IBM Security Identity Manager
Version 6.0

Guide de configuration

SC11-7069-00

IBM Security Identity Manager
Version 6.0

Guide de configuration

SC11-7069-00

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 277.

Première édition - novembre 2012

Réf. US : SC14-7696-00

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

Liste de tables

A propos de cette publication

Le document *IBM Security Identity Manager – Guide de configuration* fournit des informations sur la configuration et la personnalisation d'IBM Security Identity Manager. Le produit a été conçu pour nécessiter une configuration minimale. Il vous revient de décider si vous souhaitez modifier les paramètres par défaut lorsque cela est nécessaire.

Accès aux publications et à la terminologie

Cette section inclut les éléments suivants :

- Liste des publications se trouvant dans la bibliothèque IBM Security Identity Manager.
- Liens vers «Publications en ligne».
- Lien vers la «Site Web de terminologie IBM», à la page x.

Bibliothèque IBM Security Identity Manager

Les documents suivants sont disponibles dans la bibliothèque IBM Security Identity Manager :

- *IBM Security Identity Manager – Guide de démarrage rapide*, CF3L2ML
- *IBM Security Identity Manager - Guide de présentation du produit*, GC11-7064
- *IBM Security Identity Manager - Guide des scénarios*, SC11-7065
- *IBM Security Identity Manager - Guide de planification*, GC11-7066
- *IBM Security Identity Manager - Guide d'installation*, GC11-7067
- *IBM Security Identity Manager - Guide de configuration*, SC11-7069
- *IBM Security Identity Manager - Guide de sécurité*, SC11-7070
- *IBM Security Identity Manager - Guide d'administration*, SC11-7071
- *IBM Security Identity - Guide de traitement des incidents*, GC11-7072
- *IBM Security Identity Manager - Guide de référence des messages d'erreur*, GC11-7073
- *IBM Security Identity Manager - Guide de référence*, SC11-7074
- *IBM Security Identity Manager - Guide de référence des bases de données et des schémas*, SC11-7075
- *IBM Security Identity Manager - Glossaire*, SC11-7076

Publications en ligne

IBM présente ses publications lors du lancement du produit et lorsque ces documents sont mis à jour aux emplacements suivants :

Centre de documentation IBM Security Identity Manager
Le site http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm présente la page d'accueil du centre de documentation pour ce produit.

Centre de documentation IBM Security
Le site http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp affiche une liste alphabétique répertoriant les différents documents IBM Security ainsi que des informations générales.

IBM Publications Center

Le site http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss comporte des fonctions de recherche personnalisée vous permettant de trouver toutes les publications IBM dont vous avez besoin.

Site Web de terminologie IBM

Le site Web de terminologie IBM regroupe la terminologie des bibliothèques de logiciels en un seul emplacement. Vous pouvez accéder au site Web de terminologie à l'adresse http://www.ibm.com/software/globalization/terminology.

Accessibilité

Les fonctions d'accessibilité permettent aux personnes souffrant d'un handicap physique (par exemple, une mobilité réduite ou une déficience visuelle) de pouvoir utiliser les logiciels. Ce produit permet d'utiliser des technologies d'assistance pour entendre et naviguer dans l'interface. Vous pouvez également utiliser le clavier au lieu de la souris pour toutes les fonctions de l'interface graphique.

Pour plus d'informations, voir la rubrique relative aux fonctions d'accessibilité d'IBM Security Identity Manager dans le document *IBM Security Identity Manager - Guide de référence*.

Formation technique

Pour obtenir des informations sur la formation technique, voir le site Web de formation IBM suivant sur la page http://www.ibm.com/software/tivoli/education.

Informations de support

IBM Support vous offre des services d'assistance lorsqu'il existe des problèmes de code, de routine, d'installation de courte durée et répond aux questions concernant l'utilisation. Vous pouvez accéder directement au site de support logiciel IBM à l'adresse http://www.ibm.com/software/support/probsub.html.

Le document *IBM Security Identity Manager - Guide de traitement des incidents* fournit des informations sur :

- les informations à collecter avant de contacter le support IBM.
- les différents moyens de contacter le support IBM.
- le mode d'utilisation d'IBM Support Assistant.
- des instructions et de des ressources de détermination des incidents permettant d'isoler et de résoudre le problème.

Remarque : L'onglet **Communauté et support** dans le centre de documentation du produit peut fournir des ressources de support supplémentaires.

Chapitre 1. Présentation de la personnalisation de l'interface utilisateur

Beaucoup d'utilisateurs veulent une interface utilisateur simple pour que leurs employés interagissent avec IBM® Security Identity Manager afin d'exécuter les fonctions de base de gestion et d'application des accès. IBM Security Identity Manager fournit une interface utilisateur double personnalisable et fournit les fonctions IBM Security Identity Manager de base nécessaires à la fois pour les utilisateurs de base et les administrateurs.

Les options de personnalisation d'interface fournies par IBM Security Identity Manager apportent aux clients le contrôle et la souplesse requis pour gérer la façon dont les fonctions IBM Security Identity Manager sont présentées à leurs employés. Avec ces options, les clients peuvent intégrer une interface utilisateur en libre-service et une interface de console d'administration dans le site Web de leur intranet et appliquer une présentation commune à l'entreprise.

Personnalisation de l'interface utilisateur en libre-service

Cette section décrit comment personnaliser l'interface utilisateur en libre-service.

L'interface utilisateur en libre-service IBM Security Identity Manager peut être personnalisée. Les clients peuvent intégrer une présentation commune de l'entreprise tout en conservant la souplesse d'exécuter les tâches d'auto-gestion d'identité inhérentes à leurs rôles et responsabilités.

Vous pouvez définir et personnaliser l'interface en libre-service de deux manières, à l'aide de l'infrastructure préfabriquée de la console intégrée ou bien en modifiant directement les fichiers installés dans IBM Security Identity Manager :

- Fonctions de la console intégrée :
  - Eléments de contrôle d'accès (ACI)
  - Vues
- Fichiers modifiables :
  - Fichiers de propriétés
  - Fichiers de feuille de style en cascade (CSS)
  - Un sous-ensemble de fichiers Java Server Pages (JSP)
  - Fichiers image

Sauvegardez tous les fichiers modifiables à des fins de récupération avant d'apporter des modifications personnalisées à IBM Security Identity Manager.

Fichiers de configuration et leurs descriptions

Les fichiers de configuration définissent l'aspect de l'interface utilisateur IBM Security Identity Manager en libre-service.

Les tables suivantes affichent la liste des noms de fichier et décrivent leur rôle dans la personnalisation d'IBM Security Identity Manager.

Tableau 1. Fichiers de configuration des propriétés et leurs descriptions

Nom du fichier	Description du fichier
SelfServiceUI.properties	• Contrôle l'aspect de l'interface utilisateur (bannière, en-tête, barre de navigation, barre d'outils), le nombre de pages affichées et le nombre de résultats de recherche renvoyés. • Configure les éléments disponibles dans la zone "Rechercher par" pour la recherche d'utilisateur dans l'interface en libre-service. • Active l'accès direct à l'écran de modification du mot de passe expiré et ignore la page de connexion en libre-service sous certaines conditions. La clé de propriété qui permet ces actions est ui.directExpiredChangePasswordEnabled.
SelfServiceScreenText.properties	Fournit le texte sur l'interface utilisateur en libre-service.
SelfServiceScreenText_*langue* .properties	Fournit le texte spécifique à la langue sur l'interface utilisateur en libre-service. Par défaut, ce fichier est SelfServiceScreenText_en.properties, qui contient l'ensemble en anglais.
SelfServiceHomePage.properties	Définit les sections de la page d'accueil de l'interface utilisateur en libre-service et l'ordre dans lequel elles sont affichées.
SelfServiceHelp.properties	Définit les liens vers les pages d'aide HTML relative à l'interface utilisateur en libre-service. Les fichiers HTML sont disponibles dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ ITIM.ear\itim_self_service_help.war. Vous pouvez réacheminer l'aide en modifiant les informations figurant dans ce fichier.
SelfServiceScreenTextKeys .properties	Fournit des clés de libellé pour l'interface utilisateur en libre-service. Ce fichier peut être utilisé pour faciliter la personnalisation du texte de l'écran en fournissant un modèle pour développer des libellés et des instructions. Le fichier contient des libellés qui sont définis sur le nom de clé. Par exemple, password_title=password_title. A des fins de personnalisation et de développement, vous pouvez copier ce fichier dans SelfServiceScreenText_*langue*.properties, où *langue* est un suffixe de langue qui n'est pas installé. Vous pouvez alors basculer les environnements locaux de votre navigateur de la langue en cours vers la langue inutilisée. Redémarrez l'application Web pour parcourir les pages et voir les clés de libellé au lieu du texte de la valeur. En basculant les environnements locaux de votre navigateur, vous pouvez alors basculer entre les clés et les valeurs. Lorsque la personnalisation est terminée, vous pouvez copier et renommer le fichier selon le suffixe de langue que vous voulez utiliser, par exemple SelfServiceScreenText_en.properties, pour parachever les modifications.

Tableau 2. Fichiers de configuration JSP (Java Server Pages) et descriptions

Nom du fichier	Description du fichier
loginBanner.jsp	Comporte le contenu de la bannière sur la page de connexion en libre-service.
loginFooter.jsp	Comporte le contenu du pied de page sur la page de connexion en libre-service.
loginToolbar.jsp	Comporte le contenu de la barre d'outils sur la page de connexion en libre-service.
Home.jsp	Comporte le contenu de la page d'accueil en libre-service.
banner.jsp	Comporte le contenu de la bannière en libre-service.
footer.jsp	Comporte le contenu du pied de page en libre-service.
nav.jsp	Comporte le contenu de la barre de navigation en libre-service.
toolbar.jsp	Comporte le contenu de la barre d'outils en libre-service.

Tableau 3. Fichiers de configuration de feuille de style en cascade (CSS) et leurs descriptions

Nom du fichier	Description du fichier
calendar.css	Fichier CSS contenant les styles utilisés avec les objets fenêtre d'agenda.
customForm.css	Fichier CSS contenant les styles utilisés pour la présentation des formulaires personnalisés dans le cas d'une orientation de langue de gauche à droite.
customForm_rtl.css	Fichier CSS contenant les styles utilisés pour la présentation des formulaires personnalisés dans le cas d'une orientation d'une langue de droite à gauche.
dateWidget_ltr.css	Fichier CSS contenant les styles utilisés avec les objets fenêtre de date pour l'orientation d'une langue de gauche à droite.
dateWidget_rtl.css	Fichier CSS contenant les styles utilisés avec les objets fenêtre de date pour l'orientation d'une langue de droite à gauche.
enduser.css	Fichier CSS contenant les styles CSS principaux pour l'orientation d'une langue de gauche à droite.
enduser_rtl.css	Fichier CSS contenant les styles CSS principaux pour l'orientation d'une langue de droite à gauche.
time.css	Fichier CSS contenant les styles utilisés avec les objets fenêtre d'agenda.
widgets.css	Fichier CSS contenant les styles utilisés avec d'autres objets fenêtre pour l'orientation d'une langue de gauche à droite.
widgets_rtl.css	Fichier CSS contenant les styles utilisés avec d'autres objets fenêtre pour l'orientation d'une langue de droite à gauche.

Sauvegarde et restauration des fichiers de configuration de l'interface utilisateur en libre-service

Avant de commencer la personnalisation de l'interface utilisateur en libre-service, sauvegardez tous les fichiers de configuration dans IBM Security Identity Manager pour pouvoir les récupérer ultérieurement.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Connectez-vous à chaque ordinateur qui exécute IBM Security Identity Manager. Effectuez une copie de sauvegarde des fichiers suivants :

- Dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_self_service.war\custom :
  - banner.jsp
  - calendar.css
  - customForm.css
  - customForm_rtl.css
  - dateWidget_ltr.css
  - dateWidget_rtl.css
  - enduser.css
  - enduser_rtl.css
  - footer.jsp
  - Home.jsp
  - loginBanner.jsp
  - loginFooter.jsp
  - loginToolbar.jsp
  - nav.jsp
  - time.css
  - toolbar.jsp
  - widgets.css
  - widgets_rtl.css

  Remarque : Les fichiers par défaut sont aussi disponibles dans le répertoire *ITIM_HOME*\data\defaults.
- Dans le répertoire *ITIM_HOME*\data :
  - SelfServiceHelp.properties
  - SelfServiceHomePage.properties
  - SelfServiceScreenText.properties
  - SelfServiceUI.properties
  - SelfServiceScreenTextKeys.properties

Pourquoi et quand exécuter cette tâche

Si vous avez apporté des modifications aux fichiers de propriétés, vous devez redémarrer l'application IBM Security Identity Manager. Par exemple, après avoir récupéré des fichiers de propriétés, exécutez les étapes suivantes :

Procédure

1. Avec la console d'administration de WebSphere, cliquez sur le groupe **Applications** dans le cadre gauche, puis cliquez sur le lien **Applications d'entreprise**.

2. Cochez la case en regard de l'application IBM Security Identity Manager puis cliquez sur le bouton **Arrêter**.
3. Une fois l'application arrêtée, cochez la case en regard de l'application IBM Security Identity Manager puis cliquez sur le bouton **Démarrer**.
4. Vérifiez que la récupération a été exécutée en vous connectant à l'interface utilisateur en libre-service.

Eléments de l'interface utilisateur concernés par les définitions de vue

Les vues définies déterminent la visibilité des panneaux de tâche et des autres éléments à l'intérieur de l'interface en libre-service.

Eléments de définition de la vue

Les définitions de la vue peuvent avoir les attributs suivants dans l'interface utilisateur en libre-service :

Page d'accueil

La page d'accueil s'adapte aux vues de l'utilisateur en n'affichant dans la page d'accueil que les tâches et les panneaux de tâche auxquels l'utilisateur a accès. Si l'utilisateur n'est autorisé à visualiser aucune tâche dans une section, alors le panneau de tâche n'apparaît pas non plus dans la page d'accueil.

Certaines vues de tâche, telles que la tâche Compte de demande, comportent des vues avancées. Pour clarifier, Compte de demande est une tâche unique. Si la vue Compte de demande avancé est autorisée ou que les vues Compte de demande et Compte de demande avancé sont autorisées toutes les deux, l'utilisateur aura une seule tâche **Compte de demande** dans la page d'accueil et la page principale Compte de demande affiche une page de recherche dans laquelle l'utilisateur peut rechercher un service pour lequel il peut demander un compte. Si seule la vue Compte de demande standard est autorisée, mais pas la vue avancée, alors la tâche **Compte de demande** apparaît dans la page d'accueil et la page principale Compte de demande affiche une table avec la liste des services pour lesquels l'utilisateur peut demander un compte, au lieu d'une page de recherche.

Si l'utilisateur a la possibilité d'exécuter à la fois les tâches Modifier et Afficher pour un compte ou un profil, les deux tâches sont fusionnées en une seule tâche. Par exemple, la tâche apparaît comme **Afficher ou modifier un compte**.

Certaines tâches peuvent ne pas apparaître si elles ne sont pas activées par l'administrateur système, par exemple **Modifier les informations en cas de mot de passe oublié**, qui nécessite l'activation de la réponse à une demande d'authentification.

La tâche **Intervention nécessaire** est uniquement disponible s'il y a des éléments d'état to-do en attente ou si les informations de réponse à une demande d'authentification ne sont pas configurées.

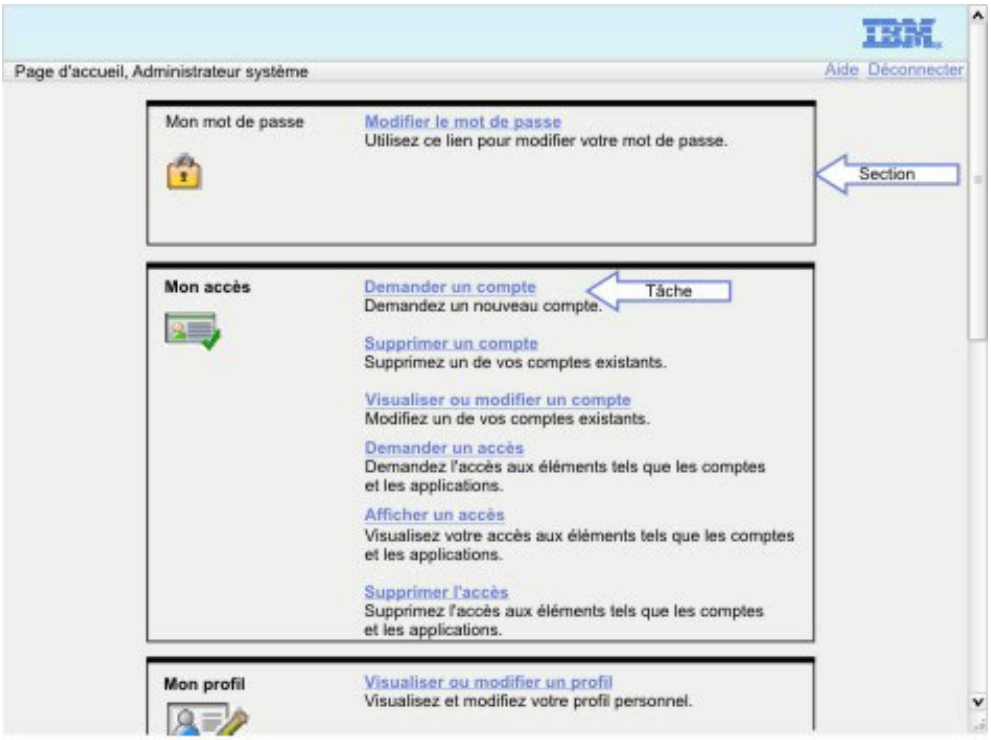


Figure 1. Eléments de la page d'accueil

Tâches connexes

Les sections de tâches connexes sont affichées dans de nombreuses zones de l'application en libre-service, par exemple lorsqu'une demande est soumise. Les définitions de la vue peuvent filtrer l'affichage de tout ou partie de ces sections d'après les droits de définition de vue. Par exemple, si l'utilisateur n'a pas d'accès normal à **Visualiser mes demandes**, cet élément n'apparaît pas dans le panneau de la tâche **Tâches connexes**.

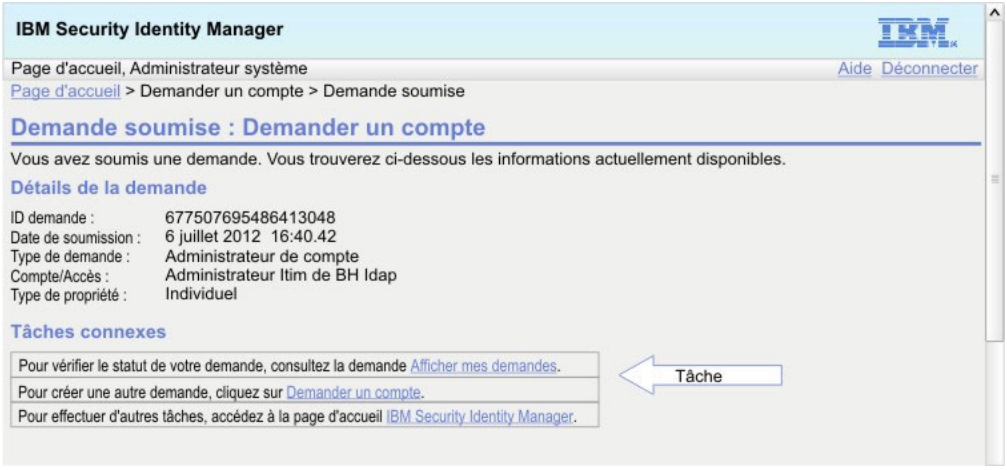


Figure 2. Elément de panneau de tâche connexe

Texte de l'instruction du panneau

Le texte de l'instruction sur certains écrans peut contenir des liens vers la tâche **Visualiser mes demandes**. Un message d'instruction différent s'affiche sans le lien de tâche si l'utilisateur n'a pas accès à la tâche **Visualiser mes demandes** dans une définition de la vue.

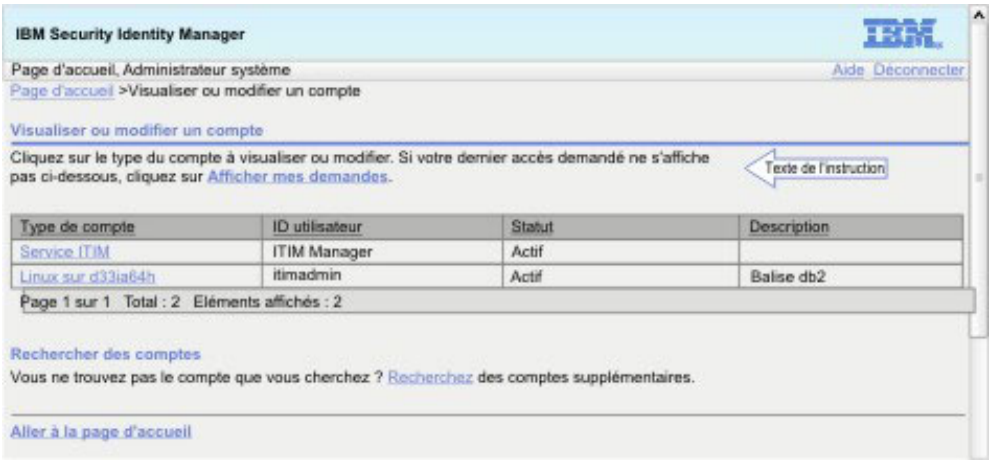


Figure 3. Elément du panneau de texte d'instruction

Personnalisation des libellés, descriptions et autres textes à l'écran

Vous pouvez modifier la majorité du texte affiché dans l'interface utilisateur en libre-service par personnalisation.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Tous les libellés ne peuvent pas être personnalisés par l'utilisateur. Seuls ceux qui possèdent une entrée dans le fichier SelfServiceScreenTextKeys.properties peuvent être personnalisés.

Les éléments de texte d'écran suivants peuvent être personnalisés :

- Titres
- Titres de sous-section
- Descriptions de sous-section
- Libellés de zone
- En-têtes et pieds de page de colonne de la table
- Texte de bouton

La figure suivante montre la représentation visuelle de ces éléments de texte d'écran.

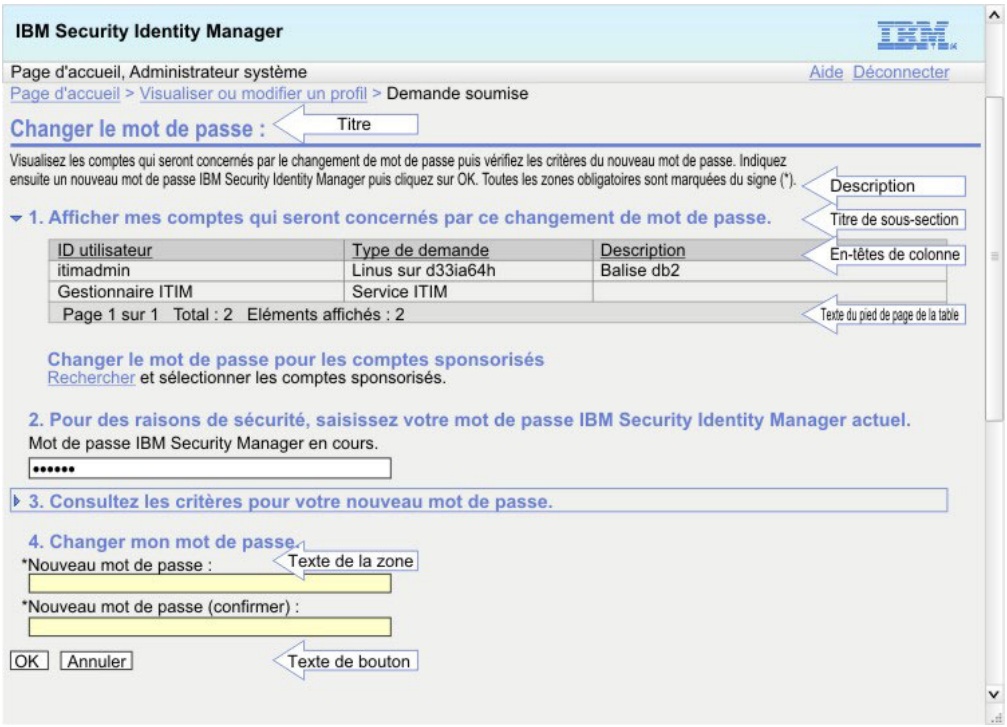


Figure 4. Texte d'écran

Le texte qui ne peut pas être remplacé correspond aux messages d'erreur et au texte du contenu d'aide auquel vous accédez en cliquant sur le lien d'aide. Cependant, il est possible de réacheminer les demandes d'aide vers une URL différente.

Pour personnaliser le texte d'écran, exécutez les étapes suivantes :

Procédure

1. Effectuez une copie de sauvegarde des fichiers `SelfServiceScreenText.properties` et `SelfServiceScreenTextKeys.properties`. Si vous avez installé un module de langue, vous devez aussi sauvegarder tous les autres fichiers du module de langue que vous prévoyez de modifier, notamment le fichier `SelfServiceScreenText_en.properties`. `SelfServiceScreenText.properties` est le fichier par défaut utilisé si aucune autre langue correspondante n'est trouvée.
2. Editez les fichiers de propriétés. Modifiez les valeurs des zones de texte d'écran et enregistrez les fichiers. Notez que les modifications que vous apportez au fichier `SelfServiceScreenText.properties` doivent aussi être apportées au fichier `SelfServiceScreenText_en.properties` pour préserver la cohérence.
3. Redémarrez l'application IBM Security Identity Manager pour que les modifications prennent effet.

Personnalisation de la présentation du site Web

Vous pouvez modifier la présentation de l'interface utilisateur en libre-service en effectuant des opérations de personnalisation.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Les éléments de présentation de haut niveau peuvent être activés et désactivés dans l'affichage de l'interface utilisateur en libre-service à l'aide de paramètres figurant dans le fichier `SelfServiceUI.properties`. La présentation par défaut contient une bannière, une barre d'outils et un pied de page.

L'activation et la désactivation d'éléments de page peuvent offrir diverses options de présentation. Le seul élément de page nécessaire est l'élément de contenu, qui comprend les tâches et les pages de tâches.

Pour afficher ou masquer un élément de page, modifiez la propriété ui.layout.show*nom* dans le fichier `SelfServiceUI.properties`. Par exemple, ui.layout.showBanner commande l'affichage de la section de la bannière. Lorsqu'une propriété a la valeur true, l'élément est inclus dans la page. Si la valeur false est définie, l'élément n'est pas inclus dans la page.

Toute modification du fichier `SelfServiceUI.properties` nécessite un redémarrage de l'application IBM Security Identity Manager dans WebSphere pour que la modification prenne effet.

Les figures suivantes affichent une représentation visuelle des différents éléments et options de présentation.

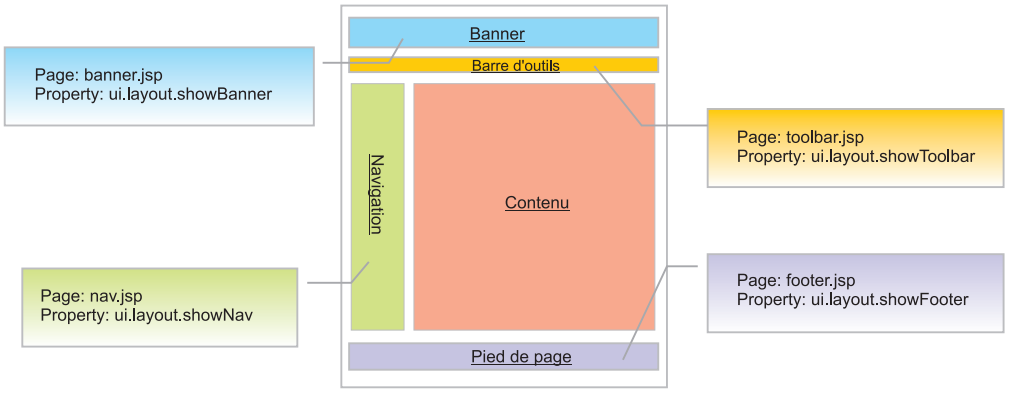


Figure 5. Eléments de présentation

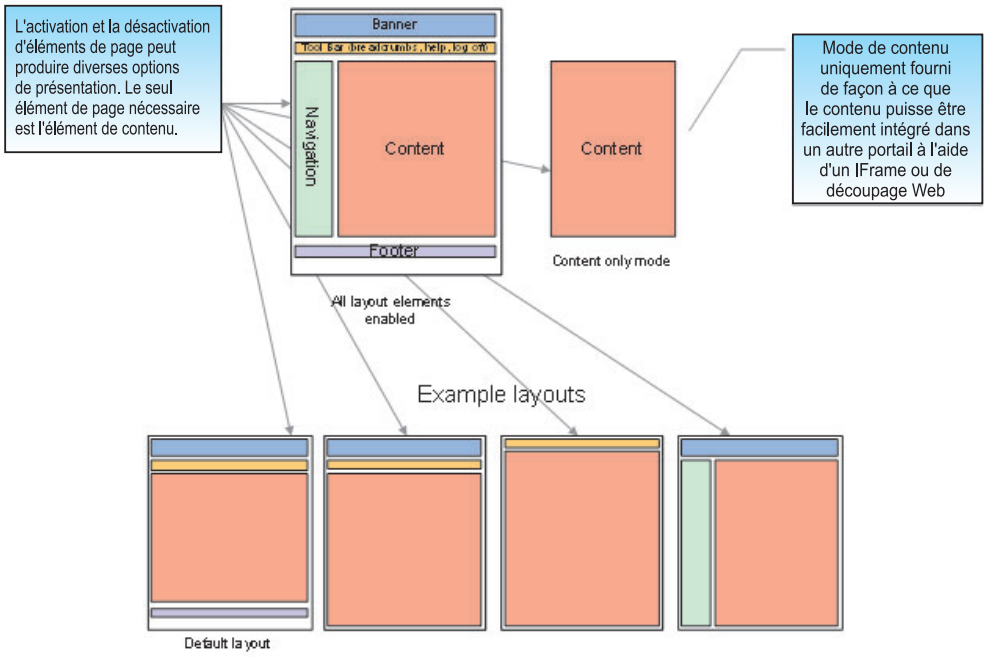


Figure 6. Options de présentation

La table suivante affiche la liste des propriétés et de leurs caractéristiques.

Tableau 4. Propriétés de présentation et leurs caractéristiques

Propriété	Description
ui.layout.showBanner	Commande la section de la bannière. La bannière par défaut contient IBM et des images du produit.
ui.layout.showFooter	Commande la section du pied de page. Le pied de page par défaut contient la mention de droit d'auteur du produit.
ui.layout.showToolbar	Commande la section de la barre d'outils. La barre d'outils par défaut contient le message de bienvenue, le lien d'aide, le lien de fermeture de session et les éléments de navigation.
ui.layout.showNav	Commande la barre de navigation. **Remarque :** Aucun contenu par défaut n'est inclus pour la barre de navigation.

Pour personnaliser la présentation, exécutez les étapes suivantes :

Procédure

1. Effectuez une copie de sauvegarde du fichier `SelfServiceUI.properties` se trouvant dans le répertoire *ITIM_HOME*`\data`.
2. Editez le fichier `SelfServiceUI.properties`. Modifiez les valeurs des zones de texte d'écran et enregistrez le fichier.
3. Redémarrez l'application IBM Security Identity Manager pour que les modifications prennent effet.

Personnalisation du contenu des bannières, pieds de page, barres d'outils et barres de navigation

Vous pouvez modifier la présentation de l'interface utilisateur en libre-service en personnalisant la bannière, le pied de page, la barre d'outils et la barre de navigation.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Le contenu du répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_self_service.war\custom peut être remplacé ou modifié pour ajuster la présentation de l'interface utilisateur en libre-service. Vous pouvez remplacer ou modifier la bannière, le pied de page, la barre d'outils et la barre de navigation.

Les éléments de présentation sont des fragments JavaServer Pages qui sont inclus dans la présentation de la page Web lorsque JavaServer Pages est affiché.

Le tableau suivant affiche une liste d'éléments de présentation et des fichiers correspondants se trouvant dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_self_service.war\custom.

Tableau 5. Eléments de présentation et noms de fichier

Elément de présentation	Nom de fichier
Bannière	banner.jsp
Pied de page	footer.jsp
Barre d'outils	toolbar.jsp
Barre de navigation	nav.jsp

Pour modifier ces fichiers, exécutez les étapes suivantes :

Procédure

1. Effectuez des copies de sauvegarde des fichiers et stockez les fichiers que vous voulez modifier dans un répertoire temporaire.
2. Editez les fichiers dans le répertoire temporaire et copiez les fichiers mis à jour de nouveau dans le répertoire WebSphere déployé. Aucun redémarrage de l'application IBM Security Identity Manager n'est nécessaire pour que ces modifications prennent effet.

Que faire ensuite

La version par défaut de ces fichiers est fournie avec l'archive du produit. N'oubliez pas de sauvegarder la version personnalisée des fichiers que vous avez créée de façon à ce que vos modifications ne soient pas perdues.

Paramètres de demande et exemples de contenu à utiliser pour personnaliser le contenu de l'interface utilisateur

Cette section décrit les paramètres de demande que vous pouvez utiliser dans les fichiers JavaServer Pages pour personnaliser le contenu.

Valeurs des paramètres de demande

Pour prendre en charge les contenus dynamiques tels que les éléments de navigation, les liens d'aide et les ID utilisateur, certains paramètres de demande sont disponibles. La table suivante affiche ces propriétés, leurs valeurs possibles et leur description.

Tableau 6. Paramètres, valeurs et descriptions de demande

Nom de propriété	Valeur	Description
loggedIn	vrai ou faux	Indicateur qui précise si l'utilisateur est actuellement connecté.
usercn	Nom usuel du propriétaire du compte connecté	**Remarque :** Cette valeur est uniquement définie si l'utilisateur est connecté.
langOrientation	ltr ou rtl	Indique le sens d'écriture de la langue de l'environnement local en cours, de gauche à droite ou de droite à gauche.
helpUrl	/itim/self/Help.do?helpId=*url_d_exemple*	URL vers la page Web d'aide avec le paramètre *helpId* défini sur la page en cours.
helpLink	Exemple : home_help_url	*helpId* pour la page en cours. La valeur *home_help_url* est mappée à la clé correspondante dans le fichier SelfServiceHelp.properties.
éléments de navigation	*clé_message_exemple1* *clé_message_exemple2* *clé_message_exemple3*	Liste de clés de message correspondant aux entrées du fichier SelfServiceScreenText.properties.
breadcrumbLinks	*chemin1* *chemin2* *chaîne_vide*	Liste de liens de la même longueur que la liste des éléments de navigation.

Exemples de paramètres de demande dans toolbar.jsp

Le fichier par défaut « toolbar.jsp » contient la logique pour afficher le message de bienvenue et les liens d'aide. Cette logique peut être déplacée vers d'autres éléments de présentation. Par exemple, le message de bienvenue peut être fourni dans la bannière.

Affichage du message de bienvenue

Le code ci-dessous examine si le nom usuel de l'utilisateur est défini. Si oui, il convertit le message de bienvenue et remplace le nom dans le message.

Remarque : Les libellés et clés du message de l'interface utilisateur en libre-service sont définis dans le fichier SelfServiceScreenText.properties.

```
<%-- If the Users Common Name is not empty display it. Note this value is not
     set until the user is logged in --%>

<c:if test="${!empty usercn and loggedIn == true}">
    <%--Translate the Welcome, Common Name message passing in the name --%>
    <fmt:message key="toolbar_username" >
        <fmt:param><c:out value="${usercn}"/></fmt:param>
    </fmt:message>
</c:if>
</div>
<%-- end user info -- %>
```

Affichage des liens d'aide

Le code suivant ajoute le lien d'aide à la page. helpUrl est extrait des attributs d'aide et le libellé d'aide est converti pour l'affichage.

```
<%-- Add Help Link to the page --%>

<a id="helpLink" href="javascript:launchHelp('<c:out value='${helpUrl}')">
      <fmt:message key="toolbar_help"/></a>
```

Prise en charge de la fermeture de session

Le lien de fermeture de session ne doit être affiché que si l'utilisateur est actuellement connecté. Le code suivant effectue un test afin de vérifier si le paramètre de demande loggedIn a la valeur true. Le cas échéant, le code convertit le libellé pour le lien de fermeture de session et inclut le lien dans la page.

```
<%-- If the user is logged in display the logoff link --%>
<c:if test="${loggedIn == true}">
   <a id="logofflink" href="/itim/self/Login/Logoff.do">
       <fmt:message key="toolbar_logoff"/></a>
</c:if>
```

Affichage des éléments de navigation

Le code suivant ajoute les éléments de navigation à la page. L'attribut des éléments de navigation contient la liste des clés de libellé pour les éléments de navigation. breadcrumbLinks contient les informations d'adresse URL pour chaque libellé d'élément de navigation. Une valeur "null" ou vide pour breadcrumbLinks indique que l'élément de navigation n'est pas liable.

```
<%-- If the breadcrumbs label keys are not empty then display --%>

<c:if test="${!empty breadcrumbs}">
    <c:forEach items="${breadcrumbs}" var="breadcrumb" varStatus="status">

        <c:if test="${status.index > 0}">
            &amp;nbsp;&amp;gt;&amp;nbsp;
        </c:if>

        <c:choose>
            <%-- If the action link is not empty for the current label then
                 create a link for the breadcrumb --%>

           <c:when test="${!empty breadcrumbLinks{status.index}}">
               <html:link action="${breadcrumbLinks{status.index}}">
               <fmt:message key="${breadcrumb}"/></html:link>
           </c:when>
           <%-- If the action link is empty then just translate the
                label for the breadcrumb --%>
           <c:otherwise>
               <fmt:message key="${breadcrumb}"/>
           </c:otherwise>
```

```
        <c:choose>

    </c:forEach>

</c:if>
```

Personnalisation de la page d'accueil en libre-service

Vous pouvez changer la page d'accueil de l'interface utilisateur en libre-service via la personnalisation.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

La page d'accueil renvoie à la page principale qui est chargée dans l'élément de présentation du contenu lorsqu'un utilisateur se connecte à l'interface utilisateur en libre-service.

Les définitions de section et de tâche combinent les vues définies en tâches et groupent les tâches en sections, également appelées pages de tâches. Cette section et ces définitions de tâches sont définies dans le fichier `SelfServiceHomePage.properties` figurant dans le répertoire *ITIM_HOME*`\data`.

L'élément de la mise en page de la page d'accueil est un fragment JavaServer Pages qui est inclus dans la présentation de la page Web. Ces informations de présentation sont stockées dans le fichier `Home.jsp` dans le répertoire *WAS_PROFILE_HOME*`\installedApps\`*nom_noeud*`\ITIM.ear\itim_self_service.war\custom`.

Vous pouvez ajouter des tâches et des sections à la page d'accueil en mettant à jour le fichier `SelfServiceHomePage.properties`. Les commentaires dans le fichier explicitent le format de fichier. Cela vous permet de modifier le contenu sans modifier le fichier jsp.

Pour personnaliser la page d'accueil, exécutez les étapes suivantes :

Procédure

1. Effectuez une copie de sauvegarde du fichier `SelfServiceHomePage.properties` se trouvant dans le répertoire *ITIM_HOME*`\data`.
2. Effectuez une copie de sauvegarde du fichier `Home.jsp` dans le répertoire *WAS_PROFILE_HOME*`\installedApps\`*nom_noeud*`\ITIM.ear\itim_self_service.war\custom`.
3. Editez le fichier `SelfServiceHomePage.properties`. Modifiez les valeurs et enregistrez le fichier.
4. Copiez le fichier `Home.jsp` dans un autre répertoire, puis modifiez le fichier dans ce répertoire et copiez de nouveau le fichier mis à jour dans le répertoire *WAS_PROFILE_HOME*`\installedApps\`*nom_noeud*`\ITIM.ear\itim_self_service.war\custom`. La version par défaut de ces fichiers est fournie avec l'archive du produit. Veillez à sauvegarder la version personnalisée des fichiers que vous avez créée afin que vos personnalisations ne soient pas perdues.

5. Redémarrez l'application IBM Security Identity Manager dans WebSphere pour que les modifications prennent effet.

Paramètres de demande et exemples de contenu à utiliser pour personnaliser le contenu de la page d'accueil

Cette section décrit les paramètres de demande que vous pouvez utiliser dans les fichiers JavaServer Pages pour personnaliser le contenu de la page d'accueil.

Paramètres du formulaire de la page d'accueil

Pour prendre en charge le contenu dynamique de la page d'accueil, tel que les sections, les sections nécessitant une action, les tâches, un bean Java est disponible en tant que paramètre de demande appelé **HomePageForm**. Le bean Java de la page d'accueil contient quelques méthodes pouvant être utilisées pour accéder à des informations sur les sections et les tâches

Tableau 7. Paramètres, valeurs et descriptions de demande de la page d'accueil

Nom de propriété	Valeur	Description
sections	Liste des beans Java de la section	Liste des sections que l'utilisateur en cours peut afficher.
sectionToTaskMap	Correspondance entre les sections et leurs tâches	Mappe reliant une section de bean Java donnée à un bean Java de tâche.
actionNeededSection	Bean Java de section ou nul	Un bean Java de section contenant les actions en attente pour l'utilisateur en cours. Une valeur null est utilisée s'il n'y a pas d'action en attente pour l'utilisateur en cours.

Les propriétés suivantes sont disponibles pour le bean Java de section :

Tableau 8. Paramètres, valeurs et descriptions de demande de bean Java de section

Nom de propriété	Valeur	Description
titleKey	Clé de message de titre pour la section	Clé de message pour le titre de section.
iconUrl	URL d'icône ou null	Chemin de l'URL pour l'icône à utiliser avec cette section. La valeur null est utilisée pour indiquer qu'aucune icône n'est utilisée.
iconAltTextKey	Clé du texte	Clé de texte à utiliser comme autre texte pour l'icône de cette section.
tasks	Liste des beans Java de tâche	Liste des tâches pouvant être affichées dans cette section

Les propriétés suivantes sont disponibles pour le bean Java de tâche :

Tableau 9. Paramètres, valeurs et descriptions de la demande de bean Java de tâche

Nom de propriété	Valeur	Description
urlPath	URL	Chemin URL vers cette tâche.
urlKey	Clé du texte	Clé de texte à utiliser avec le lien vers cette tâche.
descriptionKey	Clé du texte	Clé de texte à utiliser comme description de cette tâche.

Exemples de paramètres de demande dans home.jsp

Le code suivant obtient le bean **Java** HomePageForm et itère à travers les sections et tâches disponibles pour créer des liens vers chaque tâche disponible.

```
<c:set var="pageConfig" value="${HomePageForm}" scope="page" />
<c:forEach items="${pageConfig.sections}" var="section">
      <%-- Process each section here --%>
      <c:forEach items="${pageConfig.sectionToTaskMap[section]}" var="task">
      <%-- Process each section here --%>
            <a href="/itim/self/<c:out value="${task.urlPath}"/>"
               title="<fmt:message key="${task.urlKey}" />">
               <fmt:message key="${task.urlKey}" />
            </a>
            <fmt:message key="${task.descriptionKey}" />
      </c:forEach>
</c:forEach>
```

Personnalisation des feuilles de style

Vous pouvez modifier la présentation de l'interface utilisateur en libre-service en personnalisant des feuilles de style en cascade (CSS).

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Les feuilles de style en cascade (CSS) sont utilisées pour définir des styles de présentation de l'interface utilisateur en libre-service. Vous pouvez éditer les feuilles de style pour modifier les polices de caractères, les couleurs et les autres styles associés à l'interface utilisateur en libre-service. Cette section décrit l'emplacement des feuilles de style et des styles de clé afin de personnaliser l'interface utilisateur en fonction de l'aspect de votre site Web.

Les fichiers CSS déployés par défaut sont compressés et optimisés en tenant compte de la bande passante dans l'intérêt de l'évolutivité. Les versions non optimisées (avec blancs/formatage intacts) figurent dans le répertoire *ITIM_HOME*\defaults\custom. Les fichiers CSS stockés dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_self_service.war\custom ne conviennent pas pour l'édition. Copiez les fichiers par défaut du répertoire *ITIM_HOME*\defaults\custom dans un autre répertoire. Editez les

feuilles de style puis copiez les fichiers modifiés dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_self_service.war\custom.

Le tableau suivant affiche les fichiers CSS qui peuvent être modifiés pour ajuster l'interface utilisateur en libre-service.

Tableau 10. Noms de fichier des feuilles de style en cascade

Nom de fichier CSS	Description
end_user.css	Fichier CSS contenant les styles CSS principaux pour l'orientation d'une langue de gauche à droite.
end_user_rtl.css	Fichier CSS contenant les styles CSS principaux pour l'orientation d'une langue de droite à gauche.
widgets.css	Fichier CSS contenant les styles utilisés pour les objets fenêtre, tels ceux figurant dans les formulaires de profil, de compte et de demande d'informations, pour l'orientation d'une langue de gauche à droite. **Remarque :** L'édition de ce fichier exige une maîtrise des feuilles de style en cascade plus poussée.
widgets_rtl.css	Fichier CSS contenant les styles utilisés pour les objets fenêtre, tels ceux figurant dans les formulaires de profil, de compte et de demande d'informations, pour l'orientation d'une langue de droite à gauche. **Remarque :** L'édition de ce fichier exige une maîtrise des feuilles de style en cascade plus poussée.
dateWidget_ltr.css	Fichier CSS contenant les styles utilisés pour les objets fenêtre de date, tels ceux figurant dans les formulaires de profil, de compte et de demande d'informations, pour l'orientation d'une langue de gauche à droite. **Remarque :** L'édition de ce fichier exige une maîtrise des feuilles de style en cascade plus poussée.
dateWidget_rtl.css	Fichier CSS contenant les styles utilisés pour les objets fenêtre de date, tels ceux figurant dans les formulaires de profil, de compte et de demande d'informations, pour l'orientation d'une langue de droite à gauche. **Remarque :** L'édition de ce fichier exige une maîtrise des feuilles de style en cascade plus poussée.
time.css	Fichier CSS contenant les styles utilisés avec les objets fenêtre d'heure, tels ceux figurant dans les formulaires de profil, de compte et de demande d'informations. **Remarque :** L'édition de ce fichier exige une maîtrise des feuilles de style en cascade plus poussée.

Tableau 10. Noms de fichier des feuilles de style en cascade (suite)

Nom de fichier CSS	Description
customForm.css	Fichier CSS contenant les styles utilisés avec les formulaires de présentation, tels ceux figurant dans les formulaires de profil, de compte et de demande d'informations, pour l'orientation d'une langue de gauche à droite. **Remarque :** L'édition de ce fichier exige une maîtrise des feuilles de style en cascade plus poussée.
customForms_rtl.css	Fichier CSS contenant les styles utilisés avec les formulaires de présentation, tels ceux figurant dans les formulaires de profil, de compte et de demande d'informations, pour l'orientation d'une langue de droite à gauche. **Remarque :** L'édition de ce fichier exige une maîtrise des feuilles de style en cascade plus poussée.

Les figures suivantes fournissent une représentation visuelle des éléments de page pour lesquels des modifications de style peuvent être appliquées.

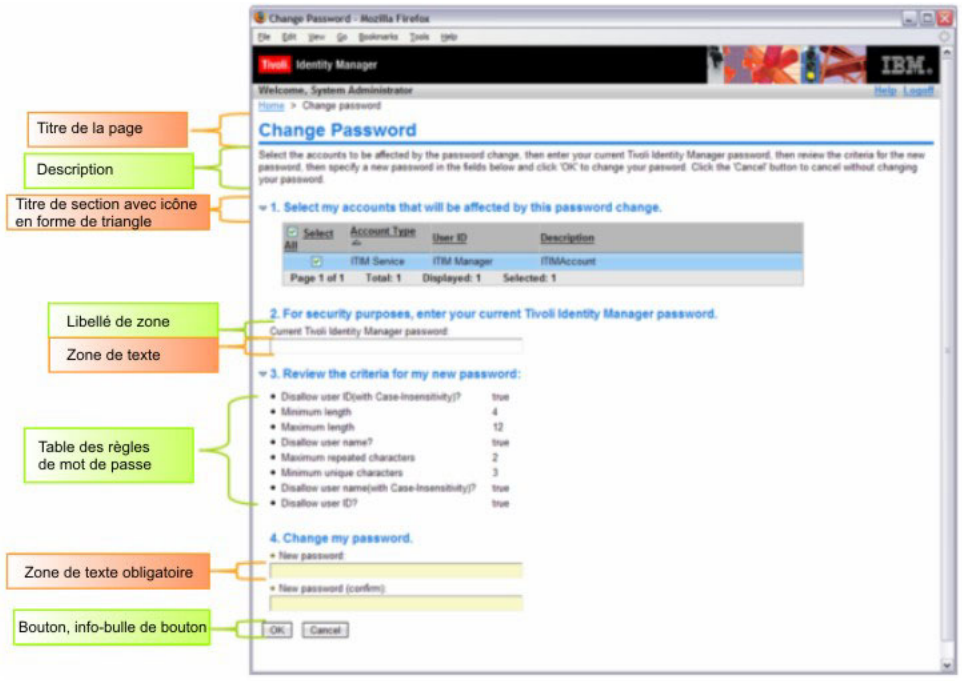


Figure 7. Eléments de page pour les modifications de style

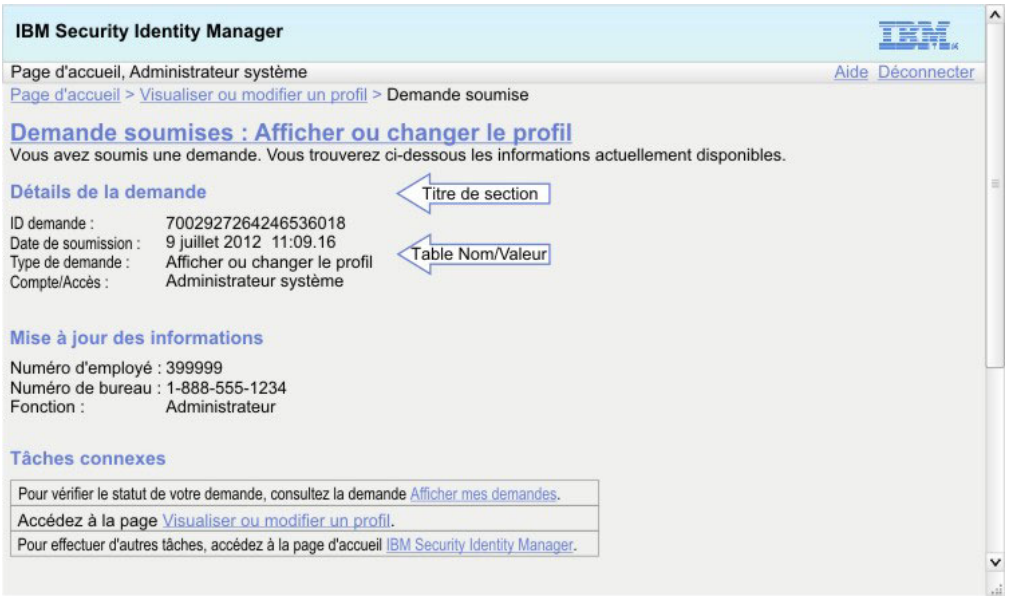


Figure 8. Eléments de page pour les modifications de style (suite)

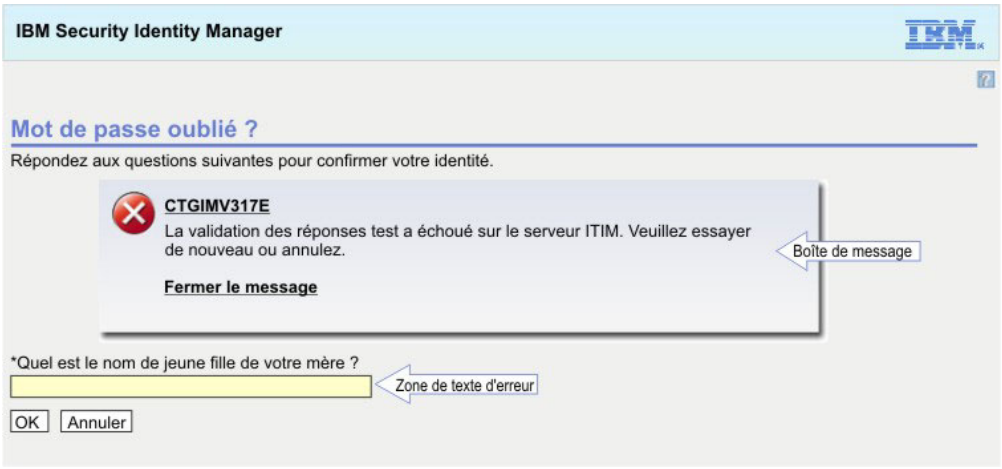


Figure 9. Eléments de page pour les modifications de style

Le tableau suivant fournit une référence des principaux styles CSS.

Tableau 11. Référence des styles CSS

Elément	Exemple	Sélecteur de style principal	Description
Titre de la page	**Titre de la page**	Sélecteur de type : h1	Elément utilisé avec tous les titres de page.
Titre de section	**Titre de sous-section**	Sélecteur de type : h2	Titres de section pour les pages ne contenant pas d'icône en forme de triangle.

Tableau 11. Référence des styles CSS (suite)

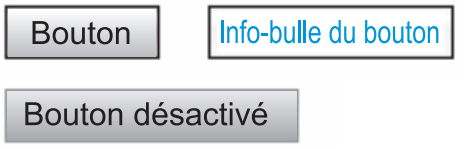
Elément	Exemple	Sélecteur de style principal	Description
Titre de section (icône en forme de triangle)	**Titre d'icône en forme de triangle**	Sélecteur de type : h3	Titres de section sur les pages contenant des sections avec l'icône en forme de triangle. Les titres sont conçus pour laisser de l'espace pour l'image de l'icône en forme de triangle.
Eléments de navigation	Accueil > Visualiser ou modifier un profil	Sélecteur de type : #breadcrumbs	Trajet de navigation des éléments de navigation affichés en haut à gauche au-dessus du titre de la page.
Bouton, info-bulle de bouton, bouton désactivé		Sélecteurs de classe : • .button • .button_hover • .button_disabled	Ces styles de bouton couvrent la majorité des boutons dans l'interface utilisateur. Le style d'info-bulle est utilisé lorsqu'une souris survole le bouton
Bouton en ligne, info-bulle du bouton en ligne		Sélecteurs de classe : • .button_inline • .button_inline_hover	Utilisé pour un sous-ensemble de boutons avec des exigences de présentation spéciales.
Descriptions de page/section	Ceci est une description.	Sélecteur de classe : .description	Descriptions de page et de section. La description figure dans un bloc . Vous pourriez donc ajouter des bordures, des couleurs etc. si vous le souhaitez.
Libellés de zone	Libellé de zone	Sélecteur de type : label	Libellés de zone dans les formulaires.
Zone de texte	Zone de texte (arrière-plan de zone blanc par défaut)	Sélecteur de classe : input.textField_std	Zones de texte standard.
Zone de texte obligatoire	Zone de texte obligatoire (arrière-plan de zone jaune par défaut)	Sélecteur de classe : input.textField_required	Zones de texte obligatoires.
Zone de texte d'erreur	Zone de texte d'erreur (bordure de zone rouge par défaut)	Sélecteur de classe : input.textField_error	Zones de texte en état d'erreur.

Tableau 11. Référence des styles CSS (suite)

Elément	Exemple	Sélecteur de style principal	Description
Zone de texte d'avertissement	Zone de texte d'avertissement (bordure de zone jaune par défaut)	Sélecteur de classe : input.textField_warning	Zones de texte en état d'avertissement.
Tables de zones/valeurs	Field Name1 Field value1 Field Name2 Field value2 Multi-valued Field3 Item 1 Item 2 Item 3 Item 4 Multi-valued Field3 Item 1 Item 2	Sélecteur de classe : table.nameValueTable	Les tables de valeurs de zone sont utilisées dans toute l'interface utilisateur pour afficher un nom de zone et une ou plusieurs valeurs correspondantes. Par exemple, la section Information des pages de demande soumise utilise les tables de valeurs de nom. Le sélecteur est affiché pour la table. Il existe d'autres sélecteurs définissant le style des lignes, des cellules, des listes à valeurs multiples et des colonnes de nom pour cette table.
Table des règles de mot de passe	◆ Règle1 Valeur1 AccountInfo1 ◆ Règle2 Valeur2 AccountInfo2	Sélecteurs de classe : • .pwRulesTable • .pwRulesTable .ruleCol • .pwRulesTable .valueCol • .pwRulesTable .accountInfoCol • .button_inline_hover	La table de règles du mot de passe est utilisée pour définir le style des sections de règles d'administration des mots de passe dans toute l'interface utilisateur. La table se compose de trois colonnes : une colonne de règles, une colonne de valeurs et une colonne d'informations de compte.

Tableau 11. Référence des styles CSS (suite)

Elément	Exemple	Sélecteur de style principal	Description
Boîte de message		div.messageBoxComposite	La boîte de message composite est le sélecteur de feuille de style en cascade principal pour la boîte de message. D'autres sélecteurs permettent de définir la présentation de l'image / du lien / et du message.

Pour personnaliser les feuilles de style, exécutez les étapes suivantes :

Procédure

1. Effectuez une copie de sauvegarde des fichiers CSS dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_self_service.war\custom.
2. Copiez les fichiers CSS du répertoire *ITIM_HOME*\defaults\custom vers un autre répertoire, puis modifiez les fichiers dans ce répertoire et copiez les fichiers mis à jour dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_self_service.war\custom. Veillez à sauvegarder la version personnalisée des fichiers que vous avez créée afin que vos personnalisations ne soient pas perdues.

Fusion des personnalisations de feuille de style d'une version précédente

Après la mise à niveau à partir d'une version précédente d'IBM Tivoli Identity Manager, vous devez appliquer à nouveau les personnalisations apportées à la feuille de style en cascade pour l'interface utilisateur en libre-service.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vous devez avoir accès au système de fichiers sur lequel est déployé Tivoli Identity Manager.

Vous devez maîtriser IBM Security Identity Manager et les feuilles de style en cascade.

Pourquoi et quand exécuter cette tâche

Les personnalisations (y compris les définitions de vues) définies à l'aide de la console d'administration sont conservées lors de la mise à niveau. Les mises à jour apportées à SelfServiceScreenText.properties sont automatiquement fusionnées.

Cependant, une fois le programme de mise à niveau terminé, la feuille de style en cascade (CSS) en libre-service déployée est restaurée selon ses paramètres d'usine. Fusionnez tout d'abord les valeurs CSS mises à jour dans votre habillage CSS personnalisé pour la version précédente du produit. Appliquez ensuite à nouveau vos fichiers personnalisés au fichier War en libre-service déployé.

Remarque : Lors de la mise à niveau, le fichier `ITIM.ear` est sauvegardé à partir du serveur WebSphere Application Server dans le répertoire *ISIM_HOME*`/data/backup/ITIM.ear`. Vous pouvez consulter le répertoire `itim_self_service.war/custom` pour obtenir une copie de l'habillage CSS déployé avant la mise à niveau.

Pour fusionner des personnalisations CSS, effectuez les modifications et ajouts suivants dans vos fichiers CSS IBM Tivoli Identity Manager d'origine.

Remarque : Si des modifications concernant les fichiers CCS des langues s'écrivant de droite à gauche (`enduser_rtl.css`, par exemple) ont été effectuées, fusionnez les modifications en utilisant un outil de comparaison de texte. Appliquez au fichier `enduser_rtl.css` les modifications correspondantes apportées au fichier `enduser.css`, mais en prenant en compte la présentation de droite à gauche.

Procédure

1. Ouvrez le fichier CSS existant dans un éditeur.

   Ce fichier figure dans le répertoire `ITIM_HOME/data/backup/ITIM.ear`.

   Remarque : Pour une mise à niveau du système pris séparément, copiez les fichiers du fichier ITIM.ear déployé.
2. Ajoutez les modifications appropriées en fonction du chemin de migration. Voir «Mises à jour CSS».

   Pour la migration de la version 5.0 à la version 5.1

   Pour la migration de la version 5.1 vers la version 6.0, ajoutez les modifications CSS effectuées dans la version 6.0 uniquement.
3. Copiez les fichiers CSS mis à jour dans le répertoire personnalisé d'interface utilisateur en libre-service `itim_self_service.war/custom`.

Résultats

Ces modifications prennent effet immédiatement, sans qu'un redémarrage de l'application IBM Security Identity Manager ne soit nécessaire.

Mises à jour CSS

Modifications CSS effectuées dans la version 5.1 :

enduser.css

Description : Ajout du triangle pour les titres H2.

Ajoutez le texte suivant :

```
a.twistie_open h2{
 margin-left:0px;
 background-repeat: no-repeat;
 background-position: left;
 padding-left: 15px;
 background-image: url("/itim/self/images/twistie_open.gif");
}

a.twistie_closed h2{
```

```
 margin-left:0px;
 background-repeat: no-repeat;
 background-position: left;
 padding-left: 15px;
 background-image: url("/itim/self/images/twistie_closed.gif");
}
```

Description : Les instructions de révision sont désormais affichées via un triangle permettant de développer des sections.

Ajoutez le texte suivant :

```
/* Review Activity Styles */
#instructionDetailTwistieDiv {
 white-space: expression("pre"); /* IE */
 white-space: -moz-pre-wrap; /* Firefox */
 word-wrap: break-word;
}
/* End Review Activity Styles */
```

Description : Ajout de styles CSS pour la recertification des utilisateurs.

Ajoutez le texte suivant :

```
/* Recertification items table styles */
table.recertItemsTable {
 width: auto;
}

table.recertItemsTable th {
 padding: .2em 1em .2em 1em;
 background-color: #C0C0C0;
 white-space: nowrap;
 text-align: left;
}

table.recertItemsTable td {
 padding: .2em 1em .2em 1em;
 border: 1px solid #C0C0C0;
}

table.recertItemsTable tr.recertItemRow td {
 border-bottom-style: none;
}

table.recertItemsTable tr.recertSubItemRow td {
 border-top-style: none;
 border-bottom-style: none;
}

table.recertItemsTable tr.altRow {
 background-color: #F6F6F6;
}

table.recertItemsTable .selectAllOptions {
 display: inline;
 padding: 0 .5em 0 .5em;
 font-weight: normal;
}

table.recertItemsTable .selectAllOptions a {
 padding: 0 .3em 0 .3em;
 color:#1375D7;
 font-weight: normal;
}

table.recertItemsTable .recertItemSelectAllOptions {
```

```
 display: inline;
 padding: 0 .5em 0 .5em;
 font-weight: normal;
 font-size: .8em;
}

table.recertItemsTable .recertItemSelectAllOptions a {
 padding: 0 .3em 0 .3em;
}

table.recertItemsTable a.recertExpandCollapseLink {
 margin-right: .2em;
}

table.recertItemsTable a.recertExpandCollapseLink img {
 border: none;
 vertical-align: bottom;
}

table.recertItemsTable div.recertItem {
 display: inline;
 margin-bottom: 2px;
}

table.recertItemsTable td.recertItemImpact {
 text-align: center;
}

table.recertItemsTable div.recertItemDescription {
 max-width: 300px;
 font-size: .8em;
}

table.recertItemsTable div.recertItemImpactedBy {
 display: inline;
 margin-bottom: 2px;
}

table.recertItemsTable td.recertItemActionRecertify {
 width: expression("0%"); /* IE */
 width: 1px; /* Firefox */
 white-space: nowrap;
 padding-right: 0;
 border-right: none;
}

table.recertItemsTable td.recertItemActionRecertifyErrorNone {
 width: expression("0%"); /* IE */
 width: 1px; /* Firefox */
 white-space: nowrap;
 padding: .2em 0 .2em 13px;
 border-right: none;
}

table.recertItemsTable td.recertItemActionRecertifyErrorExists {
 width: expression("0%"); /* IE */
 width: 1px; /* Firefox */
 white-space: nowrap;
 padding: .2em 0 .2em 5px;
 border-right: none;
}

table.recertItemsTable td.recertItemActionReject {
 width: 0%;
 white-space: nowrap;
 padding-left: 0;
 border-left: none;
```

```
 border-right: none;
}

table.recertItemsTable td.recertItemActionBlank {
 height: 24px;
}

table.recertItemsTable label.recertItemAction {
 display: inline;
}

table.recertItemsTable td.recertItemSelectAll {
 width: 0%;
 white-space: nowrap;
 padding-left: 0;
 border-left: none;
}

table.recertItemsTable .recertSubItem {
    font-size: 1em;
    margin: 0 0 0 1em;
}

table.recertItemsTable div.recertItemDecision {
 display: block;
 margin-bottom: 2px;
 margin-top: 5px;
}
/* Fin des styles du tableau de recertification */

.simpleLink:link, .simpleLink:visited {
 font-weight: normal;
}


.requiredInstruction {
 font-size: .8em;
 margin: 1em 0 0 1em;
 background-image: url("/itim/self/images/required_field.gif");
 background-repeat: no-repeat;
 background-position: center left;
 padding-left: 12px;
}
```

Modifications CSS ajoutées dans la version 6.0 :

enduser_extra.css

Importez enduser_extra.css

Ajoutez le texte suivant :

```
@import "enduser_extra.css";
```

Description : la couleur d'arrière-plan de la console automatique devient blanc grisé.

Ajoutez le style suivant dans le sélecteur de balise de corps

```
background-color: #F5F5F5;
```

Description : la couleur d'arrière-plan de la bannière devient bleu clair.

Mettez à jour le style suivant dans le sélecteur d'ID de bannière :

```
background-color: black;
```

to

```
background-color: #c8e0f8;
```

Description : diverses modifications dans l'écran de connexion.

Mettez à jour le sélecteur d'ID loginContainer en utilisant le style suivant :

```
#loginContainer{
  width:619px;
  margin:20px auto;
  margin-left: auto ;
  margin-right: auto ;
    background-position:left top;
   background-repeat: no-repeat;
  background-color:#FFF;
  padding:0;
  border: solid 1px #bbbbbb;
  font-family:Arial,Verdana,Helvetica,Tahoma,sans-serif;
  font-size:12px;
  color:#555555;
  overflow:hidden;
  text-align: left;
  }
```

Description : modifications de la présentation pour l'image de connexion du produit

Ajoutez le style suivant dans le sélecteur d'ID loginImage :

```
margin-left: 40px;
margin-top: -30px;
```

Description : modifications de la présentation et modifications de taille de police pour la version du produit

Mettez à jour le sélecteur d'ID loginVersion :

```
margin-left: 110px;
font-size:10px;
```

Description : modifications de la présentation et modifications de taille de police pour le contenu de la connexion

Mettez à jour le contenu dans le sélecteur d'ID loginContent

```
margin-left: 40px ;
margin-right: 20px ;
font-size:14px;
```

Description : style pour le nouveau lien d'aide dans l'écran de connexion

Ajoutez le style suivant :

```
#loginToolbar {
  margin-right: 20px ;
  }
```

Description : style pour la boîte de message

Ajoutez le style suivant :

```
#messageBox {
  margin-right:80px;
  font-size:14px;
  }
```

Description : ajoutez un sélecteur de balise supplémentaire h2i à la zone de déclaration de sélecteur de groupe existant pour h1, h2, h3. Ajoutez également le style correspondant pour le sélecteur de balise h2i.

