrer une description et un ID pour le modèle en question, ainsi que des paramètres régionaux. Cela permet à l'assistant social de choisir parmi plusieurs modèles à partir des paramètres régionaux du participant concerné lorsqu'il crée une communication pro forma. Il est impossible de créer plusieurs modèles XSL utilisant les mêmes ID et paramètres régionaux.

Les modèles XSL peuvent être extraits et téléchargés. Extraire un modèle permet de conserver ses anciennes versions. Les modèles peuvent être extraits simultanément par plusieurs personnes. Les administrateurs système peuvent choisir d'ignorer les autres versions extraites d'un modèle. Le contrôle des versions des modèles permet de veiller à ce que les modèles ne soient pas écrasés par erreur. C'est le développeur de feuilles de style XSL qui est responsable de la création et de la gestion des modèles XSL. Lorsqu'une nouvelle version est disponible au téléchargement, l'administrateur système peut restituer l'ancienne version et télécharger le nouveau fichier XML.

Pour plus d'informations sur le XML et la génération de documents à partir de modèles XML et XSL, consulter le Guide Cúram - Infrastructure XML.

Assigner des modèles de communication à des types de dossiers ou de participants

Les modèles XSL et Microsoft Word peuvent être assignés à un type de dossier ou de participant spécifique, car certains modèles sont restreints à un type de dossier ou de participant bien précis. Exemple : le modèle "Décision d'appel" ne peut être assigné qu'aux participants ayant entamé une procédure d'appel. Les administrateurs peuvent attribuer des modèles à des types de dossiers ou de participants par catégorie. Exemple : le dossier "Catégories" comprend un certain nombre de types de dossiers (Soutien aux revenus, Examen préalable, etc.). Une fois configuré, le modèle ne sera accessible à l'assistant social qui crée la communication que pour le type de dossier spécifié.

Un modèle Microsoft Word compte plusieurs zones qui permettent de remplir automatiquement la communication Microsoft Word à sa création avec certaines données, comme l'adresse du correspondant. Pour plus de détails sur la façon d'insérer ces zones, consulter l'Annexe A.

Configuration des traitements par lots

Introduction

Ce chapitre donne un aperçu des différentes options permettant de configurer les traitements par lots. Les traitements par lots sont des exécutables ou des "mini-programmes" qui permettent de traiter un grand nombre d'enregistrements, selon les paramètres définis. Compte tenu du temps de traitement de certains lots, ce processus est souvent planifié pendant les périodes creuses par les organisations (nuit, week-ends, etc.).

Ajouter un nouveau traitement par lots à l'application

Il est possible d'ajouter de nouveaux traitements par lots à l'application. Avant de pouvoir utiliser le traitement par lots dans l'application, il est nécessaire de développer le processus correspondant dans le modèle d'application. Pour ce faire, il suffit d'assigner un stéréotype de lot au processus. Une fois le modèle généré, un exécutable SQL est créé pour le traitement par lots. Cet exécutable peut ensuite être ajouté à l'application par l'administrateur système. Un exécutable de lots ne peut être associé qu'à un seul traitement par lots. L'administrateur système sélectionne le traitement par lots requis à partir de la liste des traitements disponibles. Il convient d'ajouter un nom et une description au traitement par lots, et de spécifier son type. Les traitements par lots peuvent être des lots de reporting ou d'archivage. Chaque type de traitement par lots est associé à une description codée, utilisée pour regrouper des traitements par lots similaires.

Pour plus d'informations sur la création de nouveaux traitements par lots, consulter le Guide Cúram - Traitements par lots.

Organiser les traitements par lots en groupes

Les groupes de traitements par lots organisent les traitements par lots en groupes logiques. Exemple : il est possible de regrouper des traitements financiers par lots afin que les utilisateurs n'aient pas à rechercher dans toute la liste des traitements par lots pour retrouver un traitement financier particulier. Pour ce faire, il suffit d'ajouter des traitements par lots à un groupe et de nommer le groupe en question.

Les groupes de traitements par lots offrent la flexibilité nécessaire à une organisation pour gérer ses listes de traitements par lots, et regrouper ses traitements par lots selon ses besoins.

Soumettre un traitement par lots pour exécution

Les traitements par lots peuvent être exécutés en les sélectionnant dans la liste des traitements par lots disponibles. Selon le traitement par lots concerné, un certain nombre de paramètres doivent être entrés avant de pouvoir exécuter le lot. La demande de lot sera traitée une fois le lanceur par lots exécuté. Pour plus de détails sur les paramètres requis et l'exécution du lanceur par lots, consulter le Guide Cúram - Traitements par lots.

L'utilisateur peut définir les valeurs des paramètres en soumettant un traitement par lots. Cela limite le nombre d'informations qui seront traitées. Exemple de traitement par lots : DetermineProductDeliveryEligibility ("Déterminer l'éligibilité d'une prestation produit"). Il permet d'activer un grand nombre de dossiers simultanément et est exécuté en tant que traitement par lots pour différer le traitement de ces dossiers pendant les heures creuses, et ainsi minimiser l'impact sur le système. Le traitement par lots est configuré pour inclure le paramètre product (produit). Définir un produit spécifique comme paramètre permettra de traiter les dossiers correspondant au produit en question. À noter : Les valeurs de certains paramètres doivent être définies afin que les traitements par lots puissent être exécutés (les autres paramètres ne sont pas à définir). Il est possible de définir une valeur par défaut pour un paramètre. Elle s'appliquera alors à chaque exécution du traitement par lots, sauf si l'utilisateur définit une autre valeur.

