



Sécurisation des applications et de leurs environnements



Sécurisation des applications et de leurs environnements

Important

Avant d'utiliser ces informations, veuillez à lire les informations générales à la section Remarques située à la fin du présent document.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

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
Tour Descartes
92066 Paris-La Défense Cedex 50*

© Copyright IBM France 2009. Tous droits réservés.

© **Copyright International Business Machines Corporation 2005, 2008.**

Manuels au format PDF et centre de documentation

Les manuels au format PDF facilitent l'impression et permettent la lecture en mode déconnecté, tandis que le centre de documentation en ligne contient les informations les plus récentes.

Pris dans l'ensemble, les manuels au format PDF ont le même contenu que celui du centre de documentation.

La documentation PDF est disponible dans le trimestre suivant une édition importante du centre de documentation (version 6.0 ou 6.1, par exemple).

Ses mises à jour sont moins fréquentes que celles du centre de documentation, mais plus fréquentes que celles des Redbooks. En général, les manuels au format PDF sont mis à jour lorsqu'un nombre suffisant de changements a été apporté depuis la dernière édition.

Les liens vers des rubriques externes à un manuel lancent le centre de documentation sur le Web. Ils sont signalés par des icônes qui indiquent si la cible est une page Web ou un manuel au format PDF.

Tableau 1. Icônes accompagnant les liens vers des rubriques externes au manuel



Icône	Description
	<p>Lien vers une page Web, qui peut être une page du centre de documentation.</p> <p>Les liens qui pointent vers le centre de documentation passent par un service de routine d'indirection, en sorte qu'ils ne sont jamais rompus, même lorsque la cible a changé d'emplacement.</p> <p>Si vous souhaitez rechercher une page liée dans un centre de documentation local, vous pouvez lancer une recherche sur le titre du lien ou sur l'ID rubrique. Si votre recherche renvoie plusieurs rubriques de même nom pour différentes variantes de produits, vous pouvez utiliser les fonctions Regrouper par pour indiquer l'instance à consulter. Exemple :</p> <ol style="list-style-type: none">1. Copiez l'URL du lien (entre autres, vous pouvez cliquer avec le bouton droit sur le lien, puis sélectionner Copier l'emplacement du lien). Exemple : <code>http://www14.software.ibm.com/webapp/wsbroker/redirect?version=wbpm620&product=wesb-dist&topic=tins_apply_service</code>2. Copiez l'ID rubrique qui suit le texte <code>&topic=</code>. Exemple : <code>tins_apply_service</code>3. Dans la zone de recherche de votre centre de documentation local, collez cet ID rubrique. Si la fonction de documentation est installée en local, la rubrique apparaîtra dans les résultats de la recherche. Exemple : <div data-bbox="613 1577 1458 1776" style="border: 1px solid black; border-radius: 10px; padding: 10px;"><p>1 résultat(s) trouvé(s) pour</p><p>Regrouper par : Aucun(e) Plateforme Version Produit</p><p>Afficher le récapitulatif</p><p>Installation de groupes de correctifs et de groupes de mises à jour avec Update Installer</p></div> <ol style="list-style-type: none">4. Cliquez sur le lien figurant dans les résultats de la recherche pour afficher la rubrique correspondante.
	Lien vers un manuel au format PDF.

Table des matières

Manuels au format PDF et centre de documentation iii

Sécurisation des applications et de leur environnement 1

Présentation générale de la sécurité 1

Initiation à la sécurité 3

Installation de WebSphere Process Server : remarques sur la sécurité 5

 Informations d'authentification lors de l'installation 6

Configuration de la sécurité de WebSphere Process Server pour un serveur autonome 7

 Sécurisation d'une installation WebSphere Process Server autonome 7

 Activation de la sécurité 10

 Configuration d'un référentiel de comptes utilisateur 14

 Démarrage et arrêt du serveur 20

 Rôles de sécurité 22

 Sécurité par défaut des composants installés 24

Configuration de la sécurité de WebSphere Process Server pour un serveur d'environnement de déploiement 27

Sécurisation d'un environnement de déploiement de WebSphere Process Server 27

 Activation de la sécurité 30

 Configuration d'un référentiel de comptes utilisateur 34

 Démarrage et arrêt du serveur 40

 Rôles de sécurité 42

 Sécurité par défaut des composants installés 44

Sécurisation des applications dans WebSphere Process Server 46

 Éléments de sécurité 47

 Déploiement (installation) d'applications sécurisées 53

 Sécurité pour Business Calendar Manager 56

 Sécurité des adaptateurs 60

 Sécurité des tâches utilisateur et des processus métier 61

 Configuration de la sécurité de Business Space 62

Mise en place de la sécurité de bout en bout 65

Remarques 69

Sécurisation des applications et de leur environnement

La sécurisation de l'environnement WebSphere Process Server implique l'activation de la sécurité administrative, l'activation de la sécurité des applications, la création de profils de sécurité et la limitation de l'accès aux fonctions vitales à des utilisateurs sélectionnés.

La sécurité de WebSphere Process Server est basée sur la sécurité de WebSphere Application Server version 6.1. Ces documents complètent la documentation principale relative à la sécurité, disponible dans le centre de documentation de WebSphere Application Server, et plus particulièrement dans la documentation relative à la sécurité de WebSphere Application Server, «Sécurisation des applications et de leur environnement».

Information associée

 [Documentation PDF](#)

Documentation de WebSphere Process Server (au format PDF)

 [Organigramme des informations](#)

L'organigramme des informations Business Process Management sous IBM developerWorks permet de trouver des informations sur WebSphere Process Server, WebSphere ESB et les autres produits du portefeuille.

 [IBM Education Assistant](#)

Modules de formation multimédia sur WebSphere Process Server fournis par IBM Education Assistant.

 [Notes techniques](#)

Support de WebSphere Process Server > Recherche de notes techniques dans les documents 6.2 de la catégorie sécurité. Indiquez un type de document, une catégorie de produit et/ou entrez des termes de recherche pour rechercher les informations souhaitées.

 [Présentation](#)

Onglet Présentation, sur la page Web de la bibliothèque du produit. Cette page permet d'accéder aux annonces, aux fiches techniques et à d'autres documents de bibliothèques générales relatifs à WebSphere ESB.

Présentation générale de la sécurité

La sécurité de WebSphere Process Server est basée sur la sécurité de WebSphere Application Server version 6.1.

Pour plus d'informations sur la sécurité, voir le centre de documentation de WebSphere Application Server Network Deployment.

De manière générale, les opérations de sécurité se répartissent entre les opérations d'administration de la sécurité dans l'environnement WebSphere Process Server et celles liées à l'exécution des applications dans WebSphere Process Server. La sécurité de l'environnement serveur est essentielle à la sécurité applicative ; les deux aspects ne doivent donc pas être traités isolément.

La sécurisation d'un environnement implique l'activation de la sécurité administrative, l'activation de la sécurité des applications, la création des profils de sécurité et la limitation de l'accès des utilisateurs aux fonctions vitales.

La sécurisation d'une application comprend plusieurs aspects. Par exemple :

- Authentification des utilisateurs - Un utilisateur ou un processus qui appelle une application doit être authentifié. Avec l'authentification unique, un utilisateur peut ne fournir ses données d'authentification qu'une seule fois et les transmettre ensuite aux composants en aval.
- Contrôle d'accès - L'utilisateur authentifié dispose-t-il des droits nécessaires pour effectuer l'opération ?
- Intégrité des données - Les données accessibles à partir des applications doivent être sécurisées afin qu'aucun utilisateur non autorisé ne puisse les visualiser ni les modifier.

Vous trouverez plus loin dans cette section des remarques de sécurité détaillées concernant différentes étapes du fonctionnement de WebSphere Process Server.

Concepts associés

«Authentification des utilisateurs», à la page 48

Si la sécurité administrative est activée, les clients doivent être authentifiés.

«Contrôle d'accès», à la page 50

Le contrôle d'accès permet de garantir qu'un utilisateur authentifié dispose des droits nécessaires pour accéder à des ressources ou effectuer une opération donnée.

«Intégrité et confidentialité des données», à la page 51

La confidentialité et l'intégrité des données auxquelles les processus WebSphere Process Server accèdent lorsqu'ils sont appelés sont des éléments essentiels de votre sécurité.

«Authentification unique», à la page 52

Un client ne doit fournir son nom d'utilisateur et son mot de passe qu'une seule fois. Son identité est ensuite propagée dans l'ensemble du système.

Remarques sur la sécurité spécifiques à WebSphere Process Server

La sécurité de WebSphere Process Server repose sur la sécurité de WebSphere Application Server 6.1. La section suivante répertorie les considérations propres à WebSphere Process Server.

- Le panneau Sécurité Business Integration de la console d'administration est spécifique à WebSphere Process Server. Pour y accéder, développez **Sécurité** et cliquez sur **Sécurité Business Integration**. Ce panneau permet aux utilisateurs d'attribuer des identités spécifiques de leur registre d'utilisateurs aux alias d'authentification Business Integration. En outre, ce panneau vous permet d'administrer vos paramètres de sécurité de Business Process Choreographer.
- La sécurité des applications est activée par défaut dans WebSphere Process Server. Ce n'est pas le cas dans WebSphere Application Server.
- WebSphere Process Server contient un ensemble de rôles de sécurité spécifiques aux composants.

Initiation à la sécurité

La sécurité doit être prise en compte lors de la planification de l'installation de WebSphere Process Server, lors du développement et du déploiement d'applications et dans les opérations quotidiennes de votre serveur de processus.

La liste suivante présente les tâches que vous effectuez pour sécuriser WebSphere Process Server.

1. Prenez en compte la sécurité lorsque vous installez WebSphere Process Server.
2. Assurez-vous que la sécurité est activée pour votre installation autonome ou en environnement de déploiement.
 - a. Assurez-vous que la sécurité administrative est activée.
 - b. Assurez-vous que la sécurité applicative est activée.
 - c. Si nécessaire, activez la sécurité Java 2.
 - d. Utilisez l'assistant de configuration de la sécurité dans la console d'administration pour configurer les options de sécurité.
 - e. Configurez un mécanisme d'authentification sécurisé et un référentiel de comptes utilisateur.
 - f. Affectez des noms et des mots de passe utilisateur à des alias d'authentification Business Integration importants.
 - g. Affectez les utilisateurs aux rôles de sécurité appropriés.
3. Définissez la sécurité pour des composants WebSphere Process Server spécifiques. Par exemple, utilisez le gestionnaire de sécurité pour définir un contrôle d'accès basé sur les rôles pour les plannings de Business Calendar Manager.
4. Sécurisez les applications que vous déployez dans votre environnement Process Server.
 - a. Développez vos applications dans WebSphere Integration Developer en utilisant l'ensemble des fonctions de sécurité prévues.
 - b. Déployez vos applications dans votre environnement WebSphere Process Server.
 - c. Affectez des utilisateurs ou des groupes aux rôles de sécurité appropriés pour contrôler l'accès à l'application venant d'être déployée.
5. Gérez la sécurité de votre environnement WebSphere Process Server.

Tâches associées

«Installation de WebSphere Process Server : remarques sur la sécurité», à la page 5
Prenez en compte la méthode d'implémentation de la sécurité avant, pendant et après l'installation de WebSphere Process Server.

«Activation de la sécurité», à la page 10

La première étape du processus de sécurisation de votre environnement WebSphere Process Server et de vos applications est l'activation de la sécurité administrative.

«Configuration d'un référentiel de comptes utilisateur», à la page 14

Les noms d'utilisateur et les mots de passe des utilisateurs enregistrés sont stockés dans un référentiel de comptes utilisateur. Vous pouvez utiliser soit le référentiel de comptes utilisateur du système d'exploitation local (option par défaut), le registre LDAP (Lightweight Directory Access Protocol) et des référentiels fédérés, soit un référentiel de comptes personnalisé.

Développement de composants sécurisés

Sécurisez les composants que vous développez. Les composants implémentent des interfaces dotées de méthodes. Utilisez le qualificatif SCA (Service Component Architecture) SecurityPermission pour sécuriser une interface ou une méthode.

«Déploiement (installation) d'applications sécurisées», à la page 53

Le déploiement d'applications disposant de contraintes de sécurité (applications sécurisées) est similaire au déploiement d'applications sans contraintes de sécurité. La seule différence réside dans l'affectation éventuelle d'utilisateurs ou de groupes à des rôles dans le cas d'applications sécurisées, ce qui implique que le registre d'utilisateurs que vous utilisez est correct. Lorsque vous installez une application sécurisée, des rôles doivent y avoir été définis. Si l'application utilise la délégation, les rôles RunAs doivent également être définis ; en outre, un nom d'utilisateur et un mot de passe valides doivent être saisis.

«Affectation d'utilisateurs à des rôles», à la page 54

Une application sécurisée utilise un des deux (ou les deux) qualificatifs de sécurité securityPermission et securityIdentity. Lorsque ces deux qualificatifs sont utilisés, des opérations supplémentaires doivent être effectuées au moment du déploiement afin que l'application et ses fonctions de sécurité fonctionnent correctement.

«Sécurité pour Business Calendar Manager», à la page 56

Le gestionnaire de sécurité vous permet de sécuriser l'accès à chaque planning dans Business Calendar Manager. Vous pouvez utiliser le gestionnaire de sécurité pour attribuer des rôles aux membres d'une organisation. Ce sont ces rôles qui déterminent le niveau d'accès aux plannings.

Information associée

«Configuration de la sécurité de WebSphere Process Server pour un serveur autonome», à la page 7

La configuration de la sécurité d'une installation autonome de WebSphere Process Server implique des tâches telles que l'activation de la sécurité administrative et la configuration d'un registre des comptes utilisateur.

«Configuration de la sécurité de WebSphere Process Server pour un serveur d'environnement de déploiement», à la page 27

La configuration de la sécurité d'une installation en environnement de déploiement de WebSphere Process Server implique des tâches telles que l'activation de la sécurité administrative et la configuration d'un registre des comptes utilisateur.

Installation de WebSphere Process Server : remarques sur la sécurité

Prenez en compte la méthode d'implémentation de la sécurité avant, pendant et après l'installation de WebSphere Process Server.

Procédure

1. Sécurisez votre environnement avant l'installation.

Les commandes nécessaires pour installer WebSphere Process Server avec un niveau de sécurité adéquat dépendent du système d'exploitation. Pour plus d'informations sur les opérations à effectuer avant l'installation, voir la rubrique **Sécurisation de l'environnement avant l'installation** du centre de documentation de WebSphere Application Server.

i5/OS Les commandes nécessaires pour installer WebSphere Process Server avec un niveau de sécurité adéquat dépendent du système d'exploitation. Pour plus d'informations sur les opérations à effectuer avant l'installation, voir la rubrique **Préparation des systèmes i5/OS en vue de l'installation** dans les tâches connexes.

2. Préparez le système d'exploitation en vue de l'installation de WebSphere Process Server.

Cette étape explique comment préparer les différents systèmes d'exploitation en vue de l'installation de WebSphere Process Server. Pour plus d'informations, consultez la rubrique **Préparation du système d'exploitation en vue de l'installation du produit** du centre de documentation de WebSphere Application Server.

3. Sécurisez votre environnement après l'installation.

Cette étape explique comment protéger les informations relatives aux mots de passe, une fois WebSphere Process Server installé. Pour plus d'informations sur la sécurisation de votre environnement, voir la rubrique **Sécurisation de l'environnement avant l'installation** du centre de documentation de WebSphere Application Server.

Que faire ensuite

Une fois l'installation effectuée, la sécurité peut être administrée à partir de la console d'administration.

Concepts associés

«Initiation à la sécurité», à la page 3

La sécurité doit être prise en compte lors de la planification de l'installation de WebSphere Process Server, lors du développement et du déploiement d'applications et dans les opérations quotidiennes de votre serveur de processus.

Information associée

- ➡ Sécurisation de l'environnement avant l'installation
- ➡ Préparation du système d'exploitation en vue de l'installation du produit
- ➡ Sécurisation de l'environnement après l'installation
- ➡ Préparation des systèmes i5/OS en vue de l'installation

Informations d'authentification lors de l'installation

Lors de l'installation, vous êtes invité à indiquer des informations de sécurité de telle sorte que l'environnement WebSphere Process Server soit immédiatement sécurisé.

Dans les éditions précédentes de WebSphere Process Server, vous deviez entrer différentes informations d'authentification au cours l'installation. Maintenant, tous les composants utilisent par défaut les données d'identification principales que vous indiquez pour la sécurité d'administration. Ces valeurs par défaut assurent une sécurité de base, mais pour renforcer la sécurité de votre installation, vous devez utiliser la console d'administration pour configurer les différents composants de WebSphere Process Server afin de leur attribuer les identités de sécurité appropriées.

Lors de la création d'un profil WebSphere Process Server, si vous laissez l'option **Activer la sécurité administrative**, vous êtes invité à saisir un nom d'utilisateur. Cette identité est utilisée par défaut pour les composants sous-jacents. Vous devez également configurer ces identités après la création du profil afin de renforcer la sécurité.

Plusieurs composants de WebSphere Process Server utilisent les alias d'authentification. Ces alias servent à authentifier le composant d'exécution pour l'accès aux bases de données et aux moteurs de messagerie. Ces alias peuvent être modifiés sur le panneau Sécurité Business Integration de la console d'administration.

Création de profils WebSphere Process Server avec sécurité

Lorsque vous créez un profil WebSphere Process Server, les valeurs par défaut sont utilisées pour les données d'identification de sécurité. Vous devez configurer ces paramètres de sécurité sur la console d'administration après avoir créé le profil.

A propos de cette tâche

Lorsque vous créez un profil WebSphere Process Server, trois composants de WebSphere Process Server endossent par défaut l'identité de l'administrateur.

Il s'agit des composants suivants :

- Architecture SCA (Service Component Architecture)
- Business Process Choreographer
- Common Event Infrastructure (CEI)

Les identités associées à ces composants sont utilisées pour créer des alias d'authentification qui sont requis lorsque la sécurité est activée. Il est important de remplacer ces identités par des utilisateurs appropriés issus de votre référentiel de comptes.

Procédure

1. Dans la console d'administration, affichez le panneau Sécurité Business Integration. Cliquez sur **Sécurité**, puis sur **Sécurité Business Integration**.
2. Pour chacun des alias d'authentification de l'architecture Service Component Architecture, de Business Process Choreographer et de Common Event Infrastructure, fournissez un nom d'utilisateur et un mot de passe appropriés.
 - a. Sélectionnez l'alias que vous voulez modifier en cliquant sur son nom dans la colonne **Alias**.

Remarque : Dans certains cas, la colonne **Alias** peut ne pas contenir de lien. Dans ce cas, cochez la case de la colonne **Sélectionner** correspondant à l'alias que vous voulez éditer et cliquez sur **Editer**.

- b. Dans le panneau suivant, indiquez le nom d'utilisateur et le mot de passe devant servir d'alias d'authentification pour ce composant.

Remarque : Les données d'identification que vous indiquez doivent exister dans le référentiel de comptes utilisateur que vous utilisez.

- c. Cliquez sur **OK**.

Tâches associées

«Modification des alias d'authentification», à la page 49

Vous pouvez être amené à modifier les alias d'authentification existants.

Configuration de la sécurité de WebSphere Process Server pour un serveur autonome

La configuration de la sécurité d'une installation autonome de WebSphere Process Server implique des tâches telles que l'activation de la sécurité administrative et la configuration d'un registre des comptes utilisateur.

Concepts associés

«Initiation à la sécurité», à la page 3

La sécurité doit être prise en compte lors de la planification de l'installation de WebSphere Process Server, lors du développement et du déploiement d'applications et dans les opérations quotidiennes de votre serveur de processus.

Sécurisation d'une installation WebSphere Process Server autonome

La sécurité de votre environnement WebSphere Process Server est gérée dans la console d'administration. Un utilisateur disposant de droits d'accès appropriés peut activer ou désactiver toutes les fonctions de sécurité des applications depuis la console d'administration. Il est donc capital que vous sécurisiez l'environnement avant de déployer des applications sécurisées.

Avant de commencer

Vous devez avoir installé WebSphere Process Server et vérifié l'installation avant de commencer à effectuer les opérations ci-dessous.

A propos de cette tâche

Votre environnement WebSphere Process Server est défini dans un profil. Ouvrez la console d'administration pour le profil que vous souhaitez sécuriser. Connectez-vous à la console en utilisant n'importe quel ID utilisateur ; dans la mesure où le profil est sécurisé, tous les noms d'utilisateur seront acceptés.

La procédure suivante fournit une feuille de route pour les tâches à effectuer pour activer la sécurité. Vous trouverez des informations détaillées spécifiques pour ces tâches dans les rubriques suivantes.

Procédure

1. Assurez-vous que la sécurité administrative est activée. «Activation de la sécurité», à la page 10.
2. Assurez-vous que la sécurité applicative est activée. «Sécurisation des applications dans WebSphere Process Server», à la page 46.
3. Ajoutez des utilisateurs ou des groupes au rôle administratif. Vous pouvez accorder des droits d'administration à des utilisateurs individuels ou à un groupe d'utilisateurs en suivant respectivement **Rôles de l'utilisateur administratif** ou **Rôles du groupe administratif**.
4. Sélectionnez le référentiel de comptes utilisateur que vous voulez utiliser.
Le tableau suivant décrit les différents registres d'utilisateurs et les opérations à effectuer pour le sélectionner et le configurer.

