IBM WebSphere Process Server for Multiplatforms

Sécurisation des applications et de leurs environnements

Version 7.0.0

juin 2012

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
17, avenue de l'Europe
92275 Bois-Colombes Cedex

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 de WebSphere Process Server et des applications

La protection de WebSphere Process Server et des applications dépend de la sécurisation de l'environnement d'exécution et des applications.

La sécurisation de l'environnement d'exécution WebSphere Process Server implique l'activation de la sécurité administrative et de la sécurité des applications, la création de profils de sécurité et la limitation de l'accès aux fonctions essentielles pour que seuls les utilisateurs sélectionnés en bénéficient.

La sécurisation d'une application inclut l'authentification des utilisateurs, l'implémentation du contrôle d'accès pour les opérations et les ressources, ainsi que la préservation de l'intégrité des données et de la confidentialité.

La sécurité de WebSphere Process Server est basée sur la sécurité de WebSphere Application Server version 7.0. Ces documents sont en supplément de la documentation sur la sécurité fondamentale située dans le centre de documentation de WebSphere Application Server (plus spécifiquement, dans les rubriques du document «Sécurisation des applications et de leur environnement»).

Présentation générale de la sécurité

La sécurité de WebSphere Process Server est basée sur la sécurité de WebSphere Application Server version 7.0.

Pour obtenir des informations détaillées sur la sécurité, consultez le WebSphere Application Server Network Deploymentcentre de documentation.

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 des applications ; 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. Cela inclut :

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

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 7.0. La section suivante répertorie les caractéristiques spécifiques à WebSphere Process Server.

- La page Sécurité Business Integration de la console d'administration est spécifique à WebSphere Process Server. Pour accéder à cette page, développez **Sécurité** et cliquez sur **Sécurité Business Integration**.

  Cette page permet aux utilisateurs d'attribuer des identités spécifiques de leur registre d'utilisateurs aux alias d'authentification Business Integration. Elle 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.
- WebSphere Process Server contient un ensemble de rôles de sécurité spécifiques aux composants.

Initiation à la sécurité

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

La liste suivante présente les tâches à effectuer lorsque vous sécurisez WebSphere Process Server.

1. Prenez en compte la sécurité lorsque vous installez WebSphere Process Server.
   a. Sécurisez votre environnement avant l'installation.
   b. Préparez le système d'exploitation en vue de l'installation de WebSphere Process Server.
   c. Préparez votre environnement après l'installation.
2. Assurez-vous que la sécurité est activée pour votre installation autonome ou en environnement de déploiement.
   a. Assurez-vous que la sécurité administrative est activée.
   b. Assurez-vous que la sécurité des applications est activée.
   c. Si nécessaire, activez la sécurité Java 2.
   d. Utilisez l'assistant de configuration de la sécurité dans la console d'administration pour configurer les options de sécurité.
   e. Configurez un mécanisme d'authentification sécurisé et un référentiel de comptes utilisateur.
   f. Affectez des noms et des mots de passe utilisateur à des alias d'authentification Business Integration importants.
   g. Affectez les utilisateurs aux rôles de sécurité appropriés.
3. Configurez la sécurité des composants de WebSphere Process Server spécifiques. Par exemple, configurez le contrôle d'accès basé sur les rôles des calendriers, à l'aide du widget Rôles de sécurité, dans le widget Agendas métier.
4. Sécurisez les applications que vous déployez dans votre environnement Process Server.
   a. Développez vos applications dans WebSphere Integration Developer en utilisant l'ensemble des fonctions de sécurité prévues.

b. Déployez vos applications dans votre environnement WebSphere Process Server.
c. Affectez des utilisateurs ou des groupes aux rôles de sécurité appropriés pour contrôler l'accès à l'application venant d'être déployée.

5. Gérez la sécurité de votre environnement WebSphere Process Server.

Installation d'WebSphere Process Server : remarques sur la sécurité

Envisagez de quelle façon la sécurité sera mise en oeuvre avant, pendant et après l'installation de WebSphere Process Server.

Procédure

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 **Préparation de la sécurité lors de l'installation** du centre de documentation de WebSphere Application Server du centre de documentation de.

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

   Windows Linux UNIX Cette étape explique comment préparer les différents systèmes d'exploitation en vue de l'installation de WebSphere Process Server. Pour des informations détaillées sur la préparation de votre système d'exploitation en vue de l'installation, voir la rubrique **Préparation du système d'exploitation en vue de l'installation du produit** dans le centre de documentation de WebSphere Application Server .

3. Sécurisation de l'environnement après l'installation.

   Cette étape explique comment protéger les informations relatives aux mots de passe, une fois WebSphere Process Server installé. Pour des informations détaillées sur la sécurisation de l'environnement après l'installation, voir la rubrique **Sécurisation de l'environnement après l'installation** dans le 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.

Informations d'authentification fournies au moment de l'installation

Lors de l'installation, tous les composants utilisent par défaut les données d'identification principales que vous indiquez. Ces valeurs par défaut offrent une sécurité de base. Cependant, pour renforcer la sécurité de votre installation, nous vous conseillons de configurer les divers composants de WebSphere Process Server afin d'obtenir les identités de sécurité appropriées.

Lorsque vous créez un profil WebSphere Process Serveret maintenez l'option **Activer la sécurité administrative** sélectionnée, une invite de saisie du nom d'utilisateur s'affiche. 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 des 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 dans la page Sécurité Business Integration de la console d'administration.

Création de profils WebSphere Process Server avec sécurité

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

Pourquoi et quand exécuter 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

Procédure

1. Dans la console d'administration, affichez la page Sécurité Business Integration. Cliquez sur **Sécurité**, puis sur **Sécurité Business Integration**.
2. Pour chacun des alias d'authentification Service Component Architecture, Business Process Choreographer et Common Event Infrastructure, indiquer le nom d'utilisateur et le mot de passe appropriés à utiliser comme alias.
   a. Sélectionner l'alias que vous souhaitez modifier en cliquant sur son nom dans la colonne **Alias**.

      Remarque : Dans certains cas, la colonne **Alias** peut ne pas contenir de lien. Dans ce cas, cochez la case de la colonne **Sélectionner** correspondant à l'alias que vous souhaitez éditer et cliquez sur **Editer**.
   b. Dans la page suivante, spécifiez le nom d'utilisateur et le mot de passe devant servir d'alias d'authentification pour ce composant.

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

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

La configuration de la sécurité d'une installation autonome de WebSphere Process Server comprend des tâches comme l'activation de la sécurité administrative et la configuration d'un registre de compte utilisateur.

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 à partir de la console d'administration. Il est donc capital que vous sécurisiez l'environnement avant de déployer des applications sécurisées.

Pourquoi et quand exécuter cette tâche

Les étapes suivantes constituent un plan des tâches à effectuer pour activer la sécurité. Dans les rubriques sui suivent, vous trouverez plus de précisions sur ces tâches.

Procédure

Procédure

1. S'assurer que la sécurité d'administration est activée. «Activation de la sécurité».
2. S'assurer que la sécurité des applications est activée. «Activation de la sécurité».
3. Sélectionner le référentiel de comptes utilisateur que vous voulez utiliser. «Configuration d'un référentiel de comptes utilisateur», à la page 7

   Assurez-vous d'avoir défini le registre sélectionné comme étant votre registre courant à l'aide de l'option **Définir comme courant**.
4. Ajouter des utilisateurs ou des groupes au rôle d'administrateur.
5. Si nécessaire, arrêtez et redémarrez le serveur. «Démarrage et arrêt du serveur», à la page 14
6. Configurez les alias d'authentification, les contrôles d'accès et les autres mécanismes de sécurité de vos composants installés. «Sécurisation des applications dans WebSphere Process Server», à la page 30

Activation de la sécurité

La première étape de la sécurisation de votre environnement WebSphere Process Server et de vos applications est de s'assurer que la sécurité d'administration est activée.

Avant de commencer

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

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

Pourquoi et quand exécuter cette tâche

A l'aide de la console d'administration, vous pouvez activer la sécurité d'administration, la sécurité des applications et la sécurité Java 2.

- La *sécurité d'administration* 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 configuration de la sécurité administrative s'applique à chaque serveur du domaine de sécurité.

- 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.

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

- La *sécurité Java 2* présente un mécanisme de contrôle d'accès à granularité fine et reposant sur des règles, qui augmente l'intégrité de l'ensemble du système en vérifiant les droits d'accès avant d'autoriser l'accès à certaines ressources du système. La sécurité Java 2 protège l'accès aux ressources système, telles que les E-S de fichiers, les sockets et les propriétés. Elle protège également l'accès aux ressources Web, telles que les servlets, les fichiers JSP (JavaServer Pages) et les méthodes d'EJB (Enterprise JavaBeans).

  La sécurité Java 2 étant relativement nouvelle, il est possible que beaucoup d'applications existantes, voire des applications nouvelles, ne soient pas adaptées pour le modèle de programmation de contrôle d'accès à granularité très fine que la sécurité Java 2 est capable d'appliquer. Les administrateurs doivent connaître les conséquences possibles de l'activation de la sécurité Java 2 lorsque les applications n'y sont pas prêtes. La sécurité Java 2 implique de nouvelles exigences pour les développeurs d'applications et les administrateurs.

  Avertissement : Les groupes de correctifs qui incluent des mises à jour du kit de développement de logiciels (SDK) sont susceptibles de remplacer les fichiers de règles sans restriction. Faites une sauvegarde de ces fichiers avant d'appliquer le groupe de correctifs, puis restaurez cette sauvegarde une fois le groupe de correctifs appliqué.

Procédure

Procédure

1. Ouvrez la page de la sécurité d'administration dans la console d'administration.

   Développez **Sécurité** et cliquez sur **Sécurité globale**.
2. Activation de la sécurité d'administration.

   Sélectionnez **Activer la sécurité d'administration**.
3. Activez la sécurité des applications.

   Sélectionnez **Activer la sécurité des applications**.
4. Facultatif : Exécutez la sécurité de Java 2, si nécessaire.

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

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

a. Facultatif : Sélectionnez **Prévenir si des applications accordent des permissions personnalisées**. Le fichier `filter.policy` contient une liste de droits d'accès qu'une application ne doit pas posséder conformément à la spécification J2EE 1.4. Si une application est installée avec un droit d'accès indiqué dans ce fichier de règles et que cette option est activée, un avertissement est émis. Par défaut, elle est activée.

b. Facultatif : Sélectionnez **Limiter l'accès aux données d'authentification des ressources**. Activez cette option si vous devez restreindre l'accès des applications à des données sensibles d'authentification de mappage Java Connector Architecture (JCA).