L'ordre dans lequel les traitements par lots sont exécutés doit également entrer en ligne de compte, car certains traitements par lots ne fonctionneront pas si d'autres n'ont pas été exécutés avant. Exemple : DetermineProductDeliveryEligibility ("Déterminer l'éligibilité d'une prestation produit") doit être exécuté avant GenerateInstructionLineItems ("Générer des lignes d'instructions"), car les lignes d'instruction ne peuvent être générées que pour les dossiers qui ont été activés.

Une fois que l'administrateur système a soumis les traitements par lots, ces derniers sont mis en file d'attente jusqu'à ce que le lanceur de lots soit exécuté. Le lanceur de lots est un programme autonome qui exécute les traitements par lots dans l'ordre dans lequel ils ont été soumis. À noter : il est possible de spécifier une date de traitement pour un lot. La date de traitement correspond d'ordinaire à la date du système. Si une date de traitement est spécifiée, elle remplacera la date du système.

Créer un code d'erreur de traitement par lots

Les codes d'erreur de traitement par lots permettent aux utilisateurs de spécifier les codes d'erreur qui seront renvoyés par le lanceur de lots de l'application en cas d'échec du traitement par lots. Les informations contenues dans un code d'erreur comprennent l'ID du code d'erreur et le code d'erreur lui-même.

Lorsqu'un traitement par lots échoue, un message d'erreur est généré et transféré au lanceur de lots de l'application. Le lanceur de lots recherche le code d'erreur correspondant à l'ID du message d'erreur. S'il trouve le code correspondant, le lanceur de lots lancera les actions nécessaires pour régler l'erreur. Ces actions sont configurées par le développeur de l'application.

Exemple : si l'ID du code d'erreur renvoyé par le traitement en échec est CANNOT_CONNECT_TO_DATABASE ("Impossible de se connecter à la base de

données"), le lanceur de lots compare ce code à tous les codes d'erreur enregistrés dans le système. S'il trouve l'ID de code CANNOT_CONNECT_TO_DATABASE, le lanceur de lots récupère le code d'erreur associé à cet ID (ex. : «11»). Il le transfère ensuite à un Responsable de tâches qui examinera ses propres fichiers de configuration pour déterminer ce qu'il convient de faire en cas de réception du code d'erreur 11. Pour plus d'informations sur le lanceur de lots et les autres aspects liés à l'administration des traitements par lots, consulter le Guide Cúram - Traitements par lots.

Configuration de la sécurité

Introduction

Ce chapitre donne un aperçu des différentes options permettant de configurer l'administration de la sécurité. Au plus haut niveau, la sécurité de l'application veille à ce que seuls des utilisateurs valides puissent accéder à l'application. Elle définit spécifiquement ce qu'un utilisateur peut visualiser et modifier dans l'application. L'administration de sécurité est divisée en deux grandes catégories : l'authentification et les autorisations. L'authentification permet de garantir que seuls des utilisateurs valides peuvent accéder à l'application en fournissant un nom d'utilisateur et un mot de passe valides. Tandis que l'authentification sécurise l'application à la phase de connexion, les autorisations, elles, sécurisent l'application une fois qu'un utilisateur valide s'est connecté. Elles définissent les droits des utilisateurs, et ainsi leur possibilité de lancer des actions ou d'accéder aux informations.

Pour plus d'informations sur les utilisateurs, les rôles de sécurité, les groupes de sécurité et la mise en place de mesures de sécurité dans l'application, consulter le Guide du développeur de serveur Cúram.

Types de sécurité s'appliquant aux éléments de l'application

Un identificateur de sécurité (SID) est une ressource protégée. Chaque élément sécurisé dans l'application est doté d'un SID unique. Ces SID permettent de sécuriser les fonctions administratives et les zones d'un écran, ainsi que les unités, les emplacements, les audits de dossiers et les programmes de l'organisation (dont les produits et les plans de services).

Le type de SID le plus répandu est le SID fonctionnel, aussi appelé identificateur de fonction ou FID. Les FID sont utilisés pour sécuriser les processus métier. Comme exemple de FID, on peut citer celui assigné au processus d'enregistrement des bénéficiaires. Il existe également un autre type d'identificateur de sécurité : le SID de zone. La sécurité de zone permet de sécuriser les informations spécifiques affichées dans une zone, une page ou un ensemble de pages. Comme exemple de SID de zone, on peut citer le SID utilisé pour sécuriser la zone "Solde de compte bancaire" d'un participant.

Sécuriser les fonctions de l'application

Les fonctions du serveur sont sécurisées par le biais de FID. Pendant la phase de développement de l'application, lorsqu'une méthode est rendue accessible publiquement, un identificateur de sécurité unique est automatiquement généré pour cette fonction. Dans l'application déployée, les méthodes comprises dans le modèle deviennent des fonctions de serveur. Si la sécurité d'une méthode de processus est désactivée dans le modèle au moment du développement, un identificateur de fonction sera généré mais ne pourra pas être utilisé. Une fois les fonctions générées, des FID peuvent être créés et ajoutés à la hiérarchie de sécurité

par un administrateur système, en recherchant une fonction et en lui associant un FID. Seules les fonctions qui ne sont pas déjà associées à un FID seront sélectionnables. Les modifications apportées à un FID ne prendront effet qu'une fois publiées.

