WebSphere® Process Server for Multiplatforms

Version 6.1.0

Sécurisation des applications et de leurs environnements

WebSphere® Process Server for Multiplatforms

Version 6.1.0

Sécurisation des applications et de leurs environnements

Important

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

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

Table des matières

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Sécurisation des applications et de leur environnement

La sécurité de l'environnement WebSphere Process Server et de vos applications est essentielle.

1. Les informations présentées ici sont disponibles au format PDF (Adobe) via le lien suivant : WebSphere Process Server (au format PDF).
2. Les Guides informatifs de Business Process Management relatifs à IBM developerWorks organisent les informations relatives à WebSphere Process Server et aux autres produits du portefeuille.

Ces documents complètent la documentation principale sur la sécurité, disponible dans le centre de documentation de WebSphere Application Server Network Deployment, version 6 et plus particulièrement dans la WebSphere Application Server Network Deployment, version 6 documentation sur la sécurité.

La sécurité de vos données et de vos processus est essentielle. La sécurité de WebSphere Process Server est basée sur la sécurité de WebSphere Application Server version 6.1. Pour obtenir des informations détaillées sur la sécurité, consultez le centre de documentation de WebSphere Application Server Network Deployment, version 6.

Présentation générale

La sécurité de vos données et de vos processus est essentielle.

La sécurité de WebSphere Process Server repose sur la sécurité de WebSphere Application Server version 6.1. Pour obtenir des informations détaillées sur la sécurité, consultez le WebSphere Application Server Network Deployment, version 6 centre de documentation de .

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. Notamment :

- **«Authentification», à la page 37** ; un utilisateur ou un processus qui appelle une application doit être authentifié.
- **«Contrôle d'accès», à la page 38** ; l'utilisateur authentifié dispose-t-il des droits nécessaires pour effectuer l'opération ?
- **«Intégrité et confidentialité des données», à la page 39** ; les données accessibles à partir des applications doivent être sécurisées afin qu'aucun utilisateur non autorisé ne puisse les visualiser ni les modifier.
- **«Authentification unique», à la page 40** ; authentification unique, qui permet à un utilisateur de ne fournir ses données d'authentification qu'une seule fois. Ces données sont ensuite transmises aux composants en aval.

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

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 caractéristiques propres à WebSphere Process Server.

Dispositifs de sécurité de 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. Ce panneau permet également de gérer les 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.
- Un ensemble de rôles de sécurité spécifiques aux composants a été défini.

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 Process Server.

A propos de cette tâche

Pour assurer la sécurité de vos données sensibles, vous devez sécuriser à la fois l'environnement Process Server et les applications que vous déployez dans cet environnement.

Procédure

1. Prenez en compte la sécurité lorsque vous installez WebSphere Process Server. Voir «Installation de WebSphere Process Server : remarques sur la sécurité», à la page 3
2. Assurez-vous que la sécurité est activée pour votre installation autonome ou en environnement de déploiement.
   a. Assurez-vous que la «Sécurité administrative», à la page 8 est activée. La sécurité administrative est activée par défaut.
   b. Assurez-vous que la «Sécurité des applications», à la page 10 est activée. La sécurité applicative est activée par défaut.
   c. Si nécessaire, activez la «Sécurité Java 2», à la page 10.
   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. 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.
d. Gérez la sécurité de votre environnement WebSphere Process Server.

Installation de WebSphere Process Server : remarques sur la sécurité

Effectuez ces tâches pour implémenter la sécurité avant, pendant et après l'installation de WebSphere Process Server.

A propos de cette tâche

Ces tâches doivent être effectuées pendant 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.

Tâches associées

Préparation des systèmes i5/OS en vue de l'installation

Etudiez la préparation d'un système i5/OS en vue de l'installation de WebSphere Process Server.

Information associée

Sécurisation de votre environnement avant l'installation

Préparation du système d'exploitation en vue de l'installation du produit

Sécurisation de votre environnement après l'installation

Informations d'authentification lors de l'installation

Dans les précédentes versions de WebSphere Process Server vous deviez entrer différentes informations d'authentification durant 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 : pour renforcer la sécurité de votre installation, vous devez configurer les différents composants de WebSphere Process Server sur la console d'administration afin de leur attribuer les identités de sécurité appropriées.

Lors de la création d'un profil WebSphere Process Server, vous êtes invité à saisir un nom d'utilisateur et un mot de passe si vous laissez l'option **Activer la sécurité administrative** activée. 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 justificatifs 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, accédez au 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. Sélectionnez l'alias à modifier en cochant la case dans la colonne Sélectionner, en cliquant sur Editer, puis en indiquant dans le panneau suivant le nom d'utilisateur et le mot de passe devant servir d'alias d'authentification pour ce composant. Les justificatifs que vous indiquez doivent exister dans le référentiel de comptes utilisateur que vous utilisez.

Que faire ensuite

Vous trouverez plus d'informations concernant la gestion des alias d'authentification dans les rubriques suivantes.

Tâches associées

«Modification des alias d'authentification», à la page 37
Vous pouvez être amené à modifier les alias d'authentification existants.

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

Cliquez sur les liens ci-dessous pour suivre la procédure de configuration de la sécurité d'une installation autonome de WebSphere Process Server.

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.

Procédure

1. Assurez-vous que la sécurité administrative est activée. «Activation de la sécurité administrative», à la page 7.
2. Assurez-vous que la sécurité applicative est activée. «Sécurisation des applications dans WebSphere Process Server», à la page 35.
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 : • le référentiel de fichiers intégré au système, • un ou plusieurs référentiels externes, • 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 Managing the realm in a federated repository configuration.
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», à la page 12.
Registre LDAP autonome	Pour configurer le protocole LDAP comme registre d'utilisateurs, suivez les instructions de la section Configuration du protocole LDAP en tant que 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», à la page 12.