Registre d'utilisateurs	Action
Référentiels fédérés	Indiquez ce paramètre pour gérer des profils dans plusieurs référentiels sous un domaine unique. Le domaine peut se composer d'identités dans : <ul style="list-style-type: none">• Le référentiel de fichiers intégré au système• Un ou plusieurs référentiels• Le référentiel de fichiers intégré et un ou plusieurs référentiels externes Remarque : Seul un utilisateur disposant de droits d'administration peut visualiser la configuration des référentiels fédérés. Pour plus d'informations, voir <i>Managing the realm in a federated repository configuration</i> .
Système d'exploitation local	Registre d'utilisateurs par défaut. Pour plus d'informations sur la configuration du registre de comptes utilisateur, voir «Configuration du référentiel de comptes utilisateur personnalisé autonome ou du système d'exploitation local», à la page 15.
Registre LDAP autonome	Suivez les instructions de la section <i>Configuration du protocole LDAP</i> en tant que registre d'utilisateurs pour configurer le protocole LDAP en tant que registre de comptes utilisateur.

Registre d'utilisateurs	Action
Registre personnalisé autonome	Pour plus de détails sur la configuration du registre de comptes utilisateur, voir «Configuration du référentiel de comptes utilisateur personnalisé autonome ou du système d'exploitation local», à la page 15.

5. Assurez-vous d'avoir défini le registre sélectionné comme étant votre registre courant.
Si vous ne l'avez pas déjà fait, cliquez sur **Défini comme courant** en bas de la page Administration, applications et infrastructure sécurisées.
6. Assurez-vous d'avoir appliqué les modifications après avoir sélectionné le registre d'utilisateurs.
Si vous ne l'avez pas déjà fait, cliquez sur **Appliquer** en bas de la page Administration, applications et infrastructure sécurisées.
7. Accédez au panneau Sécurité Business Integration. Cliquez sur **Sécurité**, puis sur **Sécurité Business Integration**.
8. Fournissez les identités utilisateur appropriées pour les alias d'authentification répertoriés. Les données d'identification que vous indiquez doivent exister dans le référentiel de comptes utilisateur que vous utilisez.
9. Dans le même panneau, vous pouvez configurer la sécurité pour Business Process Choreographer.
Définissez les mappages de rôles utilisateur de Business Process Choreographer pour les gestionnaires Business Flow Manager et Human Task Manager :
 - **Administrateur** : Noms d'utilisateur et/ou noms de groupe liés au rôle d'administrateur de flux métier et de tâches utilisateur. Les utilisateurs qui se voient affecter ce rôle disposent de tous les privilèges.
 - **Superviseur** : Noms d'utilisateur et/ou noms de groupe liés au rôle de surveillance des flux métier et tâches utilisateur. Les utilisateurs associés à ce rôle peuvent visualiser les propriétés de tous les processus métier et objets de tâches.

Les alias d'authentification de Business Process Choreographer peuvent être configurés pour chaque cible de déploiement sur laquelle Business Process Choreographer a été installé. Les alias d'authentification répertoriés sont les suivants :

 - **Authentification d'API JMS** : Authentification permettant au bean géré par message du gestionnaire de flux métier de traiter les appels asynchrones émis par les interfaces de programme d'application.
 - **Authentification d'utilisateur d'escalade** : Authentification permettant au bean géré par message du gestionnaire de tâches utilisateur de traiter les appels asynchrones émis par les interfaces de programme d'application.
10. Validez ces modifications.
Cliquez sur le bouton **Valider** dans la partie inférieure du panneau.
11. Enregistrez les modifications dans la configuration locale.
Cliquez sur **Sauvegarder** dans la fenêtre de message.
12. Si nécessaire, arrêtez et redémarrez le serveur.
Si le serveur doit être redémarré, un message s'affiche dans la console d'administration.

Résultats

A votre prochaine connexion à la console d'administration, vous devrez fournir un nom d'utilisateur et un mot de passe valides.

Que faire ensuite

Chaque profil créé doit être sécurisé de cette manière. L'identité de l'administrateur système a peut-être été utilisée à plusieurs emplacements au cours de l'installation et de la configuration de l'environnement. Il est conseillé de remplacer cette identité par des données d'identification de l'utilisateur appropriées issues du référentiel de comptes utilisateur pour toutes les fonctions à l'exception des fonctions principales de sécurité. Le panneau **Sécurité Business Integration** de la console d'administration permet de gérer ces identités et alias.


Tâches associées

«Activation de la sécurité»

La première étape du processus de sécurisation de votre environnement WebSphere Process Server et de vos applications est l'activation de la sécurité administrative.

«Sécurisation des applications dans WebSphere Process Server», à la page 46
Les applications que vous déployez dans votre instance de WebSphere Process Server requièrent que les fonctions de sécurité soient intégrées et appliquées au moment de leur exécution.

Information associée

 Utilisation des outils de vérification de l'installation avec WebSphere Process Server

Activation de la sécurité

La première étape du processus de sécurisation de votre environnement WebSphere Process Server et de vos applications est l'activation de la sécurité administrative.

Avant de commencer

Installez WebSphere Process Server et vérifiez l'installation avant de commencer à effectuer les opérations ci-dessous.

Ouvrez la console d'administration pour le profil que vous souhaitez sécuriser. Connectez-vous à la console en utilisant n'importe quel ID utilisateur ; dans la mesure où le profil est sécurisé, tous les noms d'utilisateur seront acceptés.

A propos de cette tâche

Pour plus d'informations sur la sécurité administrative, la sécurité des applications et la sécurité Java 2, reportez-vous aux informations répertoriées sous **Sous-rubriques**.

Procédure

1. Ouvrez le panneau de sécurité administrative dans la console d'administration. Développez **Sécurité**, puis cliquez sur **Administration, applications et infrastructure sécurisées**.
2. Procéder à l'activation de la sécurité administrative. Sélectionnez **Activer la sécurité administrative**.

3. Activez la sécurité des applications.

Sélectionnez **Activer la sécurité des applications**.

4. Facultatif : Appliquez la sécurité Java 2, si nécessaire.

Sélectionnez **Utiliser la sécurité Java 2 pour limiter l'accès aux applications des ressources locales** pour appliquer le contrôle des droits de sécurité Java 2.

Lorsque la sécurité Java 2 est activée, une application nécessitant plus de droits de sécurité Java 2 que la politique par défaut n'en accorde, peut ne pas s'exécuter correctement. Les droits nécessaires doivent alors être définis dans le fichier app.policy ou le fichier was.policy de l'application. Des exceptions de contrôle d'accès sont générées par les applications qui ne disposent pas des droits requis. Pour plus d'informations sur la sécurité Java 2, consultez la rubrique relative à la configuration des fichiers de règles de sécurité Java 2 du Centre de documentation de WebSphere Application Server.

Remarque : Les mises à jour du fichier app.policy ne s'appliquent qu'aux applications d'entreprise du noeud auquel appartient ce fichier app.policy.

- a. Facultatif : Sélectionnez **Prévenir si des applications accordent des permissions personnalisées**. Le fichier filter.policy contient une liste de droits d'accès qu'une application ne doit pas posséder conformément à la spécification J2EE 1.3. Si une application est installée avec un droit d'accès indiqué dans ce fichier de règles et que cette option est activée, un avertissement est émis. Par défaut, elle est activée.
 - b. Facultatif : Sélectionnez **Limiter l'accès aux données d'authentification des ressources**. Activez cette option si vous devez restreindre l'accès des applications à des données sensibles d'authentification de mappage Java Connector Architecture (JCA).
5. Validez ces modifications.
Cliquez sur le bouton **Valider** dans la partie inférieure du panneau.
 6. Enregistrez les modifications dans la configuration locale.
Cliquez sur **Sauvegarder** dans la fenêtre de message.
 7. Si nécessaire, arrêtez et redémarrez le serveur.
Si le serveur doit être redémarré, un message s'affiche dans la console d'administration.

Que faire ensuite

Vous devez activer la sécurité administrative pour chaque profil que vous créez.

Concepts associés

«Initiation à la sécurité», à la page 3

La sécurité doit être prise en compte lors de la planification de l'installation de WebSphere Process Server, lors du développement et du déploiement d'applications et dans les opérations quotidiennes de votre serveur de processus.

Tâches associées

«Sécurisation des applications dans WebSphere Process Server», à la page 46

Les applications que vous déployez dans votre instance de WebSphere Process Server requièrent que les fonctions de sécurité soient intégrées et appliquées au moment de leur exécution.

Information associée

 Configuration des fichiers de règles de sécurité Java 2

Sécurité administrative

La sécurité administrative détermine si la sécurité est utilisée, le type de registre sur lequel effectuer l'authentification, ainsi que d'autres fonctions, qui sont souvent associées à une valeur par défaut. Lors de la planification, si l'activation de la sécurité n'est pas définie de façon appropriée, cela peut bloquer l'accès à la console d'administration ou entraîner l'arrêt du serveur.

La sécurité administrative constitue un "commutateur central" qui active différents paramètres de sécurité pour WebSphere Process Server. Vous pouvez définir les valeurs de ces paramètres, mais elles ne sont appliquées que lorsque la sécurité administrative est activée. Ces paramètres concernent notamment l'authentification des utilisateurs, l'utilisation de la couche SSL (Secure Sockets Layer) et la sélection du référentiel des comptes utilisateur. La sécurité des applications, notamment l'authentification et les autorisations par rôle, n'est appliquée que lorsque la sécurité administrative est active. La sécurité administrative est activée par défaut.

La sécurité administrative est la configuration de la sécurité appliquée à l'ensemble du domaine de sécurité. Un domaine de sécurité est constitué de tous les serveurs configurés avec le même nom de domaine de registre d'utilisateurs. Dans certains cas, le domaine peut être le nom de l'ordinateur d'un registre de système d'exploitation local. Dans ce cas, tous les serveurs d'application doivent se trouver sur la même machine physique. Dans d'autres cas, le domaine peut être le nom de l'ordinateur d'un registre LDAP autonome.

La configuration peut inclure plusieurs noeuds car vous pouvez accéder à distance aux registres d'utilisateurs qui prennent en charge le protocole LDAP. Vous pouvez donc activer l'authentification depuis n'importe quel emplacement.

Une condition doit être remplie dans un domaine de sécurité : l'ID d'accès renvoyé par le registre ou le référentiel d'un serveur du domaine de sécurité doit être identique à l'ID d'accès renvoyé par le registre ou le référentiel de tout autre serveur du même domaine de sécurité. L'ID d'accès est l'identification unique d'un utilisateur utilisée lors de l'autorisation pour déterminer si l'accès à la ressource est autorisé.

La configuration de la sécurité administrative s'applique à chaque serveur du domaine de sécurité.

Pourquoi activer la sécurité administrative ?

L'activation de la sécurité d'administration permet d'activer les paramètres protégeant votre ordinateur des utilisateurs non autorisés. La sécurité administrative est activée par défaut lors de la création du profil. Dans certains environnements (comme un système de développement), l'activation de la sécurité n'est pas nécessaire. Sur ces systèmes, vous pouvez désactiver la sécurité administrative. Cependant, dans la plupart des environnements il est préférable d'empêcher les utilisateurs non autorisés d'accéder à la console d'administration et aux applications métier. La sécurité administrative doit être activée de façon à restreindre l'accès.

Quelle protection apporte la sécurité administrative ?

La configuration de la sécurité administrative d'un domaine de sécurité implique la configuration des technologies suivantes :

- Authentification des clients HTTP
- Authentification des clients IIOP
- Sécurité de la console d'administration
- Sécurité de la dénomination
- Utilisation des transports SSL
- Contrôle d'autorisation par rôle des servlets, des beans enterprise et des MBeans
- Propagation des identités (RunAs)
- Registre d'utilisateurs commun
- Méthode d'authentification

Autres informations liées à la sécurité qui définissent le fonctionnement d'un domaine de sécurité, notamment :

- Protocole d'authentification (sécurité RMI/IIOP, c'est-à-dire l'invocation RMI sur IIOP)
- Autres attributs divers

Sécurité des applications

La sécurité des applications permet d'activer la sécurité pour les applications de votre environnement. Ce type de sécurité permet d'isoler les applications et d'appliquer l'authentification des utilisateurs des applications.

Dans les précédentes versions de WebSphere Process Server, lorsqu'un utilisateur activait la sécurité globale, cela activait la sécurité administrative et la sécurité des applications. La fonction de sécurité globale a été séparée en deux fonctions distinctes : la sécurité administrative et la sécurité des applications.

La sécurité administrative de WebSphere Process Server est activée par défaut. La sécurité des applications est également activée par défaut. La sécurité des applications est appliquée uniquement lorsque la sécurité administrative est activée.

Sécurité Java 2

La sécurité Java 2 fournit un mécanisme de contrôle d'accès à granularité plus fine, fondé sur des règles, qui permet d'améliorer l'intégrité de l'ensemble du système grâce à la vérification des droits d'accès avant d'autoriser l'accès à certaines ressources système protégées. La sécurité Java 2 protège l'accès aux ressources système, telles que les E-S de fichiers, les sockets et les propriétés. La sécurité Java

2 Platform, Enterprise Edition (J2EE) protège l'accès aux ressources Web comme les servlets, les fichiers JSP (JavaServer Pages), et les méthodes EJB (Enterprise JavaBeans).

La sécurité WebSphere Process Server inclut les technologies suivantes :

- Gestionnaire de sécurité Java 2 Security Manager
- Service JAAS (Java Authentication and Authorization Service)
- Entrées de données d'authentification Java 2 Connector
- Autorisation par rôle J2EE
- Configuration SSL (Secure Sockets Layer)

Comme la sécurité Java 2 est récente, de nombreuses applications (anciennes ou récentes) ne sont pas prêtes pour le modèle de programmation du contrôle d'accès à granularité fine que la sécurité Java 2 peut mettre en oeuvre. Les administrateurs doivent connaître les conséquences possibles de l'activation de la sécurité Java 2 lorsque les applications ne sont pas prêtes pour la sécurité Java 2. La sécurité Java 2 implique de nouvelles exigences pour les développeurs d'applications et les administrateurs.

Pour plus d'informations sur la sécurité Java 2, consultez les rubriques connexes.

Information associée

 Sécurité Java 2

Configuration d'un référentiel de comptes utilisateur

Les noms d'utilisateur et les mots de passe des utilisateurs enregistrés sont stockés dans un référentiel de comptes utilisateur. Vous pouvez utiliser soit le référentiel de comptes utilisateur du système d'exploitation local (option par défaut), le registre LDAP (Lightweight Directory Access Protocol) et des référentiels fédérés, soit un référentiel de comptes personnalisé.

A propos de cette tâche

Le référentiel de comptes utilisateur est le registre des utilisateurs et des groupes que le mécanisme d'authentification consulte pour procéder à une authentification. Sélectionnez un référentiel de comptes utilisateur dans la console d'administration.

Remarque : Windows Linux UNIX i5/OS Dans un environnement de déploiement réseau, vous devez utiliser LDAP comme registre d'utilisateurs.

Procédure

1. Accédez au panneau Administration, applications et infrastructure sécurisées dans la console d'administration. Développez **Sécurité**, puis cliquez sur **Administration, applications et infrastructure sécurisées**.
2. Sélectionnez le registre d'utilisateurs que vous voulez utiliser.

Le tableau suivant décrit les différents registres d'utilisateurs et les opérations à effectuer pour le sélectionner et le configurer.

Registre d'utilisateurs	Action
Référentiels fédérés	<p>Indiquez ce paramètre pour gérer des profils dans plusieurs référentiels sous un domaine unique. Le domaine peut se composer d'identités dans :</p> <ul style="list-style-type: none"> • Le référentiel de fichiers intégré au système • Un ou plusieurs référentiels • Le référentiel de fichiers intégré et un ou plusieurs référentiels externes <p>Remarque : Seul un utilisateur disposant de droits d'administration peut visualiser la configuration des référentiels fédérés. Pour plus d'informations, voir <i>Managing the realm in a federated repository configuration</i>.</p>
Système d'exploitation local	<p>Il s'agit du registre d'utilisateurs par défaut.</p> <p>Suivre les instructions de la section «Configuration du référentiel de comptes utilisateur personnalisé autonome ou du système d'exploitation local».</p> <p>Remarque : N'utilisez pas le système d'exploitation local comme registre d'utilisateurs dans un environnement de déploiement réseau.</p>
Lightweight Directory Access Protocol (LDAP)	<p>Suivez les instructions de la section Configuration du protocole LDAP en tant que registre d'utilisateurs pour configurer le protocole LDAP comme registre d'utilisateurs.</p>
Registre d'utilisateurs personnalisé	<p>Suivez les instructions de la section «Configuration du référentiel de comptes utilisateur personnalisé autonome ou du système d'exploitation local» pour sélectionner un référentiel de comptes personnalisé et le configurer selon vos besoins.</p>
Tivoli Access Manager	<p>Remarque : Cette option n'est pas disponible via la console d'administration. Elle doit être configurée à l'aide de la commande <code>wsadmin</code>.</p>

Concepts associés

«Initiation à la sécurité», à la page 3

La sécurité doit être prise en compte lors de la planification de l'installation de WebSphere Process Server, lors du développement et du déploiement d'applications et dans les opérations quotidiennes de votre serveur de processus.

Configuration du référentiel de comptes utilisateur personnalisé autonome ou du système d'exploitation local

Vous pouvez configurer votre référentiel de comptes utilisateur à l'aide de la console d'administration. Les étapes de configuration du système d'exploitation local (par défaut) ou d'un référentiel de comptes utilisateur personnalisé autonome sont similaires.

A propos de cette tâche

Vous pouvez choisir d'autoriser WebSphere Process Server à générer automatiquement une identité utilisateur de serveur ou vous pouvez en indiquer une issue du référentiel de comptes utilisateur que vous utilisez. Cette dernière option améliore l'auditabilité des opérations d'administration.

Procédure

1. A partir de la console d'administration, ouvrez la page de configuration pour votre registre d'utilisateurs.
Développez **Sécurité**, cliquez sur **Administration, applications et infrastructure sécurisées**, puis sélectionnez le registre d'utilisateurs que vous utilisez dans le menu **Définitions de domaines disponibles**. Cliquez sur **Configurer**.
2. Facultatif : Entrez un nom d'utilisateur valide dans la zone **Nom de l'utilisateur administratif primaire**.
Cette valeur est le nom d'un utilisateur possédant des droits d'administration qui est défini dans le registre. Ce nom d'utilisateur est utilisé pour accéder à la console d'administration. Il est également utilisé par la commande wsadmin.
3. Sélectionnez soit l'option **Identité de serveur générée automatiquement**, soit l'option **Identité de serveur stockée dans un référentiel**.
 - Si vous sélectionnez **Identité de serveur générée automatiquement**, le serveur d'applications génère l'identité de serveur utilisée pour la communication de processus interne.
Vous pouvez modifier cette identité de serveur sur la page Mécanismes et expiration de l'authentification. Pour accéder à la page Mécanismes et expiration de l'authentification, cliquez sur **Sécurité** → **Administration, applications et infrastructure sécurisées** → **Mécanismes et expiration de l'authentification**. Modifiez la valeur de la zone **ID de serveur interne**.
 - Si vous sélectionnez l'option **Identité de serveur stockée dans un référentiel**, entrez les informations suivantes :
 - Pour **ID de l'utilisateur du serveur ou de l'utilisateur administrateur sur un noeud version 6.0.x**, indiquez un ID utilisateur utilisé pour exécuter le serveur d'applications pour la sécurité.
 - Pour **Mot de passe**, indiquez le mot de passe associé à cet utilisateur.
4. Facultatif : Pour les registres personnalisés autonomes uniquement, procédez comme suit :
 - a. Vérifiez que la valeur de **Nom de classe du registre personnalisé** est correcte ou modifiez-la si nécessaire.
 - b. Cochez ou décochez **Ignorer la casse pour l'authentification**.
Lorsque vous sélectionnez cette option, la vérification de l'autorisation n'est pas sensible à la casse.
5. Cliquez sur **Appliquer**.
6. En bas de la page Administration, applications et infrastructure sécurisées, cliquez sur **Définir comme courant**.
7. Cliquez sur **OK** puis soit sur **Appliquer**, soit sur **Enregistrer**.

Configuration de WebSphere Process Server pour utiliser Tivoli Access Manager comme référentiel de comptes utilisateur

Vous pouvez utiliser Tivoli Access Manager comme référentiel de comptes utilisateur. Vous devez cependant le configurer à l'aide de la commande wsadmin, en dehors de la console d'administration.