Sécuriser les zones de l'application

La sécurité de zone détermine les droits des utilisateurs et leur possibilité de visualiser les informations contenues dans des zones spécifiques. Tout comme les fonctions, les différentes zones de l'application peuvent être sécurisées par le biais de SID dont les utilisateurs doivent disposer dans leur profil de sécurité afin de visualiser ou d'accéder aux zones en question. Pendant la phase de développement de l'application, les développeurs créent des SID pour les zones devant être sécurisées. Par défaut, une zone n'est pas sécurisée. C'est au développeur d'indiquer qu'une zone spécifique a besoin d'un SID. Le SID est ensuite ajouté dans la base de données. Ce SID doit néanmoins être ajouté à la hiérarchie de sécurité par un administrateur système, qui veillera également à ce que le SID soit ajouté aux bons profils utilisateur. Les modifications apportées à un SID ne prendront effet qu'une fois publiées.

Sécuriser les unités, les emplacements et les programmes de l'organisation

L'administrateur système peut créer des SID pour sécuriser l'accès aux unités, aux emplacements, aux audits de dossiers et aux programmes de l'organisation (dont les produits et les plans de services). Exemple : l'administrateur système peut créer un SID pour un type de produit, qui sera ensuite utilisé par un administrateur pour sécuriser l'accès à ce type de produit. De la même manière, l'administrateur système peut créer un SID pour une unité de l'organisation, qui sera ensuite utilisé par un administrateur pour déterminer quels utilisateurs sont en droit de manipuler les informations liées à cette unité. Les modifications apportées à un SID ne prendront effet qu'une fois publiées.

Pour plus d'informations sur la sécurité de l'organisation, de ses emplacements et de ses produits, consulter le `Guide d'administration des localisations Cúram`, le `Guide d'administration des organisations Cúram` et le `Guide de gestion des dossiers intégrés Cúram`.

Grouper les FID et les SID connexes

Un groupe de sécurité est constitué d'identificateurs de sécurité connexes. Ce niveau de la hiérarchie de sécurité permet à l'administrateur de regrouper un grand nombre d'identificateurs de sécurité dans un petit nombre de groupes. Tous les utilisateurs ayant un groupe de sécurité spécifique assigné à leur rôle de sécurité auront accès à toutes les ressources représentées par les identificateurs de sécurité appartenant au groupe. Exemple : les utilisateurs sont autorisés à enregistrer un bénéficiaire si leur rôle de sécurité inclut le groupe de sécurité comprenant l'identificateur de sécurité dédié à l'enregistrement de bénéficiaires.

Profils de sécurité utilisateur

Les profils de sécurité utilisateur sont définis par une hiérarchie d'identificateurs de sécurité (SID). Ils s'appliquent aux utilisateurs internes comme externes. Les SID sont les éléments qui structurent le profil de sécurité d'un utilisateur. Ils permettent de sécuriser les fonctions administratives et les zones d'un écran, ainsi que les unités, les emplacements et les audits de dossiers de l'organisation. Ils sont également utilisés pour sécuriser les programmes offerts par l'organisation, dont les produits et les plans de services.

Le premier objectif du profil de sécurité utilisateur est de garantir que tous les utilisateurs sont bien autorisés à accéder aux informations dont ils ont besoin pour mener à bien leur activité dans l'organisation, tout en limitant l'accès de ces utilisateurs aux informations sécurisées. Le second objectif est de trouver un moyen de mieux gérer ces profils de façon à ce que les tâches de l'administrateur système ne deviennent pas répétitives.

Identifier les rôles de sécurité

La première étape à la création d'un profil de sécurité utilisateur est d'identifier les rôles requis de l'organisation. Une organisation pouvant être relativement grande et donc avoir beaucoup d'utilisateurs, il est logique de créer des profils de sécurité pour les utilisateurs partageant le même accès de sécurité. Parallèlement, il est important de distinguer les différents niveaux de compétence parmi les utilisateurs ayant des profils similaires. Même si les assistants sociaux junior et senior travaillent sur des dossiers, certaines opérations métier ne pourront pas être réalisées par les assistants sociaux junior. Exemple : un assistant social junior ne peut pas conduire de revues de dossiers, ni approuver des dossiers. Dès lors, ce n'est pas seulement la fonction principale d'un utilisateur qui définit son rôle de sécurité, mais aussi son niveau de compétence. En organisant les SID dans une hiérarchie, les processus métier similaires et partagés entre les utilisateurs peuvent facilement être distribués, sans avoir à déclarer manuellement tous les éléments sécurisés pour chaque profil utilisateur.

Limiter l'accès d'un utilisateur aux éléments de l'application en utilisant des profils de sécurité

Les profils de sécurité s'appliquent aux utilisateurs internes comme externes. En organisant les SID dans une hiérarchie, les processus métier similaires et partagés entre les utilisateurs peuvent facilement être distribués, sans avoir à déclarer manuellement tous les éléments sécurisés pour chaque rôle de sécurité. Les rôles de sécurité peuvent être constitués de plusieurs groupes de sécurité, eux-mêmes composés d'identificateurs connexes. Toutes les modifications apportées à un rôle de sécurité ne prendront effet qu'une fois publiées.