5. Validez ces modifications.

   Cliquez sur le bouton **Valider** dans la partie inférieure de la page.

6. Enregistrez les modifications dans la configuration locale.

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

7. Si nécessaire, arrêtez et redémarrez le serveur.

   Si le serveur doit être redémarré, un message s'affiche dans la console d'administration.

Que faire ensuite

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

Configuration d'un référentiel de comptes utilisateur

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

Pourquoi et quand exécuter 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 Dans un environnement de déploiement réseau, vous devez utiliser LDAP comme registre d'utilisateurs.

Procédure

Procédure

1. Accédez au panneau Administration, applications et infrastructure sécurisées dans la console d'administration. Développez **Sécurité** et cliquez sur **Sécurité globale**.
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 basé sur fichiers qui est 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	Il s'agit du registre d'utilisateurs par défaut. **Remarque :** Windows Linux UNIX N'utilisez pas le système d'exploitation local comme registre d'utilisateurs dans un environnement de déploiement réseau. Suivre les instructions de la section «Configuration du registre de comptes utilisateur autonome personnalisé ou sur système d'exploitation local», à la page 9.
LDAP (Lightweight Directory Access Protocol)	Suivez les instructions de la section «Configuration de LDAP (Lightweight Directory Access Protocol) comme annuaire des utilisateurs», à la page 10 pour configurer le protocole LDAP comme registre d'utilisateurs.
Registre d'utilisateurs personnalisé	Suivez les instructions dans «Configuration du registre de comptes utilisateur autonome personnalisé ou sur système d'exploitation local», à la page 9 pour choisir un référentiel de comptes personnalisé et le configurer selon vos besoins=.
Tivoli Access Manager	**Remarque :** Cette option n'est disponible que par la console d'administration. Elle doit être configurée au moyen de la commande wsadmin.

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

Vous pouvez configurer votre référentiel de comptes utilisateur à l'aide de la console d'administration. Les étapes de configuration du registre de comptes utilisateurs sur système d'exploitation local, valeur par défaut, ou en mode autonome personnalisé sont similaires.

Pourquoi et quand exécuter cette tâche

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

Procédure

Procédure

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

   Développer **Sécurité**, cliquer sur **Sécurité globale** et sélectionner le registre d'utilisateurs que vous employez sous le menu **Définitions de domaine disponibles**. Cliquer sur **Configurer**.
2. Facultatif : Entrer un nom d'utilisateur valide dans la zone **Nom de l'utilisateur principal d'administration**.

   Cette valeur est le nom d'un utilisateur possédant des droits d'administration qui est défini dans le registre. Ce nom d'utilisateur sert à accéder à la console d'administration. Il est également employé par la commande **wsadmin**.
3. Sélectionner l'option **Identité de serveur généré automatiquement** ou **Identité de serveur stockée dans un référentiel**.
   - Si vous sélectionnez **Identité serveur générée automatiquement**, le serveur d'applications générera l'identité serveur utilisée pour communiquer les processus en interne.

     Vous pourrez modifier cette identité serveur sur la page Mécanismes d'authentification et expiration. Pour accéder à la page Mécanismes d'authentification et d'expiration, cliquer sur **Sécurité** > **Sécurité globale** > **Mécanismes d'authentification et d'expiration**. Modifier la valeur de la zone **ID de serveur interne**.
   - Si vous sélectionnez l'option **Identité de serveur stockée dans un référentiel**, entrez les informations suivantes :
     - Dans **ID utilisateur ou utilisateur d'administration du serveur sur un noeud de version 7.0**, indiquez un ID utilisateur qui serve à exécuter le serveur d'applications à des fins de sécurité.
     - Dans **Mot de passe**, indiquer le mot de passe associé à ce nom d'utilisateur.
4. Facultatif : Pour les registres personnalisés autonomes uniquement, suivre la procédure ci-dessous :
   a. Vérifier que la valeur dans la zone **Nom de classe du registre personnalisé** est correcte ou la modifier le cas échéant.
   b. Cocher ou décocher la case **Ignorer la casse pour l'authentification**.

      Cette option cochée, le contrôle d'autorisation n'est pas sensible à la casse.
5. Cliquez sur **Valider**.
6. Au bas de la page, cliquer sur **Définir comme authentification en vigueur**.

7. Cliquer sur **OK**, puis sur **Appliquer** ou **Sauvegarder**.

Que faire ensuite

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

Si le serveur démarre sans problème, c'est que sa configuration d'installation est correcte.

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

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

Pourquoi et quand exécuter 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**. Consultez la rubrique du centre de documentation WebSphere Application Server : Transmission des règles de sécurité des applications installées à un fournisseur JACC à l'aide de wsadmin.

Configuration de LDAP (Lightweight Directory Access Protocol) comme annuaire des utilisateurs

Par défaut, l'annuaire des utilisateurs est l'annuaire du système d'exploitation local. Si vous préférez, vous pouvez utiliser un annuaire LDAP externe comme annuaire des utilisateurs.

Avant de commencer

Cette tâche part du principe que la sécurité d'administration est activée.

Pour accéder à un annuaire d'utilisateurs via LDAP, vous devez connaître un nom d'utilisateur (ID) et un mot de passe valides, le nom d'hôte et le numéro de port du serveur d'annuaire, le nom distinctif (DN) de base et, si nécessaire, le DN de connexion et le mot de passe de connexion.

Dans un environnement de déploiement réseau, il vous faut utiliser LDAP.

Vous pouvez choisir n'importe quel utilisateur qui peut être recherché dans l'annuaire d'utilisateurs. Vous pouvez utiliser tout ID utilisateur doté du rôle d'administrateur pour vous connecter.

Important : Si vous configurez WebSphere Process Server pour utiliser plusieurs serveurs LDAP, sachez que la valeur affichée dans la page **Sécurité globale** > **Annuaire LDAP autonome** de la console d'administration risque de ne pas refléter le serveur LDAP utilisé.

Procédure

Procédure

1. Démarrez la console d'administration.
   - Si la sécurité est désactivée, vous êtes invité à entrer un ID utilisateur. Utilisez l'ID utilisateur de vos souhaits pour vous connecter.

- Si la sécurité est activée, vous êtes invité à entrer un ID utilisateur et un mot de passe. Connectez-vous avec un ID utilisateur et un mot de passe d'administration prédéfinis.

2. Développez **Sécurité** et cliquez sur **Sécurité globale**.
3. De la page Administration, applications et infrastructure sécurisées, suivre les étapes ci-dessous.
   a. Assurez-vous que **Activer la sécurité d'administration** est sélectionné.
   b. Dans la liste **Définitions de domaine disponibles**, sélectionnez **Annuaire LDAP autonome**.
   c. Cliquer sur **Configurer**.
4. Sur l'onglet **Configuration** de la page Annuaire LDAP autonome, suivez les étapes ci-dessous.
   a. Entrer 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 sert à accéder à la console d'administration. Il est également employé par la commande **wsadmin**.

      Vous pouvez entrer soit le nom distinctif (DN) complet de l'utilisateur ou son nom abrégé, tel que défini par le filtre d'utilisateurs à la page Paramètres LDAP avancés.
   b. Facultatif : Sélectionnez l'option **Identité de serveur généré automatiquement** ou **Identité de serveur stockée dans un référentiel**.
      - Si vous sélectionnez **Identité serveur générée automatiquement**, le serveur d'applications générera l'identité serveur utilisée pour communiquer les processus en interne.

        Vous pourrez modifier cette identité serveur sur la page Mécanismes d'authentification et expiration. Pour accéder à la page Mécanismes d'authentification et d'expiration, cliquez sur **Sécurité** > **Sécurité globale** > **Mécanismes d'authentification et d'expiration**. Modifier la valeur de la zone **ID de serveur interne**.
      - Si vous sélectionnez l'option **Identité de serveur stockée dans un référentiel**, entrez les informations suivantes :
        – Dans **ID utilisateur ou utilisateur d'administration du serveur sur un noeud de version 7.0**, indiquez un ID utilisateur qui serve à exécuter le serveur d'applications à des fins de sécurité.
        – Dans **Mot de passe**, indiquer le mot de passe associé à ce nom d'utilisateur.

      Même si cet ID n'est pas l'ID utilisateur de l'administrateur LDAP, cette entrée doit exister dans l'annuaire LDAP.
   c. Facultatif : Sélectionnez le serveur LDAP à utiliser dans la liste **Type du serveur LDAP**.

      Le type de serveur LDAP détermine les filtres utilisés par défaut par WebSphere Process Server. Ces filtres par défaut changent la zone **Type du serveur LDAP** en **Personnalisé**, ce qui indique que des filtres personnalisés sont employés. Cette action a lieu une fois cliqué sur **OK** ou sur **Appliquer** sur la page Paramètres LDAP avancés. Sélectionnez le type **Personnalisé** dans la liste et modifiez les filtres d'utilisateurs et de groupes pour utiliser d'autres serveurs LDAP au besoin.

Les utilisateurs d'IBM Tivoli Directory Server peuvent sélectionner **IBM Tivoli Directory Server** comme type d'annuaire. Utilisez le type d'annuaire IBM Tivoli Directory Server pour de meilleures performances.

d. Dans la zone **Hôte**, entrez le nom complet qualifié de la machine sur laquelle réside le LDAP.

   Vous pouvez entrer soit son adresse IP, soi son nom DNS (domain name system).

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

   le nom d'hôte et le numéro de port constituent le domaine de ce serveur LDAP dans la cellule WebSphere Process Server. Donc si des cellules différentes communiquent les unes avec les autres à l'aide de jetons LTPA (Lightweight Third Party Authentication), ces domaines doivent concorder de façon exacte dans toutes les cellules.

   La valeur par défaut est 389.

   Si des WebSphere Process Server multiples sont installés et configurés pour s'exécuter dans le même domaine de connexion unique (SSO) ou que WebSphere Process Server interopère avec une version précédente de WebSphere Process Server, assurez-vous que le numéro de port concorde dans toutes les configurations.

f. Facultatif : Entrez le nom distinctif de base dans la zone **Nom distinctif (DN) de base**.