Ajoutez le style suivant :

```
h2i {
  font-size:120%;
  border-bottom-style: none;
  border-bottom-width: 2px;
  margin-bottom: 0px;
  margin-left: 15px;
  }
```

Description : curseur sous forme de main ajouté pour l'ancre.

Ajoutez le style suivant dans la pseudo-classe a:LINK, a:VISITED:

```
cursor: hand;
```

Description : nouvelle classe **descriptioni** ajoutée.

Ajoutez le style suivant :

```
.descriptioni {
  display: block;
    margin-bottom: 20px;
  margin-left: 15px;
  }
```

Description : nouveau style ajouté pour les tables.

Ajoutez le style suivant :

```
span.tableLayout {
  display:inline-block;
  min-width:80%;
  margin : 10px 10px 10px 0 ;
  }
```

Description : largeur mise à jour pour l'en-tête de colonne de table.

Ajoutez le style suivant dans le sélecteur **thead th** :

```
width: auto;
```

Description : nouvelle classe dataTable ajoutée

Ajoutez le style suivant :

```
.dataTable {
  width:100%;
  margin: 0px;
  }
```

Description : nouvelle classe customHeader ajoutée

Ajoutez le style suivant :

```
customHeader {
  text-align: left;
  border-style: solid;
  background-color: #E6E6E6;
```

```
   border-width:1px 1px 1px 1px;
  border-color:#C8C8C8 #C8C8C8 #737373 #C8C8C8;
  width: auto;
  }
```

Description : nouvelle classe customHeaderTable ajoutée

Ajoutez le style suivant :

```
.customHeaderTable {
  border-top-style:hidden;
  }
```

Description : largeur mise à jour des ancres dans l'en-tête de colonne

Ajoutez le style suivant dans le sélecteur **thead th a:LINK, thead th a:VISITED** :

```
width: auto;
```

Description : style ajouté pour les tables de compte

Ajoutez le style suivant :

```
table #global_table_accounttype {
   width: 20%;
  }

  table #global_table_userid_10 {
    width: 10%;
    }

  table #global_table_description_30 {
  width: 30%;
  }
```

Description : nouvelle classe viewRequestsCustomHeaderStyle ajoutée

Ajoutez le style suivant :

```
.viewRequestsCustomHeaderStyle{
  text-align: left;
  padding: 5px;
  vertical-align: middle;
  }
```

Description : style ajouté pour les libellés d'en-tête personnalisés

Ajoutez le style suivant :

```
div.viewRequestsCustomHeaderStyle label{
  display: inline;
  font-weight: bold;
  }
```

Description : nouveau style ajouté pour recertItemOwnershipType

Ajoutez le style suivant :

```
table.recertItemsTable div.recertItemOwnershipType {
   max-width: 300px;
  font-size: 1em;
  }
```

Description : styles ajoutés pour les cellules de table

Ajoutez le style suivant :

```
div.tableCellContent {
  white-space: nowrap;
  overflow:hidden;
  width:25em;
  text-overflow:ellipsis;"
  }
```

Ajoutez une classe de balise supplémentaire tfootTd à la zone de déclaration de sélecteur de groupe pour le sélecteur tfoot th. Ajoutez également un libellé de classe de balise supplémentaire à la zone de déclaration de sélecteur de groupe pour le sélecteur de libellé.

Description : styles suivants supprimés qui ne sont plus utilisés.

Supprimez les styles suivants :

```
th.reviewActivitiesCustomHeader {
  text-align: left;
  border-style: solid;
  border-width:1px 1px 1px 1px;
  background-color: #E6E6E6;
  border-color:#FFFFFF #C8C8C8 #737373 #FFFFFF;
  }

.simpleLink:link, .simpleLink:visited {
  font-weight: normal;
  }

  .label_accessibility {
   display: none;
  }

.requiredInstruction {
   font-size: .8em;
   margin: 1em 0 0 1em;
   background-image: url("/itim/self/images/required_field.gif");
   background-repeat: no-repeat;
   background-position: center left;
   padding-left: 12px;
  }
```

Que faire ensuite

Ces modifications prennent effet immédiatement. Le redémarrage de l'application IBM Security Identity Manager n'est pas nécessaire.

Réacheminement du contenu de l'aide

Vous pouvez réacheminer les demandes d'aide vers votre propre site Web pour fournir un contenu d'aide personnalisé.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

L'édition du contenu d'aide fourni avec l'interface utilisateur en libre-service n'est pas prise en charge. Il est cependant possible de réacheminer les demandes d'aide vers votre propre site Web pour fournir un contenu d'aide personnalisé adapté à la présentation de votre entreprise.

Le fichier `SelfServiceHelp.properties` indique l'URL de base à laquelle les demandes sont envoyées. Ces fichiers se trouvent dans le répertoire *ITIM_HOME*`\data`.

La table suivante affiche les propriétés et descriptions de propriété pour l'aide en libre-service.

Tableau 12. Propriétés et descriptions de l'aide en libre-service

Propriété	Description
helpBaseUrl	Indique l'URL de base vers laquelle envoyer les demandes d'aide. Une valeur vide indique que l'aide doit aller vers l'URL par défaut pour l'interface utilisateur en libre-service.
Help ID mappings: helpID = URL de page relative	La section des mappages d'aide mappe les ID de certaines pages à une adresse URL relative envoyée au serveur d'aide.

L'URL d'aide est la combinaison de helpBaseUrl + locale + relativeHelppageURL

Par exemple :

```
helpBaseUrl=http://myserver:80
locale = en_US
```

L'environnement local est déterminé en résolvant le regroupement de ressources SelfServiceScreenText.properties pour l'utilisateur actuellement connecté et en utilisant l'environnement local associé.

```
loginId/relativeURL = login_help_url=ui/ui_eui_login.html
```

Par conséquent, l'URL finale est http://myserver:80/en_US/ui/ui_eui_login.html.

Pour réacheminer l'aide, exécutez les étapes suivantes :

Procédure

1. Effectuez une copie de sauvegarde du fichier `SelfServiceHelp.properties` se trouvant dans le répertoire *ITIM_HOME*`\data`.
2. Modifiez la propriété helpBaseUrl dans le fichier `SelfServiceHelp.properties`.
3. Mettez à jour les mappages helpId pour utiliser les URL relatives pour votre serveur.
4. Ajoutez des pages à votre serveur pour les paramètres nationaux appropriés.
5. Redémarrez l'application IBM Security Identity Manager dans WebSphere pour que les modifications prennent effet.

Configuration de l'accès direct aux tâches en libre-service

Cette section décrit comment configurer l'accès direct par URL aux tâches de l'interface de libre-service.

De nombreuses pages de l'interface sont directement accessibles à partir d'autres pages HTML, ce qui facilite l'intégration avec un portail d'intranet de la société.

L'utilisateur doit tout d'abord s'authentifier en se connectant via la page Connexion ou via la connexion unique. Lorsqu'un utilisateur essaie d'accéder à une page pour laquelle l'accès direct est pris en charge, les événements suivants surviennent :

- Si la page à laquelle l'utilisateur tentait d'accéder est définie par une vue configurée par l'administrateur, cette page s'affiche.
- Si la page à laquelle un utilisateur essaie d'accéder n'est pas dans une vue configurée, une page d'erreur s'affiche au lieu de la page demandée.

Remarque : L'accès direct à la tâche **Approuver et consulter les demandes** est pris en charge même s'il n'est pas activé dans une vue configurée. De plus, en fonction de l'appartenance de groupe, plusieurs configurations de vue peuvent s'appliquer. Si au moins une configuration de vue qui s'applique à un utilisateur comporte la tâche à laquelle l'utilisateur tente d'accéder, la page s'affiche.

La table suivante affiche les tâches et les URL qui sont prises en charge pour l'accès direct et avec lesquelles vous pouvez établir une liaison à partir du portail d'intranet de votre société.

Tableau 13. URL et tâches à accès direct

Tâche	**URL**
Page d'ouverture de session	http://*nom_de_serveur*/itim/self
Modifier le mot de passe	http://*nom_de_serveur*/itim/self/PasswordChange.do
Modifier les informations pour les mots de passe oubliés	http://*nom_de_serveur*/itim/self/changeForgottenPasswordInformation.do
Mot de passe expiré (ignorer la page de connexion)	http://*nom_de_serveur*/itim/self/Login/DirectExpiredPasswordChange.do?expiredUserId=*userID* **Remarque :** Cette solution fonctionne uniquement si la connexion unique n'est pas activée et que la propriété ui.directExpiredChangePasswordEnabled a la valeur true dans le fichier SelfServiceUI.properties.
Demander un accès	http://*nom_de_serveur*/itim/self/RequestAccess.do
Demande d'accès (pour une demande d'accès spécifique)	http://*nom_de_serveur*/itim/self/RequestAccess.do?accessDN=*accessDN*
Afficher l'accès	http://*nom_de_serveur*/itim/self/ViewAccess.do
Supprimer l'accès	http://*nom_de_serveur*/itim/self/DeleteAccess.do
Confirmation de la suppression d'accès (pour une suppression d'accès spécifique)	http://*nom_de_serveur*/itim/self/DeleteAccess.do?accessDN=*accessDN*
Compte de demande	http://*nom_de_serveur*/itim/self/RequestAccounts.do
Compte de demande (accès direct au formulaire de compte de demande pour un service spécifique)	http://*nom_de_serveur*/itim/self/RequestAccounts.do?serviceDN=*serviceDN*

Tableau 13. URL et tâches à accès direct (suite)

Tâche	URL
Visualiser le compte	• http://*nom_de_serveur*/itim/self/ViewAccount.do (vue de plusieurs comptes) • http://*nom_de_serveur*/itim/self/ViewAccount.do?userID=*userID*&serviceDN=*serviceDN* (compte de service spécifique)
Visualiser ou modifier un compte	http://*nom_de_serveur*/itim/self/ViewChangeAccount.do
Modifier le compte	• http://*nom_de_serveur*/itim/self/ChangeAccount.do (vue de plusieurs comptes) • http://*nom_de_serveur*/itim/self/ChangeAccount.do?userID=*userID*&serviceDN=*serviceDN* (compte de service spécifique)
Supprimer un compte	http://*nom_de_serveur*/itim/self/DeleteAccount.do
Confirmation de la suppression de compte	http://*nom_de_serveur*/itim/self/DeleteAccount.do?userID=*userID*&serviceDN=*serviceDN* (compte de service spécifique)
Visualiser mon profil	http://*nom_de_serveur*/itim/self/ViewProfile.do
Modifier le profil	http://*nom_de_serveur*/itim/self/ChangeProfile.do
Visualiser mes demandes	• http://*nom_de_serveur*/itim/self/ViewRequests.do (vue de plusieurs demandes) • http://*nom_de_serveur*/itim/self/ViewRequests.do?request=*requestID* (vue de demande spécifique)
Approuver et consulter les demandes	• http://*nom_de_serveur*/itim/self/ReviewActivities.do (vue de plusieurs activités) • http://*nom_de_serveur*/itim/self/ReviewActivities.do?activity=*activityID* (vue d'activité spécifique)
Déléguer des activités	http://*nom_de_serveur*/itim/self/delegateActivities.do

Personnalisation de la fonction de recherche d'utilisateur

Vous pouvez activer la fonction de recherche d'utilisateur dans l'interface utilisateur en libre-service.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

La fonction de recherche de personne est un outil puissant qui vous permet de sélectionner uniquement les personnes qui correspondent à certains critères de recherche. La recherche de personne utilise une gamme étendue d'attributs de recherche.

Les noms d'attributs prennent la forme `ui.usersearch.attr.`*nom_attribut=nom_attribut* dans les cas où *nom_attribut* est commun à tous les profils Utilisateur et Utilisateur d'une organisation partenaire. *nom_attribut* est une valeur qui mappe à cet attribut de profil. Par exemple, `ui.usersearch.attr.cn=cn` effectue une recherche par nom commun.

Certains attributs isolés peuvent être associés à plusieurs attributs si les profils changent. Dans ce cas, les noms d'attributs prennent la forme `ui.usersearch.attr.`*nom_attribut=profil1.nom_attribut1*`,`*profil2.nom_attribut1*

Par exemple, `ui.usersearch.attr.telephone=Person.mobile,BPPerson.telephonenumber` mapperait le numéro de téléphone portable du profil d'utilisateur et le numéro de téléphone du profil d'utilisateur d'une organisation partenaire.

La valeur convertie du nom d'attribut s'affiche dans la recherche par zone d'attribut.

Pour activer la fonction de recherche d'utilisateur pour l'interface utilisateur en libre-service, exécutez les tâches suivantes :

Procédure

1. Effectuez une copie de sauvegarde du fichier `SelfServiceUI.properties` se trouvant dans le répertoire *ITIM_HOME*`\data`.
2. Ajoutez ou supprimez des attributs dans le fichier `SelfServiceUI.properties` sous la section de configuration de la recherche des utilisateurs.
3. Redémarrez l'application IBM Security Identity Manager dans WebSphere pour que les modifications prennent effet.

Personnalisation de l'interface utilisateur de la console d'administration

Cette section décrit comment personnaliser l'interface utilisateur de la console d'administration.

L'interface utilisateur de la console d'administration IBM Security Identity Manager peut être personnalisée. Les clients peuvent disposer d'une présentation d'entreprise commune tout en conservant la souplesse d'exécuter les tâches d'identité d'administration inhérentes à leurs rôles et responsabilités.

Vous pouvez définir et personnaliser l'interface de la console d'administration de deux manières, à l'aide de l'infrastructure préfabriquée de la console intégrée ou bien en modifiant directement les fichiers installés dans IBM Security Identity Manager :

- Fonctions de la console intégrée :
  - Eléments de contrôle d'accès (ACI)
  - Vues
- Fichiers modifiables :
  - Fichiers de propriétés
  - Fichiers image

Sauvegardez tous les fichiers modifiables à des fins de récupération avant d'apporter des modifications personnalisées à IBM Security Identity Manager.

Fichiers de configuration et leurs descriptions

Les fichiers de configuration définissent l'aspect de l'interface utilisateur de la console d'administration IBM Security Identity Manager.

La table suivante affiche la liste des noms de fichier et décrit leurs rôles dans la personnalisation d'IBM Security Identity Manager.

Tableau 14. Fichiers de configuration des propriétés et leurs descriptions

Nom du fichier	Description du fichier
ui.properties	Commande la présentation de l'en-tête, du pied de page et de la page d'accueil et configure le titre, le nombre de pages affichées et le nombre de résultats de recherche renvoyés.
helpmapping.properties	Commande le réacheminement et le mappage de l'aide html de la console d'administration.

Sauvegarde et restauration des fichiers de configuration de l'interface utilisateur de la console d'administration

Avant de commencer la personnalisation de l'interface utilisateur de la console d'administration, sauvegardez tous les fichiers de configuration dans IBM Security Identity Manager pour pouvoir les récupérer ultérieurement.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Créez un répertoire nommé `custom` dans le répertoire *`WAS_PROFILE_HOME`*`\installedApps\`*`nom_noeud`*`\ITIM.ear\itim_console.war` et placez-y les nouveaux fichiers de personnalisation.

Connectez-vous à chaque ordinateur sur lequel IBM Security Identity Manager est exécuté et sauvegardez les fichiers suivants :

- Dans le répertoire *`ITIM_HOME`*`\data` :
  - `ui.properties`
  - `helpmappings.properties`

Pourquoi et quand exécuter cette tâche

Si vous avez apporté des modifications aux fichiers de propriétés, vous devez redémarrer l'application IBM Security Identity Manager. Par exemple, après avoir récupéré des fichiers de propriétés, exécutez les étapes suivantes :

Procédure

1. Avec la console d'administration de WebSphere, cliquez sur le groupe **Applications** dans le cadre gauche, puis cliquez sur le lien **Applications d'entreprise**.
2. Cochez la case en regard de l'application IBM Security Identity Manager et cliquez sur le bouton **Arrêter**.
3. Une fois l'application arrêtée, cochez la case en regard de l'application IBM Security Identity Manager et cliquez sur le bouton **Démarrer**.

4. Vérifiez que la récupération a été exécutée en vous connectant à l'interface utilisateur en libre-service.

Personnalisation du contenu des bannières

Vous pouvez modifier la présentation de l'interface utilisateur de la console d'administration en personnalisant la bannière.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter ou modifier du contenu de bannière pour modifier la présentation de l'interface utilisateur de la console d'administration.

La zone de la bannière par défaut est définie dans deux fichiers, un fichier JSP `banner.jsp` et un fichier de propriétés nommé `ui.properties`. La zone de la bannière se compose de quatre éléments :

- Lien de lancement de la bannière
- Logo de lancement de la bannière
- Logo de la bannière
- Image d'arrière-plan de la bannière

Lors de la personnalisation de la bannière, définissez les dimensions (largeur et hauteur) des composants du fichier banner.jsp. Définissez ces dimensions de telle sorte que la taille de l'image de logo personnalisé soit adaptée et que l'image ne soit pas déformée. Assurez-vous également que le cadre de bannière n'est pas déformé.

Vous pouvez modifier le lien de lancement et le logo de la bannière en modifiant le fichier `ui.properties`. Si vous souhaitez modifier l'image d'arrière-plan et le logo de bannière, vous devez créer un fichier pour afficher votre bannière. Ce fichier peut être un fichier de bannière JSP ou HTML.

Les clés de propriété suivantes du fichier `ui.properties` définissent le lien de lancement de bannière et le logo de lancement de bannière. Elles définissent également l'URL du logo et de l'image d'arrière-plan de bannière.

Tableau 15. Clés de propriété de bannière

Clé de propriété	Valeur par défaut	Description
enrole.ui.customerLogo.image	ibm_banner.gif	Logo du lien de lancement, se trouvant dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_console.war\html\images. Vous pouvez également indiquer une URL pointant vers le fichier image ou placer ce fichier dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_console.war\custom. Si ce répertoire n'existe pas, vous devez le créer. Dans le fichier ui.properties, placez la chaîne /itim/console/custom au début du nom du chemin. Si aucune valeur n'est indiquée, c'est le fichier par défaut ibm_banner.gif qui est affiché.
enrole.ui.customerLogo.url	www.ibm.com	URL du lien de lancement. Cette valeur peut être indiquée avec ou sans le préfixe HTTP. Par exemple, vous pouvez utiliser www.ibm.com ou http://www.ibm.com pour indiquer l'URL du lien de lancement.
ui.banner.URL	Cette valeur est laissée vide par défaut et affiche la zone de la bannière par défaut.	Fichier HTML ou JSP fournissant le logo, l'image d'arrière-plan, le lien et le logo de lancement de la bannière. Vous pouvez indiquer une URL ou placer ce fichier dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_console.war\custom. Si ce répertoire n'existe pas, vous devez le créer. Dans le fichier ui.properties, placez la chaîne /itim/console/custom au début du nom du chemin.
ui.banner.height	48	Entrez la hauteur en pixels de la bannière.

Pour modifier ces fichiers, exécutez les étapes suivantes :

Procédure

1. Effectuez des copies de sauvegarde des fichiers et stockez les fichiers que vous voulez modifier dans un répertoire temporaire.
2. Editez les fichiers dans le répertoire temporaire et copiez les fichiers mis à jour de nouveau dans le répertoire WebSphere déployé. Vous devez redémarrer l'application IBM Security Identity Manager pour que ces modifications prennent effet.

Que faire ensuite

Veillez à sauvegarder la version personnalisée des fichiers que vous avez créée pour que vos personnalisations ne soient pas perdues.

Personnalisation du contenu des pieds de page

Vous pouvez modifier la présentation de l'interface utilisateur de la console d'administration en personnalisant le pied de page.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter ou modifier le contenu du pied de page pour modifier la présentation de l'interface utilisateur de la console d'administration.

La zone de pied de page par défaut est définie dans le fichier `ui.properties`.

Les clés de propriété suivantes du fichier `ui.properties` définissent le pied de page et indiquent sa visibilité et sa hauteur.

Tableau 16. Clés de propriété du pied de page

Clé de propriété	Valeur par défaut	Description
ui.footer.isVisible	no	Indique si le pied de page est visible. Par défaut, le pied de page est désactivé.
ui.footer.URL	Cette valeur est laissée vide par défaut.	Indique l'emplacement du fichier HTML ou JSP qui fournit le pied de page. Vous pouvez entrer une URL. Vous pouvez également placer ce fichier dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_console.war\custom (si ce répertoire n'existe pas, créez-le) et placer la chaîne /itim/console/custom au début du nom du chemin dans le fichier ui.properties.
ui.footer.height	50	Entrez la hauteur en pixels du pied de page.

Pour modifier ces fichiers, exécutez les étapes suivantes :

Procédure

1. Effectuez une copie de sauvegarde du fichier `ui.properties` et stockez le fichier dans un répertoire temporaire.
2. Editez le fichier dans le répertoire temporaire et copiez de nouveau le fichier mis à jour dans le répertoire WebSphere déployé. Vous devez redémarrer l'application IBM Security Identity Manager pour que ces modifications prennent effet.

Que faire ensuite

Veillez à sauvegarder la version personnalisée du fichier que vous avez créée pour que vos personnalisations ne soient pas perdues.

Personnalisation de la page d'accueil de la console d'administration

Vous pouvez changer la page d'accueil de l'interface utilisateur de la console d'administration.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

La page d'accueil renvoie à la page principale qui est chargée lorsqu'un utilisateur se connecte à l'interface utilisateur de la console d'administration.

Les définitions de section et de tâche combinent les vues définies en tâches et groupent les tâches en sections, également appelées pages de tâches. Cette section et ces définitions de tâches sont définies dans un fichier de propriétés du répertoire *ITIM_HOME*\data.

Vous pouvez coder des liens directs vers des tâches de la page d'accueil vers les fonctions d'administration. Utilisez JSP pour générer du code HTML dynamique afin que les fonctions d'administration soient limitées aux utilisateurs disposant des droits d'accès appropriés.

Pour personnaliser la page d'accueil, exécutez les étapes suivantes :

Procédure

1. Effectuez une copie de sauvegarde du fichier `ui.properties` se trouvant dans le répertoire *ITIM_HOME*\data.
2. Editez le fichier `ui.properties`. Modifiez la clé ui.homepage.path et enregistrez le fichier. Entrez une URL du fichier HTML ou JSP que vous utilisez pour une page d'accueil. Vous pouvez également placer ce fichier dans le répertoire *WAS_PROFILE_HOME*\installedApps*nom_noeud*\ITIM.ear\itim_console.war\custom (si ce répertoire n'existe pas, créez-le) et placer la chaîne /itim/console/custom au début du nom de fichier.
3. Redémarrez l'application IBM Security Identity Manager dans WebSphere pour que les modifications prennent effet.

Liens URL d'accès direct aux tâches de la console d'administration

Cette section fournit des liens d'accès direct par URL aux tâches dans l'interface utilisateur de la console d'administration.

La table suivante affiche les liens vers les tâches qui sont prises en charge pour l'accès direct et vers lesquelles vous pouvez créer des liens à partir de la page d'accueil.

Tableau 17. Tâches et liens d'accès direct

Tâche	URL
Modifier le mot de passe	Modifier le mot de passe
Gérer les rôles	Gérer les rôles
Gérer la structure de l'organisation	Gérer la structure de l'organisation
Gérer les utilisateurs	Gérer les utilisateurs
Gérer les services	Gérer les services
Gérer les règles d'administration des identités	Gérer les règles d'administration des identités
Gérer les règles d'administration des mots de passe	Gérer les règles d'administration des mots de passe
Gérer les règles d'adoption	Gérer les règles d'adoption
Gérer les règles d'administration des recertifications	Gérer les règles d'administration des recertifications
Gérer les règles d'application des accès	Gérer les règles d'application des accès
Gérer les règles de sélection des services	Gérer les règles de sélection des services
Gérer les flux de travaux de demandes de comptes	Gérer les flux de travaux de demandes de comptes
Gérer les flux de travaux de demandes d'accès	Gérer les flux de travaux de demandes d'accès
Gérer les groupes	Gérer les groupes
Gérer les éléments de contrôle d'accès	Gérer les éléments de contrôle d'accès
Gérer les vues	Gérer les vues

Tableau 17. Tâches et liens d'accès direct (suite)

Tâche	URL
Définir les propriétés de sécurité	Définir les propriétés de sécurité
Configurer les paramètres pour les mots de passe oubliés	Configurer les paramètres pour les mots de passe oubliés
Rapports sur les demandes	Rapports sur les demandes
Rapports sur les services	Rapports sur les services
Rapports sur l'audit et la sécurité	Rapports sur l'audit et la sécurité
Rapports personnalisés	Rapports personnalisés
Propriétés de rapport	Propriétés de rapport
Configurer le schéma de réplication	Configurer le schéma de réplication
Concevoir des rapports	Concevoir des rapports
Gérer les types de services	Gérer les types de services
Concevoir des formulaires	Concevoir des formulaires
Définir les propriétés de notification du flux de travaux	Définir les propriétés de notification du flux de travaux
Configurer le bureau de poste	Configurer le bureau de poste
Gérer les entités	Gérer les entités
Gérer des opérations	Gérer des opérations
Gérer les règles de cycle de vie	Gérer les règles de cycle de vie
Gérer les types d'accès	Gérer les types d'accès
Configurer les comportements de jointure des règles	Configurer les comportements de jointure des règles
Configurer une mise en application des règles d'administration globales	Configurer une mise en application des règles d'administration globales
Importer des données	Importer des données

Tableau 17. Tâches et liens d'accès direct (suite)

Tâche	URL
Exporter des données	Exporter des données
Afficher les demandes en attente par utilisateur	Afficher les demandes en attente par utilisateur
Afficher toutes les demandes par utilisateur	Afficher toutes les demandes par utilisateur
Afficher les demandes en attente par service	Afficher les demandes en attente par service
Afficher toutes les demandes par service	Afficher toutes les demandes par service
Afficher toutes les demandes	Afficher toutes les demandes
Afficher les activités	Afficher les activités
Afficher les activités par utilisateur	Afficher les activités par utilisateur
Gérer les planifications de la délégation	Gérer les planifications de la délégation
A propos de	A propos de
Définir les questions pour les mots de passe oubliés	Définir les questions pour les mots de passe oubliés

Personnalisation de la barre de titre

Vous pouvez modifier la barre de titre affichée dans le navigateur Web lorsque vous vous connectez à la console d'administration d'IBM Security Identity Manager.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Pour personnaliser la barre de titre, exécutez les étapes suivantes :

Procédure

1. Effectuez une copie de sauvegarde du fichier `ui.properties` et stockez le fichier dans un répertoire temporaire.

2. Editez la propriété ui.titlebar.text avec le titre que vous voulez utiliser et enregistrez le fichier. La valeur par défaut est laissée vide et le texte IBM Security Identity Manager s'affiche.
3. Copiez de nouveau le fichier mis à jour dans le répertoire WebSphere déployé. Vous devez redémarrer l'application IBM Security Identity Manager pour que ces modifications prennent effet.

Que faire ensuite

Veillez à sauvegarder la version personnalisée des fichiers que vous avez créée pour que vos personnalisations ne soient pas perdues.

Réacheminement du contenu de l'aide

Vous pouvez réacheminer les demandes d'aide vers votre propre site Web afin de fournir un contenu d'aide personnalisé pour l'interface utilisateur de la console d'administration.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

L'édition du contenu d'aide fourni avec l'interface utilisateur de la console d'administration n'est pas prise en charge. Il est, toutefois, possible de réacheminer les demandes d'aide vers votre propre site Web pour fournir un contenu d'aide personnalisé.

Le fichier `helpmappings.properties` indique l'URL de base à laquelle les demandes d'aide sont envoyées. Ces fichiers se trouvent dans le répertoire *ITIM_HOME*`\data`.

La table suivante affiche la propriété et la description de la propriété pour l'aide.

Tableau 18. Propriétés et descriptions de l'aide en libre-service

Propriété	Description
helpBaseUrl	Indique l'URL de base vers laquelle envoyer les demandes d'aide. Une valeur vide indique que l'aide doit être envoyée à l'URL par défaut pour l'interface utilisateur de la console d'administration.
Help ID mappings: helpID = URL de page relative	La section des mappages d'aide mappe les ID de certaines pages à une adresse URL relative envoyée au serveur d'aide.

L'URL d'aide est la combinaison de helpBaseUrl + locale + relativeHelppageURL

Par exemple :

```
helpBaseUrl=http://myserver:80
locale = en_US
```

Remarque : L'environnement local est déterminé en comparant les paramètres du navigateur de l'utilisateur actuellement connecté avec les modules de langue IBM Security Identity Manager actuellement installés.

```
loginID/relativeURL = login_help_url=ui/ui_eui_login.html
```

Par conséquent, l'URL finale est http://myserver:80/en_US/ui/ui_eui_login.html.

Pour réacheminer l'aide, exécutez les étapes suivantes :

Procédure

1. Effectuez une copie de sauvegarde du fichier `helpmappings.properties` se trouvant dans le répertoire *ITIM_HOME*\data.
2. Modifiez la propriété helpBaseUrl dans le fichier `helpmappings.properties`. Il est important que les clients ne modifient pas les helpID. Ils sont en effet utilisés dans les panneaux de l'interface utilisateur IBM Security Identity Manager pour la recherche d'aide appropriée.
3. Mettez à jour les mappages des helpID pour utiliser les URL correspondantes pour votre serveur.
4. Ajoutez des pages à votre serveur pour les paramètres nationaux appropriés.
5. Redémarrez l'application **ITIM** dans WebSphere pour que les modifications prennent effet.

Personnalisation du nombre d'éléments affichées sur les pages

Vous pouvez modifier le nombre d'éléments affichés sur les pages.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Le tableau suivant affiche les propriétés, les valeurs par défaut et la description de ces paramètres de page.

Tableau 19. Paramètres, valeurs par défaut et descriptions de panneau

Propriété	Valeur par défaut	Description
enrole.ui.pageSize	50	Indique le nombre d'éléments de liste affichés sur une page.
enrole.ui.maxSearchResults	1000	Indique le nombre maximum d'éléments de recherche renvoyés.

Remarque : Ces modifications peuvent affecter l'utilisation de la mémoire si elles sont définies sur des valeurs excessives.

Pour modifier les paramètres de page, procédez comme suit :

Procédure

1. Effectuez une copie de sauvegarde du fichier `ui.properties` se trouvant dans le répertoire *ITIM_HOME*`\data`.
2. Editez le fichier dans un répertoire temporaire et copiez de nouveau le fichier mis à jour dans le répertoire.
3. Redémarrez l'application IBM Security Identity Manager dans WebSphere pour que les modifications prennent effet.

Que faire ensuite

Veillez à sauvegarder la version personnalisée du fichier pour que vos personnalisations ne soient pas perdues.

Chapitre 2. Gestion des types de service

Un *type de service* est une catégorie de services connexes qui partagent les mêmes schémas. Le type de service définit les attributs de schéma communs à un ensemble de ressources gérées similaires.

Présentation

Les types de services sont des profils ou modèles qui permettent de créer des services pour des instances spécifiques de ressources gérées. Par exemple, si vous disposez de plusieurs serveurs Lotus Domino auxquels les utilisateurs ont besoin d'accéder, vous pouvez créer un service pour chaque serveur Lotus Domino avec le type de service Lotus Domino. Dans les versions précédentes d'IBM Security Identity Manager, un type de service est appelé *profil de service*.

Certains types de services sont installés par défaut lors de l'installation d'IBM Security Identity Manager. D'autres types de services peuvent être installés lorsque vous importez les fichiers de définitions de services pour les adaptateurs pour les ressources gérées. Une définition de type de service est fournie par l'adaptateur IBM Security Identity Manager pour une ressource gérée. Il y a un type de service pour chaque type de ressource gérée prise en charge par IBM Security Identity Manager, par exemple UNIX, Linux, Windows, IBM Security Access Manager etc.

Un type de service est défini dans le fichier de définition de service d'un adaptateur, qui est un fichier d'archive Java (JAR) contenant le profil. Le type de service pour un adaptateur est créé lorsque le profil d'adaptateur (le fichier JAR) est importé. Par exemple, un type de service est défini dans le fichier `WinLocalProfileJAR`. Vous pouvez également définir un type de service dans l'interface de IBM Security Identity Manager.

IBM Security Identity Manager prend en charge les types de fournisseurs de services suivants :

- DAML pour l'adaptateur local Windows, pour l'adaptateur Lotus Notes, etc
- IDI (IBM Tivoli Directory Integrator pour les adaptateurs UNIX et Linux)
- Classe Java personnalisée pour définir votre propre implémentation d'un fournisseur de services
- Manuel pour gérer des activités « manuelles » définies par l'utilisateur

Types de service par défaut

Les types de service par défaut suivants sont fournis avec IBM Security Identity Manager :

Types de service de l'alimentation d'identité :

DSML
Un service d'alimentation d'identité DSML importe les données utilisateur, sans données de compte, stockées depuis une base de données ou un fichier de ressources humaines et les place dans le répertoire de IBM Security Identity Manager. Le service utilise une règle de positionnement pour déterminer où placer un utilisateur dans l'organisation. Le service peut recevoir les informations de

deux manières : par rapprochement ou par notification d'événement. Ce service repose sur le profil de service d'alimentation d'identité DSML.

Remarque : DSMLv2 est obsolète dans IBM Security Identity Manager Version 5.0 en faveur de la structure éloignée de l'adaptateur IDI (RMI) d'appel des méthodes. L'utilisation de DSMLv2 reste prise en charge dans cette édition.

AD Le service d'alimentation d'identité AD importe les données utilisateur depuis Windows Active Directory. Les objets organizationalPerson sont insérés dans IBM Security Identity Manager et ajoutent ou mettent à jour des utilisateurs de IBM Security Identity Manager. Les profils utilisateur sélectionnés dans ce service doivent avoir une classe d'objets dérivée de la classe organizationalPerson.

CSV Le service d'alimentation d'identité CSV importe les données utilisateur à partir d'un fichier CSV et ajoute ou met à jour les utilisateurs dans IBM Security Identity Manager. Le fichier CSV contient un ensemble d'enregistrements séparés par la paire de caractères CR/LF (retour chariot - saut de ligne, \r\n). Chaque enregistrement contient un ensemble de zones séparées par une virgule. Si une zone contient une virgule ou une marque de fin CR/LF, la virgule doit être neutralisée par des guillemets doubles, en tant que délimiteur. Le premier enregistrement du fichier source CSV définit les attributs fournis dans chacun des enregistrements suivants. Les attributs doivent être valides d'après le schéma de classe pour le profil d'utilisateur sélectionné pour ce service.

Service IDI Data Feed
Le type de service de source de données IDI utilise Tivoli Directory Integrator pour importer des données utilisateur, sans données de compte, dans IBM Security Identity Manager et pour gérer les comptes dans le magasin de données IBM Security Identity Manager sur des ressources externes. Ce service repose sur le profil de service de source de données IDI.

INetOrgPerson
L'alimentation d'identité InetOrgPerson importe les données utilisateur de l'annuaire LDAP. Les objets inetOrgPerson sont chargés et ajoutent ou mettent à jour des utilisateurs dans IBM Security Identity Manager.

Types de services de compte :

Reposant sur Tivoli Directory Integrator
Ce type de service peut être installé, si vous le souhaitez, pendant l'installation de IBM Security Identity Manager. Ce sont tous des adaptateurs reposant sur Tivoli Directory Integrator, dont chacun est un type de service spécifique. Tivoli Directory Integrator est un type de fournisseur de services. Il peut y avoir plusieurs types de service définis pour le même type de fournisseur de services.

Service ITIM
Le type de service ITIM est utilisé pour créer des comptes dans le système IBM Security Identity Manager et pour représenter le serveur IBM Security Identity Manager lui-même. Il s'agit d'un service standard sans paramètres de configuration. Tous les

utilisateurs ayant besoin d'accéder au système IBM Security Identity Manager doivent être dotés d'un compte IBM Security Identity Manager.

Service hébergé
Le type Service hébergé est utilisé pour créer un service qui est un proxy pour le service d'hébergement qui se trouve dans l'organisation du fournisseur de services.

Le service hébergé se connecte à la cible de ressource gérée indirectement à travers le service d'hébergement. Les détails de la configuration du service d'hébergement sont invisibles et sont protégés des administrateurs dans l'organisation secondaire où le service hébergé est défini. Les administrateurs peuvent définir des règles spécialement pour le service hébergé, sans effet sur le service d'hébergement.

L'utilisation première d'un service hébergé est de permettre aux utilisateurs dans des organisations partenaire d'avoir des comptes et un accès aux ressources informatiques internes d'une organisation et de permettre aux administrateurs de l'organisation secondaire de définir des règles de service spécifiques pour les comptes utilisateur.

Classe Java personnalisée
Le type de service de classe Java personnalisée vous permet de définir votre propre profil en définissant et en implémentant une classe Java.

Services manuels et types de service

Le type de service manuel permet de gérer manuellement des comptes utilisateur dans une ressource cible. Les demandes de compte sont routées vers un utilisateur spécifique et non vers un fournisseur de services, de façon à pouvoir être traitées manuellement ou à l'aide d'autres outils en dehors du serveur IBM Security Identity Manager.

Ce sont des ressources pour lesquelles au moins une des affirmations suivantes est vraie :

- Il n'existe actuellement pas d'adaptateur disponible pour exécuter l'application des accès et il n'est pas possible ou pratique de développer un adaptateur personnalisé.
- Tout ou partie de l'activité de l'application des accès nécessite qu'un utilisateur exécute le traitement de configuration nécessaire.
- Vous choisissez d'exécuter la tâche manuellement.

Voici des exemples de ressources pour des types de service manuels et pour des services manuels :

- Configuration de messagerie vocale
- Configuration du téléphone
- Configuration d'un ordinateur personnel
- Configuration de messagerie physique
- Demande de badge d'employé

  Services manuels

  Activation du mode de connexion

Création de services manuels

Créez une instance de service manuel lorsqu'IBM Security Identity Manager ne fournit pas d'adaptateur pour la ressource gérée.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Avant de pouvoir créer un service manuel dans IBM Security Identity Manager, vous devez créer un type de service en ajoutant des attributs et des classes de schéma pour le service manuel à votre annuaire LDAP.

Pourquoi et quand exécuter cette tâche

Un service manuel est un type de service qui requiert une intervention manuelle pour compléter la demande. Par exemple, un service manuel peut être défini pour configurer la messagerie vocale d'un utilisateur. Un service manuel génère un ordre de travail qui définit l'intervention manuelle requise.

Si vous choisissez de créer une règle d'application des accès dans le cadre de cette tâche, le service sera automatiquement ajouté à la règle d'application des accès en tant qu'habilitation. En outre, une appartenance de “Tous” est définie pour la règle d'application des accès. De plus, un type de propriété "Individuel" est défini pour la règle d'application des accès. Vous pouvez ultérieurement éditer cette règle et changer l'appartenance et les types de propriété une fois le service créé.

Le nom de service et la description que vous fournissez pour chaque service sont affichés sur la console. Il est donc important d'indiquer des valeurs qui aient un sens pour vos utilisateurs et vos administrateurs.

Pour créer une instance de service manuel, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, cliquez sur **Créer**. L'assistant Créer un service s'affiche.
3. Dans la page Sélectionner le type de service, cliquez sur **Rechercher** pour localiser une unité commerciale. La page Unité commerciale s'affiche.
4. Dans le page Unité commerciale, procédez comme suit :
   a. Entrez les informations relatives à l'unité commerciale dans la zone **Rechercher des informations**.
   b. Sélectionnez un type d'unité dans la liste **Rechercher par**, puis cliquez sur **Rechercher**. Une liste des unités commerciales qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.

c. Dans le tableau **Unités commerciales**, sélectionnez l'unité commerciale dans laquelle vous voulez créer la service, et cliquez sur **OK**. La page Sélectionner le type de service s'affiche, et l'unité commerciale que vous avez spécifiée s'affiche dans la zone **Unité commerciale**.

5. Dans la page Sélectionner le type de service, sélectionnez un type de service manuel, et cliquez sur **Suivant**.

   Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

   - Cliquez sur la flèche pour accéder à la page suivante.
   - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.

6. Dans la page Informations générales, indiquez les valeurs appropriés pour l'instance de service manuel et cliquez sur **Suivant**. Le contenu de cette page dépend du type de service que vous créez. La création de certains services nécessitent des étapes supplémentaires.
7. Sur la page Participants, indiquez les utilisateurs impliqués dans les activités pour le service manuel. Définissez la durée avant que le service ne passe au niveau supérieur. Cliquez sur **Suivant**.
8. Facultatif : Dans la page Messages, complétez les zones suivantes et cliquez sur **Rapprochement** :
   a. Sélectionnez le message électronique par défaut à modifier puis cliquez sur **Modifier**. La page Modifier le message s'affiche.
   b. Modifiez les zones **Objet** et **Corps** puis cliquez sur **OK**.
9. Dans la page Configurer une règle, sélectionnez une option de règle d'application des accès, puis cliquez sur **Suivant** ou **Terminer**. La règle d'application des accès détermine les types de propriété disponibles pour les comptes. La règle d'application des accès par défaut active uniquement les comptes dont le type de propriété est Individuel. Des types de propriété supplémentaires peuvent être ajoutés en créant des droits sur la règle d'application des accès.
10. Facultatif : Dans la page Synchronisation, cliquez sur **Parcourir** pour localiser le fichier de synchronisation, puis sur **Télécharger le fichier** pour charger le nouveau fichier de synchronisation. Vous pouvez également choisir de synchroniser les données de support uniquement.

    Remarque : Le type de fichier pris en charge pour le fichier de synchronisation est CSV. Pour plus d'informations, voir la rubrique "Exemple de fichier CSV (fichier de valeurs séparées par des virgules)" dans le document *IBM Security Identity Manager – Guide d'administration*.
11. Cliquez sur **Terminer**.

Résultats

Un message s'affiche indiquant que vous avez correctement créé l'instance de service manuel pour un type de service spécifique.

Que faire ensuite

Sélectionnez une autre tâche de services ou cliquez sur **Fermer**. Lorsque la page Sélectionner un service s'affiche, cliquez sur **Régénérer** pour régénérer la table **Services** et afficher la nouvelle instance du service.

Modification d'un service manuel

Modifiez les informations d'une instance de service manuel.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Avant de pouvoir modifier un service dans IBM Security Identity Manager, vous devez créer une instance de service.

Procédure

Pour modifier une instance de service manuel, procédez comme suit :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être appliquée à des services ou à des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :
      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.
3. Dans la table **Services**, sélectionnez la case à cocher en regard du service manuel à modifier puis cliquez sur **Modifier**.
4. Dans la page Informations générales, modifiez les valeurs appropriées pour l'instance de service, puis cliquez sur **Participants**.
5. Dans la page Participants, modifiez le type de participant, la période de transfert à un niveau supérieur en jours ou le type de responsable de niveau supérieur.
6. Facultatif : Dans la page Messages, complétez les zones suivantes et cliquez sur **Rapprochement** :
   a. Sélectionnez le message électronique à modifier puis cliquez sur **Modifier**. La page Modifier le message s'affiche.
   b. Modifiez les zones **Objet** et **Corps** puis cliquez sur **OK**.
7. Facultatif : Dans la page Synchronisation, cliquez sur **Parcourir** pour localiser le fichier de synchronisation, puis sur **Télécharger le fichier** pour charger le nouveau fichier de synchronisation. Vous pouvez également choisir de synchroniser les données de support uniquement.

Remarque : Le type de fichier pris en charge pour le fichier de synchronisation est CSV. Pour plus d'informations, voir la rubrique "Exemple de fichier CSV (fichier de valeurs séparées par des virgules)" dans le document *IBM Security Identity Manager – Guide de planification*.

8. Cliquez sur **OK** pour enregistrer les modifications et fermer la page.

Résultats

Un message s'affiche et indique que la modification de l'instance de service a abouti.

Que faire ensuite

Sélectionnez une autre tâche de services ou cliquez sur **Fermer**. Lorsque la page Sélectionner un service s'affiche, cliquez sur **Régénérer** pour régénérer le tableau **Services**.

Configuration d'un type de service manuel pour prendre en charge des groupes

Pour prendre en charge l'affectation de groupes mais pas leur gestion pour les services manuels, le profil du groupe doit être configuré lors de la configuration du type de service manuel.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Pour configurer un type de service manuel en vue de prendre en charge l'affectation de groupes mais pas leur gestion (qui inclut la création, la lecture, la mise à jour, la suppression) pour les services manuels, procédez comme suit :

Procédure

1. Définissez le schéma du groupe comme un objet de classe LDAP dans le serveur IBM Security Identity Manager.
2. Définissez un service manuel (complétez avec les classes d'objet du compte et du service). La classe d'objets du compte doit contenir un attribut facultatif à valeur multiple qui est utilisé pour stocker les informations d'une appartenance au groupe. Ce type de service doit faire référence au schéma de groupe créé à l'étape précédente.

   La page Gérer les types de service permet à l'administrateur de sélectionner un objet de classes LDAP existant à utiliser comme classe de schéma du groupe. Si vous voulez créer une nouvelle classe d'objets, vous devez la créer manuellement et la charger directement dans le serveur LDAP.

   Les attributs mappés **ID de groupe**, **Nom de groupe** et **Description de groupe** peuvent tous référencer le même attribut de schéma de groupe, en cas de besoin. Vous ne pouvez pas définir plusieurs groupes qui utilisent le même ID de groupe. L'ID doit être unique par groupe.

Plusieurs schémas de groupe peuvent être définis pour un type de service donné. La définition du second schéma et des schémas suivants se fait de la même manière que la première.

3. Modifiez les formulaires de service et de compte pour le type de service à l'aide Form Designer. Cette étape est obligatoire pour correctement afficher les informations utiles lors de la création d'une instance de service et des comptes.
4. Créez une instance de service manuel à l'aide du type de service manuel que vous avez créé auparavant dans ce processus.

Synchronisation des services manuels

Initiez une activité de synchronisation sur un service manuel.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vous devez avoir effectué les étapes de configuration d'un type de service manuel pour prendre en charge des groupes. Vous devez également avoir créé une instance de service manuel avant de commencer cette tâche.

Pourquoi et quand exécuter cette tâche

Les étapes de création d'une instance de service vous permettent de réaliser une synchronisation d'un service manuel à l'aide d'un fichier CSV que vous fournissez. La synchronisation remplit IBM Security Identity Manager avec les comptes et les groupes qui existent sur le service manuel. Le fichier CSV contient les informations relatives au groupe et au compte.

Vous pouvez fournir le fichier de synchronisation lors de la création du service ou lors de toute modification du service. Il existe également une option *données de support uniquement* pour la synchronisation utilisée quand vous voulez extraire des informations de groupe du fichier CSV sans toucher aux comptes IBM Security Identity Manager.

Pour effectuer une synchronisation sur un service manuel, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être appliquée à des services ou à des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**, puis cliquez sur **Rechercher**. Une liste des services correspondant aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

      • Cliquez sur la flèche pour accéder à la page suivante.

- Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.

3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service afin d'afficher les tâches qui peuvent être réalisées sur le service, puis cliquez sur **Modifier**. Les tâches pouvant être effectuées dépendent du type de service. La page Sélection des demandes s'affiche.
4. Dans la page Synchronisation, cliquez sur **Parcourir** pour localiser le fichier de synchronisation, puis sur **Télécharger le fichier** pour charger le nouveau fichier de synchronisation. Vous pouvez également choisir de ne synchroniser que les données de prise en charge.
5. Cliquez sur **OK** pour enregistrer les modifications et fermer la page.

Résultats

Un message s'affiche et indique que la soumission d'une demande de synchronisation a abouti.

Que faire ensuite

Pour visualiser les résultats de la synchronisation, cliquez sur **Afficher le statut de la demande de synchronisation**. Vous pouvez sélectionner une autre tâche de service, ou cliquez sur **Fermer**. Lorsque la page Sélectionner un service s'affiche, cliquez sur **Régénérer** pour régénérer le tableau **Services**.

Fichier de définition de service ou profil d'adaptateur

Un *fichier de définition du service*, appelé également *profil d'adaptateur*, définit le type de ressource gérée qu'IBM Security Identity Manager peut gérer.

Le fichier de définition du service crée les types de services sur le serveur IBM Security Identity Manager.

Le fichier de définition du service est un fichier d'archive Java (fichier JAR) contenant les informations suivantes :

- Informations sur le service, y compris les définitions des opérations d'application des accès aux comptes pouvant être effectuées pour le service, telles que l'ajout, la suppression, la suspension et la restauration.
- Informations sur le fournisseur de services, qui définissent l'implémentation sous-jacente de la méthode de communication du serveur IBM Security Identity Manager avec les ressources gérées.
- Informations sur le schéma, comprenant les classes LDAP et les attributs.
- Formulaires de compte et formulaires de service, avec le libellé des attributs, qui s'affichent dans l'interface utilisateur et permettent de créer des services et de demander des comptes sur ces services.

Création de types de service

En tant qu'administrateur, vous pouvez créer un type de service. Par exemple, vous pouvez créer un type de service pour un service manuel que vous voulez créer.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

La définition d'un nouveau type de service permet de définir de nouveaux attributs et classes d'objet LDAP. Vous pouvez également changer les attributs et les classes d'objet LDAP existants. Vous devez comprendre les effets d'une modification du schéma LDAP avec cette tâche. Ne changez la syntaxe ou le schéma des classes d'objet et des attributs existants. Si un nouveau type de service est requis, définissez-en un. Reportez-vous à votre répertoire de documentation pour connaître les restrictions et les valeurs recommandées concernant l'extension de schéma. Pour IBM Tivoli Directory Server version 6.1, voir http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/admin_gd13.htm#wq78.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer un type de service pour un service manuel ou pour un service personnalisé.

Pour créer un type de service, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Gérer les types de service**. La page Gérer les types de services s'affiche.
2. Dans la page Gérer les types de services, cliquez sur **Créer**. Le bloc-notes Gérer les types de services s'affiche.
3. Dans la page Général du bloc-notes Gérer les types de services, exécutez les étapes suivantes :
   a. Dans la zone **Nom du type de service**, fournissez un nom unique pour votre type de service.
   b. Dans la liste **Fournisseur de services**, sélectionnez le protocole qu'utilise IBM Security Identity Manager pour appliquer des accès aux comptes pour ce type de service.
   c. Cliquez sur l'onglet **Service**.
4. Dans la page Service, indiquez une classe et des attributs LDAP à associer au type de service, puis cliquez sur l'onglet **Compte**. La classe et les attributs LDAP varient en fonction des comptes fournis par la ressource gérée.
5. Dans la page Compte, indiquez une classe et des attributs LDAP à associer au schéma de compte, puis cliquez sur l'onglet **Groupe** ou sur le bouton **OK**.
6. Facultatif : Dans la page Groupe, exécutez les étapes suivantes :
   a. Pour ajouter un groupe au type de service, cliquez sur **Ajouter**. La page Ajouter un groupe s'affiche.
   b. Dans la page Ajouter un groupe, indiquez une classe et des informations de schéma LDAP. Un schéma de groupe doit être pris en charge par l'adaptateur pour ce type de service.
   c. Cliquez sur l'onglet **Divers** ou sur le bouton **OK**.
7. Facultatif : Dans la page Divers, exécutez les étapes suivantes :

a. Cochez cette case pour indiquer si vous voulez que le type de service figure dans les rapports des comptes inactifs.
b. Dans la liste **Date du dernier accès**, sélectionnez un attribut du schéma de compte qui est associé au type de service, puis cliquez sur le bouton **OK**.

Résultats

Un message indique que vous avez créé un type de service.

Que faire ensuite

Vérifiez les formulaires de compte et de service générés pour le nouveau type de service à l'aide du concepteur de formulaire, configurez les valeurs de compte par défaut du type de service ou cliquez sur **Fermer**.

Conseil : Vous pouvez aussi indiquer des valeurs pour les zones **Nom du type de service** et **Description** dans le fichier `CustomLabels.properties`.

Modification de types de service

Vous pouvez modifier un type de service pour sélectionner un fournisseur de services différent. Vous pouvez également changer un type de service pour changer les attributs ou la classe LDAP pour le type de service ou les comptes.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Un type de service doit exister, mais aucune instance du type de service ne peut exister.

La définition d'un nouveau type de service permet de définir de nouveaux attributs et classes d'objet LDAP. Vous pouvez également changer les attributs et les classes d'objet LDAP existants. Vous devez comprendre les effets d'une modification du schéma LDAP avec cette tâche. Ne changez la syntaxe ou le schéma des classes d'objet et des attributs existants. Si un nouveau type de service est requis, définissez-en un. Reportez-vous à votre répertoire de documentation pour connaître les restrictions et les valeurs recommandées concernant l'extension de schéma. Pour IBM Tivoli Directory Server version 6.1, voir http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/admin_gd13.htm#wq78.

Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas modifier un type de service s'il existe pour ce dernier une instance de service. Les utilisateurs peuvent utiliser des comptes sur cette instance de service.

Pour modifier un type de service, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Gérer les types de service**. La page Gérer les types de services s'affiche.
2. Dans la page Gérer les types de service, cochez la case à côté du type de service que vous voulez modifier, puis cliquez sur **Modifier**. Le bloc-notes Gérer les types de services s'affiche.
3. Dans le bloc-notes Gérer les types de services, effectuez les modifications souhaitées, puis cliquez sur **OK**. Le nom du type de service ne peut pas être modifié.

Résultats

Un message s'affiche indiquant que vous avez modifié le type de service.

Que faire ensuite

Si nécessaire, utilisez le concepteur de formulaire pour mettre à jour les formulaires de service et de compte en fonction des modifications des attributs du type de service ou cliquez sur **Fermer**.

Importation de types de service

En tant qu'administrateur, vous pouvez importer un fichier de définition de service qui crée un type de service. Les fichiers de définition de service sont également appelés des fichiers de profil d'adaptateur, qui sont fournis avec les différents adaptateurs IBM Security Identity Manager.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Le fichier à importer doit être un fichier d'archive Java (fichier JAR).

Pourquoi et quand exécuter cette tâche

Vous pouvez créer un type de service pour un adaptateur fournissant un fichier JAR.

Pour importer un type de service, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Gérer les types de service**. La page Gérer les types de services s'affiche.
2. Dans la page Gérer les types de services, cliquez sur **Importer**. La page Importer le type de service s'affiche.
3. Dans la page Importer le type de service, exécutez les étapes suivantes :
   a. Dans la zone **Fichier de définition du service**, entrez l'emplacement du répertoire du fichier ou cliquez sur **Parcourir** pour trouver le fichier. Par exemple, si vous installez l'adaptateur IBM Security Identity Manager pour un serveur Windows exécutant Active Directory, recherchez et importez le fichier `ADProfileJAR`.

b. Cliquez sur **OK** pour importer le fichier.

Résultats

Un message indique que vous avez importé un type de service.

Que faire ensuite

L'importation se déroule de manière asynchrone, ce qui peut donc prendre un certain temps. Dans la page Gérer les types de services, cliquez sur **Régénérer** pour voir le nouveau type de service. Si le nouveau type de service ne s'affiche pas après quelques minutes, vérifiez les fichiers journaux pour déterminer la raison de l'échec de l'importation.

Suppression de types de service

Vous pouvez supprimer un type de service ne contenant pas d'instance de service. Par exemple, si votre entreprise remplace une application, vous pouvez faire migrer les enregistrements utilisateur vers la nouvelle application, puis supprimer le type de service obsolète.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Avant de supprimer un type de service, vous devez supprimer toutes ses instances de service.

Pourquoi et quand exécuter cette tâche

Lorsque vous supprimez un type de service, les modifications apportées à la classe LDAP persistent même après la suppression du type de service.

Pour supprimer un type de service, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Gérer les types de service**. La page Gérer les types de services s'affiche.
2. Dans la page Gérer les types de service, cochez la case à côté du type de service que vous voulez modifier, puis cliquez sur **Supprimer**. Pour sélectionner tous les types de service, cochez la case située en haut de cette colonne. Le bloc-notes Gérer les types de services s'affiche.
3. Dans la page Confirmer, cliquez sur **Supprimer** pour supprimer le type de service ou cliquez sur **Annuler**.

Résultats

Un message s'affiche indiquant que vous avez supprimé le type de service.

Que faire ensuite

Effectuez d'autres tâches de gestion de type de service ou cliquez sur **Fermer**.

Gestion des valeurs par défaut des comptes pour un type de service

Vous pouvez définir des valeurs par défaut des attributs de compte pour un service ou pour un type de service.

Types de valeurs par défaut de compte

Valeurs par défaut de compte de type de service

Lorsque des valeurs par défaut de compte sont définies au *niveau du type de service*, elles s'appliquent à tous les services de ce type. Cependant, les valeurs par défaut d'un type de service peuvent être remplacées en définissant des valeurs par défaut de compte au *niveau du service*.

Vous pouvez définir des valeurs par défaut globales du compte à un seul emplacement. Vous n'avez pas besoin de définir les valeurs par défaut du même compte pour un service à plusieurs emplacements. Cette définition unique réduit le travail de personnalisation et les risques d'omissions ou d'erreurs.

Valeurs par défaut du compte de service

Ces valeurs par défaut sont initialement héritées des valeurs par défaut de compte du type de service, mais elles deviennent des valeurs locales du service dès qu'il est modifié. Elles deviennent des valeurs par défaut locales du compte et peuvent être modifiées ou supprimées. Les modifications (y compris les suppressions) ne s'appliquent pas aux valeurs par défaut de compte du type de service.

Options pour définir des valeurs par défaut pour des attributs de compte

De base

Vous permet de coder en dur des valeurs par défaut. Vous pouvez également générer une règle pour extraire des informations d'un attribut pour tout objet de la classe d'utilisateur IBM Security Identity Manager. Vous pouvez l'utiliser pour définir la valeur pour un attribut de compte.

Avancée

Vous permet de coder JavaScript pour extraire des données LDAP d'objets IBM Security Identity Manager et pour définir la valeur d'un attribut de compte. Comme point de départ, vous pouvez créer un compte de base par défaut, puis utiliser l'option avancée pour éditer le code JavaScript généré.

Ajout de valeurs de compte par défaut à un type de service

Ajouter des valeurs par défaut des comptes à un type de service.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Le type de service souhaité doit exister. S'il n'existe pas, vous devez importer le profil du type de service.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter des valeurs par défaut pour des attributs. Lorsque vous créez une instance de service pour ce type de service, les valeurs de compte par défaut pour le type de service sont copiées dans le service.

Pour ajouter les valeurs par défaut des comptes à un type de service, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Gérer les types de service**. La page Gérer les types de services s'affiche.
2. Dans le tableau **Types de service**, cliquez sur l'icône (▸) à côté du type de service, puis cliquez sur **Valeurs par défaut du compte**. La page Sélectionner un attribut de compte s'affiche.
3. Dans la page Sélectionner un attribut de compte, cliquez sur **Ajouter** pour ajouter un attribut. La page Sélectionner un attribut à définir comme valeur par défaut s'affiche.
4. Sur la page Sélectionner un attribut à définir comme valeur par défaut, sélectionnez un attribut de compte. Faites l'un des choix suivants :
   - **Ajouter**, qui permet d'ajouter une valeur par défaut pour l'attribut sélectionné. Remplissez les zones appropriées, qui varient en fonction du type de service, puis cliquez sur le bouton **OK**. L'attribut par défaut est ajouté à la liste de la page Sélectionner un attribut à définir comme valeur par défaut.
   - **Ajouter (Avancé)**, qui permet d'ajouter un script indiquant une valeur par défaut pour l'attribut sélectionné. Entrez le code JavaScript souhaité dans la zone **Script** puis cliquez sur **OK**. L'attribut par défaut est ajouté à la liste de la page Sélectionner un attribut à définir comme valeur par défaut.
5. Sur la page Sélectionner un attribut de compte, continuez d'ajouter des attributs par défaut au type de service. Une fois cette tâche terminée, cliquez sur **OK** pour sauvegarder les modifications et fermer la page.

Résultats

Un message indique que vous avez sauvegardé avec succès les valeurs de compte par défaut sur le type de service.

Modification des valeurs par défaut des comptes pour un type de service

Modifier les valeurs de compte par défaut pour un type de service.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Pour modifier les valeurs par défaut des comptes pour un type de service, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Gérer les types de service**. La page Gérer les types de services s'affiche.
2. Dans le tableau **Types de service**, cliquez sur l'icône ( ) à côté du type de service, puis cliquez sur **Valeurs par défaut du compte**. La page Sélectionner un attribut de compte s'affiche.
3. Sur la page Sélectionner un attribut de compte, sélectionnez la case à cocher en regard de l'attribut à modifier puis cliquez sur une des options suivantes :
   - **Modifier**, qui permet de modifier la valeur par défaut de l'attribut sélectionné. Remplissez les zones appropriées, qui varient en fonction du type de service, puis cliquez sur le bouton **OK**. La valeur de modèle pour l'attribut est mise à jour dans la liste de la page Sélectionner un attribut à définir comme valeur par défaut.

     Remarque : Si vous sélectionnez cette option alors qu'un attribut comporte actuellement une valeur par défaut définie dans un script, le script existant est remplacé par la valeur de modèle que vous indiquez.
   - **Modifier (Avancé)**, qui permet d'ajouter ou de modifier le script indiquant une valeur par défaut pour l'attribut sélectionné. Entrez le code JavaScript souhaité dans la zone **Script** puis cliquez sur **OK**. La valeur de modèle pour l'attribut est mise à jour dans la liste de la page Sélectionner un attribut à définir comme valeur par défaut.
4. Sur la page Sélectionner un attribut de compte, continuez de modifier les valeurs par défaut d'attribut pour le type de service. Une fois cette tâche terminée, cliquez sur **OK** pour sauvegarder les modifications et fermer la page.

Résultats

Un message indique que vous avez sauvegardé avec succès les valeurs de compte par défaut sur le type de service.

Suppression des valeurs par défaut des comptes d'un type de service

Supprimer des valeurs de compte par défaut d'un type de service.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Pour supprimer des valeurs de compte par défaut d'un type de service, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Gérer les types de service**. La page Gérer les types de services s'affiche.
2. Dans le tableau **Types de service**, cliquez sur l'icône ( ) à côté du type de service, puis cliquez sur **Valeurs par défaut du compte**. La page Sélectionner un attribut de compte s'affiche.

3. Sur la page Sélectionner un attribut de compte, sélectionnez la case à cocher en regard de l'attribut à supprimer puis cliquez sur **Supprimer**. Pour sélectionner tous les attributs, cochez la case située en haut de cette colonne. L'attribut par défaut est supprimé de la liste de la page Sélectionner un attribut à définir comme valeur par défaut.
4. Sur la page Sélectionner un attribut de compte, continuez de supprimer les attributs du type de service. Une fois cette tâche terminée, cliquez ensuite sur **OK** pour sauvegarder les modifications et fermer la page.

Résultats

Un message indique que vous avez supprimé avec succès les valeurs de compte par défaut du type de service.

Chapitre 3. Gestion des types d'accès

Les *types d'accès* permettent de classer les catégories d'accès vues par les utilisateurs. Utilisez la tâche **Gérer les types d'accès** pour classer les types d'accès dans votre organisation.

Les types d'accès suivants sont inclus à IBM Security Identity Manager :

- AccessRole, qui est un rôle pour l'accès aux ressources informatiques
- Application, qui est un accès à une application
- SharedFolder, qui est un accès à un dossier partagé
- MailGroup, qui est l'appartenance à un groupe de messages

En tant qu'administrateur, vous pouvez créer des types d'accès supplémentaires, par exemple pour des dossiers partagés d'applications Web d'intranet ou de l'application Active Directory (AD).

Il est possible de définir plusieurs accès. Vous devez donc les classer en accès couramment disponibles ou utiliser des catégories pour permettre des recherches plus pertinentes des accès moins fréquents.

Création de types d'accès

En tant qu'administrateur, vous pouvez créer des types d'accès supplémentaires, par exemple pour des dossiers partagés d'applications Web d'intranet ou de l'application Active Directory (AD).

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Il est possible de définir plusieurs accès. Vous devez donc les classer en accès couramment disponibles ou utiliser des catégories pour permettre des recherches des accès moins fréquents.

Pour créer un type d'accès dans la structure arborescente, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer les types d'accès** pour afficher la page Gérer les types d'accès. Cette page répertorie les types d'accès par défaut.
2. Sur la page Gérer les types d'accès, cliquez sur l'icône en regard du noeud **Types d'accès**.
3. Cliquez sur **Créer le type** pour afficher la page Créer un type d'accès.
4. Dans la page Créer un type d'accès, exécutez les étapes suivantes :

a. Dans la zone **Clé du type d'accès**, indiquez un nom de clé, `Payroll`, par exemple.
b. Dans la zone **Description**, entrez une description du type d'accès.

5. Cliquez sur **OK** pour sauvegarder le type d'accès.

Résultats

Un message s'affiche indiquant que vous avez créé un type d'accès. La page Gérer les types d'accès affiche le nouveau type d'accès dans la structure arborescente.

Que faire ensuite

Il pourrait également être nécessaire de mettre à jour le regroupement de ressources `CustomLabels.properties` afin de fournir le libellé d'affichage de ce type d'accès. Voir la rubrique `CustomLabels.properties` dans le document *IBM Security Identity Manager - Guide de référence*.

Les utilisateurs peuvent demander accès au nouveau type d'accès.

Créez d'autres types d'accès ou cliquez sur **Fermer**.

Modification des types d'accès

En tant qu'administrateur, vous pouvez modifier des types d'accès, par exemple pour des dossiers partagés d'applications Web d'intranet ou de l'application Active Directory (AD).

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vérifiez que vous avez créé au moins un type d'accès dans la structure arborescente. Voir «Création de types d'accès», à la page 65.

Pourquoi et quand exécuter cette tâche

Les noeuds que vous pouvez sélectionner dépendent de l'emplacement ou du lien hyper texte que vous sélectionnez dans la structure arborescente.