A propos de cette tâche

Tivoli Access Manager peut être utilisé comme référentiel de comptes utilisateur. Vous ne pouvez pas le configurer dans la console d'administration mais devez utiliser la commande wsadmin. Reportez-vous à la rubrique suivante du centre de documentation de WebSphere Application Server : Transmission des règles de sécurité des applications installées à un fournisseur JACC à l'aide de wsadmin.

Configuration du protocole LDAP en tant que registre d'utilisateurs

Par défaut, le registre d'utilisateurs est le registre du système d'exploitation local. Vous pouvez également, si vous préférez, utiliser un protocole LDAP externe comme registre d'utilisateurs.

Avant de commencer

Cette tâche considère que vous avez activé la sécurité administrative.

Pour accéder à un registre d'utilisateurs à l'aide du protocole LDAP, vous devez connaître un nom d'utilisateur (ID) et un mot de passe valides, le serveur hôte et le port du serveur de registre, le nom distinctif et, le cas échéant, le nom distinctif de liaison et le mot de passe de liaison.

Dans un environnement de déploiement réseau, vous devez utiliser le protocole LDAP.

Vous pouvez sélectionner n'importe quel utilisateur valide dans le registre d'utilisateurs consultable. Vous pouvez utiliser n'importe quel ID utilisateur ayant le rôle d'administrateur pour vous connecter.

Procédure

1. Démarrez la console d'administration.
 - Si la sécurité est actuellement désactivée, vous êtes invité à entrer un ID utilisateur. Connectez-vous à l'aide d'un ID utilisateur.
 - Si la sécurité est actuellement activée, vous êtes invité à saisir un ID utilisateur et un mot de passe. Connectez-vous à l'aide de l'ID utilisateur et du mot de passe d'un compte administrateur prédéfini.
2. Développez **Sécurité**, puis cliquez sur **Administration, applications et infrastructure sécurisées**.
3. Sur la page Administration, applications et infrastructure sécurisées, procédez comme suit :
 - a. Vérifiez que l'option **Activer la sécurité administrative** est sélectionnée.
 - b. Dans la liste **Définitions de domaines disponibles**, sélectionnez **Registre LDAP autonome**.
 - c. Cliquez sur **Configurer**.
4. Sur l'onglet **Configuration** de la page Registre LDAP autonome, procédez comme suit :
 - a. Entrez un nom d'utilisateur valide dans la zone **Nom de l'utilisateur administratif primaire**.

Cette valeur est le nom d'un utilisateur possédant des droits d'administration qui est défini dans le registre. Ce nom d'utilisateur est utilisé pour accéder à la console d'administration. Il est également utilisé par la commande wsadmin.

Vous pouvez soit entrer le nom distinctif complet de l'utilisateur, soit le nom abrégé de l'utilisateur, tels que définis par le filtre utilisateur sur la page des paramètres LDAP avancés.

- b. Facultatif : Sélectionnez soit l'option **Identité de serveur générée automatiquement**, soit l'option **Identité de serveur stockée dans un référentiel**.

- Si vous sélectionnez **Identité de serveur générée automatiquement**, le serveur d'applications génère l'identité de serveur utilisée pour la communication de processus interne.

Vous pouvez modifier cette identité de serveur sur la page Mécanismes et expiration de l'authentification. Pour accéder à la page Mécanismes et expiration de l'authentification, cliquez sur **Sécurité** → **Administration, applications et infrastructure sécurisées** → **Mécanismes et expiration de l'authentification**. Modifiez la valeur de la zone **ID de serveur interne**.

- Si vous sélectionnez l'option **Identité de serveur stockée dans un référentiel**, entrez les informations suivantes :
 - Pour **ID de l'utilisateur du serveur ou de l'utilisateur administrateur sur un noeud version 6.0.x**, indiquez un ID utilisateur utilisé pour exécuter le serveur d'applications pour la sécurité.
 - Pour **Mot de passe**, indiquez le mot de passe associé à cet utilisateur.

Bien que cet ID ne soit pas l'ID utilisateur de l'administrateur LDAP, cette entrée doit être présente dans LDAP.

- c. Facultatif : Sélectionnez le serveur LDAP à utiliser dans la liste **Type de serveur LDAP**.

Le type de serveur LDAP détermine les filtres par défaut utilisés par WebSphere Process Server. Ces filtres par défaut changent la zone **Type de serveur LDAP en Personnalisé**, qui indique que des filtres personnalisés sont utilisés. Cette action se produit après avoir cliqué sur **OK** ou sur **Appliquer** sur la pages des paramètres LDAP avancés. Sélectionnez le type **Personnalisé** dans la liste et modifiez les filtres d'utilisateur et de groupe pour utiliser d'autres serveurs LDAP, si nécessaire.

Les utilisateurs IBM Tivoli Directory Server peuvent sélectionner **IBM Tivoli Directory Server** comme type d'annuaire. Pour obtenir de meilleures performances, utilisez le type d'annuaire IBM Tivoli Directory Server.

- d. Dans la zone **Hôte**, entrez le nom qualifié complet de l'ordinateur hébergeant LDAP.

Vous pouvez entrer soit l'adresse IP, soit le nom du système de nom de domaine.

- e. Facultatif : Dans la zone **Port**, entrez le numéro de port sur lequel le serveur LDAP écoute.

Le nom d'hôte et le numéro de port représentent le domaine de ce serveur LDAP dans la cellule WebSphere Process Server. Ainsi, si des serveurs se trouvant dans des cellules différentes communiquent entre eux à l'aide de jetons d'authentification LTPA, ces domaines doivent correspondre de façon exacte dans toutes les cellules.

La valeur par défaut est 389.

Si plusieurs serveurs WebSphere Process Server sont installés et configurés afin d'être exécutés dans le même domaine SSO (single sign-on) ou si WebSphere Process Server interagit avec une version précédente de WebSphere Process Server, il est alors important que le numéro de port corresponde à toutes les configurations.

- f. Facultatif : Entrez le nom distinctif dans la zone **Nom distinctif de base**.

Le nom distinctif de base définit le point de départ des recherches LDAP dans ce serveur d'annuaire LDAP. Par exemple, pour un utilisateur ayant comme nom distinctif cn=John Doe, ou=Rochester, o=IBM, c=US, définissez le nom distinctif de base avec l'une des options suivantes (à partir d'un suffixe c=us) : ou=Rochester, o=IBM, c=us or o=IBM c=us ou c=us.

Dans le cadre des autorisations, cette zone est sensible à la casse. Par conséquent, lors de la réception d'un jeton, par exemple, d'une autre cellule ou d'un serveur Lotus Domino, le nom distinctif de base sur le serveur doit correspondre exactement à celui de l'autre cellule ou de l'autre serveur Domino. Si vous ne voulez pas prendre en compte le respect de la casse pour l'autorisation, activez l'option **Ignorer la casse pour l'autorisation**.

Dans WebSphere Process Server, le nom distinctif est normalisé en fonction des spécifications du protocole LDAP (Lightweight Directory Access Protocol). La normalisation consiste à supprimer les espaces dans le nom distinctif avant ou après les virgules ou les signes égal. Exemple de nom distinctif de base non normalisé : o = ibm, c = us or o=ibm, c=us. Exemple de nom distinctif de base normalisé : o=ibm,c=us.

Cette option est obligatoire pour tous les annuaires LDAP (Lightweight Directory Access Protocol) à l'exception de Lotus Domino Directory, pour lequel elle est facultative.

- g. Facultatif : entre le nom distinctif de liaison dans la zone **Nom distinctif de liaison**.

Le nom distinctif de liaison est obligatoire si les liaisons anonymes ne sont pas possibles sur le serveur LDAP pour obtenir les informations d'utilisateur et de groupe.

Si le serveur LDAP est défini pour utiliser des liaisons anonymes, laissez cette zone vide. Si vous n'indiquez pas de nom, le serveur d'applications effectue une liaison anonyme. Reportez-vous à la description de la zone Nom distinctif de base pour obtenir des exemples de noms distinctifs.

- h. Facultatif : Entrez le mot de passe correspondant au nom distinctif de liaison dans la zone **Mot de passe de liaison**.

- i. Facultatif : Modifiez la valeur **Délai d'attente de la recherche**.

Cette valeur de délai d'attente indique le délai maximal attendu par le serveur LDAP pour envoyer une réponse au client produit avant d'arrêter la demande. La valeur par défaut est 120 secondes.

- j. Vérifiez que l'option **Réutiliser la connexion** est sélectionnée.

Cette option indique que le serveur doit réutiliser la connexion LDAP. Ne désélectionnez cette option que dans de rares cas, lorsqu'un routeur est utilisé pour envoyer des demandes à plusieurs serveurs LDAP et que le routeur ne prend pas en charge l'affinité. Gardez cette option sélectionnée dans les autres cas.

- k. Facultatif : Vérifiez que l'option **Ignorer la casse pour l'autorisation** est activée.

Lorsque vous activez cette option, la vérification de l'autorisation n'est pas sensible à la casse.

Normalement, une vérification de l'autorisation implique la vérification du nom distinctif complet d'un utilisateur, qui est unique sur le serveur LDAP et sensible à la casse. Cependant, lorsque vous utilisez soit IBM Directory Server, soit les serveurs Sun ONE (anciennement iPlanet) Directory Server LDAP, vous devez activer cette option car la casse des informations de groupe obtenues auprès des serveurs LDAP n'est pas cohérente. Cette

incohérence n'affecte que la vérification de l'autorisation. Sinon, cette zone est facultative et peut être activée lorsqu'une vérification d'autorisation sensible à la casse est nécessaire.

Par exemple, vous pouvez sélectionner cette option lorsque vous utilisez des certificats et que le contenu des certificats ne correspond pas à la casse de l'entrée sur le serveur LDAP. Vous pouvez également activer l'option **Ignorer la casse pour l'autorisation** lorsque vous utilisez une connexion unique entre le produit et Lotus Domino.

Par défaut, elle est activée.

- l. Facultatif : Sélectionnez **Couche SSL activée** si vous voulez utiliser les communications de couche Secure Sockets Layer avec le serveur LDAP.

Si vous sélectionnez l'option **Couche SSL activée**, vous pouvez sélectionner soit **Géré de façon centrale**, soit **Utiliser un alias SSL spécifique**.

- **Géré de façon centrale**

Cette option vous permet de définir une configuration SSL pour une portée donnée. Par exemple, la cellule, le noeud, le serveur ou le cluster en un seul emplacement. Pour utiliser l'option **Géré de façon centrale**, vous devez définir la configuration SSL pour l'ensemble de noeuds finaux spécifique.

La page Gérer les configurations de sécurité des noeuds finaux affiche tous les noeuds finaux entrants et sortants qui utilisent le protocole SSL.

Développez la section **Entrant** ou la section **Sortant** de la page Gérer les configurations de sécurité des noeuds finaux et cliquez sur le nom d'un noeud pour définir une configuration SSL utilisée pour les tous les noeuds finaux de ce noeud. Dans le cas d'un registre LDAP, vous pouvez remplacer la configuration SSL héritée en définissant une configuration SSL pour LDAP.

- **Utiliser un alias SSL spécifique**

Cette option permet de sélectionner l'une des configurations SSL de la liste affichée sous l'option.

Cette configuration n'est utilisée que lorsque la couche SSL est activée pour LDAP. La valeur par défaut est **NodeDefaultSSLSettings**.

- m. Cliquez sur **OK** puis soit sur **Appliquer**, soit sur **Enregistrer** pour revenir à la page Administration, applications et infrastructure sécurisées.
5. Sur la page Administration, applications et infrastructure sécurisées, cliquez sur **Définir comme courant**.
6. Cliquez sur **OK** puis soit sur **Appliquer**, soit sur **Enregistrer**.

Que faire ensuite

Enregistrez, arrêtez et redémarrez tous les serveurs pour que les mises à jour puissent prendre effet.

Si le serveur démarre sans problème, la configuration est correcte.

Démarrage et arrêt du serveur

Lorsque la sécurité administrative est activée, vous devez utiliser le nom d'utilisateur et le mot de passe appropriés pour pouvoir arrêter le serveur. Il n'est pas nécessaire de vous authentifier pour démarrer le serveur, mais vous devez le faire pour accéder à la console d'administration.

Avant de commencer

La sécurité administrative doit être activée.

Procédure

1. Démarrez le serveur.

Le tableau suivant décrit les options de démarrage du serveur.

Démarrer le serveur	Procédure
Depuis l'interface Premiers pas	Cliquez sur Démarrer le serveur.
Depuis une ligne de commande	Entrez : <ul style="list-style-type: none">• Windows Sous Windows : <code>startserver nom_serveur</code>• Linux UNIX Sous Linux et UNIX : <code>startserver.sh nom_serveur</code>• i5/OS Sous System i (à partir de la ligne de commande QShell) : <code>startserver nom_serveur</code> à l'invite de commande dans le répertoire <code>répertoire_installation/bin</code>.

Remarque : Il n'est pas nécessaire de saisir un nom d'utilisateur et un mot de passe pour démarrer le serveur. Cependant, vous devrez vous authentifier pour pouvoir lancer la console d'administration ou effectuer une tâche d'administration.

Le serveur démarre ou un message d'erreur est affiché.

2. Arrêter le serveur.

Le tableau suivant décrit les options d'arrêt du serveur.

Arrêter le serveur	Procédure
Depuis l'interface Premiers pas	Cliquez sur Arrêter le serveur et entrez un nom d'utilisateur et un mot de passe valides lorsque le système vous y invite. Le nom d'utilisateur doit appartenir au groupe des opérateurs ou des administrateurs.
Depuis une ligne de commande	Entrez : <ul style="list-style-type: none">• Windows Sous Windows : <code>stopserver nom_serveur -profileName nom_profil -username nom_utilisateur -password mot_de_passe</code>• Linux UNIX Sous Linux et UNIX : <code>stopserver.sh nom_serveur -profileName nom_profil -username nom_utilisateur -password mot_de_passe</code>• i5/OS Sous System i (à partir de la ligne de commande QShell) : <code>stopserver nom_serveur -profileName nom_profil -username nom_utilisateur -password mot_de_passe</code> à l'invite de commande dans le répertoire <code>répertoire_installation/bin</code>. Le nom d'utilisateur saisi doit être membre du rôle opérateur ou administrateur.

Remarque : Vous devez saisir un nom d'utilisateur et un mot de passe pour arrêter le serveur.

Si le nom d'utilisateur et le mot de passe que vous avez entrés appartiennent au groupe des opérateurs ou des administrateurs, le serveur s'arrête.

3. Vérifier que le serveur s'est arrêté correctement

Le tableau suivant décrit les options de vérification de l'arrêt du serveur.

Vérifier que le serveur s'est arrêté correctement	Procédure
Depuis l'interface utilisateur	La fenêtre Premiers pas affiche les résultats de votre demande.
Depuis une ligne de commande	Le résultat de votre demande est affiché dans la fenêtre de commande dans laquelle vous l'avez faite.

Rôles de sécurité

Plusieurs rôles de sécurité administrative sont définis lors de l'installation de WebSphere Process Server.

Sept rôles sont définis sur la console d'administration. Ces rôles accordent des droits à des groupes de fonctionnalités de la console d'administration. Si la sécurité administrative est activée, un utilisateur doit être mappé à l'un de ces sept rôles afin d'accéder à la console d'administration.

Le premier utilisateur qui se connecte au serveur après l'installation est associé au rôle d'administrateur.

Tableau 2. Rôles de sécurité

Rôle de sécurité	Description
Moniteur	Un moniteur peut visualiser la configuration de WebSphere Process Server et l'état en cours du serveur.
Configurateur	Un configurateur peut modifier la configuration de WebSphere Process Server.
Opérateur	Un membre du rôle opérateur dispose des privilèges d'un moniteur, plus la capacité de modifier l'état d'exécution du serveur (c'est-à-dire démarrer et arrêter le serveur).
Administrateur	Un administrateur dispose à la fois des droits d'un configurateur et d'un opérateur, plus quelques privilèges qui sont propres à ce rôle. Par exemple : <ul style="list-style-type: none">• Modifier l'ID utilisateur et le mot de passe du serveur• Mapper les utilisateurs et les groupes vers le rôle d'administrateur L'administrateur dispose également des droits requis pour accéder à des informations sensibles, comme : <ul style="list-style-type: none">• Mot de passe LTPA• Clés

Tableau 2. Rôles de sécurité (suite)

Rôle de sécurité	Description
Adminsecuritymanager	Seuls les utilisateurs associés à ce rôle peuvent mapper les utilisateurs aux rôles d'administration. De plus, si la sécurité administrative est définie selon une granularité fine, seuls les utilisateurs associés à ce rôle peuvent gérer les groupes d'autorisation. Pour plus d'informations, voir Rôles d'administration.
Déployeur	Seuls les utilisateurs associés à ce rôle peuvent effectuer des opérations de configuration et d'exécution sur les applications.
iscadmins	<p>Ce rôle est disponible uniquement pour les utilisateurs de la console d'administration et pas pour les utilisateurs wsadmin. Les utilisateurs associés à ce rôle ont des droits d'administration leur permettant de gérer les utilisateurs et les groupes des référentiels fédérés. Par exemple, un utilisateur du rôle iscadmins peut effectuer les tâches suivantes :</p> <ul style="list-style-type: none"> • Création, mise à jour ou suppression d'utilisateurs dans la configuration des référentiels fédérés • Création, mise à jour ou suppression de groupes dans la configuration des référentiels fédérés

L'ID de serveur qui est indiqué lors de l'activation de la sécurité administrative est automatiquement mappé au rôle d'administrateur. Des utilisateurs et des groupes peuvent être ajoutés ou supprimés d'un rôle à tout moment via la console d'administration de WebSphere Process Server. Cependant, pour que ces modifications soient prises en compte, il est nécessaire de redémarrer le serveur. Pour faciliter l'administration du système, il est préférable de mapper un ou plusieurs groupes d'utilisateurs vers des rôles de sécurité, plutôt que des utilisateurs individuels. Le mappage d'un groupe d'utilisateurs vers un rôle de sécurité, ainsi que l'ajout ou la suppression d'utilisateurs dans un groupe, s'effectuent à l'extérieur de WebSphere Process Server et ne nécessitent donc pas de redémarrer le serveur.

Le gestionnaire d'événements ayant échoué peut être exploité par tous les utilisateurs dotés du rôle d'opérateur ou d'administrateur.

Les sélecteurs peuvent être configurés par tous les utilisateurs dotés du rôle de configurateur ou d'administrateur.

Outre le mappage d'utilisateurs ou de groupes, un sujet spécial peut également être mappé vers des rôles de sécurité. Un sujet spécial est une généralisation d'une classe d'utilisateurs particuliers.

- Le sujet spécial **AllAuthenticated** signifie que le contrôle d'accès du rôle d'administration garantit que l'utilisateur effectuant la requête est au moins authentifié.
- Le sujet spécial **Everyone** signifie que tous les utilisateurs, authentifiés ou non, peuvent effectuer l'opération, comme si la sécurité était désactivée.

Sécurité par défaut des composants installés

Plusieurs composants essentiels de WebSphere Process Server disposent d'informations de sécurité par défaut. Ces informations sont des alias vers lesquels les utilisateurs par défaut sont mappés et les rôles de sécurité pour lesquels les utilisateurs doivent disposer d'un droit d'accès pour pouvoir appeler ces composants.

Les composants Business Process Choreographer, Common Event Infrastructure et Service Component Architecture de WebSphere Process Server utilisent des alias prédéfinis pour l'authentification auprès des moteurs de messagerie et des bases de données. Lors de la création du profil, la valeur attribuée par défaut à ces alias d'authentification est l'identité et le mot de passe de l'administrateur principal. Vous devez configurer ces alias afin qu'ils correspondent à d'autres utilisateurs du référentiel de comptes utilisateur.

Alias d'authentification du Chorégraphe de processus métier

Les processus métier sont dotés d'alias d'authentification prédéfinis. Vous pouvez modifier ces alias à l'aide de la console d'administration.

Les alias figurant dans le tableau 3, à la page 25 sont utilisés pour appeler les composants, quelque soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 3. Alias d'authentification associés aux processus métier

Alias	Description	Information
BPEAuthDataAliasJMS_noeud_serveur	Utilisé pour effectuer une authentification avec le moteur de messagerie.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration de Business Process Choreographer de l'outil de gestion des profils.
BPEAuthDataAliasTypeBdD_noeud_serveur	Utilisé pour effectuer une authentification avec des bases de données.	Configurez les bases de données à l'aide des scripts fournis.

Le tableau 4 décrit les rôles RunAs créés pour les processus métier.

Tableau 4. Rôles RunAs associés aux processus métier

Rôle RunAs	Description	Information
JMSAPIUser	Utilisé par le bean géré par message de l'API JMS BFM dans bpecontainer.ear.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration de Business Process Choreographer de l'outil de gestion des profils.
EscalationUser	Utilisé par le bean géré par message task.ear.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration de Business Process Choreographer de l'outil de gestion des profils.

Le nom d'utilisateur que vous indiquez est ajouté au rôle RunAs.

Alias d'authentification Common Event Infrastructure

Common Event Infrastructure est doté d'alias d'authentification prédéfinis. Vous pouvez modifier ces alias à l'aide de la console d'administration.