   Le nom distinctif de base indique le point de départ des recherches LDAP dans ce serveur d'annuaire LDAP. Par exemple, pour un utilisateur au DN `cn=John Doe, ou=Rochester, o=IBM, c=US`, indiquez le DN de base en tant que l'une des options parmi les suivantes (en présumant d'un suffixe de c=us): `ou=Rochester, o=IBM, c=us` or `o=IBM c=us` or `c=us`.

   A des fins d'autorisation, cette zone est sensible à la casse. Cette spécification implique que si un jeton est reçu (d'une autre cellule ou d'un serveur Lotus Domino, par exemple), le nom distinctif (DN) de base dans le serveur doit correspondre au DN de base d'une autre cellule ou d'un serveur Domino. Si le respect de la casse n'est pas pris en compte pour l'autorisation, activez **Ignorer la casse pour l'autorisation**.

   Dans WebSphere Process Server, le nom distinctif est normalisé au regard de la spécification de LDAP (Lightweight Directory Access Protocol). La normalisation consiste en la suppression des espaces dans le nom distinctif de base avant ou après les virgules ou les signes égal. Voici un exemple de nom distinctif de base non normalisé : `o = ibm, c = us` ou `o=ibm, c=us`. Voici un exemple de nom distinctif de base normalisé : `o=ibm,c=us`.

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

g. Facultatif : Entrez le DN de connexion dans la zone **Nom distinctif de connexion**.

   Le DN de connexion est obligatoire si les sessions de liaison ne sont pas possibles sur le serveur LDAP pour obtenir les informations d'utilisateurs et de groupe.

   Si le serveur LDAP est paramétré pour utiliser les sessions de liaison anonymes, laissez cette zone vierge. Si aucun nom n'est précisé, le serveur d'applications effectuera la liaison de façon anonyme. Pour des exemples de noms distinctifs, voir la description de la zone Nom distinctif de base.

h. Facultatif : Entrez le mot de passe correspondant au DN de connexion dans la zone **Mot de passe de connexion**.

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

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

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

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

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

   Lorsque vous activez cette option, la vérification des autorisations ne fait pas de distinction entre les majuscules et les minuscules.

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

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

   Par défaut, elle est activée.

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

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

   - **Géré de façon centrale**

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

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

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

   - **Utiliser un alias SSL spécifique**

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

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

m. Cliquez sur **OK** puis soit sur **Appliquer**, soit sur **Enregistrer** pour revenir à la page Administration, applications et infrastructure sécurisées.

5. Sur la page Administration, applications et infrastructure sécurisées, cliquez sur **Définir comme courant**.
6. Cliquer sur **OK**, puis sur **Appliquer** ou **Sauvegarder**.

Que faire ensuite

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

Si le serveur démarre sans problème, c'est que sa configuration d'installation est correcte.

Démarrage et arrêt du serveur

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

Avant de commencer

La sécurité administrative doit être activée.

Eviter les incidents : Vista Windows 7 Si le contrôle de compte utilisateur (UAC) est activé à certains niveaux, le serveur d'applications doit être démarré avec des droits d'administrateur si vous utilisez un invite de commande. Démarrez le serveur d'applications depuis l'invite de commande qui s'ouvre en exécutant les actions suivantes :

- Cliquez avec le bouton droit sur un raccourci d'invite de commande.
- Cliquez sur **Exécuter en tant qu'administrateur**.
- Quand vous ouvrez la fenêtre d'invite de commande en tant qu'administrateur, une boîte de dialogue du système d'exploitation apparaît et vous demande si vous voulez continuer. Cliquez sur **Continuer** pour poursuivre.

Procédure

Procédure

1. Démarrez le serveur.

   Le tableau suivant décrit les options de démarrage du serveur.

Démarrer le serveur	Détails
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`***

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	Détails
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`***

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	Détails
A partir de l'interface utilisateur	Le panneau Premiers pas affiche les résultats de votre demande.
Depuis une ligne de commande	Le résultat de votre demande est affiché dans le panneau 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.

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

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

Tableau 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 membre du rôle opérateur dispose des privilèges d'un moniteur, plus la capacité de modifier l'état d'exécution du serveur (c'est-à-dire démarrer et arrêter le serveur).
Administrateur	Un administrateur dispose à la fois des droits d'un configurateur et d'un opérateur, plus quelques privilèges qui sont propres à ce rôle. Par exemple : • Modifier l'ID utilisateur et le mot de passe du serveur • Mapper les utilisateurs et les groupes vers le rôle d'administrateur L'administrateur dispose également des droits requis pour accéder à des informations sensibles, comme : • Mots de passe LTPA (Lightweight Third Party Authentication) • Clés
ISC Admins	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 ISC Admins peut effectuer les tâches suivantes : • Création, mise à jour ou suppression d'utilisateurs dans la configuration des référentiels fédérés • Créer, mettre à jour ou supprimer les groupes dans la configuration des référentiels fédérés
Déployeur	Seuls les utilisateurs associés à ce rôle peuvent effectuer des opérations de configuration et d'exécution sur les applications.
Gestionnaire de la sécurité administrative	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.
Auditeur	Seuls les utilisateurs associés à ce rôle peuvent afficher et modifier les paramètres de configuration du sous-système d'audit de la sécurité. **Remarque :** Le rôle d'auditeur inclut le rôle de moniteur. Cela permet à l'auditeur d'afficher le reste de la configuration de sécurité sans y apporter de modifications.

Pour plus d'informations, voir Rôles d'administration dans le centre de documentation de WebSphere Application Server.

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.

Conseil : Pour faciliter l'administration du système, mappez un ou plusieurs groupes d'utilisateurs vers des rôles de sécurité, plutôt que des utilisateurs individuels. Le mappage d'un groupe d'utilisateurs vers un rôle de sécurité, ainsi que l'ajout ou la suppression d'utilisateurs dans un groupe, s'effectuent à l'extérieur de WebSphere Process Server et ne nécessitent donc pas de redémarrer le serveur.

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

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

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

- Le sujet spécial **AllAuthenticated** signifie que le contrôle d'accès du rôle d'administration garantit que l'utilisateur effectuant la requête est au moins authentifié.
- Le sujet spécial **Everyone** signifie que n'importe quel utilisateur, authentifié ou non, peut effectuer l'action, comme si la sécurité n'était pas activée.

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

La configuration de la sécurité d'une installation d'environnement de déploiement de WebSphere Process Server comprend des tâches comme l'activation de la sécurité administrative et la configuration d'un registre de compte utilisateur.

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 à partir de la console d'administration. Il est donc capital que vous sécurisiez l'environnement avant de déployer des applications sécurisées.

Pourquoi et quand exécuter cette tâche

Les étapes suivantes constituent un plan des tâches à effectuer pour activer la sécurité. Dans les rubriques sui suivent, vous trouverez plus de précisions sur ces tâches.

Procédure

Procédure

1. S'assurer que la sécurité d'administration est activée. «Activation de la sécurité» , à la page 5.
2. S'assurer que la sécurité des applications est activée. «Activation de la sécurité», à la page 5.

3. Sélectionner le référentiel de comptes utilisateur que vous voulez utiliser. «Configuration d'un référentiel de comptes utilisateur», à la page 7

   Assurez-vous d'avoir défini le registre sélectionné comme étant votre registre courant à l'aide de l'option **Définir comme courant**.
4. Ajouter des utilisateurs ou des groupes au rôle d'administrateur.
5. Si nécessaire, arrêtez et redémarrez le serveur. «Démarrage et arrêt du serveur», à la page 14
6. Configurez les alias d'authentification, les contrôles d'accès et les autres mécanismes de sécurité de vos composants installés. «Sécurisation des applications dans WebSphere Process Server», à la page 30

Activation de la sécurité

La première étape de la sécurisation de votre environnement WebSphere Process Server et de vos applications est de s'assurer que la sécurité d'administration est activée.

Avant de commencer

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

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

Pourquoi et quand exécuter cette tâche

A l'aide de la console d'administration, vous pouvez activer la sécurité d'administration, la sécurité des applications et la sécurité Java 2.

- La *sécurité d'administration* 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 configuration de la sécurité administrative s'applique à chaque serveur du domaine de sécurité.
- 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.

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

- La *sécurité Java 2* présente un mécanisme de contrôle d'accès à granularité fine et reposant sur des règles, qui augmente l'intégrité de l'ensemble du système en vérifiant les droits d'accès avant d'autoriser l'accès à certaines ressources du système. La sécurité Java 2 protège l'accès aux ressources système, telles que les E-S de fichiers, les sockets et les propriétés. Elle protège également l'accès aux ressources Web, telles que les servlets, les fichiers JSP (JavaServer Pages) et les méthodes d'EJB (Enterprise JavaBeans).

  La sécurité Java 2 étant relativement nouvelle, il est possible que beaucoup d'applications existantes, voire des applications nouvelles, ne soient pas adaptées pour le modèle de programmation de contrôle d'accès à granularité très fine que la sécurité Java 2 est capable d'appliquer. Les administrateurs doivent connaître les conséquences possibles de l'activation de la sécurité Java 2 lorsque les applications n'y sont pas prêtes. La sécurité Java 2 implique de nouvelles exigences pour les développeurs d'applications et les administrateurs.

  Avertissement : Les groupes de correctifs qui incluent des mises à jour du kit de développement de logiciels (SDK) sont susceptibles de remplacer les fichiers de règles sans restriction. Faites une sauvegarde de ces fichiers avant d'appliquer le groupe de correctifs, puis restaurez cette sauvegarde une fois le groupe de correctifs appliqué.

Procédure

Procédure

1. Ouvrez la page de la sécurité d'administration dans la console d'administration.

   Développez **Sécurité** et cliquez sur **Sécurité globale**.
2. Activation de la sécurité d'administration.

   Sélectionnez **Activer la sécurité d'administration**.
3. Activez la sécurité des applications.

   Sélectionnez **Activer la sécurité des applications**.
4. Facultatif : Exécutez la sécurité de Java 2, si nécessaire.