5. Validez ces modifications.

   Cliquez sur le bouton **Valider** dans la partie inférieure du panneau.
6. Accédez au panneau Sécurité Business Integration. Cliquez sur **Sécurité**, puis sur **Sécurité Business Integration**.
7. Fournissez les identités utilisateur appropriées pour les alias d'authentification répertoriés. Le justificatif que vous indiquez doit exister dans le référentiel de comptes utilisateur que vous utilisez.
8. 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(s) d'utilisateur et/ou de groupe liés au rôle d'administrateur de flux métier et de tâches manuelles. Les utilisateurs qui se voient affecter ce rôle disposent de tous les privilèges.
   - **Superviseur** : Noms(s) d'utilisateur et/ou de groupe liés au rôle de surveillance des flux métier et tâches manuelles. 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 manuelles de traiter les appels asynchrones émis par les interfaces de programme d'application.

9. Validez ces modifications.

   Cliquez sur le bouton **Valider** dans la partie inférieure du panneau.
10. Enregistrez les modifications dans la configuration locale.

    Cliquez sur **Sauvegarder** dans la fenêtre de message.
11. Eventuellement, arrêtez, puis 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.

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 justificatifs utilisateur appropriés issus 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

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

Utilisez les outils de vérification de l'installation pour vérifier que l'installation de WebSphere Process Server et la création des profils de serveur autonome ou de gestionnaire de déploiement ont abouti. Un *profil* se compose de fichiers définissant l'environnement d'exécution d'un gestionnaire de déploiement ou d'un serveur. Vérifiez les fichiers de base du produit à l'aide de l'outil de somme de contrôle installver_wbi. Vérifiez chaque profil en utilisant l'outil IVT (Installation Verification Test).

Activation de la sécurité administrative

La première étape du processus de sécurisation de votre environnement WebSphere Process Server et 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.

A propos de cette tâche

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.

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. 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 AccessControl 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 dans le 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.

   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).
4. Validez ces modifications.

   Cliquez sur le bouton **Valider** dans la partie inférieure du panneau.
5. Enregistrez les modifications dans la configuration locale.

   Cliquez sur **Sauvegarder** dans la fenêtre de message.
6. Eventuellement, arrêtez, puis 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.

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 le même ordinateur 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, tels qu'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 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 J2EE (Java 2 Platform, Enterprise Edition) protège l'accès aux ressources Web, telles que 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 l'utilisation du modèle de programmation du contrôle d'accès à granularité fine Java 2. 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 le référentiel de comptes utilisateur du système d'exploitation local (option par défaut), le registre LDAP (Lightweight Directory Access Protocol), des référentiels fédérés ou 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	Indiquez ce paramètre pour gérer des profils dans plusieurs référentiels sous un domaine unique. Le domaine peut se composer d'identités dans : • le référentiel de fichiers intégré au système, • un ou plusieurs référentiels externes, • 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 Managing the realm in a federated repository configuration.
Système d'exploitation local	Registre d'utilisateurs par défaut. Sous **Définitions de domaines disponibles**, sélectionnez **Système d'exploitation local**, cliquez sur **Configurer**. Sur la page Registre d'utilisateurs du système d'exploitation local, indiquez un nom d'utilisateur et un mot de passe. Ce nom d'utilisateur est utilisé comme identité pour le serveur. L'utilisateur est automatiquement ajouté au rôle **Administrateur**. **Remarque :** N'utilisez pas le système d'exploitation local comme registre d'utilisateurs dans un environnement de déploiement réseau.

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	Sélectionnez un référentiel de comptes personnalisé et configurez-le selon vos besoins.
Tivoli Access Manager	**Remarque :** Cette option n'est pas disponible dans la console d'administration et doit être configurée à l'aide de la commande wsadmin.

Configuration du référentiel de comptes utilisateur

Vous pouvez configurer votre référentiel de comptes utilisateur à l'aide de la console d'administration. Vous pouvez choisir une identité utilisateur de serveur ou générer automatiquement une identité de serveur.

A propos de cette tâche

Vous pouvez configurer le référentiel de comptes utilisateur à l'aide de la console d'administration. 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 **Référentiel de comptes utilisateur** de 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 administratif primaire**. Indique le nom d'un utilisateur possédant des droits d'administration qui est défini dans le système d'exploitation local. Le nom d'utilisateur sert à la connexion à la console d'administration lorsque la sécurité administrative est activée.
3. Sélectionnez l'option **Identité de serveur généré automatiquement** ou **Identité de serveur stockée dans un référentiel**.

   Si vous sélectionnez l'option **Identité de serveur stockée dans un référentiel**, entrez les informations suivantes :

   - ID utilisateur ou administrateur du serveur.
   - Mot de passe associé à cet utilisateur.

   Cette identité doit exister dans le référentiel de comptes utilisateur.

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, en le configurant 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 le souhaitez, utiliser un protocole LDAP externe comme registre d'utilisateurs. Dans un environnement de déploiement réseau, vous devez utiliser LDAP.

A propos de cette tâche

Cette tâche suppose que vous avez activé la sécurité globale.

Procédure

1. Démarrez WebSphere Process Server.
2. Lancez la console d'administration.
3. Ouvrez la page de configuration du registre d'utilisateurs LDAP.

   Développez **Sécurité**, cliquez sur **Administration, applications et infrastructure sécurisées**, puis sélectionnez **LDAP** dans le menu **Définitions de domaines disponibles**. Cliquez sur **Configurer**.
4. 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 ou dans la commande wsadmin.
5. Cliquez sur **Appliquer**.
6. Sélectionnez l'option **Identité de serveur généré automatiquement** ou **Identité de serveur stockée dans un référentiel**.

   Si vous sélectionnez l'option **Identité de serveur stockée dans un référentiel**, entrez les informations suivantes :

   - ID utilisateur ou administrateur du serveur.
   - 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.
7. Choisissez le type de protocole LDAP que vous utilisez.

   Dans la liste **Type**, choisissez le protocole LDAP que vous souhaitez utiliser comme registre d'utilisateurs.
8. Entrez le nom de l'ordinateur hébergeant LDAP.

   Dans la zone **Hôte**, entrez le nom du serveur hébergeant LDAP.
9. Entrez le numéro de port sur lequel LDAP écoute.

   Dans la zone **Port**, entrez le numéro de port sur lequel le serveur LDAP écoute.
10. Entrez le **Nom distinctif de base**.