Les alias figurant dans le tableau 5 sont utilisés pour appeler les composants, quelque soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 5. Alias d'authentification associés à Common Event Infrastructure

Alias	Description	Information
CommonEventInfrastructureJMSAuthAlias Remarque : L'alias réel ne contient pas d'espace.	Utilisé pour effectuer une authentification avec le moteur de messagerie.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration de Common Event Infrastructure de l'outil de gestion des profils.

Tableau 5. Alias d'authentification associés à Common Event Infrastructure (suite)

Alias	Description	Information
EventAuthAliasTypeBdD	Utilisé pour effectuer une authentification avec des bases de données.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration de Common Event Infrastructure de l'outil de gestion des profils.

Alias d'authentification de l'architecture SCA

L'architecture SCA est dotée d'un alias d'authentification prédéfini. Modifiez l'alias à l'aide de la console d'administration.

Dans tableau 6, l'alias permet d'appeler les composants, quelque soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 6. Alias d'authentification associé aux composants SCA

Alias	Description	Information
SCA_Auth_Alias	Utilisé pour effectuer une authentification avec le moteur de messagerie.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration SCA de l'outil de gestion des profils.

Contrôle d'accès dans les applications de tâches utilisateur et de processus métier

Le Chorégraphe de processus métier est installé lors de l'installation de WebSphere Process Server. Au cours de l'installation, les fichiers d'archive d'entreprise (EAR) ayant des rôles associés (pour le contrôle d'accès) sont installés. Human Task Manager utilise les rôles pour déterminer les fonctions d'un utilisateur d'un système de production.

Les fichiers EAR et les rôles associés sont indiqués dans tableau 7.

Tableau 7. Rôles et droits d'accès par défaut pour les fichiers EAR

Fichier EAR	Rôles	Droits d'accès par défaut	Remarques
bpecontainer.ear	BPESystem Administrator	Nom du groupe saisi lors de l'installation.	A accès à tous les processus métier et à toutes les opérations.
bpecontainer.ear	BPESystemMonitor	Tous les utilisateurs authentifiés	A accès aux opérations de lecture.
task.ear	TaskSystem Administrator	Nom du groupe saisi lors de l'installation.	A accès à toutes les tâches utilisateur.
task.ear	TaskSystemMonitor	Tous les utilisateurs authentifiés	A accès aux opérations de lecture.
Bpcexplorer.ear	WebClientUser	Tous les utilisateurs authentifiés	A accès à Business Process Choreographer Explorer.

Contrôle d'accès dans les applications Common Event Infrastructure

Common Event Infrastructure est installé lors de l'installation de WebSphere Process Server. Au cours de l'installation, le fichier EventServer.ear ayant des rôles associés (pour le contrôle d'accès) est installé.

Les rôles suivants sont associés au fichier EventServer.ear :

Rôles	Droits d'accès par défaut
eventAdministrator	Tous les utilisateurs authentifiés
eventConsumer	Tous les utilisateurs authentifiés
eventUpdater	Tous les utilisateurs authentifiés
eventCreator	Tous les utilisateurs authentifiés
catalogAdministrator	Tous les utilisateurs authentifiés
catalogReader	Tous les utilisateurs authentifiés

Configuration de la sécurité de WebSphere Process Server pour un serveur d'environnement de déploiement

La configuration de la sécurité d'une installation en environnement de déploiement de WebSphere Process Server implique des tâches telles que l'activation de la sécurité administrative et la configuration d'un registre des comptes utilisateur.

Concepts associés

«Initiation à la sécurité», à la page 3

La sécurité doit être prise en compte lors de la planification de l'installation de WebSphere Process Server, lors du développement et du déploiement d'applications et dans les opérations quotidiennes de votre serveur de processus.

Sécurisation d'un environnement de déploiement de WebSphere Process Server

La sécurité de votre environnement WebSphere Process Server est gérée dans la console d'administration. Un utilisateur disposant de droits d'accès appropriés peut activer ou désactiver toutes les fonctions de sécurité des applications depuis la console d'administration. Il est donc capital que vous sécurisiez l'environnement avant de déployer des applications sécurisées.

Avant de commencer

Vous devez avoir installé WebSphere Process Server et vérifié l'installation avant de commencer à effectuer les opérations ci-dessous.

A propos de cette tâche

Votre environnement WebSphere Process Server est défini dans un profil. Ouvrez la console d'administration pour le profil que vous souhaitez sécuriser. Connectez-vous à la console en utilisant n'importe quel ID utilisateur ; dans la mesure où le profil est sécurisé, tous les noms d'utilisateur seront acceptés.

La procédure suivante fournit une feuille de route pour les tâches à effectuer pour activer la sécurité. Vous trouverez des informations détaillées spécifiques pour ces tâches dans les rubriques suivantes.

Procédure

1. Assurez-vous que la sécurité administrative est activée. «Activation de la sécurité», à la page 10.
2. Assurez-vous que la sécurité applicative est activée. «Sécurisation des applications dans WebSphere Process Server», à la page 46.
3. Ajoutez des utilisateurs ou des groupes au rôle administratif. Vous pouvez accorder des droits d'administration à des utilisateurs individuels ou à un groupe d'utilisateurs en suivant respectivement **Rôles de l'utilisateur administratif** ou **Rôles du groupe administratif**.
4. Sélectionnez le référentiel de comptes utilisateur que vous voulez utiliser.
Le tableau suivant décrit les différents registres d'utilisateurs et les opérations à effectuer pour le sélectionner et le configurer.

Registre d'utilisateurs	Action
Référentiels fédérés	Indiquez ce paramètre pour gérer des profils dans plusieurs référentiels sous un domaine unique. Le domaine peut se composer d'identités dans : <ul style="list-style-type: none">• Le référentiel de fichiers intégré au système• Un ou plusieurs référentiels• Le référentiel de fichiers intégré et un ou plusieurs référentiels externes Remarque : Seul un utilisateur disposant de droits d'administration peut visualiser la configuration des référentiels fédérés. Pour plus d'informations, voir <i>Managing the realm in a federated repository configuration</i> .
Système d'exploitation local	Registre d'utilisateurs par défaut. Pour plus de détails sur la configuration du registre de comptes utilisateur, voir «Configuration du référentiel de comptes utilisateur personnalisé autonome ou du système d'exploitation local», à la page 15.
Registre LDAP autonome	Suivez les instructions de la section Configuration du protocole LDAP en tant que registre d'utilisateurs pour configurer le protocole LDAP comme registre d'utilisateurs.
Registre personnalisé autonome	Pour plus de détails sur la configuration du registre de comptes utilisateur, voir «Configuration du référentiel de comptes utilisateur personnalisé autonome ou du système d'exploitation local», à la page 15.

5. Assurez-vous d'avoir défini le registre sélectionné comme étant votre registre courant.
Si vous ne l'avez pas déjà fait, cliquez sur **Défini comme courant** en bas de la page Administration, applications et infrastructure sécurisées.
6. Assurez-vous d'avoir appliqué les modifications après avoir sélectionné le registre d'utilisateurs.
Si vous ne l'avez pas déjà fait, cliquez sur **Appliquer** en bas de la page Administration, applications et infrastructure sécurisées.

7. Accédez au panneau Sécurité Business Integration. Cliquez sur **Sécurité**, puis sur **Sécurité Business Integration**.
8. Fournissez les identités utilisateur appropriées pour les alias d'authentification répertoriés. Les données d'identification que vous indiquez doivent exister dans le référentiel de comptes utilisateur que vous utilisez. Il est important pour la sécurité du système de choisir des identités utilisateur appropriées comme alias d'authentification.
9. Dans le même panneau, vous pouvez configurer la sécurité pour Business Process Choreographer.
Définissez les mappages de rôles utilisateur de Business Process Choreographer pour les gestionnaires Business Flow Manager et Human Task Manager :
 - **Administrateur** : Noms d'utilisateur et/ou noms de groupe liés au rôle d'administrateur de flux métier et de tâches utilisateur. Les utilisateurs qui se voient affecter ce rôle disposent de tous les privilèges.
 - **Superviseur** : Noms d'utilisateur et/ou noms de groupe liés au rôle de surveillance des flux métier et tâches utilisateur. Les utilisateurs associés à ce rôle peuvent visualiser les propriétés de tous les processus métier et objets de tâches.Les alias d'authentification de Business Process Choreographer peuvent être configurés pour chaque cible de déploiement sur laquelle Business Process Choreographer a été installé. Les alias d'authentification répertoriés sont les suivants :
 - **Authentification d'API JMS** : Authentification permettant au bean géré par message du gestionnaire de flux métier de traiter les appels asynchrones émis par les interfaces de programme d'application.
 - **Authentification d'utilisateur d'escalade** : Authentification permettant au bean géré par message du gestionnaire de tâches utilisateur de traiter les appels asynchrones émis par les interfaces de programme d'application.
10. Validez ces modifications.
Cliquez sur le bouton **Valider** dans la partie inférieure du panneau.
11. Enregistrez les modifications dans la configuration locale.
Cliquez sur **Sauvegarder** dans la fenêtre de message.
12. Assurez-vous que les informations de sécurité sont transmises aux noeuds de la cellule.
Développez **Administration système** dans la console d'administration, puis cliquez sur **Noeuds**. Cliquez sur **Resynchronisation complète**.
13. Si nécessaire, arrêtez et redémarrez le serveur.
Si le serveur doit être redémarré, un message s'affiche dans la console d'administration.

Résultats

A votre prochaine connexion à la console d'administration, vous devrez fournir un nom d'utilisateur et un mot de passe valides.

Que faire ensuite

Chaque profil créé doit être sécurisé de cette manière. L'identité de l'administrateur système a peut-être été utilisée à plusieurs emplacements au cours de l'installation et de la configuration de l'environnement. Il est conseillé de remplacer cette identité par des données d'identification de l'utilisateur

appropriées issues du référentiel de comptes utilisateur pour toutes les fonctions à l'exception des fonctions principales de sécurité. Le panneau **Sécurité Business Integration** de la console d'administration permet de gérer ces identités et alias.

Tâches associées


«Activation de la sécurité», à la page 10

La première étape du processus de sécurisation de votre environnement WebSphere Process Server et de vos applications est l'activation de la sécurité administrative.

«Sécurisation des applications dans WebSphere Process Server», à la page 46

Les applications que vous déployez dans votre instance de WebSphere Process Server requièrent que les fonctions de sécurité soient intégrées et appliquées au moment de leur exécution.

Information associée

 Utilisation des outils de vérification de l'installation avec WebSphere Process Server

Activation de la sécurité

La première étape du processus de sécurisation de votre environnement WebSphere Process Server et de vos applications est l'activation de la sécurité administrative.

Avant de commencer

Installez WebSphere Process Server et vérifiez l'installation avant de commencer à effectuer les opérations ci-dessous.

Ouvrez la console d'administration pour le profil que vous souhaitez sécuriser. Connectez-vous à la console en utilisant n'importe quel ID utilisateur ; dans la mesure où le profil est sécurisé, tous les noms d'utilisateur seront acceptés.

A propos de cette tâche

Pour plus d'informations sur la sécurité administrative, la sécurité des applications et la sécurité Java 2, reportez-vous aux informations répertoriées sous **Sous-rubriques**.

Procédure

1. Ouvrez le panneau de sécurité administrative dans la console d'administration. Développez **Sécurité**, puis cliquez sur **Administration, applications et infrastructure sécurisées**.
2. Procéder à l'activation de la sécurité administrative. Sélectionnez **Activer la sécurité administrative**.
3. Activez la sécurité des applications. Sélectionnez **Activer la sécurité des applications**.
4. Facultatif : Appliquez la sécurité Java 2, si nécessaire. Sélectionnez **Utiliser la sécurité Java 2 pour limiter l'accès aux applications des ressources locales** pour appliquer le contrôle des droits de sécurité Java 2.

Lorsque la sécurité Java 2 est activée, une application nécessitant plus de droits de sécurité Java 2 que la politique par défaut n'en accorde, peut ne pas s'exécuter correctement. Les droits nécessaires doivent alors être définis dans le fichier app.policy ou le fichier was.policy de l'application. Des exceptions de contrôle d'accès sont générées par les applications qui ne disposent pas des

droits requis. Pour plus d'informations sur la sécurité Java 2, consultez la rubrique relative à la configuration des fichiers de règles de sécurité Java 2 du Centre de documentation de WebSphere Application Server.

Remarque : Les mises à jour du fichier app.policy ne s'appliquent qu'aux applications d'entreprise du noeud auquel appartient ce fichier app.policy.

- a. Facultatif : Sélectionnez **Prévenir si des applications accordent des permissions personnalisées**. Le fichier filter.policy contient une liste de droits d'accès qu'une application ne doit pas posséder conformément à la spécification J2EE 1.3. Si une application est installée avec un droit d'accès indiqué dans ce fichier de règles et que cette option est activée, un avertissement est émis. Par défaut, elle est activée.
 - b. Facultatif : Sélectionnez **Limiter l'accès aux données d'authentification des ressources**. Activez cette option si vous devez restreindre l'accès des applications à des données sensibles d'authentification de mappage Java Connector Architecture (JCA).
5. Validez ces modifications.
Cliquez sur le bouton **Valider** dans la partie inférieure du panneau.
 6. Enregistrez les modifications dans la configuration locale.
Cliquez sur **Sauvegarder** dans la fenêtre de message.
 7. Si nécessaire, arrêtez et redémarrez le serveur.
Si le serveur doit être redémarré, un message s'affiche dans la console d'administration.

Que faire ensuite

Vous devez activer la sécurité administrative pour chaque profil que vous créez.

Concepts associés

«Initiation à la sécurité», à la page 3

La sécurité doit être prise en compte lors de la planification de l'installation de WebSphere Process Server, lors du développement et du déploiement d'applications et dans les opérations quotidiennes de votre serveur de processus.

Tâches associées

«Sécurisation des applications dans WebSphere Process Server», à la page 46

Les applications que vous déployez dans votre instance de WebSphere Process Server requièrent que les fonctions de sécurité soient intégrées et appliquées au moment de leur exécution.

Information associée

 Configuration des fichiers de règles de sécurité Java 2

Sécurité administrative

La sécurité administrative détermine si la sécurité est utilisée, le type de registre sur lequel effectuer l'authentification, ainsi que d'autres fonctions, qui sont souvent associées à une valeur par défaut. Lors de la planification, si l'activation de la sécurité n'est pas définie de façon appropriée, cela peut bloquer l'accès à la console d'administration ou entraîner l'arrêt du serveur.

La sécurité administrative constitue un "commutateur central" qui active différents paramètres de sécurité pour WebSphere Process Server. Vous pouvez définir les valeurs de ces paramètres, mais elles ne sont appliquées que lorsque la sécurité administrative est activée. Ces paramètres concernent notamment l'authentification des utilisateurs, l'utilisation de la couche SSL (Secure Sockets Layer) et la sélection

du référentiel des comptes utilisateur. La sécurité des applications, notamment l'authentification et les autorisations par rôle, n'est appliquée que lorsque la sécurité administrative est active. La sécurité administrative est activée par défaut.

La sécurité administrative est la configuration de la sécurité appliquée à l'ensemble du domaine de sécurité. Un domaine de sécurité est constitué de tous les serveurs configurés avec le même nom de domaine de registre d'utilisateurs. Dans certains cas, le domaine peut être le nom de l'ordinateur d'un registre de système d'exploitation local. Dans ce cas, tous les serveurs d'application doivent se trouver sur la même machine physique. Dans d'autres cas, le domaine peut être le nom de l'ordinateur d'un registre LDAP autonome.

La configuration peut inclure plusieurs noeuds car vous pouvez accéder à distance aux registres d'utilisateurs qui prennent en charge le protocole LDAP. Vous pouvez donc activer l'authentification depuis n'importe quel emplacement.

Une condition doit être remplie dans un domaine de sécurité : l'ID d'accès renvoyé par le registre ou le référentiel d'un serveur du domaine de sécurité doit être identique à l'ID d'accès renvoyé par le registre ou le référentiel de tout autre serveur du même domaine de sécurité. L'ID d'accès est l'identification unique d'un utilisateur utilisée lors de l'autorisation pour déterminer si l'accès à la ressource est autorisé.

La configuration de la sécurité administrative s'applique à chaque serveur du domaine de sécurité.

Pourquoi activer la sécurité administrative ?

L'activation de la sécurité d'administration permet d'activer les paramètres protégeant votre ordinateur des utilisateurs non autorisés. La sécurité administrative est activée par défaut lors de la création du profil. Dans certains environnements (comme un système de développement), l'activation de la sécurité n'est pas nécessaire. Sur ces systèmes, vous pouvez désactiver la sécurité administrative. Cependant, dans la plupart des environnements il est préférable d'empêcher les utilisateurs non autorisés d'accéder à la console d'administration et aux applications métier. La sécurité administrative doit être activée de façon à restreindre l'accès.

Quelle protection apporte la sécurité administrative ?

La configuration de la sécurité administrative d'un domaine de sécurité implique la configuration des technologies suivantes :

- Authentification des clients HTTP
- Authentification des clients IIOP
- Sécurité de la console d'administration
- Sécurité de la dénomination
- Utilisation des transports SSL
- Contrôle d'autorisation par rôle des servlets, des beans enterprise et des MBeans
- Propagation des identités (RunAs)
- Registre d'utilisateurs commun
- Méthode d'authentification

Autres informations liées à la sécurité qui définissent le fonctionnement d'un domaine de sécurité, notamment :

- Protocole d'authentification (sécurité RMI/IIOP, c'est-à-dire l'invocation RMI sur IIOP)
- Autres attributs divers

Sécurité des applications

La sécurité des applications permet d'activer la sécurité pour les applications de votre environnement. Ce type de sécurité permet d'isoler les applications et d'appliquer l'authentification des utilisateurs des applications.

Dans les précédentes versions de WebSphere Process Server, lorsqu'un utilisateur activait la sécurité globale, cela activait la sécurité administrative et la sécurité des applications. La fonction de sécurité globale a été séparée en deux fonctions distinctes : la sécurité administrative et la sécurité des applications.

La sécurité administrative de WebSphere Process Server est activée par défaut. La sécurité des applications est également activée par défaut. La sécurité des applications est appliquée uniquement lorsque la sécurité administrative est activée.

Sécurité Java 2

La sécurité Java 2 fournit un mécanisme de contrôle d'accès à granularité plus fine, fondé sur des règles, qui permet d'améliorer l'intégrité de l'ensemble du système grâce à la vérification des droits d'accès avant d'autoriser l'accès à certaines ressources système protégées. La sécurité Java 2 protège l'accès aux ressources système, telles que les E-S de fichiers, les sockets et les propriétés. La sécurité Java 2 Platform, Enterprise Edition (J2EE) protège l'accès aux ressources Web comme les servlets, les fichiers JSP (JavaServer Pages), et les méthodes EJB (Enterprise JavaBeans).

La sécurité WebSphere Process Server inclut les technologies suivantes :

- Gestionnaire de sécurité Java 2 Security Manager
- Service JAAS (Java Authentication and Authorization Service)
- Entrées de données d'authentification Java 2 Connector
- Autorisation par rôle J2EE
- Configuration SSL (Secure Sockets Layer)

Comme la sécurité Java 2 est récente, de nombreuses applications (anciennes ou récentes) ne sont pas prêtes pour le modèle de programmation du contrôle d'accès à granularité fine que la sécurité Java 2 peut mettre en oeuvre. Les administrateurs doivent connaître les conséquences possibles de l'activation de la sécurité Java 2 lorsque les applications ne sont pas prêtes pour la sécurité Java 2. La sécurité Java 2 implique de nouvelles exigences pour les développeurs d'applications et les administrateurs.

Pour plus d'informations sur la sécurité Java 2, consultez les rubriques connexes.

Information associée

 Sécurité Java 2

Configuration d'un référentiel de comptes utilisateur

Les noms d'utilisateur et les mots de passe des utilisateurs enregistrés sont stockés dans un référentiel de comptes utilisateur. Vous pouvez utiliser soit le référentiel de comptes utilisateur du système d'exploitation local (option par défaut), le registre LDAP (Lightweight Directory Access Protocol) et des référentiels fédérés, soit un référentiel de comptes personnalisé.

A propos de cette tâche

Le référentiel de comptes utilisateur est le registre des utilisateurs et des groupes que le mécanisme d'authentification consulte pour procéder à une authentification. Sélectionnez un référentiel de comptes utilisateur dans la console d'administration.

Remarque : Windows Linux UNIX i5/OS Dans un environnement de déploiement réseau, vous devez utiliser LDAP comme registre d'utilisateurs.

Procédure

1. Accédez au panneau Administration, applications et infrastructure sécurisées dans la console d'administration. Développez **Sécurité**, puis cliquez sur **Administration, applications et infrastructure sécurisées**.
2. Sélectionnez le registre d'utilisateurs que vous voulez utiliser.

Le tableau suivant décrit les différents registres d'utilisateurs et les opérations à effectuer pour le sélectionner et le configurer.