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

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

   a. Facultatif : Sélectionnez **Prévenir si des applications accordent des permissions personnalisées**. Le fichier `filter.policy` contient une liste de droits d'accès qu'une application ne doit pas posséder conformément à la spécification J2EE 1.4. Si une application est installée avec un droit d'accès indiqué dans ce fichier de règles et que cette option est activée, un avertissement est émis. Par défaut, elle est activée.

   b. Facultatif : Sélectionnez **Limiter l'accès aux données d'authentification des ressources**. Activez cette option si vous devez restreindre l'accès des applications à des données sensibles d'authentification de mappage Java Connector Architecture (JCA).

5. Validez ces modifications.
   Cliquez sur le bouton **Valider** dans la partie inférieure de la page.
6. Enregistrez les modifications dans la configuration locale.
   Cliquez sur **Sauvegarder** dans la fenêtre de message.
7. Si nécessaire, arrêtez et redémarrez le serveur.
   Si le serveur doit être redémarré, un message s'affiche dans la console d'administration.

Que faire ensuite

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

Configuration d'un référentiel de comptes utilisateur

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

Pourquoi et quand exécuter 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 Dans un environnement de déploiement réseau, vous devez utiliser LDAP comme registre d'utilisateurs.

Procédure

Procédure

1. Accédez au panneau Administration, applications et infrastructure sécurisées dans la console d'administration. Développez **Sécurité** et cliquez sur **Sécurité globale**.
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 basé sur fichiers qui est 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	Il s'agit du registre d'utilisateurs par défaut. **Remarque :** Windows Linux UNIX N'utilisez pas le système d'exploitation local comme registre d'utilisateurs dans un environnement de déploiement réseau. Suivre les instructions de la section «Configuration du registre de comptes utilisateur autonome personnalisé ou sur système d'exploitation local», à la page 9.
LDAP (Lightweight Directory Access Protocol)	Suivez les instructions de la section «Configuration de LDAP (Lightweight Directory Access Protocol) comme annuaire des utilisateurs», à la page 10 pour configurer le protocole LDAP comme registre d'utilisateurs.
Registre d'utilisateurs personnalisé	Suivez les instructions dans «Configuration du registre de comptes utilisateur autonome personnalisé ou sur système d'exploitation local», à la page 9 pour choisir un référentiel de comptes personnalisé et le configurer selon vos besoins=.
Tivoli Access Manager	**Remarque :** Cette option n'est disponible que par la console d'administration. Elle doit être configurée au moyen de la commande wsadmin.

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

Vous pouvez configurer votre référentiel de comptes utilisateur à l'aide de la console d'administration. Les étapes de configuration du registre de comptes utilisateurs sur système d'exploitation local, valeur par défaut, ou en mode autonome personnalisé sont similaires.

Pourquoi et quand exécuter cette tâche

Vous pouvez choisir d'autoriser WebSphere Process Server à générer automatiquement une identité utilisateur de serveur ou vous pouvez en indiquer

une issue du référentiel de comptes utilisateur que vous utilisez. Cette dernière option améliore l'auditabilité des opérations d'administration.

Procédure

Procédure

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

   Développer **Sécurité**, cliquer sur **Sécurité globale** et sélectionner le registre d'utilisateurs que vous employez sous le menu **Définitions de domaine disponibles**. Cliquer sur **Configurer**.
2. Facultatif : Entrer un nom d'utilisateur valide dans la zone **Nom de l'utilisateur principal d'administration**.

   Cette valeur est le nom d'un utilisateur possédant des droits d'administration qui est défini dans le registre. Ce nom d'utilisateur sert à accéder à la console d'administration. Il est également employé par la commande **wsadmin**.
3. Sélectionner l'option **Identité de serveur généré automatiquement** ou **Identité de serveur stockée dans un référentiel**.
   - Si vous sélectionnez **Identité serveur générée automatiquement**, le serveur d'applications générera l'identité serveur utilisée pour communiquer les processus en interne.

     Vous pourrez modifier cette identité serveur sur la page Mécanismes d'authentification et expiration. Pour accéder à la page Mécanismes d'authentification et d'expiration, cliquer sur **Sécurité** > **Sécurité globale** > **Mécanismes d'authentification et d'expiration**. Modifier la valeur de la zone **ID de serveur interne**.
   - Si vous sélectionnez l'option **Identité de serveur stockée dans un référentiel**, entrez les informations suivantes :
     - Dans **ID utilisateur ou utilisateur d'administration du serveur sur un noeud de version 7.0**, indiquez un ID utilisateur qui serve à exécuter le serveur d'applications à des fins de sécurité.
     - Dans **Mot de passe**, indiquer le mot de passe associé à ce nom d'utilisateur.
4. Facultatif : Pour les registres personnalisés autonomes uniquement, suivre la procédure ci-dessous :
   a. Vérifier que la valeur dans la zone **Nom de classe du registre personnalisé** est correcte ou la modifier le cas échéant.
   b. Cocher ou décocher la case **Ignorer la casse pour l'authentification**.

      Cette option cochée, le contrôle d'autorisation n'est pas sensible à la casse.
5. Cliquez sur **Valider**.
6. Au bas de la page, cliquer sur **Définir comme authentification en vigueur**.
7. Cliquer sur **OK**, puis sur **Appliquer** ou **Sauvegarder**.

Que faire ensuite

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

Si le serveur démarre sans problème, c'est que sa configuration d'installation est correcte.

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

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

Pourquoi et quand exécuter 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**. Consultez la rubrique du centre de documentation WebSphere Application Server : Transmission des règles de sécurité des applications installées à un fournisseur JACC à l'aide de wsadmin.

Configuration de LDAP (Lightweight Directory Access Protocol) comme annuaire des utilisateurs

Par défaut, l'annuaire des utilisateurs est l'annuaire du système d'exploitation local. Si vous préférez, vous pouvez utiliser un annuaire LDAP externe comme annuaire des utilisateurs.

Avant de commencer

Cette tâche part du principe que la sécurité d'administration est activée.

Pour accéder à un annuaire d'utilisateurs via LDAP, vous devez connaître un nom d'utilisateur (ID) et un mot de passe valides, le nom d'hôte et le numéro de port du serveur d'annuaire, le nom distinctif (DN) de base et, si nécessaire, le DN de connexion et le mot de passe de connexion.

Dans un environnement de déploiement réseau, il vous faut utiliser LDAP.

Vous pouvez choisir n'importe quel utilisateur qui peut être recherché dans l'annuaire d'utilisateurs. Vous pouvez utiliser tout ID utilisateur doté du rôle d'administrateur pour vous connecter.

Important : Si vous configurez WebSphere Process Server pour utiliser plusieurs serveurs LDAP, sachez que la valeur affichée dans la page **Sécurité globale** > **Annuaire LDAP autonome** de la console d'administration risque de ne pas refléter le serveur LDAP utilisé.

Procédure

Procédure

1. Démarrez la console d'administration.
   - Si la sécurité est désactivée, vous êtes invité à entrer un ID utilisateur. Utilisez l'ID utilisateur de vos souhaits pour vous connecter.
   - Si la sécurité est activée, vous êtes invité à entrer un ID utilisateur et un mot de passe. Connectez-vous avec un ID utilisateur et un mot de passe d'administration prédéfinis.
2. Développez **Sécurité** et cliquez sur **Sécurité globale**.
3. De la page Administration, applications et infrastructure sécurisées, suivre les étapes ci-dessous.
   a. Assurez-vous que **Activer la sécurité d'administration** est sélectionné.

b. Dans la liste **Définitions de domaine disponibles**, sélectionnez **Annuaire LDAP autonome**.

c. Cliquer sur **Configurer**.

4. Sur l'onglet **Configuration** de la page Annuaire LDAP autonome, suivez les étapes ci-dessous.

   a. Entrer 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 sert à accéder à la console d'administration. Il est également employé par la commande **wsadmin**.

      Vous pouvez entrer soit le nom distinctif (DN) complet de l'utilisateur ou son nom abrégé, tel que défini par le filtre d'utilisateurs à la page Paramètres LDAP avancés.

   b. Facultatif : Sélectionnez l'option **Identité de serveur généré automatiquement** ou **Identité de serveur stockée dans un référentiel**.

      - Si vous sélectionnez **Identité serveur générée automatiquement**, le serveur d'applications générera l'identité serveur utilisée pour communiquer les processus en interne.

        Vous pourrez modifier cette identité serveur sur la page Mécanismes d'authentification et expiration. Pour accéder à la page Mécanismes d'authentification et d'expiration, cliquez sur **Sécurité** > **Sécurité globale** > **Mécanismes d'authentification et d'expiration**. Modifier la valeur de la zone **ID de serveur interne**.

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

        – Dans **ID utilisateur ou utilisateur d'administration du serveur sur un noeud de version 7.0**, indiquez un ID utilisateur qui serve à exécuter le serveur d'applications à des fins de sécurité.

        – Dans **Mot de passe**, indiquer le mot de passe associé à ce nom d'utilisateur.

      Même si cet ID n'est pas l'ID utilisateur de l'administrateur LDAP, cette entrée doit exister dans l'annuaire LDAP.

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

      Le type de serveur LDAP détermine les filtres utilisés par défaut par WebSphere Process Server. Ces filtres par défaut changent la zone **Type du serveur LDAP** en **Personnalisé**, ce qui indique que des filtres personnalisés sont employés. Cette action a lieu une fois cliqué sur **OK** ou sur **Appliquer** sur la page Paramètres LDAP avancés. Sélectionnez le type **Personnalisé** dans la liste et modifiez les filtres d'utilisateurs et de groupes pour utiliser d'autres serveurs LDAP au besoin.

      Les utilisateurs d'IBM Tivoli Directory Server peuvent sélectionner **IBM Tivoli Directory Server** comme type d'annuaire. Utilisez le type d'annuaire IBM Tivoli Directory Server pour de meilleures performances.

   d. Dans la zone **Hôte**, entrez le nom complet qualifié de la machine sur laquelle réside le LDAP.

      Vous pouvez entrer soit son adresse IP, soi son nom DNS (domain name system).

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

le nom d'hôte et le numéro de port constituent le domaine de ce serveur LDAP dans la cellule WebSphere Process Server. Donc si des cellules différentes communiquent les unes avec les autres à l'aide de jetons LTPA (Lightweight Third Party Authentication), ces domaines doivent concorder de façon exacte dans toutes les cellules.

La valeur par défaut est 389.