Cette valeur spécifie le nom distinctif de base du service d'annuaire, indiquant le point de démarrage des recherches LDAP (Lightweight Directory Access Protocol) du service d'annuaire.

Dans le cadre des autorisations, les majuscules et les minuscules sont prises en compte dans cette zone. 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 à celui de l'autre cellule ou de l'autre serveur Lotus Domino. Si vous ne voulez pas prendre en compte les majuscules et les minuscules pour l'autorisation, activez l'option **Ignorer maj/min**. 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.

11. Pour les autres paramètres, conservez les valeurs par défaut puis confirmez vos modifications.

    Cliquez sur **OK**.

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 : • Windows **Sous Windows :** startserver *nom_serveur* • Linux UNIX **Sous Linux et UNIX :** startserver.sh *nom_serveur* • i5/OS **Sous System i (à partir de la ligne de commande QShell) :** startserver *nom_serveur* à l'invite de commande dans le répertoire *rép_installation*/bin.

   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 : • Windows **Sous Windows :** stopserver *nom_serveur* -profileName *nom_profil* -username *nom_utilisateur* -password *mot_de_passe* • Linux UNIX **Sous Linux et UNIX :** stopserver.sh *nom_serveur* -profileName *nom_profil* -username *nom_utilisateur* -password *mot_de_passe* • i5/OS **Sous System i (à partir de la ligne de commande QShell) :** stopserver *nom_serveur* -profileName *nom_profil* -username *nom_utilisateur* -password *mot_de_passe* à l'invite de commande dans le répertoire *rép_installation*/bin. 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, l'accès à la console d'administration est limité aux utilisateurs associés à l'un de ces rôles.

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

Tableau 1. 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 opérateur dispose des droits d'un moniteur plus la capacité de modifier l'état de l'exécution du serveur (c'est-à-dire l'arrêter et le démarrer).
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 : • Modifier l'ID utilisateur et le mot de passe du serveur • Mapper les utilisateurs et les groupes vers le rôle d'administrateur Il peut également accéder à certaines informations sensibles comme : • Mot de passe LTPA • Clés
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 : • Création, mise à jour et suppression d'utilisateurs dans la configuration des référentiels fédérés. • Création, mise à jour et 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.

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.

Objet

Plusieurs composants essentiels 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 de profil, la valeur attribuée par défaut à ces alias d'authentification est l'identité et le mot de passe de l'administrateur. 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 des alias d'authentification répertoriés ci-après. Vous pouvez modifier ces alias à l'aide de la console d'administration.

Les alias figurant dans le tableau 2 sont utilisés pour appeler les composants, quelque soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 2. 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 sur le panneau de configuration du Chorégraphe de processus métier de l'Assistant de gestion des profils.

Tableau 2. Alias d'authentification associés aux processus métier (suite)

Alias	Description	Information
BPEAuthDataAlias*TypeBdD_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 3 décrit les rôles RunAs créés pour les processus métier.

Tableau 3. 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 sur le panneau de configuration du Chorégraphe de processus métier de l'Assistant de gestion des profils.
EscalationUser	Utilisé par le bean géré par message task.ear.	Indiquez un nom d'utilisateur et un mot de passe sur le panneau de configuration du Chorégraphe de processus métier de l'Assistant 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 des alias d'authentification répertoriés ci-après. Vous pouvez modifier ces alias à l'aide de la console d'administration.

Les alias figurant dans le tableau 4 sont utilisés pour appeler les composants, quelque soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 4. Alias d'authentification associés à Common Event Infrastructure

Alias	Description	Information
CommonEventInfrastructure JMSAuthAlias Un espace a été ajouté à cette entrée pour des questions de mise en forme. 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'Assistant de gestion des profils.
EventAuthAlias*TypeBdD*	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'Assistant de gestion des profils.

Alias d'authentification Service Component Architecture

Service Component Architecture (SCA) est doté des alias d'authentification répertoriés ci-après. 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 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 de SCA de l'Assistant de gestion des profils.

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

Les fichiers d'archive d'entreprise (EAR) répertoriés ci-après sont installés avec un contrôle d'accès lors de l'installation du Chorégraphe de processus métier. Le Chorégraphe de processus métier est installé lors de l'installation de WebSphere Process Server. Human Task Manager utilise les rôles pour déterminer les fonctions d'un utilisateur d'un système de production.

Fichier EAR	Rôles	Droits d'accès par défaut	Remarques
bpecontainer.ear	BPESystemAdministrator	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	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	Peut accéder à l'explorateur du Chorégraphe de processus métier.

Contrôle d'accès dans les applications Common Event Infrastructure

Le fichier d'archive d'entreprise (EAR) ci-après est installé avec un contrôle d'accès lors de l'installation de Common Event Infrastructure. Common Event Infrastructure est installé lors de l'installation de WebSphere Process Server.

Le fichier EventServer.ear est le seul fichier EAR installé lors de l'installation de Common Event Infrastructure.

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

Cliquez sur les liens ci-dessous pour suivre la procédure de configuration de la sécurité d'une installation de WebSphere Process Server en environnement de déploiement.

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.

Procédure

1. Assurez-vous que la sécurité administrative est activée. «Activation de la sécurité administrative», à la page 7.
2. Assurez-vous que la sécurité applicative est activée. «Sécurisation des applications dans WebSphere Process Server», à la page 35.
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 : • le référentiel de fichiers intégré au système, • un ou plusieurs référentiels externes, • 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 Managing the realm in a federated repository configuration.
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», à la page 12.
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», à la page 12.

5. Validez ces modifications.

   Cliquez sur le bouton **Valider** dans la partie inférieure du panneau.
6. Accédez au panneau Sécurité Business Integration. Cliquez sur **Sécurité**, puis sur **Sécurité Business Integration**.
7. Fournissez les identités utilisateur appropriées pour les alias d'authentification répertoriés. Le justificatif que vous indiquez doit 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.
8. 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(s) d'utilisateur et/ou de groupe liés au rôle d'administrateur de flux métier et de tâches manuelles. Les utilisateurs qui se voient affecter ce rôle disposent de tous les privilèges.
   - **Superviseur** : Noms(s) d'utilisateur et/ou de groupe liés au rôle de surveillance des flux métier et tâches manuelles. 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 manuelles de traiter les appels asynchrones émis par les interfaces de programme d'application.