Registre d'utilisateurs	Action
Référentiels fédérés	<p>Indiquez ce paramètre pour gérer des profils dans plusieurs référentiels sous un domaine unique. Le domaine peut se composer d'identités dans :</p> <ul style="list-style-type: none">• Le référentiel de fichiers intégré au système• Un ou plusieurs référentiels• Le référentiel de fichiers intégré et un ou plusieurs référentiels externes <p>Remarque : Seul un utilisateur disposant de droits d'administration peut visualiser la configuration des référentiels fédérés. Pour plus d'informations, voir <i>Managing the realm in a federated repository configuration</i>.</p>
Système d'exploitation local	<p>Il s'agit du registre d'utilisateurs par défaut.</p> <p>Suivre les instructions de la section «Configuration du référentiel de comptes utilisateur personnalisé autonome ou du système d'exploitation local», à la page 15.</p> <p>Remarque : N'utilisez pas le système d'exploitation local comme registre d'utilisateurs dans un environnement de déploiement réseau.</p>

Registre d'utilisateurs	Action
Lightweight Directory Access Protocol (LDAP)	Suivez les instructions de la section Configuration du protocole LDAP en tant que registre d'utilisateurs pour configurer le protocole LDAP comme registre d'utilisateurs.
Registre d'utilisateurs personnalisé	Suivez les instructions de la section «Configuration du référentiel de comptes utilisateur personnalisé autonome ou du système d'exploitation local», à la page 15 pour sélectionner un référentiel de comptes personnalisé et le configurer selon vos besoins.
Tivoli Access Manager	Remarque : Cette option n'est pas disponible via la console d'administration. Elle doit être configurée à l'aide de la commande wsadmin.

Concepts associés

«Initiation à la sécurité», à la page 3

La sécurité doit être prise en compte lors de la planification de l'installation de WebSphere Process Server, lors du développement et du déploiement d'applications et dans les opérations quotidiennes de votre serveur de processus.

Configuration du référentiel de comptes utilisateur personnalisé autonome ou du système d'exploitation local

Vous pouvez configurer votre référentiel de comptes utilisateur à l'aide de la console d'administration. Les étapes de configuration du système d'exploitation local (par défaut) ou d'un référentiel de comptes utilisateur personnalisé autonome sont similaires.

A propos de cette tâche

Vous pouvez choisir d'autoriser WebSphere Process Server à générer automatiquement une identité utilisateur de serveur ou vous pouvez en indiquer une issue du référentiel de comptes utilisateur que vous utilisez. Cette dernière option améliore l'auditabilité des opérations d'administration.

Procédure

1. A partir de la console d'administration, ouvrez la page de configuration pour votre registre d'utilisateurs.

Développez **Sécurité**, cliquez sur **Administration, applications et infrastructure sécurisées**, puis sélectionnez le registre d'utilisateurs que vous utilisez dans le menu **Définitions de domaines disponibles**. Cliquez sur **Configurer**.

2. Facultatif : Entrez un nom d'utilisateur valide dans la zone **Nom de l'utilisateur administratif primaire**.

Cette valeur est le nom d'un utilisateur possédant des droits d'administration qui est défini dans le registre. Ce nom d'utilisateur est utilisé pour accéder à la console d'administration. Il est également utilisé par la commande wsadmin.

3. Sélectionnez soit l'option **Identité de serveur générée automatiquement**, soit l'option **Identité de serveur stockée dans un référentiel**.

- Si vous sélectionnez **Identité de serveur générée automatiquement**, le serveur d'applications génère l'identité de serveur utilisée pour la communication de processus interne.
Vous pouvez modifier cette identité de serveur sur la page Mécanismes et expiration de l'authentification. Pour accéder à la page Mécanismes et expiration de l'authentification, cliquez sur **Sécurité** → **Administration, applications et infrastructure sécurisées** → **Mécanismes et expiration de l'authentification**. Modifiez la valeur de la zone **ID de serveur interne**.
- Si vous sélectionnez l'option **Identité de serveur stockée dans un référentiel**, entrez les informations suivantes :
 - Pour **ID de l'utilisateur du serveur ou de l'utilisateur administrateur sur un noeud version 6.0.x**, indiquez un ID utilisateur utilisé pour exécuter le serveur d'applications pour la sécurité.
 - Pour **Mot de passe**, indiquez le mot de passe associé à cet utilisateur.

4. Facultatif : Pour les registres personnalisés autonomes uniquement, procédez comme suit :
 - a. Vérifiez que la valeur de **Nom de classe du registre personnalisé** est correcte ou modifiez-la si nécessaire.
 - b. Cochez ou décochez **Ignorer la casse pour l'authentification**.
Lorsque vous sélectionnez cette option, la vérification de l'autorisation n'est pas sensible à la casse.
5. Cliquez sur **Appliquer**.
6. En bas de la page Administration, applications et infrastructure sécurisées, cliquez sur **Définir comme courant**.
7. Cliquez sur **OK** puis soit sur **Appliquer**, soit sur **Enregistrer**.

Configuration de WebSphere Process Server pour utiliser Tivoli Access Manager comme référentiel de comptes utilisateur

Vous pouvez utiliser Tivoli Access Manager comme référentiel de comptes utilisateur. Vous devez cependant le configurer à l'aide de la commande wsadmin, en dehors de la console d'administration.

A propos de cette tâche

Tivoli Access Manager peut être utilisé comme référentiel de comptes utilisateur. Vous ne pouvez pas le configurer dans la console d'administration mais devez utiliser la commande wsadmin. Reportez-vous à la rubrique suivante du centre de documentation de WebSphere Application Server : Transmission des règles de sécurité des applications installées à un fournisseur JACC à l'aide de wsadmin.

Configuration du protocole LDAP en tant que registre d'utilisateurs

Par défaut, le registre d'utilisateurs est le registre du système d'exploitation local. Vous pouvez également, si vous préférez, utiliser un protocole LDAP externe comme registre d'utilisateurs.

Avant de commencer

Cette tâche considère que vous avez activé la sécurité administrative.

Pour accéder à un registre d'utilisateurs à l'aide du protocole LDAP, vous devez connaître un nom d'utilisateur (ID) et un mot de passe valides, le serveur hôte et le port du serveur de registre, le nom distinctif et, le cas échéant, le nom distinctif de liaison et le mot de passe de liaison.

Dans un environnement de déploiement réseau, vous devez utiliser le protocole LDAP.

Vous pouvez sélectionner n'importe quel utilisateur valide dans le registre d'utilisateurs consultable. Vous pouvez utiliser n'importe quel ID utilisateur ayant le rôle d'administrateur pour vous connecter.

Procédure

1. Démarrez la console d'administration.
 - Si la sécurité est actuellement désactivée, vous êtes invité à entrer un ID utilisateur. Connectez-vous à l'aide d'un ID utilisateur.
 - Si la sécurité est actuellement activée, vous êtes invité à saisir un ID utilisateur et un mot de passe. Connectez-vous à l'aide de l'ID utilisateur et du mot de passe d'un compte administrateur prédéfini.
2. Développez **Sécurité**, puis cliquez sur **Administration, applications et infrastructure sécurisées**.
3. Sur la page Administration, applications et infrastructure sécurisées, procédez comme suit :
 - a. Vérifiez que l'option **Activer la sécurité administrative** est sélectionnée.
 - b. Dans la liste **Définitions de domaines disponibles**, sélectionnez **Registre LDAP autonome**.
 - c. Cliquez sur **Configurer**.
4. Sur l'onglet **Configuration** de la page Registre LDAP autonome, procédez comme suit :
 - a. Entrez un nom d'utilisateur valide dans la zone **Nom de l'utilisateur administratif primaire**.

Cette valeur est le nom d'un utilisateur possédant des droits d'administration qui est défini dans le registre. Ce nom d'utilisateur est utilisé pour accéder à la console d'administration. Il est également utilisé par la commande wsadmin.

Vous pouvez soit entrer le nom distinctif complet de l'utilisateur, soit le nom abrégé de l'utilisateur, tels que définis par le filtre utilisateur sur la page des paramètres LDAP avancés.
 - b. Facultatif : Sélectionnez soit l'option **Identité de serveur générée automatiquement**, soit l'option **Identité de serveur stockée dans un référentiel**.
 - Si vous sélectionnez **Identité de serveur générée automatiquement**, le serveur d'applications génère l'identité de serveur utilisée pour la communication de processus interne.

Vous pouvez modifier cette identité de serveur sur la page Mécanismes et expiration de l'authentification. Pour accéder à la page Mécanismes et expiration de l'authentification, cliquez sur **Sécurité** → **Administration, applications et infrastructure sécurisées** → **Mécanismes et expiration de l'authentification**. Modifiez la valeur de la zone **ID de serveur interne**.
 - Si vous sélectionnez l'option **Identité de serveur stockée dans un référentiel**, entrez les informations suivantes :

- Pour **ID de l'utilisateur du serveur ou de l'utilisateur administrateur sur un noeud version 6.0.x**, indiquez un ID utilisateur utilisé pour exécuter le serveur d'applications pour la sécurité.
- Pour **Mot de passe**, indiquez le mot de passe associé à cet utilisateur.

Bien que cet ID ne soit pas l'ID utilisateur de l'administrateur LDAP, cette entrée doit être présente dans LDAP.

- c. Facultatif : Sélectionnez le serveur LDAP à utiliser dans la liste **Type de serveur LDAP**.

Le type de serveur LDAP détermine les filtres par défaut utilisés par WebSphere Process Server. Ces filtres par défaut changent la zone **Type de serveur LDAP** en **Personnalisé**, qui indique que des filtres personnalisés sont utilisés. Cette action se produit après avoir cliqué sur **OK** ou sur **Appliquer** sur la pages des paramètres LDAP avancés. Sélectionnez le type **Personnalisé** dans la liste et modifiez les filtres d'utilisateur et de groupe pour utiliser d'autres serveurs LDAP, si nécessaire.

Les utilisateurs IBM Tivoli Directory Server peuvent sélectionner **IBM Tivoli Directory Server** comme type d'annuaire. Pour obtenir de meilleures performances, utilisez le type d'annuaire IBM Tivoli Directory Server.

- d. Dans la zone **Hôte**, entrez le nom qualifié complet de l'ordinateur hébergeant LDAP.

Vous pouvez entrer soit l'adresse IP, soit le nom du système de nom de domaine.

- e. Facultatif : Dans la zone **Port**, entrez le numéro de port sur lequel le serveur LDAP écoute.

Le nom d'hôte et le numéro de port représentent le domaine de ce serveur LDAP dans la cellule WebSphere Process Server. Ainsi, si des serveurs se trouvant dans des cellules différentes communiquent entre eux à l'aide de jetons d'authentification LTPA, ces domaines doivent correspondre de façon exacte dans toutes les cellules.

La valeur par défaut est 389.

Si plusieurs serveurs WebSphere Process Server sont installés et configurés afin d'être exécutés dans le même domaine SSO (single sign-on) ou si WebSphere Process Server interagit avec une version précédente de WebSphere Process Server, il est alors important que le numéro de port corresponde à toutes les configurations.

- f. Facultatif : Entrez le nom distinctif dans la zone **Nom distinctif de base**.

Le nom distinctif de base définit le point de départ des recherches LDAP dans ce serveur d'annuaire LDAP. Par exemple, pour un utilisateur ayant comme nom distinctif cn=John Doe, ou=Rochester, o=IBM, c=US, définissez le nom distinctif de base avec l'une des options suivantes (à partir d'un suffixe c=us) : ou=Rochester, o=IBM, c=us or o=IBM c=us ou c=us.

Dans le cadre des autorisations, cette zone est sensible à la casse. Par conséquent, lors de la réception d'un jeton, par exemple, d'une autre cellule ou d'un serveur Lotus Domino, le nom distinctif de base sur le serveur doit correspondre exactement à celui de l'autre cellule ou de l'autre serveur Domino. Si vous ne voulez pas prendre en compte le respect de la casse pour l'autorisation, activez l'option **Ignorer la casse pour l'autorisation**.

Dans WebSphere Process Server, le nom distinctif est normalisé en fonction des spécifications du protocole LDAP (Lightweight Directory Access Protocol). La normalisation consiste à supprimer les espaces dans le nom distinctif avant ou après les virgules ou les signes égal. Exemple de nom

distinctif de base non normalisé : o = ibm, c = us or o=ibm, c=us. Exemple de nom distinctif de base normalisé : o=ibm,c=us.

Cette option est obligatoire pour tous les annuaires LDAP (Lightweight Directory Access Protocol) à l'exception de Lotus Domino Directory, pour lequel elle est facultative.

- g. Facultatif : entre le nom distinctif de liaison dans la zone **Nom distinctif de liaison**.

Le nom distinctif de liaison est obligatoire si les liaisons anonymes ne sont pas possibles sur le serveur LDAP pour obtenir les informations d'utilisateur et de groupe.

Si le serveur LDAP est défini pour utiliser des liaisons anonymes, laissez cette zone vide. Si vous n'indiquez pas de nom, le serveur d'applications effectue une liaison anonyme. Reportez-vous à la description de la zone Nom distinctif de base pour obtenir des exemples de noms distinctifs.

- h. Facultatif : Entrez le mot de passe correspondant au nom distinctif de liaison dans la zone **Mot de passe de liaison**.
- i. Facultatif : Modifiez la valeur **Délai d'attente de la recherche**. Cette valeur de délai d'attente indique le délai maximal attendu par le serveur LDAP pour envoyer une réponse au client produit avant d'arrêter la demande. La valeur par défaut est 120 secondes.
- j. Vérifiez que l'option **Réutiliser la connexion** est sélectionnée.

Cette option indique que le serveur doit réutiliser la connexion LDAP. Ne désélectionnez cette option que dans de rares cas, lorsqu'un routeur est utilisé pour envoyer des demandes à plusieurs serveurs LDAP et que le routeur ne prend pas en charge l'affinité. Gardez cette option sélectionnée dans les autres cas.

- k. Facultatif : Vérifiez que l'option **Ignorer la casse pour l'autorisation** est activée.

Lorsque vous activez cette option, la vérification de l'autorisation n'est pas sensible à la casse.

Normalement, une vérification de l'autorisation implique la vérification du nom distinctif complet d'un utilisateur, qui est unique sur le serveur LDAP et sensible à la casse. Cependant, lorsque vous utilisez soit IBM Directory Server, soit les serveurs Sun ONE (anciennement iPlanet) Directory Server LDAP, vous devez activer cette option car la casse des informations de groupe obtenues auprès des serveurs LDAP n'est pas cohérente. Cette incohérence n'affecte que la vérification de l'autorisation. Sinon, cette zone est facultative et peut être activée lorsqu'une vérification d'autorisation sensible à la casse est nécessaire.

Par exemple, vous pouvez sélectionner cette option lorsque vous utilisez des certificats et que le contenu des certificats ne correspond pas à la casse de l'entrée sur le serveur LDAP. Vous pouvez également activer l'option **Ignorer la casse pour l'autorisation** lorsque vous utilisez une connexion unique entre le produit et Lotus Domino.

Par défaut, elle est activée.

- l. Facultatif : Sélectionnez **Couche SSL activée** si vous voulez utiliser les communications de couche Secure Sockets Layer avec le serveur LDAP. Si vous sélectionnez l'option **Couche SSL activée**, vous pouvez sélectionner soit **Géré de façon centrale**, soit **Utiliser un alias SSL spécifique**.
- **Géré de façon centrale**

Cette option vous permet de définir une configuration SSL pour une portée donnée. Par exemple, la cellule, le noeud, le serveur ou le cluster en un seul emplacement. Pour utiliser l'option **Géré de façon centrale**, vous devez définir la configuration SSL pour l'ensemble de noeuds finaux spécifique.

La page Gérer les configurations de sécurité des noeuds finaux affiche tous les noeuds finaux entrants et sortants qui utilisent le protocole SSL. Développez la section **Entrant** ou la section **Sortant** de la page Gérer les configurations de sécurité des noeuds finaux et cliquez sur le nom d'un noeud pour définir une configuration SSL utilisée pour les tous les noeuds finaux de ce noeud. Dans le cas d'un registre LDAP, vous pouvez remplacer la configuration SSL héritée en définissant une configuration SSL pour LDAP.

- **Utiliser un alias SSL spécifique**

Cette option permet de sélectionner l'une des configurations SSL de la liste affichée sous l'option.

Cette configuration n'est utilisée que lorsque la couche SSL est activée pour LDAP. La valeur par défaut est **NodeDefaultSSLSettings**.

- m. Cliquez sur **OK** puis soit sur **Appliquer**, soit sur **Enregistrer** pour revenir à la page Administration, applications et infrastructure sécurisées.
5. Sur la page Administration, applications et infrastructure sécurisées, cliquez sur **Définir comme courant**.
 6. Cliquez sur **OK** puis soit sur **Appliquer**, soit sur **Enregistrer**.

Que faire ensuite

Enregistrez, arrêtez et redémarrez tous les serveurs pour que les mises à jour puissent prendre effet.

Si le serveur démarre sans problème, la configuration est correcte.

Démarrage et arrêt du serveur

Lorsque la sécurité administrative est activée, vous devez utiliser le nom d'utilisateur et le mot de passe appropriés pour pouvoir arrêter le serveur. Il n'est pas nécessaire de vous authentifier pour démarrer le serveur, mais vous devez le faire pour accéder à la console d'administration.

Avant de commencer

La sécurité administrative doit être activée.

Procédure

1. Démarrez le serveur.

Le tableau suivant décrit les options de démarrage du serveur.

Démarrer le serveur	Procédure
Depuis l'interface Premiers pas	Cliquez sur Démarrer le serveur.

Démarrer le serveur	Procédure
Depuis une ligne de commande	<p>Entrez :</p> <ul style="list-style-type: none"> • Windows Sous Windows : <code>startserver nom_serveur</code> • Linux UNIX Sous Linux et UNIX : <code>startserver.sh nom_serveur</code> • i5/OS Sous System i (à partir de la ligne de commande QShell) : <code>startserver nom_serveur</code> à l'invite de commande dans le répertoire <code>répertoire_installation/bin</code>.

Remarque : Il n'est pas nécessaire de saisir un nom d'utilisateur et un mot de passe pour démarrer le serveur. Cependant, vous devrez vous authentifier pour pouvoir lancer la console d'administration ou effectuer une tâche d'administration.

Le serveur démarre ou un message d'erreur est affiché.

2. Arrêter le serveur.

Le tableau suivant décrit les options d'arrêt du serveur.

Arrêter le serveur	Procédure
Depuis l'interface Premiers pas	Cliquez sur Arrêter le serveur et entrez un nom d'utilisateur et un mot de passe valides lorsque le système vous y invite. Le nom d'utilisateur doit appartenir au groupe des opérateurs ou des administrateurs.
Depuis une ligne de commande	<p>Entrez :</p> <ul style="list-style-type: none"> • Windows Sous Windows : <code>stopserver nom_serveur -profileName nom_profil -username nom_utilisateur -password mot_de_passe</code> • Linux UNIX Sous Linux et UNIX : <code>stopserver.sh nom_serveur -profileName nom_profil -username nom_utilisateur -password mot_de_passe</code> • i5/OS Sous System i (à partir de la ligne de commande QShell) : <code>stopserver nom_serveur -profileName nom_profil -username nom_utilisateur -password mot_de_passe</code> à l'invite de commande dans le répertoire <code>répertoire_installation/bin</code>. Le nom d'utilisateur saisi doit être membre du rôle opérateur ou administrateur.

Remarque : Vous devez saisir un nom d'utilisateur et un mot de passe pour arrêter le serveur.

Si le nom d'utilisateur et le mot de passe que vous avez entrés appartiennent au groupe des opérateurs ou des administrateurs, le serveur s'arrête.

3. Vérifier que le serveur s'est arrêté correctement

Le tableau suivant décrit les options de vérification de l'arrêt du serveur.

Vérifier que le serveur s'est arrêté correctement	Procédure
Depuis l'interface utilisateur	La fenêtre Premiers pas affiche les résultats de votre demande.
Depuis une ligne de commande	Le résultat de votre demande est affiché dans la fenêtre de commande dans laquelle vous l'avez faite.

Rôles de sécurité

Plusieurs rôles de sécurité administrative sont définis lors de l'installation de WebSphere Process Server.

Sept rôles sont définis sur la console d'administration. Ces rôles accordent des droits à des groupes de fonctionnalités de la console d'administration. Si la sécurité administrative est activée, un utilisateur doit être mappé à l'un de ces sept rôles afin d'accéder à la console d'administration.

Le premier utilisateur qui se connecte au serveur après l'installation est associé au rôle d'administrateur.