Pour changer un type d'accès dans la structure arborescente, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer les types d'accès** pour afficher la page Gérer les types d'accès. Cette page répertorie les types d'accès par défaut.
2. Sur la page Gérer les types d'accès, cliquez sur l'icône en regard du noeud **Types d'accès** puis sélectionnez **Modifier**. Vous pouvez également cliquer sur un type d'accès. La page de modification des types d'accès s'affiche.
3. Sur cette page, modifiez la description dans la zone **Description**. Vous pouvez fournir une description associée à la clé de type d'accès.

Remarque : La valeur de la zone **Clé du type d'accès** est en lecture seule.

4. Cliquez sur **OK** pour sauvegarder le type d'accès.

Résultats

Un message s'affiche indiquant que vous avez modifié un type d'accès. La page Gérer les types d'accès affiche le type d'accès modifié dans la structure arborescente.

Que faire ensuite

Les utilisateurs peuvent demander accès au nouveau type d'accès.

Changez d'autres types d'accès ou cliquez sur **Fermer**.

Suppression de types d'accès

En tant qu'administrateur, vous pouvez supprimer les types d'accès qui ne sont plus nécessaires dans votre organisation.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vous devez supprimer toutes les définitions d'accès pour un type d'accès avant de pouvoir supprimer un type d'accès.

Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas supprimer un type d'accès s'il existe des définitions d'accès pour ce type d'accès.

Pour supprimer un type d'accès dans la structure arborescente, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer les types d'accès** pour afficher la page Gérer les types d'accès. Cette page répertorie les types d'accès par défaut.
2. Sur la page Gérer les types d'accès, cliquez sur l'icône en regard du noeud **Types d'accès** à supprimer. Cliquez ensuite sur **Supprimer** pour afficher la page Confirmer. Vous ne pouvez pas supprimer un noeud de type d'accès qui possède des éléments enfant ou une association de groupe ou de rôle. Vous devez tout d'abord supprimer les éléments enfant ou l'association de groupe ou de rôle avant de supprimer le type d'accès.
3. Dans la page Confirmer, cliquez sur **Supprimer** pour supprimer le type d'accès ou cliquez sur **Annuler**.

Résultats

Un message s'affiche indiquant que vous avez supprimé un type d'accès. La structure arborescente de la page Gérer les types d'accès n'inclut plus le type d'accès supprimé.

Que faire ensuite

Créez ou changez les types d'accès, supprimez les types d'accès supplémentaires ou cliquez sur **Fermer**.

Chapitre 4. Configuration de l'accès partagé

Vous pouvez définir des paramètres de configuration pour l'accès partagé selon les besoins de votre déploiement. Vous pouvez également définir des paramètres par défaut pour les droits d'accès, configurer un serveur de coffre de droits d'accès externe, définir un ID unique pour un service et personnaliser plusieurs opérations différentes.

Configuration des paramètres par défaut des droits d'accès

Indiquez les paramètres par défaut pour chaque droit d'accès ajouté au coffre.

Pourquoi et quand exécuter cette tâche

La console d'administration prend en charge l'ajout de droits d'accès utilisateur dans un coffre de droits d'accès. Lors de cette opération d'ajout, vous pouvez appliquer des valeurs par défaut pour chaque paramètre de droits d'accès. Utilisez cette tâche pour définir la valeur par défaut pour chaque paramètre.

Remarque : Certains paramètres par défaut peuvent être remplacés au niveau des droits d'accès mais d'autres ne peuvent être modifiés qu'à un niveau global.

Procédure

Pour configurer les paramètres par défaut des droits d'accès, procédez comme suit :

1. Dans l'arborescence de navigation, sélectionnez **Gérer les accès partagés** > **Configurer les paramètres de droits d'accès par défaut**. La page Configurer les paramètres de droits d'accès par défaut s'affiche.
2. Sous **Paramétrage des droits d'accès**, sélectionnez l'une des options suivantes pour définir les processus de réservation et de libération pour les comptes. Voir l'aide en ligne pour obtenir plus de détails sur les paramètres individuels.

   Exiger le processus de restitution et de réservation pour les ID partagés
   Sélectionnez cette option pour indiquer que par défaut, les utilisateurs doivent restituer des droits d'accès partagés avant de les utiliser. Lors de la sélection de cette option, définissez les options suivantes :

   Modification du mot de passe lors de la restitution
   Sélectionnez la case à cocher pour changer le mot de passe.

   Durée maximale de réservation
   Planifiez le nombre maximal d'heures, de jours ou de semaines durant lesquelles des droits d'accès peuvent être réservés.

   Déterminez si les droits d'accès sont activés pour la recherche de réservation
   Sélectionnez la case à cocher **Activer la recherche de réservation** afin d'activer les droits d'accès pour une recherche de réservation. Une recherche des processus de réservation est alors effectuée dans l'interface utilisateur en libre service.

Indiquez si le mot de passe des droits d'accès est visible pour l'utilisateur en libre service
Sélectionnez la case à cocher permettant d'afficher le mot de passe**c** sur l'interface utilisateur en libre service.

Opération de réservation
Dans la zone **Nom de l'opération**, entrez un nom d'opération pour définir une opération de cycle de vie globale et démarrer l'extension de flux de travaux de réservation.

Traitement de l'expiration des crédits-bails

Envoyer une notification de violation
Sélectionnez cette option pour envoyer une notification lorsque le système détecte que les droits d'accès arrivés à expiration sont réservés.

Envoyer une notification de violation et restituer
Sélectionnez cette option lorsque vous souhaitez que le système notifie les destinataires que les droits d'accès sont arrivés à expiration et qu'il restitue automatiquement ces derniers.

Modèle de notification
Cliquez sur ce lien pour afficher ou changer le modèle de message électronique utilisé par le système pour générer la notification à propos des droits d'accès arrivés à expiration.

Envoyer les notifications à
Sélectionnez un destinataire dans la liste.

Rechercher les baux arrivés à expiration tou(te)s les
Planifiez une fréquence de vérification des baux de droits d'accès arrivés à expiration par le système.

Remarque : La durée entrée doit être égale ou supérieure à la durée définie pour la vérification des baux arrivés à expiration. Vous pouvez, par exemple, définir un intervalle d'une heure pour la vérification des baux arrivés à expiration. Vous devez définir un délai d'au moins une heure pour envoyer des notifications aux destinataires chargés des baux arrivés à expiration.

Envoyer les notifications au moins tou(te)s les
Planifiez une fréquence d'envoi de notifications pour informer les destinataires des baux arrivés à expiration.

Ne pas exiger le processus de restitution et de réservation pour les ID partagés
Sélectionnez cette option pour indiquer que, par défaut, les utilisateurs n'ont pas besoin de réserver de droits d'accès partagés avant de les utiliser.

Indiquez si le mot de passe des droits d'accès est visible pour l'utilisateur en libre service
Sélectionnez la case à cocher permettant d'afficher le mot de passe sur l'interface utilisateur en libre service.

Pas de partage des droits d'accès
Sélectionnez cette option pour indiquer que, par défaut, les droits d'accès ajoutés au coffre de droits d'accès ne sont pas accessibles via une règle d'accès partagé.

3. Cliquez sur **Soumettre** pour sauvegarder les paramètres de configuration.
4. Dans la page Réussite, cliquez sur **Fermer**.

Personnalisation du modèle de formulaire de service afin d'inclure l'attribut eruri (identificateur unique)

Mettez à jour le modèle de formulaire pour le service de ressources géré afin d'inclure une zone pour l'identificateur unique utilisé pour la connexion à la ressource gérée.

Pourquoi et quand exécuter cette tâche

Vous devez suivre cette procédure pour chaque type de service que vous souhaitez configurer pour l'accès partagé. Les formulaires par défaut pour les services, les groupes et les comptes dépendent de l'adaptateur.

Pour pouvoir effectuer cette tâche, vous devez être administrateur système.

Procédure

Pour ajouter l'attribut `eruri` au modèle de formulaire de service, procédez comme suit :

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Concevoir des formulaires**. L'applet Java **Concevoir des formulaires** s'affiche.
2. Facultatif : Pour ouvrir l'applet dans une autre fenêtre de navigateur, cliquez sur **Lancer comme fenêtre séparée**.
3. Dans le panneau de gauche, cliquez deux fois sur le dossier de catégorie **Service** pour afficher les profils d'objet.
4. Dans le panneau de gauche, cliquez deux fois sur un profil, tel **Profil Linux POSIX**, pour ouvrir le modèle pour ce profil. Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.
5. Dans la zone **Liste d'attributs**, sélectionnez l'attribut **eruri** puis cliquez sur l'icône **Ajouter une ligne**  . L'attribut `$eruri` est ajouté au modèle de formulaire.
6. Sélectionnez l'attribut `$eruri` puis cliquez sur l'icône **Liste modifiable**  . L'attribut `$eruri` comporte plusieurs valeurs.
7. Dans la section **Propriétés**, entrez un nouveau nom de libellé dans la zone **Libellé**. Entrez, par exemple `Identificateur unique`. Le nom de libellé entré s'affiche dans le formulaire de service lorsque vous créez ou changez un service s'appuyant sur ce profil. Par exemple, le nom de libellé s'affiche dans un service Linux POSIX que vous avez créé ou modifié.
8. Cliquez sur l'icône **Enregistrer le modèle de formulaire**  pour enregistrer les modifications puis cliquez sur **OK**.
9. Facultatif : Si vous avez ouvert l'applet Java **Concevoir des formulaires** dans une autre fenêtre, fermez cette dernière.

10. Cliquez sur **Fermer** pour fermer l'applet **Concevoir des formulaires**.

Que faire ensuite

Créez une instance de service à partir du profil (Linux POSIX, par exemple) et renseignez la nouvelle zone **Identificateur unique**.

Tâches associées :

Définition de l'identificateur unique de service

Création de services

Configuration d'un serveur de coffre de droits d'accès externe

Indiquez les propriétés requises pour configurer un serveur de coffre de droits d'accès externe.

Pourquoi et quand exécuter cette tâche

Configurez IBM Security Identity Manager pour établir une connexion en tant que client de coffre de droits d'accès à un serveur de coffre de droits d'accès externe. Ce dernier fournit des services KMIP (Key Management Interoperability Protocol).

Vous devez spécifier des valeurs pour les paramètres dans plusieurs fichiers de configuration. Vous devez ensuite configurer la communication SSL entre le client et le serveur.

Procédure

Pour configurer un serveur de coffre de droits d'accès externe, procédez comme suit :

1. Enregistrez le fournisseur de données confidentielles en éditant le fichier de propriétés *ISIM_HOME*/data/pim.properties. Indiquez le nom du fournisseur qui implémente l'interface SecretDataProvider :

   ```
   secret.data.provider=com.ibm.itim.pim.credstore.TKLMExternalCredProvider
   ```

2. Enregistrez le gestionnaire qui synchronise les droits d'accès entre IBM Security Identity Manager et le serveur de coffre des droits d'accès. Editez le fichier *ISIM_HOME*/data/dataSynchronization.properties pour spécifier ou remplacer le nom de la classe de gestionnaire qui implémente l'interface DirectoryObjectSynch pour les objets de droits d'accès. Voir l'entrée suivante :

   ```
   erCredential=com.ibm.itim.dataservices.synch.CredentialSynchHandler,
   com.ibm.itim.pim.credstore.CVCredentialSynchHandler
   ```

   Remarque : L'exemple est présenté sur plusieurs lignes pour une meilleure lisibilité. Dans le fichier de propriétés, entrez les valeurs sur une seule ligne sans espace après la virgule.

3. Créez le fichier CVClient.properties. Placez-le dans le répertoire de votre choix :
   a. Attribuez au paramètre host le nom de l'ordinateur qui exécute le serveur du coffre de droits d'accès.
   b. Attribuez au paramètre port le numéro de port sur lequel s'exécute le serveur de coffre de droits d'accès.

Tableau 20. Fichier `CVClient.properties` exemple

```
protocol=ssl
host=myCVserver.mySubnet.example.com
port=19696
path=/cvsvc/kmip.html
debug=all
debug.output.file=logs/kmip/tklm_debug.log
Audit.event.outcome=success,failure
Audit.eventQueue.max=0
Audit.handler.file.name=logs/kmip/audit/tklm_audit.log
Audit.handler.file.size=10000
Audit.event.types=runtime,authorization,authorization_terminate,
resource_management,key_management
```

4. Editez le fichier *ISIM_HOME*/data/cvserver.properties.

   Définissez la propriété KMIPConfigProperties en fonction de l'emplacement dans lequel vous avez placé le fichier CVClient.properties Par exemple,

   ```
   KMIPConfigProperties=/opt/cvserver/CVClient.properties
   ```

   Il n'est pas nécessaire de spécifier de valeurs pour les autres propriétés du fichier cvserver.properties. Pour obtenir une description des propriétés facultatives, voir tableau 21.

Tableau 21. Propriétés facultatives dans cvserver.properties

Propriété	Description
javax.net.ssl.trustStore	Spécifie le nom et l'emplacement du fichier de clés certifiées pour les transactions SSL (Secure Socket Layer). Cette valeur correspond au fichier clientTrust généré lors de la configuration du serveur de coffre de droits d'accès. Exemple : `javax.net.ssl.trustStore= /opt/cvserver/trustStore.jks`
javax.net.ssl.trustStorePassword	Spécifie le mot de passe pour l'accès au fichier de clés certifiées. Exemple : `javax.net.ssl.trustStorePassword=password`
javax.net.ssl.keyStore	Spécifie le nom et l'emplacement du fichier de clés pour les transactions SSL (Secure Socket Layer). Cette valeur correspond au fichier clientStore généré lors de la configuration du serveur de coffre de droits d'accès. Exemple : `javax.net.ssl.keyStore=/opt/cvserver/keyStore.jks`
javax.net.ssl.keyStorePassword	Spécifie le mot de passe permettant d'accéder au fichier de stockage des clés. Exemple : `javax.net.ssl.keyStorePassword=password`
javax.net.ssl.keyStoreType	Spécifie le type de fichier de clés certifiées spécifié pour `javax.net.ssl.trustStore`. Exemple : `javax.net.ssl.trustStoreType=jks`

Voir tableau 22, à la page 74 pour obtenir un exemple du fichier cvserver.properties avec des propriétés facultatives définies.

Tableau 22. Fichier de propriétés KMIP exemple

```
KMIPConfigProperties=/opt/cvserver/CVClient.properties
javax.net.ssl.trustStore=/newcerts/clientTrust
javax.net.ssl.trustStorePassword=myPassw0rd
javax.net.ssl.keyStore=/newcerts/clientStore
javax.net.ssl.keyStorePassword=myPassw0rd
javax.net.ssl.keyStoreType=jks
javax.net.ssl.trustStoreType=jks
```

5. Configurez SSL sur l'ordinateur qui héberge le client de coffre de droits d'accès et sur l'ordinateur qui héberge le serveur de coffre de droits d'accès.

   Les serveurs WebSphere Application Server de chaque ordinateur doivent se faire confiance mutuellement.

   Configurez SSL sur l'ordinateur sur lequel le client de coffre de droits d'accès est déployé. Par exemple, le serveur IBM Security Identity Manager peut être déployé en tant que client de coffre de droits d'accès sur un ordinateur et le serveur de coffre de droits d'accès peut être déployé sur un autre ordinateur. Dans cet exemple, suivez la procédure ci-dessous sur l'ordinateur qui héberge le serveur IBM Security Identity Manager :

   a. Connectez-vous à la console d'administration de WebSphere Application Server.
   b. Sélectionnez **Sécurité** > **Certificat SSL et gestion des clés** > **Magasins de clés et certificats** > **NodeDefaultTrustStore** > **Certificats de signataires**.
   c. Cliquez sur l'option d'extraction à partir d'un port.
   d. Dans les zones **Hôte** et **Port**, entrez les informations pour le serveur de droits d'accès externe.
   e. Dans la zone **Alias**, entrez un nom d'alias.
   f. Cliquez sur **Récupérer les informations du signataire** puis cliquez sur **OK**.
   g. Enregistrez les modifications de configuration puis redémarrez WebSphere Application Server.

6. Configurez SSL sur l'ordinateur où le serveur de coffre de droits d'accès est déployé.

   Dans un environnement en cluster WebSphere Application Server, chaque noeud peut être associé à différents paramètres SSL. C'est pourquoi, vous devez mettre à jour le fichier de clés certifiées pour chaque noeud. Répétez la procédure pour chaque noeud :

   a. Connectez-vous à la console d'administration de WebSphere Application Server.
   b. Sélectionnez **Sécurité** > **Certificat SSL et gestion des clés** > **Magasins de clés et certificats** > **NodeDefaultTrustStore** > **Certificats de signataires**.
   c. Cliquez sur l'option d'extraction à partir d'un port.
   d. Dans les zones **Hôte** et **Port**, entrez les valeurs pour le serveur de coffre de droits d'accès.
   e. Dans la zone **Alias**, entrez un nom d'alias.
   f. Cliquez sur **Récupérer les informations du signataire** puis cliquez sur **OK**.
   g. Mettez à jour `trustStorePath` dans *`ISIM_HOME`*`/data/KMIPServer.properties`.

      Editez `KMIPServer.properties` afin de définir la valeur de `trustStorePath`, de telle sorte qu'elle corresponde au chemin de **NodeDefaultTrustStore**.

      La valeur de trustStorePath doit correspondre à la valeur du fichier de clés certifiées pour le noeud sur lequel le serveur de coffre de droits d'accès est exécuté. La valeur de **NodeDefaultTrustStore** est généralement la valeur du

fichier de clés certifiées par défaut mais les administrateurs peuvent changer cette valeur. Vérifiez que vous indiquez le chemin correct.

Dans un environnement en cluster, un serveur de coffre de droits d'accès est installé sur chaque noeud. Toutefois, lorsque votre déploiement inclut un serveur IBM Security Identity Manager qui se trouve hors du cluster, vous configurez ce serveur IBM Security Identity Manager de telle sorte qu'il utilise le serveur de coffre de droits d'accès sur un seul noeud du cluster. Pour activer l'utilisation de ce coffre sur un noeud spécifique, vous devez définir `trustStorePath` de telle sorte qu'il corresponde à la valeur de **NodeDefaultTrustStore**.

h. Editez *ISIM_HOME*`/data/KMIPServer.properties` pour permettre au serveur de coffre de droits d'accès d'utiliser SSL.

1) Définissez `KMIPEnableSSL=true`.

   La valeur par défaut est false.

2) Définissez le port de telle sorte qu'il utilise les communications SSL. Par exemple, `KMIPSSLServerPort=19696`.

Remarque : Sur l'ordinateur qui héberge le serveur de coffre de droits d'accès externe, la valeur du port de serveur SSL KMIP doit correspondre à la valeur configurée sur l'ordinateur qui héberge le client de coffre de droits d'accès.

Les valeurs suivantes doivent correspondre :

Tableau 23. Paramètres de configuration pour l'activation de SSL et la spécification du port

Ordinateur	Serveur (exemple)	Fichier de configuration	Paramètre
1	Client de coffre de droits d'accès, tel un serveur IBM Security Identity Manager qui se comporte comme un client sur le serveur de coffre de droits d'accès	Fichier de propriétés de configuration KMIP.Le fichier *ISIM_HOME*`/data/cvserver.properties` définit l'emplacement de KMIPConfigProperties. Par exemple : `KMIPConfigProperties= /opt/cvserver/CVClient.properties`	Dans cet exemple, le fichier `CVClient.properties` spécifie le port : `port=19696`
2	Serveur de coffre de droits d'accès externe. Par exemple, une installation séparée d'IBM Security Identity Manager déployée uniquement pour se comporter en tant que serveur de coffre de droits d'accès externe.	*ISIM_HOME*`/data/KMIPServer.properties`	`KMIPEnableSSL=true` `KMIPSSLServerPort=19696`

i. Enregistrez les modifications de configuration puis redémarrez WebSphere Application Server.

Configuration avancée pour l'accès partagé

Vous pouvez utiliser les tâches de configuration avancée pour personnaliser l'accès partagé afin de prendre en charge les cas d'utilisation dans votre déploiement

Voir les rubriques suivantes :

- «Personnalisation de l'opération de réservation»
- «Approbation et recertification d'accès partagé»
- «Personnalisation du formulaire de réservation», à la page 77

Personnalisation de l'opération de réservation

Le module d'accès partagé prend en charge à la fois la réservation synchrone et la réservation asynchrone des comptes partagés. La réservation synchrone est activée par défaut. Si vous souhaitez utiliser la réservation asynchrone, vous devez l'activer et la configurer.

Pour activer la réservation asynchrone, vous devez définir une opération de cycle de vie globale pour démarrer l'extension de flux de travaux de réservation. Vous devez également configurer le nom de l'opération dans les paramètres globaux pour le module d'accès partagé.

IBM Security Identity Manager fournit un code exemple qui présente comment effectuer la configuration. L'exemple présente comment définir une opération de réservation avec ou sans le noeud RFI suivi de l'extension de réservation.

Pour plus d'informations, voir l'exemple relatif à la réservation asynchrone d'accès partagé dans *ISIM_HOME*\extensions\6.0\examples\workflow\sa_checkout.

Approbation et recertification d'accès partagé

Vous pouvez ajouter un processus d'approbation à l'opération par défaut pour l'ajout de droits d'accès au coffre. Vous pouvez également définir un flux de travaux personnalisé pour certifier à nouveau les droits d'accès dans le coffre.

Approbation pour l'ajout de droits d'accès au coffre

Le module d'accès partagé utilise le module d'opération de cycle de vie pour ajouter des droits d'accès au coffre. L'opération par défaut addCredentialToVault n'inclut pas l'approbation mais peut être personnalisée pour intégrer l'activité d'approbation.

IBM Security Identity Manager prend en charge une opération globale utilisée par tous les droits d'accès, quels que soient les services, le type de service ou l'unité organisationnelle à laquelle appartient le compte.

IBM Security Identity Manager fournit un exemple qui indique comment ajouter le processus d'approbation. Pour plus d'informations, voir l'exemple concernant l'approbation pour l'ajout de droits d'accès au coffre (accès partagé) dans *ISIM_HOME*\extensions\6.0\examples\workflow\sa_addToVault.

Recertification des droits d'accès partagés

Vous pouvez utiliser le module d'accès partagé pour gérer les droits d'accès dans le coffre. Vous pouvez souhaiter revalider régulièrement les droits d'accès dans le coffre. Par défaut, la recertification de ces données n'est pas configurée. Vous

pouvez configurer la recertification en définissant une règle de cycle de vie pour le type d'entité de compte. La règle filtre les comptes dans le coffre et démarre une opération de flux de travaux selon les planifications.

IBM Security Identity Manager fournit un exemple qui indique comment ajouter la recertification. Ce dernier présente comment effectuer les actions suivantes :

- Définition d'un flux de travaux personnalisé pour recertifier les droits d'accès dans le coffre
- Définition d'une règle de cycle de vie pour filtrer les comptes dans le coffre
- Association de la règle au flux de travaux personnalisé

Dans le flux de travaux personnalisé exemple, les droits d'accès sont supprimés du coffre si l'activité d'approbation de recertification est refusée par le participant.

Pour plus d'informations, voir l'exemple *ISIM_HOME*\extensions\6.0\examples\workflow\sa_recertifyCerdential.

Personnalisation du formulaire de réservation

Vous pouvez personnaliser le formulaire utilisé pour la réservation des comptes partagés. Vous pouvez ajouter des attributs supplémentaires à renseigner lors de la réservation. Cette personnalisation augmente la responsabilité individuelle lorsque les droits d'accès sont partagés.

Pourquoi et quand exécuter cette tâche

Pour pouvoir effectuer cette tâche, vous devez être administrateur système. Le formulaire de réservation est global pour tous les accès partagés. Lorsque vous personnalisez le formulaire de réservation, vos modifications ont des conséquences sur la réservation pour l'accès partagé. Suivez cette procédure pour ajouter ou supprimer des attributs dans le modèle de formulaire de réservation.

Procédure

1. Connectez-vous à la console d'administration, sélectionnez **Configurer le système>Concevoir des formulaires**.

   L'applet Java Concevoir des formulaires s'affiche.
2. Facultatif : pour ouvrir l'applet dans une autre fenêtre de navigateur, cliquez sur **Lancer comme fenêtre séparée**.
3. Dans le panneau de gauche, cliquez deux fois sur le dossier de catégorie “Bail de droits d'accès” pour sélectionner le formulaire correspondant. Cliquez deux fois sur ce dernier pour l'ouvrir dans Form Designer.
4. Sélectionnez l'option d'attribut personnalisé puis cliquez sur l'icône **Ajouter une ligne** pour l'ajouter au formulaire.
5. Cliquez sur l'icône correcte pour sélectionner le widget. Définissez les attributs requis pour chaque widget. Définissez également le format et les contraintes pour chaque attribut.
6. Répétez les deux étapes précédentes pour ajouter tous les attributs personnalisés.
7. Cliquez sur l'icône **Enregistrer le modèle de formulaire** pour sauvegarder les modifications. Cliquez sur **OK**.
8. Facultatif : Si vous avez ouvert l'applet Java Concevoir des formulaires dans une autre fenêtre, fermez cette dernière.
9. Cliquez sur **Fermer** pour fermer l'applet Concevoir des formulaires.

Chapitre 5. Règles d'adoption globales

Une *règle d'adoption* est utilisée pendant la synchronisation pour déterminer le propriétaire d'un compte. Une *règle d'adoption globale* est définie pour un type de service ou pour tous les types de service, pour l'ensemble du système. Les règles d'adoption globales sont applicables à toutes les instances de service si aucune règle d'adoption n'est définie pour le service spécifique.

La règle d'adoption globale par défaut attribue un compte à un utilisateur si l'attribut d'ID utilisateur du compte correspond à l'attribut UID utilisateur IBM Security Identity Manager. Une règle d'adoption spécifique à un service prévaut sur la règle d'adoption globale.

Pour plus d'informations concernant les migrations, voir Known issues for migrating to Tivoli Identity Manager Version 5.1.

Création d'une règle d'adoption globale

Vous pouvez ajouter une règle personnalisée pour générer des mots de passe à l'aide du serveur IBM Security Identity Manager.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Pour créer une règle d'adoption globale, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Règles d'adoption globales**.
2. Dans la page Règles d'adoption globales, dans le tableau **Règles d'adoption**, cliquez sur **Créer**.
3. Dans la fenêtre Gérer les règles d'adoption, dans la page Général, saisissez un nom pour votre règle d'adoption. Vous pouvez aussi ajouter une description.
4. Cliquez sur l'onglet Type de service et sélectionnez un type de service spécifique à associer à la règle. Vous devez indiquer au moins un type de service pour la règle d'adoption globale. Vous ne pouvez pas associer plusieurs règles d'adoption globales à un type de service.
5. Cliquez sur l'onglet Règle et indiquez une règle personnalisée pour régir les attributs que la règle d'adoption utilise pour établir la correspondance entre les comptes et les utilisateurs. Si vous choisissez de définir des correspondances, cliquez sur **Ajouter une zone de correspondance** pour sélectionner les attributs de compte et d'utilisateur qui doivent correspondre pendant la synchronisation. La liste déroulante des attributs d'utilisateur fournit quelques combinaisons d'attributs couramment utilisées pouvant servir à définir la correspondance. Par exemple la première lettre du nom indiqué plus le nom de famille ou le nom

indiqué plus la première lettre du nom de famille. Si votre règle d'adoption est plus complexe, vous pouvez sélectionner le chemin plus avancé en sélectionnant **Saisie d'un script**. Si vous avez défini des correspondances, les scripts associés sont remplis pour vous dans la zone de définition de script.

Important : Si vous choisissez de fournir un script, le serveur Security Identity Manager ne vérifie pas que le script JavaScript est correct. Vérifiez le script JavaScript avant de l'utiliser pour définir la règle.

6. Cliquez sur **OK** pour enregistrer les modifications.
7. Dans la page Réussite, cliquez sur **Fermer**. La nouvelle règle d'adoption globale s'affiche sur la page Règles d'adoption globales. Cette règle d'adoption globale peut être modifiée et supprimée.

Modification d'une règle d'adoption globale

Un administrateur peut modifier une règle d'adoption globale qui est définie pour un type de service.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

L'effet des modifications apportées à une règle d'adoption apparaît lorsque la synchronisation suivante est exécutée. La modification d'une règle d'adoption existante n'a pas d'effet sur les comptes existants du service ou type de service considéré. Les modifications sont sans effet sur les comptes déjà adoptés. Seuls les comptes orphelins nouveaux et existants sont adoptés selon la nouvelle règle.

Pour modifier une règle d'adoption globale, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Règles d'adoption globales**.
2. Dans le tableau **Règles d'adoption globales**, recherchez et sélectionnez une règle d'adoption à modifier, puis cliquez sur **Modifier**.
3. Dans la page Règles d'adoption globales, modifiez les informations des pages Général, Service ou Règle.
4. Cliquez sur **OK** pour enregistrer les modifications.
5. Sur la page Réussite, cliquez sur **Fermer**.

Suppression d'une règle d'adoption globale

Un administrateur peut supprimer une règle d'adoption globale définie pour un type de service.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

La suppression d'une règle d'adoption existante n'a pas d'effet sur les comptes existants du type de service considéré.

Pour supprimer une règle d'adoption globale, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Règles d'adoption globales**.
2. Dans le tableau **Règles d'adoption globales**, recherchez et sélectionnez la règle d'adoption à supprimer, puis cliquez sur **Supprimer**.
3. Dans la page Confirmation, examinez la règle d'adoption à supprimer et cliquez sur **Supprimer**.
4. Sur la page Réussite, cliquez sur **Fermer**.

Chapitre 6. Configuration du bureau de poste

Le bureau de poste fournit un mécanisme de réduction du nombre de notifications par courrier électronique reçues par un utilisateur et relatives à des tâches similaires dans IBM Security Identity Manager.

Présentation

Vous pouvez configurer le bureau de poste pour la collecte de notifications similaires pendant une période définie. La configuration regroupe ces messages électroniques dans une notification envoyée à un utilisateur. Dans le concepteur du flux de travaux, vous utilisez la zone **Rubrique E-mail de groupe** dans la définition de chaque activité manuelle pour déterminer les tâches similaires afin de regrouper les notifications par courrier électronique.

Supposons que le bureau de poste est activé. Si l'option **Utiliser la rubrique E-mail de groupe** est activée dans les activités manuelles qui génèrent des notifications, le bureau de poste intercepte les notifications par courrier électronique générées par le système pour ces activités manuelles et les retient pendant l'intervalle indiqué. A l'expiration de cet intervalle, le bureau de poste utilise le modèle d'agrégation des messages pour agréger toutes les notifications comportant la même valeur **Rubrique E-mail de groupe** en un même courrier électronique pour chaque destinataire de message. L'emplacement préféré du destinataire, indiqué dans l'objet d'utilisateur, est respecté. Ce processus réduit le volume des messages électroniques individuels reçus par un utilisateur qui correspondent aux notifications pour une même valeur **Rubrique E-mail de groupe**.

Le bureau de poste utilise la valeur **Rubrique E-mail de groupe**, située dans l'onglet **Notification** du panneau de configuration d'activités manuelles, afin de déterminer les messages à regrouper. Toutes les notifications générées à l'aide de la même valeur **Rubrique E-mail de groupe** sont regroupées durant l'intervalle de temps indiqué. Cette zone peut être n'importe quelle chaîne, mais la valeur par défaut est l'ID activité. Cette zone accepte toutes les balises de contenu dynamique et JavaScript qui ont pour résultat l'exécution d'une chaîne.

Supposons que l'intervalle de collecte expire et que les notifications sont agrégées. S'il existe une seule notification pour une valeur **Rubrique Email de groupe** et une adresse électronique, ce message sera envoyé sous sa forme d'origine. Le modèle de message du bureau de poste n'est sera pas appliqué. Bien que la notification soit envoyée sous sa forme d'origine, son envoi est différé jusqu'à l'expiration du délai de collecte du bureau de poste.

Il peut exister des erreurs lors de la tentative d'agrégation des messages électroniques individuels. Les messages sont envoyés sous leur forme d'origine et un message d'erreur est inscrit dans le journal. Ce processus signifie que l'envoi des notifications pourrait être différé, mais cela ne devrait pas entraîner de perte de notifications. Le bouton **Test** qui se trouve sur la page Bureau de poste est utile pour résoudre les erreurs du modèle.

Exemple de notification par courrier électronique

Le modèle par défaut génère une notification par courrier électronique similaire à ce message :

```
Subject: You have 3 work items requiring your attention.

Body:
You have 3 work items requiring your attention.

Here are the email subjects:
This is subject 1
This is subject 2
This is subject 3

Here are the email message bodies:
This is the text body 1
This is the text body 2
This is the text body 3
```

Le modèle peut comprendre une balise de contenu dynamique et du code JavaScript valides. De plus, le bureau de poste dispose d'un ensemble de balises de contenu dynamique et d'extensions JavaScript personnalisées.

Personnalisation du modèle de messagerie du bureau de poste

Vous pouvez activer ou désactiver le bureau de poste et définir l'intervalle de temps que le bureau de poste utilise pour collecter les messages à agréger. Vous pouvez également personnaliser le modèle de message utilisé pour générer le message unifié qui est envoyé aux destinataires.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Lorsque vous activez le bureau de poste, toutes les notifications par courrier électronique sont stockées jusqu'à l'intervalle de temps que vous indiquez. A ce moment, les notifications sont regroupées dans un seul courrier électronique qui est envoyé aux destinataires.

Le modèle de message du bureau de poste peut utiliser le contenu dynamique. Le contenu dynamique inclut des balises de contenu dynamique pour les messages et le code JavaScript. Il inclut également des balises qui remplacent des variables par d'autres valeurs ou renvoient à une propriété qui permet la traduction à l'aide d'un fichier `CustomLabels.properties`.

Ce modèle est appliqué à l'ensemble des messages de notification conservés par le système pour une valeur **Rubrique E-mail de groupe** donnée et pour un destinataire du message. Ce modèle peut être simple ou complexe, au choix. La valeur **Rubrique E-mail de groupe** est définie dans le concepteur de flux de travaux.

Pour activer le bureau de poste et configurer un modèle de courrier de regroupement de bureau de poste, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Bureau de poste**. La page Bureau de poste s'affiche.
2. Dans la page Bureau de poste, cochez la case **Activer le transfert de stockage**.
3. Dans la zone **Intervalle de collecte**, entrez le nombre de minutes souhaitées avant que le bureau de poste ne regroupe les messages électroniques stockés et ne les envoie aux destinataires. La valeur de l'intervalle de collecte doit être un nombre entier compris entre 5 et 10080.
4. Dans la zone **Objet**, entrez le texte indiquant l'objet de la notification par courrier électronique envoyée comme message unifié au lieu d'être envoyée comme courrier électronique séparé. L'objet peut contenir du texte brut et des balises de contenu dynamique.
5. Dans la zone **Corps texte en clair**, entrez le texte à afficher dans le corps du message unifié. Le contenu peut être constitué de texte brut, de balises de contenu dynamique et de code JavaScript. Ce contenu est affiché pour les destinataires du message qui ne voient pas les notifications par courrier électronique HTML.
6. Dans la zone **Corps XHTML**, entrez le texte à afficher dans le corps de la notification par courrier électronique au format HTML. Le contenu peut être constitué de texte brut, de balises de contenu dynamique et de code JavaScript. Ce contenu est affiché pour les destinataires du message qui voient les notifications par courrier électronique HTML. Pour obtenir un regroupement correct des corps en XHTML de modèles de messages individuels à l'aide du modèle de regroupement de courriers électroniques du bureau de poste, utilisez un attribut facultatif 'escapeentities'. Cet attribut se trouve dans la balise <JS> du modèle de corps en XHTML du bureau de poste. Définissez la valeur sur `false`. Pour plus de détails, consultez le modèle de regroupement de courriers électroniques du bureau de poste.
7. Cliquez sur le bouton **OK** pour enregistrer les modifications, puis cliquez sur **Fermer**.

Résultats

A l'expiration du prochain intervalle, les notifications fusionnées sont agrégées et envoyées sous forme d'une notification par courrier électronique.

Que faire ensuite

Testez le modèle de regroupement de messages du bureau de poste que vous avez créé avant de l'utiliser pour agréger des notifications par courrier électronique qui seront envoyées aux participants à une activité.

Balises personnalisées du contenu dynamique du bureau de poste

Le bureau de poste définit un ensemble de balises personnalisées permettant de simplifier la création du modèle de message unifié. Ce modèle est un modèle d'interface utilisateur permettant de définir la façon dont plusieurs notifications par courrier électronique sont regroupées dans une seule notification adressée à l'utilisateur.

Les balises personnalisées du contenu dynamique du bureau de poste suivantes peuvent être utilisées pour obtenir des données :

<POGetAllBodies/>

Renvoie une chaîne contenant le corps du texte de chacune des notifications d'origine, séparées par une nouvelle ligne. Par exemple :

```
You have the following ToDo items in Identity Manager.
Here are the notification bodies <POGetAllBodies/>
```

<POGetAllSubjects/>

Renvoie tous les objets des notifications associées à la notification par courrier électronique unifiée sous forme d'une chaîne séparée par un retour à la ligne. Par exemple :

```
You have the following ToDo items in Identity Manager.
Here are the notification subjects. <POGetAllSubjects/>
```

<POGetEmailAddress/>

Renvoie l'adresse électronique correspondant à la destination de la notification par courrier électronique unifiée en tant que chaîne sans nouvelle ligne. Par exemple :

```
This collection of notifications was sent to <POGetEmailAddress/>.
```

<POGetNumOfEmails/>

Renvoie le nombre d'e-mails associés aux notifications par courrier électronique unifiées en tant que chaîne sans nouvelle ligne. Par exemple :

```
You have <POGetNumOfEmails/> ToDo items in Identity Manager.
```

Propriétés des libellés du bureau de poste et des messages

Libellés personnalisés pour les éléments d'interface

Pour personnaliser les libellés des éléments de l'interface graphique de configuration du bureau de poste, il suffit de modifier les propriétés suivantes contenues dans le fichier `Labels.properties` :

- POST_OFFICE_CONFIG=Configuration du bureau de poste
- POST_OFFICE_PROPERTIES_CUE=Modifier les propriétés du bureau de poste
- POST_OFFICE_PATH=Bureau de poste
- GENERAL_TAB=Général
- AGGREGATE_MESSAGE_TAB=Unifier un message
- ENABLE_STORE_FORWARDING_LABEL=Activer le transfert de stockage
- COLLECTION_INTERVAL_LABEL=Intervalle de collecte
- SUBJECT=Objet
- TEXT_BODY=Corps du texte
- HTML_BODY=Corps XHTML
- POST_OFFICE_DONE_ALT=Enregistrer les propriétés du bureau de poste
- POST_OFFICE_CANCEL_ALT=Annuler les modifications

Propriétés personnalisées pour les messages de notification

Les propriétés suivantes peuvent être personnalisées pour des messages de notification du bureau de poste. Ces propriétés constituent des clés de messages pour les balises de contenu dynamique (`<RE>`) comprises dans la configuration du modèle de bureau de poste par défaut.

- postoffice_subject=Vous avez {0} éléments de travaux nécessitant votre attention.
- postoffice_subject_list=Voici les objets des e-mails :
- postoffice_body_list=Voici les corps des messages électroniques :

Extensions du modèle de bureau de poste

Vous trouverez ici des exemples d'utilisation du contenu dynamique et de code JavaScript pouvant être saisi dans la page Bureau de poste.

Objet

```
Identity Manager: You have <POGetNumOfEmails/> work items requiring your attention.
```

Corps texte en clair

```
You have <POGetNumOfEmails/> work items requiring your attention.
The emails are all addressed to: <POGetEmailAddress/>
Here are the email Subjects:
<POGetAllSubjects/>
Here are the email bodies:
<POGetAllBodies/>
Here is the topic fetched using the JavaScript extension:
<JS>
    return PostOffice.getTopic();
</JS>
Here is the recipient's email address fetched using the JavaScript extension:
<JS>
    return PostOffice.getEmailAddress();
</JS>
Here are the email text bodies fetched using the JavaScript extension:
<JS>
       var msgListIterator = PostOffice.getAllEmailMessages().iterator();
       var returnString = "\n";
       while (msgListIterator.hasNext()) {
                    returnString = returnString + msgListIterator.next().getMessage() + "\n"; }
       return returnString;
</JS>
Here is the recipient's surname taken from the Person fetched using the JavaScript extension:
<JS>
        var person = PostOffice.getPersonByEmailAddress(PostOffice.getEmailAddress());
        return "Last: " + person.getProperty("sn")[0] + "\n";
</JS>
```

Corps XHTML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>You have <POGetNumOfEmails/> work items requiring your attention.</title>
</head>
<body>
<POGetNumOfEmails/> notifications have been collected by Identity Manager Post Office
and aggregated below. These indicate you can have up to <POGetNumOfEmails/> work items
requiring your attention.<br />
The notifications were all addressed to: <POGetEmailAddress/><br />
<hr />
Here are the notification Subjects:<br />
<POGetAllSubjects/><br />
<hr />
Here are the notification bodies: <br />
<POGetAllBodies/><br />
<hr />
    Here is the topic fetched using the JavaScript extension:
    <JS>
return PostOffice.getTopic();
    </JS>
    <br />
    Here is the email address fetched using the JavaScript extension:
    <JS>
return PostOffice.getEmailAddress();
    </JS>
    <br />
    Here are the email text bodies fetched using the JavaScript extension:
    <JS>
var msgListIterator = PostOffice.getAllEmailMessages().iterator();
var returnString = "<br />";
while (msgListIterator.hasNext()) {
     returnString = returnString + msgListIterator.next().getMessage() + "<br />"; }
```

```
return returnString;
    </JS>
    <br />
    Here is the recipient's surname taken from the Person fetched using the JavaScript extension:
    <JS>
var person = PostOffice.getPersonByEmailAddress(PostOffice.getEmailAddress());
return "<br />Last: " + person.getProperty("sn")[0] + "<br />";
    </JS>
<hr />
Please take care of these right away.  Have a nice day !<br />
     IT Dept
  </body>
</html>
```

Extensions JavaScript du bureau de poste

Utiliser l'interface de programme d'application (API) de messagerie pour personnaliser le contenu de la messagerie, son format et les destinataires des notifications.

Les clients qui utilisent cette API peuvent effectuer des demandes de notification et étendre la construction des messages de notification. L'API Messagerie contient l'API Client de messagerie, qui crée les demandes de notification et l'API Fournisseur de messagerie, qui les implémente.

L'API Messagerie contient également une fonction de Bureau de poste, qui évite aux participants du flux de travaux de recevoir plusieurs notifications par courrier électronique avec un contenu similaire. Les courriers électroniques similaires sont stockés, regroupés dans une seule notification par courrier électronique, puis transférés à un utilisateur.

Test et résolution des incidents du modèle de messagerie du bureau de poste

Testez et validez le modèle de regroupement de messages du bureau de poste que vous avez créé avant de l'envoyer à un participant à une activité.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Un modèle de regroupement de messages du bureau de poste doit déjà être configuré.

Pourquoi et quand exécuter cette tâche

Pour tester le modèle de regroupement de données, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Bureau de poste**.
2. Cliquez sur **Test**. La page Tester une adresse électronique s'affiche.
3. Sur la page Tester une adresse électronique, indiquez une adresse électronique pour recevoir le message test, puis cliquez sur **Test**. Le modèle de regroupement de messages est validé et en cas de réussite, une notification par

courrier électronique est envoyée à l'adresse électronique indiquée. Ce courrier électronique contient des informations système simulées, qui sont fournies par défaut dans le fichier de propriétés. Le message est présenté dans le modèle de message du bureau de poste que vous avez créé.

4. Cliquez sur le bouton **OK** pour enregistrer les modifications, puis cliquez sur **Fermer**.

Que faire ensuite

Si un message d'erreur s'affiche, corrigez le contenu de la zone indiquée dans l'erreur, puis cliquez de nouveau sur **Test**.

Le message d'erreur décrit le problème et fournit le numéro approximatif de ligne et colonne correspondant à l'endroit où l'erreur s'est produite dans le message. La valeur renvoyée est considérée comme un pointeur général désignant le lieu approximatif du problème, mais pas l'endroit exact. Vous ne pouvez pas inclure le contenu du corps XHTML des notifications d'origine directement dans le corps XHTML du modèle de regroupement. Par défaut, le bureau de poste ne dispose d'aucun modèle de regroupement de corps XHTML.

Visualisez l'exemple de notification par courrier électronique que vous avez envoyé à l'adresse électronique indiquée. Si nécessaire, vous pouvez apporter d'autres modifications au modèle et le tester de nouveau.

Modification du contenu du message d'exemple

Vous pouvez modifier le contenu des exemples de notifications par courrier électronique qui sont utilisés pour les tests.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Un modèle de regroupement de messages du bureau de poste doit déjà être configuré.

Pourquoi et quand exécuter cette tâche

Pour modifier le contenu de l'exemple de notification par courrier électronique, procédez comme suit :

Procédure

1. Editez le fichier `enRole.properties`.
2. Indiquez les nouvelles valeurs `enrole.postoffice` souhaitées, puis enregistrez le fichier `enRole.properties`. `enRole.properties` est le nom du fichier de propriétés et `enrole.postoffice` est le nom de la clé pour laquelle vous indiquez une valeur. Cette paire clé-valeur se trouve dans le fichier de propriétés.
3. Redémarrez votre serveur d'applications pour que les nouvelles valeurs prennent effet.

Résultats

Les résultats de cette tâche ne peuvent être vus qu'une fois que vous avez testé le modèle de regroupement que vous avez créé ou modifié. Le nouvel exemple de notifications par courrier électronique est agrégé et envoyé à l'adresse électronique de test.

Exemple

Le fichier `enRole.properties` contient les valeurs par défaut suivantes :

```
############################################################
## Post Office Template Test Configuration
############################################################
# These are the contents of the emails that will be used
# when the "test" button is used on the Post Office
# configuration page. These 3 emails will be used as the
# content to which the template will be applied.
enrole.postoffice.test.subject1=This is subject 1
enrole.postoffice.test.textbody1=This is the text body 1
enrole.postoffice.test.xhtmlbody1=This is the xhtml body 1

enrole.postoffice.test.subject2=This is subject 2
enrole.postoffice.test.textbody2=This is the text body 2
enrole.postoffice.test.xhtmlbody2=This is the xhtml body 2

enrole.postoffice.test.subject3=This is subject 3
enrole.postoffice.test.textbody3=This is the text body 3
enrole.postoffice.test.xhtmlbody3=This is the xhtml body 3