9. Validez ces modifications.

   Cliquez sur le bouton **Valider** dans la partie inférieure du panneau.

10. Enregistrez les modifications dans la configuration locale.

    Cliquez sur **Sauvegarder** dans la fenêtre de message.

11. 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**.

12. Eventuellement, arrêtez, puis 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.

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 justificatifs utilisateur appropriés issus 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

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

Utilisez les outils de vérification de l'installation pour vérifier que l'installation de WebSphere Process Server et la création des profils de serveur autonome ou de gestionnaire de déploiement ont abouti. Un *profil* se compose de fichiers définissant l'environnement d'exécution d'un gestionnaire de déploiement ou d'un serveur. Vérifiez les fichiers de base du produit à l'aide de l'outil de somme de contrôle installver_wbi. Vérifiez chaque profil en utilisant l'outil IVT (Installation Verification Test).

Activation de la sécurité administrative

La première étape du processus de sécurisation de votre environnement WebSphere Process Server et 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.

A propos de cette tâche

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.

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. 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 AccessControl 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 sécuritéJava 2 dans le centre e de documentation dfWebSphere 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.

   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).
4. Validez ces modifications.

   Cliquez sur le bouton **Valider** dans la partie inférieure du panneau.
5. Enregistrez les modifications dans la configuration locale.

   Cliquez sur **Sauvegarder** dans la fenêtre de message.
6. Eventuellement, arrêtez, puis 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.

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 le même ordinateur 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, tels qu'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 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 J2EE (Java 2 Platform, Enterprise Edition) protège l'accès aux ressources Web, telles que 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 l'utilisation du modèle de programmation du contrôle d'accès à granularité fine Java 2. 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 le référentiel de comptes utilisateur du système d'exploitation local (option par défaut), le registre LDAP (Lightweight Directory Access Protocol), des référentiels fédérés ou 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	Indiquez ce paramètre pour gérer des profils dans plusieurs référentiels sous un domaine unique. Le domaine peut se composer d'identités dans : • le référentiel de fichiers intégré au système, • un ou plusieurs référentiels externes, • 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 Managing the realm in a federated repository configuration.

Registre d'utilisateurs	Action
Système d'exploitation local	Registre d'utilisateurs par défaut. Sous **Définitions de domaines disponibles**, sélectionnez **Système d'exploitation local**, cliquez sur **Configurer**. Sur la page Registre d'utilisateurs du système d'exploitation local, indiquez un nom d'utilisateur et un mot de passe. Ce nom d'utilisateur est utilisé comme identité pour le serveur. L'utilisateur est automatiquement ajouté au rôle **Administrateur**. **Remarque :** N'utilisez pas le système d'exploitation local comme registre d'utilisateurs dans un environnement de déploiement réseau.
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	Sélectionnez un référentiel de comptes personnalisé et configurez-le selon vos besoins.
Tivoli Access Manager	**Remarque :** Cette option n'est pas disponible dans la console d'administration et doit être configurée à l'aide de la commande wsadmin.

Configuration du référentiel de comptes utilisateur

Vous pouvez configurer votre référentiel de comptes utilisateur à l'aide de la console d'administration. Vous pouvez choisir une identité utilisateur de serveur ou générer automatiquement une identité de serveur.

A propos de cette tâche

Vous pouvez configurer le référentiel de comptes utilisateur à l'aide de la console d'administration. 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 **Référentiel de comptes utilisateur** de 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 administratif primaire**. Indique le nom d'un utilisateur possédant des droits d'administration qui est défini dans le système d'exploitation local. Le nom d'utilisateur sert à la connexion à la console d'administration lorsque la sécurité administrative est activée.
3. Sélectionnez l'option **Identité de serveur généré automatiquement** ou **Identité de serveur stockée dans un référentiel**.

Si vous sélectionnez l'option **Identité de serveur stockée dans un référentiel**, entrez les informations suivantes :

- ID utilisateur ou administrateur du serveur.
- Mot de passe associé à cet utilisateur.

Cette identité doit exister dans le référentiel de comptes utilisateur.

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, en le configurant 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 le souhaitez, utiliser un protocole LDAP externe comme registre d'utilisateurs. Dans un environnement de déploiement réseau, vous devez utiliser LDAP.

A propos de cette tâche

Cette tâche suppose que vous avez activé la sécurité globale.

Procédure

1. Démarrez WebSphere Process Server.
2. Lancez la console d'administration.
3. Ouvrez la page de configuration du registre d'utilisateurs LDAP.

   Développez **Sécurité**, cliquez sur **Administration, applications et infrastructure sécurisées**, puis sélectionnez **LDAP** dans le menu **Définitions de domaines disponibles**. Cliquez sur **Configurer**.
4. 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 ou dans la commande wsadmin.
5. Cliquez sur **Appliquer**.
6. Sélectionnez l'option **Identité de serveur généré automatiquement** ou **Identité de serveur stockée dans un référentiel**.

   Si vous sélectionnez l'option **Identité de serveur stockée dans un référentiel**, entrez les informations suivantes :

   - ID utilisateur ou administrateur du serveur.
   - 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.

7. Choisissez le type de protocole LDAP que vous utilisez.

   Dans la liste **Type**, choisissez le protocole LDAP que vous souhaitez utiliser comme registre d'utilisateurs.

8. Entrez le nom de l'ordinateur hébergeant LDAP.

   Dans la zone **Hôte**, entrez le nom du serveur hébergeant LDAP.

9. Entrez le numéro de port sur lequel LDAP écoute.

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

10. Entrez le **Nom distinctif de base**.

    Cette valeur spécifie le nom distinctif de base du service d'annuaire, indiquant le point de démarrage des recherches LDAP (Lightweight Directory Access Protocol) du service d'annuaire.