Les autorisations déterminent les droits d'accès d'un utilisateur aux éléments sécurisés de l'application à partir du rôle de sécurité de l'utilisateur en question. Chaque utilisateur autorisé se voit attribuer un rôle de sécurité. Il est donc possible d'autoriser tous les utilisateurs à accéder aux éléments sécurisés d'une application. Les utilisateurs externes ont un accès plus restreint par rapport aux utilisateurs internes.

Optimiser les autorisations en utilisant le cache de sécurité : Le cache de sécurité est une structure en mémoire créée pour conserver les informations de sécurité liées aux rôles utilisateur. Les informations de sécurité sont conservées dans ce cache pour optimiser les performances du processus d'autorisation.

Le cache est rafraîchi à chaque redémarrage de l'application ou lorsque l'administrateur système utilise l'option correspondante. Le cache doit être rafraîchi à chaque modification apportée aux rôles utilisateur (identificateur de sécurité, groupes de sécurité, rôles de sécurité, etc.), sauf en cas d'ajout d'un nouvel utilisateur, si d'autres modifications de sécurité (apportées à des rôles ou à des groupes) ne sont pas prévues.

Configuration de Business Intelligence

Introduction

Ce chapitre donne un aperçu des différentes options permettant de configurer au niveau système la Business Intelligence (BI). Business Intelligence permet aux assistants sociaux, aux superviseurs et aux responsables senior de l'organisation d'obtenir des informations d'aide à la décision. Les informations utiles à chaque fonction sont différentes et sont répercutées dans les outils de Business Intelligence dédiés à chaque fonction.

La Business Intelligence couvre trois grands domaines : les entrepôts de données, l'analyse intégrée et les tableaux de bord/rapports interactifs. Les entrepôts de données sont une composante de la fonction Reporting de l'application, utilisée par la BI pour remplir des rapports avec des données. L'analyse intégrée permet de représenter les données extraites des entrepôts de données et de les afficher à l'attention de l'utilisateur. Les tableaux de bord interactifs servent à publier des informations de manière graphique et intuitive (graphiques sous forme de numéros, de jauges ou de feux de circulation). Ces affichages indiquent la progression de l'attribut de performance par rapport à un objectif ou une valeur cible. La fonction Reporting permet de créer des rapports formatés et interactifs avec des capacités de distribution et de planification ultra évolutives.

Le Concepteur de rapports BIRT (Business Intelligence and Reporting Tools, ou "Outils de Business Intelligence et de reporting"), est un plug-in Eclipse permettant aux développeurs de créer des rapports BI personnalisés qui peuvent ensuite être importés dans l'application. Un grand nombre de graphiques utilisant le moteur graphique BIRT sont pris en charge, tout comme le listage de données. Les contenus BI peuvent être affichés dans les pages de l'application suivant les besoins. Un tableau de bord BI licenciable est également disponible. Une fois les rapports créés et disponibles dans le système, ils peuvent être affichés dans l'application via le moteur de reporting BIRT, qui permet de concevoir des rapports. Ce moteur génère des rapports dans plusieurs formats, dont les formats HTML et PDF. Les données agrégées d'un rapport BI sont affichées de manière à ce que l'utilisateur puisse interagir avec elles.

Pour plus d'informations sur la génération et le déploiement de rapports BI, consulter le `Guide du développeur BIRT Cúram`.

Configurer des rapports de Business Intelligence

La Business Intelligence inclut un certain nombre d'exemples de rapports préconfigurés. Ces exemples de rapports montrent la manière dont les rapports sont structurés et comment ils peuvent être utilisés pour lire et déployer les informations contenues dans la base de données. Des tâches de développement seront nécessaires pour rendre ces rapports disponibles dans l'application. Une fois ces tâches réalisées, les rapports devront être copiés vers le répertoire de contenu BI sur le serveur de l'application.

Les options de reporting BIRT qui peuvent être configurées via l'interface d'administration système de l'application sont notamment les suivantes :

Tableau 1. Options de configuration de reporting BIRT.

Cette table décrit les options de reporting BIRT

Option de configuration de reporting	Description
Nom du rapport	Il s'agit du nom d'affichage du rapport. Les rapports peuvent avoir plusieurs configurations avec des noms d'affichage différents.
Nom du fichier de rapport	Le véritable chemin de fichier vers le rapport sur le serveur de rapports.
Catégorie du rapport	La catégorie permet de classifier le rapport à des fins de recherche (ex. : dossier, participant, etc.).
Servlet de rapport	Servlet de rapport utilisé pour rendre le rapport.
Paramètres	Les paramètres correspondent à l'image du graphique, et non au graphique lui-même. La largeur et la hauteur peuvent être définies, ainsi que la possibilité d'activer le défilement. Il est également possible d'afficher une bordure autour du rapport.

D'autres paramètres peuvent être ajoutés aux rapports BI, à partir d'une liste reconnue par BIRT, ou des paramètres métier spécifiques supportés par les rapports (après programmation).

Configurer le visualiseur de rapports de Business Intelligence

Le visualiseur BIRT peut être utilisé pour afficher les rapports BI dans l'application. Les options qui peuvent être configurées pour le visualiseur sont notamment les suivantes :

Tableau 2. Options de configuration du visualiseur de rapports BIRT.