Si des WebSphere Process Server multiples sont installés et configurés pour s'exécuter dans le même domaine de connexion unique (SSO) ou que WebSphere Process Server interopère avec une version précédente de WebSphere Process Server, assurez-vous que le numéro de port concorde dans toutes les configurations.

f. Facultatif : Entrez le nom distinctif de base dans la zone **Nom distinctif (DN) de base**.

   Le nom distinctif de base indique le point de départ des recherches LDAP dans ce serveur d'annuaire LDAP. Par exemple, pour un utilisateur au DN `cn=John Doe, ou=Rochester, o=IBM, c=US`, indiquez le DN de base en tant que l'une des options parmi les suivantes (en présumant d'un suffixe de c=us): `ou=Rochester, o=IBM, c=us` or `o=IBM c=us` or `c=us`.

   A des fins d'autorisation, cette zone est sensible à la casse. Cette spécification implique que si un jeton est reçu (d'une autre cellule ou d'un serveur Lotus Domino, par exemple), le nom distinctif (DN) de base dans le serveur doit correspondre au DN de base d'une autre cellule ou d'un serveur Domino. Si le respect de la casse n'est pas pris en compte pour l'autorisation, activez **Ignorer la casse pour l'autorisation**.

   Dans WebSphere Process Server, le nom distinctif est normalisé au regard de la spécification de LDAP (Lightweight Directory Access Protocol). La normalisation consiste en la suppression des espaces dans le nom distinctif de base avant ou après les virgules ou les signes égal. Voici un exemple de nom distinctif de base non normalisé : `o = ibm, c = us` ou `o=ibm, c=us`. Voici un exemple de nom distinctif de base normalisé : `o=ibm,c=us`.

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

g. Facultatif : Entrez le DN de connexion dans la zone **Nom distinctif de connexion**.

   Le DN de connexion est obligatoire si les sessions de liaison ne sont pas possibles sur le serveur LDAP pour obtenir les informations d'utilisateurs et de groupe.

   Si le serveur LDAP est paramétré pour utiliser les sessions de liaison anonymes, laissez cette zone vierge. Si aucun nom n'est précisé, le serveur d'applications effectuera la liaison de façon anonyme. Pour des exemples de noms distinctifs, voir la description de la zone Nom distinctif de base.

h. Facultatif : Entrez le mot de passe correspondant au DN de connexion dans la zone **Mot de passe de connexion**.

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

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

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

   Cette option indique que le serveur doit réutiliser la connexion LDAP. Ne désélectionnez cette option que dans de rares cas, lorsqu'un routeur est

utilisé pour envoyer des demandes à plusieurs serveurs LDAP et que le routeur ne prend pas en charge l'affinité. Gardez cette option sélectionnée dans les autres cas.

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

   Lorsque vous activez cette option, la vérification des autorisations ne fait pas de distinction entre les majuscules et les minuscules.

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

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

   Par défaut, elle est activée.

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

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

   - **Géré de façon centrale**

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

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

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

   - **Utiliser un alias SSL spécifique**

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

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

m. Cliquez sur **OK** puis soit sur **Appliquer**, soit sur **Enregistrer** pour revenir à la page Administration, applications et infrastructure sécurisées.

5. Sur la page Administration, applications et infrastructure sécurisées, cliquez sur **Définir comme courant**.
6. Cliquer sur **OK**, puis sur **Appliquer** ou **Sauvegarder**.

Que faire ensuite

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

Si le serveur démarre sans problème, c'est que sa configuration d'installation est correcte.

Démarrage et arrêt du serveur

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

Avant de commencer

La sécurité administrative doit être activée.

Eviter les incidents : Vista Windows 7 Si le contrôle de compte utilisateur (UAC) est activé à certains niveaux, le serveur d'applications doit être démarré avec des droits d'administrateur si vous utilisez un invite de commande. Démarrez le serveur d'applications depuis l'invite de commande qui s'ouvre en exécutant les actions suivantes :

- Cliquez avec le bouton droit sur un raccourci d'invite de commande.
- Cliquez sur **Exécuter en tant qu'administrateur**.
- Quand vous ouvrez la fenêtre d'invite de commande en tant qu'administrateur, une boîte de dialogue du système d'exploitation apparaît et vous demande si vous voulez continuer. Cliquez sur **Continuer** pour poursuivre.

Procédure

Procédure

1. Démarrez le serveur.

   Le tableau suivant décrit les options de démarrage du serveur.

Démarrer le serveur	Détails
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`***

   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	Détails
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`***

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	Détails
A partir de l'interface utilisateur	Le panneau Premiers pas affiche les résultats de votre demande.
Depuis une ligne de commande	Le résultat de votre demande est affiché dans le panneau 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.

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

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

Tableau 2. Rôles de sécurité

Rôle de sécurité	Description
Moniteur	Un moniteur peut visualiser la configuration de WebSphere Process Server et l'état en cours du serveur.
Configurateur	Un configurateur peut modifier la configuration de WebSphere Process Server.

Tableau 2. Rôles de sécurité (suite)

Rôle de sécurité	Description
Opérateur	Un membre du rôle opérateur dispose des privilèges d'un moniteur, plus la capacité de modifier l'état d'exécution du serveur (c'est-à-dire démarrer et arrêter le serveur).
Administrateur	Un administrateur dispose à la fois des droits d'un configurateur et d'un opérateur, plus quelques privilèges qui sont propres à ce rôle. Par exemple : • Modifier l'ID utilisateur et le mot de passe du serveur • Mapper les utilisateurs et les groupes vers le rôle d'administrateur L'administrateur dispose également des droits requis pour accéder à des informations sensibles, comme : • Mots de passe LTPA (Lightweight Third Party Authentication) • Clés
ISC Admins	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 ISC Admins peut effectuer les tâches suivantes : • Création, mise à jour ou suppression d'utilisateurs dans la configuration des référentiels fédérés • Créer, mettre à jour ou supprimer les groupes dans la configuration des référentiels fédérés
Déployeur	Seuls les utilisateurs associés à ce rôle peuvent effectuer des opérations de configuration et d'exécution sur les applications.
Gestionnaire de la sécurité administrative	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.
Auditeur	Seuls les utilisateurs associés à ce rôle peuvent afficher et modifier les paramètres de configuration du sous-système d'audit de la sécurité. **Remarque :** Le rôle d'auditeur inclut le rôle de moniteur. Cela permet à l'auditeur d'afficher le reste de la configuration de sécurité sans y apporter de modifications.

Pour plus d'informations, voir Rôles d'administration dans le centre de documentation de WebSphere Application Server.

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.

Conseil : Pour faciliter l'administration du système, mappez un ou plusieurs groupes d'utilisateurs vers des rôles de sécurité, plutôt que des utilisateurs individuels. Le mappage d'un groupe d'utilisateurs vers un rôle de sécurité, ainsi que l'ajout ou la suppression d'utilisateurs dans un groupe, s'effectuent à l'extérieur de WebSphere Process Server et ne nécessitent donc pas de redémarrer le serveur.

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

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

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

- Le sujet spécial **AllAuthenticated** signifie que le contrôle d'accès du rôle d'administration garantit que l'utilisateur effectuant la requête est au moins authentifié.
- Le sujet spécial **Everyone** signifie que n'importe quel utilisateur, authentifié ou non, peut effectuer l'action, comme si la sécurité n'était pas activée.

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.

Pourquoi et quand exécuter 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

Procédure

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

Eléments de sécurité

Les applications qui s'exécutent dans WebSphere Process Server sont sécurisées par l'authentification et le contrôle d'accès. Par ailleurs, les données transférées pendant l'appel d'une application sont conservées de manière sécurisée par le biais de divers mécanismes. Ces mécanismes empêchent que les données soient lues ou modifiées pendant leur transfert. Le dernier élément de sécurité est la propagation des informations de sécurité dans différents systèmes, de sorte que l'utilisateur n'a pas besoin de répéter les données d'authentification.

La sécurité dans WebSphere Process Server peut se diviser 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 disposer des droits nécessaires pour appeler l'application. Les rôles sont associés à l'appel de l'application. Un utilisateur authentifié doit faire partie du rôle approprié, sinon l'application ne pourra pas s'exécuter.

Intégrité et confidentialité des données

Les données auxquelles accède une application sont sécurisées à la source, à leur destination et pendant leur transfert :

- Intégrité

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

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

Propagation de l'identité

Le dernier élément de sécurité est la propagation de l'identité, qui est obtenue par le biais d'une connexion unique.

Lorsque la demande d'un client doit passer dans plusieurs systèmes dans l'entreprise, ce dernier n'est pas forcé de fournir les données d'authentification plusieurs fois. La méthode de connexion unique est utilisée pour propager les informations d'authentification vers les systèmes en aval qui, en retour, appliquent les contrôles d'accès.

Authentification des utilisateurs

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

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

Le tableau 3 répertorie les clients standards qui peuvent appeler les composants de WebSphere Process Server, ainsi que les options d'authentification disponibles pour chacun de ces clients.

Tableau 3. Options d'authentification pour les différents clients

Client	Options d'authentification	Notes
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. 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.

Alias d'authentification par défaut :

Plusieurs composants 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 pour qu'ils correspondent à d'autres utilisateurs de votre référentiel de compte utilisateur.

Alias d'authentification du Chorégraphe de processus métier :

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

Les alias figurant dans le tableau 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 aux processus métier

Alias	Description	Information
BPEAuthDataAliasJMS_*noeud_serveur*	Utilisé pour effectuer une authentification avec le moteur de messagerie.	Entrez le nom d'utilisateur et le mot de passe dans la page de configuration Business Process Choreographer de l'outil de gestion de profil.

Tableau 4. Alias d'authentification associés aux processus métier (suite)

Alias	Description	Information
BPEAuthDataAlias*DbType_noeud_serveur*	Utilisé pour effectuer une authentification avec des bases de données.	Configurez les bases de données à l'aide des scripts fournis.

tableau 5 décrit les rôles RunAs créés pour les processus métier.

Tableau 5. 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`.	Entrez le nom d'utilisateur et le mot de passe dans la page de configuration Business Process Choreographer de l'outil de gestion de profil.
EscalationUser	Utilisé par le bean géré par message `task.ear`.	Entrez le nom d'utilisateur et le mot de passe dans la page de configuration Business Process Choreographer de l'outil de gestion de profil.

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

Alias d'authentification Infrastructure CEI :

L'infrastructure Infrastructure CEI inclut des alias d'authentification prédéfinis. Vous pouvez modifier ces alias à l'aide de la console d'administration.