    Dans le cadre des autorisations, les majuscules et les minuscules sont prises en compte dans cette zone. 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 à celui de l'autre cellule ou de l'autre serveur Lotus Domino. Si vous ne voulez pas prendre en compte les majuscules et les minuscules pour l'autorisation, activez l'option **Ignorer maj/min**. 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.

11. Pour les autres paramètres, conservez les valeurs par défaut puis confirmez vos modifications.

    Cliquez sur **OK**.

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 : • Windows **Sous Windows :** startserver *nom_serveur* • Linux UNIX **Sous Linux et UNIX :** startserver.sh *nom_serveur* • i5/OS **Sous System i (à partir de la ligne de commande QShell) :** startserver *nom_serveur* à l'invite de commande dans le répertoire *rép_installation*/bin.

   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 : • Windows **Sous Windows :** stopserver *nom_serveur* -profileName *nom_profil* -username *nom_utilisateur* -password *mot_de_passe* • Linux UNIX **Sous Linux et UNIX :** stopserver.sh *nom_serveur* -profileName *nom_profil* -username *nom_utilisateur* -password *mot_de_passe* • i5/OS **Sous System i (à partir de la ligne de commande QShell) :** stopserver *nom_serveur* -profileName *nom_profil* -username *nom_utilisateur* -password *mot_de_passe* à l'invite de commande dans le répertoire *rép_installation*/bin. 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, l'accès à la console d'administration est limité aux utilisateurs associés à l'un de ces rôles.

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

Tableau 6. 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 opérateur dispose des droits d'un moniteur plus la capacité de modifier l'état de l'exécution du serveur (c'est-à-dire l'arrêter et le démarrer).
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 : • Modifier l'ID utilisateur et le mot de passe du serveur • Mapper les utilisateurs et les groupes vers le rôle d'administrateur Il peut également accéder à certaines informations sensibles comme : • Mot de passe LTPA • Clés

Tableau 6. 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 : • Création, mise à jour et suppression d'utilisateurs dans la configuration des référentiels fédérés. • Création, mise à jour et 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.

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.

Objet

Plusieurs composants essentiels 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 de profil, la valeur attribuée par défaut à ces alias d'authentification est l'identité et le mot de passe de l'administrateur. 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 des alias d'authentification répertoriés ci-après. Vous pouvez modifier ces alias à l'aide de la console d'administration.

Les alias figurant dans le tableau 2, à la page 17 sont utilisés pour appeler les composants, quelque soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 7. 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 sur le panneau de configuration du Chorégraphe de processus métier de l'Assistant de gestion des profils.
BPEAuthDataAlias*TypeBdD_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 3, à la page 18 décrit les rôles RunAs créés pour les processus métier.

Tableau 8. 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 sur le panneau de configuration du Chorégraphe de processus métier de l'Assistant de gestion des profils.
EscalationUser	Utilisé par le bean géré par message task.ear.	Indiquez un nom d'utilisateur et un mot de passe sur le panneau de configuration du Chorégraphe de processus métier de l'Assistant 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 des alias d'authentification répertoriés ci-après. Vous pouvez modifier ces alias à l'aide de la console d'administration.

Les alias figurant dans le tableau 4, à la page 18 sont utilisés pour appeler les composants, quelque soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 9. Alias d'authentification associés à Common Event Infrastructure

Alias	Description	Information
CommonEventInfrastructure JMSAuthAlias Un espace a été ajouté à cette entrée pour des questions de mise en forme. 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'Assistant de gestion des profils.
EventAuthAlias*TypeBdD*	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'Assistant de gestion des profils.

Alias d'authentification Service Component Architecture

Service Component Architecture (SCA) est doté des alias d'authentification répertoriés ci-après. Vous pouvez modifier ces alias à l'aide de la console d'administration.

Les alias figurant dans le tableau 5, à la page 19 sont utilisés pour appeler les composants, quelque soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 10. Alias d'authentification associés 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 de SCA de l'Assistant de gestion des profils.

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

Les fichiers d'archive d'entreprise (EAR) répertoriés ci-après sont installés avec un contrôle d'accès lors de l'installation du Chorégraphe de processus métier. Le Chorégraphe de processus métier est installé lors de l'installation de WebSphere Process Server. Human Task Manager utilise les rôles pour déterminer les fonctions d'un utilisateur d'un système de production.

Fichier EAR	Rôles	Droits d'accès par défaut	Remarques
bpecontainer.ear	BPESystemAdministrator	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	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	Peut accéder à l'explorateur du Chorégraphe de processus métier.

Contrôle d'accès dans les applications Common Event Infrastructure

Le fichier d'archive d'entreprise (EAR) ci-après est installé avec un contrôle d'accès lors de l'installation de Common Event Infrastructure. Common Event Infrastructure est installé lors de l'installation de WebSphere Process Server.

Le fichier EventServer.ear est le seul fichier EAR installé lors de l'installation de Common Event Infrastructure.

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.

Avant de commencer

La sécurisation de vos applications suppose que vous ayez activé la sécurité administrative.

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. Pour plus de détails, voir «Activation de la sécurité administrative», à la page 7.
2. Assurez-vous que la sécurité applicative est activée. Dans la console d'administration, développez **Sécurité**, puis cliquez sur **Administration, applications et infrastructure sécurisées**. 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 Process Server 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.

Eléments 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 ses données de connexion plusieurs fois.

Il est possible de diviser la sécurité dans WebSphere Process Server 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 autorisé 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 :

- **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 aval qui appliquent à leur tour le contrôle d'accès.

Authentification

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.

tableau 11 répertorie les clients standards qui peuvent appeler les composants WebSphere Process Server, ainsi que les options d'authentification disponibles pour chacun d'eux.

Tableau 11. 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, développez **Sécurité**, puis cliquez sur **Alias d'authentification de 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.
2. Sélectionnez l'alias d'authentification que vous souhaitez modifier.