# The topic to use for the test emails above
enrole.postoffice.test.topic=topic1

# The locale to use for the test emails above
enrole.postoffice.test.locale=en_US
```

Que faire ensuite

Testez le nouveau modèle d'agrégat en l'envoyant à une adresse électronique de test.

Activation du bureau de poste pour les activités du flux de travaux

Utiliser le concepteur du flux de travaux pour activer les notifications du bureau de poste pour les activités de flux de travaux.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Une activité de flux de travaux doit exister.

Pourquoi et quand exécuter cette tâche

Toutes les notifications par courrier électronique ayant la même Rubrique E-mail de groupe sont regroupées à l'aide du modèle et envoyées à chaque destinataire.

Pour activer le bureau de poste pour une activité de flux de travaux, exécutez les étapes suivantes :

Procédure

1. Dans le concepteur de flux de travaux, cliquez deux fois sur une activité existante pour accéder à sa page Propriétés.
2. Dans la page Propriétés, cliquez sur l'onglet **Notification**.
3. Cochez la case **Utiliser la rubrique E-mail de groupe**.
4. Dans le champ **Rubrique E-mail de groupe**, entrez une valeur à utiliser pour regrouper les messages semblables.
5. Cliquez sur le bouton **OK** pour enregistrer l'activité de flux de travaux, puis cliquez sur le bouton **OK** pour enregistrer et quitter le concepteur de flux de travaux.

Résultats

L'activité de flux de travaux est enregistrée. Cette modification prendra effet lors du prochain déclenchement de ce flux de travaux.

Chapitre 7. Personnalisation de formulaire

Vous pouvez créer et modifier des formulaires pour les attributs sur l'interface IBM Security Identity Manager.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

IBM Security Identity Manager fournit des formulaires par défaut pour créer, visualiser et modifier des entités système. Le concepteur de formulaire permet aux administrateurs système de gérer tous les formulaires d'entité depuis un même emplacement.

Les administrateurs système peuvent personnaliser les formulaires des entités système ci-après à l'aide du concepteur de formulaire :

- Compte
- Domaine d'administration
- Organisation partenaire
- Utilisateurs d'une organisation partenaire
- Crédit-bail de droits d'accès
- Utilisateur d'Identity Manager
- Emplacement
- Organisation
- Unité organisationnelle
- Utilisateur
- Rôle
- Service

Chaque dossier de catégorie de formulaire dispose de profils d'objet représentant des entités système. Chaque profil d'objet est associé à un modèle de formulaire.

Les modèles de formulaire par défaut sont générés à partir de la configuration d'une entité. Les modèles de formulaire possèdent au moins un onglet et un élément de formulaire. Un onglet est un conteneur permettant de regrouper des éléments de formulaire. Un élément de formulaire est un attribut d'entité système. Chaque onglet comprend un libellé décrivant le groupe et au moins un élément de formulaire. Chaque élément de formulaire se compose d'un libellé décrivant ses données et le format d'entrée de ces données. Les éléments de formulaire sont répertoriés suivant leur ordre d'affichage dans le formulaire.

Personnalisation des modèles de formulaire

Vous pouvez utiliser l'applet de concepteur de formulaire pour ouvrir des modèles de formulaire qui affichent les éléments de formulaire requis, l'organisation des éléments de formulaire et le type de contrôle des éléments de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Pour ouvrir un modèle de formulaire, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Concevoir des formulaires**. L'applet du concepteur de formulaire s'affiche.
2. Dans le panneau de gauche, cliquez deux fois sur le dossier de la catégorie souhaitée pour afficher les profils d'objet pour le type d'entité. Cliquez ensuite deux fois sur le profil d'objet souhaité pour ouvrir le modèle pour ce profil. Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.

Résultats

Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.

Que faire ensuite

Vous pouvez sélectionner un élément de formulaire et cliquer dessus avec le bouton droit de la souris pour exécuter diverses actions. Déplacez la souris sur les icônes en haut du formulaire pour obtenir des astuces sur le fonctionnement de l'icône.

Ajout d'onglets aux modèles de formulaire

Utilisez ces instructions pour ajouter des onglets aux modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Pour ajouter un onglet à un modèle de formulaire, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Concevoir des formulaires**. L'applet du concepteur de formulaire s'affiche.
2. Dans le panneau de gauche, cliquez deux fois sur le dossier de la catégorie souhaitée pour afficher les profils d'objet pour le type d'entité. Cliquez ensuite deux fois sur le profil d'objet souhaité pour ouvrir le modèle pour ce profil. Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.
3. Cliquez sur **Onglet** > **Ajouter un onglet**. Un nouvel onglet s'affiche dans le modèle de formulaire.
4. Pour nommer le nouvel onglet, cliquez sur **Onglet** > **Renommer l'onglet**.
5. Entrez un nom pour le nouvel onglet dans la zone de saisie, puis cliquez sur le bouton **OK**. Le nom du nouvel onglet s'affiche dans le modèle de formulaire.
6. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Changement de nom des onglets dans les modèles de formulaire

Utilisez ces instructions pour renommer des onglets dans des modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Pour renommer un onglet sur un modèle de formulaire, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Concevoir des formulaires**. L'applet du concepteur de formulaire s'affiche.
2. Dans le panneau de gauche, cliquez deux fois sur le dossier de la catégorie souhaitée pour afficher les profils d'objet pour le type d'entité. Cliquez ensuite deux fois sur le profil d'objet souhaité pour ouvrir le modèle pour ce profil. Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.
3. Cliquez sur **Onglet** > **Renommer l'onglet**.
4. Entrez un nouveau nom pour l'onglet dans la zone de saisie, puis cliquez sur le bouton **OK**. Le nouveau nom de l'onglet s'affiche dans le modèle de formulaire.
5. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Organisation des onglets dans les modèles de formulaire

Utilisez ces instructions pour organiser des onglets dans des modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Pour déplacer un onglet vers une position différente sur un modèle de formulaire, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Concevoir des formulaires**. L'applet du concepteur de formulaire s'affiche.
2. Dans le panneau de gauche, cliquez deux fois sur le dossier de la catégorie souhaitée pour afficher les profils d'objet pour le type d'entité. Cliquez ensuite deux fois sur le profil d'objet souhaité pour ouvrir le modèle pour ce profil. Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.
3. Dans le panneau central, sélectionnez l'onglet que vous voulez déplacer.
4. Sélectionnez l'une des options suivantes :
   - Cliquez sur **Onglet** > **Déplacer l'onglet vers la gauche** pour déplacer l'onglet d'une position vers la gauche.

- Cliquez sur **Onglet** > **Déplacer un onglet vers la droite** pour déplacer l'onglet d'une position vers la droite.

5. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Suppression d'onglets dans les modèles de formulaire

Utilisez ces instructions pour supprimer des onglets de modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Si un onglet contient des attributs requis, vous ne pouvez pas supprimer l'onglet.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Pour supprimer un onglet d'un modèle de formulaire, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Concevoir des formulaires**. L'applet du concepteur de formulaire s'affiche.
2. Dans le panneau de gauche, cliquez deux fois sur le dossier de la catégorie souhaitée pour afficher les profils d'objet pour le type d'entité. Cliquez ensuite deux fois sur le profil d'objet souhaité pour ouvrir le modèle pour ce profil. Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.
3. Dans le panneau central, sélectionnez l'onglet que vous voulez supprimer.
4. Cliquez sur **Onglet** > **Supprimer l'onglet**. L'onglet est supprimé du modèle de formulaire.
5. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Ajout d'attributs aux modèles de formulaire

Utilisez ces instructions pour ajouter des attributs aux modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Pour ajouter un attribut à un modèle de formulaire, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Concevoir des formulaires**. L'applet du concepteur de formulaire s'affiche.
2. Dans le panneau de gauche, cliquez deux fois sur le dossier de la catégorie souhaitée pour afficher les profils d'objet pour le type d'entité. Cliquez ensuite deux fois sur le profil d'objet souhaité pour ouvrir le modèle pour ce profil. Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.
3. Sélectionnez l'onglet auquel vous voulez ajouter l'attribut.
4. Dans le panneau Liste d'attributs, cliquez deux fois sur le nom d'attribut que vous voulez ajouter au formulaire. L'attribut est ajouté au formulaire.
5. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Que faire ensuite

Continuez d'ajouter des attributs si nécessaire.

Modification des propriétés d'attribut

La section des propriétés de l'élément de formulaire se compose de deux onglets, **Format** et **Contrainte**. L'onglet **Format** affiche la liste de toutes les propriétés de formatage, qui peuvent être applicables ou non, suivant le type de contrôle défini pour l'élément. De même, l'onglet **Contrainte** affiche la liste de toutes les contraintes disponibles qui peuvent être applicables ou non au type de contrôle d'entrée défini. Si une propriété ou une contrainte n'est pas applicable, vous ne pouvez pas sélectionner ou définir de valeur.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Il est possible de combiner plusieurs contraintes personnalisées dans une même zone de sorte que l'entrée de données devienne impossible. L'applet de concepteur de formulaire vérifie les conflits entre les contraintes afin qu'aucune combinaison non valide ne puisse être définie pour une zone donnée.

D'une manière générale, n'utilisez qu'une contrainte de syntaxe et qu'une contrainte de type de données par zone.

Par exemple, si la valeur minimale est supérieure à la valeur maximale et que ces deux contraintes sont placées dans une même zone, un conflit se produit. En cas de conflit, vous devez modifier les valeurs ou supprimer une des contraintes.

Pour modifier les propriétés d'un attribut, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Concevoir des formulaires**. L'applet du concepteur de formulaire s'affiche.
2. Dans le panneau de gauche, cliquez deux fois sur le dossier de la catégorie souhaitée pour afficher les profils d'objet pour le type d'entité. Cliquez ensuite deux fois sur le profil d'objet souhaité pour ouvrir le modèle pour ce profil. Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.
3. Dans le panneau central, sélectionnez l'attribut pour lequel vous voulez modifier des propriétés. Les propriétés de l'attribut sont affichées dans le panneau **Propriétés**.
4. Dans l'onglet **Format**, modifiez la propriété sur la valeur souhaitée. La nouvelle valeur de la propriété apparaît et les modifications sont appliquées dans l'attribut.
5. Dans l'onglet **Contrainte**, cochez la case en regard de la contrainte que vous voulez modifier.
6. Entrez des paramètres pour les types de contrainte de valeur.
7. Entrez une valeur d'exemple dans la zone à la fin de la liste des types de contrainte.
8. Cliquez sur le bouton **Valider et mettre à jour les contraintes**.

   L'applet de concepteur de formulaire vous informe en cas de conflit entre des contraintes ou affiche un message **pass** si la valeur entrée est valide d'après les contraintes utilisées et qu'aucun conflit entre les contraintes n'a été détecté.
9. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Modification de types de contrôle d'attribut

Les types de contrôle définissent l'interface avec laquelle les utilisateurs introduisent des données dans cet élément de formulaire. Actuellement sont pris en charge les types de contrôle : case à cocher, date, zone déroulante, liste d'éléments texte modifiables, zone de liste, heures de connexion, mot de passe, fenêtre de saisie du mot de passe, contrôle de recherche, occurrence de recherche, sous-formulaire, zone de texte, bloc de texte et umask.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Pour modifier le type de contrôle d'un attribut, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Concevoir des formulaires**. L'applet du concepteur de formulaire s'affiche.
2. Dans le panneau de gauche, cliquez deux fois sur le dossier de la catégorie souhaitée pour afficher les profils d'objet pour le type d'entité. Cliquez ensuite deux fois sur le profil d'objet souhaité pour ouvrir le modèle pour ce profil. Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.
3. Dans le panneau central, sélectionnez l'attribut pour lequel vous voulez modifier le type de contrôle.
4. Cliquez sur **Attribut** > **Modifier en**. La liste des types de contrôle s'affiche.
5. Sélectionnez le type de contrôle souhaité. Pour certains types de contrôle, un éditeur s'affiche.
6. Si un éditeur du type de contrôle s'affiche, entrez les paramètres souhaités et cliquez sur le bouton **OK**.
7. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Organisation des attributs dans les modèles de formulaire

Utilisez ces instructions pour organiser les attributs dans des modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Une fois que vous avez apporté toutes vos modifications à un modèle de formulaire et que vous les avez sauvegardées, fermez le navigateur. Ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Pour déplacer un attribut vers une position différente d'un modèle de formulaire, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Concevoir des formulaires**. L'applet du concepteur de formulaire s'affiche.
2. Dans le panneau de gauche, cliquez deux fois sur le dossier de la catégorie souhaitée pour afficher les profils d'objet pour le type d'entité. Cliquez ensuite deux fois sur le profil d'objet souhaité pour ouvrir le modèle pour ce profil. Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.
3. Dans le panneau du milieu, sélectionnez l'attribut que vous voulez déplacer.
4. Sélectionnez l'une des options suivantes :
   - Cliquez sur **Attribut** > **Déplacer l'attribut vers le haut** pour déplacer l'attribut d'une position vers le haut.
   - Cliquez sur **Attribut** > **Déplacer l'attribut vers le bas** pour déplacer l'attribut d'une position vers le bas.
5. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Suppression d'attributs dans les modèles de formulaire

Utilisez ces instructions pour supprimer des attributs de modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Pour supprimer un attribut d'un modèle de formulaire, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Concevoir des formulaires**. L'applet du concepteur de formulaire s'affiche.
2. Dans le panneau de gauche, cliquez deux fois sur le dossier de la catégorie souhaitée pour afficher les profils d'objet pour le type d'entité. Cliquez ensuite deux fois sur le profil d'objet souhaité pour ouvrir le modèle pour ce profil. Le modèle de formulaire associé au profil d'objet s'affiche dans le panneau du milieu.
3. Dans le panneau central, sélectionnez l'attribut que vous voulez supprimer.
4. Cliquez sur **Attribut** > **Supprimer l'attribut**. L'attribut est supprimé du modèle de formulaire.
5. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Personnalisation des modèles de formulaire pour une instance de service

Vous pouvez ouvrir un formulaire de compte personnalisé directement à partir de l'instance de service.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

Vous pouvez personnaliser le formulaire de compte pour chaque instance de service. Lorsque l'applet de concepteur de formulaire est lancé pour la personnalisation du formulaire de compte au niveau d'instance de service, le panneau d'arborescence de navigation ne s'affiche pas. Cette session est utilisée uniquement en vue de la personnalisation du formulaire de compte pour l'instance de service spécifique. Pour obtenir des instructions sur le mode de personnalisation du formulaire, voir les sections relatives à la personnalisation des modèles de formulaire.

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Remarque : Le formulaire personnalisé pour le service ITM n'est pas pris en charge car il existe une seule instance de service ITM. Ce formulaire de compte peut être configuré au niveau du système. Toutefois, le formulaire de compte personnalisé est pris en charge pour l'instance de service ITIM hébergé car il existe une ou plusieurs instances de service ITIM hébergées.

Procédure

Pour ouvrir un modèle de formulaire, exécutez les étapes suivantes :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.
3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service pour afficher les tâches pouvant être effectuées sur le service puis cliquez sur **Personnaliser le formulaire de compte**. L'applet du concepteur de formulaire démarre.

Résultats

Le formulaire de compte personnalisé associé à l'instance de service s'affiche. S'il n'existe aucun formulaire de compte personnalisé pour l'instance de service, le modèle de formulaire s'affiche.

Que faire ensuite

Vous pouvez sélectionner un élément de formulaire et cliquer dessus avec le bouton droit de la souris pour exécuter diverses actions. Déplacez la souris sur les icônes en haut du formulaire pour obtenir des astuces sur la fonction.

Ajout d'onglets aux modèles de formulaire pour une instance de service

Utilisez ces instructions pour ajouter des onglets aux modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Procédure

Pour ajouter un onglet à un modèle de formulaire, exécutez les étapes suivantes :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.
3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service pour afficher les tâches pouvant être réalisées sur le service. Cliquez sur **Personnaliser le formulaire de compte**. L'applet du concepteur de formulaire démarre. Le modèle de formulaire associé à l'instance de service s'affiche.
4. Cliquez sur **Onglet** > **Ajouter un onglet**. Un nouvel onglet s'affiche dans le modèle de formulaire.
5. Pour nommer le nouvel onglet, cliquez sur **Onglet** > **Renommer l'onglet**.
6. Entrez un nom pour le nouvel onglet dans la zone de saisie, puis cliquez sur le bouton **OK**. Le nom du nouvel onglet s'affiche dans le modèle de formulaire.
7. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Que faire ensuite

Continuez d'ajouter des onglets si nécessaire.

Attribution de nouveaux noms aux onglets dans les modèles de formulaire pour une instance de formulaire

Utilisez ces instructions pour renommer des onglets dans des modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Procédure

Pour renommer un onglet en lui donnant le nom d'un modèle de formulaire, procédez comme suit :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :
      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.
3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service pour afficher les tâches pouvant être réalisées sur le service. Cliquez sur **Personnaliser le formulaire de compte**. L'applet du concepteur de formulaire démarre. Le modèle de formulaire associé à l'instance de service s'affiche.
4. Cliquez sur **Onglet** > **Renommer l'onglet**.
5. Entrez un nouveau nom pour l'onglet dans la zone de saisie, puis cliquez sur le bouton **OK**. Le nouveau nom de l'onglet s'affiche dans le modèle de formulaire.
6. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Que faire ensuite

Continuez de renommer des onglets si nécessaire.

Organisation des onglets dans les modèles de formulaire pour une instance de formulaire

Utilisez ces instructions pour organiser des onglets dans des modèles de formulaire pour uns instance de service.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Procédure

Pour organiser un onglet dans un modèle de formulaire, exécutez les étapes suivantes :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.
3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service pour afficher les tâches pouvant être réalisées sur le service. Cliquez sur **Personnaliser le formulaire de compte**. L'applet du concepteur de formulaire démarre. Le modèle de formulaire associé à l'instance de service s'affiche.
4. Sélectionnez l'onglet à déplacer.
5. Sélectionnez l'une des options suivantes :

- Cliquez sur **Onglet** > **Déplacer l'onglet vers la gauche** pour déplacer l'onglet d'une position vers la gauche.
- Cliquez sur **Onglet** > **Déplacer un onglet vers la droite** pour déplacer l'onglet d'une position vers la droite.

6. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Que faire ensuite

Continuez d'organiser des onglets si nécessaire.

Suppression d'onglets dans les modèles de formulaire pour une instance de service

Utilisez ces instructions pour supprimer des onglets de modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Procédure

Pour supprimer un onglet d'un modèle de formulaire, procédez comme suit :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :
      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.

3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service pour afficher les tâches pouvant être effectuées sur le service. Cliquez sur **Personnaliser le formulaire de compte**. L'applet du concepteur de formulaire démarre. Le modèle de formulaire associé à l'instance de service s'affiche.
4. Sélectionnez l'onglet à supprimer.
5. Cliquez sur **Onglet** > **Supprimer l'onglet**. L'onglet est supprimé du modèle de formulaire.
6. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Que faire ensuite

Continuez de supprimer des onglets si nécessaire.

Ajout d'attributs aux modèles de formulaire pour une instance de service

Utilisez ces instructions pour ajouter des attributs aux modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Procédure

Pour ajouter un attribut à un modèle de formulaire, exécutez les étapes suivantes :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

- Cliquez sur la flèche pour accéder à la page suivante.
- Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.

3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service pour afficher les tâches pouvant être réalisées sur le service. Cliquez sur **Personnaliser le formulaire de compte**. L'applet du concepteur de formulaire démarre. Le modèle de formulaire associé à l'instance de service s'affiche.
4. Sélectionnez l'onglet auquel vous voulez ajouter l'attribut.
5. Dans le panneau Liste d'attributs, cliquez deux fois sur le nom d'attribut que vous voulez ajouter au formulaire. L'attribut est ajouté au formulaire.
6. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Que faire ensuite

Continuez d'ajouter des attributs si nécessaire.

Modification des propriétés d'attribut

La section des propriétés de l'élément de formulaire se compose de deux onglets, **Format** et **Contrainte**. L'onglet **Format** affiche la liste de toutes les propriétés de formatage, qui peuvent être applicables ou non, suivant le type de contrôle défini pour l'élément. De même, l'onglet **Contrainte** affiche la liste de toutes les contraintes disponibles qui peuvent être applicables ou non au type de contrôle d'entrée défini. Si une propriété ou une contrainte n'est pas applicable, vous ne pouvez pas sélectionner ou définir de valeur.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Procédure

Pour modifier les propriétés d'un attribut, exécutez les étapes suivantes :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.

b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
c. Sélectionnez un type de service dans la liste **Type de recherche**.
d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

   Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

   - Cliquez sur la flèche pour accéder à la page suivante.
   - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.

3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service pour afficher les tâches pouvant être réalisées sur le service. Cliquez sur **Personnaliser le formulaire de compte**. L'applet du concepteur de formulaire démarre. Le modèle de formulaire associé à l'instance de service s'affiche.
4. Sélectionnez l'attribut pour lequel vous souhaitez modifier les propriétés. Les propriétés de l'attribut sont affichées dans le panneau **Propriétés**.
5. Dans l'onglet **Format**, modifiez la propriété et attribuez-lui la valeur souhaitée. La nouvelle valeur de la propriété apparaît et les modifications sont appliquées dans l'attribut.
6. Dans l'onglet **Contrainte**, cochez la case en regard de la contrainte que vous voulez modifier.
7. Entrez des paramètres pour les types de contrainte de valeur.
8. Entrez une valeur d'exemple dans la zone à la fin de la liste des types de contrainte.
9. Cliquez sur le bouton **Valider et mettre à jour les contraintes**.

   L'applet de concepteur de formulaire vous informe en cas de conflit entre des contraintes ou affiche un message **pass** si la valeur entrée est valide d'après les contraintes utilisées et qu'aucun conflit entre les contraintes n'a été détecté.
10. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Que faire ensuite

Continuez de modifier des attributs si nécessaire.

Modification de types de contrôle d'attribut

Les types de contrôle définissent l'interface avec laquelle les utilisateurs introduisent des données dans cet élément de formulaire. Actuellement sont pris en charge les types de contrôle suivants : case à cocher, date, zone déroulante, liste d'éléments texte modifiables, zone de liste, heures de connexion, mot de passe, fenêtre de saisie du mot de passe, contrôle de recherche, occurrence de recherche, sous-formulaire, zone de texte, bloc de texte et umask.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Procédure

Pour modifier le type de contrôle d'un attribut, exécutez les étapes suivantes :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.
3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service pour afficher les tâches pouvant être réalisées sur le service. Cliquez sur **Personnaliser le formulaire de compte**. L'applet du concepteur de formulaire démarre. Le modèle de formulaire associé à l'instance de service s'affiche.
4. Sélectionnez l'attribut pour lequel vous souhaitez changer le type de contrôle.
5. Cliquez sur **Attribut** > **Modifier en**. La liste des types de contrôle s'affiche.
6. Sélectionnez le type de contrôle. Pour certains types de contrôle, un éditeur s'affiche.
7. Si un éditeur du type de contrôle s'affiche, entrez les paramètres puis cliquez sur le bouton **OK**.
8. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Que faire ensuite

Continuez de changer les types de contrôle des attributs si nécessaire.

Organisation des attributs dans les modèles de formulaire pour une instance de formulaire

Utilisez ces instructions pour organiser les attributs dans des modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Procédure

Pour déplacer un attribut vers une position différente d'un modèle de formulaire, exécutez les étapes suivantes :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.
3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service pour afficher les tâches pouvant être réalisées sur le service. Cliquez sur **Personnaliser le formulaire de compte**. L'applet du concepteur de formulaire démarre. Le modèle de formulaire associé à l'instance de service s'affiche.
4. Sélectionnez l'attribut à déplacer.
5. Sélectionnez l'une des options suivantes :

- Cliquez sur **Attribut** > **Déplacer l'attribut vers le haut** pour déplacer l'attribut d'une position vers le haut.
- Cliquez sur **Attribut** > **Déplacer l'attribut vers le bas** pour déplacer l'attribut d'une position vers le bas.

6. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Que faire ensuite

Continuez d'organiser les attributs si nécessaire.

Suppression d'attributs dans les modèles de formulaire pour une instance de service

Utilisez ces instructions pour supprimer des attributs de modèles de formulaire.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Procédure

Pour supprimer un attribut d'un modèle de formulaire, exécutez les étapes suivantes :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

      - Cliquez sur la flèche pour accéder à la page suivante.

- Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.

3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service pour afficher les tâches pouvant être réalisées sur le service. Cliquez sur **Personnaliser le formulaire de compte**. L'applet du concepteur de formulaire démarre. Le modèle de formulaire associé à l'instance de service s'affiche.
4. Dans le panneau central, sélectionnez l'attribut que vous voulez supprimer.
5. Cliquez sur **Attribut** > **Supprimer l'attribut**. L'attribut est supprimé du modèle de formulaire.
6. Cliquez sur **Formulaire** > **Enregistrer le modèle de formulaire**, puis cliquez sur le bouton **OK** lorsqu'un message indique que le modèle de formulaire a été enregistré avec succès.

Que faire ensuite

Continuez de supprimer des attributs si nécessaire.

Suppression d'un modèle de formulaire personnalisé d'une instance de service

Vous pouvez supprimer un compte personnalisé d'une instance de service et restaurer le formulaire de compte système.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Procédure

Pour supprimer un modèle de formulaire de compte personnalisé, procédez comme suit :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :
      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.

3. Dans le tableau **Services**, cliquez sur l'icône (▸) en regard du service pour afficher les tâches pouvant être réalisées sur le service. Cliquez sur l'option permettant de supprimer le formulaire de compte. Une page de confirmation s'affiche.
4.
   - Cliquez sur **Supprimer** pour supprimer le formulaire personnalisé de l'instance de service.
   - Cliquez sur **Annuler** pour retourner à la page de sélection de service sans supprimer le formulaire personnalisé.

   Un message s'affiche pour indiquer si le formulaire de compte a été supprimé.
5. Cliquez sur **Fermer** pour retourner à la page de sélection de service.

Que faire ensuite

Effectuez des actions de service supplémentaires.

Réinitialisation des modèles de formulaire

Avant d'enregistrer les modifications dans le modèle de formulaire, vous pouvez réinitialiser le modèle de formulaire sur sa configuration d'origine.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Seules les personnes faisant partie du groupe administrateur peuvent accéder à cette fonction.

Pourquoi et quand exécuter cette tâche

L'applet Java du concepteur de formulaire ne se ferme pas automatiquement et n'est pas supprimé de la mémoire à la suite du démarrage. Apportez des modifications à un modèle de formulaire et sauvegardez ces dernières. Fermez le navigateur et ouvrez-le à nouveau avant de lancer une nouvelle procédure si vous avez rencontré des problèmes de navigateur ou de performances.

Pour réinitialiser le modèle de formulaire sur sa configuration d'origine, exécutez les étapes suivantes :

Procédure

1. Dans l'applet de concepteur de formulaire, cliquez sur **Formulaire** > **Réinitialiser le modèle de formulaire**.
2. Cliquez sur **Oui** lorsque vous êtes informé que les modifications du modèle de formulaire seront perdues.

Interface Form Designer

Utilisez les zones de travail de l'applet Form Designer pour concevoir des formulaires personnalisés en exécutant des actions sur des modèles de formulaire, des onglets et des attributs.

L'interface de conception de formulaires présente les zones suivantes :

Boutons de la barre de menus et de la barre d'outils

Utilisez les boutons de la barre de menus et de la barre d'outils pour exécuter des opérations sur les modèles de formulaire, les onglets et les attributs. Placez le curseur de la souris sur un bouton de la barre d'outils pour afficher sa fonction. Les boutons de barre de menus et de barre d'outils sont les suivants :

Tableau 24. Menu et boutons de barre d'outils de l'applet de concepteur de formulaire

Barre de menus	Option de menu	Bouton de barre d'outils	Action
Cliquez sur **Formulaire** pour ouvrir, sauvegarder ou réinitialiser un modèle de formulaire à la dernière conception sauvegardée.	**Ouvrir le modèle de formulaire**		Ouvre le modèle de formulaire qui est sélectionné dans les dossiers de catégorie de formulaire.
	Sauvegarder le modèle de formulaire		Sauvegarde le modèle de formulaire ouvert.
	Réinitialiser le modèle de formulaire	Aucun	Réinitialise le modèle de formulaire à la dernière conception sauvegardée.
Cliquez sur **Onglet** pour ajouter, renommer, supprimer ou décaler un onglet vers la gauche ou vers la gauche dans l'interface. Les onglets apparaissent dans la zone de travail Attributs de modèle de l'applet Form Designer. Les noms des onglets du concepteur de formulaire correspondent à ceux des onglets figurant dans les formulaires de bloc-notes générés dans l'interface IBM Security Identity Manager.	**Ajouter un onglet**		Ajoute un conteneur pour le regroupement des éléments de formulaire.
	Renommer l'onglet	Aucun	Renomme un conteneur d'onglets.
	Déplacer l'onglet vers la gauche		Déplace un conteneur d'onglets vers la gauche.
	Déplacer un onglet vers la droite		Déplace un conteneur d'onglets vers la droite.
	Supprimer l'onglet		Supprime un onglet du modèle de formulaire.

Tableau 24. Menu et boutons de barre d'outils de l'applet de concepteur de formulaire (suite)

Barre de menus	Option de menu	Bouton de barre d'outils	Action
Cliquez sur **Attribut** pour modifier, supprimer ou déplacer un attribut vers le haut ou vers le bas dans l'interface, ou modifier le type de contrôle d'un attribut. Les attributs apparaissent dans la zone de travail Attributs de modèle de l'applet Form Designer.	**Modifier l'attribut**	Aucun	Edite et configure un attribut.
	Supprimer l'attribut		Supprime un attribut d'un modèle de formulaire.
	Déplacer l'attribut vers le haut		Déplace l'attribut d'un rang vers le haut dans la liste des attributs du modèle de formulaire.
	Déplacer l'attribut vers le bas		Déplace l'attribut d'un rang vers le bas dans la liste des attributs du modèle de formulaire.
	Modifier en	Aucun	Change le type de contrôle d'attribut sélectionné en un type de contrôle nouvellement sélectionné.
Cliquez sur **Afficher** pour sélectionner plusieurs options d'affichage de l'interface, telles que les zones de travail flottantes ou l'affichage de la source du modèle de formulaire.	**Déplacer la liste d'attributs**		Déplace la liste d'attributs de Form Designer vers une fenêtre en incrustation flottante.
	Déplacer les propriétés		Déplace la liste de propriétés de Form Designer vers une fenêtre en incrustation flottante.
	Afficher la source		Ouvre une fenêtre en incrustation affichant la source XML du modèle de formulaire.
Cliquez sur **Menu.theme** pour sélectionner un thème d'interface pour l'applet Form Designer.	**Thème par défaut**	Aucun	Applique le thème du menu par défaut à l'interface Form Designer.
	Thème Contraste élevé, Police de grande taille	Aucun	Applique une police de grande taille et des couleurs à fort contraste à l'interface Form Designer.
	Thème Contraste élevé	Aucun	Applique des couleurs à fort contraste à l'interface Form Designer.

Catégories

Utilisez le panneau de gauche de Form Designer pour sélectionner une catégorie, telle qu'un compte, une organisation ou un service. Chaque catégorie de formulaire est associée à des profils d'objet représentant des entités système. Chaque profil d'objet est associé à un modèle de formulaire.

Cliquez deux fois sur un dossier de catégorie pour développer la liste des modèles de formulaire disponibles pour cette catégorie. Le chargement de la liste des modèles de formulaire peut prendre un certain temps. Pour certaines catégories, la liste des modèles de formulaire varie en fonction des types de services existants.

Cliquez deux fois sur un modèle de formulaire pour l'ouvrir.

Attributs de modèle

Utilisez le panneau central de Form Designer pour afficher et modifier les attributs actifs pour un modèle de formulaire sélectionné. Cliquez avec le bouton droit sur l'attribut pour afficher les actions disponibles pour cet attribut.

Par exemple, un modèle de formulaire de service a un attribut `$servicename`. Pour modifier le type de contrôle associé à un attribut, cliquez avec le bouton droit sur l'attribut et cliquez sur **Modifier en** dans la liste.

Liste d'attributs

Utilisez cette liste pour afficher tous les attributs de l'objet sélectionné qui ne sont pas actuellement inclus dans le formulaire. Vous pouvez la trier par ordre croissant ou décroissant et ajouter des attributs à la liste des attributs des modèles actifs. Par exemple, un objet Organisation comporte des attributs supplémentaires, tels que `$postalcode`, que vous pouvez ajouter à la liste des attributs des modèles actifs.

Propriétés

Contient les onglets **Format** et **Contrainte** qui indiquent le type de données et d'autres paramètres pour un attribut spécifique. Par exemple, le type de données d'un attribut `$servicename` est Chaîne d'annuaire et cet attribut est obligatoire.

Types de contrôle utilisés par Form Designer

Utilisez les types de contrôle de l'applet Form Designer pour indiquer la façon dont les utilisateurs entrent la valeur d'un attribut.

Case à cocher

Attribue une seule case à cocher comme zone de collecte de données. Ce type de contrôle est généralement utilisé pour les attributs de nature booléenne.

Date

Fournit une fenêtre de calendrier en incrustation qui permet aux utilisateurs de sélectionner la date voulue. Ce type de contrôle comporte des attributs supplémentaires permettant de configurer la date.

Lorsque vous sélectionnez ce type de contrôle dans l'applet Form Designer, la page Editeur de dates s'affiche. Vous pouvez utiliser les zones de cet éditeur pour configurer le type de contrôle. L'éditeur de dates contient les zones suivantes :

Type d'entrée de date
Sélectionnez le type d'entrée de date pour la fenêtre de calendrier en incrustation.

Par défaut
Fournit une fenêtre de calendrier en incrustation comportant une case à cocher **Jamais**. Si l'utilisateur cochez cette dernière, la valeur de l'attribut n'expire jamais.

Autre date
Fournit une fenêtre de calendrier en incrustation ne comportant pas de case à cocher **Jamais**. Utilisez ce type si la valeur de l'attribut doit expirer à un instant donné.

Afficher l'heure
Cochez cette case pour inclure une fenêtre en incrustation permettant d'afficher et d'indiquer l'heure.

Zone déroulante

Crée une liste pour un attribut. Vous devez renseigner les attributs devant être contenus dans la liste en utilisant l'une des options suivantes :

Valeurs personnalisées
Limite les informations disponibles dans la liste figurant dans le formulaire généré. Lorsque vous sélectionnez cette option, la page Editeur de sélection s'affiche. Vous pouvez utiliser les zones de cet éditeur pour configurer le type de contrôle. L'éditeur de sélection contient les zones et boutons de barre d'outils suivants :

Nombre de lignes
Saisissez le nombre de lignes à inclure dans la liste et appuyez sur **Entrée**. Utilisez cette zone pour indiquer le nombre de lignes dans une liste. Si la liste d'origine contient plus de ligne que le nombre que vous avez entré, les lignes supplémentaires sont supprimées.

Valeur des données
Entrez une valeur de données.

Valeur affichée
Entrez une valeur d'affichage qui apparaîtra dans la liste.

Utiliser une ligne vierge
Cochez cette case pour insérer une entrée vierge dans la liste.

Ajouter une ligne
Cliquez dessus pour ajouter une ligne à afficher dans la liste.

Supprimer une ligne
Cochez cette case pour supprimer une ligne de la liste.

Utiliser la valeur affichée comme valeur
Cochez cette case pour utiliser la même valeur que celle qui figure dans la colonne **Valeur affichée** pour la colonne **Valeur des données**.

Utiliser l'indice comme valeur
Cochez cette case pour utiliser la même valeur que celle qui figure dans l'index pour la colonne **Valeur des données**.

Filtre de recherche
Fournit une gamme plus importante dans laquelle des informations peuvent être collectées en vue de remplir la zone. Utilisez un filtre de recherche LDAP qui attribue une valeur à un attribut via l'utilisation d'un contrôle de recherche. Lorsque vous sélectionnez cette option, la page Editeur des filtres de recherche s'affiche. Vous pouvez utiliser les zones de cet éditeur pour configurer le type de contrôle. L'éditeur de filtres de recherche contient les zones suivantes :

Base de recherche
Sélectionnez la portée de la recherche parmi les options suivantes :

org permet de rechercher l'organisation du conteneur sélectionné dans l'arborescence des organisations.

contextuel permet de rechercher l'unité organisationnelle sélectionnée dans l'arborescence des organisations.

Classe d'objet
Entrez le nom de la classe LDAP à rechercher, telle que `erNTGlobalGroup`. La valeur de la zone de groupe figurant dans le formulaire généré doit être `erroles`.

Attribut
Entrez l'attribut à rechercher, tel que `erNTLocalName`.

Attribut source
Entrez la valeur d'attribut à renvoyer une fois la recherche terminée, telle qu'`erNTGlobalGroupId`.

Filtre Entrez tout filtre supplémentaire à appliquer à la recherche, tel que `(objectclass=erNTLocalGroup)`. La valeur de la zone de groupe figurant dans le formulaire généré doit être `objectclass=erroles`.

Délimiteur
Entrez le délimiteur à utiliser pour séparer les valeurs d'attribut dans le formulaire généré.

Valeur multiple
Cochez cette case pour transformer une zone déroulante en zone de liste dans le formulaire généré. La zone de liste permet aux utilisateurs de sélectionner plusieurs valeurs.

Afficher l'interface de requête
Cochez cette case pour afficher une page de recherche dans le formulaire généré. Lorsque cette option n'est pas sélectionnée, seuls les résultats de recherche s'affichent dans une page distincte.

Paginer les résultats
Cochez cette case pour afficher les résultats de la recherche sur plusieurs pages.

Liste modifiable

Autorise l'affichage d'attributs à plusieurs valeurs dans l'interface utilisateur. Ce type de contrôle est une zone de liste affichant des informations que l'utilisateur a fournies. Les utilisateurs peuvent entrer des informations dans la zone de texte et les ajouter à la zone de liste en cliquant sur **Ajouter**. Ils peuvent ensuite les supprimer de cette dernière en sélectionnant l'entrée et en cliquant sur **Supprimer**.

Zone de liste

Fournit une zone de liste pour un attribut. La zone de liste contient des données sélectionnées par l'utilisateur. Les utilisateurs peuvent ajouter ou un ou plusieurs éléments à une zone de liste et les supprimer de cette dernière.

Valeurs personnalisées
Limite les informations disponibles dans la liste figurant dans le formulaire généré. Lorsque vous sélectionnez cette option, la page Editeur de sélection s'affiche. Vous pouvez utiliser les zones de cet éditeur pour configurer le type de contrôle. L'éditeur de sélection contient les zones et boutons de barre d'outils suivants :

Nombre de lignes
Saisissez le nombre de lignes à inclure dans la liste et appuyez sur **Entrée**. Utilisez cette zone pour indiquer le nombre de lignes dans une liste. Si la liste d'origine contient plus de ligne que le nombre que vous avez entré, les lignes supplémentaires sont supprimées.

Valeur des données
Entrez une valeur de données.

Valeur affichée
Entrez une valeur d'affichage qui apparaîtra dans la liste.

Utiliser une ligne vierge
Cochez cette case pour insérer une entrée vierge dans la liste.

Ajouter une ligne
Cliquez dessus pour ajouter une ligne à afficher dans la liste.

Supprimer une ligne
Cochez cette case pour supprimer une ligne de la liste.

Utiliser la valeur affichée comme valeur
Utilisez la même valeur que celle qui figure dans la colonne **Valeur affichée** pour la colonne **Valeur des données**.

Utiliser l'indice comme valeur
Utilisez la même valeur que celle qui figure dans l'index pour la colonne **Valeur des données**.

Filtre de recherche
Fournit une gamme plus importante dans laquelle des informations peuvent être collectées en vue de remplir la zone. Utilisez un filtre de recherche LDAP pour attribuer une valeur à un attribut via l'utilisation d'un contrôle de recherche. Lorsque vous sélectionnez cette option, la page Editeur des filtres de recherche s'affiche. Vous pouvez utiliser les zones de cet éditeur pour configurer le type de contrôle. L'éditeur de filtres de recherche contient les zones suivantes :

Base de recherche
Sélectionnez la portée de la recherche parmi les options suivantes :

org permet de rechercher l'organisation du conteneur sélectionné dans l'arborescence des organisations.

contextuel permet de rechercher l'unité organisationnelle sélectionnée dans l'arborescence des organisations.

Classe d'objet
Entrez le nom de la classe LDAP à rechercher, telle que `erNTGlobalGroup`. La valeur de la zone de groupe figurant dans le formulaire généré doit être `erroles`.

Attribut
Entrez l'attribut à rechercher, tel que `erNTLocalName`.

Attribut source
Entrez la valeur d'attribut à renvoyer une fois la recherche terminée, telle qu'`erNTGlobalGroupId`.

Filtre Entrez tout filtre supplémentaire à appliquer à la recherche, tel que `(objectclass=erNTLocalGroup)`. La valeur de la zone de groupe figurant dans le formulaire généré doit être `objectclass=erroles`.

Délimiteur
Entrez le délimiteur à utiliser pour séparer les valeurs d'attribut dans le formulaire généré.

Valeur multiple
Cochez cette case pour transformer une zone déroulante en zone de liste dans le formulaire généré. La zone de liste permet aux utilisateurs de sélectionner plusieurs valeurs.

Afficher l'interface de requête
Cochez cette case pour afficher une page de recherche dans le formulaire généré. Lorsque cette option n'est pas sélectionnée, seuls les résultats de recherche s'affichent dans une page distincte.

Paginer les résultats
Cochez cette case pour afficher les résultats de la recherche sur plusieurs pages.

Heures de connexion

Définit les heures auxquelles les utilisateurs peuvent se connecter à un service. Utilisez ce type de contrôle uniquement dans les formulaires concernant les services dans lesquels les heures de connexions sont limitées, tels qu'un service Windows 2000.

Lorsque vous sélectionnez ce type de contrôle dans l'applet Form Designer, la page Editeur des heures de connexion s'affiche. Vous pouvez utiliser les zones de cet éditeur pour configurer par défaut le type de contrôle à un type de recherche spécifique. L'éditeur des heures de connexion contient les zones suivantes :

Intervalle
Sélectionnez l'intervalle de temps à afficher dans le formulaire généré :

Une heure définit l'intervalle de temps à des blocs d'une heure.

Demi-heure définit l'intervalle de temps à des blocs d'une demi-heure.

Orientation
Sélectionnez l'orientation de l'éditeur qui est utilisée pour définir les heures de connexion dans le formulaire généré :

Portrait place les jours de la semaine sur l'axe des X et l'heure (en blocs d'une demi-heure ou d'une heure) sur l'axe des Y.

Paysage place l'heure (en blocs d'une demi-heure ou d'une heure) sur l'axe des X et les jours de la semaine sur l'axe des Y.

Mot de passe

Fournit une zone de texte pour un attribut qui n'affiche pas les informations fournies par un utilisateur. Pour plus de sécurité, les informations sont masquées à l'écran.

Fenêtre de saisie du mot de passe

Ouvre une fenêtre permettant à l'utilisateur d'entrer des informations sécurisées. Les informations à l'écran sont masquées et offrent deux zones de texte pour la saisie. Ce type de contrôle est généralement utilisé pour le secret partagé d'un individu.

Contrôle de recherche

Fournit une page de recherche de zone de texte pour l'attribut sélectionné et inclut les boutons **Rechercher** et **Effacer**. Les utilisateurs renseignent la zone de texte en sélectionnant le résultat de la recherche de leur choix. Le bouton **Rechercher** figurant dans le formulaire généré dans l'interface utilisateur permet d'afficher une page de recherche dans laquelle le type de recherche est déjà sélectionné. Le bouton **Effacer** permet de supprimer le contenu de la zone de texte.

Lorsque vous sélectionnez ce type de contrôle dans l'applet Form Designer, la page Editeur d'options de recherche s'affiche. Vous pouvez utiliser les zones de cet éditeur pour configurer par défaut le type de contrôle à un type de recherche spécifique. L'éditeur d'options de recherche contient les zones suivantes :

Catégorie
Sélectionnez la catégorie pour la recherche.

Profil Sélectionnez le profil à utiliser pour la recherche.

Attribut
Sélectionnez l'attribut à utiliser pour la recherche.

Opérateur
Sélectionnez l'opérateur, tel que **Contains** ou **Equals**, qui lie entre elles les zones **Attribut** et **Valeur**.

Valeur Entrez la valeur de l'attribut.

Type Sélectionnez le type des attributs à renvoyer. Un type de valeur unique fournit une zone de texte que l'utilisateur doit remplir. Un type de valeurs multiples fournit une zone de liste d'attributs. Dans le scénario, les utilisateurs peuvent identifier les attributs à rechercher, en sélectionnant ceux qu'ils ne souhaitent pas inclure dans la recherche, puis en cliquant sur le bouton **Supprimer**. Cette action supprime les attributs sélectionnés de la liste des attributs pouvant être recherchés.

Rechercher dans toute l'organisation (si l'option n'est pas cochée, la recherche est limitée au conteneur en cours)
Cochez cette case pour que la recherche concerne l'organisation toute entière.

Le type de contrôle Occurrence de recherche est un type de contrôle connexe. Le type de contrôle est un type de contrôle connexe, qui correspond au type de contrôle Contrôle de recherche avec une fonctionnalité supplémentaire qui permet la recherche et le renseignement automatiques de la zone de liste de l'attribut.

Occurrence de recherche

Similaire au type de contrôle Contrôle de recherche, mais avec une fonctionnalité supplémentaire qui permet la recherche et le renseignement automatiques de la zone de liste d'un attribut. Les utilisateurs peuvent utiliser la fonction de recherche automatique en saisissant les premières lettres de la valeur désirée dans la zone de texte, puis en cliquant sur **Ajouter**. Si un résultat est détecté, le résultat est automatiquement ajouté à la zone de liste. Si plusieurs résultats sont détectés, une page Résultats de la recherche s'affiche. L'utilisateur peut alors sélectionner les éléments à ajouter à la zone de liste.

Fournit une page affichant une zone de texte pour l'attribut sélectionné. Les utilisateurs renseignent la zone de texte en sélectionnant le résultat de la recherche de leur choix. Dans le formulaire généré, le bouton **Rechercher** permet d'ouvrir une page de recherche dans laquelle le type de recherche est déjà sélectionné. Le bouton **Effacer** efface le contenu de la zone de texte. Le bouton **Supprimer** permet de supprimer un élément sélectionné dans la zone de liste.

Lorsque vous sélectionnez ce type de contrôle dans l'applet Form Designer, la page Editeur d'options de recherche s'affiche. Vous pouvez utiliser les zones de cet éditeur pour configurer par défaut le type de contrôle à un type de recherche spécifique. L'éditeur d'options de recherche contient les zones suivantes :

Catégorie
Sélectionnez la catégorie pour la recherche.

Profil Sélectionnez le profil à utiliser pour la recherche.

Attribut
Sélectionnez l'attribut à utiliser pour la recherche.

Opérateur
Sélectionnez l'opérateur, tel que **Contains** ou **Equals**, qui lie entre elles les zones **Attribut** et **Valeur**.

Valeur Entrez la valeur de l'attribut.

Type Sélectionnez le type des attributs à renvoyer. Un type de valeur unique fournit une zone de texte que l'utilisateur doit remplir. Un type de valeurs multiples fournit une zone de liste d'attributs. Dans le scénario, les utilisateurs peuvent identifier les attributs à rechercher, en sélectionnant ceux qu'ils ne souhaitent pas inclure dans la recherche, puis en cliquant sur le bouton **Supprimer**. Cette action supprime les attributs sélectionnés de la liste des attributs pouvant être recherchés.

Rechercher dans toute l'organisation (si l'option n'est pas cochée, la recherche est limitée au conteneur en cours)
Cochez cette case pour que la recherche concerne l'organisation toute entière.

Un type de contrôle associé est Contrôle de recherche.

Sous-formulaire

Le type de contrôle Sous-formulaire est un moyen d'utiliser des interfaces utilisateur personnalisées pour des attributs complexes à plusieurs valeurs. Certains adaptateurs IBM Security Identity Manager utilisent rarement ce type de contrôle.

Le sous-formulaire est un type de contrôle spécial utilisé pour démarrer une page de servlet, JSP ou HTML statique à partir d'une fenêtre en incrustation qui s'ouvre à partir d'un formulaire IBM Security Identity Manager personnalisé. Les sous-formulaires permettent de soumettre un nombre arbitraire de noms de paramètres et de valeurs à un servlet ou à une page JSP personnalisé et de créer des interfaces utilisateur personnalisées pour les attributs à plusieurs valeurs complexes.

Tableau 25. Paramètres de sous-formulaire

Paramètre	Description	Valeur
customServletURI	URI du servlet, JSP, ou de la page HTML statique à démarrer à partir du formulaire principal. Si un servlet est implémenté et déployé dans l'application Web par défaut pour IBM Security Identity Manager, la valeur de ce paramètre est identique à celle du *modèle d'URL* définie dans web.xml dans la balise *servlet-mapping*, sans la barre oblique (/). Si une page JSP est implémentée, la valeur de ce paramètre est le nom de fichier JSP avec une extension de fichier jsp. Ce paramètre est obligatoire sur tous les sous-formulaires.	Nom de servlet ou de fichier JSP, par exemple `sample.jsp`
Nom de paramètre	Nom et valeur de paramètre arbitraires inclus dans la demande HTTP qui démarre la ressource dans customServletURI.	*Valeur de paramètre*, par exemple le servlet racfconnectgroup

Bloc de texte

Place une zone de texte en regard de l'attribut. Un bloc de texte est une zone de texte à plusieurs lignes, utilisée pour regrouper la saisie de l'utilisateur et afficher les données précédemment recueillies.

Zone de texte

Place une zone de texte en regard de l'attribut. Un bloc de texte est une zone de texte à plusieurs lignes, utilisée pour regrouper la saisie de l'utilisateur ou afficher les données précédemment recueillies.

UMask

Permet à un utilisateur de définir des droits d'accès UNIX aux fichiers et répertoires.

Propriétés utilisées par Form Designer

Utiliser la page Propriétés pour configurer le format et les contraintes des attributs.

La page Propriétés comporte les onglets suivants :

Format

Utilisez cet onglet pour modifier le format d'un formulaire. Les zones disponibles dans cet onglet sont les suivantes :

Nom Utilisez cette zone pour ajouter ou modifier le nom d'un attribut. Cette valeur correspond à l'identifiant utilisé par le formulaire pour traiter des attributs LDAP.

Type de données
Utilisez cette zone pour ajouter ou modifier le type de données d'un attribut, tel que chaîne d'annuaire, nom distinctif, code binaire ou un autre type de données.

Libellé
Utilisez ce champ pour ajouter ou modifier un libellé lisible par l'utilisateur pour l'attribut. Par exemple, $homepostaladdress, où le symbole $ (dollar) indique une clé permettant de rechercher une chaîne dans un regroupement de ressources.

Taille Utilisez cette zone pour ajouter ou modifier la largeur visible en pixels pour les types de contrôle suivants : Zone de texte, Mot de passe, Contrôle de recherche et Occurrences de recherche. La taille représente le nombre d'éléments visibles pour les types de contrôle : Zone de liste (ListBox) et Liste de texte éditable (Editable TextList).

Lignes
Utilisez cette zone pour ajouter ou modifier la valeur utilisée par le type de contrôle Zone de texte (TextArea) pour représenter le nombre de lignes de texte visibles.

Colonnes
Utilisez cette zone pour ajouter ou modifier la valeur utilisée par le type de contrôle Zone de texte (TextArea) pour représenter la largeur visible en largeur de caractères moyenne.

Largeur
Utilisez cette zone pour ajouter ou modifier la valeur utilisée par le type de contrôle Sous-formulaire (SubForm) pour représenter la largeur d'une fenêtre en incrustation en pixels.

Cette propriété est également utilisée par les contrôles Liste déroulante (DropDownBox), Liste de texte modifiable (EditableTextList), Zone de liste (ListBox), Contrôle de recherche (SearchControl) et Occurrence de recherche (SearchMatch) pour représenter la largeur de leur zone de liste modifiable associée, en pixels. Pour les contrôles Liste de texte modifiable (EditableTextList) et Occurrence de recherche (SearchMatch), la largeur détermine également celle des zones de texte associées, en pixels.

Si la largeur n'est pas spécifiée, la valeur supposée par défaut est de 300 pixels. Si la largeur de ces contrôles est égale à zéro, les zones de liste modifiables associées ne sont pas de taille fixe et sont redimensionnées de façon dynamique. La taille dépend des options ajoutées.

Hauteur
Utilisez cette zone pour ajouter ou modifier la valeur utilisée par le type de contrôle Sous-formulaire (SubForm) pour représenter la hauteur d'une fenêtre en incrustation en pixels.

Lecture seule lors de la modification
Cochez cette case pour définir un attribut en lecture seule. Seul le libellé apparaît dans le formulaire et les utilisateurs ne peuvent pas modifier la valeur de l'attribut.

Direction
Sélectionnez la direction du texte :

hériter permet d'afficher le texte dans le même sens que la catégorie de formulaire à laquelle appartient l'attribut

ltr permet d'afficher le texte de gauche à droite

rtl permet d'afficher le texte de droite à gauche

Masquer lors de la modification

Cochez cette case pour masquer la zone d'attribut dans le formulaire lorsque ce dernier est à l'état modifié. Par exemple, si vous cochez cette case pour la zone Propriétaire dans un formulaire de service, cette zone apparaît lorsque les utilisateurs créent un service mais elle n'apparaît pas lorsqu'ils le modifient.

Contraintes

Utilisez cet onglet pour entrer les valeurs des zones de contraintes pour garantir le type et la syntaxe des données que les utilisateurs sont autorisés à entrer dans les zones du formulaire. Les contraintes personnalisées sont des restrictions de divers types appliquées aux données entrées dans les zones. Lorsque vous sélectionnez un type de contrôle **Contrôle de recherche** (Search Control), **Occurrence de recherche** (Search Match), **Zone de liste** (ListBox) ou **Zone de liste déroulante** (DropDownBox), toutes les zones de contrainte sont désactivées, sauf pour la contrainte **Requis** (Requis).

Requis

Cochez cette case pour empêcher la soumission du formulaire sauf si une certaine valeur est saisie dans le champ où la contrainte est placée.

Valider et mettre à jour les contraintes

Dans la zone en regard du bouton **Valider et mettre à jour les contraintes**, qui se trouve au bas de la liste des types de contrainte, entrez un exemple de valeur pour l'attribut que vous avez sélectionné dans la zone de présentation du modèle de formulaire, puis cliquez sur le bouton **Valider et mettre à jour les contraintes**. Cela testera la valeur entrée par rapport aux contraintes activées pour l'attribut. Si la valeur de test que vous entrez répond à toutes les contraintes, un message de réussite s'affiche lorsque vous cliquez sur le bouton **Valider et mettre à jour les contraintes**.

Les contraintes peuvent être classées dans les catégories générales suivantes :

Contraintes syntaxiques

Autorise uniquement les valeurs respectant les règles qui définissent des suites de caractères et des segments structurés.

Adresse électronique

Cochez cette case pour garantir que la syntaxe de la valeur fournie dans le champ où la contrainte est placée satisfait les règles suivantes :

- Contient un signe @
- Les caractères non valides, tels que `< > ( ) . ; " \ [ ]` n'apparaissent pas avant le signe @
- Le signe @ doit être suivi d'un nom de domaine ou d'une adresse IP valide

Adresse IP (IPV4)
Sélectionnez cette case à cocher pour garantir que la valeur entrée dans la zone où se trouve cette contrainte est une adresse IPV4 valide sous la forme `127.0.0.1`. Les quatre octets sont séparés par un point et aucun des octets ne dépasse `255`.

Adresse IP (IPV6)
Cochez cette case pour garantir que la valeur entrée dans le champ où cette contrainte est placée respecte la représentation textuelle des adresses IP définies dans RFC 2373. Par exemple, `0:0:0:0:0:0:0:1` correspond à l'adresse IPV6 en boucle. Pour plus de détails, voir RFC 2373.

Nom de domaine
Cochez cette case pour garantir que la valeur entrée dans la zone où cette contrainte est placée respecte la syntaxe des noms de domaine Windows NT. Le nom doit commencer par deux barres obliques inversées (\\) et peut contenir jusqu'à 15 caractères, à l'exception de : `" / \ [ ] : ; | = , + * ? < >`

Il ne peut pas comporter uniquement des points et des espaces.

Caractères non valides
Dans cette zone, tapez les caractères qui seront considérés comme non valides pour la zone.

Nom distinctif
Cochez cette case pour s'assurer que la valeur entrée dans cette zone est conforme à la structure de nom distinctif. Par exemple, `cn=`*`nom commun`*`, ou=`*`nom organisationnel`*`, o=`*`organisation`*.

Contraintes de type de données
Accepte les valeurs comprises dans une fourchette de caractères ou de nombres.

ASCII uniquement
Cochez cette case pour restreindre les caractères autorisés dans le champ aux seuls caractères ASCII.

ASCII7
Cochez cette case pour restreindre les caractères autorisés dans le champ aux seuls caractères ASCII-7.

ASCII8
Cochez cette case pour restreindre les caractères autorisés dans le champ aux seuls caractères ASCII-8.

Entier uniquement
Cochez cette case pour n'autoriser que des nombres entiers dans ce champ.

Numérique
Cochez cette case pour n'autoriser que des valeurs numériques dans ce champ.

Plage de dates
Tapez une plage de dates pour forcer une date de fin à se situer après une date de début.

Contraintes de valeur
Requiert un paramètre, tel que `Longueur maximale = 10`, où `10` correspond au paramètre auquel la valeur doit se conformer.

Caractères non valides
Caractères qui ne sont pas autorisés.

Longueur maximale
Tapez une valeur numérique limitant la longueur de la valeur entrée pour le champ au nombre de caractères indiqué.

Longueur minimale
Tapez une valeur numérique empêchant la soumission du formulaire, à moins que la valeur entrée ait au moins autant de caractères que le nombre indiqué par cette contrainte.

Valeur maximale
Entrez une valeur numérique pour définir un point de fin supérieur pour la valeur entrée (correspondant au maximum à *n*).

Valeur minimale
Entrez une valeur numérique pour définir un point de fin inférieur pour la valeur entrée (correspondant au minimum à *n*).

Nombre de lignes maximal
Entrez une valeur numérique pour garantir que la valeur entrée dans le formulaire ne dépasse pas le nombre maximal de lignes indiqué (dans une zone à plusieurs lignes).

Pas d'espace
Cochez cette case pour interdire tout espace sur le formulaire.

Propriétés modifiant l'interface utilisateur de Form Designer

IBM Security Identity Manager comporte des propriétés qui déterminent la présentation de l'interface du concepteur de formulaire.

Dans le fichier `ui.properties`, les propriétés suivantes modifient l'apparence de l'interface utilisateur du concepteur de formulaire :

express.java.formDesignHeightIE
Hauteur en pixels de l'applet Form Designer pour Internet Explorer

express.java.formDesignWidthIE
Largeur en pixels de l'applet Form Designer pour Internet Explorer

express.java.formDesignHeightMZ
Hauteur en pixels de l'applet Form Designer pour Mozilla

express.java.formDesignWidthMZ
Largeur en pixels de l'applet Form Designer pour Mozilla

Chapitre 8. Gestion des modèles de notification manuelle

Cette tâche permet de modifier les messages électroniques par défaut affichés pour les services manuels.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Vous pouvez modifier les messages par défaut affichés pour les services manuels. En modifiant les modèles, vous pouvez appliquer les modifications à chaque service manuel créé. Il n'est pas nécessaire de modifier les messages à chaque création d'un service manuel, sauf si cette modification est demandée par le service.

Remarque : Les modifications apportées aux modèles de notification n'ont aucune conséquence sur les messages pour les services manuels existants.

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **puis sur l'option permettant de configurer les modèles de notification manuelle**. La page Modèles s'affiche.
2. Sélectionnez l'opération puis cliquez sur **Modifier**. La page de modification de modèle s'affiche.
3. Dans la zone **Objet**, modifiez le texte indiquant l'objet de la notification par courrier électronique qui sera envoyée. L'objet peut contenir du texte brut et des balises de contenu dynamique.
4. Dans la zone **Corps texte en clair**, modifiez le texte à afficher dans le corps du message. Le contenu peut être constitué de texte brut, de balises de contenu dynamique et de code JavaScript. Ce contenu est affiché pour les destinataires du message qui ne voient pas les notifications par courrier électronique HTML.
5. Dans la zone **Corps XHTML**, entrez le texte à afficher dans le corps de la notification par courrier électronique au format HTML. Le contenu peut être constitué de texte brut, de balises de contenu dynamique et de code JavaScript. Ce contenu est affiché pour les destinataires du message qui voient les notifications par courrier électronique HTML.
6. Cliquez sur **OK** pour enregistrer les modifications. La page Modèles s'affiche à nouveau.

Que faire ensuite

Modifiez le modèle de notification pour une autre opération ou cliquez sur **Fermer** pour quitter cette page.

Chapitre 9. Gestion d'entités

Une *entité* est un utilisateur ou un objet pour lequel des informations sont stockées.

Il existe de nombreux types d'entités système, tels que des règles et des flux de travaux, mais seuls les types d'entité suivants peuvent être personnalisés :

- Compte
- BPPerson (utilisateur d'une organisation partenaire)
- BusinessPartnerOrganization
- Organisation
- Utilisateur
- Service

Les administrateurs système peuvent personnaliser des entités système existantes en mappant sélectivement des attributs de l'entité à des attributs classe LDAP personnalisés. Les administrateurs système peuvent également créer des entités personnalisées Utilisateur et Utilisateur d'une organisation partenaire en associant des noms d'entité uniques à des types d'entité IBM Security Identity Manager standard.

Ajout d'entités système

Créer des entités Utilisateur et Utilisateur d'une organisation partenaire à associer à une nouvelle classe LDAP personnalisée.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Lorsque vous ajoutez une entité de type Utilisateur ou Utilisateur d'une organisation partenaire, la classe LDAP réelle qui stocke l'entité doit être créée avant que vous n'utilisiez cette tâche pour ajouter des entités.

Les classes LDAP personnalisées et leurs attributs doivent être créés directement dans votre magasin de données en utilisant des outils compatibles avec le logiciel de référentiel de données LDAP. Créez les classes avant de les associer à une entité IBM Security Identity Manager personnalisée. Une fois créée, la classe peut être associée à une entité IBM Security Identity Manager personnalisée. Mappez ses attributs aux attributs IBM Security Identity Manager.

Pourquoi et quand exécuter cette tâche

Toutes les classes LDAP, auxiliaires et structurelles, qui commencent par `er` sont considérées comme des classes gérées par IBM Security Identity Manager. Elles sont donc exclues de la liste des classes LDAP à l'intérieur de la tâche Gérer les entités.

Lorsque vous ajoutez une entité personnalisée, vous devez examiner le type de contrôle par défaut de chaque attribut. Remplacez-le par un type de contrôle approprié dans la page de personnalisation. Reportez-vous à une entité IBM Security Identity Manager standard ayant le même type que l'entité personnalisée pour afficher les types de contrôles affectés aux attributs de l'entité standard.

Pour ajouter une entité système personnalisée, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer les entités**. La page Gérer les entités s'affiche.
2. Dans la page Gérer les entités, cliquez sur **Ajouter**. L'assistant Créer une entité s'affiche.
3. Dans la page Sélectionner un type, sélectionnez le type d'entité que vous voulez créer, puis cliquez sur **Suivant**.
4. Dans la page Informations détaillées sur l'entité, exécutez les étapes suivantes :
   a. Dans la zone **Nom d'entité**, entrez un nom unique pour l'entité.
   b. Cliquez sur **Rechercher** pour rechercher et indiquer une classe LDAP qui stocke l'entité.
   c. Dans la page Sélectionner une classe LDAP, cliquez sur **Rechercher** pour afficher une liste de classes LDAP.
   d. Sélectionnez le nom de la classe d'objets, puis cliquez sur le bouton **OK**. La zone **Classe LDAP** est remplie avec le nom de classe d'objets que vous avez indiqué.
   e. Cliquez sur **Parcourir les attributs de nom** pour rechercher et indiquer Les entrées valides pour la zone **Attributs de nom** dépendent de la classe LDAP qui est sélectionnée. La page Sélectionner un attribut qui s'affiche contient la liste des attributs de nom de la classe LDAP que vous avez sélectionnée.
   f. Dans la page Sélectionner un attribut, sélectionnez l'attribut de nom que vous voulez associer à la nouvelle entité, puis cliquez sur le bouton **OK**. La zone **Attribut de nom** est remplie avec l'attribut de nom que vous avez sélectionné.
   g. Dans la liste **Attributs de recherche par défaut**, sélectionnez les attributs de recherche que vous voulez ajouter à l'entité, puis cliquez sur **Ajouter**. Sélectionnez les attributs qui peuvent être recherchés, par exemple le type chaîne ou le type numérique.
   h. Une fois les informations de l'entité indiquées, cliquez sur **Suivant**.
5. Dans la page Mappage d'attributs, mappez un attribut en exécutant les étapes suivantes :
   a. Sélectionnez un attribut dans la liste **Attributs d'Identity Manager**.
   b. Sélectionnez un attribut dans la liste **Attributs LDAP personnalisés**.
   c. Cliquez sur **Mapper**.
   d. Facultatif : Pour obtenir le mappage par défaut, sélectionnez une paire d'attributs dans la table et cliquez sur **Réinitialiser**.
   e. Une fois le mappage terminé, cliquez sur **Terminer**.

Résultats

Un message indique que vous avez correctement créé une entité.

Que faire ensuite

Exécutez d'autres tâches de gestion de l'entité ou cliquez sur **Fermer**.

Modification des entités système

Visualiser et modifier le mappage qui indique comment une entité IBM Security Identity Manager se réfère à une classe LDAP personnalisée.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas modifier le type d'entité en raison de la définition du schéma associé. A la place, vous devez supprimer l'entité et créer une entité avec le type souhaité.

Pour modifier une entité existante, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer les entités**. La page Gérer les entités s'affiche.
2. Sur la page Gérer les entités, cochez la case à côté de l'entité que vous voulez modifier, puis cliquez sur **Modifier**. Le bloc-notes Modifier une entité s'affiche.
3. Cliquez sur l'onglet **Informations détaillées sur l'entité** ou sur l'onglet **Mappage d'attributs**.
4. Changez l'entité puis cliquez sur **OK**.

Que faire ensuite

Un message s'affiche indiquant que vous avez mis à jour l'entité.

Exécutez d'autres tâches de gestion de l'entité ou cliquez sur **Fermer**.

Suppression d'entités système

Supprimer des entités système du système IBM Security Identity Manager.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas supprimer d'entité système s'il existe des unités dépendantes dans cette entité.

Pour supprimer une entité système, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer les entités**. La page Gérer les entités s'affiche.
2. Sur la page Gérer les entités, cochez la case à côté de l'entité que vous voulez supprimer, puis cliquez sur **Supprimer**. Pour sélectionner toutes les entités système, cochez la case située en haut de cette colonne.
3. Dans la page Confirmer, cliquez sur **Supprimer** pour supprimer l'entité ou cliquez sur **Annuler**.

Résultats

Un message s'affiche indiquant que vous avez supprimé l'entité.

Que faire ensuite

Exécutez d'autres tâches de gestion de l'entité ou cliquez sur **Fermer**.

Personnalisation du schéma de rôle

Les administrateurs personnalisent un schéma de rôle en ajoutant des attributs facultatifs au protocole LDAP IBM Security Identity Manager puis au schéma de définition de rôle (classe d'objet *erRole*).

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez au protocole LDAP IBM Security Identity Manager.
2. Ajoutez de nouveaux attributs de type facultatifs. Ajoutez, par exemple, l'attribut `designation`. Pour plus d'informations, voir *LDAP - Guide d'installation et de configuration*.
3. Mettez à jour la classe d'objet *erRole* dans le protocole IBM Security Identity Manager pour associer les nouveaux attributs. Par exemple, mettez à jour la classe d'objet *erRole* dans IBM Tivoli Directory Server en utilisant la console d'administration Web Tivoli Directory Server et en associant l'attribut `designation` à la classe d'objet *erRole*. Pour plus d'informations sur Tivoli Directory Server, voir le centre de documentation *IBM Security Identity Manager*.
4. Vérifiez que le schéma de rôle est correctement personnalisé.
5. Vérifiez qu'IBM Security Identity Manager et que le protocole LDAP IBM Security Identity Manager sont en cours d'exécution.
6. Lancez la console d'administration IBM Security Identity Manager.
7. Sélectionnez **Configurer le système > Concevoir des formulaires**.
8. Mettez à jour le modèle de formulaire de rôle pour afficher le nouvel attribut.

Résultats

Vous pouvez afficher les nouveaux attributs sur la console d'administration IBM Security Identity Manager lors de l'affichage des définitions de rôle.

Que faire ensuite

Vous pouvez définir, modifier, sauvegarder et restaurer des attributs personnalisés lors de la création ou de la modification d'un rôle.

Chapitre 10. Gestion des types de propriété

Les *types de propriété* permettent de classer les comptes. La tâche **Gérer les types de propriété** permet de classer les types de propriété dans votre entreprise. Si vous configurez plusieurs types de propriété de compte, IBM Security Identity Manager invite les utilisateurs à sélectionner le type de propriété lors de la demande d'un compte ou de l'attribution de compte à des utilisateurs.

IBM Security Identity Manager inclut les éléments suivants : :

- Périphérique
- Individuel
- Système
- Fourn.

En tant qu'administrateur, vous pouvez créer des types de propriété supplémentaires.

Un compte ne peut avoir qu'un seul type de propriété. Le type de propriété dépend de l'utilisation souhaitée du compte. Il a des conséquences sur le processus de gestion des mots de passe. Par exemple, la synchronisation des mots de passe permet de changer les mots de passe pour les comptes ayant le type de propriété, "Individuel".

Création de types de propriété

En tant qu'administrateur, vous pouvez créer des types de propriété supplémentaires.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Pour créer un type de propriété, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Gérer les types de propriété**. La page **Gérer les types de propriété** affiche les types de propriété par défaut.

   Les types de propriété par défaut sont les suivants :

   - Périphérique
   - Individuel
   - Système
   - Fourn.
2. Cliquez sur **Créer**. La page **Créer type de propriété** s'affiche.
3. Procédez comme suit :

a. Dans la zone **Clé du type de propriété**, entrez un nom personnalisé pour le type de propriété.
b. (Facultatif) Dans la zone **Description**, entrez une description du type de propriété.

4. Cliquez sur **OK** pour sauvegarder le nouveau type de propriété.

Résultats

Un message indique que vous avez créé un type de propriété. Le nouveau type de propriété s'affiche sur la page **Gérer les types de propriété**.

Que faire ensuite

Créez ou modifiez des types de propriété supplémentaires ou cliquez sur **Fermer**.

Suppression des types de propriété

Lorsque les types de propriété ne sont plus valides, les administrateurs peuvent définir tous les types de propriété, sauf Individuel.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système. Un type de propriété peut être défini uniquement s'il n'est associé à aucun compte.

Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas supprimer un type de propriété s'il est associé à un compte.

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Gérer les types de propriété** pour afficher la page qui répertorie les types de propriété actuellement définis.
2. Sélectionnez le type de propriété à supprimer :
   a. Pour sélectionner un type spécifique, sélectionnez la case à cocher correspondante.
   b. Pour sélectionnez tous les types, cliquez sur la case à cocher dans la partie supérieure de la colonne.
3. Cliquez sur **Supprimer**. Une page de confirmation s'affiche.
4. Sur la page Confirmer, effectuez une des actions suivantes :
   a. Cliquez sur **Supprimer** pour supprimer le type de propriété.
   b. Cliquez sur **Annuler** pour arrêter le processus de suppression.

Résultats

Un message s'affiche indiquant que vous avez supprimé le type de propriété. La page **Gérer les types de propriété** n'affiche plus le type de propriété supprimé.

Que faire ensuite

Vous pouvez créer ou supprimer un type de propriété.

Chapitre 11. Gestion des opérations

Vous pouvez configurer des flux de travaux opérationnels pour des entités et des types d'entité système IBM Security Identity Manager. Les opérations de types d'entité fournies avec le produit peuvent être personnalisées pour implémenter les exigences de sécurité de votre organisation.

Une *opération* est une action qui peut être effectuée sur une entité. Les opérations définies pour un type d'entité spécifique sont utilisées par toutes les entités de ce type. Toutefois, si une opération est définie pour une entité spécifique, l'opération définie est prioritaire par rapport à l'opération de type entité.

Les administrateurs système peuvent créer des opérations ou modifier les opérations existantes pour des entités et des types d'entité.

Les opérations relatives aux types d'entité suivants peuvent être personnalisées :

- Compte
- Utilisateur
- Utilisateur d'une société partenaire

Une opération relative à un utilisateur, à une entreprise partenaire ou à un compte s'applique à toute entité Utilisateur, Utilisateur d'une organisation partenaire ou Compte, sauf si une opération personnalisée est définie au niveau de l'entité.

Opération d'ajout

L'opération d'ajout est lancée chaque fois qu'une demande d'ajout est transmise pour un type d'entité donné. Par exemple, une opération d'ajout pour un type d'entité Utilisateur est effectuée lorsqu'un nouvel utilisateur est ajouté au système.

Le flux de travaux défini par défaut pour l'opération d'ajout dépend du type d'entité ajouté.

Pour les entités Utilisateur et Utilisateur d'une organisation partenaire, le flux de travaux par défaut des opérations d'ajout d'entité fait appel aux extensions de flux de travaux `createPerson` et `enforcePolicyForPerson`.

Figure 10. Flux de travaux de l'opération d'ajout Utilisateur et Utilisateur d'une organisation partenaire

Le flux de travaux défini par défaut pour l'opération d'ajout d'une entité Compte utilise l'extension de flux de travaux `createAccount`.

Figure 11. Flux de travaux de l'opération d'ajout de compte

Figure 12. Flux de travaux de l'opération d'ajout d'utilisateur d'Identity Manager

Opération de changement du mot de passe

L'opération de changement du mot de passe (changePassword) est lancée chaque fois qu'une demande de changement du mot de passe est transmise pour une entité Compte.

Le flux de travaux défini par défaut pour l'opération de modification du mot de passe utilise l'extension de flux de travaux `changePassword`.

Figure 13. Flux de travaux de l'opération changePassword

Opération de suppression

L'opération de suppression est lancée chaque fois qu'une demande de suppression est transmise pour un type d'entité donné.

Le flux de travaux défini par défaut pour l'opération de suppression utilise les extensions de flux de travaux `deletePerson` ou `deleteAccount`.

Figure 14. Flux de travaux de l'opération de suppression de compte

Figure 15. Flux de travaux de l'opération de suppression d'Utilisateur et d'Utilisateur d'une organisation partenaire

Opération de modification

L'opération de modification est lancée chaque fois qu'une demande est transmise pour modifier une entité.

Le flux de travaux défini par défaut pour l'opération de modification dépend du type d'entité modifié.

Le flux de travaux défini par défaut pour l'entité Compte utilise l'extension de flux de travaux `modifyAccount`.

Figure 16. Flux de travaux de l'opération de modification de compte

Le flux de travaux défini par défaut pour les entités Utilisateur et utilisateur d'une organisation partenaire utilise les extensions de flux de travaux `modifyPerson` et `enforcePolicyForPerson`.

Figure 17. Flux de travaux de l'opération de modification de type d'entité Utilisateur et Utilisateur d'une organisation partenaire

Opération de restauration

L'opération de restauration est lancée chaque fois qu'une demande de restauration est transmise pour un type d'entité donné.

Le flux de travaux défini par défaut pour l'opération de restauration utilise l'extension de flux de travaux `restorePerson` ou `restoreAccount`.

Figure 18. Flux de travaux de l'opération de restauration de compte

Figure 19. Flux de travaux de l'opération de restauration des entités Utilisateur et Utilisateur d'une organisation partenaire

Opération d'auto-inscription

L'opération d'auto-inscription (selfRegister) est lancée lorsqu'une personne tente de s'ajouter elle-même à IBM Security Identity Manager. Cette opération est disponible uniquement pour une entité Utilisateur ou Utilisateur d'une organisation partenaire.

L'opération selfRegister comporte par défaut les étapes suivantes :

1. Création d'une entité d'utilisateur
2. Vérification que l'entité d'utilisateur respecte les règles existantes

Pour que l'opération selfRegister puisse être utilisée, l'élément de démarrage ou la ligne de transition entre l'élément de démarrage et l'élément d'extension createPerson doit contenir un code JavaScript qui calcule le conteneur auquel

l'entité d'utilisateur est ajoutée. Ce code JavaScript peut être un PostScript dans l'élément de démarrage ou une définition personnalisée pour la ligne de transition.

Ce diagramme illustre le flux de travaux par défaut défini pour l'opération selfRegister.

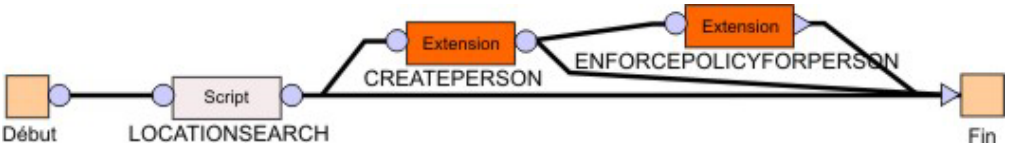


Figure 20. Flux de travaux de l'opération selfRegister

Opération de suspension

L'opération de suspension est lancée chaque fois qu'une demande de restauration est transmise pour un type d'entité donné.

Le flux de travaux par défaut de l'opération de suspension utilise l'extension de flux de travaux `suspendAccount` ou `suspendPerson`. Ce diagramme illustre le flux de travaux de l'opération de suspension de base.

Figure 21. Flux de travaux de l'opération de suspension de compte

Figure 22. Flux de travaux de l'opération de suspension des entités Utilisateur et Utilisateur d'une organisation partenaire

Opération de transfert

L'opération de transfert est lancée chaque fois qu'une demande de transfert est transmise pour une entité Utilisateur ou Utilisateur d'une organisation partenaire.

Le flux de travaux par défaut de l'opération de transfert utilise les extensions de flux de travaux `transferPerson` et `enforcePolicyForPerson`.

Figure 23. Flux de travaux de l'opération de transfert des entités Utilisateur et Utilisateur d'une organisation partenaire

Ajout d'opérations pour des entités

Les administrateurs système ajoutent des opérations d'entité.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

A titre d'exemple, la définition d'une nouvelle opération peut impliquer l'ajout d'une opération pour recertifier un utilisateur ou une entité de compte. Spécifiez un flux de travaux d'approbation qui approuve ou suspend l'entité.

Pour ajouter une opération pour une entité, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer des opérations**. La page Gérer des opérations s'affiche.
2. Dans la page Gérer des opérations, sélectionnez un des niveaux d'opération suivants :
   - Sélectionnez **Niveau global** pour définir une opération applicable à toutes les entités et à tous les types d'entité. Les opérations globales n'ont pas d'effet implicite sur les entités à moins d'être explicitement démarrées à l'intérieur des opérations au niveau du type d'entité ou de l'entité. Les opérations globales peuvent également être appelées dans une règle de cycle de vie.
   - Sélectionnez le niveau **Type d'entité** pour définir une opération au niveau du type d'entité. Sélectionnez un type d'entité dans la liste **Type d'entité**.
   - Sélectionnez **Niveau de l'entité** pour remplacer les opérations qui sont définies au niveau du type d'entité. Sélectionnez un type d'entité dans la liste **Type d'entité**, puis sélectionnez une entité dans la liste **Entité**.
3. Cliquez sur **Ajouter**. La page Opération d'ajout s'affiche.
4. Dans la zone **Nom de l'opération**, entrez un nom pour l'opération du flux de travaux que vous voulez définir dans l'entité système correspondante. Pour remplacer une opération définie au niveau du type d'entité, indiquez son nom et cliquez sur **Continuer**. La page Définir une opération s'affiche et l'applet Java du concepteur de flux de travaux est démarré.
5. Dans le concepteur de flux de travaux, définissez le processus de flux de travaux, puis cliquez sur le bouton **OK**. Pour définir le processus de flux de travaux, faites glisser les noeuds de conception de la palette des noeuds vers l'espace de conception de l'opération. Connectez-les ensuite avec les lignes de transition. Après avoir placé un noeud de conception dans l'espace de conception de l'opération, cliquez deux fois dessus pour configurer ses propriétés. Assurez-vous que tous les noeuds sont connectés et que toutes les propriétés requises sont définies pour chaque noeud. Vérifiez que la condition de transition est définie pour chaque lien.

Résultats

Un message s'affiche indiquant que vous avez créé l'opération pour le niveau spécifié. Cliquez sur **Fermer**.

Que faire ensuite

Lorsque la page Gérer des opérations s'affiche, cliquez sur **Régénérer** pour régénérer le tableau **Opérations** et afficher la nouvelle opération.

Modification d'opérations pour des entités

Les administrateurs système peuvent modifier des opérations d'entité existante.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Pour modifier une opération pour une entité, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer des opérations**. La page Gérer des opérations s'affiche.
2. Dans la page Gérer des opérations, sélectionnez **Niveau global**, **Niveau type d'entité** ou **Niveau de l'entité** pour afficher la liste des opérations que vous voulez modifier.
3. Cochez la case en regard de l'opération que vous voulez modifier, puis cliquez sur **Modifier**. Pour sélectionner toutes les opérations, cochez la case située en haut de cette colonne. La page Définir une opération s'affiche et l'applet Java du concepteur de flux de travaux est démarré.
4. Dans le concepteur de flux de travaux, modifiez l'opération pour l'entité système, puis cliquez sur le bouton **OK**. Pour définir le processus de flux de travaux, faites glisser les noeuds de conception de la palette des noeuds vers l'espace de conception de l'opération. Connectez-les ensuite avec les lignes de transition. Après avoir placé un noeud de conception dans l'espace de conception de l'opération, cliquez deux fois dessus pour configurer ses propriétés. Assurez-vous que tous les noeuds sont connectés et que toutes les propriétés requises sont définies pour chaque noeud. Vérifiez que la condition de transition est définie pour chaque lien.

Résultats

Un message s'affiche indiquant que vous avez mis à jour l'opération pour l'entité. Cliquez sur **Fermer**.

Que faire ensuite

Lorsque la page Gérer des opérations s'affiche, cliquez sur **Régénérer** pour régénérer le tableau **Opérations**.

Suppression d'opérations pour des entités

Les administrateurs système peuvent supprimer une opération d'entité existante.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Seules les opérations définies par l'utilisateur peuvent être supprimées.

Pour supprimer une opération pour une entité, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer des opérations**. La page Gérer des opérations s'affiche.
2. Dans la page Gérer des opérations, sélectionnez **Niveau global**, **Niveau type d'entité** ou **Niveau de l'entité** pour afficher la liste des opérations que vous voulez supprimer.
3. Cochez la case en regard de l'opération que vous voulez supprimer, puis cliquez sur **Supprimer**. Pour sélectionner toutes les opérations, cochez la case située en haut de cette colonne. Une page de confirmation s'affiche.
4. Dans la page Confirmer, cliquez sur **Supprimer** pour supprimer l'opération ou cliquez sur **Annuler**.

Résultats

Un message s'affiche indiquant que vous avez supprimé l'opération pour l'entité. Cliquez sur **Fermer**.

Que faire ensuite

Lorsque la page Gérer des opérations s'affiche, cliquez sur **Régénérer** pour régénérer le tableau **Opérations**.

Chapitre 12. Gestion des règles de cycle de vie

Les règles de cycle de vie peuvent être utilisées pour automatiser les nombreuses tâches manuelles que les administrateurs doivent exécuter en raison d'événements fréquents récurrents comme l'inactivité des comptes, l'expiration du mot de passe ou l'expiration du contrat, qui sont régis par les règles métier. Les règles de cycle de vie peuvent également limiter le risque d'inapplication de certaines règles.

Présentation

La mise en place de règles de cycle de vie permet aux administrateurs de définir des événements pouvant être déclenchés à intervalles de temps réguliers, à certains horaires et d'après des critères évalués au niveau d'une entité. L'administrateur peut ensuite associer des opérations de cycle de vie qui s'exécuteront à la suite de cet événement. Toutes les règles de cycle de vie se composent de deux éléments :

- La définition d'un événement qui déclenche la règle
- L'identification de l'opération de cycle de vie qui exécute les actions indiquées dans la règle

Chaque règle peut être définie de l'une des manières suivantes :

- Globale
- Associée à un type d'entité
- Associée à une entité

En ce qui concerne les règles globales, un événement est défini par un intervalle de temps. Par exemple, une fois par mois ou chaque lundi à 8h00. Les règles de cycle de vie globales sont indépendantes de toute entité système particulière. Les opérations de cycle de vie qui peuvent être appelées par une règle globale doivent également être de nature globale, car aucun contexte n'est disponible pour appeler une opération basée sur une entité ou sur un type d'entité.

En ce qui concerne les règles Entité et Type d'entité, elles possèdent également un événement défini par un intervalle de temps. Toutefois, ces règles ont pour objectif d'affecter plusieurs entités simultanément.

Critères de correspondance des événements

Un événement distinct se déclenche pour chaque objet de cycle de vie. Pour empêcher le déclenchement d'événements pouvant concerner des milliers d'objets susceptibles de ne pas être associés à la règle, des critères de correspondance sont disponibles.

Sans ces critères de correspondance, l'opération de cycle de vie associée sera appliquée à chaque objet de l'entité ou du type d'entité donné.

Avec les critères, les opérations s'appliqueront uniquement aux objets correspondant à ces critères. Les critères sont définis à l'aide de la syntaxe de filtre LDAP. Le filtre identifie tous les objets répondant aux critères et déclenche l'événement uniquement pour ces objets. Si aucun objet ne correspond au filtre, l'événement n'est pas déclenché. Par exemple, les critères pourraient être définis pour tous les comptes où `(erAccountStatus = 1)`, ce qui signifie que les comptes sont suspendus.

Planifications et filtres de règle de cycle de vie

Le filtre reposant sur les attributs, seuls les attributs associés au schéma de l'entité ou du type d'entité sont acceptés.

Vous pouvez également être amené à inclure des données d'environnement ou des données externes dans le filtre Par exemple, il peut être nécessaire d'inclure l'heure actuelle ou une valeur obtenue dans une base de données client. L'inclusion de ces données s'effectue en autorisant l'insertion de macros dans le filtre. Par exemple, un filtre vérifiant si un mot de passe a été changé au cours des 30 derniers jours peut se présenter comme suit : `(erPswdLastChanged>=${system.date - 30})`.

Remarque : Sans filtre, toutes les entités sont renvoyées. Des macros de relations d'entité peuvent être utilisées dans les filtres de règles de cycle de vie.

L'intervalle défini pour un événement peut être créé à partir des options suivantes :

Quotidien
Déclenche l'événement de cycle de vie de manière quotidienne. Après avoir sélectionné cette option, cliquez sur l'icône représentant une horloge pour indiquer une heure dans la zone **A ce stade**.

Hebdomadaire
Déclenche l'événement de cycle de vie une fois par semaine. Après avoir sélectionné cette option, sélectionnez un jour dans la liste **A ce jour de la semaine**, puis cliquez sur l'icône représentant une horloge pour indiquer une heure dans la zone **A cette heure**.

Mensuel
Déclenche l'événement de cycle de vie une fois par mois. Après avoir sélectionné cette option, sélectionnez une date dans la liste **A ce jour du mois**, puis cliquez sur l'icône représentant une horloge pour indiquer une heure dans la zone **A cette heure**.

Par heure
Déclenche l'événement de cycle de vie une fois par heure. Après avoir sélectionné cette option, sélectionnez une heure dans la liste **A cette minute**.

Annuel
Déclenche l'événement de cycle de vie à une date et une heure spécifiques de l'année. Après avoir sélectionné cette option, sélectionnez un mois dans la liste **Mois**. Sélectionnez ensuite une date dans la liste **A ce jour du mois** puis cliquez sur l'icône représentant une horloge pour indiquer une heure dans la zone **A cette heure**.

Pendant un mois spécifique
Déclenche l'événement de cycle de vie à un mois, un jour et une heure spécifiques. Après avoir sélectionné cette option, sélectionnez un mois dans la liste **Mois**. Sélectionnez ensuite un jour dans la liste **A ce jour de la semaine** puis cliquez sur l'icône représentant une horloge pour indiquer une heure dans la zone **A cette heure**.

Trimestriel
Déclenche l'événement de cycle de vie quatre fois dans l'année, au jour et à l'heure définis au cours du trimestre. La synchronisation s'effectue au jour indiqué après le 1er janvier, le 1er avril et le 1er octobre. Après avoir

sélectionné cette option, sélectionnez un jour dans la liste **A ce jour** et cliquez sur l'icône représentant une horloge pour indiquer une heure dans la zone **A cette heure**.

Semestriel
Déclenche l'événement de cycle de vie deux fois dans l'année, au jour et à l'heure définis au cours du semestre. La synchronisation s'effectue au jour indiqué après le 1er janvier et le 1er juillet. Après avoir sélectionné cette option, sélectionnez un jour dans la liste **A ce jour** et cliquez sur l'icône représentant une horloge pour indiquer une heure dans la zone **A cette heure**.

Remarque : Il est possible d'indiquer plusieurs planifications.

Une planification d'évaluation de règle de cycle de vie contient uniquement une référence à une définition de règle correspondante. Si une définition de règle de cycle de vie change avant que l'évaluation planifiée ne commence, cette dernière utilise la version mise à jour de la définition et non la définition de règle qui était initialement planifiée.

Dans cet exemple, une règle de cycle de vie est créée. Elle recherche une fois par jour les comptes dans lesquels aucune modification de mot de passe n'a eu lieu au depuis 90 jours. Une notification par courrier électronique est envoyée aux propriétaires des comptes qui répondent aux critères de recherche pour la règle de cycle de vie, les informant qu'ils doivent changer leur mot de passe.

Tout d'abord, une opération de cycle de vie appelée `remindToChangePassword` est construite pour le type d'entité Compte. Elle est définie comme une opération basée sur une instance (non statique). Par conséquent, elle a l'objet de compte lui-même comme paramètre d'entrée. La logique applicative de l'opération est définie à l'aide d'une activité d'ordre de travail qui envoie le message de rappel au propriétaire du compte en incluant l'ID utilisateur du compte dans le message.

Une règle de cycle de vie est ensuite créée pour le type d'entité Compte appelé `passwordExpiration` qui référence l'opération `remindToChangePassword`. Elle inclut un événement avec un intervalle d'évaluation **quotidien** à **12h00** ainsi que le filtre suivant : `(&(erAccountStatus=0)(erPswdLastChanged<=${system.date - 90}))`.

Traitement des règles de cycle de vie

L'exécution des opérations de cycle de vie peut prendre un certain temps pour traiter le jeu de résultats complet renvoyé par l'évaluation du filtre de règles de cycle de vie.

L'achèvement est principalement dû au temps requis pour accomplir les activités de flux de travaux manuelles associées à l'opération. Il est possible de planifier ou de lancer manuellement une évaluation de règle de cycle de vie afin qu'elle soit réexécutée avant que les opérations issues de la première évaluation de règle de cycle de vie ne se terminent pour l'ensemble des cibles. La seconde itération de l'évaluation de la règle de cycle de vie identifie les cibles restant en état opérationnel depuis l'évaluation d'origine. La deuxième itération ne lance pas à nouveau l'opération de cycle de vie pour ces cibles. Elle s'exécute toutefois pour toutes les cibles identifiées lors de la période d'évaluation de la règle de cycle de vie qui ne sont pas à l'état d'exécution.

Par exemple, une règle de cycle de vie peut détecter 100 entités correspondant à ses critères. Elle lance l'opération associée à la règle pour ces 100 entités. Supposons que 10 entités sont ajoutées au système. Des ajouts ont lieu après l'évaluation du cycle de vie initial et tandis que l'opération de règle de cycle de vie est appliquée aux 100 entités d'origine. Une deuxième itération de la règle de cycle de vie peut être initiée avant la fin de la première itération. La seconde itération ignore toutes les entités dont l'opération de règle de cycle de vie a été exécutée à partir de la première itération. La seconde itération ignore les entités jusqu'à ce qu'elle détecte une entité qui correspond à l'évaluation du filtre de règle de cycle de vie, mais pour laquelle cette règle de cycle de vie (correspondance de nom de règle) n'est pas exécutée. Dans ce cas, la seconde itération retrouve les 10 nouvelles entités ajoutées et s'exécute.

Il est important de comprendre ce comportement dans la mesure où il peut arriver que la seconde itération d'une règle de cycle de vie se termine avant la première itération. En théorie, l'évaluation de règle de cycle de vie que vous avez planifiée pour 10 heures peut se terminer avant l'évaluation de règle de cycle de vie planifiée pour 9 heures. Ne supposez pas qu'une opération de règle de cycle de vie est terminée pour toutes les cibles correspondantes d'après la fin d'une itération suivante de la même règle de cycle de vie. Pour déterminer quels éléments de demande sont terminés et lesquels ont été ignorés, consultez le journal d'audit de la demande terminée.

Modification des règles de cycle de vie

Une modification apportée au filtre ou à l'opération d'une règle de cycle de vie ne prendra effet qu'à la prochaine évaluation de la règle de cycle de vie.

La règle de cycle de vie peut être évaluée activement lorsque la modification est effectuée. L'évaluation en cours d'exécution continue d'utiliser la définition précédente de la règle de cycle de vie jusqu'à sa fin. Le flux de travaux peut changer pour l'opération alors que la règle de cycle de vie est activement évaluée par le système. La modification affecte l'évaluation en cours, quel que soit le moment où la modification est effectuée. Par exemple, si le filtre de règle de cycle de vie identifie 50 personnes et que l'opération de la règle de vie est nommée `Recertify`. Le fait de changer le nom de l'opération en `CheckPassword` n'affectera pas l'itération en cours de la règle. La modification ne s'appliquera qu'au prochain lancement de la règle. Cependant, si vous modifiez le flux de travaux relatif à l'opération `Recertifier` alors qu'il est actif, il se peut que 25 utilisateurs soient traités sous le flux de travaux d'origine. Les 25 utilisateurs restants seront traités sous le nouveau flux de travaux.

L'implémentation de la règle de cycle de vie est fortement dépendante du fait que la base de données contienne les informations de planification. Supprimer, mettre au rebut ou purger la table qui contient les informations de planification de la règle de cycle de vie a pour effet de désactiver les règles de cycle de vie associées. Dans ce cas, vous devez reconfigurer toutes les règles de cycle de vie et redéfinir leurs planifications.

Si l'opération associée à une règle de cycle de vie est supprimée ou renommée, elle ne peut pas être implémentée dans la règle de cycle de vie tant que la règle n'est pas reconfigurée.

Remarque : Lorsque vous ajoutez ou modifiez une règle de cycle de vie d'un entité, les mises à jour entrent en vigueur une fois que le délai du cache s'est écoulé (10 minutes, par défaut).

Informations relatives au schéma d'événement de cycle de vie

IBM Security Identity Manager fournit des attributs de schéma spécifiques qui facilitent la création d'événements du cycle de vie.

Ces attributs sont gérés par le serveur IBM Security Identity Manager et sont rendus disponibles par les services de données et depuis l'interface d'événement de cycle de vie. Voici la liste des ajouts :

- `erPersonItem`
  - `erCreateDate` – Date à laquelle l'utilisateur a été ajouté au système
  - `erLastStatusChangeDate` – Date de dernière modification de l'état de l'utilisateur. L'horodatage est mis à jour chaque fois que l'utilisateur est ré-enregistré ou suspendu.
  - `erlastoperation` – Disponible pour une utilisation personnalisée
  - `erpswdlastchanged` – Date de la dernière modification du mot de passe synchronisé de l'utilisateur
- `erAccountItem`
  - `erCreateDate` – Date à laquelle le compte a été ajouté au système
  - `erLastStatusChangeDate` – Date de la dernière modification de l'état du compte. L'horodatage est mis à jour chaque fois que l'utilisateur est ré-enregistré ou suspendu.
  - `erlastoperation` – Disponible pour une utilisation personnalisée

A l'exception des éléments à usage personnalisé, ces éléments de schéma sont gérés par le système.

Ajout de règles de cycle de vie pour les entités

Utilisez ces instructions pour définir des règles de cycle de vie pour les entités.

Avant de commencer

Seuls les administrateurs système peuvent exécuter cette tâche.

Pourquoi et quand exécuter cette tâche

Les règles de cycle de vie déclenchent des opérations qui sont définies dans la tâche Gérer des opérations. Suivant le type de règle de cycle de vie, les opérations correspondantes définies à ce niveau sont disponibles.

Les règles de cycle de vie diffèrent des opérations. La règle de cycle de vie qui est définie au niveau du type d'entité ou de l'entité ne remplace pas la règle de cycle de vie définie à un niveau supérieur. Chaque niveau a des événements de cycle de vie valides qui peuvent être exécutées séparément d'après la planification définie.

Pour ajouter une règle de cycle de vie pour un type d'entité, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer des règles de cycle de vie**. La page Gérer des règles de cycle de vie s'affiche.
2. Sur la page Gérer des règles de cycle de vie, sélectionnez un des niveaux de règle de cycle de vie suivants :

- Sélectionnez **Niveau global** pour définir une règle de cycle de vie sans aucun contexte d'entité.
- Sélectionnez le niveau **Type d'entité** pour définir une règle de cycle applicable au type d'entité. Sélectionnez un type d'entité dans la liste **Type d'entité**.
- Sélectionnez **Niveau de l'entité** pour définir une règle de cycle de vie applicable à un type d'instance de l'entité spécifique. Sélectionnez un type d'entité dans la liste **Type d'entité**, puis sélectionnez une entité dans la liste **Entité**.

3. Cliquez sur **Ajouter**. Le bloc-notes Gérer des règles de cycle de vie s'affiche.
4. Dans la page **Général** du bloc-notes Gérer des règles de cycle de vie, exécutez les étapes suivantes :
   a. Dans la zone **Nom**, entrez un nom unique pour la règle de cycle de vie à définir pour l'entité système correspondante.
   b. Facultatif : Dans la zone **Description**, entrez une description de la règle de cycle de vie.
   c. Dans la liste **Opération**, sélectionnez une opération à appeler lorsque l'événement se produit. Seules les opérations sans paramètre d'entrée peuvent être exécutées par la règle de cycle de vie.
   d. Cliquez sur l'onglet **Evénement**.
5. Dans la page **Evénement** du bloc-notes Gérer des règles de cycle de vie, exécutez les étapes suivantes :
   a. Dans la zone **Filtre de recherche**, entrez un filtre LDAP identifiant les objets concernés par l'événement. Par exemple, le filtre suivant capture tous les employés actifs qui n'ont pas modifié leur mot de passe depuis 90 jours à compter de la date à laquelle l'événement de cycle de vie se produit :
   ```
   (&(employeeType=active) (erPswdLastChanged<=${system.date - 90}))
   ```

   Remarque : Le filtre de recherche n'est pas applicable aux règles de cycle de vie du niveau global car les règles de cycle de vie du niveau global n'ont pas de contexte d'entité.
   b. Cliquez sur **Ajouter** pour définir une planification pour la règle de cycle de vie. La page Définir une planification s'affiche.
6. Sur la page Définir une planification, définissez une planification pour la règle de cycle de vie à exécuter, puis cliquez sur le bouton **OK**. Les zones qui s'affichent varient selon l'option de planification sélectionnée. La nouvelle planification s'affiche dans la page **Evénement** du bloc-notes Gérer des règles de cycle de vie.
7. Cliquez sur le bouton **OK** pour enregistrer la règle de cycle de vie et fermer le bloc-notes.

Résultats

Un message indique que vous avez créé avec succès une règle de cycle de vie pour l'entité. Cliquez sur **Fermer**.

Que faire ensuite

Lorsque la page Gérer des règles de cycle de vie s'affiche, cliquez sur **Régénérer** pour régénérer le tableau **Règles de cycle de vie** et afficher la nouvelle règle de cycle de vie.

Modification des règles de cycle de vie pour les entités

Utilisez ces instructions pour modifier des règles de cycle de vie.

Avant de commencer

Seuls les administrateurs système peuvent exécuter cette tâche.

Pourquoi et quand exécuter cette tâche

Pour modifier une règle de cycle de vie pour un type d'entité, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer des règles de cycle de vie**. La page Gérer des règles de cycle de vie s'affiche.
2. Sur la page Gérer des règles de cycle de vie, cochez la case en regard de la règle de cycle de vie que vous voulez modifier, puis cliquez sur **Modifier**. Le bloc-notes Gérer des règles de cycle de vie s'affiche.
3. Cliquez sur l'onglet **Général** ou l'onglet **Evénement**.
4. Effectuez les modifications souhaitées puis cliquez sur **OK**.

Résultats

Un message indique que vous avez mis à jour avec succès une règle de cycle de vie pour l'entité. Cliquez sur **Fermer**.

Que faire ensuite

Lorsque la page Gérer des règles de cycle de vie s'affiche, cliquez sur **Régénérer** pour régénérer le tableau **Règles de cycle de vie**.

Suppression des règles de cycle de vie pour les entités

Utilisez ces instructions pour supprimer des règles de cycle de vie.

Avant de commencer

Seuls les administrateurs système peuvent exécuter cette tâche.

Pourquoi et quand exécuter cette tâche

Pour supprimer une règle de cycle de vie pour un type d'entité, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer des règles de cycle de vie**. La page Gérer des règles de cycle de vie s'affiche.
2. Sur la page Gérer des règles de cycle de vie, cochez la case en regard de la règle de cycle de vie que vous voulez supprimer, puis cliquez sur **Supprimer**. Pour sélectionner toutes les règles de cycle de vie, cochez la case située en haut de cette colonne.
3. Sur la page Confirmer, cliquez sur **Supprimer** pour supprimer la règle de cycle de vie ou cliquez sur **Annuler**.

Résultats

Un message indique que vous avez supprimé avec succès une règle de cycle de vie pour l'entité. Cliquez sur **Fermer**.

Que faire ensuite

Lorsque la page Gérer des règles de cycle de vie s'affiche, cliquez sur **Régénérer** pour régénérer le tableau **Règles de cycle de vie**.

Exécution de règles de cycle de vie pour les entités

Utilisez ces instructions pour supprimer des règles de cycle de vie.

Avant de commencer

Seuls les administrateurs système peuvent exécuter cette tâche.

Pourquoi et quand exécuter cette tâche

L'exécution d'une règle de cycle de vie déclenche l'événement immédiatement au lieu de l'exécuter selon une planification définie.

Pour exécuter une règle de cycle de vie pour un type d'entité, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Gérer des règles de cycle de vie**. La page Gérer des règles de cycle de vie s'affiche.
2. Sur la page Gérer des règles de cycle de vie, cochez la case en regard de la règle de cycle de vie que vous voulez exécuter, puis cliquez sur **Exécuter**.
3. Sur la page Confirmer, cliquez sur **Exécuter** pour exécuter la règle de cycle de vie ou cliquez sur **Annuler**.

Résultats

Un message indique que vous avez soumis avec succès la règle de cycle de vie à exécuter. Cliquez sur **Fermer**.

Que faire ensuite

Lorsque la page Gérer des règles de cycle de vie s'affiche, cliquez sur **Régénérer** pour régénérer le tableau **Règles de cycle de vie**.

Expressions de filtre LDAP

IBM Security Identity Manager fournit un interpréteur intégré pour les filtres LDAP RFC 2254 et pour les deux extensions personnalisées de la syntaxe de filtre définie par le document RFC.

La première extension fournit une notation pour les variables des filtres LDAP qui référencent les relations IBM Security Identity Manager. Il s'agit de variables qui sont résolues en objets associés ou connectés. La seconde extension fournit une notation pour les variables dans les filtres LDAP qui font référence à un objet système et à un mot clé de date qui sont résolus en date et heure courantes. Ces

deux extensions de la syntaxe de filtrage LDAP sont interprétées et évaluées lors de l'exécution et s'appellent des *expressions de filtrage*. Ces expressions de filtrage permettent aux administrateurs de définir des filtres avec des parties dynamiques qui font référence à des abstractions utiles dans IBM Security Identity Manager. Les deux types d'expressions de filtrage pris en charge sont appelés *expressions de relation* et *expressions système*.

Expressions de relation

La connexion entre les objets domaine IBM Security Identity Manager est fournie par une relation.

Le propriétaire d'un compte, par exemple, est fourni par la relation propriétaire. Le service hôte d'un compte est fourni par la relation service. Le rôle d'un utilisateur est fourni par la relation rôle.

En général :

Objet cible	relation	Objet associé

Par exemple :

Utilisateur	rôle	Rôle

Où Utilisateur doit être associé à un rôle via la relation rôle. Les expressions de relation dans les filtre fournissent une méthode pour faire correspondre les objets domaine en fonction de leur relation avec les autres objets domaine.

La connexion entre les objets domaine IBM Security Identity Manager est fournie par une relation.

La syntaxe d'une expression de filtrage consiste en un symbole de dollar en ouverture ($) suivi d'une accolade gauche ({) immédiatement suivie d'un nom de relation, d'un point (.) , puis d'un nom d'attribut et enfin d'une accolade droite (}) pour fermer l'expression. Par exemple :