Les alias figurant dans le tableau 6 sont utilisés pour appeler les composants, quelle que soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 6. Alias d'authentification associés à Infrastructure CEI

Alias	Description	Information
CommonEventInfrastructure JMSAuthAlias **Remarque :** L'alias réel ne contient pas d'espace.	Utilisé pour effectuer une authentification avec le moteur de messagerie.	Entrez le nom d'utilisateur et le mot de passe dans la page de configuration Infrastructure CEI de l'outil de gestion de profil.
EventAuthAlias*TypeBdD*	Utilisé pour effectuer une authentification avec des bases de données.	Entrez le nom d'utilisateur et le mot de passe dans la page de configuration Infrastructure CEI de l'outil de gestion de profil.

Alias d'authentification de l'architecture SCA :

L'architecture SCA (Service Component Architecture) inclut un alias d'authentification prédéfini. Modifiez l'alias à l'aide de la console d'administration.

L'alias dans le tableau 7, à la page 34 est utilisé pour appeler les composants, quelle que soit l'identité de l'utilisateur qui procède à l'appel.

Tableau 7. Alias d'authentification associé à des composants SCA

Alias	Description	Information
SCA_Auth_Alias	Utilisé pour effectuer une authentification avec le moteur de messagerie.	Entrez le nom d'utilisateur et le mot de passe dans la page de configuration SCA de l'outil de gestion de profil.

Modification des alias d'authentification :

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

Pourquoi et quand exécuter cette tâche

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

Procédure

Procédure

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

   Remarque : Vous pouvez également accéder à cette page à partir de diverses pages de la console d'administration qui exigent des informations sur l'alias d'authentification.
   La page de configuration de l'alias d'authentification s'affiche.

   Cette page présente une liste d'alias d'authentification, le composant associé, l'ID utilisateur associé à cet alias et, en option, une description de l'alias.
2. Sélectionner l'alias d'authentification que vous souhaitez modifier en cliquant sur son nom dans la colonne **Alias**.

   Remarque : Dans certains cas, la colonne **Alias** peut ne pas contenir de lien. Dans ce cas, cochez la case de la colonne **Sélectionner** correspondant à l'alias que vous voulez éditer et cliquez sur **Editer**.
3. Modifier les propriétés de l'alias.
   Dans la page 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. Confirmer les modifications effectuées.
   Cliquez sur **OK** ou sur **Valider**. Retournez à la page 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*

Contrôle d'accès

Lorsqu'un utilisateur général est authentifié sur WebSphere Process Server, il est important, pour des raisons de sécurité, qu'il n'ait as accès à toutes les opérations possibles. Permettre à certains utilisateurs d'effectuer certaines tâches et pas à d'autres s'appelle le *contrôle d'accès*.

Le contrôle d'accès peut être adapté à des composants en cours de développement, afin de les sécuriser. Vous fournissez le contrôle d'accès aux composants en utilisant des qualifiants de l'architecture de composants de service lors de l'étape de développement. Pour plus d'informations, voir le centre de documentation de WebSphere Integration Developer.

Certains composants WebSphere Process Server, fournis sous forme de fichiers d'archive d'entreprise (EAR), sécurisent leurs opérations à l'aide de la sécurité basée sur des rôles Java EE. Contrairement à la sécurité basée sur le code, qui sécurise le fonctionnement des composants, un contrôle d'accès basé sur les rôles sécurise les *ressources*. Par exemple, dans le widget Agendas métier, vous pouvez préciser le type d'accès, des utilisateurs, aux plannings individuels.

Widget Rôles de sécurité

Utilisez le widget Rôles de sécurité dans Business Space pour indiquer, pour chaque planning, le propriétaire du planning ainsi que les personnes ayant un accès en écriture et en lecture à ce planning.

Le tableau ci-après illustre les rôles d'administration et leurs droits par défaut.

Rôles	**Droits d'accès par défaut**
BPMAdmin	Administrateur principal
BPMRoleManager	Tous les utilisateurs authentifiés

Fichiers EAR et rôles associés

Business Process Choreographer et Infrastructure CEI sont installés avec WebSphere Process Server.

Tableau 8. Fichiers EAR et rôles associés dans WebSphere Process Server

Nom du fichier .ear	**Rôle**	**Valeur par défaut**
BPEContainer_*nomNoeud_nomServeur*.ear OU BPEContainer_*nomCluster*	APIUser	Tous les utilisateurs authentifiés
	SystemAdministrator	Néant
	SystemMonitor	Néant
	JMSAPIUser	Tous les utilisateurs authentifiés
	AdminJobUser	Tous les utilisateurs authentifiés
	JAXWSAPIUser	Tous les utilisateurs
BPCExplorer_*nomNoeud_nomServeur*.ear OU BPCExplorer_*nomCluster*	WebClientUser	Tous les utilisateurs authentifiés

Tableau 8. Fichiers EAR et rôles associés dans WebSphere Process Server (suite)

Nom du fichier .ear	**Rôle**	**Valeur par défaut**
BPCArchiveExplorer_*nom_noeud_nom_serveur*.ear OU BPCArchiveExplorer_*nom_cluster*	WebClientUser	Tous les utilisateurs authentifiés
BSpaceEAR_*nomNoeud_serveur*.ear	businessspaceusers	Tous les utilisateurs authentifiés
BSpaceWebformsEnabler_*nomNoeud_serveur*.ear	WebFormUsers	Tous les utilisateurs authentifiés
BusinessRulesManager.ear	BusinessRuleUsers	Tous les utilisateurs authentifiés
	NoOne	Aucune
	AnyOne	Tous les utilisateurs
BusinessRules_*nomNoeud_serveur*.ear	Administrateur	Tous les utilisateurs authentifiés
EventService.ear	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
mm.was_*nomNoeud_serveur*.ear	Tous les utilisateurs authentifiés	Tous les utilisateurs authentifiés
	everyone	Tous les utilisateurs
REST Services Gateway.ear	RestServicesUser	Tous les utilisateurs authentifiés
REST Services Gateway Dmgr .ear	RestServicesUser	Tous les utilisateurs authentifiés
TaskContainer_*nomNoeudnomServeur*.ear OU TaskContainer_*nomCluster*	APIUser	Tous les utilisateurs authentifiés
	SystemAdministrator	Néant
	SystemMonitor	Néant
	EscalationUser	Tous les utilisateurs authentifiés
	AdminJobUser	Tous les utilisateurs authentifiés
	JAXWSAPIUser	Tous les utilisateurs
wpsFEMgr_7.0.0 Security	WBIOperator	Tous les utilisateurs

Rôles Business Process Choreographer Java EE

Le tableau suivant répertorie les rôles Java EE de Business Process Choreographer :

Tableau 9. Rôles Business Process Choreographer

Composant	Rôles	Valeur
BPEContainer	APIUser	Tous les utilisateurs authentifiés
	SystemAdministrator	Noms d'utilisateur et/ou noms de groupe entrés lors de la configuration
	SystemMonitor	Tous les utilisateurs authentifiés
	JMSAPIUser	Nom d'utilisateur entré lors de la configuration
	AdminJobUser	Nom d'utilisateur entré lors de la configuration
	JAXWSAPIUser	Tous les utilisateurs
TaskContainer	APIUser	Tous les utilisateurs authentifiés
	SystemAdministrator	SystemAdministrator
	SystemMonitor	SystemMonitor
	EscalationUser	EscalationUser
	AdminJobUser	AdminJobUser
	JAXWSAPIUser	Tous les utilisateurs

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

Business Process Choreographer, qui est installé conjointement à WebSphere Process Server, utilise des rôles utilisateur pour déterminer les capacités de l'utilisateur sur un système de production.

Les rôles Business Process Choreographer sont décrits dans tableau 10.

Tableau 10. Rôles et droits d'accès par défaut

Rôles	Droits d'accès par défaut	Notes
Administrateur système	Noms d'utilisateur et/ou noms de groupe entrés lors de la configuration	A accès à tous les processus métier et à toutes les opérations.
Moniteur système	Tous les utilisateurs authentifiés	A accès aux opérations de lecture.
JMSAPIUser	Nom d'utilisateur entré lors de la configuration	Toutes les API JMS de Business Process Choreographer sont exécutées au nom de cet ID utilisateur unique.
EscalationUser	Nom d'utilisateur entré lors de la configuration	Utilisé par le gestionnaire de tâches manuelles pour traiter des appels d'API asynchrones.
AdminJobUser	Nom d'utilisateur entré lors de la configuration **Remarque :** L'utilisateur fourni doit être membre du rôle Administrateur système de Business Process Choreographer.	Les travaux d'administration (par exemple le service de nettoyage ou la migration d'instance de processus métier) sont exécutés au nom de cet ID utilisateur unique.

Remarque : Le rôle WebClientUser, qui est associé au fichier Bpcexlorer.ear, peut accéder à Business Process Choreographer Explorer. Les droits d'accès par défaut de ce rôle correspondent à Tous les utilisateurs authentifiés.

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 une discussion plus approfondie, consultez le centre de documentation de WebSphere Application Server Network Deployment.

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 et il est adapté pour les communications 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.

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.

Configuration dans un client web de services web de l'utilisation de SSL :

Vous pouvez configurer un client de services web pour qu'il appelle un service web via la couche SSL (Secure Sockets Layer).

Pourquoi et quand exécuter cette tâche

Pour des détails sur la façon de configurer votre client web de services web pour qu'il utilise SSL, consultez cette technote WebSphere Application Server. Une discussion plus générale à propos de la sécurisation des services web est disponible à la WebSphere Application Server rubrique Sécurisation des applications au niveau transport pour les services Web.

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.

Lorsqu'une demande du client passe par différents systèmes dans l'entreprise, le client ne doit s'identifier qu'une seule 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.

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.

Pourquoi et quand exécuter cette tâche

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

Si un rôle RunAs a été défini dans l'application, celle-ci appellera des méthodes qui nécessitent d'avoir paramétré des identités pendant le déploiement. Utilisez le rôle RunAs pour spécifier l'identité sous laquelle les appels en aval seront effectués. Par exemple, si le rôle RunAs est affecté à l'utilisateur «bob» et que le client «alice» appelle un servlet (avec la délégation définie) qui appelle les beans enterprise, 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 sécurités vers les utilisateurs/groupes** est affiché pendant l'installation de l'application (ou sa gestion), dans la section Propriétés supplémentaires.