   Le panneau Alias d'authentification de sécurité Business Integration contient une liste d'alias d'authentification, le composant associé, l'ID utilisateur associé à cet alias et, parfois, une description de l'alias. Cliquez sur l'alias que vous souhaitez modifier. Vous pouvez également cocher la case de la colonne **Sélectionner** qui correspond à l'alias que vous souhaitez éditer, puis cliquer sur le bouton **Editer**. Le panneau de configuration de l'alias d'authentification s'affiche.
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 4
   Lorsque vous créez un profil WebSphere Process Server, les valeurs par défaut sont utilisées pour les justificatifs 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 s'est authentifié dans WebSphere Process Server, il est important, pour garantir la sécurité, qu'il n'ait pas accès à toutes les opérations disponibles. 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 WebSphere Integration Developer centre de documentation.

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. Le Chorégraphe de processus métier 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.

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

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/csec_plan.html

http://publib.boulder.ibm.com/infocenter/dmndhelp/v6r1mx/topic/com.ibm.wbit.610.help.runtime.doc/topics/tusergoal.html

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 WebSphere Application Servernote technique. Vous trouverez des informations plus générales sur la sécurisation des services Web à 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 doit transiter 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 capacité d'authentification unique avec Tivoli Access Manager ou WebSEAL

Développement de composants sécurisés

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

Avant de commencer

Développez une application sécurisée dans WebSphere Integration Developer. Exportez l'application en tant que fichier d'archive d'entreprise (EAR) en vue d'un déploiement dans WebSphere Process Server.

A propos de cette tâche

Importez une application sécurisée dans WebSphere Process Server en suivant les étapes décrites ci-après.

Procédure

1. Installez le fichier EAR de l'application.

Sur la console d'administration, sélectionnez **Applications**, puis cliquez sur **Applications d'entreprise**. Cliquez sur **Installation** et indiquez les caractéristiques relatives à la nouvelle application.

2. Affectation de rôles de sécurité à la nouvelle application.

   Cliquez sur **Mappage des rôles de sécurité vers les utilisateurs/groupes**. Vous disposez de quatre rôles pour l'application.

Option	Description
Tous les utilisateurs	Aucune sécurité.
Tous les utilisateurs authentifiés	Tout utilisateur qui s'authentifie avec un nom d'utilisateur et un mot de passe corrects est associé au rôle.
Utilisateurs mappés	Des utilisateurs sont individuellement répertoriés en tant que membres du rôle.
Groupes mappés	La constitution d'un groupe est la méthode la plus simple pour ajouter des utilisateurs : chaque membre d'un groupe identifié devient un membre du rôle.

   Utilisez les options **Rechercher des utilisateurs** et **Rechercher des groupes** pour afficher les utilisateurs et les groupes pouvant être mappés vers le rôle.

Dans l'exemple SCDL (Service Component Definition Language) ci-dessous, l'accès à la méthode **onewayinvoke** est limitée aux utilisateurs qui sont membres du rôle de **gestionnaire**.

```
<?xml version="1.0" encoding="UTF-8"?>
<scdl:component xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:java="http://www.ibm.com/xmlns/prod/websphere/scdl/java/6.0.0"
xmlns:ns1="http://sample.recovery.security/Itarget"
xmlns:scdl="http://www.ibm.com/xmlns/prod/websphere/scdl/6.0.0"
xmlns:wsdl="http://www.ibm.com/xmlns/prod/websphere/scdl/wsdl/6.0.0"
displayName="secure" name="Component1">
  <interfaces>
    <interface xsi:type="wsdl:WSDLPortType" portType="ns1:Itarget">
      <method name="onewayinvoke">
       <scdl:interfaceQualifier xsi:type="scdl:SecurityPermission"
role="manager"/>
      </method>
      </interface>
  </interfaces>
  <references/>
  <implementation xsi:type="java:JavaImplementation"
class="sca.component.java.impl.Component1Impl1">
 </implementation>
</scdl:component>
```

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 role 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/groupes" est affiché pendant l'installation de l'application (ou sa gestion), dans la section Propriétés supplémentaires.

Procédure

1. Dans la console d'administration, cliquez sur Applications, puis 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/groupes".
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 que les autres identifiants. 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.

Information associée


Affectation d'utilisateurs et de groupes et 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) qualifiants de sécurité securityPermission et securityIdenitity. Lorsque ces deux qualifiants 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 qualifiant SCA (Service Component Architecture) securityPermission. Lorsque vous appelez ce qualifiant, vous spécifiez un rôle (par exemple, «moniteur») 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 qualifiant securityIdentity est équivalent au rôle RunAs utilisé pour les délégations dans WebSphere Application Server. La valeur associée à ce qualifiant est un rôle. Pendant le déploiement, le rôle est mappé vers une identité. L'appel d'un composant sécurisé avec securityIdentity prend en compte l'identité spécifiée, sans considérer 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.

Qualifiant de sécurité	Opération à effectuer
Droit de sécurité	Affectez un ou des utilisateurs au rôle spécifié. Quatre options sont possibles : • 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. 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.
Identité de sécurité	Définissez un nom d'utilisateur et un mot de passe valides pour l'identité vers laquelle le rôle est mappé.

Information associée

Délégations

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

Les adaptateurs sont des mécanismes qui permettent aux applications de communiquer avec des systèmes EIS (Enterprise Information Systems). 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. WebSphere Business Integration Adapters s'appuie sur la messagerie JMS ; or JMS ne prend pas en charge la diffusion de contexte de sécurité.

WebSphere Adapters permet une connectivité bidirectionnelle et gérée entre des systèmes EIS 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 de prise en charge au niveau de la sécurité des communications entrantes. Ainsi WebSphere Adapters ne dispose pas non plus d'un mécanisme d'authentification pour des communications entrantes.

L'entrée d'un adaptateur vers WebSphere Process Server s'effectue toujours via une exportation SCA (Service Component Architecture). 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 qualifiant SCA SecurityIdentity lors de la phase de développement (pour plus d'informations, voir le centre de documentation de WebSphere Integration Developer). 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 sur la sécurité des 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 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 aux processus

Information associée

Autorisation et affectation d'utilisateur

Didacticiels

Les didacticiels présentent quelques scénarios courants afin de vous aider à effectuer votre configuration.

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 globale est activée.