```
(${relationship.attribute}=value)
```

relation est le nom d'une relation dans IBM Security Identity Manager et comporte les éléments suivants :

- Parent
- Propriétaire
- Organisation
- Superviseur
- Parrain
- Administrateur
- Rôle
- Compte
- Service

attribut correspond à n'importe quel nom d'attribut valide pour l'objet associé. Les références à ces connexions ou liaisons entre les objets domaine sont souvent utiles dans les recherches. Elles sont également utiles pour la correspondance lors de l'autorisation (dans les ACI) et dans la gestion des cycles de vie (règles de cycle de vie) lors de l'exécution des opérations.

Dans les ACI, les expressions de relation sont utilisées pour accorder des accès aux objets domaine en partie en fonction de leur relation mutuelle. Par exemple, un ACI pour un utilisateur, qui accorde une autorisation de modification avec l'expression de relation suivante utilisée comme filtre ACI, accorde un droit à tous les utilisateurs dont le superviseur a pour nom usuel Jen Jenkins :

```
(${supervisor.cn}=Jen Jenkins)
```

De même, un ACI de compte qui accorde l'autorisation de recherche avec l'expression de relation suivante utilisée comme filtre ACI accorde un droit à tous les comptes dont le service (l'hôte) est nommé `Serveur SuSE`. L'accès est accordé en fonction de la relation d'un objet à un autre.

```
(${service.erservicename}=SuSE Server)
```

Dans la gestion du cycle de vie, les expressions de relation sont également utilisées dans les règles de cycle de vie pour faire correspondre les objets domaine en fonction de leur relation avec les autres objets domaine. Les règles peuvent lancer la même opération sur toutes les correspondances. Par exemple, une règle de cycle de vie pour un utilisateur, pour laquelle l'opération est définie pour s'interrompre avec l'expression de relation utilisée comme règle, suspend effectivement tous les utilisateurs dans le rôle Brokers (dynamique ou statique) à chaque exécution de la règle de cycle de vie :

```
(${role.errolename}=Brokers)
```

Evaluation d'expressions de relation

L'évaluation de l'expression de relation peut être conçue comme la réponse par oui ou par non à quatre questions.

Il s'agit des questions suivantes :

- Qu'est-ce qui entre (l'expression elle-même) ?
- Qu'est-ce qui sert de comparaison (l'objet cible) ?
- Qu'est-ce qui sort (l'objet connecté ou associé) ?
- L'objet associé correspond-il à la valeur à droite du signe égale ?

Si tel est le cas, la réponse fournie par l'évaluation est oui, et l'objet cible est dit correspondre à l'expression de relation.

La première colonne de la table suivante présente les expressions de relation utilisées dans un exemple de filtre. la seconde colonne contient le type des objets valides pour l'expression et la troisième colonne indique le type d'objet désigné par la relation.

Tableau 26. Exemples d'expressions de relation de filtrage

Expression de relation	Objet cible	Objet associé
`(${parent.ou}=Sales)`	N'importe lequel (sauf Compte)	N'importe quel conteneur
`(${owner.cn}=John Smith)`	Compte	Utilisateur
`(${organization.o}=Marketing)`	N'importe lequel (sauf Compte)	Organisation
`(${supervisor.cn}=Jen Jenkins)`	N'importe lequel (sauf Compte)	Utilisateur
`(${sponsor.cn}=Pete West)`	N'importe lequel (sauf Compte)	Utilisateur

Tableau 26. Exemples d'expressions de relation de filtrage (suite)

Expression de relation	Objet cible	Objet associé
(${administrator.cn}=Joe Peterson)	N'importe lequel (sauf Compte)	Utilisateur
(${role.errolename}=Brokers)	N'importe lequel (sauf Compte)	Rôle
(${account.uid}=JUser)	N'importe lequel (sauf Compte)	Compte
(${service.erservicename}=SuSE Server)	Compte	Service

Il est important de se souvenir des étapes d'évaluation lors de la création des expressions de relation. Plus important encore, le type d'objet associé doit être connu pour pouvoir faire référence à un nom d'attribut valide après l'opérateur point (.) pour garantir que le format des expression est correct, qu'elles sont valides et qu'elles peuvent générer une correspondance. Une vue du schéma LDAP est une référence utile ici. Le système résout les expressions de relation à la première entité répondant aux critères de filtre. Le système envoie ensuite des requêtes pour tous les objets dont la relation est indiquée dans le filtre pour cette entité. Assurez-vous de créer des filtres suffisamment spécifiques pour renvoyer l'entité que vous tentez de prendre comme destinataire.

Mot-clé nom

Une variation de la syntaxe des expressions de relation se matérialise par l'inclusion du mot clé `nom` spécial apparaissant après le point (`.`) .

L'utilisation du mot-clé `nom` après le point (`.`) fait référence à l'attribut `nom` dans un profil. Cette syntaxe constitue une méthode générale pour pointer vers un objet en fonction du nom au lieu d'utiliser un nom d'attribut explicite. Cette généralité comporte, toutefois, cette limite qu'elle n'est utile que dans les contextes dans lesquels un profil est connu au moment de l'évaluation.

Par exemple, supposez que vous ayez un ACI pour un compte Lotus Notes. Cet ACI permet de modifier des comptes et utilise le filtre suivant :

```
(${service.name}=SuSE Server)
```

Le mot-clé `nom` désigne l'attribut nom du profil de service `Lotus Notes`. Il est possible d'utiliser `nom` dans ce contexte. Lors de l'autorisation (au moment de l'évaluation), le profil de service Lotus Notes est toujours connu et son attribut `nom` peut être résolu. Le mot clé `nom` n'est pas valide dans les règles de cycle de vie, car la référence à l'attribut `nom` dans un profil donné est ambiguë lorsque la règle de cycle de vie est exécutée. L'attribut `nom` ne peut donc pas être résolu.

Expressions système

Ces expressions sont utilisées pour cibler des objets domaine en fonction d'une valeur de temps généralisées par rapport à la date système en cours.

La syntaxe des expressions système comporte relativement peu d'éléments.

Les expressions de système se composent des éléments suivants :

- un nom d'attribut
- un opérateur relationnel (`<=` ou `>=`)
- un symbole dollar ($) suivi d'une accolade gauche ({)

immédiatement suivi des mots clés `system.date`

un opérateur arithmétique plus ou moins (+/-) suivi d'un nombre de jours

une accolade droite (}) pour fermer l'expression

Par exemple :

```
(gmtattributename[<=|>=]${system.date [ + | - ] days})
```

Les expressions système résolvent un filtre LDAP concret qui est compris par un serveur d'annuaires LDAP ou par l'interpréteur de filtre intégré IBM Security Identity Manager. Voici, par exemple, un filtre qui cible les comptes avec des mots de passe dont l'ancienneté est égale ou supérieure à 90.

```
(erpswdlastchanged<=${system.date – 90})
```

L'exemple ci-dessus peut être utilisé dans un ACI de comptes qui accorde un accès en lecture et en écriture à l'attribut password (mot de passe) pour permettre aux utilisateurs de mettre à jour leurs mots de passe. Le même filtre peut être également utilisé dans une règle de cycle de vie qui suspend les comptes si le mot de passe du compte n'a pas été modifié au cours des 90 derniers jours. Cette expression de filtre particulière donne le filtre LDAP concret suivant :

```
(erpswdlastchanged<=200912311200Z)
```

Il est également possible et valide syntactiquement d'exprimer une plage de dates comme critère de correspondance par rapport aux objets de domaine. Intégrez plusieurs expressions système dans un filtre composite, comme dans l'exemple suivant :

```
(&(erpswdlastchanged>=${system.date – 90})(!(erpswdlastchanged>
=${system.date – 30})))
```

Le filtre fait correspondre les comptes et les mots de passe dont l'âge est compris entre 90 et 30 jours. D'autres combinaisons et filtres composites peuvent être utiles selon la complexité du filtre et le nombre d'objets devant faire l'objet d'une correspondance.

Chapitre 13. Configuration des directives de jointure de règle

Les *directives de jointure* de règles d'application des accès déterminent les valeurs de paramètres d'application des accès qui prévalent lorsqu'il existe plusieurs règles d'application des accès concernant le même compte. Une directive de jointure définit la façon de traiter un attribut lorsqu'un conflit se produit entre les règles d'attribution des accès. Les directives de jointure applicables uniquement à l'attribut sélectionné s'affichent.

Le type de cible d'habilitation joue également un rôle important dans la manière dont les directives de jointure de règles déterminent l'habilitation accordée lorsqu'il existe des conflits de règles. Lorsque deux règle ou plus accordent la même habilitation, l'habilitation la plus spécifique est prioritaire. Par exemple, une règle d'application des accès inclut un droit défini pour accorder un accès à un type de service (c'est-à-dire AIX nommé AIX105). La seconde règle peut inclure un droit défini pour accorder un accès à une instance spécifique de ce service (c'est-à-dire, AIX). Dans ce cas, le droit le plus spécifique est prioritaire.

IBM Security Identity Manager fournit plusieurs types de directives de jointure. La table suivante affiche la liste des types et décrit chacun d'entre eux.

Remarque : Les types Union et Intersection sont définis uniquement dans les attributs à valeurs multiples.

Tableau 27. Directives de jointure

Directive de jointure	Description
`Union`	Regroupe les valeurs d'attributs et supprime les redondances. Cette directive de jointure est le paramètre par défaut pour les attributs à valeurs multiples si aucune autre directive de jointure n'est indiquée.
`Intersection`	Uniquement les valeurs de paramètre communes à toutes les règles.
`Append`	Ajoute la valeur d'attribut textuelle définie dans une règle à la suite de la valeur d'attribut définie dans une autre règle. Le type de jointure APPEND a été conçu pour les attributs de texte à valeur unique, tels que `comment on winlocal service`. Lorsque vous effectuez une jointure de paramètres d'application des accès à l'aide du type de jointure APPEND, toutes les valeurs individuelles sont concaténées dans une même valeur de chaîne. La concaténation fournit un délimiteur défini par l'utilisateur entre les valeurs. Ce délimiteur peut être défini (modifié) dans le fichier enrolepolicies.properties, où la ligne en cours s'affiche de la façon suivante : `provisioning.policy.join.Textual.AppendSeparator=<<<>>>`
`And`	Désigne l'opérateur mathématique AND appliqué à une chaîne booléenne représentant une valeur booléenne. TRUE & TRUE = TRUE TRUE & FALSE = FALSE FALSE & FALSE = FALSE
`Or`	Désigne l'opérateur mathématique OR appliqué à une chaîne booléenne représentant une valeur booléenne. TRUE || TRUE = TRUE TRUE || FALSE = TRUE FALSE || FALSE = FALSE
`Highest`	Utilise uniquement la valeur d'attribut numérique maximale tirée des règles conflictuelles.

Tableau 27. Directives de jointure (suite)

Directive de jointure	Description
`Lowest`	Utilise uniquement la valeur d'attribut numérique minimale tirée des règles conflictuelles.
`Average`	Calcule la moyenne des valeurs d'attribut numériques à partir des règles conflictuelles et utilise la valeur moyenne.
`Bitwise_Or`	Désigne l'opérateur mathématique bit par bit OR appliqué à une valeur d'attribut représentant une chaîne de bits.
`Bitwise_And`	Désigne l'opérateur mathématique bit par bit OR appliqué à une valeur d'attribut représentant une chaîne de bits.
`Precedence_Sequence`	Utilise une priorité d'ordre définie par l'utilisateur pour déterminer la valeur d'attribut à utiliser.
`Priority`	Utilise la priorité de la règle d'administration pour déterminer la valeur d'attribut à utiliser. Si les règles conflictuelles ont la même priorité, l'ordre dans lequel ces règles sont évaluées est aléatoire. L'évaluation dépend de la règle utilisée par le système pour la première extraction. Par exemple, deux règles ont la même priorité et définissent le même attribut avec différentes valeurs. Si l'attribut utilise le type de directive de jointure 'Priority', la valeur d'attribut renvoyée par la règle varie en fonction de l'extraction du système.

Le tableau suivant présente chaque type d'attribut de service, la directive de jointure correspondante et la directive de jointure par défaut.

Tableau 28. Attributs de maintenance

Type d'attribut de service	Directive de jointure applicable	Directive de jointure par défaut
Attribut de nombre ou chaîne à valeurs multiples	UNION, INTERSECTION.PRIORITY, CUSTOM	UNION
Chaîne comportant une valeur unique	PRECEDENCE_SEQUENCE, PRIORITY, AND, OR, APPEND, BITWISE_AND, BITWISE_OR, HIGHEST, LOWEST, AVERAGE, CUSTOM	PRIORITY
Chaîne booléenne comportant une valeur unique	AND, OR, PRIORITY, CUSTOM	OR
Entier comportant une valeur unique	HIGHEST, LOWEST, AVERAGE, PRIORITY, PRECEDENCE_SEQUENCE, CUSTOM	HIGHEST
Chaîne binaire comportant une valeur unique	BITWISE_AND, BITWISE_OR, PRIORITY, CUSTOM	BITWISE_OR

Remarque : Des directives de jointure personnalisées peuvent être définies à l'aide de Java. Les administrateurs peuvent utiliser des directives de jointure personnalisées pour modifier complètement la logique de jointure intégrée.

Personnalisation des comportements de jointure des règles

Vous pouvez personnaliser le comportement des directives de jointure avec vos règles d'application des accès pour chaque attribut en fonction du type de service.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

IBM Security Identity Manager fournit plusieurs types de directives de jointure. Vous pouvez étendre les fonctions de directive de jointure existantes ou en créer vous-même.

Vous pouvez définir des directives de jointure personnalisées en créant une classe Java personnalisée, en l'ajoutant au chemin de classe de votre serveur d'applications et en fournissant le nom de classe Java qualifié complet dans l'interface de configuration des règles lorsque vous paramétrez une directive de jointure pour un attribut.

Si, en plus des tâches ci-dessus, vous étendez ou remplacez une des classes des directives de jointure, vous devez ajouter la clé et la valeur de la propriété personnalisée au fichier `enrolepolicies.properties`. Par exemple, si vous aviez développé une nouvelle classe telle que `com.abc.TextualEx` afin de remplacer la classe existante pour les jointures textuelles, la ligne d'enregistrement serait similaire à l'exemple suivant :

```
provisioning.policy.join.Textual= com.abc.TextualEx
```

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Configurer les comportements de jointure des règles**. La table Comportement de jointure des règles d'administration pour configurer les directives de jointure des règles d'application des accès s'affiche sous la forme de deux sous-fenêtres dans la fenêtre.
2. Dans la fenêtre Comportement de jointure des règles d'administration, cliquez sur **Type de service** pour choisir un service dans une liste de services disponibles, par exemple `ITIMService`.
3. Sélectionnez un des attributs pour le type. La sous-fenêtre de droite affiche le nom, la description et les directives de jointure applicables de l'attribut sélectionné.
4. Cliquez sur **Directive de jointure** dans le panneau de droite pour configurer la priorité des règles d'application des accès en sélectionnant l'une des directives de jointure répertoriées. Les valeurs suivantes peuvent s'appliquer, suivant l'attribut que vous sélectionnez :

   Union Indique les valeurs d'attributs et supprime les redondances. Cette directive de jointure est sélectionnée par défaut si aucune autre directive de jointure n'est indiquée.

   Intersection
   Indique uniquement les valeurs de paramètre qui sont communes à toutes les règles.

   Priority
   Utilise la priorité de la règle d'administration pour déterminer la valeur d'attribut à utiliser. Si les règles conflictuelles ont la même priorité, la première règle trouvée par le système est utilisée.

OR Désigne l'opérateur mathématique OR appliqué à une chaîne booléenne représentant une valeur booléenne. TRUE || TRUE = TRUE TRUE || FALSE = TRUE FALSE || FALSE = FALSE

AND Désigne l'opérateur mathématique AND appliqué à une chaîne booléenne représentant une valeur booléenne. TRUE & TRUE = TRUE TRUE & FALSE = FALSE FALSE & FALSE = FALSE

Append
Ajoute la valeur d'attribut textuelle définie dans une règle à la suite de la valeur d'attribut définie dans une autre règle.

Le type de jointure APPEND est utilisé sur les attributs de texte à valeur unique (tels que `comment` dans le service WinNT).

Lorsque vous effectuez une jointure de paramètres d'application des accès à l'aide du type de jointure APPEND, toutes les valeurs individuelles sont rassemblées en une valeur de chaîne unique et séparées par un délimiteur défini par l'utilisateur. Ce délimiteur peut être défini (modifié) dans le fichier enrolepolicies.properties, où la ligne en cours s'affiche de la façon suivante :

```
provisioning.policy.join.Textual.AppendSeparator=<<<>>>
```

Bitwise OR
Indique l'opérateur mathématique OU bit par bit appliqué à une chaîne de bits.

Bitwise AND
Indique l'opérateur mathématique ET bit par bit appliqué à une chaîne de bits.

Highest
Utilise la valeur d'attribut numérique maximale d'après les règles conflictuelles.

Lowest
Utilise la valeur d'attribut numérique minimale d'après les règles conflictuelles.

Average
Calcule la moyenne des valeurs d'attribut numériques à partir des règles conflictuelles et utilise la valeur moyenne.

Precedence sequence
Utilise une priorité d'ordre définie par l'utilisateur pour déterminer la valeur d'attribut à utiliser.

Custom
Définit une directive de jointure commune à l'aide du code Java. Ces directives permettent aux administrateurs de modifier complètement la logique de jointure intégrée. Entrez le nom de classe Java qualifié complet de la classe de directive de jointure personnalisée que vous avez créée pour l'attribut.

5. Cliquez sur **Règle d'alerte de conformité** pour configurer une règle d'alerte de conformité qui indique quand des alertes de conformité sont envoyées. Pour configurer une règle d'alerte de conformité, sélectionnez l'une des options suivantes :

Ordre numérique (la valeur la plus élevée génère une alerte)
Sélectionnez cette option si vous souhaitez générer une alerte de conformité avant d'envoyer une valeur d'attribut plus élevée à la ressource gérée. Utilisez cette option si la valeur d'attribut a été

augmentée suite à une évaluation de règle d'application des accès. Si la valeur d'attribut a été diminuée à la suite de l'évaluation, elle est automatiquement envoyée à la ressource gérée. Aucune alerte n'est générée.

Ordre numérique (la valeur la plus basse génère une alerte)
Sélectionnez cette option si vous souhaitez générer une alerte de conformité avant d'envoyer une valeur d'attribut plus faible au noeud géré. Utilisez cette option si la valeur d'attribut a été réduite suite à une évaluation de règle d'application des accès. Si la valeur d'attribut a été augmentée à la suite de l'évaluation, elle est automatiquement envoyée à la ressource gérée et aucune alerte n'est générée.

Ne jamais générer d'alerte
Sélectionnez cette option si vous ne voulez pas générer d'alerte de conformité lorsqu'une évaluation des règles d'attribution des accès conduit à une nouvelle valeur pour un attribut. Parce qu'aucune alerte de conformité n'est générée, la nouvelle valeur d'attribut est automatiquement envoyée à la ressource gérée.

Toujours générer une alerte
Sélectionnez cette option si vous voulez générer une alerte de conformité lorsqu'une évaluation des règles d'attribution des accès conduit à une nouvelle valeur pour un attribut. Le participant doit accepter la nouvelle valeur d'attribut avant que celle-ci ne soit envoyée à la ressource gérée. Cette valeur est la valeur par défaut pour les attributs comportant une seule valeur.

Ordre de priorité
Sélectionnez cette option si vous voulez que les valeurs supérieures de la liste soient considérées comme privilégiées par rapport aux valeurs inférieures. Lorsqu'une évaluation de règle d'application des accès génère une attribution de valeur d'attribut plus élevée, la valeur d'attribut est envoyée à la ressource gérée. Aucune alerte de conformité n'est générée. Si la valeur d'attribut a été diminuée suite à l'évaluation, une alerte de conformité est générée. Cette valeur est ensuite envoyée à la ressource gérée.

Remarque : Lorsque vous sélectionnez cette option, vous pouvez sélectionner **Déplacer vers le haut**, **Déplacer vers le bas**, **Supprimer** ou **Ajouter** pour organiser votre ordre de priorité.

6. Cliquez sur **Enregistrer** pour enregistrer les modifications.

Logique de validation des comptes

La logique de validation de compte fournit des informations sur une collection de règles de validation qui affectent un groupe de paramètres joints après application des règles de jointure de règles d'administration.

`Autoriser ou refuser les unions de paramètres`
Un groupe de valeurs de paramètres d'*autorisation* correspond à l'union des éléments suivants :

- Valeurs de paramètre constante obligatoire (sauf null)
- Valeurs de paramètres constantes facultatives (sauf null)
- Expressions régulières non rejetées avec habilitation optionnelle
- Valeur null exclue

Un groupe de valeurs de paramètres de *refus* correspond à l'union des éléments suivants :

- Expressions régulières non rejetées avec habilitation exclue
- Valeurs constantes exclues (sauf null)
- Valeur null avec habilitation optionnelle, obligatoire ou par défaut

Remarque : Les expressions régulières négatives, par exemple : `Correspondance avec tout, sauf un mot donné`, peuvent être difficiles à créer manuellement. Les paramètres optionnels et exclus se complètent mutuellement et doivent être utilisés chaque fois que possible.

Valeurs de paramètre null

Une valeur de paramètre obligatoire null implique que les valeurs de l'attribut correspondant d'un compte nouveau ou existant ne sont pas autorisées, sauf celles autorisées par toute autre valeur valide. Lorsque des valeurs d'attribut d'un compte existant sont refusées par un paramètre obligatoire de valeur null, ces valeurs sont supprimées automatiquement.

Une valeur de paramètre par défaut ou facultatif null implique que les valeurs de l'attribut correspondant d'un compte nouveau ou existant ne sont pas autorisées, sauf celles autorisées par toute autre valeur d'autorisation. Les valeurs actuellement définies ne sont pas supprimées.

Une valeur de paramètre null implique que toutes les valeurs de l'attribut correspondant d'un compte nouveau ou existant sont autorisées, sauf celles non autorisées par toute autre valeur d'autorisation.

Effets des valeurs d'attributs déterminantes sur un attribut à une seule valeur

Les valeurs de paramètre d'un attribut à une seule valeur ne peuvent être qualifiées qu'avec une habilitation par défaut ou obligatoire.

Une valeur de paramètre obligatoire implique que l'attribut doit toujours avoir la valeur indiquée. Toute modification de la valeur de paramètre obligatoire déterminante est automatiquement répercutée sur l'attribut de compte concerné. La suppression d'une valeur de paramètre obligatoire d'une habilitation déterminante peut entraîner la modification automatique de la valeur d'un attribut correspondant si aucun autre paramètre obligatoire ne régit le même attribut.

Une valeur de paramètre par défaut est utilisée pour l'application des accès des nouveaux comptes. Les valeurs d'attribut régies par un paramètre par défaut peuvent être remplacées à tout moment par une autre valeur du groupe de paramètres d'autorisation. La suppression d'une valeur de paramètre par défaut d'un paramètre déterminant ne supprime pas une valeur d'un attribut correspondant, sauf si une règle de jointure de paramètre est utilisée, par l'intermédiaire de laquelle un autre paramètre obligatoire régit désormais le même attribut.

Effets des valeurs de paramètres déterminantes sur un attribut à valeurs multiples

Les valeurs de paramètres d'un attribut à plusieurs valeurs peuvent être qualifiées avec les types d'habilitation obligatoire, par défaut, optionnel et exclu.

Une valeur de paramètre obligatoire implique que l'attribut correspondant doit avoir cette valeur. L'ajout d'une nouvelle valeur obligatoire (sauf null) ajoute automatiquement la valeur à tous les comptes existants. La suppression d'une valeur de paramètre obligatoire existante (sauf null) supprime

automatiquement la valeur de l'attribut, sauf s'il existe un autre paramètre d'autorisation pour la même valeur. Toute modification de la valeur d'un paramètre obligatoire revient à une suppression et à un ajout.

Une valeur de paramètre par défaut non null, n'est effective que dans l'application des accès des nouveaux comptes. Des valeurs d'attribut correspondantes peuvent être remplacées ensuite par une autre valeur du groupe d'autorisation. L'ajout d'une nouvelle valeur de paramètre par défaut (sauf null) n'a pas d'impact sur un attribut conforme. La suppression d'une valeur de paramètre par défaut (sauf null) ne supprime pas la valeur de l'attribut correspondant, sauf s'il existe un autre paramètre d'autorisation (autre que la valeur par défaut) pour la même valeur.

Valeurs de paramètre facultatives
Les valeurs de paramètre par défaut peuvent être définie comme constantes ou comme expressions régulières.

L'ajout d'une nouvelle valeur de paramètre constante facultative (sauf null) n'a pas d'effet sur un attribut conforme par ailleurs. La suppression d'une valeur de paramètre constante optionnelle (sauf null) peut supprimer cette valeur de l'attribut correspondant, sauf si un autre paramètre d'autorisation autorise la même valeur. La modification d'une valeur de paramètre constante optionnelle revient à une suppression et à un ajout.

L'ajout d'une nouvelle expression régulière optionnelle n'a pas d'effet sur un attribut conforme. La suppression ou la modification d'une expression régulière optionnelle peut entraîner la suppression des valeurs d'un attribut conforme par ailleurs, sauf s'il existe un autre paramètre d'autorisation pour la même valeur.

Valeurs de paramètres exclues
Les valeurs de paramètres exclues peuvent être définies comme constantes ou expressions régulières. Les valeurs de paramètres avec une habilitation exclue ne sont appliquées que dans le contexte d'une habilitation générique implicite.

L'ajout d'une valeur de paramètre constante exclue peut entraîner la suppression de la valeur de l'attribut correspondant, sauf s'il existe un autre paramètre d'autorisation pour la même valeur. La suppression d'une valeur de paramètre constante exclue (sauf null) n'a pas d'effet sur un attribut conforme par ailleurs. Toute modification d'une valeur de paramètre constante revient à une suppression et à un ajout.

L'ajout d'une expression régulière exclue peut entraîner la suppression des valeurs d'un attribut conforme, sauf s'il existe un autre paramètre d'autorisation pour la même valeur. La suppression ou la modification d'une expression régulière exclue n'a pas d'effet sur un attribut conforme.

Règle de priorité autorisée et non autorisée
Si une valeur d'attribut est en même temps autorisée et non autorisée en raison de l'existence de valeurs de paramètre conflictuelles, la valeur de paramètre d'autorisation prévaut sur la valeur de paramètre de rejet.

Habilitation d'attribut générique implicite
Pour vous aider à créer facilement des règles d'autorisation totale par défaut, vous pouvez utiliser une habilitation d'attribut *générique implicite*. Une valeur générique implicite existe pour un attribut si aucune valeur de paramètre d'autorisation n'est définie dans l'attribut. Par conséquent, toutes les valeurs sont autorisées, sauf les valeurs de paramètres exclues. La suppression du dernier paramètre d'un attribut change l'état de la valeur générique implicite.

Exemples de directives de jointure

Cette rubrique fournit des exemples qui montrent comment utiliser des directives de jointure des règles d'application des accès.

L'exemple suivant analyse la résolution des conflits en utilisant la priorité de règles, qui est une directive de jointure par défaut des attributs à une seule valeur. L'attribut erMaxStorage sur un serveur Windows permet de fournir à un utilisateur un espace de stockage limité sur un serveur.

Règle 1

Appartenance
Gestionnaires

Priorité
1

erMaxStorage
1000 (Mo), application : obligatoire

Règle 2

Appartenance
Employés

Priorité
2

erMaxStorage
200 (Mo), application: obligatoire

Lorsqu'un utilisateur appartient aux rôles Gestionnaires et employés, la priorité est utilisée pour résoudre le conflit entre les deux valeurs du paramètre erMaxStorage. Une personne qui appartient aux deux rôles reçoit la valeur erMaxStorage 1000 (Mo).

L'exemple suivant analyse la résolution des conflits en utilisant la séquence de priorité, qui est une directive de jointure non définie par défaut pour l'attribut à une seule valeur.

Règle 1

Appartenance
Gestionnaires

Priorité
2

eraddialincallback
4, application : obligatoire

Règle 2

Appartenance
Employés

Priorité
1

eraddialincallback
2, application : obligatoire

directive de jointure personnalisée dans l'attribut eraddialincallback
séquence de priorité (la plus élevée en premier)

- **4** Rappel utilisateur
- **2** Rappel fixe
- **1** Pas de rappel

Une personne peut appartenir aux rôles Gestionnaires et Employés. La séquence de priorité est utilisée pour résoudre le conflit entre deux valeurs de paramètre, même si la priorité dans la règle Employés est plus élevée. Cet utilisateur obtiendrait la valeur `eraddialincallback` 4 (rappel d'utilisateur).

Exemples de logique de jointure

Cette rubrique fournit des exemples qui montrent comment utiliser des directives de jointure des règles d'application des accès.

Cette section fournit des exemples supplémentaires de logique de jointure.

Scénario 1

Plusieurs droits applicables peuvent être joints. Si aucune valeur de paramètre n'est sélectionnée pour un attribut dans une règle (toutes les valeurs sont autorisées) et qu'une valeur de paramètre autorisée est entrée pour un attribut dans une autre règle (seule la valeur indiquée est autorisée), la valeur de paramètre ne peut avoir que la valeur indiquée par la seconde règle.

Scénario 2

Cet exemple illustre une directive de jointure des règles d'application des accès avec application de la priorité pour un attribut à valeur unique. La table suivante identifie deux règles d'application des accès pour ce scénario :

Tableau 29. Deux règles d'application des accès

Policy	Description
Policy 1	Priority = 1 Attribute: `erdivision` = divisionA, `enforcement` = DEFAULT
Policy 2	Priority = 2 Attribute: `erdivision` = divisionB, `enforcement` = MANDATORY

La règle d'administration 1 ayant une priorité plus élevée, seule sa définition de l'attribut `erdivision` est utilisée. La valeur de la règle 2 pour l'attribut `erdivision` est ignorée. Les valeurs autres que divisionA ne sont pas autorisées.

Scénario 3

Cet exemple illustre une directive de jointure des règles d'application des accès avec union pour un attribut à valeurs multiples. La table suivante identifie deux règles d'application des accès pour ce scénario :

Tableau 30. Exemples de règle d'application des accès

Policy	Description
Policy 1	Priority = 1 Attribute: `localgroup` = groupA, `enforcement` = DEFAULT

Tableau 30. Exemples de règle d'application des accès (suite)

Policy	Description
Policy 2	Priority = 2 Attribute: `localgroup = groupB, enforcement = MANDATORY`

Dans la mesure où la directive de jointure est définie comme étant UNION, la règle résultante utilise les définitions suivantes pour les règles :

- Lors de la création du compte, l'attribut `localgroup` est défini avec les deux valeurs groupA et groupB.
- Au cours des synchronisations, `localgroup` est défini comme groupB si l'attribut n'est pas défini ou qu'il est défini de façon incorrecte.

Chapitre 14. Mise en application des règles globales

L'*application des règles d'administration globales* représente la manière dont le système IBM Security Identity Manager accepte globalement ou non les comptes qui ne respectent pas les règles d'application des accès.

Lorsqu'une action d'application d'une règle est globale, l'application de la règle pour un service est définie par le paramètre de configuration par défaut. Vous pouvez définir que l'une des actions d'attribution des règles d'administration suivantes se produira si un compte possède un attribut non conforme.

Marquer
Caractérise par un signe un compte qui possède un attribut non conforme.

Suspendre
Suspend un compte qui possède un attribut non conforme.

Corriger
Remplace un attribut non conforme d'un compte par un attribut correct.

Alerte Emet une alerte pour un compte qui possède un attribut non conforme.

Remarque : Si un paramètre de mise en application des règles a été défini spécialement pour un service, ce paramètre est appliqué aux comptes non conformes, le paramètre de mise en application globale ne s'y appliquant pas.

Configuration de règles de mise en application globale

Un administrateur peut créer des règles de mise en application globale pour résoudre les comptes non conformes dans les services.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser les options suivantes lorsque vous configurez des règles de mise en application globale :

- **Marquer**
- **Suspendre**
- **Corriger**
- **Alerte**

Apposition d'une marque sur un compte

Un administrateur peut créer des règles de mise en application globale et apposer une marque sur un compte comportant un attribut non conforme.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Pour apposer une marque sur un compte comportant un attribut non conforme, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Configurer une mise en application des règles d'administration globales**.
2. Dans la page Configurer une mise en application des règles d'administration globales, sélectionnez **Marque**, puis **Soumettre** dans la section Mise en application.

   Remarque : La modification de l'action de mise en application des règles globales pour le système peut entraîner une réévaluation de la conformité du compte et une modification des données du compte.
3. Dans la page Confirmation, sélectionnez une heure et une date pour la planification de cette opération.

   Remarque : Lorsque vous sélectionnez cette option, vous pouvez sélectionner les icônes de l'agenda et de l'horloge pour personnaliser les date et heure planifiées.
   - Sélectionnez **Immédiatement**, puis **Soumettre** si vous voulez exécuter la demande immédiatement.

     Remarque : Les date et heure en cours sont affichées.
   - Sélectionnez **Date d'effet**, puis **Soumettre** si vous voulez exécuter la demande aux date et heure que vous avez personnalisées.
4. Sur la page Réussite, cliquez sur **Fermer**.

Suspension d'un compte

Un administrateur peut créer des règles de mise en application globale et suspendre un compte comportant un attribut non conforme.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Pour suspendre un compte comportant un attribut non conforme, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Configurer une mise en application des règles d'administration globales**.
2. Dans la page Configurer une mise en application des règles d'administration globales, sélectionnez **Suspendre**, puis **Soumettre** dans la section Mise en application.

   Remarque : La modification de l'action de mise en application des règles globales pour le système peut entraîner une réévaluation de la conformité du compte et une modification des données du compte.
3. Dans la page Confirmation, sélectionnez une heure et une date pour la planification de cette opération.

   Remarque : Lorsque vous sélectionnez cette option, vous pouvez sélectionner les icônes de l'agenda et de l'horloge pour personnaliser les date et heure planifiées.
   - Sélectionnez **Immédiatement**, puis **Soumettre** si vous voulez exécuter la demande immédiatement.

     Remarque : Les date et heure en cours sont affichées.
   - Sélectionnez **Date d'effet**, puis **Soumettre** si vous voulez exécuter la demande aux date et heure que vous avez personnalisées.
4. Sur la page Réussite, cliquez sur **Fermer**.

Remplacement d'un attribut non conforme par un attribut conforme

Un administrateur peut créer des règles de mise en application globale pour résoudre les comptes non conformes interdits dans les services. Il peut annuler l'accès des comptes qui n'ont pas été autorisés par les droits de la règle d'application des accès. Les comptes interdits peuvent ne pas être supprimés du service distant s'ils répondent aux critères des comptes d'exemption. Les critères sont définis dans le gestionnaire d'exemptions.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pour plus d'informations sur le mode de définition des comptes d'exemption, voir *Actions d'application d'administration* dans la rubrique ../admin/cpt/cpt_ic_services_policy.dita "Actions d'application d'administration" du document *IBM Security Identity Manager - Guide d'administration*.

Remarque : Votre administrateur peut remplacer le gestionnaire d'exemptions défini ou créé.

Pourquoi et quand exécuter cette tâche

Pour remplacer un attribut non conforme dans un compte par un attribut conforme, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Configurer une mise en application des règles d'administration globales**.
2. Dans la page Configurer une mise en application des règles d'administration globales, sélectionnez **Corriger**, puis **Soumettre** dans la section Mise en application.

   Remarque : La modification de l'action de mise en application des règles globales pour le système peut entraîner une réévaluation de la conformité du compte et une modification des données du compte. En outre, la sélection de l'option **Corriger** peut entraîner une *annulation de l'accès* du compte, sauf si le compte est exempté, ce qui correspond à la suppression du compte, si un compte n'est pas autorisé par les droits de la règle d'application des accès.
3. Dans la page Confirmation, sélectionnez une heure et une date pour planifier cette opération.

   Remarque : Après avoir sélectionné cette option, vous pouvez sélectionner les icônes de l'agenda et de l'horloge pour personnaliser les date et heure planifiées.
   - Sélectionnez **Immédiatement**, puis **Soumettre** si vous voulez exécuter la demande immédiatement.

     Remarque : Les date et heure en cours sont affichées.
   - Sélectionnez **Date d'effet**, puis **Soumettre** si vous voulez exécuter la demande aux date et heure que vous avez personnalisées.
4. Sur la page Réussite, cliquez sur **Fermer**.

Création d'une alerte sur un compte

Vous pouvez créer une **Alerte** pour émettre une alarme pour un compte ayant un attribut non conforme et configurer la notification par courrier électronique de cette alerte.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Si vous travaillez avec un service particulier en utilisant **Gérer les services** dans l'arborescence de navigation, vous pouvez configurer une alerte de mise en application des règles globales pour ce service. Cliquez sur l'icône en regard de ce dernier dans la liste. Sélectionnez **Configurer une mise en application des règles d'administration**. En cliquant sur **Utiliser une action de mise en application globale : alerte**, vous mettez en place une alerte de règle globale pour ce service aux date et heure que vous indiquez.

Pour configurer une alerte pour un compte comportant un attribut non conforme, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, sélectionnez **Configurer le système** > **Configurer une mise en application des règles d'administration globales**.
2. Dans la page Configurer une mise en application des règles d'administration globales, sélectionnez **Alerte** dans la section Mise en application.
3. Cliquez sur **Continuer**.
4. Dans la page Configurer une mise en application des règles d'administration globales, sélectionnez la page Général afin de fournir des informations et des paramètres pour l'alerte. Fournissez les informations sur les participants et les intervalles de temps. Indiquez les types de processus pour lesquels une alerte est générée et cliquez sur **Soumettre**.

   Fournissez les informations suivantes :

   Nom de l'alerte
   Indiquez le nom qui identifie l'alerte.

   Envoyer l'alerte de conformité à
   Indiquez les participants qui reçoivent une alerte de conformité.

   Nombre de jours d'attente avant de transférer l'alerte de conformité à un niveau supérieur
   Indiquez le nombre de jours avant le transfert d'une alerte à un niveau supérieur.

   Transférer l'alerte de conformité au niveau supérieur, à
   Indiquez les participants qui reçoivent une alerte de conformité transférée au niveau supérieur.

   Nombre de jours avant l'intervention du système
   Indiquez le nombre de jours que le système attend avant qu'une intervention n'ait lieu.

   Tableau Types de processus
   Indiquez les processus qui génèrent une alerte de conformité.

   Remarque : Si aucun type de processus n'est sélectionné, le système corrige automatiquement un compte non conforme pour ce type de processus. La correction consiste à modifier ou supprimer le compte.

   Générer une alerte
   Indiquez le type de processus pour lequel une alerte est générée. Cochez la case du type de processus pour lequel vous voulez générer des alertes.

   Type de processus
   Indiquez le type de processus de flux de travaux qui génère une alerte de conformité.
5. Sur la page Configurer une mise en application des règles d'administration globales, sélectionnez la page de messagerie électronique pour entrer du texte pour le message électronique de notification d'alerte. Vous pouvez également choisir d'utiliser le modèle par défaut. Si vous n'utilisez pas le modèle par défaut, accédez à la ligne Objet de la notification par courrier électronique et saisissez le corps du texte en clair ou le contexte dynamique XHTML.
6. Cliquez sur **Soumettre**.
7. Dans la page de confirmation, sélectionnez une heure et une date pour la planification de cette opération.

Remarque : Après avoir sélectionné cette option, vous pouvez sélectionner les icônes de l'agenda et de l'horloge pour personnaliser les date et heure planifiées.

- Sélectionnez **Immédiatement**, puis **Soumettre** si vous voulez exécuter la demande immédiatement.

  Remarque : Les date et heure en cours sont affichées.
- Sélectionnez **Date d'effet**, puis **Soumettre** si vous voulez exécuter la demande aux date et heure que vous avez personnalisées.

8. Sur la page Réussite, cliquez sur **Fermer**.

Chapitre 15. Importation et exportation de données

IBM Security Identity Manager importe et exporte des données tout en préservant l'intégrité des données.

Présentation

De nombreuses applications d'entreprise, notamment IBM Security Identity Manager, sont souvent déployées par étapes. De nouvelles règles d'administration et une logique applicative peuvent être développées et testées dans un environnement de test, puis migrées vers un environnement de fabrication.

Les tâches d'importation et d'exportation permettent de migrer les éléments de données IBM Security Identity Manager et les objets dépendants depuis un environnement de test vers un environnement de fabrication tout en préservant l'intégrité des données.

Vous pouvez utiliser les tâches d'importation et d'exportation pour importer des objets précédemment exportés à partir d'un fichier d'archive Java (fichier JAR). L'importation des types d'objet pris en charge est limitée aux seuls objets IBM Security Identity Manager exportés.

Le téléchargement de fichiers est limité à l'affichage de noms de fichiers à caractères codés sur deux octets dans HTTPServletResponse Java. Essayez d'utiliser des noms de fichiers conformes à ASCII lorsque vous vous dénommez les fichiers JAR d'exportation.

Migration des données

Le processus de migration des données sur les serveurs IBM Security Identity Manager consiste à rechercher des objets configurés et à les exporter depuis un serveur source, puis à les importer sur un serveur cible. La migration importe les objets dans un serveur cible.

La migration de données automatise l'extraction des types d'objet généralement configurés et leurs dépendances. Elle permet également de déplacer les configurations de travail ou les configurations transférées depuis un environnement de test vers un environnement de fabrication avec la garantie que les données sont importées sans perte d'intégrité. Ces informations sont destinées aux administrateurs qui souhaitent tirer parti de la fonction de migration des données de IBM Security Identity Manager avec les tâches d'importation et d'exportation.

Exportations

Il existe deux types d'exportation : partielle et complète. Ces deux types d'exportation génèrent un fichier JAR pouvant être téléchargé. Ce fichier contient un fichier XML d'objets sérialisés qui est ajouté à la liste des exportations réalisées.

Importations

Les importations sont initialisées par un administrateur sur un serveur cible après extraction des objets (après création d'un fichier JAR d'exportation) depuis un serveur source. Les importations comportent les étapes suivantes :

- Téléchargement du fichier JAR
- Evaluation des différences
- Résolution des conflits
- Validation des données dans le système

Application des règles d'administration

L'importation de règles d'application des accès et de rôles organisationnels dynamiques pourrait entraîner l'association de différentes personnes à de nouveaux rôles. Les règles importées comportant des modifications qui nécessitent une réévaluation peuvent déboucher sur les tâches de mise en application des règles suivantes :

- Evaluation des modifications de rôle dynamique et mise à jour des appartenances de rôle
- Recherche des règles d'application des accès associées aux règles de sélection d'hôte
- Association des règles d'application des accès et des appartenances au rôle aux règles qui sont importées
- Application des règles à tous les utilisateurs concernés avec un nouveau processus de flux de travaux.

Organigrammes

S'il existe des différences dans les organigrammes entre le serveur source (test) et le serveur cible (production), les objets importés seront alors traités comme de nouveaux objets.

Pour éviter la création d'objets en double, lorsque ces objets existent dans le système de production, assurez-vous que les organigrammes correspondent bien dans chaque système.

Dépendances d'objet pour la migration de données

Pour migrer des données, vous devez inclure toutes les dépendances de l'objet migré.

Une *dépendance* est en règle générale un objet référencé par un objet racine ou parent qui est requis dans un système cible pour importer le parent. Pour préserver l'intégrité des données tout au long du processus de migration, les tâches d'importation et d'exportation détectent et incluent automatiquement les dépendances d'objet exporté.

Comparaison entre les exportations complètes et les exportations partielles

L'exportation de tous les éléments avec **Exporter tout** permet d'enregistrer toutes les données prises en charge par cette fonction dans le système. Si vous exportez des éléments individuellement avec la fonction d'exportation partielle, vous risquez de ne pas exporter toutes les dépendances nécessaires au fonctionnement de l'objet.

Une exportation partielle enregistre uniquement les dépendances nécessaires à la création de l'objet enregistré. Par exemple, vous pouvez exporter une règle d'application des accès qui inclut une fonction de création de compte automatique. La règle d'identité permettant de créer l'ID utilisateur n'est pas exportée en tant que dépendance de la règle d'application des accès. La règle d'identité n'est pas requise pour la création de l'objet de règle d'application des accès. Elle pourrait, cependant, être nécessaire au but que vous prévoyez pour votre règle d'application des accès. Si tel est le cas, exportez et importez la dépendance en tant qu'objet distinct.

Règles d'administration

Les règles d'administration des identités et les règles d'administration des mots de passe ne sont pas exportées lors de l'exportation d'une règle d'application des accès. Vous devez exporter explicitement ces règles dans le processus d'exportation.

Les objets de rôle et de service des règles d'administration des identités, des mots de passe ou d'application des accès ne sont pas exportés par défaut. Pour exporter ces éléments, vous devez les ajouter manuellement à la liste d'exportation.

Services

Si un service est exporté, les informations du propriétaire du service sont également exportées. Le nom descriptif `dn` est défini comme il convient si un utilisateur portant ce nom existe dans le système cible.

Relations entre les rôles

Lors de l'exportation d'un rôle comportant une relation de rôle Parent ou Enfant, la relation est aussi exportée. Le rôle apparenté en lui-même n'est pas exporté en tant que dépendance.

Si le rôle dépendant existe dans le système cible, la relation de rôle sera alors créée. Sinon, elle ne le sera pas. Les relations de rôle ne sont jamais supprimées lors des importations.

Exportation de plusieurs objets

L'exportation de plusieurs objets pendant une période donnée peut avoir pour résultat d'enregistrer des variations de dépendances mutuellement partagées au cours de l'activité quotidienne du système. Tenez compte de ce point lorsque vous planifiez la stratégie d'exportation.

Dépendances et objets parent

La suppression d'un objet parent est admise. Toutefois, dans ce cas, les tâches d'importation et d'exportation suppriment automatiquement toutes ses dépendances de la liste d'exportation.

Tableau 31. Dépendances et objets parent

Objet parent	Dépendances
Règle d'administration des identités Règle de cycle de vie Opération de cycle de vie	Profil d'objet

Tableau 31. Dépendances et objets parent (suite)

Objet parent	Dépendances
Règle d'administration des identités Règle de cycle de vie Opération de cycle de vie Règle d'administration des mots de passe Règle d'application des accès Service Règle de sélection des services Flux de travaux	Profil de service
Règle d'application des accès Flux de travaux	Rôle organisationnel
Règle d'adoption Règle d'administration des identités Règle d'administration des mots de passe Règle d'application des accès	Service
Règle de cycle de vie	Opération de cycle de vie

Exécution d'une exportation complète

Utilisez cette procédure pour exporter tous les types d'objet exportables et générer un fichier d'archive Java (fichier JAR) contenant les données d'exportation.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Le fichier JAR qui est généré par cette tâche comporte un extrait complet de tous les objets exportables existants, avec leurs dépendances et les références aux conteneurs.

Pour effectuer une exportation complète, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Exporter des données**. La page Exporter des données s'affiche.
2. Dans la page Exporter des données, cliquez sur **Exporter tout**. La page Exporter tout s'affiche.
3. Facultatif : Dans la zone **Nom de l'exportation**, entrez un nom pour identifier l'exportation.
4. Dans la zone **Exporter vers le fichier (.jar)**, entrez un nom de fichier pour l'exportation, puis cliquez sur **Soumettre**. La page Exporter des données s'affiche.

5. Dans la page Exporter des données, cliquez sur **Régénérer** pour mettre à jour la liste des éléments d'exportation dans le tableau.

Résultats

Un fichier JAR d'exportation totale est créé et s'affiche dans la page Exporter des données.

Que faire ensuite

Exécutez d'autres tâches de gestion des exportations, telles qu'un téléchargement de fichier JAR ou cliquez sur **Fermer**.

Exécution d'une exportation partielle

Utilisez cette procédure pour exporter sélectivement des types d'objet et générer un fichier d'archive Java (fichier JAR) contenant les données d'exportation.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vérifiez que vous avez identifié toutes les dépendances nécessaires pour les objets que vous voulez exporter.

Pourquoi et quand exécuter cette tâche

Le fichier JAR qui est généré par cette tâche comporte un extrait complet de tous les objets exportables existants, avec leurs dépendances spécifiées. L'extraction inclut les dépendances et les références aux conteneurs.

Vous pouvez rechercher et sélectionner les types d'objet suivants pour les inclure dans un fichier JAR d'exportation partielle :

- Règle d'adoption
- Groupe
- Règle d'administration des identités
- Opération de cycle de vie
- Règle de cycle de vie
- Rôle organisationnel
- Règle de gestion des mots de passe
- Règle d'application des accès
- Service
- Règle de sélection des services
- Flux de travaux

Pour effectuer une exportation complète, procédez comme suit :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Exporter des données**. La page Exporter des données s'affiche.

2. Dans la page Exporter des données, cliquez sur **Créer**. La page Créer une exportation partielle s'affiche.
3. Pour ajouter des objets à la liste d'exportation, cliquez sur **Ajouter**. La page Sélectionner des objets s'affiche.
4. Pour trouver un objet à exporter, exécutez les étapes suivantes :
   a. Dans la zone de **Nom**, entrez les informations sur l'objet que vous voulez exporter.
   b. Sélectionnez le type d'objet que vous voulez rechercher dans la liste **Type d'objet**, puis cliquez sur **Rechercher**. Les objets qui correspondent à vos critères de recherche sont affichés dans le tableau.
5. Sélectionnez la case à cocher en regard de l'objet à exporter puis cliquez sur **OK**. Pour sélectionner tous les objets, cochez la case située en haut de cette colonne. Les objets que vous avez ajoutés sont affichés dans la page Créer une exportation partielle.
6. Vérifiez la liste des éléments que vous voulez exporter, puis cliquez sur **Continuer**. La page Exportation partielle s'affiche.
7. Facultatif : Dans la zone **Nom de l'exportation**, entrez un nom pour identifier l'exportation.
8. Dans la zone **Exporter vers le fichier (.jar)**, entrez un nom de fichier pour l'exportation, puis cliquez sur **Soumettre**. La page Exporter des données s'affiche.
9. Dans la page Exporter des données, cliquez sur **Régénérer** pour mettre à jour la liste des éléments d'exportation dans le tableau.

Résultats

Un fichier JAR d'exportation partielle est créé et s'affiche dans la page Exporter des données.

Que faire ensuite

Exécutez d'autres tâches de gestion des exportations, telles qu'un téléchargement de fichier JAR ou cliquez sur **Fermer**.

Téléchargement du fichier JAR

Utilisez cette procédure pour télécharger un fichier d'archive Java (fichier JAR) d'exportation partielle ou totale sur le système local.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vérifiez que vous avez créé un fichier d'exportation, avec toutes les dépendances et les références aux conteneurs.

Pourquoi et quand exécuter cette tâche

Les fichiers JAR d'exportation varient en taille selon le type et le nombre d'objets exportés. Chaque ligne de la liste des exportations exécutées indique le type d'exportation (partielle ou totale) et le nombre d'objets qui ont été traités. Chaque

ligne spécifie un horodatage des débuts et fins de l'exportation, le statut de l'exportation et un lien vers le fichier JAR lui-même. Le lien vers le fichier JAR vous permet de télécharger le fichier et de l'enregistrer dans un emplacement sur un système local.

Pour télécharger un fichier JAR sur un système local, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Exporter des données**. La page Exporter des données s'affiche.
2. Dans la page Exporter des données, cliquez sur le nom du fichier JAR que vous voulez télécharger. La boîte de dialogue Télécharger un fichier s'affiche.
3. Dans la boîte de dialogue Télécharger un fichier, cliquez sur **Enregistrer**. La boîte de dialogue **Enregistrer sous** s'affiche.
4. Naviguez jusqu'à l'emplacement pour enregistrer le fichier, puis cliquez sur **Enregistrer**.

Résultats

Le fichier JAR est téléchargé sur le système local.

Que faire ensuite

Exécutez d'autres tâches de gestion des exportations ou cliquez sur **Fermer**.

Suppression des enregistrements d'exportations

Utilisez cette procédure pour supprimer des enregistrements d'exportation du tableau.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Lorsque l'enregistrement d'exportation est supprimé, tous ses enregistrements sont supprimés de la base de données, y compris le fichier d'archive Java (fichier JAR). Si vous voulez conserver le fichier JAR, vous devez le télécharger de l'enregistrement d'exportation vers votre système local avant de supprimer l'enregistrement d'exportation.

Vous ne pouvez pas supprimer un enregistrement d'exportation si celle-ci est encore en cours de traitement.

Pour supprimer des enregistrements d'exportation du tableau, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Exporter des données**. La page Exporter des données s'affiche.

2. Dans la page Exporter des données, sélectionnez l'exportation que vous voulez supprimer, puis cliquez sur **Supprimer**.

Résultats

L'enregistrement d'exportation est supprimé du tableau dans la page Exporter des données.

Que faire ensuite

Exécutez d'autres tâches de gestion des exportations ou cliquez sur **Fermer**.

Téléchargement du fichier JAR

Utilisez cette procédure pour télécharger un fichier d'archive Java (fichier JAR) d'exportation partielle ou totale depuis le système local.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vérifiez que vous avez enregistré sur votre système local un fichier JAR exporté.

Pourquoi et quand exécuter cette tâche

Cette tâche lance l'importation du fichier JAR dans des flux Java standard lorsque le contenu est inséré dans une base de données de service de données en vrac en tant qu'objet BLOB.

Pour télécharger un fichier JAR depuis un système local, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Importer des données**. La page Importer des données s'affiche.
2. Dans la page Importer des données, cliquez sur **Téléchargement du fichier**. La page Téléchargement du fichier s'affiche.
3. Facultatif : Dans la zone **Nom de l'importation**, entrez un nom pour identifier l'importation, puis cliquez sur **Parcourir**. La boîte de dialogue Sélectionner un fichier s'affiche.
4. Dans la boîte de dialogue Sélectionner un fichier, naviguez jusqu'à l'emplacement du fichier, sélectionnez le fichier, puis cliquez sur **Ouvrir**. Le nom du fichier s'affiche sur la page Importer des données.
5. Cliquez sur **Soumettre** pour télécharger le fichier. La page Importer des données s'affiche.
6. Dans la page Importer des données, cliquez sur **Régénérer** pour mettre à jour la liste d'éléments d'importation dans le tableau.

Résultats

Le fichier JAR est téléchargé depuis le système local et s'affiche sur la page Importer des données.

Que faire ensuite

Exécutez d'autres tâches de gestion des importations ou cliquez sur **Fermer**.

Résolution des conflits

Le processus d'importation analyse les différences existant entre les données importées et les données du serveur cible. Il permet également de résoudre les conflits ces deux types de données.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vérifiez que vous avez importé un fichier d'archive Java (fichier JAR) depuis votre système local.

Pourquoi et quand exécuter cette tâche

L'analyse des différences génère une liste d'objets trouvés dans le fichier JAR d'importation et dans le système cible. Un administrateur peut utiliser la liste pour résoudre les conflits objet par objet. L'administrateur détermine la priorité par rapport aux données existantes ou remplace les données existantes par les données importées. L'analyse des différences et la résolution des conflits sont effectuées pour les types d'exportation intégrale et partielle.

Les objets, existant dans IBM Security Identity Manager au moment de l'importation et qui sont sélectionnés dans le récapitulatif des conflits pour être remplacés, sont mis à jour.

Les objets dans le fichier JAR téléchargé qui ne sont pas dans IBM Security Identity Manager au moment de l'importation sont ajoutés.

Pour résoudre les conflits entre les données dans un fichier JAR téléchargé et les données sur le serveur, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Importer des données**. La page Importer des données s'affiche et la colonne **Statut** du tableau indique si des conflits sont détectés.
2. Dans la colonne **Statut** du tableau, cliquez sur le lien **Conflits détectés**. La page Evaluer un fichier d'importation s'affiche.
3. Sur la page Evaluer un fichier d'importation, cochez la case en regard de l'objet que vous voulez importer pour remplacer l'objet existant, puis cliquez sur **Importer**. Pour sélectionner tous les objets, cochez la case située en haut de cette colonne. La page Importer des données s'affiche.

4. Dans la page Importer des données, cliquez sur **Régénérer** pour mettre à jour le statut de l'importation dans le tableau. La colonne **Statut** indique que l'importation a réussi.

Résultats

L'importation valide les données, rétablit les relations entre les objets parent et leurs dépendances. Le processus place les objets dans leurs conteneurs appropriés à l'intérieur de l'organigramme IBM Security Identity Manager.

Si votre session avec la console IBM Security Identity Manager est en veille et que son délai d'attente expire pendant que des conflits sont évalués ou si vous fermez explicitement une session, alors le statut de l'importation passe de `Traitement en cours` à `Echec - conflits non résolus`. Si cette modification de statut a lieu, répétez cette procédure de façon à ce que les données soient validées. Généralement, les sessions utilisateur sont configurées pour être en veille jusqu'à 10 minutes avant que le délai d'attente n'expire.

Que faire ensuite

Exécutez d'autres tâches de gestion des importations ou cliquez sur **Fermer**.

Suppression d'importations

Utilisez cette procédure pour supprimer des enregistrements d'importation du tableau.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Pourquoi et quand exécuter cette tâche

Cette procédure supprime l'enregistrement d'importation et le fichier d'archive Java (fichier JAR) qui ont été téléchargés.

Pour supprimer des enregistrements d'importation du tableau, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Configurer le système** > **Importer des données**. La page Importer des données s'affiche.
2. Dans la page Importer des données, sélectionnez l'importation que vous voulez supprimer, puis cliquez sur **Supprimer**.

Résultats

L'enregistrement d'importation est supprimé du tableau dans la page Importer des données.

Que faire ensuite

Exécutez d'autres tâches de gestion des importations ou cliquez sur **Fermer**.

Activer la portabilité des fichiers JAR d'importation et d'exportation

Afin que la portabilité de fichiers d'archive Java (JAR) soit donnée pour leur importation et exportation d'une machine à l'autre, certains paramètres de configuration doivent être les mêmes dans les deux systèmes.

Pourquoi et quand exécuter cette tâche

Pour vous assurer que des fichiers JAR d'importation et d'exportation sont transposables entre deux systèmes, vérifiez que les paramètres de configuration suivants sont les mêmes dans les deux systèmes :

- Fichier de clés
- Mot de passe du fichier de clés
- Algorithme de hachage

Chapitre 16. Configuration et administration d'IBM Tivoli Common Reporting

IBM Tivoli Common Reporting (également appelé groupe de rapports) se focalise sur les informations de compte, de service et de demande.

IBM Tivoli Common Reporting contient un sous-ensemble des rapports par défaut disponibles dans l'interface utilisateur IBM Security Identity Manager version 6.0. Ces rapports n'appliquent aucune information de contrôle d'accès depuis IBM Security Identity Manager aux données qu'ils affichent.

Tout rapport exécuté à partir d'IBM Tivoli Common Reporting peut être lancé par un administrateur IBM Security Identity Manager doté de tous les droits pour visualiser les données du rapport à partir de la console Tivoli Common Reporting. Ces rapports ne prennent pas en compte les informations ACI actuellement définies par IBM Security Identity Manager.

Les versions de DB2, Oracle et Microsoft SQL Server prises en charge par IBM Security Identity Manager version 6.0 prennent également en charge ces rapports.

Vous pouvez administrer et exécuter les rapports grâce au logiciel Tivoli Common Reporting inclus avec IBM Security Identity Manager 6.0. Pour plus d'informations sur Tivoli Common Reporting, consultez le site Web suivant :

http://www.ibm.com/developerworks/spaces/tcr

Vous pouvez modifier les rapports avec Eclipse Business Intelligence Reporting Tool version 2.2.1 disponible sur le site Web suivant :

http://catalog.lotus.com/wps/portal/topal/details?catalog.label=1TW10OT02

Installation ou mise à niveau vers Tivoli Common Reporting Version 2.1.1

Vous pouvez installer ou mettre à niveau votre instance Tivoli Common Reporting vers la version 2.1.1.

Remarque :

- Si Tivoli Common Reporting Version 2.1.1 est déjà installé sur votre ordinateur via IBM Security Role and Policy Modeler, vous pouvez l'utiliser et non le réinstaller.
- Vérifiez que les exigences du serveur Tivoli Common Reporting sont respectées. Consultez ces exigences dans le document *IBM Security Identity Manager - Guide de présentation du produit*.
- Configurez IBM Tivoli Common Reporting afin qu'il s'exécute sur des ports autres que le port par défaut s'il est installé sur le même système respectant les exigences d'IBM Security Identity Manager version 6.0. Il est fort possible que les ports par défaut d'Tivoli Common Reporting entrent en conflit avec les ports des produits installés et il est donc fort probable que l'installation d'Tivoli Common Reporting échoue.

- Pour installer Tivoli Common Reporting Version 2.1.1, consultez le site Web http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ttcr_install.html.
- Pour effectuer une mise à niveau vers Tivoli Common Reporting Version 2.1.1, consultez le site Web http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ctcr_upgrade.html.

Importation du module de rapports dans Tivoli Common Reporting

Importez le package de rapports dans Tivoli Common Reporting pour exécuter des rapports serveur IBM Security Identity Manager Version 6.0 à partir de Tivoli Common Reporting. Le package de rapports installe les rapports de la version 6.0 pour IBM Security Identity Manager dans Tivoli Common Reporting.

Avant de commencer

- Installez IBM Security Identity Manager Version 6.0. Pour plus d'informations, voir le document *IBM Security Identity ManagerInstallation Guide*.
- Installez Tivoli Common Reporting Version 2.1.1. Voir http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html.

Procédure

1. Procurez-vous le fichier `tcr_tim6.0_reporting_pack.zip` dans le répertoire *ISIM_HOME*`/extensions/tcr/tcrpack`. *ISIM_HOME* correspond au répertoire d'installation d'IBM Security Identity Manager.
2. Importez le package de rapports avec la commande **`trcmd -import`**. Voir http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ctcr_birt_reps_in_cog_importing.html.

Résultats

Lorsque vous importez les rapports, ils sont placés dans **Common Reporting** > **Dossiers publics** > **Produits Tivoli**. Sélectionnez **IBM Security Identity Manager 6.0** pour voir les rapports disponibles.

Que faire ensuite

Générez le rapport.

Voir la rubrique "Génération de rapports dans Tivoli Common Reporting" du document *IBM Security Identity Manager - Guide d'administration*

Configuration du serveur WebSphere Application Server intégré

Vous devez configurer une source de données JDBC dans IBM Tivoli Common Reporting serveur WebSphere Application Server intégré pour pouvoir exécuter les rapports IBM Security Identity Manager.

Pourquoi et quand exécuter cette tâche

Vous devez configurer Tivoli Common Reporting pour la connexion à la base de données IBM Security Identity Manager. Procédez comme suit :

- «Création d'un alias de service JAAS (Java Authentication and Authorization Service)», à la page 193

- «Création d'un fournisseur de connectivité JDBC (Java Database Connectivity)», à la page 194
- «Création de la source de données», à la page 198
- «Sauvegarde de la configuration», à la page 202

Vous pouvez effectuer ces étapes manuellement ou en mode automatique :

- La configuration manuelle est décrite dans «Configuration du serveur WebSphere Application Server intégré avec les commandes **wsadmin**», à la page 192
- La configuration en mode automatique est décrite dans «Configuration du serveur WebSphere Application Server intégré à l'aide d'un script Jython»

Les deux méthodes aboutissent au même résultat.

Que faire ensuite

Configurez serveur WebSphere Application Server intégré en utilisant, soit les commandes **wsadmin**, soit un script Jython.

Configuration du serveur WebSphere Application Server intégré à l'aide d'un script Jython

IBM Security Identity Manager comprend un script pour faciliter la configuration de la source de données nécessaire aux rapports mis en forme.

Pourquoi et quand exécuter cette tâche

Le fichier *ITIM_HOME*/extensions/tcr/scripts/TIMsetupDatasource.py est un script Jython utilisé pour automatiser la configuration de Tivoli Common Reporting dans votre environnement IBM Security Identity Manager. Pour utiliser le script, procédez comme suit :

1. Copiez le fichier TIMsetupDatasource.py de *ITIM_HOME*/extensions/tcr/scripts/TIMsetupDatasource.py sur l'ordinateur où est installé Tivoli Common Reporting.
2. Editez le fichier TIMsetupDatasource.py et mettez les paramètres suivants à jour afin qu'ils correspondent aux valeurs de votre environnement :

   ```
   aliasUser
   aliasPW
   dsDBVendor
   ```

   Pour les serveurs de base de données DB2 ou MS SQL :

   ```
   dsDBName
   dsDBServer
   dsDBPort
   dsDBType
   ```

   Pour les serveurs de bases de données Oracle :

   ```
   dsDBURL
   ```

   Pour tous les serveurs de bases de données :

   ```
   providerCP
   providerImplClass
   dsDBHelper
   ```

   Le script fournit les valeurs de chacun des paramètres précédents.
3. Exécutez la commande **wsadmin** dans Tivoli Common Reporting serveur WebSphere Application Server intégré :

- Sous Windows, ouvrez une invite de commande et entrez une commande semblable à l'exemple suivant :