Procédure

Procédure

1. Sur la console d'administration, développez **Applications** et cliquez sur **Installation d'une nouvelle application**.

   Effectuez les opérations nécessaires à l'installation des applications jusqu'à l'étape "Mappage des rôles de sécurité vers les utilisateurs/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. Cette tâche est utile au déployeur pour qu'il prenne connaissance des méthodes répertoriées dans la page 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.

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.

Pourquoi et quand exécuter cette tâche

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

Le 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 utilise l'identité indiquée, quelle que soit l'identité de l'utilisateur qui appelle l'application.

Procédure

Procédure

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

Qualifiant de sécurité	Opération à exécuter
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.

Widget des rôles de sécurité

Le widget Agendas métier offre la possibilité de sécuriser l'accès aux calendriers individuels dans le widget Agendas métier. Il permet d'affecter des rôles aux membres d'une organisation. Ce sont ces rôles qui déterminent le niveau d'accès aux calendriers.

Le widget Rôles de sécurité, qui permet de gérer les contrôles d'accès du widget Agendas métier, se trouve dans Business Space qui repose sur WebSphere.

Cet accès basé sur les rôles repose sur un standard ouvert, XACML (eXtensible Access Control Markup Language).

Quels sont les avantages à utiliser le contrôle d'accès basé sur les rôles du widget Rôles de sécurité dans le widget Agendas métier ?

- Vous pouvez contrôler l'accès à une instance particulière d'un calendrier.

  Par exemple, vous pouvez indiquer qu'un utilisateur n'a accès qu'à son propre calendrier et n'a pas la possibilité de consulter, ni de modifier le calendrier des autres utilisateurs.
- Le contrôle d'accès est accompli au niveau du rôle et non pas au niveau de l'utilisateur individuel.

  Vous affectez les utilisateurs à des rôles. C'est le rôle qui détermine le droit d'accès des membres à l'instance spécifique de la ressource.

Rôles associés à un calendrier

Lors de l'installation d'un calendrier, trois rôles sont créés pour ce dernier : propriétaire, accès en écriture et accès en lecture. Ces rôles sont connus comme des rôles spécifiques aux composants.

Comment ces rôles sont-ils utilisés ? Prenons le cas d'un calendrier des congés dans une entreprise. Vous voulez que tous les employés aient accès au calendrier, mais qu'un nombre limité puisse le mettre à jour.

Lors de l'installation de ce calendrier, les rôles suivants sont créés :

- HolidayOwner

  Les membres affectés à ce rôle ont un accès en lecture et en écriture au calendrier des congés. Par exemple, si l'entreprise décide de rajouter des congés, un membre ayant le rôle HolidayOwner pourrait effectuer cette modification.

  Ce rôle permet également d'affecter des membres aux rôles HolidayWriter et HolidayReader. Par exemple, un HolidayOwner peut décider d'ajouter un responsable senior au rôle HolidayWriter.
- HolidayWriter

  Les membres affectés à ce rôle ont un accès en lecture et en écriture au calendrier des congés. Comme pour le rôle HolidayOwner, les membres ayant le rôle HolidayWriter peuvent ajouter les congés supplémentaires décidés par l'entreprise.
- HolidayReader

  Les membres affectés à ce rôle ont un accès en lecture au calendrier des congés mais pas en écriture.

Vous pourriez affecter le rôle HolidayOwner au responsable des ressources humaines, le rôle HolidayWriter au groupe de spécialistes des ressources humaines et le rôle HolidayReader au groupe des employés, comme illustré ci-dessous :

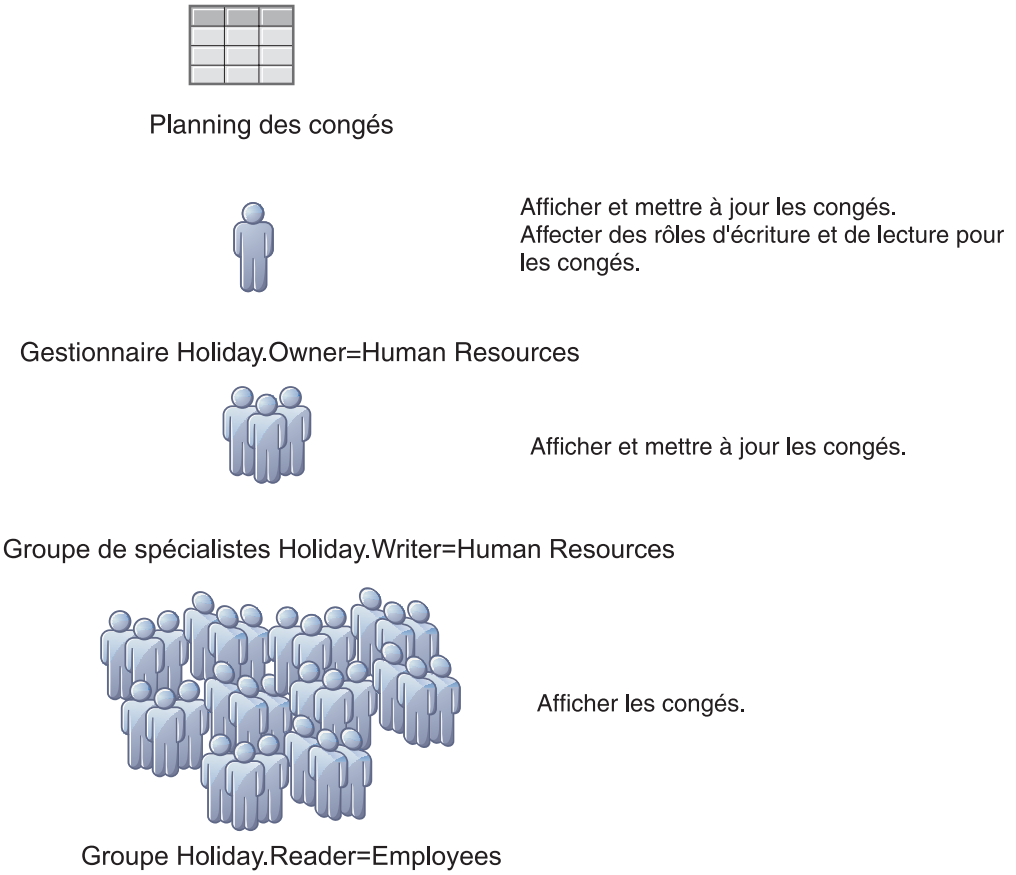


Figure 1. Exemple des rôles affectés pour un calendrier

Lorsque vous déployez un calendrier, les trois rôles, propriétaire, accès en écriture et accès en lecture, sont créés. Les droits d'accès correspondant à ces rôles sont définis initialement sur **Tous les utilisateurs authentifiés**. Pensez à modifier cette désignation pour affecter les membres de l'entreprise aux rôles appropriés.

Remarque : Vous pouvez modifier l'appartenance à un rôle (par exemple, vous pouvez supprimer le rôle d'accès en lecture d'un membre), mais vous ne pouvez pas modifier le nom d'un rôle, ajouter ou supprimer un rôle, ni modifier les droits d'accès associés à ce rôle. Les droits d'accès sont définis comme suit :

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

Dans le widget Rôles de sécurité, ces rôles liés à un calendrier sont également connus sous le terme de *rôles module*.

Rôles système du widget Rôles de sécurité

Les rôles BPMAdmin et BPMRoleManager sont automatiquement créés lorsque vous activez la sécurité après avoir installé WebSphere Process Server (ou migré vers WebSphere Process Server 7.0).

- BPMAdmin

BPMAdmin a le droit d'ajouter des membres au rôle BPMRoleManager ou d'en retirer des membres. Par exemple, si la personne ayant le rôle BPMRoleManager quitte l'organisation, seul le BPMAdmin peut affecter un autre membre à ce rôle.

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

- BPMRoleManager

  BPMRoleManager a le droit d'ajouter des membres aux trois rôles liés au calendrier - propriétaire, accès en écriture et accès en lecture - et de retirer ces rôles à des membres. Par exemple, si un calendrier de congés est créé, le rôle BPMRoleManager affecte des membres aux rôles HolidayOwner, HolidayWriter, et HolidayReader.

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

Administration des rôles dans l'objet fenêtre Rôles de sécurité

A l'aide de l'objet fenêtre Rôles de sécurité, vous pouvez affecter un utilisateur ou un groupe aux rôles système. Vous pouvez également affecter un utilisateur ou un groupe aux rôles de composant associés à des plannings.

Affectation de rôles de composant

Chaque planning de l'objet fenêtre Agendas métier est associé à trois rôles de composant : propriétaire, accès en écriture et accès en lecture. Vous utilisez l'objet fenêtre Rôles de sécurité pour affecter des utilisateurs ou des groupes à ces rôles.

Avant de commencer

Vérifiez que l'objet fenêtre Rôles de sécurité est affiché.

Pourquoi et quand exécuter cette tâche

Le rôle BPMRoleManager peut affecter des utilisateurs ou des groupes à des rôles de composant.

Le propriétaire d'un planning peut également affecter des utilisateurs ou des groupes au rôle propriétaire, accès en écriture ou accès en lecture de ce planning.

Procédure

Procédure

1. Pour affecter des membres individuels à un rôle de module, procédez comme suit :
   a. Dans la liste **Module** , sélectionnez un planning.
   b. Pour un rôle (par exemple, le rôle accès en écriture du planning), cliquez sur le nom du rôle.
   c. Dans la partie droite de la page, cliquez sur **Ajouter**.
   d. Entrez un nom, ou une partie de nom, dans la zone **Utilisateurs ou groupes à rechercher**.
   e. Pour restreindre le nombre d'utilisateurs ou de groupes renvoyés en fonction des critères de recherche, modifiez la valeur de la zone **Nombre maximal de résultats**. Spécifiez la valeur `0` pour renvoyer l'intégralité du jeu de résultats.

f. Cliquer sur **Rechercher**.
g. Dans la liste affichée, sélectionnez un ou plusieurs utilisateurs ou groupes et cliquez sur **OK**.
h. Une fois que vous avez affecté tous les membres, cliquez sur **Sauvegarder**.