A propos de cette tâche

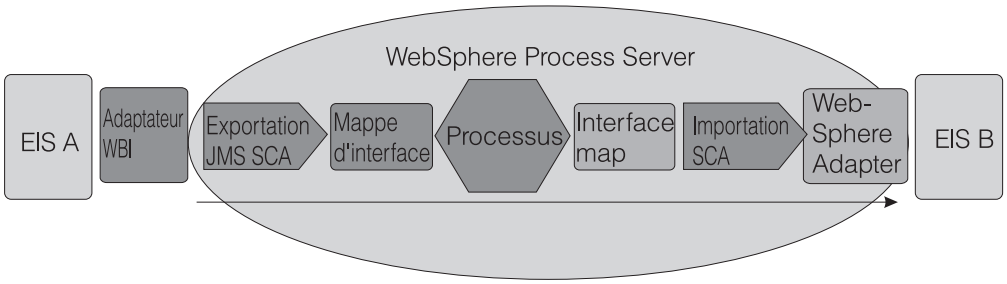
Procédure

1. Déterminez lequel des exemples présentés dans cette section correspond le mieux à vos besoins en sécurité. Dans certains cas, votre scénario comprendra une combinaison d'informations issues de plusieurs de ces exemples.

2. Prenez connaissance des informations relatives à la sécurité de chaque scénario et appliquez-les à votre situation.

Scénario d'intégration classique - Adaptateurs entrants et sortants

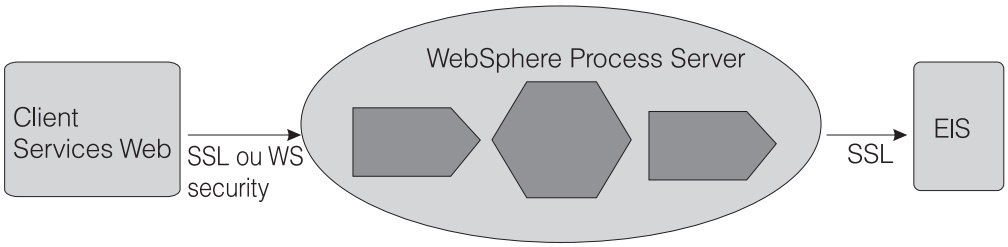
Une demande entrante provient d'un adaptateur WebSphere Business Integration Adapter. L'architecture SCA (Service Component Architecture) appelle une mappe d'interface basée sur l'exportation SCA. La demande est acheminée via un composant de processus, une deuxième mappe d'interface, puis est transmise 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 qualifiant 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 qualifiant SecurityPermission.

Demande entrante d'un service Web à WebSphere Process Server

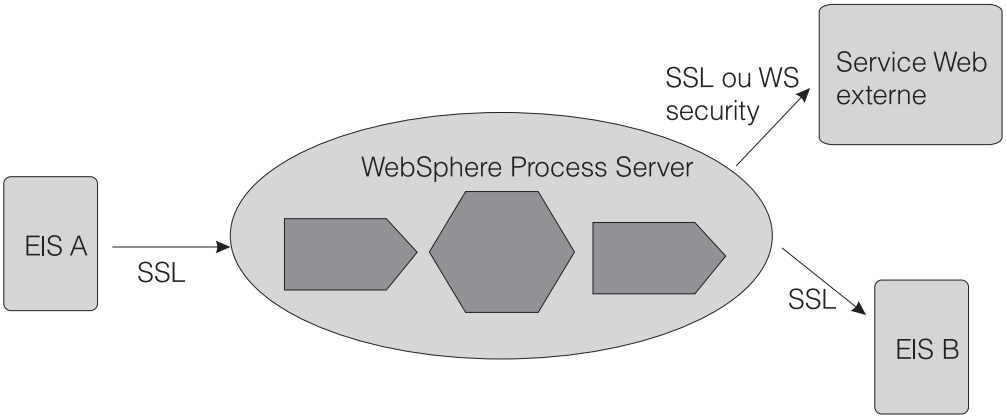
Dans ce scénario, un client de services Web appelle un composant WebSphere Process Server. La demande transite par plusieurs composants de l'environnement WebSphere Process Server avant d'être transmise à un EIS via un adaptateur.



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 qualifiant 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 sortante de service Web émise par WebSphere Process Server

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.



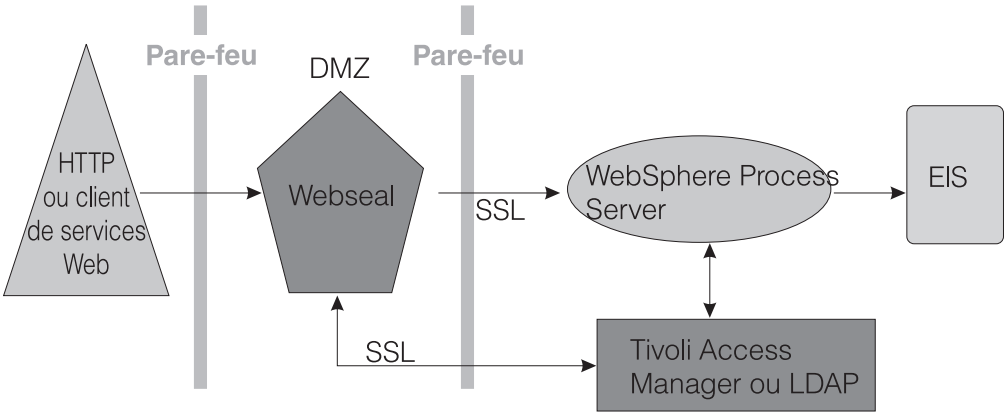
Comme dans le cas de la demande entrante de service Web, vous pouvez vous authentifier au service Web externe comme client SSL, en utilisant une authentification HTTP de base ou une authentification WS-Security. Utilisez LTPACallBackHandler comme mécanisme de rappel pour extraire le usernameToken du 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 sur la sécurité des bus d'intégration de services

Didacticiel : Rédaction d'un script Jacl permettant de répertorier les rôles de sécurité

Ce didacticiel explique comment élaborer et exécuter un script Jacl simple capable d'accéder à un bean JMX MBean et de le gérer. Ce script permet d'appeler des rôles lorsque la sécurité globale est activée. Il vous permet également d'imprimer le nom de chacun des rôles impliqué dans une relation.