  ```
  TCR_HOME\profiles\TIPProfile\bin\wsadmin.bat –f TIMsetupDatasource.py
  ```

- Sous UNIX, ouvrez un shell et entrez une commande semblable à l'exemple suivant :

  ```
  TCR_HOME/profiles/TIPProfile/bin/wsadmin.sh –f TIMsetupDatasource.py
  ```

Que faire ensuite

Configurez la source de données dans Tivoli Common Reporting. Pour plus d'informations, voir «Configuration de la source de données dans Tivoli Common Reporting», à la page 203.

Configuration du serveur WebSphere Application Server intégré avec les commandes `wsadmin`

Pour configurer IBM Tivoli Common Reporting afin de l'utiliser manuellement avec IBM Security Identity Manager, vous devez exécuter une série de commandes **`wsadmin`**.

Pourquoi et quand exécuter cette tâche

Procédez comme suit :

- «Création d'un alias de service JAAS (Java Authentication and Authorization Service)», à la page 193
- «Création d'un fournisseur de connectivité JDBC (Java Database Connectivity)», à la page 194
- «Création de la source de données», à la page 198
- «Sauvegarde de la configuration», à la page 202

Les commandes **`wsadmin`** doivent être exécutées à partir d'une invite **`wsadmin`**. Pour démarrer **`wsadmin`** en vue d'exécuter les commandes **`wsadmin`**, accédez au répertoire `bin` du profil Tivoli Common Reporting serveur WebSphere Application Server intégré et démarrez l'interpréteur Jython **`wsadmin`**.

Procédure

1. Pour accéder au répertoire `bin` du profil Tivoli Common Reporting serveur WebSphere Application Server intégré, procédez comme suit.
   - Sous Windows, ouvrez une invite de commande et entrez une commande semblable à l'exemple suivant :

     ```
     cd "C:\Program Files\IBM\tcr\eWas61\profiles\tcrProfile\bin"
     ```

   - Sous UNIX, ouvrez un shell et entrez une commande semblable à l'exemple suivant :

     ```
     cd /opt/IBM/tcr/eWas61/profiles/tcrProfile/bin
     ```

2. Entrez l'une des commandes suivantes :
   - Sous Windows, entrez `wsadmin.bat -lang jython`
   - Sous UNIX, entrez `./wsadmin.sh -lang jython`
3. A l'invite de connexion, entrez vos informations d'identification de type administrateur Tivoli Common Reporting. Ces entrées correspondent aux mêmes informations d'identification que celles utilisées pour accéder à la console d'administration de Tivoli Common Reporting, tels que `tcrAdmin`.

Que faire ensuite

Créez un alias d'authentification JAAS. Pour plus d'informations, voir «Création d'un alias de service JAAS (Java Authentication and Authorization Service)».

Création d'un alias de service JAAS (Java Authentication and Authorization Service)

Créez un alias d'authentification JAAS de manière à pouvoir authentifier les connexions de la base de données depuis le serveur IBM Tivoli Common Reporting vers le serveur de la base IBM Security Identity Manager.

Pourquoi et quand exécuter cette tâche

L'alias d'authentification JAAS n'est pas tributaire du fournisseur de base de données.

Avant de créer l'alias, examinez les informations suivantes sur l'identification de l'utilisateur par l'alias :

- L'utilisateur doit être en mesure d'accéder aux tables contenant les données nécessaires aux rapports définis.
- L'utilisateur est généralement la personne prévue dans la configuration pour l'établissement de la connexion de la base de données au serveur de la base IBM Security Identity Manager.
- L'ID utilisateur par défaut dans IBM Security Identity Manager Version 5.0 et Version 5.1 est `itimuser`.
- L'ID utilisateur par défaut dans les éditions antérieures était `enrole`.

Le tableau 32 répertorie les paramètres requis pour la création d'un alias d'authentification JAAS à l'aide de la console **wsadmin**.

Tableau 32. Données requises pour l'alias d'authentification JAAS

Paramètre	Description	Exemple de valeur
alias	Nom défini par l'utilisateur pour identifier cette collecte de données.	Alias de la base de données IBM Security Identity Manager
description	Description définie par l'utilisateur pour cette collecte de données.	Alias d'authentification JAAS pour la base de données IBM Security Identity Manager
userId	ID utilisateur utilisé pour la connexion à la base de données.	`itimuser`

mot de passe	Mot de passe associé à l'ID utilisateur
	
	Vous trouvez l'ID utilisateur dans le serveur IBM Security Identity Manager à l'emplacement suivant :
	ITIM_HOME`/data/enRoleDatabase.properties`
	`# IBM Tivoli Identity Manager Database User`
	`database.db.user=itimuser`
	
	où *ITIM_HOME* est le répertoire d'installation de IBM Security Identity Manager.
		`mypassword`

1. Collectez les données requises comme indiqué dans le tableau 32, à la page 193.
2. Exécutez la commande **wsadmin** figurant dans le répertoire WAS_HOME/bin/ du serveur Tivoli Common Reporting.
3. A l'aide des données collectées, créez une configuration d'alias d'authentification JAAS avec **wsadmin** en utilisant le format suivant :

```
wsadmin> AdminConfig.create(
'JAASAuthData',
AdminConfig.getid("/Security:/"),
[["alias", "alias"],
["description", "description"],
["userId", "userId"],
["password", "password"]])
```

où :

- *alias* et *description* sont des valeurs définies par l'utilisateur. Notez-les quelque part afin de vous en souvenir pour une étape ultérieure.
- *userId* correspond à un utilisateur valide du serveur de la base IBM Security Identity Manager pourvu des droits d'accès nécessaires à la connexion et à la lecture de données depuis la base de données IBM Security Identity Manager.
- *password* est le mot de passe correspondant au *userId*.

Les lignes suivantes donnent un exemple de commande **wsadmin** :

```
wsadmin> AdminConfig.create(
'JAASAuthData',
AdminConfig.getid("/Security:/"),
[["alias", "IBM Tivoli Identity Manager DB Alias"],
["description", "JAAS alias for the IBM Tivoli Identity Manager DB"],
["userId", "itimuser"],
["password", "mypassword"]])
```

Que faire ensuite

Créez un fournisseur JDBC. Pour plus d'informations, voir «Création d'un fournisseur de connectivité JDBC (Java Database Connectivity)».

Création d'un fournisseur de connectivité JDBC (Java Database Connectivity)

La création d'une source de données nécessite à la fois l'identification des valeurs du fournisseur de connectivité JDBC pour votre environnement et l'exécution d'une seule commande **wsadmin**.

Pourquoi et quand exécuter cette tâche

Les informations sur le fournisseur de connectivité JDBC varient selon le fournisseur de base de données.

Le tableau 33 référence les paramètres nécessaires à la création du fournisseur de connectivité JDBC avec la console **wsadmin**.

Tableau 33. Données requises pour le fournisseur de connectivité JDBC

Paramètre	Description	Exemple de valeur
classpath	Chemin d'accès aux classes requis par la classe du fournisseur de connectivité JDBC	Voir tableau 34, à la page 195

Tableau 33. Données requises pour le fournisseur de connectivité JDBC (suite)

Paramètre	Description	Exemple de valeur
implementationClassName	Nom de la classe d'implémentation du fournisseur de connectivité JDBC	Voir tableau 35
name	Nom défini par l'utilisateur pour identifier ce fournisseur de connectivité JDBC	Fournisseur de connectivité JDBC pour la base de données IBM Security Identity Manager
description	Description définie par l'utilisateur pour ce fournisseur de connectivité JDBC	Fournisseur JDBC dans lequel ajouter la base de données IBM Security Identity Manager en tant que source de données

Tableau 34. Exemples de valeurs de chemin d'accès aux classes pour les fournisseurs JDBC pris en charge par IBM Security Identity Manager

Type de base de données	Chemin d'accès aux classes
DB2	`/opt/IBM/db2/V9.1/java/db2jcc.jar;/opt/IBM/db2/V9.1/java/db2jcc_license_cu.jar`
Microsoft SQL Server	`C:/Program Files/Microsoft SQL Server 2005 JDBC Driver/sqljdbc_1.1/enu/sqljdbc.jar`
Oracle	`/u01/app/oracle/product/10.2.0/Db_1/jdbc/lib/ojdbc14.jar`

Tableau 35. Noms de classe d'implémentation pour les fournisseurs de connectivité JDBC pris en charge par IBM Security Identity Manager

Type de base de données	Nom de classe d'implémentation
DB2	`com.ibm.db2.jcc.DB2ConnectionPoolDataSource`
Microsoft SQL Server	`com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource`
Oracle	`oracle.jdbc.pool.OracleConnectionPoolDataSource`

1. Collectez les données requises comme indiqué dans les tableaux suivants :
   - tableau 33, à la page 194
   - tableau 34
   - tableau 35

   Pour obtenir de l'aide concernant la collecte de ces données, voir «Identification d'informations du fournisseur JDBC à partir d'IBM Security Identity Manager», à la page 196.
2. Démarrez la commande **wsadmin** comme indiqué dans «Configuration du serveur WebSphere Application Server intégré avec les commandes **wsadmin**», à la page 192.
3. A l'aide des données collectées, créez le fournisseur JDBC en utilisant le format suivant :

```
wsadmin> AdminConfig.create(
'JDBCProvider',
AdminConfig.getid("/Cell:/"),
[["classpath", "classpath"],
["implementationClassName", "implementationClassName"],
["name", "name"],
["description", "description"]])
```

Dans cet exemple, `'JDBCProvider'` et `"/Cell:/"` identifient le type et l'emplacement de cet objet de configuration.

Dans la liste, le premier élément de chaque paire d'attributs (`"classpath"`, `"implementation"`, `"name"` et `"description"`) identifie les noms des attributs spécifiques utilisés lors de la création de cet élément de configuration.

Le second élément de chaque paire d'attributs en est la valeur, susceptible de varier d'une installation à l'autre.

Les valeurs `"name"` et `"description"` sont définies par l'utilisateur. Notez quelque part la valeur `"name"` afin de vous en souvenir pour une étape ultérieure.

Les valeurs `"classpath"` et `"implementationClassName"` doivent correspondre au nom de classe d'implémentation et au chemin d'accès aux classes requis par la base de données.

Les lignes suivantes donnent un exemple de commande **wsadmin** :

```
wsadmin> AdminConfig.create(
'JDBCProvider',  AdminConfig.getid("/Cell:/"),
[["classpath",
"C:/Program Files/Microsoft SQL Server 2005 JDBC Driver/
sqljdbc_1.1/enu/sqljdbc.jar"],
["implementationClassName",
"com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource"],
["name", "JDBC provider for the ITIM DB"],
["description", "JDBC provider for the ITIM DB
under which to add the ITIM DB as a data source"]])
```

Que faire ensuite

Créez la source de données. Pour plus d'informations, voir «Création de la source de données», à la page 198.

Identification d'informations du fournisseur JDBC à partir d'IBM Security Identity Manager

La création d'un fournisseur JDBC nécessite l'identification des paramètres corrects. Cette section vous permet de déterminer les valeurs déjà utilisées par IBM Security Identity Manager.

Pourquoi et quand exécuter cette tâche

Le nom le la classe d'implémentation et les informations d'exemples de chemin d'accès aux classes sont également disponibles dans IBM Security Identity Manager WebSphere Application Server.

Les valeurs de chemins d'accès aux classes définies dans le serveur IBM Security Identity Manager WebSphere Application Server dépendent des variables de serveur qui ne se trouvent pas sur le serveur Tivoli Common Reporting serveur WebSphere Application Server intégré. Par conséquent, les valeurs de chemins

d'accès aux classes peuvent vous guider de manière générale vers les fichiers requis. Elles ne désignent pas un emplacement spécifique.

Procédure

1. A l'aide de la console d'administration WebSphere Application Server sur le serveur IBM Security Identity ManagerWebSphere Application Server, connectez-vous et sélectionnez **Ressources** > **JDBC** > **Fournisseurs JDBC**.
2. Visualisez la liste de fournisseurs JDBC. Si plusieurs fournisseurs JDBC correspondants à IBM Security Identity Manager s'affichent, sélectionnez celui qui est identifié comme non XA. Par exemple, sélectionnez le fournisseur JDBC DB2 IBM Security Identity Manager non XA pour afficher le nom de la classe d'implémentation et le chemin d'accès aux classes.

Exemple

Vous pouvez également obtenir ces informations concernant le serveur IBM Security Identity Manager WebSphere Application Server à l'aide d'une session **wsadmin** sur ce même serveur, afin de répertorier les identificateurs (ID) de fournisseurs JDBC.

L'exemple de sortie suivant affiche la ligne de commande **wsadmin** dans laquelle chaque chaîne entre guillemets est un ID de fournisseur JDBC :

```
wsadmin> print AdminConfig.list("JDBCProvider")
"Derby JDBC Provider (XA)(cells/fooNode01Cell/nodes/fooNode01/servers/server1|
resources.xml#builtin_jdbcprovider)"
"Derby JDBC Provider (XA)(cells/fooNode01Cell|resources.xml#builtin_jdbcprovider)"
"Derby JDBC Provider(cells/fooNode01Cell/nodes/fooNode01/servers/server1|resources.xml
#JDBCProvider_1201014593661)"
"ITIM XA DB2 JDBC Provider(cells/fooNode01Cell/nodes/fooNode01/servers/server1|resources.xml
#JDBCProvider_1201032904744)"
"ITIM non-XA DB2 JDBC Provider(cells/fooNode01Cell/nodes/fooNode01/servers/server1|resources.xml
#JDBCProvider_1201032906859)"
```

Dans cette liste de fournisseurs JDBC, vous pouvez obtenir les attributs de paramètres d'un ID de fournisseur JDBC à l'aide de la commande **wsadmin** suivante. L'ID de fournisseur JDBC utilisé ci-dessous provient de la liste d'ID indiquée dans l'exemple :

```
wsadmin> print AdminConfig.show("ITIM non-XA DB2 JDBC
Provider(cells/fooNode01Cell/nodes/fooNode01/servers/server1|resources.xml
#JDBCProvider_1201032906859)")

[classpath
${ITIM_DB_JDBC_DRIVER_PATH}/db2jcc.jar;$
{ITIM_DB_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar;$
{ITIM_DB_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar]
[description "ITIM JDBC2 non-XA Compliant Driver (DB2)"]
[implementationClassName com.ibm.db2.jcc.DB2ConnectionPoolDataSource]
[name "ITIM non-XA DB2 JDBC Provider"]
[nativepath []]
[xa false]
```

Voici un exemple de sortie de session **wsadmin** exécutée sur un serveur IBM Security Identity Manager WebSphere Application Server basé sur Windows et configuré pour l'utilisation d'une base de données Microsoft SQL Server :

```
wsadmin> print AdminConfig.show(AdminConfig.getid("/
JDBCProvider:ITIM non-XA MSSQL JDBCProvider"))
[classpath
${ITIM_DB_JDBC_DRIVER_PATH}/sqljdbc.jar]
[description "ITIM JDBC2 non-XA Compliant Driver (MSSQL)"]
```

```
[implementationClassName com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource]
[name "ITIM non-XA MSSQL JDBC Provider"]
[nativepath []]
[xa false]
```

Ou par la chaîne de confinement "/JDBCProvider:Provider Name", comme suit :

```
wsadmin> print AdminConfig.show(AdminConfig.getid("/
JDBCProvider:ITIM non-XA DB2 JDBC Provider"))

[classpath
${ITIM_DB_JDBC_DRIVER_PATH}/db2jcc.jar;
${ITIM_DB_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar;
${ITIM_DB_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar]
[description "ITIM JDBC2 non-XA Compliant Driver (DB2)"]
[implementationClassName com.ibm.db2.jcc.DB2ConnectionPoolDataSource]
[name "ITIM non-XA DB2 JDBC Provider"]
[nativepath []]
[xa false]
```

Voici un exemple de sortie de session **wsadmin** exécutée sur un serveur IBM Security Identity Manager WebSphere Application Server basé sur Solaris et configuré pour l'utilisation d'une base de données Oracle :

```
wsadmin> print AdminConfig.show(AdminConfig.getid("/
JDBCProvider:ITIM non-XA ORACLE JDBC Provider"))
[classpath
${ITIM_DB_JDBC_DRIVER_PATH}/ojdbc14.jar]
[description "ITIM JDBC2 non-XA Compliant Driver (ORACLE)"]
[implementationClassName oracle.jdbc.pool.OracleConnectionPoolDataSource]
[name "ITIM non-XA ORACLE JDBC Provider"]
[nativepath []]
[providerType "Oracle JDBC Driver"]
[xa false]
```

Remarque : Les valeurs de chemins d'accès aux classes extraites de la configuration du serveur IBM Security Identity Manager utilisent une variable *${ITIM_DB_JDBC_DRIVER_PATH}* qui n'est pas disponible dans le serveur Tivoli Common Reporting lors de la définition d'un fournisseur JDBC. Vous devez utiliser le chemin d'accès complet lorsque vous indiquez le chemin d'accès aux classes du fournisseur JDBC.

Que faire ensuite

Créez un fournisseur JDBC. Pour plus d'informations, voir «Création d'un fournisseur de connectivité JDBC (Java Database Connectivity)», à la page 194.

Création de la source de données

La création de la source de données dépend du fournisseur et représente l'étape la plus complexe.

Pourquoi et quand exécuter cette tâche

Cette tâche exige des informations détaillées sur le serveur et la connexion de votre base de données, telles le nom d'hôte, le port, le nom de la base de données et les autres paramètres relatifs au fournisseur. Pour plus d'informations, voir tableau 36.

Tableau 36. Propriétés pour les bases de données DB2 et Microsoft SQL Server

Paramètre	Description	Exemple de valeur
databaseName	Nom de la base de données sur le serveur cible.	itimdb

Tableau 36. Propriétés pour les bases de données DB2 et Microsoft SQL Server (suite)

Paramètre	Description	Exemple de valeur
serverName	Nom d'hôte ou adresse IP du serveur de la base.	`myserver.my.com`
portNumber	Numéro de port pour la connexion au serveur de la base.	`1433`

Pour les bases de données DB2 et Microsoft SQL Server, les paramètres *databaseName*, *serverName* et *portNumber* définissent la source de données JDBC. Pour les bases de données Oracle, une seule propriété URL est utilisée.

Tableau 37. Noms de classe auxiliaire de source de données

Fournisseur de base de données	Nom de classe auxiliaire de la source de données
DB2	com.ibm.websphere.rsadapter.DB2UniversalDataStoreHelper
Microsoft SQL Server	com.ibm.websphere.rsadapter.ConnectJDBCDataStoreHelper
Oracle	com.ibm.websphere.rsadapter.Oracle10gDataStoreHelper

Procédure

1. Collectez les données requises comme indiqué dans le tableau 36, à la page 198. Pour obtenir de l'aide concernant la collecte de ces données, voir «Identification des informations de la source de données à partir d'IBM Security Identity Manager», à la page 201.
2. Démarrez la commande **wsadmin** comme indiqué dans «Configuration du serveur WebSphere Application Server intégré avec les commandes **wsadmin**», à la page 192.
3. Créez la source de données. Pour le reste des commandes, il est utile de sauvegarder le résultat de cette commande dans une variable *ds* locale.

```
wsadmin> ds = AdminConfig.create(
 'DataSource',
 AdminConfig.getid("/JDBCProvider:JDBC provider for the ITIM DB"),
 [["name", "ITIM DB Data Source"],
  ["description", "ITIM DB Data Source"]])
```

4. Créez un ensemble de propriétés de ressource pour mettre des propriétés supplémentaires en attente. Pour le reste des commandes, il est utile de sauvegarder le résultat de cette commande dans une variable *ds_props* locale.

```
wsadmin> ds_props = AdminConfig.create('J2EEResourcePropertySet', ds, [])
```

5. Créez les propriétés J2EE. Pour les sources de données DB2 et Microsoft SQL Server, il existe quatre propriétés à définir. Ces propriétés identifient le nom de base de données, le serveur de base de données, le port du serveur et le type de pilote. Pour les sources de données Oracle, elles sont définies dans une seule propriété qui identifie l'URL de connexion à JDBC complète.

   Nom de la base de données DB2 et Microsoft SQL Server

   Dans l'appel suivant, remplacez, le cas échéant, la valeur `itimdb` par le nom de votre base de données actuelle :

```
wsadmin> AdminConfig.create(
 'J2EEResourceProperty',
 ds_props,
 [["name", "databaseName"],
  ["type", "java.lang.String"],
  ["value", "itimdb"]])
```

Nom de serveur DB2 et Microsoft SQL

Dans l'appel suivant, remplacez, le cas échéant, la valeur `localhost` par le nom de votre serveur de base ou l'adresse IP actuelle :

```
wsadmin> AdminConfig.create(
 'J2EEResourceProperty',
 ds_props,
 [["name", "serverName"],
  ["type", "java.lang.String"],
  ["value", "localhost"]])
```

Numéro de port DB2 et Microsoft SQL Server

Dans l'appel suivant, remplacez, le cas échéant, la valeur `1433` par le numéro de port de votre serveur de base actuel :

```
wsadmin> AdminConfig.create(
 'J2EEResourceProperty',
 ds_props,
 [["name", "portNumber"],
  ["type", "java.lang.Integer"],
  ["value", "1433"]])
```

Type de pilote DB2 et Microsoft SQL Server

Tous les pilotes utilisés pour les sources de données IBM Security Identity Manager sont de type `4` pour les bases de données DB2 et Microsoft SQL Server ainsi que `thin` pour les bases de données Oracle :

```
wsadmin> AdminConfig.create(
 'J2EEResourceProperty',
 ds_props,
 [["name", "driverType"],
  ["type", "java.lang.String"],
  ["value", "4"]])
```

URL Oracle

Cette propriété est la seule requise pour les bases de données Oracle et ne convient pas pour les bases de données de DB2 ou Microsoft SQL Server. Dans l'appel suivant, remplacez, le cas échéant, la valeur `jdbc:oracle:thin:@myserver.mydomain.com:Port_Number:itimdb` par l'URL de votre base de données actuelle :

```
wsadmin> AdminConfig.create(
 'J2EEResourceProperty',
 ds_props,
 [["name", "URL"],
  ["type", "java.lang.String"],
  ["value", "jdbc:oracle:thin:@myserver.mydomain.com:Port_Number:itimdb"]])
```

6. Modifiez la source de données.
   a. Mettez la configuration de la source de données à jour avec le nom JNDI (Java Naming and Directory Interface) attendu par les éléments suivants :
      - IBM Security Identity Manager
      - Le module de rapports Tivoli Common Reporting (`jdbc/ibm/tivoli/tim`)
      - L'alias d'authentification JAAS défini plus haut dans ce processus de configuration
      - Le nom de classe auxiliaire de la source de données relative au fournisseur (voir tableau 37, à la page 199)
   b. Dans le code ci-dessous, remplacez si nécessaire `ITIM DB Alias` par l'alias d'authentification JAAS créé auparavant au cours de ce processus de configuration.
   c. Remplacez `com.ibm.websphere.rsadapter.ConnectJDBCDataStoreHelper` par le nom de classe auxiliaire de la source de données correspondant à votre base de données comme suit :

```
wsadmin> AdminConfig.modify(
  ds,
  [["jndiName", "jdbc/ibm/tivoli/tim"],
```

```
   ["authDataAlias", "ITIM DB Alias"],
   ["datasourceHelperClassname",
"com.ibm.websphere.rsadapter.ConnectJDBCDataStoreHelper"]])
```

Que faire ensuite

Enregistrez la configuration. Pour plus d'informations, voir «Sauvegarde de la configuration», à la page 202.

Identification des informations de la source de données à partir d'IBM Security Identity Manager

La création d'une source de données nécessite que l'identification des paramètres de configuration utilisés par IBM Security Identity Manager soit correcte.

Pourquoi et quand exécuter cette tâche

Les informations nécessaires à la configuration de la base de données sont disponibles dans IBM Security Identity Manager WebSphere Application Server.

Procédure

1. A l'aide de la console d'administration ISC WebSphere Application Server disponible dans IBM Security Identity Manager WebSphere Application Server, connectez-vous et sélectionnez **Ressources** > **JDBC** > **Sources de données**.
2. Visualisez la liste de sources de données et sélectionnez **Source de données ITIM**.

Exemple

Vous pouvez également obtenir facilement ces informations dans IBM Security Identity Manager WebSphere Application Server à l'aide d'une session **wsadmin** sur ce serveur, en procédant comme suit :

```
wsadmin> print AdminConfig.showall
(AdminConfig.showAttribute(AdminConfig.getid("/
DataSource:ITIM Data Source"), "propertySet"))
[resourceProperties "[[[name databaseName]
[required false]
[type java.lang.String]
[value itimdb]] [[name driverType]
[required false]
[type java.lang.Integer]
[value 4]] [[name serverName]
[required false]
[type java.lang.String]
[value localhost]] [[name portNumber]
[required false]
[type java.lang.Integer]
[value 50000]]]"]
```

Certaines de ces informations sont également disponibles dans le fichier *ITIM_HOME*/data/enRoleDatabase.properties sur votre serveur IBM Security Identity Manager. IBM Security Identity Manager est installé dans le répertoire *ITIM_HOME*.

Pour Microsoft SQL Server, vous pouvez procéder selon l'exemple suivant :

```
# JDBC driver URL
database.jdbc.driverUrl=jdbc:sqlserver://;
server=myserver.mydomain.com;port=1433;database=itimdb
```

où :

- *myserver.mydomain.com* est le nom d'hôte du serveur de la base de données IBM Security Identity Manager.
- *1433* est le port sur lequel le serveur de la base de données écoute.
- *itimdb* correspond au nom de la base de données IBM Security Identity Manager.

Pour Oracle, vous pouvez procéder selon l'exemple suivant :

```
# JDBC driver URL
database.jdbc.driverUrl=jdbc:oracle:thin:@myserver.mydomain.com :1521 :itimdb
```

où :

- *myserver.mydomain.com* est le nom d'hôte du serveur de la base de données IBM Security Identity Manager.
- *1521* est le port sur lequel le serveur de la base de données écoute.
- *itimdb* correspond au nom de la base de données IBM Security Identity Manager.

Que faire ensuite

Créez la source de données. Pour plus d'informations, voir «Création de la source de données», à la page 198.

Sauvegarde de la configuration

Toutes modifications se font dans une copie de l'espace de travail de la configuration à l'intérieur d'une session **wsadmin**. Pour valider les modifications, vous devez les sauvegarder expressément.

Avant de commencer

Sauvegardez la configuration en saisissant la commande suivante :

```
wsadmin> AdminConfig.save()
```

Le serveur IBM Tivoli Common Reporting est configuré pour se connecter à la base de données IBM Security Identity Manager.

Pourquoi et quand exécuter cette tâche

Procédure

1. Arrêtez, puis redémarrez le serveur Tivoli Common Reporting afin que les nouveaux paramètres de configuration prennent effet.
2. Saisissez `quit` pour quitter **wsadmin**. Si vous voulez quitter sans enregistrer, saisissez à nouveau `quit` pour annuler les modifications.
3. Testez la connexion avec **wsadmin**.
4. Saisissez la commande suivante et remplacez *ITIM DB Data Source* par le nom de la source de données créée antérieurement au cours de ce processus de configuration.

   ```
   wsadmin> AdminControl.testConnection (AdminConfig.getid(
   "/DataSource:ITIM DB Data Source"))
   ```

Résultats

Lors de l'exécution de la commande, le message suivant s'affiche :

```
WASX7217I: La connexion à la source de données fournie a réussi.
```

Que faire ensuite

Configurez la source de données dans Tivoli Common Reporting. Pour plus d'informations, voir «Configuration de la source de données dans Tivoli Common Reporting».

Configuration de la source de données dans Tivoli Common Reporting

Configurez la source de données dans Tivoli Common Reporting pour une utilisation avec des rapports serveur IBM Security Identity Manager Version 6.0.

Avant de commencer

- Installez IBM Security Identity Manager Version 6.0. Pour plus d'informations, voir le document *IBM Security Identity ManagerInstallation Guide*.
- Installez Tivoli Common Reporting Version 2.1.1. Voir http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html.

Procédure

1. Connectez-vous à Tivoli Common Reporting. Voir http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ttcr_login.html.
2. Configurez la source de données avec la commande **trcmd -modify**. Voir http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/rtcr_cli_modify.html.

   Remarque :
   - Le mot de passe de base de données MS SQL ne doit pas contenir de caractère spécial.
   - Vous devez définir la variable `Classpath` de telle sorte qu'elle contienne le pilote JDBC pour le serveur SQL.

Résultats

La nouvelle source de données est créée dans Tivoli Common Reporting.

Exécution d'un rapport

Vous pouvez exécuter un rapport sur demande ou en créer une image instantanée pour visualisation ultérieure.

Procédure

1. Pour exécuter un rapport sur demande, procédez comme suit :
   a. Dans la colonne **Format** du rapport, cliquez sur **HTML** ou **PDF**. La fenêtre On-Demand Report Parameters s'affiche.
   b. Dans cette fenêtre, indiquez les paramètres voulus et cliquez sur **Exécuter**.
2. Pour créer une image instantanée d'un rapport, procédez comme suit :
   a. Cliquez sur un rapport avec le bouton droit de la souris, puis cliquez sur **Paramètres**. La fenêtre Report Parameters s'affiche.
   b. Dans cette fenêtre, indiquez les paramètres voulus et cliquez sur **Enregistrer**.
   c. Cliquez sur un rapport avec le bouton droit de la souris, puis cliquez sur **Créer une image instantanée**.

d. Dans la fenêtre Report Parameters, indiquez les paramètres voulus et cliquez sur **Créer**. La fenêtre Report Snapshots s'affiche. Cette fenêtre indique le statut de l'image instantanée.
e. Dans la fenêtre Report Snapshots, cliquez avec le bouton droit de la souris sur une image instantanée terminée et sélectionnez **Visualisez au format**, puis indiquez sous quel format l'image instantanée doit paraître : en HTML, PDF, Excel ou PostScript.

Que faire ensuite

Créez de nouveaux rapports à l'aide du concepteur Business Intelligence Reporting Tool. Pour plus d'informations, voir «Création de rapports à l'aide du concepteur Eclipse Business Intelligence Reporting Tool».

Création de rapports à l'aide du concepteur Eclipse Business Intelligence Reporting Tool

Vous pouvez créer et éditer des rapports avec le concepteur Eclipse Business Intelligence Reporting Tool.

Pourquoi et quand exécuter cette tâche

Pour obtenir des astuces sur la manière de personnaliser des conceptions de rapports, consultez le document *Customizing Tivoli Common Reporting Report Designs* sur le site de DeveloperWorks, http://www.ibm.com/developerworks/tivoli/library/t-tcr/ibm_tiv_tcr_customizing_report_designs.pdf

Pour plus d'informations sur la base de données IBM Security Identity Manager et son schéma, consultez le document *Database and Schema Reference* à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itim.doc/im51_dbschema.htm.

Procédure

1. Téléchargez le concepteur Eclipse Business Intelligence Reporting Tool à l'adresse http://catalog.lotus.com/wps/portal/topal/details?catalog.label=1TW10OT02.
2. Ouvrez le support DVD ou le module de téléchargement ZIP dans Passport Advantage. Examinez la liste des fichiers.
3. Placez les fichiers dans Eclipse Report Project dans un ordre sélectionné.

Que faire ensuite

Visualisez les descriptions de rapport et leurs exemples de sorties. Pour plus d'informations, voir «Descriptions des rapports et paramètres».

Descriptions des rapports et paramètres

La présente section décrit les rapports et leurs paramètres.

Audit et sécurité : accès

La présente section décrit l'audit et le rapport de sécurité répertoriant toutes les définitions d'accès du système.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 38. Filtres pour le rapport des accès

Paramètre	Description
Type d'accès	Affiche le type d'accès, tel une application ou un dossier partagé. La valeur par défaut de ce paramètre est le symbole de pourcentage (%). Vous pouvez utiliser le symbole pourcentage (%) en tant que caractère générique. Par exemple, `%abc1%`. Si vous souhaitez entrer la hiérarchie d'accès, utilisez le format suivant : `Parent Access:Child Access:Child's Child Access`, etc.
Accès	Affiche l'accès pour lequel vous souhaitez générer un rapport. **Tout** indique que tous les accès peuvent être inclus en fonction de la sélection du type d'accès.
Maintenance	Affiche les informations de maintenance auxquelles est associé l'accès partagé.
Propriétaire de l'accès (Personne)	Affiche le nom du propriétaire de l'accès.

Comptes inactifs

Cette section décrit le rapport sur les comptes inactifs qui recense les comptes qui n'ont pas été utilisés récemment.

Les comptes qui ne disposent pas des dernières informations d'accès ne sont *pas* considérés comme inactifs. Les comptes qui ne sont pas inactifs incluent à la fois les nouveaux comptes pour lesquels la zone **Date du dernier accès** est vide et les comptes existants qui ne sont pas utilisés. Ces types de compte ne s'affichent *pas* dans un rapport de comptes inactifs. La synchronisation d'un service doit être effectuée.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 39. Filtres pour le rapport sur les comptes inactifs

Paramètre	Description
Service	Affiche les informations de service du compte inactif.
Période d'inactivité	Affiche le nombre de jours d'inactivité. La période d'inactivité doit être un nombre entier valide.
Comptes identifiés comme étant inactifs depuis	Affiche la liste des comptes inactifs depuis la date indiquée.

Habilitations accordées à un utilisateur

La présente section décrit le rapport sur les habilitations accordées à un utilisateur, répertoriant tous les utilisateurs et les règles d'application des accès qu'ils possèdent.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 40. Filtres pour le rapport sur les habilitations accordées à un utilisateur

Paramètre	Description
Propriétaire (Personne)	Affiche le propriétaire auquel sont accordées des habilitations.

Remarque : Ce rapport présente les droits directs et non les droits hérités.

Comptes non conformes

La présente section décrit le rapport sur les comptes non conformes.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 41. Filtres pour le rapport sur les comptes non conformes

Paramètre	Description
Service	Affiche les informations de service d'un compte non conforme.
Conformité du compte	Affiche la raison de conformité pour le compte. Par exemple : `Non autorisé` ou `Non conforme`

Comptes orphelins

La présente section décrit le rapport sur les comptes sans propriétaire.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 42. Filtres pour le rapport sur les comptes orphelins

Paramètre	Description
Service	Affiche les informations de service d'un compte orphelin.
Statut du compte	Affiche l'état du compte orphelin. Par exemple : `Actif` ou `Inactif`.

Demandes : approbations et rejets

Ce rapport répertorie les demandes approuvées ou rejetées.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 43. Filtres pour le rapport d'approbations et de rejets

Paramètre	Description
Approbateur	Affiche les informations sur les demandes faites par un approbateur spécifique.
ID utilisateur	Affiche les informations d'identification de l'utilisateur. Vous pouvez utiliser le symbole pourcentage (%) en tant que caractère générique. Par exemple : `%joe01%`
Service	Affiche les informations de service de l'approbation et du rejet.
Etat de demande d'approbation	Affiche l'état de la demande d'approbation.
Nom de l'activité d'approbation	Affiche le nom de l'activité d'approbation. Vous pouvez utiliser le symbole pourcentage (%) en tant que caractère générique. Par exemple : `%Approval for joe01%`

Tableau 43. Filtres pour le rapport d'approbations et de rejets (suite)

Paramètre	Description
Plage de dates	Affiche la plage de dates de l'approbation en nombre de jours.
Date de début	Affiche la date de début de l'approbation et du rejet.
Date de fin	Affiche la date de fin de l'approbation et du rejet.

Rapports sur les règles de séparation des tâches

La présente section décrit différents rapports sur les règles de séparation des tâches.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 44. Filtres pour le rapport de définition de règle de séparation des tâches

Paramètre	Description
Règle de séparation des tâches	Affiche le nom de la règle de séparation des tâches.
Unité commerciale	Affiche le nom de l'unité commerciale.
Remarque : Vous devez sélectionner les paramètres de nom de règle et d'unité commerciale à partir des menus correspondants.	

Rapport de violation de règle de séparation des tâches

La présente section décrit le rapport de violation de règle de séparation des tâches. Ce rapport contient les utilisateurs, les stratégies et les règles qui ont été violées, les approbations et les justifications (le cas échéant) et les responsables des modifications à l'origine des violations.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 45. Rapport de violation de règle de séparation des tâches

Paramètre	Description
Règle d'administration	Affiche le nom de la règle de séparation des tâches.
Unité commerciale	Affiche le nom de l'unité commerciale.
Nom de règle	Affiche le nom de la règle associée à la règle de séparation des tâches.

Services

La présente section décrit le rapport qui répertorie les services actuellement définis sur le système.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 46. Filtres pour le rapport sur les services

Paramètre	Description
Service	Affiche les informations de service.
Propriétaire (Personne)	Affiche les informations sur le propriétaires du service.

Tableau 46. Filtres pour le rapport sur les services (suite)

Paramètre	Description
Unité commerciale	Affiche le nom de l'unité commerciale.

Résumé des comptes sur un service

La présente section décrit un rapport qui établit un récapitulatif des comptes d'un service défini dans le système.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 47. Filtres pour le récapitulatif des comptes sur un rapport de service

Paramètre	Description
Service	Affiche les informations de service du compte.
Statut du compte	Affiche l'état du compte de service. Par exemple : `Actif` ou `Inactif`.

Comptes suspendus

La présente section décrit le rapport qui répertorie les comptes suspendus.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 48. Filtres pour le rapport des comptes suspendus

Paramètre	Description
ID utilisateur	Affiche les informations d'identification de l'utilisateur. Vous pouvez utiliser le symbole pourcentage (%) en tant que caractère générique.
Propriétaire de compte (Personne)	Affiche les informations de propriétaire du compte suspendu.
Service	Affiche les informations de service du compte suspendu.
Plage de dates	Affiche le nombre de jours pour la plage de dates dans les comptes suspendus.
Date de début	Affiche la date de début des comptes suspendus.
Date de fin	Affiche la date de fin des comptes suspendus.

Rapport de l'historique de recertification d'utilisateur

La présente section décrit le rapport historique des recertifications d'utilisateur effectuées manuellement (par des agents de recertification spécifiques) ou automatiquement (suite à un dépassement de délai d'attente).

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 49. Filtres pour le rapport de l'historique de recertification d'utilisateur

Paramètre	Description
Plage de dates	Affiche la plage de dates de l'historique de recertification d'utilisateur en nombre de jours. **Remarque :** Vous pouvez sélectionner une période de rapport standard, par exemple les 30 derniers jours, ou saisir une date de début et de fin spécifique pour le rapport.
Date de début	Affiche la date de début de l'historique de recertification d'utilisateur.
Date de fin	Affiche la date de fin de l'historique de recertification d'utilisateur.
Unité commerciale	Affiche le nom de l'unité commerciale.
Règles d'administration de recertification d'utilisateur	Affiche des informations sur les règles de recertification d'utilisateur.
Utilisateur	Affiche l'utilisateur d'une unité commerciale. Vous pouvez utiliser le symbole pourcentage (%) en tant que caractère générique. Par exemple : `%joe%`
Statut de l'utilisateur	Affiche le statut de l'utilisateur à sélectionner.
Agent de recertification	Affiche l'utilisateur à sélectionner en tant qu'agent de recertification.
Décision de recertification	Affiche la décision de recertification à sélectionner.

Rapport de définition de règle de recertification d'utilisateur

La présente section décrit un rapport qui répertorie des informations sur les règles de recertification définies dans le système.

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 50. Filtres pour le rapport de définition de règle de recertification d'utilisateur

Paramètre	Description
Règles d'administration de recertification d'utilisateur	Affiche le nom de la règle de recertification d'utilisateur.
Unité commerciale	Affiche le nom de l'unité commerciale.

Rapport de définition détaillé de règle de séparation des tâches

Le rapport de définition détaillé affiche les informations suivantes :

- Informations sur la règle de recertification d'utilisateur
- Informations sur l'agent de recertification
- Cible de rôle
- Cible de compte
- Cible de groupe

Rapport de l'historique d'accès partagé

Ce rapport affiche l'historique de l'audit d'accès partagé. Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 51. Filtres pour le rapport de l'historique d'accès partagé

Paramètre	Description
Plage de dates	Affiche la plage de dates de l'accès partagé en nombre de jours. **Remarque :** Vous pouvez utiliser Tivoli Common Reporting installé sur la machine distante. Dans de rares situations, aucune donnée ou des données partielles peuvent s'afficher dans les rapports. Pour éviter cette situation, indiquez la date et l'heure se trouvant sur le serveur Security Identity Manager.
Date de début	Affiche la date de début de l'historique de l'accès partagé.
Date de fin	Affiche la date de fin de l'historique d'accès partagé.
Unité commerciale de service	Affiche l'unité commerciale associée au service.
Service	Affiche les informations de maintenance auxquelles est associé l'accès partagé.
Unité commerciale du propriétaire d'accès partagé	Affiche l'unité commerciale associée au propriétaire d'accès partagé.
Propriétaire d'accès partagé	Affiche le nom du propriétaire d'accès partagé.
Accès partagé	Affiche le nom du droit d'accès partagé, tel le nom de droits d'accès ou le nom du pool de droits d'accès.

Droits d'accès partagés par propriétaire

Ce rapport affiche les droits d'accès partagés pour le propriétaire sélectionné. Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

Tableau 52. Filtres pour les droits d'accès partagés par rapports utilisateur

Paramètre	Description
Unité commerciale de service	Affiche l'unité commerciale associée au service.
Service	Affiche les informations de maintenance auxquelles sont associés des droits d'accès partagés.
Unité commerciale du propriétaire d'accès partagé	Affiche le nom de l'unité commerciale pour le propriétaire d'accès partagé.
Propriétaire d'accès partagé	Affiche le nom du propriétaire d'accès partagé (utilisateur ou rôle).

Droits d'accès partagés par rôle

Ce rapport affiche les droits d'accès partagés pour le rôle sélectionné. Le tableau suivant décrit les paramètres que vous pouvez utiliser pour filtrer le rapport selon vos spécifications.

L'attribut Propriétaire n'est pas présent par défaut. Vous devez mapper l'attribut `Propriétaire` se trouvant dans les `Rôles organisationnels` avec le mappage de schéma.

Voir la rubrique "Mappage des schémas de rapports" dans le document *IBM Security Identity Manager - Guide d'administration*.

Tableau 53. Filtres pour les droits d'accès partagés par rapports de rôle

Paramètre	Description
Unité commerciale	Affiche le nom de l'unité commerciale.
Rôle	Affiche la liste des rôles.
Type d'habilitation	Affiche le type d'un droit, droits d'accès ou pool de droits d'accès, par exemple.

Maintenance des rapports

Le temps d'indisponibilité n'ayant pas d'impact sur les besoins métiers représente un exemple de fenêtre de maintenance. Lorsqu'un mot de passe de droit d'accès à une base de données expire ou doit être changé, il s'agit d'un exemple de tâche de maintenance.

Modification de l'alias d'authentification JAAS

Si le nom d'utilisateur ou le mot de passe d'une base de données change, vous devez mettre à jour l'alias d'authentification du service JAAS (Java Authentication and Authorization Service).

Procédure

1. Ouvrez un shell de commandes.
2. Identifiez l'objet de configuration afin de pouvoir le repérer dans la commande MODIFY :

   ```
   wsadmin>print AdminConfig.list("JAASAuthData")
   ```

   L'objet de configuration qui s'affiche est similaire à cette valeur :

   ```
   (cells/tcrCell|security.xml#JAASAuthData_1202487694421)
   ```
3. Modifiez le mot de passe et l'ID utilisateur en exécutant la commande suivante :

   ```
   wsadmin>AdminConfig.modifyconfiguration_object
        [["userid", "newid"]])
       [["password", "newpassword"]])
   ```

   où :

   - *configuration_object* indique l'objet que vous avez précédemment identifié.
   - *newid* indique le nouvel ID utilisateur de la base de données.
   - *newpassword* indique le nouveau mot de passe correspondant à l'ID utilisateur.

Exemple

Dans l'exemple suivant, le mot de passe de l'objet de configuration `(cells/tcrCell|security.xml#JAASAuthData_12024876944 21)` devient `mynewpassword` :

```
wsadmin>AdminConfig.modify("(cells/tcrCell|
security.xml#JAASAuthData_12024876944 21)",
[["password", "mynewpassword"]])
```

Vous pouvez utiliser un appel semblable de mise à jour pour l'attribut `userId`.

Que faire ensuite

Modifiez le fournisseur JDBC. Pour plus d'informations, voir «Modification du fournisseur JDBC».

Modification du fournisseur JDBC

Le pilote JDBC est modifié lorsque vous migrez d'un fournisseur de base de données, tel que Oracle ou Microsoft SQL, vers un autre, tel que DB2. Vous pouvez migrer la base de données entre plusieurs plateformes de fournisseur de base de données, d'Oracle vers DB2, par exemple. Supprimez la configuration JDBC existante et créez un fournisseur JDBC ainsi que la configuration de la source de données.

Pourquoi et quand exécuter cette tâche

Pour créer la configuration de la source de données dans la section de configuration, procédez comme suit :

Procédure

1. Supprimez la source de données comme suit :

   ```
   wsadmin> AdminConfig.remove(
    AdminConfig.getid("/DataSource:ITIM DB Data Source"))
   ```

2. Après avoir supprimé la source de données, supprimez le fournisseur JDBC comme suit :

   ```
   wsadmin> AdminConfig.remove(
    AdminConfig.getid("/JDBCProvider:JDBC provider for the ITIM DB"))
   ```

3. Créez un fournisseur JDBC et une source de données pour la nouvelle base de données et le nouveau fournisseur. Pour plus d'informations, voir «Création d'un fournisseur de connectivité JDBC (Java Database Connectivity)», à la page 194.

Que faire ensuite

Modifiez la source de données. Pour plus d'informations, voir «Modification de la source de données».

Modification de la source de données

Si l'hôte ou le port du serveur de base de données ou le nom de la base de données change, vous devez mettre à jour la configuration de la source de données.

Pourquoi et quand exécuter cette tâche

Pour les bases de données Oracle, cette configuration nécessite une modification de la propriété URL pour appliquer la nouvelle URL JDBC. Pour les bases de données DB2 et Microsoft SQL Server, cette configuration nécessite une modification de la propriété spécifique ou des propriétés qui ont changé. Dans l'exemple suivant la propriété `portNumber` est mise à jour avec `1435` :

Exemple

```
AdminConfig.modify(AdminConfig.getid("/DataSource/
ITIM DB Data Source/J2EEResourcePropertySet:/
J2EEResourceProperty/portNumber/"),
[["value", "1435"]])
```

Des commandes semblables peuvent être utilisées pour la mise à jour des autres propriétés de ressource J2EE de sources de données :

`URL` pour bases de données Oracle

`serverName` et `databaseName` pour DB2 et des bases de données Microsoft SQL Server

Que faire ensuite

Enregistrez les modifications de configuration. Pour plus d'informations, voir «Sauvegarde des modifications apportées à la configuration».

Sauvegarde des modifications apportées à la configuration

Vous devez sauvegarder la configuration pour mettre à jour les modifications de la source de données.

Pourquoi et quand exécuter cette tâche

Pour enregistrer la configuration de la source de données, procédez comme suit :

Procédure

1. Sauvegardez la configuration avec la commande **wsadmin**.
2. Redémarrez la WebSphere Application Server.

Résultats

Les modifications apportées à la configuration sont sauvegardées dans WebSphere Application Server.

Débogage

Cette rubrique fournit les procédures de débogage.

Erreurs lors de la génération et du formatage de rapports

Cette rubrique décrit les erreurs pouvant survenir lors de la génération et du formatage de rapports.

Pourquoi et quand exécuter cette tâche

Si le formatage d'un rapport échoue, un message d'erreur semblable au suivant s'affiche :