Cette table décrit les options du visualiseur BIRT

Option de configuration du visualiseur de rapports	Description
Nom du visualiseur	Nom du moteur du visualiseur de rapports.
Servlet	Servlet de configuration du visualiseur de rapports utilisé pour rendre les rapports. Chaque configuration de rapport peut utiliser son propre paramètre de servlet. L'option par défaut est "run".
Paramètre du nom du rapport	Il spécifie le type de visualiseur de rapport. La valeur par défaut est "__report".
Contexte	Définit la manière dont l'URL du rapport est générée.
Racine	Spécifie la chaîne de configuration racine du rapport (indicateur http, nom du serveur, port sur lequel le serveur de rapport s'exécute, etc.)

D'autres paramètres par défaut peuvent être ajoutés au visualiseur de rapports, à partir d'une liste de paramètres reconnus par BIRT afin qu'ils puissent être utilisés par le visualiseur de rapports.

Configuration d'un système cible

Introduction

Ce chapitre donne un aperçu des options de base de l'interface d'administration système permettant de configurer des systèmes cibles. Un client peut avoir plusieurs installations système dans son environnement. L'application prend en charge plusieurs services qui peuvent communiquer et interagir avec ces systèmes. Lorsqu'il utilise l'un de ces services, le système à l'origine de l'interaction est considéré comme le système source, tandis que le(s) système(s) avec le(s)quel(s) il communique est/sont considéré(s) comme le(s) système(s) cible(s).

Exemple : un client configure deux installations de l'application pour effectuer deux opérations métier distinctes (ex. : Cúram for Global Income Support et Cúram for Child Care). Ce client souhaite ensuite partager les données des informations collectées entre les deux systèmes afin d'améliorer leur efficacité opérationnelle. Dans ce cas, les deux systèmes peuvent être configurés pour pouvoir communiquer entre eux et utiliser le logiciel Cúram Evidence Broker pour partager les informations collectées.

Créer un système cible

Afin que les services d'un système source puissent communiquer avec des systèmes cibles, l'administrateur système doit dans un premier temps configurer les détails du système cible dans le système source, en utilisant l'onglet de configuration système correspondant disponible dans son espace de travail.

Ajouter un service au système cible

Il est possible d'attribuer plusieurs services à un système cible. Dans l'exemple décrit dans l'introduction de ce chapitre, le service en question est le logiciel Evidence Broker. Une URL (Uniform Resource Locator) doit être définie pour tous les services associés au système cible. Cette URL permet d'identifier et d'interagir avec le service dans le système cible. Elle est générée en combinant l'URL racine du système cible (composée du nom d'hôte et du port du système) et l'URL d'extension du service associé. Exemple : une URL du type "http:// shell.example.com:9082/<servername>/services/EvidenceBroker" peut être générée pour le service Evidence Broker dans un système cible en combinant l'URL racine ("http:// shell.example.com:9082/") du système cible et l'URL d'extension ("<servername>/services/EvidenceBroker") du service Evidence Broker associé.

Les systèmes cibles peuvent également être utilisés dans le Cúram Configuration Transport Manager (CTM), où ils permettent de transférer automatiquement les données de configuration entre le système source et le système cible. La définition du système cible de CTM se fait via le service Configuration Transport Manager.

Configuration des services d'interopérabilité de gestion de contenu

Introduction

Ce chapitre décrit les options de configuration spécifiques à l'intégration de l'application à un système de gestion de contenu. Cela inclut les propriétés d'application utilisées pour activer l'intégration et la configuration des informations de métadonnées.

Lorsque l'application est activée pour l'intégration à un système de gestion de contenu, les documents associés aux pièces jointes et communications sont stockés dans et extraits depuis le système de gestion de contenu. Des informations de métadonnées concernant le document, comme le type de document, peuvent être stockées avec les documents de pièces jointes dans le système de gestion de contenu.

Pour plus d'informations sur la manière dont l'application peut être intégrée à un système de gestion de contenu, consultez le manuel Cúram Content Management Interoperability Services Integration Guide.

La section suivante décrit la méthode d'activation de l'intégration à un système de gestion de contenu.

Activation de l'intégration à un système de gestion de contenu

L'intégration à un système de gestion de contenu est activée via l'utilisation d'un groupe de propriétés d'application situé sous la catégorie 'Application - Paramètres de gestion de contenu'. Trois propriétés d'application sont disponibles pour contrôler le niveau d'intégration à un système de gestion de contenu.

La propriété d'application curam.cms.enable est utilisée pour spécifier si l'emplacement de stockage de certains fichiers doit être situé dans le système de gestion de contenu configuré au lieu de la base de données de l'application. Lorsque la propriété d'application est activée, deux propriétés supplémentaires peuvent ensuite être utilisées pour contrôler les fichiers à stocker dans le système de gestion de contenu. La propriété curam.cms.attachment.enable est utilisée pour spécifier si les fichiers considérés comme des pièces jointes doivent être stockés dans le système de gestion de contenu. Cela inclut les pièces jointes associées aux communications enregistrées et aux communications Microsoft Word. La propriété curam.cms.proforma.enable est utilisée pour spécifier si les fichiers considérés comme des communications Pro Forma doivent être stockés dans le système de gestion de contenu. Cela inclut tous les fichiers associés aux communications Pro Forma, à l'exception des communications Pro Forma créées suite à un traitement par lots.

La section suivante décrit les options de configuration disponibles pour le stockage des informations de métadonnées.

Configuration des métadonnées pour les pièces jointes

Lorsque des documents associés à des pièces jointes sont créés dans l'application et stockés dans le système de gestion de contenu, des informations de métadonnées concernant le document peuvent également être stockées. Cela inclut les documents de pièces jointes associés aux communications enregistrées et aux communications Microsoft Word.