Tableau 8. Rôles de sécurité

Rôle de sécurité	Description
Moniteur	Un moniteur peut visualiser la configuration de WebSphere Process Server et l'état en cours du serveur.
Configurateur	Un configurateur peut modifier la configuration de WebSphere Process Server.
Opérateur	Un membre du rôle opérateur dispose des privilèges d'un moniteur, plus la capacité de modifier l'état d'exécution du serveur (c'est-à-dire démarrer et arrêter le serveur).
Administrateur	Un administrateur dispose à la fois des droits d'un configurateur et d'un opérateur, plus quelques privilèges qui sont propres à ce rôle. Par exemple : <ul style="list-style-type: none"> • Modifier l'ID utilisateur et le mot de passe du serveur • Mapper les utilisateurs et les groupes vers le rôle d'administrateur L'administrateur dispose également des droits requis pour accéder à des informations sensibles, comme : <ul style="list-style-type: none"> • Mot de passe LTPA • Clés

Tableau 8. Rôles de sécurité (suite)

Rôle de sécurité	Description
Adminsecuritymanager	Seuls les utilisateurs associés à ce rôle peuvent mapper les utilisateurs aux rôles d'administration. De plus, si la sécurité administrative est définie selon une granularité fine, seuls les utilisateurs associés à ce rôle peuvent gérer les groupes d'autorisation. Pour plus d'informations, voir Rôles d'administration.
Déployeur	Seuls les utilisateurs associés à ce rôle peuvent effectuer des opérations de configuration et d'exécution sur les applications.
iscadmins	Ce rôle est disponible uniquement pour les utilisateurs de la console d'administration et pas pour les utilisateurs wsadmin. Les utilisateurs associés à ce rôle ont des droits d'administration leur permettant de gérer les utilisateurs et les groupes des référentiels fédérés. Par exemple, un utilisateur du rôle iscadmins peut effectuer les tâches suivantes : <ul style="list-style-type: none"> • Création, mise à jour ou suppression d'utilisateurs dans la configuration des référentiels fédérés • Création, mise à jour ou suppression de groupes dans la configuration des référentiels fédérés

L'ID de serveur qui est indiqué lors de l'activation de la sécurité administrative est automatiquement mappé au rôle d'administrateur. Des utilisateurs et des groupes peuvent être ajoutés ou supprimés d'un rôle à tout moment via la console d'administration de WebSphere Process Server. Cependant, pour que ces modifications soient prises en compte, il est nécessaire de redémarrer le serveur. Pour faciliter l'administration du système, il est préférable de mapper un ou plusieurs groupes d'utilisateurs vers des rôles de sécurité, plutôt que des utilisateurs individuels. Le mappage d'un groupe d'utilisateurs vers un rôle de sécurité, ainsi que l'ajout ou la suppression d'utilisateurs dans un groupe, s'effectuent à l'extérieur de WebSphere Process Server et ne nécessitent donc pas de redémarrer le serveur.

Le gestionnaire d'événements ayant échoué peut être exploité par tous les utilisateurs dotés du rôle d'opérateur ou d'administrateur.

Les sélecteurs peuvent être configurés par tous les utilisateurs dotés du rôle de configurateur ou d'administrateur.

Outre le mappage d'utilisateurs ou de groupes, un sujet spécial peut également être mappé vers des rôles de sécurité. Un sujet spécial est une généralisation d'une classe d'utilisateurs particuliers.

- Le sujet spécial **AllAuthenticated** signifie que le contrôle d'accès du rôle d'administration garantit que l'utilisateur effectuant la requête est au moins authentifié.

- Le sujet spécial **Everyone** signifie que tous les utilisateurs, authentifiés ou non, peuvent effectuer l'opération, comme si la sécurité était désactivée.

Sécurité par défaut des composants installés

Plusieurs composants essentiels de WebSphere Process Server disposent d'informations de sécurité par défaut. Ces informations sont des alias vers lesquels les utilisateurs par défaut sont mappés et les rôles de sécurité pour lesquels les utilisateurs doivent disposer d'un droit d'accès pour pouvoir appeler ces composants.

Les composants Business Process Choreographer, Common Event Infrastructure et Service Component Architecture de WebSphere Process Server utilisent des alias prédéfinis pour l'authentification auprès des moteurs de messagerie et des bases de données. Lors de la création du profil, la valeur attribuée par défaut à ces alias d'authentification est l'identité et le mot de passe de l'administrateur principal. Vous devez configurer ces alias afin qu'ils correspondent à d'autres utilisateurs du référentiel de comptes utilisateur.

Alias d'authentification du Chorégraphe de processus métier

Les processus métier sont dotés d'alias d'authentification prédéfinis. Vous pouvez modifier ces alias à l'aide de la console d'administration.

Les alias figurant dans le tableau 3, à la page 25 sont utilisés pour appeler les composants, quelque soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 9. Alias d'authentification associés aux processus métier

Alias	Description	Information
BPEAuthDataAliasJMS_noeud_serveur	Utilisé pour effectuer une authentification avec le moteur de messagerie.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration de Business Process Choreographer de l'outil de gestion des profils.
BPEAuthDataAliasTypeBdD_noeud_serveur	Utilisé pour effectuer une authentification avec des bases de données.	Configurez les bases de données à l'aide des scripts fournis.

Le tableau 4, à la page 25 décrit les rôles RunAs créés pour les processus métier.

Tableau 10. Rôles RunAs associés aux processus métier

Rôle RunAs	Description	Information
JMSAPIUser	Utilisé par le bean géré par message de l'API JMS BFM dans bpecontainer.ear.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration de Business Process Choreographer de l'outil de gestion des profils.

Tableau 10. Rôles RunAs associés aux processus métier (suite)

Rôle RunAs	Description	Information
EscalationUser	Utilisé par le bean géré par message task.ear.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration de Business Process Choreographer de l'outil de gestion des profils.

Le nom d'utilisateur que vous indiquez est ajouté au rôle RunAs.

Alias d'authentification Common Event Infrastructure

Common Event Infrastructure est doté d'alias d'authentification prédéfinis. Vous pouvez modifier ces alias à l'aide de la console d'administration.

Les alias figurant dans le tableau 5, à la page 25 sont utilisés pour appeler les composants, quelque soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 11. Alias d'authentification associés à Common Event Infrastructure

Alias	Description	Information
CommonEventInfrastructure JMSAuthAlias Remarque : L'alias réel ne contient pas d'espace.	Utilisé pour effectuer une authentification avec le moteur de messagerie.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration de Common Event Infrastructure de l'outil de gestion des profils.
EventAuthAliasTypeBdD	Utilisé pour effectuer une authentification avec des bases de données.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration de Common Event Infrastructure de l'outil de gestion des profils.

Alias d'authentification de l'architecture SCA

L'architecture SCA est dotée d'un alias d'authentification prédéfini. Modifiez l'alias à l'aide de la console d'administration.

Dans tableau 6, à la page 26, l'alias permet d'appeler les composants, quelque soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 12. Alias d'authentification associé aux composants SCA

Alias	Description	Information
SCA_Auth_Alias	Utilisé pour effectuer une authentification avec le moteur de messagerie.	Indiquez un nom d'utilisateur et un mot de passe dans le panneau de configuration SCA de l'outil de gestion des profils.

Contrôle d'accès dans les applications de tâches utilisateur et de processus métier

Le Chorégraphe de processus métier est installé lors de l'installation de WebSphere Process Server. Au cours de l'installation, les fichiers d'archive d'entreprise (EAR)

ayant des rôles associés (pour le contrôle d'accès) sont installés. Human Task Manager utilise les rôles pour déterminer les fonctions d'un utilisateur d'un système de production.

Les fichiers EAR et les rôles associés sont indiqués dans tableau 7, à la page 26.

Tableau 13. Rôles et droits d'accès par défaut pour les fichiers EAR

Fichier EAR	Rôles	Droits d'accès par défaut	Remarques
bpecontainer.ear	BPSystemAdministrator	Nom du groupe saisi lors de l'installation.	A accès à tous les processus métier et à toutes les opérations.
bpecontainer.ear	BPSystemMonitor	Tous les utilisateurs authentifiés	A accès aux opérations de lecture.
task.ear	TaskSystemAdministrator	Nom du groupe saisi lors de l'installation.	A accès à toutes les tâches utilisateur.
task.ear	TaskSystemMonitor	Tous les utilisateurs authentifiés	A accès aux opérations de lecture.
Bpcexplorer.ear	WebClientUser	Tous les utilisateurs authentifiés	A accès à Business Process Choreographer Explorer.

Contrôle d'accès dans les applications Common Event Infrastructure

Common Event Infrastructure est installé lors de l'installation de WebSphere Process Server. Au cours de l'installation, le fichier EventServer.ear ayant des rôles associés (pour le contrôle d'accès) est installé.

Les rôles suivants sont associés au fichier EventServer.ear :

Rôles	Droits d'accès par défaut
eventAdministrator	Tous les utilisateurs authentifiés
eventConsumer	Tous les utilisateurs authentifiés
eventUpdater	Tous les utilisateurs authentifiés
eventCreator	Tous les utilisateurs authentifiés
catalogAdministrator	Tous les utilisateurs authentifiés
catalogReader	Tous les utilisateurs authentifiés

Sécurisation des applications dans WebSphere Process Server

Les applications que vous déployez dans votre instance de WebSphere Process Server requièrent que les fonctions de sécurité soient intégrées et appliquées au moment de leur exécution.

A propos de cette tâche

Les applications que vous hébergez dans votre environnement WebSphere Process Server exécutent différentes fonctions critiques nécessitant une sécurisation. Certaines applications accèdent à des informations sensibles, les transfèrent ou les modifient (par exemple, informations relatives aux bulletins de paie ou aux cartes

de crédit). D'autres effectuent des opérations de facturation ou de gestion des stocks. La sécurité de ces applications joue un rôle capital.

Sécurisez vos applications en effectuant les opérations suivantes :

Procédure

1. Assurez-vous que la sécurité administrative est activée.
2. Assurez-vous que la sécurité applicative est activée.
 - a. Dans la console d'administration, développez **Sécurité**, puis cliquez sur **Administration, applications et infrastructure sécurisées**.
 - b. Sélectionnez **Activer la sécurité des applications** afin que WebSphere Process Server exige une authentification des utilisateurs qui tentent d'accéder à une application sécurisée.
3. Développez vos applications dans WebSphere Integration Developer en utilisant l'ensemble des fonctions de sécurité prévues.
4. Déployez vos applications dans votre environnement WebSphere Process Server, en affectant les utilisateurs, individuels ou en groupes, à des rôles de sécurité appropriés.
5. Gérez la sécurité de votre environnement WebSphere Process Server.

Tâches associées

«Activation de la sécurité», à la page 10

La première étape du processus de sécurisation de votre environnement WebSphere Process Server et de vos applications est l'activation de la sécurité administrative.

Éléments de sécurité

Les applications qui s'exécutent dans WebSphere Process Server sont sécurisées par l'authentification et le contrôle d'accès. En outre, la sécurité des données transférées pendant l'appel d'une application est assurée par divers mécanismes ; ceux-ci garantissent que les données ne peuvent pas être lues, ni modifiées pendant leur transfert. Enfin, le dernier élément de sécurité est la propagation des informations de sécurité à travers différents systèmes, afin que l'utilisateur n'ait pas besoin d'entrer son nom d'utilisateur et son mot de passe plusieurs fois.

La sécurité dans WebSphere Process Server peut être divisée en trois grands groupes :

- Sécurité applicative
- Intégrité et confidentialité des données
- Propagation de l'identité

Sécurité applicative

La sécurité de vos applications WebSphere Process Server est assurée de deux façons :

- Authentification

L'utilisateur qui souhaite utiliser une application doit fournir un nom d'utilisateur et un mot de passe figurant dans le registre d'utilisateurs.

- Contrôle d'accès

Un utilisateur doit être autorisé à appeler une application. Les rôles sont associés à l'appel de l'application. Un utilisateur authentifié doit appartenir au rôle approprié pour que l'application puisse s'exécuter.

Intégrité et confidentialité des données

La sécurité des données auxquelles accède l'application est assurée aux points d'origine et de destination, ainsi que pendant leur transfert :

- Intégrité
Les données envoyées sur le réseau ne peuvent pas être modifiées pendant leur transfert.
- Confidentialité
Les données envoyées sur le réseau ne peuvent pas être interceptées et lues pendant leur transfert.

Propagation de l'identité

Le dernier élément de sécurité est la propagation de l'identité, qui est assurée par la méthode de l'authentification unique.

Lorsque la demande d'un client doit transiter par plusieurs systèmes au sein de l'entreprise, le client n'est pas obligé de s'authentifier plusieurs fois. La méthode de l'authentification unique est utilisée pour propager les données d'authentification aux systèmes en aval qui appliquent à leur tour le contrôle d'accès.

Authentification des utilisateurs

Si la sécurité administrative est activée, les clients doivent être authentifiés.

Si un client tente d'accéder à une application sécurisée sans être authentifié, une exception est générée.

Le tableau 14 répertorie les clients standards qui peuvent appeler les composants de WebSphere Process Server, ainsi que les options d'authentification disponibles pour chacun de ces clients.

Tableau 14. Options d'authentification pour les différents clients

Client	Options d'authentification	Remarques
Clients de services Web	Authentification WS-Security/SOAP	
Clients Web ou HTTP	Authentification HTTP de base (invite du navigateur à saisir un nom d'utilisateur et un mot de passe).	Ces clients utilisent des documents JavaServer Pages, servlet et HTML.
Clients Java	JAAS.	
Tous les clients	Authentification client SSL.	

Certains composants de l'infrastructure WebSphere Process Server sont dotés d'alias d'authentification utilisés pour authentifier le code d'exécution permettant d'accéder aux bases de données et au moteur de messagerie. Ces alias d'authentification Chorégraphe de processus métier et Common Event Infrastructure sont présentés dans les rubriques suivantes. Le responsable de l'installation de WebSphere Process Server collecte les noms d'utilisateurs et les mots de passe pour créer ces alias.

Certains composants d'exécution sont dotés de beans gérés par messages (MDB) configurés à l'aide d'un rôle RunAs. Le responsable de l'installation de WebSphere Process Server collecte les noms d'utilisateur et les mots de passe pour le rôle RunAs.

Modification des alias d'authentification :

Vous pouvez être amené à modifier les alias d'authentification existants.

A propos de cette tâche

Modifiez les alias d'authentification à partir de la console d'administration.

Procédure

1. Accédez au panneau Alias d'authentification de sécurité Business Integration.
Dans la console d'administration, cliquez sur **Sécurité**, puis sur **Sécurité Business Integration**.

Remarque : Vous pouvez également accéder à ce panneau à partir de divers panneaux de la console d'administration qui exigent des informations sur l'alias d'authentification.

Le panneau de configuration de l'alias d'authentification s'affiche.

Ce panneau contient une liste d'alias d'authentification, le composant associé, l'ID utilisateur associé à cet alias et, parfois, une description de l'alias.

2. Sélectionnez l'alias d'authentification que vous souhaitez modifier en cliquant sur son nom dans la colonne **Alias**.

Remarque : Dans certains cas, la colonne **Alias** peut ne pas contenir de lien. Dans ce cas, cochez la case de la colonne **Sélectionner** correspondant à l'alias que vous voulez éditer et cliquez sur **Editer**.

3. Modifiez les propriétés de l'alias.

Sur le panneau de configuration de l'alias d'authentification sélectionné, vous pouvez modifier soit le nom de l'alias, soit l'ID utilisateur et le mot de passe associés. Vous pouvez également modifier la description de l'entrée des données d'authentification.

4. Confirmez les modifications effectuées.

Cliquez sur **OK** ou sur **Valider**. Revenez au panneau Alias d'authentification de sécurité Business Integration et cliquez sur **Appliquer** pour appliquer vos modifications à la configuration principale.

Remarque : Pour une installation de Network Deployment, veillez à effectuer une opération de synchronisation de fichiers pour propager les modifications sur les autres noeuds.

Pour plus d'informations, voir *Augmentation de profils WebSphere Process Server avec sécurité*

Tâches associées

«Création de profils WebSphere Process Server avec sécurité», à la page 6
Lorsque vous créez un profil WebSphere Process Server, les valeurs par défaut sont utilisées pour les données d'identification de sécurité. Vous devez configurer ces paramètres de sécurité sur la console d'administration après avoir créé le profil.

Contrôle d'accès

Le contrôle d'accès permet de garantir qu'un utilisateur authentifié dispose des droits nécessaires pour accéder à des ressources ou effectuer une opération donnée.

Lorsqu'un utilisateur est authentifié dans WebSphere Process Server, il est important qu'il n'ait pas accès à toutes les opérations disponibles afin de garantir la sécurité. Permettre à certains utilisateurs d'effectuer certaines tâches, tout en refusant ces mêmes tâches à d'autres utilisateurs correspond au *Contrôle d'accès*.

Le contrôle d'accès peut être adapté à des composants en cours de développement, afin de les sécuriser. Pour cela, vous pouvez utiliser des qualifiants de l'architecture de composants de service lors de l'étape de développement. Pour plus d'informations, consultez le centre de documentation WebSphere Integration Developer.

Certains WebSphere Process Server composants, fournis sous forme de fichiers d'archive d'entreprise (EAR), sécurisent leurs opérations à l'aide de la sécurité basée sur des rôles J2EE. Vous trouverez des informations détaillées concernant ces composants.

Contrairement à la sécurité basée sur le rôle J2EE qui sécurise l'opération des composants, un contrôle d'accès basé sur les rôles sécurise les *ressources*. Par exemple, au sein de Business Calendar Manager, vous pouvez spécifier le type d'accès des utilisateurs par rapport aux plannings individuels. Vous pouvez utiliser le gestionnaire de sécurité dans Business Space pour spécifier, pour chaque planning, le propriétaire du planning ainsi que les utilisateurs ayant des droits d'accès en lecture et en écriture sur le planning.

Business Process Choreographer et Common Event Infrastructure font partie intégrante de WebSphere Process Server. La sécurité basée sur des rôles associée à ces composants est présentée en détails dans les rubriques suivantes.

Vous trouverez ci-dessous des informations détaillées concernant ces composants.

Tableau 15. Fichiers .ear et rôles J2EE associés

Fichier EAR	Rôle J2EE	Affectation utilisateur
BPCEplorer_<node>_<server>	CleanupUser	Tous les utilisateurs authentifiés
BPCObserver_<node>_<server>	ObserverUser	Tous les utilisateurs authentifiés
BPEContainer_<node>_<server>	BPEAPIUser	Tous les utilisateurs authentifiés
	BPESystemAdministrator	wsadmin
	BPESystemMonitor	wsadmin
	CleanupUser	Tous les utilisateurs authentifiés

Tableau 15. Fichiers .ear et rôles J2EE associés (suite)

Fichier EAR	Rôle J2EE	Affectation utilisateur
	JMSAPIUser	Tous les utilisateurs authentifiés
Passerelle de services REST	RestServicesUser	Tous les utilisateurs authentifiés
TaskContainer_<node>_<server>	TaskAPIUser	Tous les utilisateurs authentifiés
	TaskSystemAdministrator	wsadmin
	TaskSystemMonitor	wsadmin
	EscalationUser	Tous les utilisateurs authentifiés
	CleanupUser	Tous les utilisateurs authentifiés
wpsFEMgr_6.2.0	WBIOperator	Tous les utilisateurs
EventService (*)	eventAdministrator	Tous les utilisateurs authentifiés
	eventConsumer	Tous les utilisateurs authentifiés
	eventUpdater	Tous les utilisateurs authentifiés
	eventCreator	Tous les utilisateurs authentifiés
	catalogAdministrator	Tous les utilisateurs authentifiés
	catalogReader	Tous les utilisateurs authentifiés

(*) EventService est une application système et n'est pas répertoriée dans la console d'administration sous Applications d'entreprise.

Tâches associées

«Sécurité pour Business Calendar Manager», à la page 56

Le gestionnaire de sécurité vous permet de sécuriser l'accès à chaque planning dans Business Calendar Manager. Vous pouvez utiliser le gestionnaire de sécurité pour attribuer des rôles aux membres d'une organisation. Ce sont ces rôles qui déterminent le niveau d'accès aux plannings.

Information associée

 Centre de documentation de WebSphere Integration Developer

Intégrité et confidentialité des données

La confidentialité et l'intégrité des données auxquelles les processus WebSphere Process Server accèdent lorsqu'ils sont appelés sont des éléments essentiels de votre sécurité.

La confidentialité et l'intégrité des données sont des concepts très proches. Pour plus d'informations, consultez les rubriques connexes.

Confidentialité

La confidentialité signifie qu'il est impossible pour un utilisateur non authentifié d'intercepter et de lire des données.

Intégrité

L'intégrité signifie qu'il est impossible pour un utilisateur non authentifié de modifier des données.

Solutions proposées par WebSphere Process Server

WebSphere Process Server prend en charge deux solutions largement répandues pour gérer la confidentialité et l'intégrité des données :

- Protocole Secure Sockets Layer (SSL). SSL établit une liaison pour authentifier deux systèmes et échanger des informations permettant de générer la clé de session qui sera utilisée par les systèmes pour le chiffrement et le déchiffrement des données. SSL est un protocole synchrone, adapté à la communication point-à-point. SSL exige que les deux systèmes maintiennent leur connexion pendant la durée de la session SSL.
- WS-Security. Cette norme définit des extensions SOAP (Simple Object Access Control) pour sécuriser les messages SOAP. WS-Security renforce la prise en charge de l'authentification, de l'intégrité et de la confidentialité des données pour un message SOAP unique. A la différence de SSL, aucune liaison n'est établie pour générer une clé de session. Ainsi, WS-Security est approprié pour la sécurisation des messages en environnement asynchrone, tel que SOAP sur JMS (Java Message Service) ou SOAP sur SIB (Service Integration Bus). Vous pouvez définir les descripteurs de déploiement WS-Security dans vos applications avant le déploiement. Pour plus de détails, consultez les rubriques connexes.