Objectif de ce didacticiel

Une fois ce didacticiel effectué, vous serez capable de :

- Rédiger un script Jacl permettant d'appeler un JMX MBean demandant une liste de toutes les relations.

Pour plus d'informations sur la rédaction de scripts, reportez-vous à la rubrique "Utilisation du scriptage (wsadmin)" du centre de documentation de WebSphere Application Server Network Deployment, version 6.

Durée requise pour effectuer ce didacticiel

Ce didacticiel nécessite 15-30 minutes environ.

Conditions préalables

Ce didacticiel utilise un script compris dans l'exemple relatif à la sécurité JMX. Cet exemple illustre la fonction de MBean qui permet d'imprimer une liste des relations établies entre les rôles.

Remarque : Pour utiliser ce script, vous devez sélectionner l'option permettant d'installer les exemples de code lors de l'installation de WebSphere Process Server.

L'exemple de script Jacl est situé dans *install_root*/samples/JMXSample/scripts et *install_root*\samples\JMXSample\scripts. Il se nomme `RelServicesAdmin.jacl`.

Pour exécuter ce script, entrez : UNIX Linux

```
wsadmin -f install_root/samples/JMXSample/scripts/RelServicesAdmin.jacl
 -serveur nomserveur -noeud nomnoeud
```

script, entrez : Windows

```
wsadmin -f install_root\samples\JMXSample\scripts\RelServicesAdmin.jacl
 -serveur nomserveur -noeud nomnoeud
```

Ce script permet d'appeler jusqu'à 10 relations dans votre environnement et d'imprimer jusqu'à 10 rôles par relations sur la console.

Exercice : Rédaction d'un script Jacl

A propos de cette tâche

Les concepts de base de ce script peuvent être utilisés pour communiquer avec n'importe quel bean du système. Les seuls éléments obligatoires sont le nom et le type de MBean ainsi que les méthodes et les attributs disponibles sur ce bean. Les commandes getAttribute et setAttribute sont utilisées pour les attributs. La commande invoke est utilisée pour les méthodes. Exécutez les étapes ci-après pour créer un script `.jacl` permettant de gérer le bean MBean relatif à la sécurité JMX.

Remarque : A chaque étape, le code est préfacé d'une instruction expliquant le rôle du code.

Procédure

1. Détermination du **nom du noeud**

   La première partie du script figurant ci-dessous permet de déterminer le nom du noeud. Si le `nom du noeud` n'est pas correctement indiqué, la syntaxe appropriée est imprimée et le script se ferme.

   ```
   # Lisez et validez les arguments

       if {{$argc == 1 } && { [lindex $argv $i] == "-nodeName" } {
               set nodeName [lindex $argv $i]
   ```

2. Identification de **MBean**

   Un bean géré MBean est identifié par un type et un nom.

   Remarque : Le nom et le type sont codés en dur dans le cas présent car vous connaissez le bean MBean que vous souhaitez utiliser.
   La seconde partie du script permet d'identifier le MBean.

   ```
   # Ces deux variables, mbeanName et mbeanType sont utilisées
     uniquement pour identifier le bean MBean.
          # Pour cet exemple, nous utiliserons le MBean qui permet d'accéder
            aux services de relations.

          set mbeanName"RelService"
          set mbeanType"WBIRelServices"
   ```

3. Localisation de MBean et définition de la **référence** correspondante

   Utilisez le code indiqué ici pour définir la référence pour le bean MBean.

   ```
   # Localisez le mbean et définissez une référence dans la variable "relSvcsMBean"

          set relSvcsMBean [$AdminControl queryNames
              name=$mbeanName,node=$nodeName,type=$mbeanType,*]
   ```

4. Appel de la **relation** à l'aide de la commande getAttribute

   La documentation propre à ce bean MBean définit un attribut nommé `allRelationshipNames`. Interrogez le MBean au sujet de cet attribut à l'aide de la commande getAttribute. La valeur de cet attribut prendra la forme d'une liste que vous serez amené à parcourir au cours de la prochaine étape dans laquelle la commande est appelée.

```
# Demandez la liste de relations à partir du mbean

       set relationships
        [$AdminControl getAttribute $relSvcsMBean allRelationshipNames]
```

5. Appel de la **commande** pour chaque nom de relation, impression du nom et retour au MBean pour obtenir des informations supplémentaires

   Dans cet exemple, le MBean définit une méthode appelée getAllRoleNames avec un seul paramètre pour le nom de relation spécifique. La commande invoke vous permet d'appeler cette méthode, en transmettant le nom de la relation en cours. Pour chaque rôle de la relation, un nom est imprimé.

```
# Parcourez toute la liste des noms de rôle et imprimez-les

         foreach roleName $roles {
           puts "    Role: $roleName"
         }
      }
   } else {
         # les arguments sont incorrects, la syntaxe correcte est imprimée
            puts "Usage: wsadmin -f RelServicesAdmin.jacl -nodeName nodeName"
   }
```

Résultats

Vous venez de rédiger un script permettant d'appeler des relations.

Remarques

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

Il se peut qu'IBM ne propose pas les produits, services ou fonctions décrits dans ce document dans d'autres pays. Contactez votre représentant IBM local pour plus d'informations sur les produits et services actuellement disponibles dans votre pays. Toute référence à un produti, 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 le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Pour les demandes relatives aux licences et informations DBCS, 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-CONTREFACON 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 matériels de ces sites Web ne font pas partie des matériels utilisés dans ce produit IBM et l'utilisation de ces sites Web s'effectue à vos risques et périls.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange 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
577 Airport Blvd., Suite 800
Burlingame, CA 94010
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.

Toute 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 écrit. 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 code sont dérivés des Programmes exemples d'IBM Corp. (c) Copyright IBM Corp. _entrez la ou les année(s)_. 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, noms de produits et logos

IBM, le logo IBM, Domino, Tivoli, WebSphere et z/OS sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

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

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

Linux est une marque de Linus Torvalds 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 6.1.0