Les informations de métadonnées pouvant être stockées sur le document dépendent du contexte dans lequel la pièce jointe a été créée. Par exemple, si une pièce jointe est créée dans le contexte d'un dossier, des informations concernant le dossier dans lequel la pièce jointe a été créée peuvent être stockées avec le document ; toutefois, si la pièce jointe est créée dans le contexte d'un participant, aucune information de dossier ne peut être stockée, cependant des informations sur le participant peuvent l'être.

Si des informations concernant un document, comme la date de réception du document, sont modifiées ultérieurement dans l'application, les informations de métadonnées associées peuvent également être mises à jour. La possibilité ou non d'effectuer une mise à jour d'un élément de métadonnées spécifique dépend également du contexte spécifique résultant d'une mise à jour de la pièce jointe.

L'application peut être configurée de manière à stocker plusieurs éléments de métadonnées prédéfinis avec le document de pièce jointe. Par défaut, les éléments de métadonnées sont activés, et chacun d'entre eux peut être désactivé individuellement de manière à ce que les informations ne soient pas stockées avec le document dans le système de gestion de contenu.

L'activation ou la désactivation d'un élément de métadonnées n'affecte pas les métadonnées précédemment stockées dans le système de gestion de contenu. Les changements apportés à la configuration des métadonnées OOTB ne prennent effet que lorsque de nouvelles pièces jointes sont créées ou lorsque des pièces jointes existantes sont mises à jour en empêchant le stockage d'éléments de métadonnées ou en autorisant le stockage d'éléments de métadonnées supplémentaires, selon les paramètres de configuration.

Chaque élément de métadonnées possède un nom d'affichage et une description visibles par l'administrateur. Plusieurs noms d'affichage et descriptions peuvent être créés pour chaque élément de métadonnées de manière à fournir une prise en charge multilingue, et les noms d'affichage et descriptions existants peuvent être modifiés si nécessaire.

Les éléments de métadonnées suivants sont disponibles pour les documents considérés comme pièces jointes, y compris les pièces jointes associées aux communications enregistrées et aux communications Microsoft Word :

Tableau 3. Eléments de métadonnées.

Ce tableau affiche les éléments de métadonnées disponibles pour les pièces jointes.

Eléments de métadonnées	Description
Référence du dossier	Numéro de référence du dossier
Référence du participant	Numéro de référence du participant
Prénom du participant	Prénom d'une personne ou d'une personne candidate
Nom du participant	Nom d'une personne ou d'une personne candidate
Date de naissance du participant	Date de naissance d'une personne ou d'une personne candidate
Type de document	Type de document
Code type du document	Code du type de document
Date de réception du document	Date à laquelle le document a été reçu

Tableau 3. Eléments de métadonnées (suite).

Ce tableau affiche les éléments de métadonnées disponibles pour les pièces jointes.

Eléments de métadonnées	Description
Date de communication	Date de communication des pièces jointes associées aux communications enregistrées

Une organisation peut également choisir d'implémenter des éléments de métadonnées supplémentaires pour répondre à leurs propres besoins métier. Pour plus d'informations sur la prise en charge des éléments de métadonnées supplémentaires, consultez le manuel `Cúram Content Management Interoperability Services Integration Guide`.

Conclusion

Récapitulatif

Voici un résumé des principaux concepts détaillés dans ce guide :

- La sécurité de l'application est configurée dans l'interface d'administration système de l'application. Les profils de sécurité déterminent la manière dont les utilisateurs interagissent avec l'application. Ils sont basés sur des identificateurs de sécurité qui sont utilisés pour sécuriser les fonctions, les zones, les produits, les appels et les plans de service.
- Il existe deux types de modèles de communication configurables via l'interface d'administration système de l'application : les modèles Microsoft Word et les modèles XSL.
- Les requêtes de sélection d'audits de dossiers sont configurées via l'interface d'administration système de l'application.
- Il existe plusieurs options permettant de configurer les traitements par lots dans l'interface d'administration système de l'application. Les traitements par lots permettent de traiter un grand nombre d'enregistrements, selon les paramètres définis.
- L'interface d'administration système de l'application offre des options de configuration pour le visualiseur de rapports de Business Intelligence.
- Les systèmes cibles permettent de partager des données entre différents systèmes.
- Des options permettant de configurer l'intégration à un système de gestion de contenu sont disponibles dans l'application d'administration de système.

Informations complémentaires

Vous trouverez des informations complémentaires sur les sujets susvisés dans les guides suivants :

Guide d'administration des organisations Cúram
Ce guide couvre les concepts de base de la fonctionnalité Administration des organisations.

Guide d'administration des localisations Cúram
Ce guide couvre les concepts de base de la fonctionnalité Administration des localisations.

Guide Cúram - Participant
Ce guide couvre le concept de base du participant.

Guide de gestion des dossiers intégrés Cúram
Ce guide couvre les concepts de base du traitement de dossiers.

Guide Cúram - Communications
Ce guide donne un aperçu de la fonctionnalité Communications.

Guide Cúram - Audits de dossiers
Ce guide donne un aperçu métier des audits de dossier.

Informations techniques

Voici une liste des documents techniques référencés dans ce guide :

Guide du développeur de serveur Cúram
Ce guide fournit des informations techniques sur les propriétés de l'application, la sécurité et les tables de codes.