Dans un environnement d'intégration composé de différents systèmes interdépendants, il est probable que certaines des communications établies seront asynchrones. C'est pourquoi WS-Security sera la plupart du temps la solution la mieux adaptée.

Information associée

- ➡ Présentation de la planification de sécurité
- ➡ Modification des propriétés du déploiement du module

Configuration d'un client de services Web pour l'utilisation de la couche SSL :

Vous pouvez configurer un client de services Web pour appeler un service Web utilisant la couche Secure Sockets Layer (SSL).

A propos de cette tâche

Pour plus de détails sur la configuration de votre client de services Web pour l'utilisation de la couche SSL, reportez-vous à cette note technique WebSphere Application Server. Vous trouverez des informations plus générales sur la sécurisation des services Web dans la rubrique WebSphere Application Server Securing Web services applications at the transport level.

Authentification unique

Un client ne doit fournir son nom d'utilisateur et son mot de passe qu'une seule fois. Son identité est ensuite propagée dans l'ensemble du système.

Lorsque la demande d'un client transite par plusieurs systèmes au sein de l'entreprise, le client ne doit s'authentifier qu'une fois. Ce concept de propagation de l'identité est assuré par la méthode de l'authentification unique.

Le contexte authentifié est propagé aux systèmes en aval, qui appliquent ensuite le contrôle d'accès.

Vous pouvez utiliser Tivoli Access Manager WebSEAL ou bien le plug-in pour serveurs Web Tivoli Access Manager en tant que serveur proxy inverse afin de fournir les fonctions de gestion des accès et d'authentification unique aux ressources de WebSphere Process Server. Pour des informations relatives à la configuration de ces outils, consultez la documentation de WebSphere Application Server.

Information associée

 Configuration de la fonction de connexion unique avec Tivoli Access Manager ou WebSEAL

Déploiement (installation) d'applications sécurisées

Le déploiement d'applications disposant de contraintes de sécurité (applications sécurisées) est similaire au déploiement d'applications sans contraintes de sécurité. La seule différence réside dans l'affectation éventuelle d'utilisateurs ou de groupes à des rôles dans le cas d'applications sécurisées, ce qui implique que le registre d'utilisateurs que vous utilisez est correct. Lorsque vous installez une application sécurisée, des rôles doivent y avoir été définis. Si l'application utilise la délégation, les rôles RunAs doivent également être définis ; en outre, un nom d'utilisateur et un mot de passe valides doivent être saisis.

Avant de commencer

Avant d'effectuer cette tâche, vérifiez que l'application que vous avez conçue, développée et assemblée comporte toutes les configurations de sécurité nécessaires. Pour plus d'informations sur ces tâches, consultez le centre de documentation de WebSphere Integration Developer. Dans ce contexte, nous considérons que le déploiement et l'installation de l'application ne constitue qu'une seule et même tâche.

A propos de cette tâche

L'une des étapes obligatoires du déploiement d'applications sécurisées est d'affecter des utilisateurs ou des groupes à des rôles qui ont été définis au moment de la construction de l'application. Cette tâche fait partie de l'étape intitulée "Mappage des rôles de sécurité vers les utilisateurs/groupes". Si vous avez utilisé un outil d'assemblage, vous avez peut-être déjà réalisé cette opération d'affectation. Dans ce cas, vous pouvez confirmer le mappage en effectuant cette opération. Vous pouvez ajouter de nouveaux utilisateurs ou groupes ; vous pouvez également modifier les informations existantes pendant cette étape.

Si un rôle RunAs a été défini dans l'application, celle-ci appellera des méthodes qui nécessitent d'avoir paramétré des identités pendant le déploiement. Utilisez le rôle RunAs pour spécifier l'identité sous laquelle les appels en aval seront effectués. Par exemple, si le rôle RunAs est affecté à l'utilisateur «bob» et que le client «alice» appelle un servlet qui appelle les beans enterprise. Si la fonction de délégation est activée, la méthode est appelée sur les beans enterprise sous l'identité «bob».

Dans le processus de déploiement, il est nécessaire d'affecter des utilisateurs ou de les modifier dans les rôles RunAs. Cette étape est intitulée "Mappage des rôles RunAs vers les utilisateurs". Utilisez cette étape pour affecter de nouveaux utilisateurs ou modifier des utilisateurs existants dans les rôles RunAs lorsque la règle de délégation est définie sur SpecifiedIdentity.

Les étapes décrites ci-dessous sont valables pour l'installation ou la modification d'une application. Si l'application contient des rôles, le lien **Mappage des rôles de sécurité vers les utilisateurs/groupe**s est affiché pendant l'installation de l'application (ou sa gestion), dans la section Propriétés supplémentaires.

Procédure

1. Dans la console d'administration, développez **Applications** et cliquez sur **Installation d'une nouvelle application**.
Effectuez les opérations nécessaires à l'installation des applications jusqu'à l'étape "Mappage des rôles de sécurité vers les utilisateurs/groupe
2. Affectez des utilisateurs et des groupes à des rôles.
3. Mappez les utilisateurs dans des rôles RunAs, si ce type de rôle existe dans l'application.
4. Cliquez sur **Utilisation correcte de l'identité système** pour spécifier les rôles RunAs, le cas échéant.
Effectuez cette opération si la fonction de délégation est définie pour utiliser l'identité système, ce qui n'est possible que pour les beans enterprise. L'identité système utilise l'ID du serveur de sécurité de WebSphere Process Server pour appeler les méthodes en aval. N'utilisez cet ID qu'avec une extrême prudence car il dispose de plus de droits d'accès aux méthodes internes de WebSphere Process Server. Cette tâche est utile au déployeur pour qu'il prenne connaissance des méthodes pour lesquelles l'identité système est définie pour la délégation et pour qu'il puisse les corriger éventuellement. Si aucune modification n'est nécessaire, ignorez cette étape.
5. Effectuez les autres opérations sans lien avec la sécurité pour achever l'installation et le déploiement de l'application.

Que faire ensuite

Après le déploiement d'une application sécurisée, vérifiez que les droits d'accès aux ressources sont correctement définis. Par exemple, si votre application dispose d'un module Web protégé, vérifiez que seuls les utilisateurs affectés à des rôles peuvent utiliser l'application.

Concepts associés

«Initiation à la sécurité», à la page 3

La sécurité doit être prise en compte lors de la planification de l'installation de WebSphere Process Server, lors du développement et du déploiement d'applications et dans les opérations quotidiennes de votre serveur de processus.

Information associée

 Affectation d'utilisateurs et de groupes à des rôles

 Affectation d'utilisateurs à des rôles RunAs

Affectation d'utilisateurs à des rôles

Une application sécurisée utilise un des deux (ou les deux) qualificatifs de sécurité securityPermission et securityIdentity. Lorsque ces deux qualificatifs sont utilisés,

des opérations supplémentaires doivent être effectuées au moment du déploiement afin que l'application et ses fonctions de sécurité fonctionnent correctement.

Avant de commencer

Cette tâche suppose que vous disposez d'une application sécurisée, en tant que fichier EAR, prête à être déployée dans WebSphere Process Server.

A propos de cette tâche

Les applications implémentent des interfaces dotées de méthodes. Vous pouvez sécuriser une interface ou une méthode avec le qualificatif SCA (Service Component Architecture) `securityPermission`. Lorsque vous appelez ce qualificatif, vous indiquez un rôle (par exemple, «superviseurs») qui dispose des droits appropriés pour appeler la méthode sécurisée. Au moment du déploiement de l'application, vous avez la possibilité d'affecter des utilisateurs au rôle spécifié.

Le qualificatif `securityIdentity` est équivalent au rôle `RunAs` utilisé pour les délégations dans WebSphere Application Server. La valeur associée à ce qualificatif est un rôle. Pendant le déploiement, le rôle est mappé vers une identité. L'appel d'un composant sécurisé avec `securityIdentity` utilise l'identité indiquée, quelle que soit l'identité de l'utilisateur qui appelle l'application.

Procédure

1. Suivez les instructions pour déployer une application dans WebSphere Process Server. Pour plus de détails, voir *Installation d'un module sur un serveur de production*.
2. Associez les utilisateurs aux rôles.

Qualificatif de sécurité	Opération à effectuer
Droit de sécurité	<p>Affectez un ou des utilisateurs au rôle spécifié. Quatre options sont possibles :</p> <ul style="list-style-type: none">• Tous les utilisateurs - Aucune sécurité.• Tous les utilisateurs authentifiés - Tous les utilisateurs authentifiés sont membres du rôle.• Utilisateurs mappés - Des utilisateurs individuels sont ajoutés au rôle.• Groupes mappés - Des groupes d'utilisateurs sont ajoutés au rôle. <p>La solution qui procure le plus de souplesse est Groupes mappés car les utilisateurs peuvent être ajoutés au groupe et ont ainsi accès à l'application, sans redémarrage du serveur.</p>
Identité de sécurité	<p>Définissez un nom d'utilisateur et un mot de passe valides pour l'identité vers laquelle le rôle est mappé.</p>

Concepts associés

«Initiation à la sécurité», à la page 3

La sécurité doit être prise en compte lors de la planification de l'installation de WebSphere Process Server, lors du développement et du déploiement d'applications et dans les opérations quotidiennes de votre serveur de processus.

Information associée

 Délégations

Sécurité pour Business Calendar Manager

Le gestionnaire de sécurité vous permet de sécuriser l'accès à chaque planning dans Business Calendar Manager. Vous pouvez utiliser le gestionnaire de sécurité pour attribuer des rôles aux membres d'une organisation. Ce sont ces rôles qui déterminent le niveau d'accès aux plannings.

Pour chaque planning au sein de Business Calendar Manager, vous pouvez attribuer des membres à l'un des trois rôles : propriétaire, rédacteur ou lecteur.

Le gestionnaire de sécurité, que vous utilisez pour administrer le contrôle d'accès basé sur les rôles pour Business Calendar Manager, se trouve dans Business Space qui repose sur WebSphere.

Cet accès basé sur les rôles pour Business Calendar Manager repose sur le langage XACML (eXtensible Access Control Markup Language), une norme ouverte.

Avantage de l'utilisation du gestionnaire de sécurité

Quels sont les avantages de l'utilisation du gestionnaire de sécurité pour le contrôle d'accès basé sur les rôles dans Business Calendar Manager ?

- Vous pouvez contrôler l'accès à une instance spécifique d'un planning.
Par exemple, vous pouvez spécifier qu'un utilisateur ne dispose que d'un accès à son propre planning et qu'il n'a pas la possibilité de consulter ou de modifier le planning d'un autre utilisateur.
- Le contrôle d'accès est accompli au niveau du rôle et non pas au niveau de l'utilisateur individuel.
Vous mappez des membres aux rôles. C'est le rôle qui définit le droit d'accès des membres à une instance spécifique d'une ressource.

Rôles associés à un planning

Lorsqu'un planning est installé, trois rôles sont créés : propriétaire, rédacteur et lecteur.

Comment ces rôles sont-ils utilisés ? Considérons le cas d'un planning de congés utilisé au sein d'une organisation. Vous souhaitez que tous les employés puissent avoir accès au planning, mais vous voulez limiter le nombre d'employés susceptibles de mettre à jour le planning.

Lorsque le planning de congés est installé, les rôles suivants sont créés :

- HolidayOwner
Les membres affectés à ce rôle disposent d'un droit en lecture et en écriture sur ce planning des congés. Par exemple, si l'entreprise a décidé d'ajouter un congé supplémentaire, un membre disposant du rôle HolidayOwner sera habilité à effectuer le changement.

Les membres de ce rôle peuvent également affecter d'autres membres aux rôles HolidayWriter et HolidayReader. Par exemple, un HolidayOwner peut décider d'ajouter un cadre supérieur au rôle HolidayWriter.

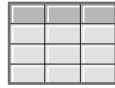
- HolidayWriter

Les membres affectés à ce rôle disposent d'un droit en lecture et en écriture sur ce planning des congés. Comme dans le cas du rôle holidayowner, les membres du rôle HolidayWriter peuvent ajouter des congés supplémentaires.

- HolidayReader

Les membres affectés à ce rôle disposent d'un droit en lecture sur ce planning des congés mais ne disposent pas d'un droit en écriture.

Vous pourriez attribuer le rôle HolidayOwner au responsable des ressources humaines, le rôle HolidayWriter à un groupe de personnes spécialisées dans la gestion des ressources humaines et le rôle HolidayReader aux employés, comme illustré dans la figure ci-dessous :



Planning des congés



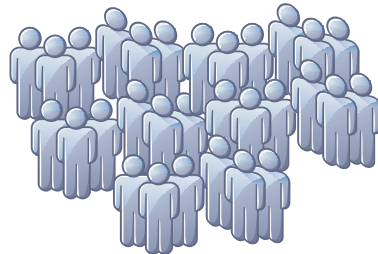
Peut voir et mettre à jour les congés.
Peut attribuer des rôles en écriture et lecture pour les congés.

Holiday.Owner=responsable RH



Peut voir et mettre à jour les congés.

Holiday.Writer=groupe des spécialistes RH



Peut voir les congés.

Holiday.Reader=groupe des employés

Figure 1. Exemple de rôles affectés à un planning

Lorsque vous déployez un planning, les trois rôles – propriétaire, rédacteur et lecteur – sont créés. Les droits octroyés pour tous les rôles sont initialement définis sur **All Authenticated (Tous les utilisateurs authentifiés)**. Assurez-vous de modifier cette définition pour affecter les membres de l'organisation aux rôles appropriés.

Remarque : Vous pouvez modifier l'appartenance à un rôle (par exemple, vous pouvez supprimer un membre du rôle lecteur), mais vous ne pouvez pas modifier le nom d'un rôle, ajouter ou supprimer un rôle ou modifier les droits associés à un rôle. Les droits sont définis de la manière suivante :

- Les membres du rôle Propriétaire ont un droit en lecture et en écriture sur le planning et peuvent affecter d'autres membres aux rôles Rédacteur et Lecteur.
- Les membres du rôle Rédacteur ont un droit en lecture et en écriture sur le planning.
- Les membres du rôle Lecteur ont un droit en lecture sur le planning.

Dans le gestionnaire de sécurité, ces rôles liés au planning sont également appelés *rôles de module*.

Rôles administratifs du gestionnaire de sécurité

Lorsque vous redémarrez le système après avoir installé WebSphere Process Server (ou après avoir procédé à une mise à niveau vers WebSphere Process Server 6.2), les rôles suivants sont créés :

- **BPMAdmin**

BPMAdmin a le droit d'ajouter des membres au rôle BPMRoleManager ou d'en retirer des membres.

Par exemple, si la personne chargée du rôle BPMRoleManager quitte l'organisation, seul BPMAdmin peut affecter un autre membre à ce rôle.

BPMAdmin est initialement affecté à un membre – l'utilisateur d'administration principal. Modifiez cette affectation et sélectionnez un autre membre dès que vous redémarrez le serveur après une installation ou une mise à niveau.

- **BPMRoleManager**

BPMRoleManager a le droit d'ajouter des membres aux trois rôles liés au planning (propriétaire, rédacteur et lecteur) ou d'en retirer.

Par exemple, si un planning de congés est créé, BPMRoleManager affecte des membres aux rôles HolidayOwner, HolidayWriter et HolidayReader.

BPMRoleManager est initialement affecté à un membre – l'utilisateur d'administration principal. Modifiez cette affectation et sélectionnez un autre membre dès que vous redémarrez le serveur après une installation ou une mise à niveau.

Remarque : Dans le gestionnaire de sécurité, ces rôles sont également appelés *rôles système*.

Configuration de rôles

Après avoir installé WebSphere Process Server, effectuez les tâches suivantes dans le gestionnaire de sécurité :

1. BPMAdmin réaffecte le rôle BPMRoleManager.
2. BPMRoleManager affecte les membres à l'un des trois rôles associés au planning.

Voir la rubrique d'aide du gestionnaire de sécurité pour plus d'informations sur la manière d'effectuer ces tâches.

Concepts associés

«Initiation à la sécurité», à la page 3

La sécurité doit être prise en compte lors de la planification de l'installation de WebSphere Process Server, lors du développement et du déploiement d'applications et dans les opérations quotidiennes de votre serveur de processus.

«Contrôle d'accès», à la page 50

Le contrôle d'accès permet de garantir qu'un utilisateur authentifié dispose des droits nécessaires pour accéder à des ressources ou effectuer une opération donnée.

 Business Space de technologie WebSphere

WebSphere Process Server comprend Business Space de technologie WebSphere, qui est une interface commune permettant aux utilisateurs des applications de créer, gérer et intégrer des interfaces Web sur toute la gamme IBM WebSphere Business Process Management.

Sécurité des adaptateurs

WebSphere Process Server prend en charge les types d'adaptateurs suivants : WebSphere Business Integration Adapters et WebSphere Adapters. Cette section traite de la sécurité pour ces deux types d'adaptateurs.

A propos de cette tâche

Un adaptateur est le mécanisme qu'utilise une application pour communiquer avec un système d'information d'entreprise EIS (Enterprise Information System). Les informations qui sont échangées entre une application et un système EIS peuvent être hautement confidentielles. Il est donc important de garantir la sécurité de cette transaction de données.

Les adaptateurs WebSphere Business Integration Adapters se composent d'un ensemble de logiciels, d'interfaces d'API et d'outils permettant à des applications d'échanger des données métier via un courtier d'intégration. Les adaptateurs WebSphere Business Integration Adapters sont basés sur la messagerie JMS (Java Message Service) et JMS ne prend pas en charge la propagation de contexte de sécurité.

WebSphere Adapters permet une connectivité bidirectionnelle et gérée entre un système d'information d'entreprise et des composants J2EE pris en charge par WebSphere Process Server.

Pour une communication entrante provenant des deux types d'adaptateurs vers WebSphere Process Server, il n'y a pas de mécanisme d'authentification. Dans le cadre de WebSphere Business Integration Adapters, le recours à la messagerie JMS exclut toute diffusion du contexte de sécurité. J2C ne dispose pas non plus de prise en charge au niveau de la sécurité des communications entrantes. De ce fait, WebSphere Adapters ne dispose pas non plus d'un mécanisme d'authentification pour les communications entrantes.

L'entrée d'un adaptateur vers WebSphere Process Server s'effectue toujours via une exportation d'architecture SCA. Cette exportation SCA doit être reliée à un composant SCA, tel qu'une médiation, un processus métier, un composant Java SCA ou un sélecteur.

Concernant la sécurité, la solution consiste à définir un rôle RunAs sur le composant qui est la cible de l'exportation WebSphere Adapter. Cette opération s'effectue via le qualificatif SCA SecurityIdentity lors de la phase de

développement (pour plus d'informations, voir le WebSphere Integration Developer centre de documentation de). Lorsque le composant s'exécute, il le fait alors sous l'identité définie dans le rôle RunAs.

La valeur de SecurityIdentity est un rôle et non un utilisateur. Néanmoins, lorsque le fichier EAR est déployé sur WebSphere Process Server, vous devez indiquer un nom d'utilisateur et un mot de passe pour l'identité qui doit être utilisée. Le recours à SecurityIdentity empêche la génération d'exceptions au cas où un composant situé en aval est sécurisé et exige que le client soit authentifié.

Remarque : L'utilisation de SecurityIdentity ne sécurise pas les communications entre l'adaptateur et le système EIS.

Les adaptateurs WebSphere Business Integration Adapter envoient des données à WebSphere Process Server sous forme de messages JMS via le bus d'intégration de services.

Les adaptateurs WebSphere Adapter résident dans la machine JVM de WebSphere Process Server, et donc, seules les communications entre l'adaptateur et le système EIS cible ont besoin d'être sécurisées. Le protocole utilisé entre l'adaptateur et EIS est propre à EIS. Consultez la documentation du système EIS pour savoir comment sécuriser cette liaison.

Concepts associés

 Remarques relatives à la sécurité pour les bus d'intégration de services

Sécurité des tâches utilisateur et des processus métier

Un certain nombre de rôles sont associés aux tâches utilisateur et aux processus métier. Cette rubrique décrit les rôles disponibles.

Par définition, les tâches utilisateur nécessitent une intervention humaine. Certains processus métier sont également susceptibles de nécessiter une intervention humaine. Ces tâches utilisateur et ces processus métier sont développés à l'aide de WebSphere Integration Developer et sont appelés via le Chorégraphe de processus métier. Lorsque vous développez une tâche ou un processus, vous devez attribuer des rôles à des utilisateurs ou des groupes concernés par les tâches utilisateurs et les processus métier. Pour plus d'informations sur l'attribution des rôles ou l'interrogation des rôles associés à des rôles spécifiques, consultez le centre de documentation de WebSphere Integration Developer .