```
CTGTRV014E: The report cannot be successfully formatted because it completed with
errors, reference ID [REPORTIT_33_OBJECTID_7fe67fe6].
Click on the following link to view the report with the errors.
CTGTRV011E: See the Tivoli Common Reporting log files for more information.
https://localhost:30343/TCR/Reports/view
```

Pour visualiser les détails de l'échec de formatage dans le rapport, procédez comme suit :

Procédure

1. Cliquez sur le lien dans le message d'erreur. Examinez le rapport généré incluant des erreurs.
2. Faites défiler le texte pour visualiser les erreurs qui apparaissent en rouge en bas du rapport.
3. Cliquez sur le symbole plus (+) à côté de la légende du message d'erreur. Vous pouvez développer la liste pour visualiser la trace de pile entière. Cette dernière peut vous aider à identifier l'incident ou le type d'erreur dont il s'agit. Par exemple, en cas d'expiration du mot de passe pour la source de données, les droits d'accès à la base nécessitent quelques mises à jour dans la console **wsadmin**. Tivoli Common Reporting nécessite une maintenance pour la mise à jour de la base de données ou des droits d'accès JDBC.
4. Modifiez le rapport dans le concepteur Eclipse Business Intelligence Reporting Tool pour corriger l'incident.

Que faire ensuite

Vérifiez les journaux. Pour plus d'informations, voir «Journaux».

Journaux

Cette section décrit les journaux associés à Tivoli Common Reporting.

Pourquoi et quand exécuter cette tâche

Tivoli Common Reporting comporte deux fichiers de journaux :

SystemErr.log
Affiche les journaux des erreurs.

SystemOut.log
Affiche les journaux des sorties système.

Les fichiers journaux se trouvent dans les répertoires suivants :

- `TCR_HOME\eWas61\profiles\tcrProfile\logs\tcrServer`
- Le répertoire temporaire dans lequel est installé Tivoli Common Reporting. Par exemple, `C:\temp` sous Windows ou `/temp` sous UNIX.

Pour savoir interpréter les informations trouvées dans les journaux, consultez le centre de documentation de Tivoli Common Reporting à l'adresse : http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.tivoli.tcr.doc/tcr_welcome.html.

Pour plus d'informations sur la consignation et la création de nouveaux rapports Tivoli Common Reporting, voir *Report Logging for JavaScript Routines* à l'adresse :

http://www.ibm.com/developerworks/tivoli/library/t-tcr/ibm_tiv_tcr_report_logging.pdf

Tivoli Common Reporting utilise des scripts de consignateur pendant la génération du rapport.

Problèmes connus et solutions

La présente section décrit les incidents recensés pour Tivoli Common Reporting ainsi que les solutions liées.

Le diagramme à barres n'affiche pas la valeur inférieure

Incident

Si un diagramme à barres contient deux totaux dont les valeurs se trouvent à une distance importante l'un de l'autre, la valeur inférieure peut ne pas apparaître. Par exemple, lorsque vous exécutez le rapport sur les comptes orphelins, un service peut avoir 10 000 comptes inactifs. L'autre service comporte uniquement trois comptes inactifs. Le logiciel n'affiche le service contenant uniquement trois comptes inactifs.

Solution

Cette omission est un problème connu.

Le moteur graphique de l'outil de génération de rapports Eclipse Business Intelligence Reporting Tool n'affiche pas toutes les catégories sur l'axe des X

Incident

Lors de l'exécution d'un rapport avec diagramme, les catégories sur l'axe des X n'affichent pas toujours tous les éléments disponibles.

Solution

Le fait que les éléments disponibles ne s'affichent pas est un problème connu.

La légende du graphique conserve l'affichage des séries non autorisées

Incident

Si vous exécutez le rapport de comptes non conformes avec le paramètre de conformité de compte étant défini sur `Non autorisé`, le graphique continue d'afficher `Non conforme` bien que le paramètre ait éliminé les comptes non conformes.

Solution

Procédez comme suit :

1. Créez un double du graphique sans les séries non conformes, mais conservez les séries non autorisées.
2. Recréez un double du graphique sans les séries non autorisées et conservez les séries non conformes. Le rapport des non-conformités comporte maintenant trois graphiques.
3. Définissez de manière conditionnelle la visibilité de chaque graphique en fonction de la valeur du paramètre de conformité.

Firefox version 1.5 affiche une génération de rapport antérieure lors de l'exécution d'un rapport PDF

Incident

Vous pouvez exécuter un rapport et définir la sortie au format PDF. Laissez alors la fenêtre de rapport ouverte pendant que vous tentez de réexécuter le même rapport avec des paramètres différents. Firefox version 1.5 affichera à nouveau le premier rapport au format PDF au lieu d'afficher le second. Tivoli Common Reporting confirme que le second rapport est en cours d'exécution et envoyé à Firefox, mais Firefox version 1.5 réaffiche le premier rapport au format PDF.

Solution

N'exécutez pas le second rapport dans la fenêtre ouverte.

Le graphique affiche la légende avec toutes les séries définies

Incident

Toutes les séries s'affichent dans les graphiques bien que les paramètres de rapport devraient éliminer des valeurs de série données.

Solution

Ce manque de filtrage dans l'affichage est un problème connu.

Un lien hypertexte s'affiche toujours dans le rapport

Incident

Le lien hypertexte d'exploration en aval dans le rapport de droits accordés à un utilisateur est toujours affiché, même si un propriétaire est défini pour un paramètre.

Solution

Eclipse Business Intelligence Reporting Tool ne peut pas désactiver de lien hypertexte à l'aide de JavaScript sous condition.

Le dernier enregistrement de la ligne du tableau est séparé entre deux pages

Incident

Eclipse Business Intelligence Reporting Tool sépare quelquefois une ligne de tableau en deux pages.

Solution

Cette division de ligne est un problème connu.

L'erreur OutOfMemoryException apparaît avec des ensembles de résultats importants

Incident

La configuration par défaut de la machine virtuelle serveur WebSphere Application Server intégré Java (JVM) intégrée peut provoquer un manque de mémoire. Le problème survient lors du traitement de rapports couvrant des ensembles de résultats importants (des dizaines de milliers).

Solution

Modifiez la taille maximale de pile de la machine virtuelle JVM à l'aide de la commande **wsadmin** sur le serveur Tivoli Common Reporting serveur WebSphere Application Server intégré. Procédez comme suit :

1. Entrez la commande suivante :

   ```
   AdminConfig.modify(
    AdminConfig.getid("/JavaVirtualMachine:/"),
     [["maximumHeapSize", "1024"]])
   ```

   La taille maximale de pile est alors définie à 1024 Mo.
2. Utilisez `AdminConfig.save()` pour enregistrer les modifications.
3. Redémarrez le serveur Tivoli Common Reporting pour que les modifications de configuration prennent effet.

Pour extraire la configuration du processus JVM en cours, entrez la commande **wsadmin** suivante :

```
print AdminConfig.show(
 AdminConfig.getid("/JavaVirtualMachine:/"))
```

Vous trouverez les fichiers journaux de l'erreur `OutOfMemoryException` dans les journaux de trace de WebSphere Tivoli Common Reporting.

Les listes de paramètres comprennent des noms en double

Incident

Si vous utilisez des valeurs en double dans un paramètre de zone de liste dynamique, il vous sera peut-être impossible de sélectionner l'élément approprié. Par exemple, il est possible que vous ayez deux utilisateurs nommés `Bob Smith` possédant des valeurs sous-jacentes qui rendent leur ID respectif unique. Lorsque vous exécutez un rapport, IBM Security Identity Manager affiche deux fois `Bob Smith` parce que leurs valeurs sous-jacentes sont uniques. Toutefois, lorsqu'un utilisateur sélectionne le deuxième `Bob Smith` dans la liste déroulante, cette dernière sélectionnera toujours le premier `Bob Smith`.

Solution

Afin de pouvoir sélectionner correctement les deux paramètres, exécutez le rapport dans le concepteur Eclipse Business Intelligence Reporting Tool et sélectionnez la prévisualisation, puis **Fichier -> Afficher le rapport**.

Le PDF d'un rapport volumineux ne se charge pas

Incident

Lorsque vous exécutez un rapport de taille importante sans indiquer de paramètres de filtrage des données, la sortie en format PDF ne se charge pas.

Solution

Lorsque vous exécutez des rapports susceptibles de fournir un nombre important de résultats, spécifiez autant de paramètres de filtrage que possible. De même, vous pouvez aussi indiquer l'option de sortie HTML.

Les valeurs du diagramme à secteurs se chevauchent

Incident

Les valeurs numériques peuvent se chevaucher et devenir illisibles pour les petites sections d'un diagramme à secteurs, tel que le diagramme de rapport Compte suspendu.

Solution

Ce chevauchement de données est un problème connu.

Les listes de paramètres du rapport ne contiennent pas toutes les valeurs

Incident

L'interface utilisateur Tivoli Common Reporting offre une visibilité restreinte des paramètres de rapport dans les listes.

Solution

Si vous ne voyez pas une valeur requise dans la liste, entrez les premières lettres de cette valeur. Entrez les lettres jusqu'à ce que la valeur s'affiche dans la liste et que vous puissiez la sélectionner. Par exemple, il peut exister 100 définitions de service nommées **Service hébergé *N*** configurées dans un déploiement IBM Security Identity Manager. La variable *N* correspond au numéro du service hébergé. Pour sélectionner **Service hébergé 810**, entrez `Service hébergé 81`.

Les rapports ne peuvent pas inclure d'utilisateurs d'une organisation partenaire

Incident

Les rapports IBM Security Identity Manager ne peuvent pas faire de compte-rendus sur les utilisateurs d'une organisation partenaire sans personnalisation des rapports via le concepteur de rapports Eclipse Business Intelligence Reporting Tool.

Solution

Pour plus d'informations sur la personnalisation des rapports, consultez le document *Customizing Tivoli Common Reporting Report Designs* sur le site DeveloperWorks, http://www.ibm.com/developerworks/tivoli/library/t-tcr/ibm_tiv_tcr_customizing_report_designs.pdf

L'exécution de rapports volumineux entraîne la fragmentation de la mémoire

Incident

Vous pouvez générer avec succès des rapports importants, l'un comportant 400.000 lignes par exemple, d'après les fichier de trace de Tivoli Common Reporting. L'exemple suivant affiche un message de trace d'un ensemble important de données de rapport :

```
[3/21/08 1:13:55:593 IST] 00000026 DiskCache     I
End of process, and the count of data is 418128
```

La quantité de données rapportées peut provoquer des incidents d'allocation de mémoire dans la machine virtuelle Java (JVM) et causer une fragmentation de la mémoire. Des exécutions ultérieures du rapport peuvent échouer en raison d'exceptions liées au manque de mémoire.

Solution

Redémarrez le serveur Tivoli Common Reporting.

Les paramètres des services affichent des valeurs non valides

Incident

Le paramètre de service utilisé dans les rapports affiche tous les noms de services dans la liste. Toutefois, le logiciel n'affiche pas certaines valeurs de paramètre de service dans la console IBM Security Identity Manager.

Solution

Cette différence dans les listes de rapport et de console est un problème connu.

Les paramètres instantanés n'affichent pas un texte normal

Incident

Les paramètres instantanés affichent une seule valeur au lieu du texte d'affichage normal des paramètres de zone de liste dynamique.

Solution

Cet affichage d'une valeur unique est un problème connu.

Le rapport instantané est vide au format Excel

Incident

Lorsque vous créez un rapport instantané d'un rapport et que l'exécution de ce rapport instantané ne donne aucun résultat, un téléchargement de ce dernier au format Microsoft Excel produit une erreur Excel. Par exemple :

```
'XML ERROR in Style'
```

Les formats PDF et HTML se téléchargent correctement.

Solution

Cette omission est un problème connu.

Le texte dans les rapports s'affiche de manière incorrecte en cas d'utilisation de langues asiatiques

Incident

Lorsque vous exécutez un rapport et essayez d'en afficher les résultats en format HTML ou PDF, le texte apparaît comme s'il était endommagé. Cet incident se produit lors de l'utilisation des langues asiatiques : chinois, coréen et japonais.

Solution

Tivoli Common Reporting transforme des graphiques en images sur le serveur. Si le serveur ne prend pas en charge les polices de caractères pour la langue à utiliser, le texte des graphiques apparaît déformé.

Installez et activez les polices de caractère asiatiques appropriées dans le système d'exploitation. Par exemple, sous Windows, procédez comme suit :

1. Cliquez sur **démarrer -> Panneau de configuration -> Options régionales et linguistiques**.
2. Sélectionnez l'onglet **Langues**.
3. Sélectionnez la case à cocher **Installer les fichiers pour les lanques d'Extrême-Orient** et cliquez deux fois sur **OK**.

Problème d'échelle de paramètre dans le rapport de nom distinctif de l'utilisateur

Le paramètre **Nom distinctif de l'utilisateur** dans la liste déroulante **Utilisateur** des rapports IBM Security Identity Manager basés sur IBM Tivoli Common Reporting ne se met pas complètement à l'échelle.

Incident

Le paramètre **Nom distinctif de l'utilisateur** ne se met pas complètement à l'échelle dans la liste déroulante **Utilisateur** quand le nombre d'entrées d'utilisateurs est important. C'est le cas, par exemple, dans le rapport sur les droits accordés à un utilisateur.

Solution

Procédez comme suit :

1. Utilisez le concepteur Eclipse Business Intelligence Reporting Tool pour modifier le rapport Tivoli Common Reporting ayant le paramètre de rapport de liste déroulante dynamique **Nom distinctif de l'utilisateur**. Changez le paramètre de rapport **Nom distinctif de l'utilisateur** en paramètre de rapport de zone de texte statique.
2. Remplacez le paramètre `AND NAPerson.DN like ?` par `AND NAPerson.GIVENNAME like ?` dans l'ensemble de données nommé `Tableau des habilitations accordées à un utilisateur`.
3. Exécutez la modification dans le concepteur Eclipse Business Intelligence Reporting Tool. Importez ensuite un fichier d'archive ZIP du package de rapport dans Tivoli Common Reporting qui permet l'exécution de ce rapport modifié sans le paramètre **Nom distinctif de l'utilisateur**.

Chapitre 17. Gestion de l'alimentation d'identité

En tant qu'administrateur, vous devez effectuer un certain nombre d'étapes initiales pour extraire les données sur les employés d'un ou de plusieurs référentiels de ressources humaines. Utilisez ces données pour remplir le registre IBM Security Identity Manager avec un ensemble d'utilisateurs équivalent.

Présentation

Une *identité* est un sous-ensemble de données de profil qui représente un utilisateur de façon unique dans un ou plusieurs référentiels, ainsi que d'autres informations associées à cet utilisateur. Par exemple, une identité peut se composer d'une combinaison unique des prénoms, nom de famille, nom complet et numéro d'employé d'une personne. Les données peuvent également contenir d'autres informations, telles que des numéros de téléphone, le nom du responsable et une adresse électronique. Une source de données peut être un référentiel d'utilisateurs d'un client ou un fichier, un répertoire, ou une source personnalisée.

IBM Security Identity Manager permet d'ajouter un nombre d'utilisateurs au système en lisant une source de données, telle qu'un référentiel d'utilisateurs, un répertoire, un fichier ou une source personnalisée. Le processus d'ajout d'utilisateurs à partir d'un référentiel de données d'utilisateur est appelé *alimentation d'identité* ou *alimentation HR*.

La *synchronisation* d'une alimentation d'identité est le processus de synchronisation des données entre la source de données et IBM Security Identity Manager. Le rapprochement initial remplit IBM Security Identity Manager de nouveaux utilisateurs, avec leurs données de profils. Une synchronisation consécutive crée de nouveaux utilisateurs et met à jour le profil des utilisateurs existants qui ont été trouvés.

Vous pouvez utiliser plusieurs formats de fichiers pour charger les enregistrements d'identité dans le registre d'utilisateurs IBM Security Identity Manager.

Vous devez anticiper l'effet d'informations manquantes dans l'enregistrement utilisateur. Par exemple, l'enregistrement placé dans IBM Security Identity Manager peut ne pas avoir d'adresse électronique pour l'utilisateur. L'utilisateur ne reçoit pas de mot de passe pour un nouveau compte dans un message électronique et doit appeler le service d'assistance ou contacter un responsable.

Sources communes pour les alimentations d'identité

IBM Security Identity Manager fournit les types de service suivants pour traiter bon nombre des sources d'alimentations d'identité les plus courantes :

- Alimentation d'identité CSV (fichier de valeurs séparées par des virgules)
- Alimentation d'identité DSML
- Alimentation d'identité AD OrganizationalPerson (Microsoft Windows Active Directory)
- Alimentation d'identité INetOrgPerson (LDAP)
- Service IDI Data Feed

Vous pouvez remplir le contenu initial et les modifications ultérieures de ce contenu du registre d'utilisateurs à partir des sources suivantes :

Fichier CSV (valeurs séparées par des virgules)
Utiliser un fichier de valeurs séparées par des virgules (CSV). Un fichier CSV contient un ensemble d'enregistrements séparés par une paire d'alimentation retour chariot - saut de ligne. Chaque enregistrement contient un ensemble de champs séparés par une virgule. Vous pouvez utiliser une règle d'administration des identités globale pour sélectionner les attributs de schéma qui créent un ID utilisateur.

Fichier DSML (Directory Services Markup Language) v1
Utiliser un fichier DSML v1 pour remplir le registre d'utilisateurs. Un fichier DSML représente des informations structurelles d'annuaire au format de fichier XML. Si vous exécutez l'alimentation d'identités plusieurs fois, les utilisateurs en double sont modifiés selon le fichier le plus récent. Une règle d'administration des identités globale ne s'applique pas à un fichier DSML.

Windows Server Active Directory
A partir de Windows Server Active Directory, importation des seules informations figurant dans la partie de schéma `inetOrgPerson` d'un utilisateur Windows Server Active Directory. Vous pouvez utiliser une règle d'administration des identités globale pour sélectionner les attributs de schéma qui créent un ID utilisateur. Le processus d'alimentation d'identité utilise tous les objets utilisateur de la base indiquée.

Alimentation d'identité INetOrgPerson
Utiliser un serveur d'annuaire LDAP. Les données utilisent la classe d'objets correspondant au nom du profil d'utilisateur indiqué dans la définition de service. Vous pouvez utiliser une règle d'administration des identités globale pour sélectionner les attributs de schéma qui créent un ID utilisateur. Le processus d'alimentation d'identité ignore les enregistrements qui n'ont pas la classe d'objets indiquée.

Sources d'identités personnalisées
Utiliser des sources d'identités personnalisées pour remplir le contenu initial et les modifications ultérieures du contenu du registre d'utilisateurs. Selon la source d'identités, vous pouvez utiliser une règle d'administration des identités globale pour sélectionner les attributs de schéma qui créent un ID utilisateur.

Par exemple, utilisez une alimentation d'identités IBM Tivoli Directory Integrator pour obtenir davantage de souplesse qu'avec une alimentation de données standard. Les fonctions supplémentaires incluent :

- Utilisation d'un sous-ensemble de données, tel que le filtrage des utilisateurs d'un service donné
- Mappage d'attributs supplémentaires au-delà du mappage standard
- Activation des recherches de données (responsable d'un employé, par exemple) obtenues à partir d'une autre source de données
- Modification de la détection sur la source de données
- Utilisation des bases de données et systèmes des ressources humaines comme DB2 Universal Database et SAP
- Commande des attributs, par exemple une mise à jour de statut telle que la suspension d'un utilisateur
- Suppression des enregistrements d'identités

- Réalisation de modifications avec IBM Tivoli Directory Integrator et non avec les synchronisations IBM Security Identity Manager

Pour plus d'informations sur le fait de fournir des alimentations d'identité personnalisées, reportez-vous aux informations sur l'intégration d'IBM Tivoli Directory Integrator dans le répertoire `extensions` d'IBM Security Identity Manager.

Activation de flux de travaux pour les alimentations d'identité

Quelle que soit la méthode utilisée, le serveur IBM Security Identity Manager peut être configuré pour appeler le moteur de flux de travaux pour les enregistrements d'alimentation d'identité. L'activation du moteur de flux de travaux provoque la mise en oeuvre de toutes les règles d'application des accès pour les identités entrantes. La configuration entraîne des performances de flux plus lentes. Les utilisateurs sont automatiquement inscrits dans les rôles dynamiques applicables, même si le moteur de flux de travaux n'est pas activé pour une alimentation d'identité. Pour les chargements initiaux, il est conseillé d'importer les identités dans le système, puis d'activer les règles d'application des accès applicables pour améliorer les performances de l'alimentation d'identité.

Alimentation d'identité CSV (fichier de valeurs séparées par des virgules)

L'alimentation d'identité avec valeurs séparées par des virgules (CSV) permet de lire le fichier de valeurs séparées par des virgules (CSV) pour ajouter des utilisateurs à IBM Security Identity Manager.

Type de service CSV

Ce type de service d'alimentation d'identité analyse les alimentations d'identité qui utilisent les formats de fichiers CSV conformes à la grammaire RFC 4180. L'analyseur syntaxique d'IBM Security Identity Manager bénéficie des améliorations suivantes par rapport à la RFC :

- Supprime les espaces de début et de fin d'un texte non placé entre guillemets, à l'intérieur d'une zone. A l'inverse, la RFC 4180 prend en compte tous les espaces, qu'ils soient à l'intérieur ou à l'extérieur des guillemets.
- Autorise l'affichage de texte entre et hors guillemets dans une même zone. A l'inverse, la RFC 4180 n'admet pas ces deux types de texte à l'intérieur d'une même zone.
- N'impose pas, à l'inverse de la RFC 4180, que tous les enregistrements aient le même nombre de zones. Toutefois, le code qui appelle l'analyseur syntaxique CSV renvoie une erreur si un enregistrement comporte plus de zones que l'en-tête de fichier CSV.
- Accepte les marques de fin d'enregistrement CR (retour chariot) et CR/LF (retour chariot - saut de ligne) pour être compatible avec les fichiers de base UNIX et DOS. A l'inverse, RFC 4180 termine tous les enregistrements par les caractères CR/LF.

Services utilisant les fichiers CSV

Dans IBM Security Identity Manager, les types suivants de services utilisent les fichiers CSV comme entrée :

- Le service d'alimentation d'identité CSV

- Les services personnalisés qui utilisent le type Fournisseur de services manuels. Ces services personnalisés utilisent un format de fichier CSV pour le fichier de téléchargement de synchronisation. Ce type de service peut être utilisé pour les alimentations d'identité et de comptes.

  Par défaut, tous les comptes définis dans un fichier CSV pour le rapprochement d'un service manuel sont marqués comme actifs dans IBM Security Identity Manager. Pour suspendre un utilisateur ou un compte à l'aide d'un rapprochement de service manuel, ajoutez l'attribut `erpersonstatus` ou `eraccountstatus` au fichier CSV (selon qu'il s'agit d'alimentations d'identités ou de comptes). Une valeur `0` (zéro) signifie actif. Une valeur `1` signifie inactif.
- Les services personnalisés qui utilisent le type Fournisseur d'adaptateurs Directory Integrator avec le connecteur CSV de IBM Tivoli Directory Integrator. Ce type de service peut être utilisé pour les alimentations d'identité et de comptes.

Format de fichier CSV

Un fichier CSV contient un ensemble d'enregistrements séparés par la paire de caractères retour chariot/saut de ligne (CR/LF, \r\n) ou par un caractère de saut de ligne (LF). Chaque enregistrement contient un ensemble de zones séparées par une virgule. Si la zone contient une virgule ou un retour chariot/saut de ligne, la virgule doit être définie en tant que caractère d'échappement à l'aide de guillemets comme délimiteur. Le premier enregistrement du fichier source CSV définit les attributs fournis dans chacun des enregistrements suivants. Par exemple :

```
uid,sn,cn,givenname,mail,initials,employeenumber,erroles
```

Les attributs `sn` et `cn` sont requis par les classes d'objets utilisées par IBM Security Identity Manager pour représenter un utilisateur. Le processus d'alimentation d'identité utilise tous les objets du fichier. Le fichier CSV ne peut pas contenir d'attributs binaires.

Vous pouvez utiliser un attribut à plusieurs valeurs pour indiquer un utilisateur qui est membre de plusieurs groupes. Il peut s'agir des groupes Propriétaire du service, Windows Local Management (groupe défini automatiquement) et Responsables. Si vous incluez des attributs à plusieurs valeurs, ils doivent être représentés en utilisant plusieurs colonnes avec le même nom d'attribut.

Pour indiquer des attributs à plusieurs valeurs, répétez la colonne autant de fois que nécessaire. Par exemple :

```
cn, erroles, erroles, erroles, sn
cn1,role1, role2, role3, sn1
cn2,rolea,,,sn2
```

L'enregistrement placé dans IBM Security Identity Manager peut ne pas avoir d'adresse électronique pour l'utilisateur. L'utilisateur ne reçoit pas de message électronique de notification contenant un mot de passe pour le nouveau compte et doit appeler le service d'assistance ou contacter un responsable.

Connecteur CSV pour IBM Tivoli Directory Integrator

Vous trouverez des informations sur le connecteur CSV pour IBM Tivoli Directory Integrator dans le répertoire suivant du produit :

ITIM_HOME/extensions/examples/idi_integration/HRFeedCSV/ITDIFeedExpress

Codage UTF-8 dans un fichier d'alimentation des identités

Le fichier d'alimentation des identités doit être au format UTF-8. Vous devez utiliser un éditeur prenant en charge le codage UTF-8.

- Windows

  Les éditeurs suivants prennent en charge le codage UTF-8 : Microsoft Word 97 ou version supérieure, ou bloc-notes (inclus avec les systèmes d'exploitation Windows 2003 Server ou Windows XP).

  Pour enregistrer un fichier au format UTF-8 à l'aide du bloc-notes, cliquez sur **Fichier** > **Enregistrer sous**. Ensuite, développez la liste d'options de la zone **Codage** et sélectionnez `UTF-8`.

- Linux

  L'éditeur de texte Vim (version de l'éditeur vi traditionnel) prend en charge le format UTF-8. Pour utiliser des fichiers au format UTF-8 dans l'éditeur de texte Vim, indiquez :

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

  Si votre version d'UNIX n'inclut pas cet éditeur de texte, téléchargez-le à partir du site Web suivant :

  http://www.vim.org

Remarque : Remarque : pour le sous-ensemble de code ASCII 7 bits, le format Unicode en UTF-8 est identique au format ASCII 7 bits. Pour les fichiers d'entrée contenant des caractères ASCII 7 bits (valeurs de caractère ASCII entre hex 20 et hex 7e), vous pouvez créer les fichiers à l'aide d'un éditeur de texte standard. Pour les fichiers contenant d'autres valeurs de caractères (y compris les caractères européens étendus), vous devez enregistrer le fichier au format UTF-8.

Pour obtenir la liste complète des caractères ASCII 7 bits compatibles avec le format UTF-8, accédez au site Web suivant, puis cliquez sur le lien de caractères **latins de base** dans la première colonne :

http://www.unicode.org/charts

Alimentation d'identité DSML (Directory Services Markup Language)

L'alimentation d'identité en langage DSML (Directory Services Markup Language) permet de lire un fichier DSML pour ajouter des utilisateurs à IBM Security Identity Manager.

Type de service DSML

Le serveur IBM Security Identity Manager permet l'intégration de sources de données de divers types de ressources humaines (HR) dans le but d'ajouter automatiquement un grand nombre de personnes au serveur IBM Security Identity Manager sans qu'il soit nécessaire d'ajouter manuellement chaque personne. Un enregistrement d'identité dans les données HR devient une instance d'un objet utilisateur dans IBM Security Identity Manager. Le service DSML Identity Feed est un type d'alimentation des données de type HR (ressources humaines). Le service peut recevoir les informations de deux manières : par rapprochement ou par notification automatique.

Les mécanismes qui gèrent les données relatives aux ressources humaines dans IBM Security Identity Manager exigent que les données de ressources humaines

soient à un format XML. Le format utilise le schéma standard défini par DSML (Directory Services Markup Language) version 1. Pour plus d'informations, voir le site Web DSML sur la page http://www.oasis-open.org. Lors de l'envoi de notifications asynchrones, un format de message XML défini par DAML version 1 (Directory Access Markup Language) est utilisé. DAML est une spécification XML, définie par IBM, qui permet la spécification d'opérations d'ajout, de modification et de suppression.

Format de fichier DSML

DSML est un format XML qui décrit les informations du répertoire. Un *fichier DSML* représente les informations de la structure d'annuaire en format de fichier XML. Le fichier DSML doit contenir uniquement des attributs valides du profil IBM Security Identity Manager. Le processus d'alimentation d'identité utilise tous les objets du fichier.

L'attribut `erPersonPassword` est utilisé dans une alimentation d'identité, uniquement lors d'un processus de création d'utilisateur, et non lors d'un processus de modification d'utilisateur. Si la valeur de l'attribut `erPersonPassword` est définie, le mot de passe du compte IBM Security Identity Manager aura cette valeur lors de la création de l'utilisateur et du compte. L'instruction suivante définit une valeur pour l'attribut `erPersonPassword` :

```
<attr name="erpersonpassword"><value>panther2</value></attr>
```

Si vous sélectionnez un format de fichier DSML pour une alimentation d'identité, indiquez un fichier DSML similaire au fichier suivant :

```
<entry dn="uid=sparker">
<objectclass><oc-value>inetOrgPerson</oc-value></objectclass>
<attr name="givenname"><value>Scott</value></attr>
<attr name="initials"><value>SVP</value></attr>
<attr name="sn"><value>Parker</value></attr>
<attr name="cn"><value>Scott Parker</value></attr>
<attr name="telephonenumber"><value>(919) 321-4666</value></attr>
<attr name="postaladdress"><value>222 E. First Street Durham, NC  27788</value></attr>
</entry>
```

Codage UTF-8 dans un fichier d'alimentation des identités

Le fichier d'alimentation des identités doit être au format UTF-8. Vous devez utiliser un éditeur prenant en charge le codage UTF-8.

- Windows

  Les éditeurs suivants prennent en charge le codage UTF-8 : Microsoft Word 97 ou version supérieure, ou bloc-notes (inclus avec les systèmes d'exploitation Windows 2003 Server ou Windows XP).

  Pour enregistrer un fichier au format UTF-8 à l'aide du bloc-notes, cliquez sur **Fichier** > **Enregistrer sous**. Ensuite, développez la liste d'options de la zone **Codage** et sélectionnez `UTF-8`.

- Linux

  L'éditeur de texte Vim (version de l'éditeur vi traditionnel) prend en charge le format UTF-8. Pour utiliser des fichiers au format UTF-8 dans l'éditeur de texte Vim, indiquez :

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

  Si votre version d'UNIX n'inclut pas cet éditeur de texte, téléchargez-le à partir du site Web suivant :

  http://www.vim.org

Remarque : Remarque : pour le sous-ensemble de code ASCII 7 bits, le format Unicode en UTF-8 est identique au format ASCII 7 bits. Pour les fichiers d'entrée contenant des caractères ASCII 7 bits (valeurs de caractère ASCII entre hex 20 et hex 7e), vous pouvez créer les fichiers à l'aide d'un éditeur de texte standard. Pour les fichiers contenant d'autres valeurs de caractères (y compris les caractères européens étendus), vous devez enregistrer le fichier au format UTF-8.

Pour obtenir la liste complète des caractères ASCII 7 bits compatibles avec le format UTF-8, accédez au site Web suivant, puis cliquez sur le lien de caractères **latins de base** dans la première colonne :

http://www.unicode.org/charts

Code JavaScript à l'intérieur des alimentations d'identité DSML

La base de données des ressources humaines peut également modifier le serveur IBM Security Identity Manager proactivement à mesure que des modifications sont détectées.

Le serveur IBM Security Identity Manager est livré avec un fournisseur de services JNDI (Java Naming and Directory Interface). Le fournisseur peut être utilisé comme interface de programmation pour communiquer les modifications au serveur. Ces modifications sont reçues par le serveur sous forme de notification de modification d'événements. Cette fonctionnalité est appelée notification d'événements. Lorsque vous utilisez un programme de notification d'événements pour importer des données de ressources humaines, il est possible d'effectuer des opérations d'ajout, de modification et de suppression.

Utilisation du fournisseur de services JNDI pour DAML

Avant d'utiliser le fournisseur de services JNDI pour DAML, vous devez bien connaître la spécification de l'interface JNDI et LDAP. Le fournisseur de services JNDI utilise ces deux concepts. Cette section fournit des liens vers les informations relatives à l'interface JNDI et à LDAP.

JNDI Interface JNDI (Java Naming and Directory Interface) permettant d'accéder aux informations de type répertoire à partir d'un programme Java. Voir le site Web relatif à Sun Microsystem à l'adresse http://java.sun.com/products/jndi/tutorial/ pour obtenir un tutoriel sur l'interface JNDI.

LDAP Lightweight Directory Access Protocol. Vous pouvez obtenir des informations sur ce protocole de différentes manières. Vous pouvez par exemple accéder au site OpenLDAP Foundation, à l'adresse http:/www.openldap.org.

Les bibliothèques Java requises pour utiliser JNDI et DAML/DSML se trouvent dans le sous-répertoire `lib` du répertoire serveur IBM Security Identity Manager.

Notifications d'événements des données HR

Les données HR peuvent être envoyées au serveur IBM Security Identity Manager par un autre programme sous forme d'un message DAML/HTTP sur SSL.

Le message DAML/HTTP sur SSL est envoyé au serveur IBM Security Identity Manager sous forme d'une demande POST HTTP sur SSL. Le fournisseur de services JNDI (Java Naming and Directory Interface) pour DAML/HTTPS est fourni dans ce but.

Initialisation du contexte

Pour toutes les opérations utilisant le fournisseur de services JNDI pour DAML, la première étape consiste à initialiser le contexte. Ce dernier doit être initialisé avec toutes les propriétés de protocole requises pour communiquer avec le serveur IBM Security Identity Manager.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vérifiez que vous avez importé ces modules :

- `import javax.naming.*;`
- `import javax.naming.directory.*;`
- `import java.util.*;`

Pourquoi et quand exécuter cette tâche

Pour initialiser le contexte, modifiez les variables d'environnement suivantes :

```
Hashtable env = new Hashtable();
env.put (Context.INITIAL_CONTEXT_FACTORY,
"com.ibm.daml.jndi.DAMLContextFactory");
env.put(Context.SECURITY_PRINCIPAL,serviceUserName);
env.put(Context.SECURITY_CREDENTIALS, servicePassword);
env.put("com.ibm.daml.jndi.DAMLContext.CA_CERT_DIR", certDirLocation);
env.put(Context.PROVIDER_URL,providerURL);
env.put("com.ibm.daml.jndi.DAMLContext.URL_TARGET_DN", serviceDN);

DirContext damlContext = new InitialDirContext (env);
```

Résultats

Une fois le contexte initialisé, une demande de liaison est envoyée au serveur Security Identity Manager. Si les variables d'environnement ne sont pas correctes, une exception d'attribution de nom `NamingException` est générée.

Que faire ensuite

Après l'initialisation, vous pouvez effectuer les tâches suivantes :

- Ajouter une entrée d'utilisateur
- Modifier une entrée d'utilisateur
- Supprimer une entrée d'utilisateur

Ajout d'un utilisateur

Les attributs permettant d'ajouter un utilisateur sont identiques à ceux utilisés dans la méthode de rapprochement des fichiers.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vérifiez que vous avez initialisé le contexte.

Pourquoi et quand exécuter cette tâche

Les attributs permettant d'ajouter un utilisateur sont identiques à ceux utilisés dans la méthode de rapprochement des fichiers. Le nom distinctif de l'entrée du nouvel utilisateur doit comporter au moins un attribut unique servant à identifier l'utilisateur, par exemple l'ID utilisateur. La règle de positionnement JavaScript définie pour le service d'alimentation d'identité DSML est utilisée pour déterminer l'unité organisationnelle à laquelle l'entrée de l'utilisateur est ajoutée. Si les informations relatives à l'organisation ne sont pas fournies, l'utilisateur est ajouté à la racine de l'organisation. (Le nom distinctif est indiqué avec les méthodes `createSubcontext / destroySubcontext / modifyAttributes` dans l'exemple suivant).

L'attribut `objectclass` doit être défini et correspondre à la classe d'objet LDAP mappée au type d'utilisateur à ajouter. Cette classe est généralement `inetOrgPerson`, mais d'autres classes d'objets peuvent être utilisées si elles sont définies avec la fonction de configuration d'entité dans serveur IBM Security Identity Manager. Ajoutez la classe d'objets nécessaire comme une nouvelle entité, avec `"Entity Type" = "Utilisateur"`.

Pour ajouter un utilisateur, exécutez les étapes suivantes :

Procédure

1. Définissez le nom distinctif de l'utilisateur que vous voulez ajouter.
2. Créez un objet Attributs pour contenir la liste d'objets d'attribut pour le nouvel utilisateur.
3. Appelez `createSubContext` dans le contexte.

Résultats

Une fois que le nom distinctif et les attributs de l'utilisateur ont été créés, la méthode `createSubcontext` est appelée avec le contexte JNDI.

Exemple

```
BasicAttributes ba = new BasicAttributes(true);
ba.put(new BasicAttribute("objectclass","inetorgperson"));
ba.put(new BasicAttribute("uid", uid));
ba.put(new BasicAttribute("cn", "JoeSmith"));
ba.put(new BasicAttribute("mail", uid + "@acme.com"));

damlContext.createSubcontext("uid="+ uid, ba);
```

Que faire ensuite

Vous avez la possibilité d'exécuter les tâches suivantes :

- Ajouter une autre entrée d'utilisateur
- Modifier les informations d'une entrée d'utilisateur
- Supprimer une entrée d'utilisateur

Modification d'une entrée d'utilisateur

Pour modifier une entité d'utilisateur, vous devez créer une liste d'éléments de modification, puis appeler `modifyAttributes` dans le contexte.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vérifiez que vous avez initialisé le contexte.

Pourquoi et quand exécuter cette tâche

Pour modifier les valeurs d'attribut pour un utilisateur (notamment pour ajouter de nouveaux attributs ou supprimer des attributs existant), exécutez les étapes suivantes :

Procédure

1. Définissez le nom distinctif de l'utilisateur que vous voulez modifier.
2. Créez une liste d'éléments de modification `ModificationItems` contenant les modifications nécessaires.
3. Appelez `modifyAttributes` dans le contexte.

Résultats

Après la définition du nom distinctif de l'utilisateur, un appel de `modifyAttributes` est effectué avec le contexte JNDI.

Exemple

```
Vector mods = new Vector();
//Ajouter un attribut (ou une valeur supplémentaire si l'attribut existe déjà)
mods.add(new ModificationItem(DirContext.ADD_ATTRIBUTE, new BasicAttribute("roomnumber", "102")));
// Modifier un attribut existant
mods.add(new ModificationItem(DirContext.REPLACE_ATTRIBUTE, new BasicAttribute("title","Consultant")));
// Modifier un attribut existant en lui affectant un attribut à plusieurs valeurs
newOuAt = new BasicAttribute("ou");
newOuAt.add("Research Department");
newOuAt.add("DevelopmentDivision");
mods.add(new ModificationItem(DirContext.REPLACE_ATTRIBUTE, newOuAt));
// Supprimer un attribut existant
mods.add(new ModificationItem(DirContext.REMOVE_ATTRIBUTE,new BasicAttribute("initials", null)));
String dn = "uid=" + uid;
damlContext.modifyAttributes(dn,(ModificationItem[])mods.toArray(new ModificationItem[mods.size()]));
```

Que faire ensuite

Vous avez la possibilité d'exécuter les tâches suivantes :

- Ajouter une entrée d'utilisateur
- Supprimer une entrée d'utilisateur

Suppression d'une entrée d'utilisateur

Pour supprimer un utilisateur, définissez le nom distinctif de l'utilisateur, puis appelez `destroySubContext` dans le contexte.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Vérifiez que vous avez initialisé le contexte.

Pourquoi et quand exécuter cette tâche

Pour supprimer une entrée d'utilisateur, exécutez les étapes suivantes :

Procédure

1. Définissez le nom distinctif de l'utilisateur que vous voulez supprimer.
2. Appelez `destroySubContext` dans le contexte.

Résultats

Après la définition du nom distinctif de l'utilisateur, un appel de `destroySubContext` est effectué avec le contexte JNDI.

Exemple

```
damlContext.destroySubcontext("uid=" + uid);
```

Que faire ensuite

Vous avez la possibilité d'exécuter les tâches suivantes :

- Ajouter une entrée d'utilisateur
- Modifier les informations d'une entrée d'utilisateur

Exemple de pilote pour les notifications d'événements des données HR

Ce programme de test Java et l'exemple de compilateur ajoutent cent entrées d'utilisateur à l'organisation IBM.

But

Ce programme suppose qu'il existe un locataire portant le nom abrégé `ibm` et contenant une organisation nommée IBM Security Identity Manager. Dans cette organisation, il existe un service d'alimentation d'identité DSML possédant les attributs suivants :

- Nom du service - dsmltest
- UID - dsml
- Mot de passe - dsml

Ces informations sont toutes indiquées dans les lignes `serviceDN`, `serviceUID` et `servicePassword` du programme d'essai suivant.

L'emplacement du serveur IBM Security Identity Manager est indiqué à la ligne `providerURL`.

Programme d'essai

Cet exemple de programme n'utilise pas de certificat client (il n'utilise pas l'authentification SSL bidirectionnelle). Une copie du certificat issu par l'autorité de certification pour le certificat du serveur installé sur le serveur IBM Security Identity Manager doit se trouver dans le répertoire `\certificates` (ligne `cerDirLocation`).

```
// TestDSML.java
import java.io.*;
import java.util.*;
import javax.naming.*;
import javax.naming.directory.*;
```

```
public class TestDSML {
  // Service DN.This is constructed of four parts:
  // "erservicename=dsmltest" specifies the name of the Service
  // "ou=itim" is the Organization
  // "ou=ibm" is the Tenant
  // "dc=com" is the base of the LDAP tree for IBM Security Identity Manager.
 static final String DEFAULT_SERVICEDN  =
     "erservicename=dsmltest, ou=itim, ou=ibm, dc=com";
 static final String DEFAULT_HOST  =
     "localhost:4443";

public static void main(String arg[]) {
  // number of people to process
  int noOfPeople = Integer.getInteger("count", 100).intValue();
  // required operation ("add", "del", "mod")
  String op = System.getProperty("op", "add").toLowerCase();

  String certDirLocation = "\\certificates";    //where to get the CA certificates
  // URL to use.
  // Use "/enrole/unsolicited_notification" to specify the Unsolicited Notification Servlet,
  // which is the servlet used for DSML requests -
  String host = System.getProperty("host", DEFAULT_HOST);
  String providerURL = "https:// " + host + "/enrole/unsolicited_notification";
  // Target DN
  String serviceDN = System.getProperty("servicedn", DEFAULT_SERVICEDN);

  String serviceUID = "dsml";      // user id defined for the service
  String servicePassword = "dsml";   // password define for the services

  // create and fill the environment table
  Hashtable env = new Hashtable();
  env.put (Context.INITIAL_CONTEXT_FACTORY,
    "com.ibm.daml.jndi.DAMLContextFactory");
  env.put(Context.SECURITY_PRINCIPAL, serviceUID);
  env.put(Context.SECURITY_CREDENTIALS, servicePassword);
  env.put("com.ibm.daml.jndi.DAMLContext.CA_CERT_DIR", certDirLocation);
  env.put(Context.PROVIDER_URL, providerURL);
  env.put("com.ibm.daml.jndi.DAMLContext.URL_TARGET_DN", serviceDN);

  DirContext damlContext = null;
  try {
    // generate connection request
    damlContext = new InitialDirContext (env);
  }
  catch (NamingException e) {
    System.out.println("Error connecting to server at \"" + providerURL + "\": " + e.getMessage());
    return;
  }
  for (int i = 1; i&lt;=noOfPeople; i++) {
    String sn = "smith" + i;
    String uid = "jsmith" + i;
    String dn = "uid=" + uid;

    try {
     if (op.startsWith("add")) {
      BasicAttributes ba = new BasicAttributes(true);
      ba.put(new BasicAttribute("objectclass","inetorgperson"));
      ba.put(new BasicAttribute("uid", uid));
      ba.put(new BasicAttribute("cn", "Joe Smith"));
      ba.put(new BasicAttribute("mail", uid + "@acme.com"));
      ba.put(new BasicAttribute("sn"));


     damlContext.createSubcontext(dn, ba);
    }
    else if (op.startsWith("del")) {
     damlContext.destroySubcontext(dn);
    }
    else if (op.startsWith("mod")) {
     Vector mods = new Vector();
     // Add a new attribute (or additional value if it already exists)
     mods.add(new ModificationItem(DirContext.ADD_ATTRIBUTE, new BasicAttribute("roomnumber", "102")));
     // Modify an existing Attribute
     mods.add(new ModificationItem(DirContext.REPLACE_ATTRIBUTE, new BasicAttribute("title", "Consultant")));
     // Modify an existing Attribute to a multi-valued value
    Attribute newOuAt = new BasicAttribute("ou");
    newOuAt.add("Research Department");
    newOuAt.add("Development Division");
    mods.add(new ModificationItem(DirContext.REPLACE_ATTRIBUTE, newOuAt));
    // Delete one existing attribute
    mods.add(new ModificationItem(DirContext.REMOVE_ATTRIBUTE, new BasicAttribute("initials", null)));

    damlContext.modifyAttributes(dn, (ModificationItem[])mods.toArray(new ModificationItem[mods.size()]));
    }
   }
   catch (Exception e)  {
     System.out.println("Error, DN \"" + dn + "\": " + e.getMessage());
     e.printStackTrace();
```

```
    }
  }
 }
}
```

Exemple de compilateur

Voici un exemple de script Windows XP pour compiler le programme de test précédent :

```
@rem compileDsmlTest.cmd - compile DSML Test Program
setlocal
rem locationof the lib directory containing the jar files from the
rem IBM Security Identity Manager installation lib directory, as listed below
set LIB=C:\ITIM\lib
set APP=TestDSML

rem Library files from IBM Security Identity Manager lib directory -
set AGENTLIB=%LIB%\enroleagent.jar
set CLASSPATH=.;%AGENTLIB%;%LIB%\jlog.jar

javac -classpath %CLASSPATH% -d . %APP%.java
endlocal
```

Importation de données de ressources à l'aide de la synchronisation

Les données de ressources humaines peuvent être importées dans le serveur IBM Security Identity Manager à partir d'un fichier écrit en DSML, à l'aide du fournisseur de services d'alimentation d'identité DSML.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Dans un environnement groupé, le fichier DSML est présent sur toutes les machines qui sont membres de la grappe sur le même site. Lors d'une synchronisation, le fichier DSML peut être trouvé quel que soit le membre du cluster qui prend l'initiative de la synchronisation.

Le fichier DSML doit être présent sur la machine du serveur Security Identity Manager pour une configuration donnée du serveur.

Pourquoi et quand exécuter cette tâche

Lorsque vous utilisez le service d'alimentation d'identité DSML pour importer des données de ressources humaines d'un fichier DSML, seules les opérations d'ajout et de modification d'utilisateurs sont effectuées. L'opération de suppression d'utilisateur n'est pas disponible lors de l'importation d'informations d'enregistrement d'identité à partir d'un fichier DSML.

Remarque : Lors du traitement des informations d'enregistrement d'identité à partir d'un fichier DSML, on suppose que le jeu de données synchronisé ne représente pas toute la population d'utilisateurs pour le serveur Security Identity Manager. Il est donc possible d'utiliser la méthode d'interrogation pour ajouter ou modifier des utilisateurs, mais pas pour en supprimer. Pour supprimer des utilisateurs, vous devez utiliser l'interface de notification des événements.

Pour importer les données de ressources humaines avec le type de service Alimentation d'identité DSM, procédez comme suit :

Procédure

1. Créez une instance du service DSML Identity Feed.
2. Configurez le service de sorte qu'il se réfère à un fichier DSML contenant les données d'enregistrement d'identité. Indiquez le chemin d'accès complet du fichier DSML. Utilisez la fonctionnalité de test du service pour vérifier que le nom de fichier est correct.
3. Rapprochez le service.

Résultats

Lors du rapprochement du service DSML Identity Feed, les entrées d'enregistrement d'identité sont extraites du fichier DSML. Pour chaque entrée d'enregistrement d'identité, la classe d'objets est comparée au profil utilisateur approprié dans IBM Security Identity Manager. En cas de correspondance, le nom distinctif (dn) est converti en filtre de recherche. Ce filtre recherche une correspondance avec une entrée d'utilisateur dans l'entreprise qui contient le service. Si une correspondance est détectée, l'entrée d'utilisateur est utilisée pour la mise à jour de l'entrée existante. Si aucune correspondance est trouvée, l'individu est ajouté en tant que nouvelle entrée d'utilisateur. Les correspondances en double renvoient une erreur et l'entrée n'est pas ajoutée.

Exemple

Ces instructions constituent un exemple d'entrée DSML pour un utilisateur.

```
<entry dn="uid=jsmith">
   <objectclass>
          <oc-value>inetOrgPerson</oc-value>
   </objectclass>
   <attr name="sn"><value>smith</value></attr>
   <attr name="uid"><value>jsmith</value></attr>
   <attr name="mail"><value>jsmith@IBM.com</value></attr>
   <attr name="givenname"><value>John</value></attr>
   <attr name="cn"><value>John Smith</value></attr>
</entry>
```

Que faire ensuite

Vous pouvez maintenant ajouter, modifier et supprimer des informations d'identité avec l'interface IBM Security Identity Manager.

Vous pouvez ajouter d'autres utilisateurs, modifier des utilisateurs existants avec le fichier DSML et supprimer des utilisateurs.

Formulaire de service DSML Identity Feed

Les zones du formulaire du service d'alimentation d'identité DSML sont utilisées pour fournir des informations sur l'alimentation d'identité DSML (Directory Services Markup Language). Par exemple, vous pouvez sélectionner un profil de service pour importer des données d'identité avec DSML. Remplissez les zones du formulaire pour établir une connexion au serveur dans lequel se trouve le service.

Les zones suivantes sont disponibles dans le formulaire du service d'alimentation d'identité DSML :

Nom du service
Indiquez un nom vous aidant à identifier l'instance de service.

Description
Indiquez des informations supplémentaires sur l'instance de service.

ID utilisateur
Indiquez l'ID utilisateur administratif pour l'instance de service.

Mot de passe
Indiquez le mot de passe administratif pour l'instance de service. Si une authentification par mot de passe est utilisée, entrez une valeur. Sinon, la synchronisation va échouer.

Nom de fichier
Indiquez le nom de fichier, y compris le nom de chemin d'accès, contenant les informations sur l'utilisateur.

Remarque : Dans les environnements groupés, le fichier doit être stocké dans le même emplacement dans tous les membres de la grappe.

Utiliser le flux de travaux
Sélectionnez cette case à cocher pour utiliser le flux de travaux pour cette instance de service et déterminer si vous souhaitez créer automatiquement des comptes pour les entrées. Cette fonction peut être utilisée pour de petits flux incrémentiels, mais pas pour importer de grands volumes de données.

Règle de positionnement
Indiquez une règle à utiliser pour placer un utilisateur (personne) dans l'arborescence de l'organisation. Cette règle est définie avec un script. Le contexte correspond aux informations d'identité de l'utilisateur en cours dans la transmission et le service qui définit la transmission.

Exemple de fichier DSML pour la synchronisation

Utilisez cet exemple comme modèle pour créer le fichier DSML que vous voulez utiliser pour importer les données de ressources humaines avec la synchronisation.

Exemple

Le fichier DSML suivant est un exemple de fichier XML complet à utiliser dans la synchronisation :

```
<?xml version="1.0" encoding="UTF-8"?>
<dsml>

   <directory-entries>

   <entry dn="uid=janesmith">
      <objectclass>
         <oc-value>inetOrgPerson</oc-value>
      </objectclass>
      <attr name="ou"><value>Engineering</value></attr>
      <attr name="sn"><value>Smith </value></attr>
      <attr name="uid"><value>janesmith</value></attr>
      <attr name="mail"><value>j.smith@ibm.com</value></attr>
      <attr name="givenname"><value>Jane</value></attr>
      <attr name="cn"><value>Jane Smith</value></attr>
      <attr name="initials"><value>JS</value></attr>
      <attr name="employeenumber"><value>E_1974</value></attr>
      <attr name="title"><value>Research and Development</value></attr>
      <attr name="telephonenumber"><value>(888) 555-1614</value></attr>
      <attr name="mobile"><value>(888) 555-8216</value></attr>
      <attr name="homepostaladdress"><value>15440 Laguna Canyon Rd, Irvine, CA 92614</value></attr>
      <attr name="roomnumber"><value>G-114</value></attr>
      <attr name="homephone"><value>(888) 555-3222</value></attr>
      <attr name="pager"><value>(888) 555-7756</value></attr>
```

```
      <attr name="erAliases">
         <value>j.smith</value>
         <value>jane_smith</value>
         <value>JaneSmith</value>
      </attr>
      <attr name="erRoles">
         <value>Engineering</value>
         <value>Development</value>
      </attr>
   </entry>
   <entry dn="uid=johndoe">
      <objectclass>
         <oc-value>inetOrgPerson</oc-value>
      </objectclass>
      <attr name="ou"><value>Sales-West</value></attr>
      <attr name="sn"><value>Doe</value></attr>
      <attr name="uid"><value>johndoe</value></attr>
      <attr name="mail"><value>j.doe@ibm.com</value></attr>
      <attr name="givenname"><value>John</value></attr>
      <attr name="cn"><value>JohnDoe</value></attr>
      <attr name="initials"><value>JD</value></attr>
      <attr name="employeenumber"><value>S_1308</value></attr>
      <attr name="title"><value>Sales Engineer</value></attr>
      <attr name="telephonenumber"><value>(888) 555-1620</value></attr>
      <attr name="mobile"><value>(888) 555-8210</value></attr>
      <attr name="homepostaladdress"><value>15440 Laguna Canyon Rd, Irvine, CA 92614</value></attr>
      <attr name="roomnumber"><value>G-120</value></attr>
      <attr name="homephone"><value>(888) 555-3228</value></attr>
      <attr name="pager"><value>(888) 555-7750</value></attr>
      <attr name="erAliases">
         <value>j.doe</value>
         <value>john_doe</value>
         <value>JohnDoe</value>
      </attr>
      <attr name="erRoles">
         <value>Sales</value>
      </attr>
   </entry>

</directory-entries>

</dsml>copy from here to there
```

Alimentation d'identité AD Organizational

L'alimentation d'identité AD Organizational permet de créer des utilisateurs à partir des enregistrements utilisateur de Windows Server Active Directory (AD).

Cette alimentation utilise une ressource de répertoire comme source d'alimentation. L'information de la classe d'objets `organizationalPerson` AD est mappée au schéma `inetOrgPerson`. Cette alimentation d'identité charge tous les objets utilisateur d'une base indiquée.

Type de service AD Organizational

Lorsque vous créez une instance de service pour cette alimentation d'identité, les informations suivantes sont nécessaires :

- L'URL utilisée pour se connecter à la ressource de répertoire
- L'ID utilisateur et le mot de passe pour accéder à la ressource
- Le contexte d'affectation de nom, qui est la base de recherche dans la terminologie LDAP et définit où commencer la recherche dans l'arborescence de répertoires
- L'attribut de nom, qui doit être sélectionné parmi les valeurs fournies

Après sa création, ce service est défini pour synchroniser une branche spécifique du répertoire.

Mappage d'attributs personnalisé

L'option **Nom de fichier du mappage d'attribut** fournit un moyen de personnaliser le mappage d'attributs LDAP aux attributs IBM Security Identity Manager.

Le format du fichier du mappage d'attributs est `feedAttrName=itimAttrName`. Les lignes commençant par un signe dièse (`#`) ou un point-virgule (`;`) sont interprétées comme des commentaires.

Le fichier de mappage d'attributs remplace complètement les mappages par défaut. Tous les attributs nécessaires de la source d'alimentation doivent être inclus dans le fichier de mappage.

Celui-ci doit contenir les attributs suivants :

- Ceux qui sont indiqués comme nécessaires dans le formulaire de profil de la personne
- Ceux qui sont indiqués comme nécessaires dans le schéma LDAP pour le profil de la personne cible

Si un attribut de la source d'identité ne figure pas dans le fichier de mappage d'attributs, la valeur n'est pas définie sur l'attribut IBM Security Identity Manager.

L'exemple suivant montre que six attributs sont mappés. Tous les autres attributs LDAP sont ignorés.

```
#feedAttrName=itimAttrName
cn=cn
sn=sn
title=title
telephonenumber=mobile
mail=mail
description=description
```

Codage UTF-8 dans un fichier d'alimentation des identités

Le fichier d'alimentation des identités doit être au format UTF-8. Vous devez utiliser un éditeur prenant en charge le codage UTF-8.

- Windows

  Les éditeurs suivants prennent en charge le codage UTF-8 : Microsoft Word 97 ou version supérieure, ou bloc-notes (inclus avec les systèmes d'exploitation Windows 2003 Server ou Windows XP).

  Pour enregistrer un fichier au format UTF-8 à l'aide du bloc-notes, cliquez sur **Fichier** > **Enregistrer sous**. Ensuite, développez la liste d'options de la zone **Codage** et sélectionnez `UTF-8`.

- Linux

  L'éditeur de texte Vim (version de l'éditeur vi traditionnel) prend en charge le format UTF-8. Pour utiliser des fichiers au format UTF-8 dans l'éditeur de texte Vim, indiquez :

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

  Si votre version d'UNIX n'inclut pas cet éditeur de texte, téléchargez-le à partir du site Web suivant :

  http://www.vim.org

Remarque : Remarque : pour le sous-ensemble de code ASCII 7 bits, le format Unicode en UTF-8 est identique au format ASCII 7 bits. Pour les fichiers d'entrée contenant des caractères ASCII 7 bits (valeurs de caractère ASCII entre hex 20 et hex 7e), vous pouvez créer les fichiers à l'aide d'un éditeur de texte standard. Pour les fichiers contenant d'autres valeurs de caractères (y compris les caractères européens étendus), vous devez enregistrer le fichier au format UTF-8.

Pour obtenir la liste complète des caractères ASCII 7 bits compatibles avec le format UTF-8, accédez au site Web suivant, puis cliquez sur le lien de caractères **latins de base** dans la première colonne :

http://www.unicode.org/charts

Alimentation d'identité inetOrgPerson

L'alimentation d'identité inetOrgPerson prend en charge le serveur d'annuaire LDAP avec RFC2798 (classe d'objets LDAP `inetOrgPerson`).

Cette alimentation utilise une ressource de répertoire comme source d'alimentation. Cette alimentation d'identité charge tous les objets `inetOrgPerson` d'une base indiquée. Les enregistrements qui n'ont pas `objectclass=inetOrgPerson` sont ignorés.

Type de service inetOrgPerson

Lorsque vous créez une instance de service pour cette alimentation d'identité, les informations suivantes sont nécessaires :

- L'URL utilisée pour se connecter à la ressource de répertoire
- L'ID utilisateur et le mot de passe pour accéder à la ressource
- Le contexte d'affectation de nom, qui est la base de recherche dans la terminologie LDAP et définit où commencer la recherche dans l'arborescence de répertoires
- L'attribut de nom, qui doit être sélectionné parmi les valeurs fournies

Après sa création, ce service est défini pour synchroniser une branche spécifique du répertoire.

Mappage d'attributs personnalisé

L'option **Nom de fichier du mappage d'attribut** fournit un moyen de personnaliser le mappage d'attributs LDAP aux attributs IBM Security Identity Manager.

Le format du fichier du mappage d'attributs est `feedAttrName=itimAttrName`. Les lignes commençant par un signe dièse (`#`) ou un point-virgule (`;`) sont interprétées comme des commentaires.

Le fichier de mappage d'attributs remplace complètement les mappages par défaut. Tous les attributs nécessaires de la source d'alimentation doivent être inclus dans le fichier de mappage. Les attributs indiqués comme nécessaires dans le formulaire du profil d'utilisateur ou dans le schéma LDAP pour le profil d'utilisateur cible doivent figurer dans le fichier de mappage. Si un attribut de la source d'identité ne figure pas dans le fichier de mappage d'attributs, la valeur n'est pas définie sur l'attribut IBM Security Identity Manager.

L'exemple suivant montre que six attributs sont mappés. Tous les autres attributs LDAP sont ignorés.