Guide Cúram - Traitements par lots
Ce guide donne un aperçu du traitement par lots.

Guide Cúram - Opérations
Ce guide donne un aperçu du fonctionnement de l'application (ex. : propriétés).

Guide du développeur BIRT Cúram
Ce guide détaille les étapes nécessaires au développement de la Business Intelligence.

Guide Cúram - Développement d'audits de dossiers
Ce guide couvre le développement des audits de dossier.

Guide Cúram - Infrastructure XML
Ce document présente tous les aspects de la fonctionnalité XML disponible dans l'environnement SDEJ (Server Development Environment) : modélisation, développement, gestion d'exécution, etc.

Manuel Cúram Content Management Interoperability Services Integration Guide
Ce manuel présente les options de configuration disponibles pour l'intégration de Cúram à un système de gestion de contenu.

Insérer des zones dans un modèle Microsoft Word

Introduction

Cette annexe donne la marche à suivre pour créer un modèle Microsoft Word contenant des zones permettant de conserver des variables, comme l'adresse d'un correspondant. Cette annexe détaille également la manière de rédiger le code de serveur qui permet d'entrer les variables dans le modèle lorsqu'une communication basée sur ce modèle est créée par un assistant social.

Créer un modèle Microsoft Word

Pourquoi et quand exécuter cette tâche

Les modèles Microsoft Word sont créés dans l'application Microsoft Word. Il est donc indispensable de bien connaître l'application Microsoft Word pour créer des modèles Microsoft Word. Lorsqu'un modèle Microsoft Word est créé, des zones sont générées. Elles seront remplacées à la création de la communication par les variables spécifiques au correspondant.

Note : une fois qu'une communication Microsoft Word a été créée à partir d'un modèle, les données spécifiques au correspondant deviennent partie intégrante de la communication. Exemple : si le modèle Microsoft Word inclut les variables relatives au nom et à l'adresse du correspondant, le nom et l'adresse du correspondant seront enregistrés à la place des variables dans le contenu de la communication.

Pour insérer une zone dans le modèle Microsoft Word - zone qui sera remplacée par la variable renvoyée par le serveur -, suivez les étapes décrites ci-après.

Procédure

1. Ouvrir un nouveau document Microsoft Word. Note : ce document doit être ouvert en dehors de l'application, c'est-à-dire localement.
2. Créer de nouvelles zones personnalisées intitulées "Propriétés du document" (comme indiqué dans la section «Contenu d'un modèle Microsoft Word exemple», à la page 25 ci-après, créer les zones suivantes : AddressLine1, AddressLine2, AddressLine3, personName, userName).
3. Insérer la zone créée dans le modèle. Pour cela :
   a. Cliquez à l'endroit où vous souhaitez insérer une zone.
   b. Dans l'onglet "Insérer" et le groupe "Texte", cliquez sur "Éléments" puis sur "Zone".
   c. Dans la liste des "Catégories", sélectionnez la catégorie "Informations du document"
   d. Dans la liste des "Noms de zones", sélectionnez "DocProperty", puis la zone que vous avez créée à partir de la liste "Propriétés de la zone".

Résultats

Lorsque les variables ont été insérées dans les zones du modèle Microsoft Word, le contenu du texte de la communication - qui restera le même pour toutes les communications générées à partir de ce modèle - peut être ajouté directement dans le document. Le fichier est ensuite sauvegardé comme un document Microsoft Word standard et peut être recherché et téléchargé comme n'importe quel fichier via l'application.

Pour plus d'informations sur la recherche et le téléchargement de modèles Microsoft Word, voir la section «Gérer les modèles Microsoft Word», à la page 11.

Rédiger un code de serveur pour remplir les données de communication

Une fois le modèle créé et disponible dans l'application, l'assistant social peut le sélectionner au moment de créer une communication. Il entre ensuite tous les autres détails requis pour créer la communication, comme le nom du correspondant, le nom de la communication, etc.

Lorsque la communication est ouverte, le serveur affiche les variables à insérer dans les zones du modèle Microsoft Word, comme le nom et l'adresse du correspondant.

Les variables renvoyées par le serveur sont affichées sous la forme d'un objet de type BLOB. Cet objet se compose de paires nom-valeur, l'attribut "nom" ("NAME") faisant référence aux zones du modèle Microsoft Word et l'attribut "valeur" ("VALUE") aux données à insérer dans les zones à la création du document.

Contenu d'un modèle Microsoft Word exemple

Voici un exemple de modèle Microsoft Word. Les éléments AddressLine1, AddressLine2, AddressLine3, personName et userName sont les propriétés personnalisées du document. Elles peuvent être remplacées par les données spécifiques au correspondant, obtenues à partir du serveur, et varieront donc dans chaque communication. En revanche, le contenu situé dans le corps du modèle restera le même pour toutes les communications créées à partir de ce modèle.

```
{ DOCPROPERTY AddressLine1 }
{ DOCPROPERTY AddressLine2 }
{ DOCPROPERTY AddressLine3 }

 Monsieur / Madame { DOCPROPERTY personName }

  Ceci est un exemple de modèle Microsoft Word.

  Merci,
  { DOCPROPERTY userName }
```

Figure 1. Contenu d'un modèle Microsoft Word exemple

Code exemple pour renvoyer des données vers un modèle de communication Microsoft Word

Le fragment de code exemple suivant illustre la manière dont il faut rédiger le code afin d'entrer les valeurs dans un objet BLOB et l'utiliser pour insérer les valeurs dans le document Microsoft Word. À noter : les valeurs sont insérées sous la forme d'une paire nom-valeur utilisant l'élément org.jdom.Element.