Human Task Manager utilise les rôles pour déterminer les fonctions de chaque utilisateur d'un système de production.

Rôles associés aux tâches utilisateur et aux processus métier

Important : Ces rôles sont propres aux tâches et aux processus qui s'exécutent dans le conteneur de tâche utilisateur et le conteneur métier du Chorégraphe de processus métier.

WebSphere Process Server prend en charge les rôles suivants pour les tâches et les processus :

Administrateur

Les utilisateurs associés à ce rôle peuvent surveiller, terminer ou supprimer des tâches et des processus. Ils peuvent également afficher des informations concernant ces tâches et ces processus.

Lecteur

Les utilisateurs associés à ce rôle peuvent uniquement afficher des tâches et des processus.

Initiateur

Les utilisateurs associés à ce rôle peuvent lancer et afficher des tâches et des processus.

Les tâches sont également associés aux rôles suivants :

Propriétaire

Les utilisateurs associés à ce rôle peuvent sauvegarder, annuler, terminer ou afficher des tâches qu'ils ont déjà réclamées.

Propriétaire potentiel

Les utilisateurs associés à ce rôle peuvent réclamer ou afficher des tâches.

Concepts associés

☞ Autorisation et affectation d'utilisateur pour les processus

Information associée

☞ Autorisation et affectation d'utilisateur

Configuration de la sécurité de Business Space

Après avoir installé et configuré Business Space de technologie WebSphere pour votre produit, vous devez déterminer les options de sécurité de l'utilisation par votre équipe des artefact dans Business Space. Vous pouvez vouloir définir la sécurité des applications, qui nécessite également la sécurité administrative pour l'application. Vous devez également exécuter un script Jython pour affecter un rôle de superutilisateur pour Business Space.

Définition de la sécurité des applications de Business Space

Pour activer la sécurité de Business Space, vous devez activer la sécurité des applications et la sécurité administrative.

Avant de commencer

Avant d'effectuer cette tâche, vous devez effectuer les tâches suivantes :

- Configuration d'un profil et configuration de Business Space sur ce profil.
- Configuration des tables de base de données (si vous utilisez une base de données distante ou un environnement de déploiement).
- Configuration des noeuds finaux de service REST pour les widgets que vous utiliserez dans Business Space.
- Vérification de l'enregistrement de votre ID utilisateur dans le registre d'utilisateurs de votre produit.

A propos de cette tâche

Le fichier d'archive d'entreprise (EAR de Business Space est préconfiguré pour permettre l'authentification et l'autorisation d'accès. Business Space utilise un rôle Java 2 Platform Enterprise Edition par défaut, qui est mappé à tous les utilisateurs authentifiés et qui s'assure que les utilisateurs sont invités à s'authentifier lorsqu'ils accèdent aux adresses URL Business Space. Les utilisateurs non authentifiés sont redirigés vers une page de connexion.

L'autorisation d'accès aux espaces et au contenu de page de Business Space est gérée en interne par Business Space, dans le cadre de la gestion des espaces.

Pour activer l'accès authentifié (autorisation par rôle Java 2 Platform Enterprise Edition) à Business Space, un registre d'utilisateurs doit être configuré et la sécurité des applications activée.

Procédure

1. Pour obtenir des instructions détaillées relatives à la sécurité, reportez-vous à la documentation de la documentation de la sécurité de votre produit.
2. Pour l'application Business Space, sur la page Administration, applications et infrastructure sécurisées de la console d'administration, sélectionnez les deux options **Activer la sécurité administrative** et **Activer la sécurité des applications**.
3. Sur cette même page de la console d'administration, sous **Référentiel de comptes utilisateur**, indiquez **Référentiels fédérés**, **Système d'exploitation local**, **Protocole LDAP (Lightweight Directory Access Protocol)** ou **Registre utilisateur personnalisé**. En revanche, si vous sélectionnez **Référentiels fédérés** pour Business Space, vous disposez de fonctions supplémentaires pour vos widgets et votre infrastructure. Par exemple, des fonctions de recherche améliorées. Lorsque vous recherchez des utilisateurs pour le partage d'espaces et de pages, la portée de la recherche comprend l'adresse électronique, le nom complet de l'utilisateur et l'ID utilisateur.

Que faire ensuite

- Une fois la sécurité administrative et la sécurité des applications activées, vous êtes invité à saisir un ID utilisateur et un mot de passe lorsque vous vous connectez à Business Space. Vous devez utiliser un ID utilisateur et un mot de passe valides figurant dans le registre d'utilisateurs sélectionné pour vous connecter. Après avoir activé la sécurité administrative, à chaque fois que vous revenez à la console d'administration, vous devez vous connecter à l'aide de l'ID utilisateur disposant de droits d'administration.
- Si vous voulez limiter l'ouverture de session à un sous-ensemble d'utilisateurs et de groupes Business Space, vous pouvez modifier le mappage du rôle Java 2 Platform Enterprise Edition Business Space. Cliquez sur **Applications** → **Applications d'entreprise** → *nom_application*. Dans le panneau droit, sous Detail Properties, sélectionnez **Security role to user/group mapping**.
- Vous pouvez gérer l'autorisation d'accès aux pages et aux espaces dans Business Space dans Business Space lorsque vous créez des pages et des espaces.
- Pour définir la sécurité des données dans les widgets en fonctions d'utilisateurs ou de groupes, vous devez modifier le mappage des utilisateurs à l'application de passerelle des services REST. Sélectionnez l'application de passerelle des services REST et, dans le panneau droit, sous Detail Properties, sélectionnez **Security role to user/group mapping**. Vous pouvez ajouter des utilisateurs et des groupes au rôle RestServicesUser pour contrôler l'accès aux données de tous les widgets de services REST.
- Si vous voulez limiter l'accès aux données des widgets en fonction de rôles de groupes d'utilisateurs, étudiez la possibilité de changer les utilisateurs affectés aux rôles du groupe administratif. Vous pouvez consulter la liste des rôles pour voir quels sont les utilisateurs affectés à ces rôles en ouvrant la console d'administration, en cliquant sur **Sécurité** → **Administration, applications et infrastructure sécurisées** → **Rôles du groupe administratif** et en sélectionnant un groupe.

Etudiez la possibilité de changer les utilisateurs affectés aux rôles du groupe administratif pour des widgets tels que les règles métier et les variables métier. Par exemple, pour le widget de moniteur d'état, les rôles administratifs suivants disposent tous de droits d'accès de surveillance, ils autorisent tous l'accès à la console d'administration et autorisent donc les utilisateurs affectés à ces rôles à accéder aux données du moniteur d'état :

- Monitor
- Configurator
- Operator
- Administrator
- Adminsecuritymanager
- Deployer
- isadmins

Les utilisateurs mappés à ces rôles du groupe administratif ont accès aux données du moniteur d'état. Les utilisateurs qui ne sont pas mappés à ces rôles ne peuvent pas accéder aux données du moniteur d'état.

- Enfin, certains widgets disposent d'une couche supplémentaire d'accès basé sur les rôles pour leurs artefacts créés par des utilisateurs métier. Pour Solution Management, le widget Security Manager vous permet d'affecter aux utilisateurs et aux groupes des rôles système ou des rôles de module qui déterminent l'accès des membres aux plannings du widget Business Calendar Manager. Pour Reviewing, le widget Publishing Server Access Control gère les droits d'accès pour les utilisateurs pouvant réviser et commenter les révisions. Pour plus d'informations, reportez-vous à l'aide en ligne de votre widget.

Affectation du rôle de superutilisateur Business Space

Dans Business Space, vous pouvez affecter aux utilisateurs le rôle de superutilisateur. Un superutilisateur peut afficher, éditer et supprimer tous les espaces et toutes les pages. Il peut également définir si des espaces peuvent être des modèles dans Business Space. Vous pouvez exécuter un script qui affecte le rôle de superutilisateur Business Space à un ID utilisateur. Vous pouvez également utiliser le client de scripts wsadmin pour créer des scripts pour activer le superutilisateur Business Space.

Avant de commencer

L'ID utilisateur doit être enregistré dans le registre d'utilisateurs de votre produit.

Procédure

1. Recherchez le script *racine_installation/BusinessSpace/scripts/createSuperUser.py* pour affecter le rôle de superutilisateur à un utilisateur.
2. Ouvrez une invite de commande et accédez au répertoire suivant : *racine_profil/bin*, où *racine_profil* correspond au répertoire du profil dans lequel est installé Business Space.
3. Entrez la commande suivante : `wsadmin -lang jython -wsadmin_classpath racine_installation\plugins\com.ibm.bspace.plugin_6.2.0.jar -f createSuperUser.py nom_court_utilisateur_dans_VMM`

Que faire ensuite

Deux autres scripts sont fournis si vous voulez effectuer une requête pour vérifier si un superutilisateur dispose du rôle de superutilisateur ou si vous voulez

supprimer un rôle de superutilisateur. Ils sont tous les deux disponibles dans le répertoire *racine_installation/BusinessSpace/scripts/* :

- `isSuperUser.py` permet d'effectuer une requête pour vérifier si un nom d'utilisateur dispose du rôle de superutilisateur.
- `removeSuperUserAccess.py` permet de supprimer le rôle de superutilisateur d'un utilisateur

Vous pouvez créer des scripts supplémentaires à partir des trois scripts fournis. Vous pouvez remplacer l'appel MBean d'un script par l'une des méthodes suivantes pour utiliser le rôle de superutilisateur :

```
public boolean assignSuperUserRole(String userId);
public boolean removeSuperUserRole(String userId);
public List getAllSuperUsers();
public boolean isSuperUser(String userId);
public boolean removeAllSuperUsers();
```

Reportez-vous au fichier de descripteur MBean, `BSpaceSecurityAdminMBean.xml`, dans le répertoire *racine_installation/BusinessSpace/scripts*.

Pour ouvrir Business Space, utilisez l'adresse URL suivante : `http://hôte:port/BusinessSpace`, où *hôte* est le nom de l'hôte sur lequel est exécuté votre serveur et où *port* est le numéro de port de votre serveur.

Mise en place de la sécurité de bout en bout

Il existe de nombreux modèles de sécurité de bout en bout. Chacun d'entre eux peut comporter des étapes de configuration très différentes. Plusieurs scénarios type, avec les options de sécurité nécessaires, sont présentés.

Avant de commencer

Tous ces scénarios supposent que la sécurité administrative est appliquée.

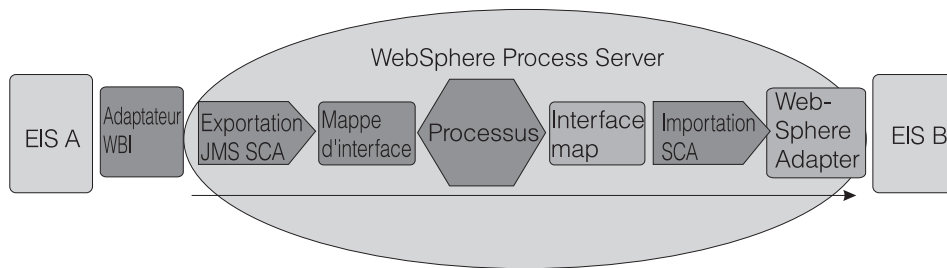
Procédure

1. Déterminez lequel des exemples présentés dans cette section correspond le mieux à vos besoins en matière de sécurité. Dans certains cas, vos besoins impliquent le recours à une combinaison d'informations issues de plusieurs de ces scénarios.
2. Prenez connaissance des informations relatives à la sécurité de chaque scénario et appliquez-les à votre situation.

Exemple

Scénario d'intégration classique - Adaptateurs entrants et sortants

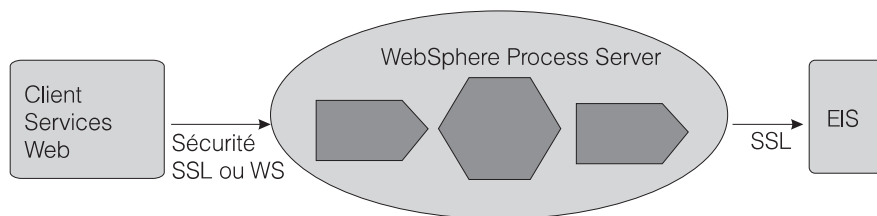
Une demande entrante provient d'un adaptateur WebSphere Business Integration Adapter. L'architecture SCA (Service Component Architecture) appelle une mappe d'interface basée sur l'exportation SCA. La demande est acheminée via un composant de processus, une deuxième mappe d'interface, puis est transmise à un deuxième EIS (B), par le biais d'un adaptateur WebSphere Adapter. Ce sont des appels SCA avec un composant qui appelle une méthode sur le composant suivant.



Il n’y a pas de mécanisme d’authentification pour l’adaptateur entrant. Vous pouvez établir le contexte de sécurité en définissant le qualificatif SecurityIdentity sur le premier composant (dans cet exemple, le premier composant de mappe d’interface). A partir de là, SCA va propager le contexte de sécurité d’un composant à l’autre. Le contrôle d’accès de chaque composant est défini en utilisant le qualificatif SecurityPermission.

Demande entrante de service Web

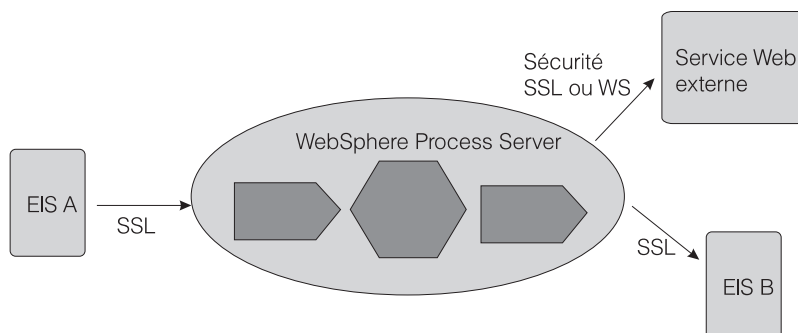
Dans ce scénario, un client de services Web appelle un composant WebSphere Process Server. La demande transite par plusieurs composants de l’environnement WebSphere Process Server avant d’être transmise à un EIS via un adaptateur.



Vous pouvez authentifier le client de services Web comme étant un client SSL, en utilisant une authentification HTTP de base ou une authentification WS-Security. Lorsque le client est authentifié, le contrôle d’accès est appliqué en définissant le qualificatif SecurityPermission. Entre le client et l’instance WebSphere Process Server, vous pouvez sécuriser l’intégrité et la confidentialité des données à l’aide de SSL ou WS-Security. SSL sécurise le circuit complet, alors que WS-Security vous permet de ne chiffrer ou signer numériquement que certaines parties du message SOAP. Pour les services Web, WS-Security est à privilégier.

Demande entrante de service Web

Dans ce scénario, la demande entrante peut provenir d’un adaptateur, d’un client de services Web ou d’un client HTTP. Un composant de WebSphere Process Server (par exemple, un composant BPEL) appelle un service Web externe.



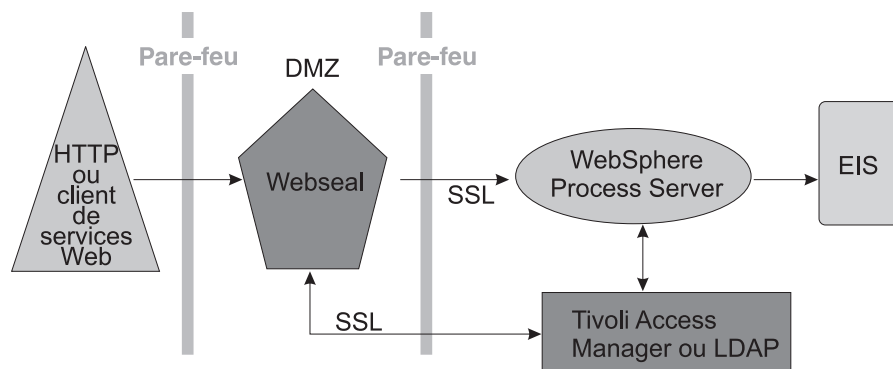
Comme dans le cas de la demande entrante de service Web, vous pouvez vous authentifier au service Web externe comme client SSL, en utilisant une authentification HTTP de base ou une authentification WS-Security. Utilisez LTPACallbackHandler comme mécanisme de rappel pour extraire le usernameToken du sujet RunAs en cours. Pour sécuriser la confidentialité et l'intégrité des données entre WebSphere Process Server et le service Web cible, vous pouvez utiliser WS-Security.

Demande entrante Application Web - HTTP vers WebSphere Process Server

WebSphere Process Server prend en charge trois types d'authentification pour HTTP :

- authentification HTTP de base
- authentification HTTP par formulaires
- authentification du client basée sur SSL (HTTPS).

En outre, pour protéger votre intranet de toute intrusion, vous pouvez placer le serveur Web dans la zone démilitarisée (DMZ) et WebSphere Process Server à l'intérieur du pare-feu interne. Dans cet exemple, WebSEAL est le proxy inverse qui procède à l'authentification. Il est dans une relation de confiance avec WebSphere Process Server derrière le pare-feu et peut réacheminer les demandes authentifiées.



Concepts associés

➡ Remarques relatives à la sécurité pour les bus d'intégration de services

Remarques

Ces informations concernent initialement des produits et services fournis aux Etats-Unis.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Contactez votre représentant IBM local pour plus d'informations sur les produits et services actuellement disponibles dans votre pays. Toute référence à un produit, programme ou service IBM n'implique pas que seul ce produit, programme ou service IBM puisse être utilisé. Tout autre produit, programme ou service fonctionnellement équivalent peut être utilisé s'il n'enfreint aucun droit de propriété intellectuelle 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. Vous pouvez envoyer des demandes de licence, en écrivant à :

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.*

Pour les demandes relatives aux licences concernant les produits utilisant un jeu de caractères double octet, prenez contact avec le service IBM Intellectual Property Department de votre pays ou envoyez vos questions par écrit à :

*IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan*

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun 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 NON-CONTREFAÇON ET D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Ces informations peuvent comporter des imprécisions techniques ou des erreurs typographiques. 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
1001 Hillside Blvd., Suite 400
Foster City, CA 94404
U.S.A.

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

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Toutes données de performance contenues dans ce document ont été déterminées dans un environnement contrôlé. De ce fait, les résultats obtenus dans d'autres environnements d'exploitation peuvent varier de manière significative. Certaines mesures peuvent avoir été effectuées sur des systèmes au niveau du développement et il n'existe aucune garantie que ces mesures seront identiques sur des systèmes disponibles de façon générale. En outre, elles peuvent résulter d'extrapolations. Les résultats obtenus peuvent varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement.

Les informations relatives aux produits non IBM ont été obtenues via les fournisseurs de ces produits, leurs annonces publiées ou d'autres sources publiquement disponibles. IBM n'a pas testé ces produits et ne peut pas confirmer avec exactitude les performances, la compatibilité ou toutes autres déclarations relatives aux produits non fournis par IBM. Toute question relative aux fonctions des produits non fournis par IBM doit être adressée aux fournisseurs de ces produits.

Toute déclaration concernant l'orientation ou les intentions futures d'IBM sont susceptibles d'être modifiées ou retirées sans préavis et ne représentent que des buts et des objectifs.

Le présent document contient 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 :

Les présentes informations contiennent des exemples de programmes d'application en langage source illustrant les techniques de programmation sur diverses plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits. Ces exemples n'ont pas été intégralement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir la fiabilité, la maintenabilité ou le fonctionnement 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 : (c) (votre société) (année). Des segments de codes sont dérivés des Programmes exemples d'IBM Corp. (c) Copyright IBM Corp. _entrez l'année ou les années_. All rights reserved.

Si vous consultez ces informations sous forme électronique, les photographies ou illustrations en couleur peuvent ne pas s'afficher.

Informations relatives à l'interface de programmation

Si elle est fournie, la documentation sur l'interface de programmation aide les utilisateurs à créer des applications en utilisant le produit.

Les interfaces de programmation génériques permettent aux utilisateurs d'écrire des applications, qui bénéficient des services proposés par les outils du produit.

Cependant, cette documentation peut également comporter des informations de diagnostic, de modification et de personnalisation. Ces informations de diagnostic, de modification et d'optimisation sont fournies pour faciliter le débogage du logiciel d'application.

Avertissement : N'utilisez pas les informations de diagnostic, de modification et d'optimisation en guise d'interface de programmation car elles peuvent être modifiées sans préavis.

Marques et marques de service

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines aux Etats-Unis et/ou dans certains autres pays. Si ces marques et d'autres marques d'IBM sont accompagnées d'un symbole de marque (^R ou TM), ces symboles signalent des marques d'IBM aux Etats-Unis à la date de publication de ce document. Ces marques peuvent également exister et éventuellement avoir été enregistrées dans d'autres pays. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à www.ibm.com/legal/copytrade.shtml.

Windows est une marque de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Java et JavaBeans sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Ce produit inclut un logiciel développé par Eclipse Project (<http://www.eclipse.org>).



IBM WebSphere Process Server for Multiplatforms, version 6.2

IBM