```
#feedAttrName=itimAttrName
cn=cn
sn=sn
title=title
telephonenumber=mobile
mail=mail
description=description
```

Codage UTF-8 dans un fichier d'alimentation des identités

Le fichier d'alimentation des identités doit être au format UTF-8. Vous devez utiliser un éditeur prenant en charge le codage UTF-8.

- Windows

  Les éditeurs suivants prennent en charge le codage UTF-8 : Microsoft Word 97 ou version supérieure, ou bloc-notes (inclus avec les systèmes d'exploitation Windows 2003 Server ou Windows XP).

  Pour enregistrer un fichier au format UTF-8 à l'aide du bloc-notes, cliquez sur **Fichier** > **Enregistrer sous**. Ensuite, développez la liste d'options de la zone **Codage** et sélectionnez `UTF-8`.

- Linux

  L'éditeur de texte Vim (version de l'éditeur vi traditionnel) prend en charge le format UTF-8. Pour utiliser des fichiers au format UTF-8 dans l'éditeur de texte Vim, indiquez :

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

  Si votre version d'UNIX n'inclut pas cet éditeur de texte, téléchargez-le à partir du site Web suivant :

  http://www.vim.org

Remarque : Remarque : pour le sous-ensemble de code ASCII 7 bits, le format Unicode en UTF-8 est identique au format ASCII 7 bits. Pour les fichiers d'entrée contenant des caractères ASCII 7 bits (valeurs de caractère ASCII entre hex 20 et hex 7e), vous pouvez créer les fichiers à l'aide d'un éditeur de texte standard. Pour les fichiers contenant d'autres valeurs de caractères (y compris les caractères européens étendus), vous devez enregistrer le fichier au format UTF-8.

Pour obtenir la liste complète des caractères ASCII 7 bits compatibles avec le format UTF-8, accédez au site Web suivant, puis cliquez sur le lien de caractères **latins de base** dans la première colonne :

http://www.unicode.org/charts

Source de données IBM Tivoli Directory Integrator (IDI)

L'alimentation d'identité IBM Tivoli Directory Integrator (IDI) est utilisée pour prendre en charge les sources de données provenant des sources d'identité personnalisées et pour fournir plus de souplesse par rapport aux sources de données standard.

La source de données IDI est fournie pour des instances dans lesquelles les autres sources HR ne sont pas suffisantes. Utilisez un flux de données pour définir des alimentations d'identités personnalisées.

L'utilisation de cette source de données exige des notions de IBM Tivoli Directory Integrator (IDI).

Cette source de données sert à fournir plus de souplesse par rapport aux sources de données standard. Voici des exemples de cette souplesse :

- La possibilité de travailler avec un sous-ensemble de données, par exemple pour filtrer les utilisateurs d'un service donné
- Un mappage d'attributs allant au-delà du mappage un à un fourni par les sources standard
- Des recherches de données, par exemple pour dériver un superviseur ou un gestionnaire d'une autre source de données
- Détection des modifications dans la source de données
- Des bases de données et des systèmes de ressources humaines, tels que DB2, Oracle, PeopleSoft et SAP
- La commande des attributs, tels que la mise à jour du statut ou la suspension d'un utilisateur
- La suppression de personnes
- Des modifications gérées par IBM Tivoli Directory Integrator et non plus par les synchronisations IBM Security Identity Manager (utilisées pour les suppressions, les mises à jour et la détection des modifications)

Codage UTF-8 dans un fichier d'alimentation des identités

Le fichier d'alimentation des identités doit être au format UTF-8. Vous devez utiliser un éditeur prenant en charge le codage UTF-8.

- Windows

  Les éditeurs suivants prennent en charge le codage UTF-8 : Microsoft Word 97 ou version supérieure, ou bloc-notes (inclus avec les systèmes d'exploitation Windows 2003 Server ou Windows XP).

  Pour enregistrer un fichier au format UTF-8 à l'aide du bloc-notes, cliquez sur **Fichier** > **Enregistrer sous**. Ensuite, développez la liste d'options de la zone **Codage** et sélectionnez `UTF-8`.
- Linux

  L'éditeur de texte Vim (version de l'éditeur vi traditionnel) prend en charge le format UTF-8. Pour utiliser des fichiers au format UTF-8 dans l'éditeur de texte Vim, indiquez :

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

  Si votre version d'UNIX n'inclut pas cet éditeur de texte, téléchargez-le à partir du site Web suivant :

  http://www.vim.org

Remarque : Remarque : pour le sous-ensemble de code ASCII 7 bits, le format Unicode en UTF-8 est identique au format ASCII 7 bits. Pour les fichiers d'entrée contenant des caractères ASCII 7 bits (valeurs de caractère ASCII entre hex 20 et hex 7e), vous pouvez créer les fichiers à l'aide d'un éditeur de texte standard. Pour les fichiers contenant d'autres valeurs de caractères (y compris les caractères européens étendus), vous devez enregistrer le fichier au format UTF-8.

Pour obtenir la liste complète des caractères ASCII 7 bits compatibles avec le format UTF-8, accédez au site Web suivant, puis cliquez sur le lien de caractères **latins de base** dans la première colonne :

http://www.unicode.org/charts

Gestion d'informations d'identité avec IBM Tivoli Directory Integrator

Vous pouvez utiliser IBM Tivoli Directory Integrator pour importer les informations d'identité dans IBM Security Identity Manager et gérer les comptes des ressources externes dans le magasin de données d'IBM Security Identity Manager. Ces données d'identité peuvent provenir d'un référentiel de ressources humaines ou d'une autre source, telle qu'un annuaire de la société. Un enregistrement d'identité dans les données de ressources humaines devient une instance d'un objet utilisateur dans IBM Security Identity Manager. L'intégration avec IBM Tivoli Directory Integrator nécessite la connectivité du réseau au système IBM Security Identity Manager et un nouveau type de service pour gérer les sources de données.

Avantages de l'utilisation d'IBM Tivoli Directory Integrator :

- La programmation personnalisée n'est plus nécessaire pour manipuler des informations personnelles brutes dans un formulaire qui peut être importé dans IBM Security Identity Manager. IBM Tivoli Directory Integrator peut être utilisé pour analyser la syntaxe des données d'une base de données ou d'un fichier délimité par des virgules et pour fournir les résultats obtenus à IBM Security Identity Manager sous forme d'informations personnelles ou de modifications de ces informations. Auparavant, un fichier DSML (Directory Services Markup Language) ou un client JNDI (Java Naming and Directory Interface) personnalisé étaient requis.
- Il est possible de gérer des données d'identité dans lesquelles IBM Security Identity Manager peut servir de client DSMLv2 pour extraire des données utilisateur d'IBM Tivoli Directory Integrator par synchronisation en effectuant des recherches dans IBM Tivoli Directory Integrator, qui est utilisé comme serveur DSMLv2. IBM Security Identity Manager peut également être utilisé comme serveur DSMLv2 et accepter les demandes d'un client DSMLv2 tel qu'IBM Tivoli Directory Integrator, à l'aide du fournisseur de services JNDI.

  Remarque : DSMLv2 est obsolète dans IBM Security Identity Manager Version 5.0 en faveur de la structure éloignée de l'adaptateur IDI (RMI) d'appel des méthodes. DSMLv2 reste pris en charge dans cette édition.
- Avantages dans la gestion des comptes. Pour plus d'informations, voir le répertoire `extensions`.

Voir les documents fournis avec le produit IBM Tivoli Directory Integrator. Pour des exemples de personnalisation des schémas et d'importation des données dans une source de données d'identité, accédez au répertoire *ITIM_HOME*`/extensions/examples`.

Scénario : Chargement par lot de données d'identité

Un scénario classique d'utilisation d'IBM Tivoli Directory Integrator serait, par exemple, un administrateur qui chargerait en vrac des données d'identité dans IBM Security Identity Manager.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Une instance de Tivoli Directory Integrator doit fonctionner.

Pourquoi et quand exécuter cette tâche

Ce scénario comporte les tâches de haut niveau suivantes :

Procédure

1. Définition de la configuration de Tivoli Directory Integrator, incluant notamment un gestionnaire d'événements DSMLv2 et une chaîne d'assemblage avec un connecteur vers la source de données souhaitée.
2. Démarrage du gestionnaire d'événements Tivoli Directory Integrator.
3. Configuration d'un service IBM Security Identity Manager pour communiquer avec la configuration Tivoli Directory Integrator.
4. Exécution de la synchronisation pour initier la communication.

Résultats

Ces événements se produisent après la synchronisation :

1. IBM Security Identity Manager envoie un message de demande de recherche à Tivoli Directory Integrator, qui recherche les données d'identité dans le magasin de données de l'entreprise.
2. Tivoli Directory Integrator renvoie ces données à IBM Security Identity Manager, qui les traite. Ce traitement inclut l'évaluation de la position dans l'arborescence de l'organisation à laquelle doivent être placés les utilisateurs, l'évaluation de l'appartenance à des rôles, l'évaluation des relations avec un superviseur, l'éventuelle évaluation des règles d'application des accès et l'insertion des données dans le magasin de données de IBM Security Identity Manager. L'évaluation des règles d'attribution des accès peut engendrer des actions de gestion des comptes.
3. Les informations d'identité sont chargées dans IBM Security Identity Manager depuis le magasin de données d'entreprise.

Que faire ensuite

Vous pouvez maintenant ajouter, modifier et supprimer des informations d'identité à l'aide de l'interface IBM Security Identity Manager.

Pour obtenir des scénarios supplémentaires sur l'utilisation de Tivoli Directory Integrator, voir le répertoire `extensions` pour consulter ces descriptions :

- Alimentation d'identité avec JNDI
- Gestion des comptes utilisateur final
- Notification d'événement de compte

Alimentations d'identités qui conservent l'appartenance aux groupes

Vérifier que les alimentations d'identité conservent l'appartenance d'un utilisateur aux groupes par défaut et aux groupes personnalisés.

Tous les groupes IBM Security Identity Manager par défaut n'ont initialement pas de membre, à l'exception du groupe administrateur, qui contient un utilisateur dont le compte est nommé `itim manager`. Lorsque vous chargez les premiers enregistrements d'identités dans IBM Security Identity Manager, certains utilisateurs peuvent devenir membres du groupe de responsables.

Tableau 54. Appartenance à un groupe après l'alimentation d'identités initiale

Nom de groupe	**Appartenance**
Administrateur	Un membre avec un compte nommé `itim manager`
Responsable	Zéro ou plus, selon que l'alimentation d'identités initiale a un enregistrement d'identité qui indique que l'utilisateur a une relation gérée.
Propriétaire du service	Zéro
Assistant du service d'assistance	Zéro

Le premier assistant du service d'assistance et premier propriétaire de service est un utilisateur que l'administrateur ajoute explicitement au groupe. Sinon, un utilisateur obtient automatiquement l'appartenance au groupe de propriétaires de services si vous indiquez l'utilisateur en tant que propriétaire d'un service. Si vous indiquez l'utilisateur en tant que responsable d'un autre utilisateur, un utilisateur obtient automatiquement l'appartenance au groupe de responsables.

Un utilisateur qui est membre d'un groupe personnalisé doit également être membre du groupe par défaut de la même catégorie. Sinon, les résultats du traitement sont imprévisibles.

Si l'enregistrement d'identité entrant d'un utilisateur indique au départ l'appartenance à un groupe personnalisé, IBM Security Identity Manager inclut l'utilisateur en tant que membre du groupe personnalisé et du groupe par défaut de la même catégorie. IBM Security Identity Manager interprète une alimentation d'identités ultérieure incluant le même utilisateur comme une modification de l'utilisateur IBM Security Identity Manager. Si l'alimentation d'identités ultérieure spécifie que l'utilisateur appartient uniquement au groupe personnalisé, et non au groupe par défaut de la même catégorie, l'utilisateur est supprimé de l'appartenance au groupe par défaut. Pour éviter ce problème, assurez-vous que les deux alimentations d'identités, de départ et ultérieure, indiquent que l'utilisateur appartient aux deux groupes, le groupe personnalisé et le groupe par défaut de la même catégorie.

Correspondance des attributs d'inetOrgPerson avec les attributs de Windows Server Active Directory

Les attributs IBM Security Identity Manager `inetOrgPerson` sont associés aux attributs Windows Server Active Directory. Les différences sont signalées par des **caractères gras**.

Tableau 55. Correspondance des attributs `inetOrgPerson` et Windows Server Active Directory `organizationalPerson`

Attributs `inetOrgPerson` d'IBM Security Identity Manager	**Attributs `organizationalPerson` de Windows Server Active Directory**
cn	cn
departmentNumber	**department**
description	**comment**
employeeNumber	**employeeID**
givenName	givenName
homePhone	homePhone
homePostalAddress	homePostalAddress
initials	initials
internationaliSDNNumber	internationallSDNNumber
jpegPhoto	**thumbnailPhoto**
l	l
mail	mail
manager	manager
mobile	mobile
o	o
ou	ou
pager	pager
physicalDeliveryOfficeName	physicalDeliveryOfficeName
postalAddress	postalAddress
postalCode	postalCode
postOfficeBox	postOfficeBox
preferredDeliveryMethod	preferredDeliveryMethod
registeredAddress	registeredAddress
secretary	**assistant**
seeAlso	seeAlso
sn	sn
st	st
street	**streetaddress**
telephoneNumber	telephoneNumber
teletexTerminalIdentifier	teletexTerminalIdentifier
telexNumber	telexNumber
title	title
uid	**< - volontairement vide - >**

Tableau 55. Correspondance des attributs `inetOrgPerson` et Windows Server Active Directory `organizationalPerson` (suite)

Attributs `inetOrgPerson` d'IBM Security Identity Manager	**Attributs `organizationalPerson` de Windows Server Active Directory**
userPassword	userPassword **Remarque :** Le chiffrement par le serveur d'annuaire empêche IBM Security Identity Manager d'utiliser la valeur de cet attribut.
x121Address	x121Address

Mots de passe utilisateur fournis par une alimentation d'identités

Le chiffrement par le serveur d'annuaire empêche IBM Security Identity Manager d'utiliser l'attribut `userPassword` dans le schéma `inetOrgPerson` pour fournir les données du mot de passe utilisateur dans une alimentation d'identité `inetOrgPerson` de LDAP ou une alimentation d'identité Windows Server Active Directory.

D'autres alimentations d'identités qui utilisent les formats CSV, DSML ou IBM Tivoli Directory Integrator peuvent fournir un mot de passe pour un nouvel utilisateur. A partir de la valeur de l'alimentation d'identité, IBM Security Identity Manager utilise l'attribut `erPersonPassword` pour créer un mot de passe pour un compte IBM Security Identity Manager d'un nouvel utilisateur. L'attribut `erPersonPassword` ne peut être utilisé que pour créer un mot de passe pour un nouvel utilisateur IBM Security Identity Manager. Si l'utilisateur existe déjà, la valeur de l'attribut `erPersonPassword` ne peut pas être utilisée pour modifier le mot de passe de connexion de l'utilisateur IBM Security Identity Manager.

Dans une alimentation d'identité où l'attribut `erPersonPassword` n'est pas fourni, IBM Security Identity Manager génère un nouveau mot de passe pour une nouvelle utilisation. L'application envoie le mot de passe généré par message électronique au nouvel utilisateur. Si l'adresse électronique de l'utilisateur n'est pas renseignée, l'utilisateur doit contacter le service d'assistance pour obtenir un mot de passe. En fonction de la configuration de votre site, le mot de passe du nouvel utilisateur peut également être envoyé au responsable hiérarchique de celui-ci.

La valeur du mot de passe fournie par IBM Tivoli Directory Integrator doit être codée au format Base64.

Ces attributs d'alimentation d'identités fournissent une valeur en texte clair qui correspond au mot de passe d'un nouvel utilisateur :

- Nom de colonne CSV : `erPersonPassword`
- Balise DSML : `erPersonPassword`

Attributs inclus dans une alimentation d'identités, mais n'appartenant pas à un schéma

Vous pouvez inclure dans une alimentation d'identité certains attributs qui ne sont pas contenus dans la classe d'objet Alimentation d'identité (`organizationalPerson` pour Windows Server Active Directory, `inetOrgPerson` pour IBM Security Identity Manager).

Par exemple, l'attribut erRoles détermine l'appartenance d'un utilisateur à un groupe IBM Security Identity Manager. L'attribut erRoles ne se trouve ni dans le schéma organizationalPerson, ni dans le schéma inetOrgPerson. En fonction de la valeur de l'attribut erRoles dans une alimentation d'identité initiale, un utilisateur peut devenir membre d'un groupe personnalisé. L'utilisateur peut également devenir membre d'un groupe Assistant du service d'assistance par défaut.

Une alimentation d'identité répétée ne contient pas de valeur pour un attribut précédemment indiqué pour l'utilisateur, pour les deux schémas organizationalPerson et inetOrgPerson. Le processus d'alimentation d'identité supprime cet attribut pour l'utilisateur IBM Security Identity Manager.

Si l'enregistrement d'identité entrant d'un utilisateur indique au départ l'appartenance à un groupe personnalisé, IBM Security Identity Manager inclut l'utilisateur en tant que membre du groupe personnalisé et du groupe par défaut de la même catégorie. IBM Security Identity Manager interprète une alimentation d'identités ultérieure incluant le même utilisateur comme une modification de l'utilisateur IBM Security Identity Manager. Si l'alimentation d'identités ultérieure spécifie que l'utilisateur appartient uniquement au groupe personnalisé, et non au groupe par défaut de la même catégorie, l'utilisateur est supprimé de l'appartenance au groupe par défaut. Pour éviter ce problème, assurez-vous que les deux alimentations d'identités, de départ et ultérieure, indiquent que l'utilisateur appartient aux deux groupes, le groupe personnalisé et le groupe par défaut de la même catégorie.

Pour l'alimentation Windows Server Active Directory, ce problème se produit pour tout attribut inetOrgPerson qui ne se trouve pas également dans le schéma organizationalPerson. Pour une alimentation d'identité inetOrgPerson, le problème se produit pour tout attribut inetOrgPerson qui n'est pas pris en charge par l'alimentation d'identité.

Formats pris en charge et traitement spécial des attributs

IBM Security Identity Manager applique un traitement spécial aux attributs manager et secretary, ainsi qu'à l'attribut erRoles.

Formats pris en charge et traitement spécial des attributs manager et secretary

Les attributs manager et secretary se réfèrent à une autre entrée de personne dans IBM Security Identity Manager.

Remarque : Le service Alimentation d'identités de Windows Server Active Directory mappe l'attribut assistant de Windows Server Active Directory à l'attribut secretary de Tivoli Identity Manager.

En interne, IBM Security Identity Manager utilise un format spécifique pour le nom distinctif (DN) des entrées d'annuaire de personnes, ce qui est peu pratique et difficile à spécifier dans les données de l'alimentation d'identité. Le code de l'alimentation d'identité permet de spécifier ces attributs dans des formats plus utiles. IBM Security Identity Manager prend en charge trois formats pour les valeurs :

- Un filtre de recherche (contenant un opérateur égal (=), mais pas erglobalid) qui est une liste de paires attribut=valeur dont les éléments sont séparés par des virgules.

- Un nom simple (ne contenant pas d'opérateur égale (=)), qui est supposé être la valeur de l'attribut d'appellation pour la classe d'objets d'utilisateur (c'est-à-dire `cn`).
- Un nom distinctif (DN) IBM Security Identity Manager (contenant un opérateur égal (=) et `erglobalid`). L'expression doit correspondre également au nom distinctif LDAP IBM Security Identity Manager d'un des objets de personne actuellement définis.

Dans les deux premiers cas, IBM Security Identity Manager convertit la valeur en un filtre de recherche LDAP. Le processus effectue une recherche par branche afin de trouver une personne correspondant aux critères de recherche. Si la recherche ne donne aucun résultat, ou qu'elle en révèle plusieurs, la valeur est alors considérée comme non valide et, à ce titre, est retirée de la liste. Un message d'avertissement approprié est consigné dans le journal de IBM Security Identity Manager.

Un problème peut éventuellement survenir avec les attributs manager et secretary, s'ils se réfèrent à une personne qui est également définie dans la même alimentation. Dans ce cas, il est possible que, lorsque la valeur de l'attribut est traitée comme indiqué ci-dessus, la personne à laquelle l'attribut se réfère n'ait pas encore été créée. Une telle situation peut se produire, même si la personne Responsable ou Secrétaire a été définie préalablement dans le fichier d'alimentation des identités en raison du traitement multiprocessus et asynchrone effectué par IBM Security Identity Manager lors d'une alimentation d'identités. Elle entraînera la suppression de l'attribut de l'objet Personne car l'attribut fait référence à une personne non valide. Un avertissement est placé dans les fichiers journaux.

Il existe deux solutions à ce problème de dépendance des références. La première consiste à exécuter le service Alimentation d'identités une deuxième fois, après exécution complète de tous les traitements de la première exécution. Cette deuxième alimentation est plus rapide car seules les entrées modifiées feront l'objet d'un traitement complet. L'autre méthode consiste à définir ces personnes (responsables et secrétaires) dans un fichier d'alimentation d'identités séparé. Commencez par exécuter ce fichier d'alimentation d'identités, puis exécutez l'alimentation principale, une fois l'exécution de ce premier fichier terminée. Ce premier fichier peut également contenir des entrées faisant référence à des responsable définis dans le même fichier d'alimentation. Il peut être nécessaire d'exécuter deux fois le premier fichier d'alimentation ou de fractionner à nouveau le fichier.

Les activités de flux de travaux asynchrones permettant de créer ou de modifier des personnes peuvent toujours être en cours d'exécution, même si le statut d'alimentation d'identité apparaît comme terminé. Dans ce cas, vous devez attendre un peu après que la première alimentation semble terminée, avant de soumettre la deuxième alimentation.

Formats pris en charge et traitement spécial des valeurs de l'attribut erRoles

L'attribut `erRoles` est utilisé pour indiquer la liste des rôles auxquels un utilisateur appartient. Dans IBM Security Identity Manager, les groupes équivalent aux rôles fournis par IBM Security Identity Manager dans sa version Enterprise. IBM Security Identity Manager utilise l'attribut `erRoles` pour indiquer les groupes auxquels un utilisateur appartient. Par exemple, si vous indiquez un attribut d'alimentation d'identité `erRoles` avec la valeur `Assistant du service`

d'assistance, l'utilisateur appartiendra au groupe Assistants du service d'assistance. L'attribut erRoles peut être à plusieurs valeurs.

Les formats suivants sont pris en charge :

- Un nom simple (ne contenant pas d'opérateur égale (=)), qui est supposé être la valeur de l'attribut erRoleName. IBM Security Identity Manager effectue une recherche par branche pour trouver un rôle statique unique correspondant à la recherche. Le nom n'est pas valide, si la recherche ne donne aucun résultat, ou qu'elle fait remonter plusieurs rôles.
- Un nom distinctif (DN) IBM Security Identity Manager complet qui doit correspondre exactement au nom distinctif LDAP IBM Security Identity Manager de l'un des rôles statiques actuellement définis.

Toute valeur non valide est supprimée de la liste des valeurs. S'il ne reste aucune valeur, l'attribut est supprimé de la liste des attributs. Un message d'avertissement approprié est consigné dans le journal.

Attributs et classes modifiables des schémas

Vous pouvez modifier certains attributs et classes de schéma IBM Security Identity Manager.

Vous pouvez créer de nouvelles classes avec des noms commençant par les caractères er, préfixe qui était précédemment réservé aux attributs et classes de schémas IBM Security Identity Manager.

Les attributs et classes de schémas IBM Security Identity Manager que vous pouvez modifier ont un préfixe d'ID objet (OID) unique. Un OID est une chaîne de nombres qui identifie une classe unique dans un schéma LDAP. Les attributs et classes de schémas IBM Security Identity Manager qui restent en lecture seule ont le préfixe OID suivant :

1.3.6.1.4.1.6054.1.**1**

Attribution d'un nom à un utilisateur et positionnement d'une organisation

Lorsque le serveur IBM Security Identity Manager importe des données de ressources humaines, le serveur crée un nom distinctif pour chaque enregistrement d'identité. Il place l'utilisateur dans une unité organisationnelle spécifique en fonction des informations fournies.

Pour identifier de manière unique et placer chaque individu, les données de chaque entrée (ou utilisateur) doivent être organisées de sorte que le serveur IBM Security Identity Manager puisse en reconnaître les différents éléments (attributs). Le serveur IBM Security Identity Manager doit également être configuré pour reconnaître les attributs transmis. La reconnaissance est effectué en comparant l'attribut objectclass aux profils d'utilisateurs définis. Par défaut, il s'agit de la classe d'objet LDAP standard inetOrgPerson.

Détermination du positionnement d'un utilisateur

Le serveur IBM Security Identity Manager détermine le placement dans l'organigramme. Le serveur utilise une règle de positionnement définie dans le service d'alimentation d'identité DSML.

Une personne peut être définie en tant que membre du département Marketing dans la source d'identité. La règle de positionnement indique au serveur de placer l'utilisateur dans le service marketing de l'organigramme IBM Security Identity Manager. Cette règle est utilisée pour le positionnement initial des utilisateurs lors d'une opération d'ajout et pour le déplacement d'un utilisateur vers un autre site lors d'une opération de modification.

Remarque : Les noms d'organisation renvoyés par les règles de positionnement doivent être uniques dans le contexte du service si aucun chemin d'organisation n'est utilisé pour définir un conteneur d'organisation. Si la règle de placement fournit un chemin d'organisation, le nom d'organisation doit être unique dans le conteneur d'organisation.

Les règles de positionnement sont rédigées à l'aide de code JavaScript, qui renvoie le chemin de l'organisation dans un format de nom distinctif. Cette information est utilisée pour rechercher une unité organisationnelle afin d'y positionner un utilisateur. Ce nom distinctif indique le chemin d'organisation requis par rapport à la base de l'organisation. La syntaxe de ce chemin peut être représentée à l'aide de la pseudo notation BNF suivante :

```
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= prefix '=' name
prefix ::= 'l' | 'o' | 'ou'
name ::= string
```

où `chaîne` représente la valeur textuelle, `l` le site, `o` l'organisation et `ou` l'unité organisationnelle, l'organisation partenaire ou le domaine d'administration.

Remarque : Les préfixes indiqués ici correspondent aux valeurs par défaut. Si le client utilise un autre schéma, ces préfixes correspondent aux valeurs mappées dans la configuration de l'entité.

Exemple

Pour illustrer ce cas, examinez l'organigramme suivant :

```
IBM (organisation)
   Marketing (organizational unit)
   Facilities (organizational unit)
      Irvine (location)
```

Le chemin du service Marketing est `ou=Marketing, o=IBM`. Le chemin du service Irvine Facilities est `l=Irvine, ou=Facilities, o=IBM`.

La fonction JavaScript renvoie une chaîne dans ce format, mais omet l'organisation. Les attributs de l'enregistrement d'identité provenant de la source des identités peuvent être extraits du code JavaScript pour créer le chemin. Grâce à la souplesse de programmation offerte par le code JavaScript, les informations de la source des identités peuvent être utilisées de différentes manières. Les éléments de programmation tels que les instructions switch peuvent être utilisés pour mapper des noms d'organisation spécifiques sur divers chemins du serveur. La manipulation des chaînes peut également être utilisée pour segmenter ou concaténer les noms afin d'en dériver les chemins. Ainsi, la chaîne `IBM/Facilities/Irvine` peut par exemple être segmentée et reconstruite au format de nom distinctif suivant : `l=Irvine, ou=Facilities, o=IBM`.

L'exemple suivant illustre une utilisation de cette fonctionnalité de script. La source d'identité de l'organisation Acme utilise les attributs `div` pour division, `bu` pour unité commerciale et `dept` pour service. La disposition logique de l'organisation est la suivante :

```
organization
   division
      business-unit
         department
```

Dans le serveur IBM Security Identity Manager, cette structure est mappée aux organisations et aux unités organisationnelles et apparaît comme cet exemple :

```
organization
   organizational unit (division)
      organizational unit (business-unit)
         organizational unit (department)
```

Le code JavaScript suivant peut être utilisé pour que la règle de positionnement effectue cette conversion :

```
return "ou=" + entry.dept[o] + ",ou=" + entry.bu[o]  + ",ou=" + entry.dw[o];
```

Remarque : On suppose que toutes les identités dans cette source se trouvent dans l'organisation Acme.

Pour une entreprise qui utilise un attribut `ou` à plusieurs valeurs, la règle de positionnement pourrait être :

```
var ou =entry.ou;
var filt = '';
for (i = 0, i < ou.length, ++i)
{
  if (i==0)
      filt = ''ou='' + ou[i];
  }
else
     {
filt = filt + '',ou='' + ou[i];
     }
}
return filt;
```

Le serveur IBM Security Identity Manager évalue ce script lors de l'ajout d'une personne pour placer cette dernière dans l'organisation. Lors d'une demande de modification, ce script est évalué. Si la valeur est différente du positionnement actuel de l'utilisateur, ce dernier est déplacé vers le nouveau site, en fonction du chemin renvoyé.

Création d'un service d'alimentation d'identité

Créer une instance de service pour un type d'identité, tel que CSV ou DSML.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Avant de pouvoir créer un service dans IBM Security Identity Manager, vous devez créer un type de service. Vous pouvez également utiliser un des types de service

automatiquement créés lors de l'installation du serveur IBM Security Identity Manager. Vous pouvez créer un type de service en installant le profil d'adaptateur. Vous pouvez également ajouter dans votre répertoire LDAP de nouveaux attributs et des classes de schéma pour le service. Pour que vous puissiez créer un service pour un adaptateur, l'adaptateur doit d'abord être installé et le profil d'adaptateur doit être créé.

Pourquoi et quand exécuter cette tâche

Le nom de service et la description que vous fournissez pour chaque service sont affichés sur la console. Il est donc important de fournir des valeurs qui aient un sens pour vos utilisateurs et vos administrateurs.

Pour créer une instance du service d'alimentation d'identité, exécutez les étapes suivantes :

Procédure

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, cliquez sur **Créer**. L'assistant Créer un service s'affiche.
3. Dans la page Sélectionner le type de service, sélectionnez un type de service d'alimentation d'identité, puis cliquez sur **Suivant**.

   Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

   - Cliquez sur la flèche pour accéder à la page suivante.
   - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.
4. Dans la page Informations sur le service, indiquez les valeurs appropriées pour l'instance de service.
5. Cliquez sur **Tester la connexion** pour vérifier que les données des zones sont correctes, puis cliquez sur **Terminer**.

Résultats

Pour l'alimentation d'identité inetOrgPerson, un message de succès du test de connexion confirme que toutes les zones obligatoires sont remplies et que la cible indiquée peut être atteinte. Cela ne garantit pas que la synchronisation de la ressource LDAP réussisse ou produise les résultats souhaités.

Un message indique que vous avez correctement créé l'instance du service pour le type de service d'alimentation d'identité concerné.

Que faire ensuite

Planifiez une synchronisation ou exécutez une synchronisation immédiatement à l'aide de la liste de tâches associée au service.

Lorsque la page Sélectionner un service s'affiche, cliquez sur **Régénérer** pour régénérer la table **Services** et afficher la nouvelle instance du service.

Application d'une synchronisation immédiate à un service d'alimentation d'identité

Lancez une activité de synchronisation immédiatement dans un service d'alimentation d'identité. Pendant une synchronisation, le serveur IBM Security Identity Manager demande les informations de l'enregistrement d'identité au fichier indiqué.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Installez un service d'alimentation d'identité adapté.

Procédure

Pour exécuter une synchronisation maintenant, appliquez les étapes suivantes :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.
3. Dans le tableau **Services**, cliquez sur l'icône (▸) à côté du service d'alimentation d'identité puis cliquez sur **Synchroniser maintenant**.

Résultats

Un message indique que vous avez soumis avec succès une demande de synchronisation en vue d'une exécution immédiate.

Que faire ensuite

Pour visualiser les résultats de la synchronisation, cliquez sur **Visualiser ma demande** ou cliquez sur **Fermer**.

Création d'une synchronisation planifiée pour un service d'alimentation d'identité

Planifier une synchronisation pour qu'elle s'exécute à un intervalle donné. Pendant une synchronisation, le serveur IBM Security Identity Manager demande les informations de l'enregistrement d'identité au fichier indiqué.

Avant de commencer

Selon la façon dont votre administrateur système a personnalisé votre système, il est possible que vous n'ayez pas accès à cette tâche. Pour avoir accès à cette tâche, ou pour que quelqu'un d'autre l'effectue pour vous, contactez votre administrateur système.

Installez un service d'alimentation d'identité adapté.

Procédure

Pour créer une planification de synchronisation pour un service d'alimentation d'identité, exécutez les étapes suivantes :

1. Dans l'arborescence de navigation, cliquez sur **Gérer les services**. La page Sélectionner un service s'affiche.
2. Dans la page Sélectionner un service, exécutez les étapes suivantes :
   a. Entrez des informations sur le service dans la zone **Rechercher des informations**.
   b. Dans la zone **Rechercher par**, indiquez si la recherche doit être effectuée sur des services ou des unités commerciales.
   c. Sélectionnez un type de service dans la liste **Type de recherche**.
   d. Sélectionnez un statut dans la liste **Statut** puis cliquez sur **Rechercher**. Une liste des services qui correspondent aux critères de recherche s'affiche.

      Si la table est composée de plusieurs pages, vous pouvez effectuer les actions suivantes :

      - Cliquez sur la flèche pour accéder à la page suivante.
      - Saisissez le numéro de la page que vous voulez afficher, puis cliquez sur **Atteindre**.
3. Dans le tableau **Services**, cliquez sur l'icône (▸) à côté du service d'alimentation d'identité, puis cliquez sur **Configurer la synchronisation**. La page Gestion des planifications s'affiche.
4. Dans la page Gestion des planifications, exécutez les étapes suivantes :
   a. Indiquez si une règle d'administration évalue les comptes renvoyés par la synchronisation.
   b. Cliquez sur **Créer**. Le bloc-notes Configurer la synchronisation de compte s'affiche.
5. Dans la page Général, entrez des informations sur la planification de synchronisation.
6. Dans la page Planification, sélectionnez un intervalle de planification pour la synchronisation. Les zones affichées dépendent de l'option de planification que vous sélectionnez.

7. Facultatif : Dans la page Requête, indiquez un filtre de recherche LDAP pour les attributs de compte à inclure dans une requête. Sélectionnez cette option si vous souhaitez effectuer une synchronisation des "données de support uniquement".
8. Cliquez sur **OK** pour enregistrer la nouvelle planification et fermer la page.

Résultats

Un message s'affiche indiquant que vous avez créé une planification de synchronisation.

Que faire ensuite

Sélectionnez une autre tâche de services ou cliquez sur **Fermer**. Lorsque la page Sélectionner un service s'affiche, cliquez sur **Régénérer** pour régénérer le tableau **Services**.

Chapitre 18. Utilitaires de IBM Security Identity Manager

IBM Security Identity Manager fournit des utilitaires pour configurer le schéma de base de données, LDAP et les propriétés système couramment utilisées.

Outil de configuration système (runConfig)

Pour configurer les propriétés système fréquemment utilisées, vous pouvez utiliser l'outil outil de configuration système (runConfig) afin de changer les fichiers de propriétés contenant les paramètres système IBM Security Identity Manager. Vous pouvez également modifier les paramètres WebSphere Application Server pour IBM Security Identity Manager.

Par exemple, lorsque vous modifiez l'ordinateur qui fournit le serveur de messagerie à votre site, l'adresse IP du serveur de messagerie peut changer. Utilisez alors l'outil de configuration système pour spécifier la nouvelle adresse du serveur de messagerie.

Pour plus d'informations sur cet utilitaire, voir le document *IBM Security Identity Manager - Guide d'installation et de configuration*.

Commande runConfig

La commande runConfig lance l'outil de configuration système fourni par IBM Security Identity Manager.

Description de la commande

Pour démarrer manuellement l'outil de configuration système, exécutez cette commande :

ITIM_HOME/bin/**runConfig**

Si les ID utilisateur ou les mots de passe associés aux utilisateurs EJB ou aux utilisateurs système sont modifiés dans le système d'exploitation, utilisez un argument `install` supplémentaire pour forcer la mise à jour dans WebSphere Application Server. Si ces ID ou mots de passe utilisateur sont modifiés, exécutez la commande suivante :

ITIM_HOME/bin/**runConfig install**

Si vous avez des problèmes avec l'outil de configuration système, examinez le fichier journal *ITIM_HOME*/install_logs/runConfig.stdout pour de plus amples informations. La configuration du système nécessite quelques minutes et dure plus longtemps si l'argument `install` est utilisé.

Outil de configuration de la base de données (DBConfig)

Pour configurer la base de données IBM Security Identity Manager, vous pouvez utiliser l'outil de configuration DBConfig.

L'outil de configuration de la base de données crée le schéma de base de données et les données par défaut dont IBM Security Identity Manager a besoin. Utilisez cet

utilitaire *uniquement* si la commande n'a pas pu configurer la base de données lors de l'installation. Si les tables de base de données IBM Security Identity Manager ont été précédemment configurées, l'exécution de la commande DBConfig affiche une invite. L'utilisateur peut alors choisir de supprimer toutes les tables IBM Security Identity Manager existantes ou de quitter sans configurer la base de données.

Voir *IBM Security Identity Manager - Guide d'installation et de configuration*.

Commande DBConfig

La commande DBConfig lance l'outil de configuration de base de données fourni par IBM Security Identity Manager.

Description de la commande

Pour démarrer manuellement l'outil de configuration de base de données, exécutez la commande suivante :

ITIM_HOME/bin/**DBConfig**

Après avoir modifié la valeur d'une zone, cliquez sur **Test** pour vérifier que la connexion à la base de données est active. Lorsque le test de la base de données a réussi, le bouton **Test** se transforme en **Continuer**. Après avoir cliqué sur **Continuer**, patientez quelques minutes jusqu'à ce que la configuration de la base de données soit terminée.

Si vous avez des problèmes avec l'outil de configuration de la base de données, consultez le fichier journal *ITIM_HOME*/install_logs/dbConfig.stdout pour de plus amples informations.

Outil de configuration du serveur d'annuaire (ldapConfig)

Pour configurer le serveur d'annuaire pour IBM Security Identity Manager, vous pouvez utiliser l'outil de configuration du serveur d'annuaire (ldapConfig).

N'exécutez pas l'outil de configuration du serveur d'annuaire, à moins que la configuration LDAP n'échoue durant le processus d'installation de ldapConfig. L'outil de configuration du serveur d'annuaire crée le schéma LDAP et les données par défaut pour IBM Security Identity Manager. L'exécution de l'outil de configuration du serveur d'annuaire après la configuration du serveur d'annuaire restaurera les valeurs par défaut utilisées par IBM Security Identity Manager. Si vous avez modifié la valeur de l'un de ces attributs IBM Security Identity Manager, la valeur est remplacée par la valeur par défaut. Par exemple, ldapConfig réinitialise le mot de passe pour l'ID utilisateur nommé itim manager et lui attribue à nouveau le mot de passe par défaut "secret".

Voir *IBM Security Identity Manager - Guide d'installation et de configuration*.

Commande ldapConfig

La commande ldapConfig lance l'outil de configuration du serveur d'annuaire fourni par IBM Security Identity Manager.

Description de la commande

Pour démarrer manuellement l'outil de configuration de serveur d'annuaire, exécutez la commande suivante :

ITIM_HOME/bin/**ldapConfig**

Cliquez sur **Test** pour vérifier que la connexion au serveur d'annuaire peut être établie. Une fois que le test de connexion au serveur d'annuaire a abouti, les zones de la section Identity Manager - Informations sur l'annuaire sont activées.

Si vous avez des problèmes avec l'outil de configuration du serveur d'annuaire, examinez le fichier journal *ITIM_HOME*/install_logs/ldapConfig.stdout pour de plus amples informations. La configuration du serveur d'annuaire prend quelques minutes.

SAConfig : utilitaire de module d'accès partagé

SAConfig permet de configurer manuellement le module d'accès partagé.

Lancez l'utilitaire à partir du répertoire dans lequel IBM Security Identity Manager est installé.

Tableau 56. Exécution de SAConfig

Système d'exploitation	Commande
Windows	Dans C:\Program Files\IBM\isim\bin, cliquez sur SAConfig ou ouvrez une fenêtre de commande et entrez **SAConfig**.
UNIX ou Linux	Dans /opt/IBM/isim/bin, entrez **./SAConfig**.

Chapitre 19. Intégration IBM Security Identity Manager pour IBM SmartCloud Control Desk

Cette section présente l'intégration IBM Security Identity Manager pour IBM SmartCloud Control Desk et apporte des instructions pour l'installation et la configuration de ce module.

Introduction à l'intégration IBM Security Identity Manager pour IBM SmartCloud Control Desk

L'intégration IBM Security Identity Manager pour IBM SmartCloud Control Desk permet les communications entre IBM Security Identity Manager et IBM SmartCloud Control Desk.

Les sections ci-après décrivent brièvement IBM SmartCloud Control Desk et son intégration avec IBM Security Identity Manager.

IBM SmartCloud Control Desk

IBM SmartCloud Control Desk est un système de gestion informatisée des actifs qui permet aux entreprises de gérer, de réparer et de prendre en charge le fonctionnement de leurs actifs générateurs de revenus, que ce soit d'un point de vue de gestion pure des actifs ou d'un point de vue de gestion informatisée des actifs. IBM SmartCloud Control Desk stocke et gère des données sur les actifs, les fonctions et l'inventaire. Vous pouvez utiliser IBM SmartCloud Control Desk pour planifier des tâches de maintenance, suivre l'état des actifs, gérer les inventaires et les ressources, répondre aux demandes de support, gérer les achats ou encore analyser les coûts.

Le logiciel IBM SmartCloud Control Desk est composé de modules, chacun de ces modules étant constitué d'un groupe d'applications associées qui vous aide à gérer une fonction donnée dans votre entreprise. Par exemple, le module Purchasing inclut les applications suivantes :

- L'application *Invoices* permet d'enregistrer les factures et de les faire correspondre aux bons de commande et aux reçus.
- L'application *Purchase Orders* permet d'enregistrer les achats de biens ou de services.
- L'application *Receiving* permet d'enregistrer des biens dans l'inventaire ou d'enregistrer la réception de services.
- Plusieurs autres applications associées aux achats.

Le module Service Desk inclut des applications permettant de gérer les demandes d'aide, d'informations et de services des clients. Le principal utilisateur du module Service Desk est un *agent*, qui se sert du logiciel pour enregistrer les demandes des clients internes ou externes et suit certaines procédures pour résoudre le problème. La résolution d'un problème nécessite souvent le suivi d'un enchaînement d'activités dans lesquelles différentes personnes interviennent. N'importe qui peut enregistrer la solution dans une base de connaissances (KnowledgeBase), depuis laquelle la solution peut être retrouvée et appliquée à des problèmes similaires.

Les applications de centre de services les plus directement associées à l'intégration IBM Security Identity Manager sont les applications *ticket* :

- L'application *Service Requests* permet de créer des enregistrements d'appels ou de messages provenant de clients qui demandent des services.
- L'application *Incidents* permet de créer des enregistrements d'incidents qui ont résulté dans l'interruption ou la réduction de la qualité d'un service.
- L'application *Problems* permet de créer des enregistrements des problèmes sous-jacents à l'origine d'incidents et de demandes de service.

Les enregistrements de type Service Request, Incident et Problem sont appelés *enregistrements de tickets* ou *types de tickets*. Les enregistrements de tickets sont créés par un agent de centre de services ou en utilisant automatiquement les données issues d'e-mails, d'outils de surveillance système ou de logiciels externes tels que IBM Security Identity Manager. Une fois qu'un ticket a été enregistré, une personne ou un groupe en prend possession et suit le problème jusqu'à sa résolution. L'intégration IBM Security Identity Manager pour IBM SmartCloud Control Desk peut créer des tickets de type Demande de service pour toutes les opérations changePassword qui se produisent. La demande de service ainsi créée reçoit l'état **Fermé** ou **Nouveau**, selon que l'opération changePassword a réussi ou non dans IBM Security Identity Manager.

Intégration entre IBM Security Identity Manager et IBM SmartCloud Control Desk

L'intégration permet la gestion des utilisateurs IBM SmartCloud Control Desk via IBM Security Identity Manager.

La gestion des utilisateurs IBM SmartCloud Control Desk est prise en charge lorsque le registre natif IBM SmartCloud Control Desk est utilisé en tant que référentiel utilisateur principal. Si la sécurité du serveur d'applications est activée, les utilisateurs IBM SmartCloud Control Desk sont gérés via LDAP et le fournisseur de services ne peut pas être utilisé pour gérer les utilisateurs. L'intégration permet également de créer des demandes de service IBM SmartCloud Control Desk lorsque des mots de passe sont modifiés via IBM Security Identity Manager. Cette fonctionnalité est particulièrement utile lorsqu'il faut pouvoir automatiser les demandes de modification des mots de passe. La plupart du temps, les demandes de service IBM SmartCloud Control Desk couvrent des demandes de modification des mots de passe. L'automatisation des tâches de modification des mots de passe, en permettant aux utilisateurs de les modifier eux-mêmes en temps réel, permet d'éviter des pertes de temps. La création de demandes de service est possible, que la sécurité du serveur d'applications soit utilisée ou non. Si la sécurité du serveur d'applications est utilisée, l'authentification est requise pour créer des tickets de demandes de service. L'intégration entre IBM Security Identity Manager et IBM SmartCloud Control Desk permet plus de flexibilité entre les deux produits et accélère le processus de gestion des utilisateurs dans IBM SmartCloud Control Desk.

Logiciels prérequis

Cette section décrit les logiciels prérequis pour l'intégration d'IBM Security Identity Manager pour IBM SmartCloud Control Desk.

Avant d'installer l'intégration de IBM Security Identity Manager pour IBM SmartCloud Control Desk, les produits suivants doivent être installés et en cours d'exécution sur l'un des systèmes d'exploitation spécifiés :

- IBM Security Identity Manager Version 6.0 on Windows, AIX, HP-UX, or Solaris
- IBM SmartCloud Control Desk Version 7.5 on Windows, AIX, Linux
- Machine d'administration IBM Maximo avec services de base sur Windows

Le produit IBM SmartCloud Control Desk doit être pris en charge par un serveur d'applications Web et par un serveur de base de données. Voir la page IBM SmartCloud Control Desk Wiki pour obtenir une liste des logiciels pris en charge.

Composants de l'intégration IBM Security Identity Manager pour IBM SmartCloud Control Desk

Cette section décrit les composants requis pour intégrer IBM Security Identity Manager et IBM SmartCloud Control Desk et les chemins de communication entre eux.

Les composants de l'intégration IBM Security Identity Manager pour la solution IBM SmartCloud Control Desk sont les suivants : Maximo Enterprise Adapter (MEA), serveur Maximo Application Server et un serveur IBM Security Identity Manager. Le serveur IBM Security Identity Manager envoie des demandes au serveur Maximo Application Server. Le serveur Maximo Application Server envoie les réponses à IBM Security Identity Manager.

Organigramme de l'installation

Cette section présente les tâches requises pour configurer la communication entre IBM Security Identity Manager et IBM SmartCloud Control Desk.

Une fois que vous avez installé les logiciels prérequis, exécutez les tâches répertoriées dans le tableau 57 pour configurer l'intégration de IBM Security Identity Manager avec IBM SmartCloud Control Desk. Le tableau 57 décrit le rôle de chaque composant de l'installation.

Tableau 57. Tâches d'installation et de configuration

Etape	Tâche	Description
1	Demandez le module d'installation. Pour plus d'informations, voir «Obtention du module d'installation», à la page 264.	L'intégration de IBM Security Identity Manager pour le module d'installation IBM SmartCloud Control Desk contient tous les fichiers nécessaires pour installer ou configurer les principaux composants requis pour l'intégration.

Tableau 57. Tâches d'installation et de configuration (suite)

Etape	Tâche	Description
2	Configurer le serveur d'applications IBM SmartCloud Control Desk. Pour plus d'informations, voir «Configuration d'IBM SmartCloud Control Desk», à la page 265	Installez et activez l'interface du serveur d'applications IBM SmartCloud Control Desk qui permet les communications entre IBM SmartCloud Control Desk et IBM Security Identity Manager. Dans cette étape, vous déployez également un nouveau fichier `maximo.ear` sur votre serveur d'applications IBM SmartCloud Control Desk pour prendre en charge l'intégration entre IBM Security Identity Manager et IBM SmartCloud Control Desk.
3	Configurez IBM Security Identity Manager. Pour plus d'informations, voir «Configuration d'IBM Security Identity Manager», à la page 270	Configurez IBM Security Identity Manager pour utiliser la nouvelle extension de flux de travaux changePassword et activer le nouveau fournisseur de services IBM SmartCloud Control Desk.

Obtention du module d'installation

Cette section décrit le contenu de l'intégration IBM Security Identity Manager pour le module d'installation IBM SmartCloud Control Desk.

1. Procurez-vous l'intégration IBM Security Identity Manager pour le module d'installation IBM SmartCloud Control Desk.
2. Téléchargez le fichier `tim_sd_integration.zip` dans votre machine Maximo Administration Machine sur laquelle les services de base sont installés. Ce fichier se trouve dans ces répertoires.
   - Systèmes d'exploitation UNIX et Linux

     ITIM_HOME`/extensions/6.0/maximo`
   - Systèmes d'exploitation Windows

     `C:\Program Files\IBM\itim60\extensions\6.0\maximo`
3. Extrayez le fichier dans le répertoire d'installation des services de base Maximo.

   Exemples : `C:\IBM\Maximo`; `C:\IBM\SMP\Maximo`

Le tableau 58 répertorie le sous-répertoire et les fichiers présents dans votre répertoire d'installation des services de base Maximo une fois le module d'installation extrait. `Maximo_Install` fait référence au répertoire d'installation des services de base Maximo.

Tableau 58. Intégration de IBM Security Identity Manager pour le module d'installation IBM SmartCloud Control Desk

Répertoire de niveau supérieur	Fichiers	Description

`Installation_Maximo\tim_51`	`maximo.jar`
	
	`maximoserviceprofile.jar`
		Les fichiers du sous-répertoire `tim_51` permettent de configurer IBM Security Identity Manager Version pour la prise en charge de l'intégration à IBM SmartCloud Control Desk.

Configuration d'IBM SmartCloud Control Desk

Dans les sections suivantes, `Installation_Maximo` fait référence au répertoire d'installation des services de base Maximo.

Tableau 59. Etapes de configuration de IBM SmartCloud Control Desk

Etape	Tâche	Description
1	Téléchargez et développez l'intégration IBM Security Identity Manager, comme décrit dans «Obtention du module d'installation», à la page 264.	Une fois le package développé, le sous-répertoire `Installation_Maximo\tim_51` contient les fichiers `maximo.jar` et `maximoserviceprofile.jar`, qui font partie de l'intégration IBM Security Identity Manager.
2	Vérifiez que votre fichier `maximo.properties` est bien configuré et qu'il pointe vers le bon serveur de base de données.	Le fichier `maximo.properties` se trouve dans le dossier suivant : `Maximo_Install\applications\maximo\properties`. Vérifiez que la chaîne de connexion JDBC spécifie le bon emplacement pour le serveur de base de données qui prend en charge l'installation IBM SmartCloud Control Desk.
3	Configurez Maximo Enterprise Adapter. Suivez les instructions de la section «Configuration de Maximo Enterprise Adapter».	Maximo Enterprise Adapter constitue le canevas d'intégration des applications externes avec Maximo. Lorsque vous configurez Maximo Enterprise Adapter, vous installez et vous activez les interfaces Maximo requises pour établir des communications entre IBM SmartCloud Control Desk et IBM Security Identity Manager.
4	Régénérez et déployez le fichier `maximo.ear` sur WebSphere. Suivez les instructions de la section «Configuration de WebSphere», à la page 266.	Lorsque vous installez IBM SmartCloud Control Desk, un fichier `maximo.ear` est généré et installé sur le serveur IBM SmartCloud Control Desk, avant d'être déployé sur WebSphere, qui prend en charge votre installation IBM SmartCloud Control Desk. (Le serveur d'applications Web peut résider sur le même ordinateur hôte que les services de base Maximo ou sur un autre.) Pour que l'intégration IBM Security Identity Manager avec IBM SmartCloud Control Desk fonctionne, vous devez régénérer le fichier `maximo.ear` sur le serveur Maximo. A l'issue de la régénération, `maximo.ear` doit être redéployé sur WebSphere.

Configuration de Maximo Enterprise Adapter

Cette section décrit comment configurer Maximo Enterprise Adapter afin de prendre en charge IBM Security Identity Manager.

La procédure de configuration de Maximo Enterprise Adapter comporte deux parties :

1. L'exécution du script `updatedb.bat` fourni avec les services de base Maximo. Ce script installe automatiquement les interfaces d'intégration Maximo requises pour la communication entre le serveur d'applications IBM SmartCloud Control Desk et IBM Tivoli Directory Integrator Server.

2. L'exécution de la configuration de Maximo Enterprise Adapter via l'activation des interfaces d'intégration depuis le module d'intégration de IBM SmartCloud Control Desk.

Exécution d'updatedb.bat

Exécutez la procédure suivante pour vous procurer et exécuter le script `updatedb.bat`.

Avant de commencer

Dans ces instructions, `Installation_Maximo` fait référence au répertoire d'installation des services de base Maximo.

Pourquoi et quand exécuter cette tâche

Pour vous procurer et exécuter le script `updatedb.bat` :

Procédure

1. Connectez-vous à la console d'administration WebSphere Application Server.
2. Cliquez sur **Serveurs > Types de serveur > Serveurs WebSphere Application Server**.
3. Sélectionnez **MXServer** et cliquez sur **Arrêter**.
4. Une fois le serveur arrêté, ouvrez une invite de commande.
5. Accédez au répertoire `Maximo_Install\tools\maximo`.
6. Exécutez le script `updatedb.bat`.
7. Revenez à la console d'administration .
8. Sélectionnez **MXServer** et cliquez sur **Démarrer**.

Résultats

Le script `updatedb.bat` appelle le script de mise à jour IBM Security Identity Manager pour IBM SmartCloud Control Desk, qui crée les structures d'objets requises pour l'intégration.

Configuration de WebSphere

Cette section décrit comment configurer WebSphere. Dans ces instructions, `Installation_Maximo` fait référence au répertoire d'installation des services de base Maximo.

Pour que l'intégration IBM Security Identity Manager fonctionne, une classe fournie avec l'intégration IBM Security Identity Manager doit être intégrée au fichier `maximo.ear`.

Si votre installation IBM SmartCloud Control Desk est prise en charge par WebSphere Application Server, terminez la procédure suivante pour intégrer `MaxUserProcess.class` dans `maximo.ear` sur la machine d'administration IBM SmartCloud Control Desk, puis déployez le fichier `maximo.ear` sur votre WebSphere Application Server.

Remarque : Lorsque le fichier `tim_sd_integration.zip` est extrait dans le répertoire `Maximo_Install`, `MaxUserProcess.class` est automatiquement ajouté au bon répertoire. Aucune autre configuration n'est nécessaire pour cette classe.

Activation de la suppression d'utilisateurs IBM SmartCloud Control Desk (facultatif)

IBM SmartCloud Control Desk ne permet pas la suppression d'utilisateurs lorsque la variable *LOGINTRACKING* est activée.

Si vous supprimez des utilisateurs IBM SmartCloud Control Desk, désactivez la variable *LOGINTRACKING*. Pour ce faire, procédez comme suit :

1. Connectez-vous au serveur IBM SmartCloud Control Desk avec des droits administrateur.
2. Cliquez sur **Accéder à** → **Sécurité** → **Utilisateurs**.
3. Dans le menu **Action**, sélectionnez **Contrôles de sécurité**.
4. Désélectionnez la case à cocher **Activer le suivi de connexion ?**.

Remarque : Si l'élément *LOGINTRACKING* n'est pas sélectionné, cochez la case **Activer la suppression d'utilisateurs Maximo ?** dans le formulaire de services IBM SmartCloud Control Desk. Cette case IBM Security Identity Manager doit être cochée pour pouvoir supprimer des utilisateurs IBM SmartCloud Control Desk. Pour plus d'informations sur la configuration d'un service IBM SmartCloud Control Desk, voir «Configuration d'IBM Security Identity Manager», à la page 270.

Ajout d'un mot de passe avec lien à IBM SmartCloud Control Desk (facultatif)

IBM Security Identity Manager gère les utilisateurs IBM SmartCloud Control Desk en cas d'utilisation du registre natif ou de LDAP pour stocker les informations utilisateur. LDAP permet de stocker les informations utilisateur quand la sécurité du serveur d'applications J2EE est activée. Lorsque le registre natif IBM SmartCloud Control Desk est utilisé, le fournisseur de services IBM SmartCloud Control Desk est utilisé pour gérer les utilisateurs. Toutefois, quand LDAP est utilisé, seul l'adaptateur LDAP est utilisé pour gérer les utilisateurs IBM SmartCloud Control Desk via IBM Security Identity Manager.

Le lien **Vous ne vous souvenez plus de votre mot de passe ?** n'est pas activé lorsque la sécurité du serveur d'applications J2EE est activée. C'est par contre le cas lorsque le registre natif est utilisé. En faisant en sorte que ce lien mène vers l'interface utilisateur IBM Security Identity Manager en libre-service, le mot de passe peut être redéfini lorsque LDAP ou le registre natif est utilisé pour stocker les utilisateurs IBM SmartCloud Control Desk, à condition qu'un service soit configuré pour gérer le serveur IBM SmartCloud Control Desk.

L'interface IBM SmartCloud Control Desk peut également être modifiée afin que le lien **Vous ne vous souvenez plus de votre mot de passe ?** désigne l'interface IBM Security Identity Manager en libre-service. Cette action permet aux utilisateurs IBM SmartCloud Control Desk de gérer leurs mots de passe via IBM Security Identity Manager. Ils peuvent également redéfinir le mot de passe IBM SmartCloud Control Desk s'ils l'ont oublié et ne peuvent plus se connecter.

Pour ajouter le lien à la page de connexion IBM SmartCloud Control Desk, procédez comme suit :

1. Sélectionnez le répertoire `Maximo_Install\applications\maximo\maximouiweb\webmodule\webclient\login`.
2. Modifiez le fichier `login.jsp`.

a. Rechercher la ligne suivante dans le fichier `login.jsp` : `<button id="forgotpwdlink" class="link" type="submit"><span>< %=labels.forgotPassword%></span></button>`
b. Mettez en commentaire la ligne en procédant comme suit : `<!--button id="forgotpwdlink" class="link" type="submit"><span>< %=labels.forgotPassword%></span></button -->`
c. Ajoutez la ligne suivante sous la ligne mise en commentaire : `<a href="http://hostname:port/itim/self"><%=labels.forgotPassword%></a>`
d. Remplacez le port et le nom d'hôte par les valeurs appropriées pour le déploiement IBM Security Identity Manager spécifique.
e. Retournez à l'étape a. pour rechercher et modifier tous les liens Mot de passe oublié.

Génération d'IBM SmartCloud Control Desk

Cette section décrit la génération de IBM SmartCloud Control Desk.

Procédez comme suit :

1. Ouvrez une invite de commande sur la machine d'administration des services de base Maximo.

   Remarque : Les services de base Maximo peuvent être installés sur l'ordinateur WebSphere Application Server qui prend en charge IBM SmartCloud Control Desk ou sur un autre.
2. Accédez au répertoire `Installation_Maximo\deployment`.
3. Saisissez la commande suivante pour régénérer le fichier `maximo.ear` :

   `buildmaximoear.cmd`

   La commande `buildmaximoear.cmd` régénère le fichier `maximo.ear` ; elle sélectionne automatiquement les fichiers de classe modifiés et remplace ceux qui étaient inclus dans le fichier `maximo.ear` de départ. Laissez ce processus se terminer.
4. Copiez le nouveau fichier `maximo.ear` du serveur des services de base Maximo vers n'importe quel emplacement de WebSphere Application Server. Le nouveau fichier `maximo.ear` se trouve dans le répertoire suivant de la machine d'administration des services de base Maximo :

   `Maximo_Install\deployment\default`

Déploiement d'IBM SmartCloud Control Desk sur WebSphere Application Server

Cette section décrit le déploiement de IBM SmartCloud Control Desk sur WebSphere Application Server.

Pour déployer IBM SmartCloud Control Desk sur WebSphere Application Server, procédez comme suit :

1. Connectez-vous à la console d'administration de WebSphere Application Server.
2. Développez le noeud **Applications** de la zone de navigation et sélectionnez **Applications d'entreprise** pour afficher la fenêtre Applications d'entreprise.
3. Cochez la case en regard de **MAXIMO** et cliquez sur **Mettre à jour**.
4. Cliquez sur **Remplacer la totalité de l'application**.
5. Cliquez sur **Système de fichiers distant** puis sur **Parcourir**.
6. Sélectionnez le noeud de votre WebSphere Application Server.
7. Naviguez jusqu'au fichier `maximo.ear` que vous avez copié. Sélectionnez le fichier et cliquez sur **OK**.
8. Cliquez sur **Suivant**.
9. Cliquez sur **Suivant** dans **Sélection des options d'installation**.
10. Cliquez sur **Suivant** dans **Mappage des modules vers les serveurs**.
11. Cliquez sur **Terminer** sur la page Récapitulatif. Le fichier `maximo.ear` est redéployé. Ce processus peut prendre quelques minutes.
12. Cliquez sur **Sauvegarde dans la configuration principale**.
13. Développez le noeud **Applications** dans la zone de navigation et sélectionnez **Applications d'entreprise**.
14. Cochez la case en regard de **MAXIMO** et cliquez sur **Démarrer**. Laissez ce processus se terminer.
15. Déconnectez-vous de la console d'administration de WebSphere Application Server.

Configuration d'IBM Security Identity Manager

Cette section décrit les étapes de configuration de IBM Security Identity Manager.

Remarque : Dans les sections suivantes, ISIM_HOME fait référence au répertoire dans lequel IBM Security Identity Manager est installé.

Tableau 60. Etapes de configuration de IBM Security Identity Manager

Etape	Tâche	Description
1	Ajoutez maximo.jar au répertoire de bibliothèques partagées	L'archive maximo.jar contient le code qui gère l'intégration entre IBM Security Identity Manager et IBM SmartCloud Control Desk.
2	Ajoutez maximo.jar aux entrées de bibliothèques partagées	IBM Security Identity Manager doit savoir où se trouve le fichier maximo.jar afin de pouvoir l'utiliser.
3	Modifiez enRole.properties	Les informations de connexion de IBM SmartCloud Control Desk pour l'extension de mot de passe doivent être définies dans le fichier de propriétés.
4	Modifiez scriptframework.properties	L'extension changePassword est une extension de script ; le fichier de propriétés doit être modifié pour refléter cette modification.
5	Redémarrez WebSphere Application Server	WebSphere Application Server doit être redémarré pour que les modifications prennent effet.
6	Configurez l'extension de flux de travaux	L'extension changePassword doit être configurée lors de la configuration de IBM Security Identity Manager.
7	Configurez le profil de service IBM SmartCloud Control Desk	Pour pouvoir gérer les utilisateurs IBM SmartCloud Control Desk, le profil de service doit être configuré.

Configuration de WebSphere

Pour que l'intégration entre IBM Security Identity Manager et IBM SmartCloud Control Desk fonctionne, procédez comme suit.

1. Copiez le fichier maximo.jar du répertoire Maximo_Install\tim_51 sur la machine d'administration des service de base Maximo dans le répertoire ISIM_HOME\lib sur le serveur IBM Security Identity Manager. Pour les environnements en cluster, copiez le fichier dans le répertoire ISIM_HOME/lib sur chaque membre de cluster.
2. Connectez-vous à la console d'administration WebSphere Application Server pour l'installation de IBM Security Identity Manager.
3. Cliquez sur **Environnement** → **Bibliothèques partagées** → **ITIM_LIB**.
4. Ajoutez la ligne suivante au chemin d'accès aux classes :

   ```
   ${ISIM_HOME}/lib/maximo.jar
   ```
5. Cliquez sur **OK**.

Configuration d'IBM Security Identity Manager 6.0

Pour que l'intégration entre IBM Security Identity Manager et IBM SmartCloud Control Desk fonctionne, procédez comme suit.

Modifiez enRole.properties

1. Accédez au répertoire ISIM_HOME\data.
2. Ajoutez le texte suivant au fichier enRole.properties.

   ```
   ###################################
   ## Maximo Workflow Extension Properties
   ###################################
   ```

```
maximo.url=http://hostname:port
maximo.security=true
maximo.user=maxadmin
maximo.password=maxadmin
```

3. Remplacez *hostname* et *port* par les valeurs correspondant à l'environnement IBM SmartCloud Control Desk.
4. Définissez la valeur `maximo.security` sur "true" ou sur "false" selon que la sécurité du serveur d'applications est ou non activée. Si la valeur est définie sur "true", les zones `maximo.user` et `maximo.password` sont requises pour permettre la création de demandes de services pour IBM SmartCloud Control Desk lorsque la sécurité du serveur d'applications est activée. Pour les environnements en clusters, ce fichier doit être modifié sur chaque membre de cluster.
5. Enregistrez le fichier `enRole.properties` et fermez-le.

Modifiez scriptframework.properties

1. Accédez au répertoire `ISIM_HOME\data`.
2. Ajoutez la ligne suivante au fichier `scriptframework.properties` dans la section Workflow extensions :

   ```
   ITIM.extension.Workflow.Maximo=com.ibm.itim.maximo.MaximoExtension
   ```

3. Enregistrez le fichier `scriptframework.properties` et fermez-le.

Redémarrez WebSphere Application Server

Redémarrez WebSphere Application Server en l'arrêtant puis en le démarrant. Pour les environnements en clusters, redémarrez tous les membres du groupe d'applications.

Configurez l'extension de flux de travaux changePasssword

Pour que l'extension changePassword fonctionne, procédez comme suit :

1. Connectez-vous à IBM Security Identity Manager en tant qu'administrateur.
2. Cliquez sur **Configurer le système** → **Gérer des opérations**.
3. Sélectionnez le bouton radio **Niveau du type d'entité**.
4. Cliquez sur le lien **changePassword**.
5. Cliquez deux fois sur la zone d'extension **CHANGEPASSWORD**.
6. Cliquez sur l'onglet **Postscript** et ajoutez le texte suivant :

   ```
   Maximo.addTicket(Entity.get(), activity);
   ```

7. Cliquez sur **OK**.
8. Cliquez sur **Appliquer**, puis sur **OK** pour vérifier les modifications.

Configurez le fournisseur de services IBM SmartCloud Control Desk

Pour activer la prise en charge de la gestion des utilisateurs IBM SmartCloud Control Desk, procédez comme suit :

1. Copiez le fichier `maximoserviceprofile.jar` depuis le répertoire `Installation_Maximo\tim_51` vers une machine équipée d'un navigateur Web qui peut se connecter à IBM Security Identity Manager. Exécutez les étapes restantes depuis cette machine.
2. Connectez-vous à IBM Security Identity Manager via la console d'administration.

3. Cliquez sur **Gérer les types de services**.
4. Cliquez sur **Importer**.
5. Cliquez sur **Parcourir** et naviguez jusqu'au répertoire où se trouve le fichier `maximoserviceprofile.jar`.
6. Sélectionnez `maximoserviceprofile.jar`.
7. Cliquez sur **OK** et patientez quelques minutes pendant que l'opération se termine.
8. Cliquez sur **Gérer les services**.
9. Cliquez sur **Créer**, sélectionnez **Maximo Service** dans le menu, puis cliquez sur **Suivant**.
10. Saisissez un nom de service unique et indiquez l'adresse URL IBM SmartCloud Control Desk sous la forme `http://hostname:port` ou `https://hostname:port`, selon que SSL est utilisé sur le serveur IBM SmartCloud Control Desk.
11. Saisissez un ID utilisateur et un mot de passe si vous souhaitez exécuter les opérations sous un utilisateur spécifique autre que l'utilisateur `MXINTADM` par défaut. Si vous laissez ces zones vides, les opérations sont exécutées en tant que `MXINTADM`.
12. Sélectionnez la case à cocher **Activer la suppression d'utilisateurs Maximo ?** si *LOGINTRACKING* a la valeur false et que vous souhaitez supprimer des utilisateurs IBM SmartCloud Control Desk.
13. Cliquez sur **Tester la connexion**, vérifiez que le test a réussi, puis cliquez sur **Terminer**.

Remarque : Lorsque vous choisissez d'exécuter les opérations en tant qu'un utilisateur spécifique, vérifiez que cet utilisateur dispose des autorisations nécessaires. Par exemple, pour ajouter des utilisateurs à des groupes, le compte configuré pour exécuter l'affectation de groupes doit pouvoir affecter des utilisateurs à ces groupes. Pour plus d'informations sur l'autorisation de réaffectations de groupes, voir la documentation IBM SmartCloud Control Desk. Il peut également être nécessaire de modifier la règle d'application des accès par défaut créée en même temps que le nouveau service pour garantir que tous les attributs nécessaires sont définis. Lorsque vous créez un service Maximo via l'API IBM Security Identity Manager, le nom de profil du service est *maximoserviceprofile*. Lors de la création d'un compte, le nom du profil de compte est *MaximoAccount*. Si SSL est utilisé, voir la documentation appropriée pour votre version de WebSphere pour plus d'instructions sur la façon d'ajouter le certificat.

Attributs de l'adaptateur

Cette section décrit les attributs de l'adaptateur.

Descriptions des attributs

Le serveur IBM Security Identity Manager communique avec le fournisseur de services IBM SmartCloud Control Desk en utilisant les attributs indiqués dans des paquets de transmission envoyés sur un réseau. La combinaison d'attributs inclus dans les paquets varie en fonction du type d'action que le serveurserveur Security Identity Manager demande au fournisseur de services IBM SmartCloud Control Desk d'exécuter.

Le tableau 61 contient une liste d'attributs utilisés par le fournisseur de services IBM SmartCloud Control Desk. Il inclut une brève description et le type de données associé à la valeur des attributs.

Tableau 61. Attributs, descriptions et types de données correspondants

Attribut	Attributs du serveur d'annuaire	Description	Format des données
Userid	eruid	Spécifie l'ID utilisateur du compte.	Chaîne
Mot de passe	erpassword	Spécifie le mot de passe du compte.	Chaîne
Statut	eraccountstatus	Spécifie l'état du compte (ACTIF, INACTIF).	Chaîne
Type	ermaximousertype	Spécifie le type de l'utilisateur Maximo.	Chaîne
Defsite	ermaximodefsite	Spécifie le site par défaut du compte.	Chaîne
Storeroomsite	ermaximostoresite	Spécifie le site de magasin du compte.	Chaîne
Querywithsite	ermaximoquerysite	Spécifie s'il faut utiliser le site d'insertion en tant que filtre d'affichage.	Booléen
Emailpswd	ermaximoemailpswd	Spécifie s'il faut envoyer le mot de passe par e-mail à l'utilisateur à la création de son compte.	Booléen
Sysuser	ermaximosysuser	Spécifie si le compte est un compte système.	Booléen
Screenreader	ermaximoscreen	Spécifie si le compte nécessite un lecteur d'écran.	Booléen
Firstname	ermaximofirstname	Spécifie le prénom de la personne prenant en charge le compte utilisateur.	Chaîne
Nom	ermaximolastname	Spécifie le nom de la personne prenant en charge le compte utilisateur.	Chaîne
Phonenum	ermaximophone	Spécifie le numéro de téléphone principal de la personne.	Chaîne
PhoneType	ermaixmophonetype	Spécifie le type du numéro de téléphone principal de la personne.	Chaîne
Courrier électronique	ermaximoemail	Spécifie l'adresse e-mail principale de la personne.	Chaîne
Memo	ermaximomemo	Spécifie le mémo de la personne.	Chaîne
Addressline1	ermaximoaddress	Spécifie l'adresse de la personne.	Chaîne
City	ermaximocity	Spécifie la ville de la personne.	Chaîne
Stateprovince	ermaximostate	Spécifie l'état de la personne.	Chaîne
Postalcode	ermaximozip	Spécifie le code postal de la personne.	Chaîne
Country	ermaximocountry	Spécifie le pays de la personne.	Chaîne
Groupname	ermaximogroupname	Définit le nom du groupe.	Chaîne
GroupDescription	ermaximogroupdescription	Spécifie la description du groupe.	Chaîne

Attributs de fournisseur de services IBM SmartCloud Control Desk par action

Les listes suivantes représentent des actions de fournisseurs de services IBM SmartCloud Control Desk typiques, organisées selon leur groupe de transaction fonctionnelle. Ces listes incluent d'autres informations sur les attributs requis et facultatifs envoyés au fournisseur de services IBM SmartCloud Control Desk pour mener l'action à bien.

System Login Add

La fonction "System Login Add" est une demande de création de compte utilisateur dans le domaine avec les attributs indiqués.

Tableau 62. Attributs de la requête d'ajout (Add)

Attributs obligatoires	Attribut facultatif
eruid ermaximoemailpswd	Tous les autres attributs pris en charge

System Login Change

La fonction "System Login Change" est une demande de modification d'un ou plusieurs attributs pour les utilisateurs indiqués.

Tableau 63. Attributs de la requête de modification (Change)

Attributs obligatoires	Attribut facultatif
eruid	Tous les autres attributs pris en charge

System Login Delete

La fonction "System Login Delete" est une demande de suppression de l'utilisateur spécifié du registre IBM SmartCloud Control Desk.

Tableau 64. Attributs de la requête de suppression (Delete)

Attributs obligatoires	Attribut facultatif
eruid	Aucun

System Login Suspend

La fonction "System Login Suspend" est une demande de désactivation d'un compte utilisateur. L'utilisateur n'est pas supprimé et les attributs ne sont pas modifiés.

Tableau 65. Attributs de la requête de suspension (Suspend)

Attributs obligatoires	Attribut facultatif
eruid eraccountstatus	Aucun

System Login Restore

La fonction "System Login Restore" est une demande d'activation d'un compte utilisateur précédemment suspendu. Lorsque le compte a été réactivé, l'utilisateur peut accéder au système avec les mêmes attributs que ceux utilisés avant l'appel de la fonction Suspend.

Tableau 66. Attributs de demande de restauration

Attributs obligatoires	Attribut facultatif
eruid eraccountstatus	Aucun

Reconciliation

La fonction "Reconciliation" synchronise les informations d'un compte utilisateur entre IBM Security Identity Manager et l'adaptateur.

Tableau 67. Attributs de demande de restauration

Attributs obligatoires	Attribut facultatif
Aucun	Aucun

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 donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM 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.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales. LE PRESENT DOCUMENT EST LIVRE «EN L'ETAT». IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE VALEUR MARCHANDE OU D'ADAPTATION A VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites ou explicites, 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
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
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

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 tout le matériel sous licence disponible pour ce programme, sont fournis par IBM conformément aux termes du contrat client IBM (IBM Customer Agreement), de l'accord de licence du programme international d'IBM (IBM International Program License Agreement) ou de tout contrat équivalent entre nous.

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.

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

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes de demande en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits. 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 programme sont fournis "en l'état", sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable de tout dommage résultant de votre utilisation de ces programmes.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit : © (nom de votre société) (année). Des segments de code sont dérivés des programmes exemples d'IBM Corp. © Copyright IBM Corp. 2004, 2012. 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.

Marques

Les termes qui suivent sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays : http://www.ibm.com/legal/copytrade.shtml

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques commerciales ou déposées d'Adobe Systems Incorporated aux États-Unis et/ou dans d'autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Le programme Oracle Outside In Technology ci-inclus fait l'objet d'une licence à utilisation limitée et peut seulement être utilisé conjointement à la présente application.

D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.

Index

I

J

L

M

N

O

P

R

S

T

U

W

SC11-7069-00