L'attribut "nom" ("NAME") dans la paire nom-valeur est le nom de la propriété du document (DocProperty) insérée dans le modèle. L'attribut "valeur" ("VALUE") correspond aux données spécifiques au correspondant qui remplaceront la zone dans le modèle de communication Microsoft Word créé.

```
org.jdom.Element rootElement = new org.jdom.Element("ROOT");
org.jdom.Element fieldsElement = new org.jdom.Element ("FIELDS");

org.jdom.Element fieldElement = new org.jdom.Element ("FIELD");
fieldElement.setAttribute ("NAME", "personName");
fieldElement.setAttribute ("VALUE", "James Smith");
fieldsElement.addContent (fieldElement);

org.jdom.Element fieldElement1 = new org.jdom.Element ("FIELD");
fieldElement1.setAttribute ("NAME", "AddressLine1");
fieldElement1.setAttribute ("VALUE", "1074, Park Terrace");
fieldsElement.addContent (fieldElement1);

org.jdom.Element fieldElement2 = new org.jdom.Element ("FIELD");
fieldElement2.setAttribute ("NAME", "AddressLine2");
fieldElement2.setAttribute ("VALUE", "Fairfield, Midway");
fieldsElement.addContent(fieldElement2);

org.jdom.Element fieldElement3 = new org.jdom.Element ("FIELD");
fieldElement3.setAttribute ("NAME", "AddressLine3");
fieldElement3.setAttribute ("VALUE", "UTAH");
fieldsElement.addContent (fieldElement3);

org.jdom.Element fieldElement4 = new org.jdom.Element ("FIELD");
fieldElement4.setAttribute ("NAME", "userName");
fieldElement4.setAttribute ("VALUE", "Caseworker");
fieldsElement.addContent (fieldElement4);

rootElement.addContent (fieldsElement);

return new curam.util.type.Blob (
new org.jdom.output.XMLOutputter
.outputString(rootElement).getBytes());
```

Figure 2. Code exemple pour renvoyer des données vers un modèle de communication Microsoft Word

Pour en savoir davantage sur la façon de rédiger un code de serveur, consultez le Guide du développeur de serveur Cúram.

Structure de l'objet obtenu à partir du code exemple

L'exemple suivant illustre la structure de l'objet généré par le système sous la forme de paires nom-valeur binaires, comme dans le fragment de code susvisé :

```
<ROOT>
<FIELDS>
<FIELD NAME= "personName", VALUE="James Smith" />
<FIELD NAME= "AddressLine1", VALUE= "1074, Park Terrace"/>
<FIELD NAME= "AddressLine2", VALUE= "Fairfield, Midway" />
<FIELD NAME= "AddressLine3", VALUE="UTAH" />
<FIELD NAME= "userName", VALUE="Caseworker" />
</FIELDS>
</ROOT>
```

Figure 3. Structure de l'objet obtenu à partir du code exemple

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM. IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous accorde aucune licence pour ces brevets. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations

IBM Canada Ltd

3600 Steeles Avenue East

Markham, Ontario

L3R 9Z7 Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing

Legal and Intellectual Property Law.

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun autre pays dans lequel il serait contraire aux lois locales. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUT RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies. Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation

Dept F6, Bldg 1

294 Route 100

Somers NY 10589-3216

U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le programme sous licence décrit dans ce document et tous les éléments sous licence associés sont fournis par IBM selon les termes de l'IBM Customer Agreement, de l'IBM International Program License Agreement ou de tout contrat équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles.

IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Ces informations contiennent des exemples de programmes d'application en langage source qui illustrent des techniques de programmation sur diverses plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programmes sont fournis "EN L'ÉTAT", sans garantie d'aucune sorte. IBM décline toute responsabilité relative aux dommages éventuels résultant de l'utilisation de ces exemples de programmes.

Toute copie intégrale ou partielle de ces exemples de programmes et des oeuvres qui en sont dérivées doit inclure une mention de droits d'auteur libellée comme suit :

© (nom de votre société) (année). Des segments de code sont dérivés des exemples de programmes d'IBM Corp.

© Copyright IBM Corp. _année ou années_. All rights reserved.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Politique de confidentialité

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels") peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent,

aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-après.

Selon la configuration déployée, la présente Offre Logiciels peut utiliser des cookies de session et des cookies persistants destinés à collecter le nom et le mot de passe des utilisateurs pour les fonctions de gestion des session et d'authentification, pour faciliter l'utilisation des produits, pour la configuration de la connexion unique et/ou pour d'autres fonctions de suivi ou buts fonctionnels. Ces cookies ou d'autres technologies similaires ne peuvent pas être désactivés.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/fr/fr, la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/details/fr/fr, ainsi que la page "IBM Software Products and Software-as-a-Service Privacy Statement" à l'adresse http://www.ibm.com/software/info/product-privacy.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse http://www.ibm.com/legal/us/en/copytrade.shtml.

Adobe, le logo Adobe et Portable Document Format (PDF) sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

BIRT est une marque d'Eclipse Foundation.

Microsoft et Word sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Oracle est une marque d'Oracle et/ou de ses sociétés affiliées.

D'autres noms peuvent être des marques de leurs propriétaires respectifs. Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.