2. Pour affecter tous les membres à un rôle de module, procédez comme suit :
   a. Dans la liste **Module** , sélectionnez un planning.
   b. Pour un rôle (par exemple, le rôle accès en lecture du planning), cliquez sur le nom du rôle.
   c. Sélectionnez **Tous les utilisateurs authentifiés**.
   d. Cliquez sur **Enregistrer**.

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.

Pourquoi et quand exécuter cette tâche

Un adaptateur est le mécanisme par lequel une application dialogue avec un système d'information d'entreprise (EIS). 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'API et d'outils permettant à des applications d'échanger des données métier à travers un courtier d'intégration. Les adaptateurs WebSphere Business Integration Adapters sont basés sur la messagerie JMS (Java Message Service) et JMS ne prend pas en charge la propagation de contexte de sécurité.

WebSphere Adapters permet une connectivité bidirectionnelle et gérée entre une EIS et des composants Java EE 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. JCA ne dispose pas non plus de prise en charge au niveau de la sécurité des communications entrantes. De ce fait, WebSphere Adapters ne dispose pas non plus d'un mécanisme d'authentification pour les communications entrantes.

L'entrée d'un adaptateur vers WebSphere Process Server s'effectue toujours à travers une exportation SCA (Service Component Architecture). Cette exportation SCA doit être câblée 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.

Sécurité des tâches utilisateur et des processus métier

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

Par définition, les tâches manuelles nécessitent une intervention humaine. Certains processus métier sont également susceptibles de nécessiter une intervention humaine. Ces tâches manuelles et ces processus métier sont développés à l'aide de WebSphere Integration Developer et sont appelés via Business Process Choreographer. Lorsque vous développez une tâche ou un processus, vous devez attribuer des rôles à des utilisateurs ou des groupes concernés par les tâches manuelless 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 manuelle et le conteneur métier de Business Process Choreographer.

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

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

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

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

Les tâches sont également associés aux rôles suivants :

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

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

Configuration de la sécurité de Business Space

Si vous utilisez Business Space powered by WebSphere avec votre environnement, vous devez étudiez les options de sécurité relatives à la manière dont votre équipe utilisera les artefacts dans Business Space. Si vous souhaitez activer la sécurité de Business Space, configurez la sécurité des applications et désignez un référentiel d'utilisateurs. Pour définir des administrateurs Business Space, affectez un rôle de superutilisateur.

Pourquoi et quand exécuter cette tâche

Pour de meilleurs résultats, activez la sécurité avant de configurer Business Space. Dans la page d'administration Sécurité globale de la console d'administration, activez la sécurité d'administration et la sécurité des applications. Désignez également un référentiel de comptes utilisateur. Pour plus d'informations, voir Configuration, activation et migration de la sécurité.

Considérations à prendre en compte pour l'utilisation d'un registre de comptes utilisateur avec Business Space :

- En fonction du type de configuration LDAP que vous utilisez, vos paramètres peuvent avoir un impact sur vos possibilités d'accéder correctement à Business Space. Vérifiez que les filtres d'utilisateurs, les filtres de groupes et les paramètres de mappage sont configurés correctement. Pour plus d'informations, voir Configuration des filtres de recherche LDAP (Lightweight Directory Access Protocol) dans le centre de documentation de WebSphere Application Server.
- En fonction du type de configuration de référentiel fédéré que vous utilisez, vos paramètres peuvent affecter vos possibilités d'accéder correctement à Business Space. Vérifiez que les domaines sont correctement configurés. Pour plus d'informations, voir Gestion du domaine d'une configuration de référentiel fédéré dans le centre de documentation de WebSphere Application Server.
- La sécurité LDAP est configurée par défaut afin d'utiliser la propriété de connexion `uid` (ID utilisateur) pour les recherches dans Business Space. Si votre sécurité LDAP est modifiée pour utiliser une autre zone LDAP unique, telle que `mail` (adresse électronique) pour la propriété de connexion, vous devez modifier la propriété userIdKey dans le fichier `ConfigServices.properties` pour que la fonction de recherche fonctionne dans Business Space. Le fichier `ConfigServices.properties` se trouve dans *racine_profil*`\BusinessSpace\`*nom_noeud*`\`*nom_serveur*`\mm.runtime.prof\config\ConfigService.properties` pour un serveur autonome ou *racine_profil_gestionnaire_déploiement*`\BusinessSpace\`*nom_cluster*`\mm.runtime.prof\config\ConfigService.properties` pour un cluster. Modifiez la valeur de l'attribut userIdKey (`uid`) pour qu'elle corresponde à la propriété de connexion de votre sécurité LDAP (par exemple, `mail`). Exécutez ensuite la commande **updatePropertyConfig** à l'aide du client de

script wsadmin, en désignant les paramètres suivants : **-serverName** et **-nodeName** pour un serveur autonome ou **-clusterName** pour un cluster, **-propertyFileName** avec la valeur du chemin d'accès du fichier `ConfigServices.properties` et **-prefix** avec la valeur `Mashups_`.

- Si vous utilisez une base de données Microsoft SQL Server et le registre **Annuaire LDAP autonome**, assurez-vous que le nom distinctif de l'utilisateur ne dépasse pas 131 caractères. Si l'une des entrées de nom distinctif dépasse 131 caractères, vous devez spécifier l'option **Référentiels fédérés** pour le référentiel de comptes utilisateur. Lorsque vous passez de référentiels fédérés à d'autres registres, les pages et les espaces existants ne sont plus accessibles dans Business Space et doivent être recréés.
- Si vous utilisez **Référentiels fédérés**, vous disposez de fonctionnalités supplémentaires dans vos widgets et votre infrastructure (par exemple, des fonctions de recherche étendues). Lors de la recherche d'utilisateurs pour le partage d'espaces et de pages, la portée de la recherche inclut une adresse électronique, un nom d'utilisateur complet et un ID utilisateur.

Important : Par défaut, la configuration du proxy Ajax utilisée avec des widgets Business Space ne restreint pas l'accès aux adresses IP. Si vous souhaitez que votre environnement Business Space soit plus sécurisé, configurez le proxy Ajax pour qu'il n'affiche que le contenu des sites sélectionnés ou le contenu de blocs des sites sélectionnés. Pour plus d'informations, voir Blocage d'adresses IP à l'aide du proxy Business Space Ajax.

Si vous utilisez IBM Tivoli Access Manager WebSEAL et que vous souhaitez l'utiliser avec votre environnement Business Space, vous devez effectuer des étapes de configuration supplémentaires. Configurez la sécurité de Tivoli Access Manager avec un fournisseur JACC (Java Authorization Contract for Containers) externe, configurez WebSEAL avec Tivoli Access Manager, configurez WebSEAL avec le serveur d'applications de votre produit et configurez les jonctions hôte de votre environnement. Pour plus d'informations, voir la sous-rubrique Configuration de Tivoli Access Manager WebSEAL pour Business Space.

Pour indiquer quels utilisateurs de l'environnement Business Space seront administrateurs, vous devez exécuter le script `createSuperUser.py` qui attribuera le rôle de superutilisateur Business Space. Pour plus d'informations, voir la sous-rubrique Affectation du rôle de superutilisateur Business Space.

Configuration de la sécurité des applications de Business Space

Pour activer la sécurité pour Business Space vous devez activer la sécurité des applications et la sécurité d'administration.

Avant de commencer

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

- Vérifier que l'ID utilisateur est enregistré dans le registre d'utilisateurs de votre produit.

Si vous envisagez d'utiliser un environnement sécurisé, activez bien la sécurité avant de configurer Business Space. Si vous souhaitez activer ou désactiver la sécurité une fois que vous avez configuré Business Space, vous devez modifier les propriétés `MashupAdminForOOBSpace` et `noSecurityAdminInternalUserOnly` dans le fichier `ConfigServices.properties` pour définir l'ID utilisateur approprié comme

ID administrateur valide. Le fichier `ConfigServices.properties` se trouve dans *racine_profil*`\BusinessSpace\`*nom_noeud*`\`*nom_serveur*`\mm.runtime.prof\config\ConfigService.properties` pour un serveur autonome ou *racine_profil_gestionnaire_déploiement*`\BusinessSpace\`*nom_cluster*`\mm.runtime.prof\config\ConfigService.properties` pour un cluster. Copiez le fichier modifié dans un dossier vide de votre système. Exécutez ensuite la commande **updatePropertyConfig** en utilisant le client des scripts wsadmin et en désignant les paramètres suivants :

- **-serverName** et **-nodeName** pour un serveur autonome ou **-clusterName** pour un cluster
- **-propertyFileName** avec la valeur du chemin d'accès du fichier `ConfigServices.properties`
- **-prefix** avec la valeur `Mashups_`

Pourquoi et quand exécuter cette tâche

Business Space est préconfiguré pour garantir l'authentification et l'autorisation des accès. Les utilisateurs sont invités à s'authentifier lorsqu'ils accèdent aux URL de Business Space. Les utilisateurs non authentifiés sont redirigés vers une page de connexion. Business Space est accessible via HTTP ou HTTPS. Si vous craignez que les mots de passe soient compromis en raison d'un manque de protection SSL, vous pouvez envisager de désactiver l'accès HTTP à l'aide de WebSphere Application Server. Pour plus d'informations, reportez-vous au centre de documentation WebSphere Application Server. Par conséquent, si vous utilisez un serveur Web tel qu'IBM HTTP Server, vous devez le configurer pour qu'il prenne en charge HTTPS.

L'autorisation d'accès aux espaces et au contenu des pages dans Business Space est gérée en interne dans Business Space lors de la procédure de gestion des espaces.

Pour activer l'accès authentifié à Business Space, un registre d'utilisateurs doit être configuré et une application de sécurité activée.

Procédure

Procédure

1. Pour des instructions complètes sur la sécurité, reportez-vous à la documentation sur la sécurité de votre produit.
2. Pour l'application Business Space, dans la page Sécurité globale de la console d'administration, sélectionnez **Activer la sécurité d'administration** et **Activer la sécurité des applications**.
3. Dans la même page de la console d'administration, sous **Référentiel de comptes utilisateur**, sélectionnez **Référentiels fédérés**, **Système d'exploitation local**, **Registre LDAP autonome** ou **Registre personnalisé autonome**. Etudiez les considérations à prendre en compte pour la sélection d'un registre d'utilisateurs dans la rubrique Configuration de la sécurité de Business Space.
4. Si Business Space et votre produit sont sur des noeuds distincts et dans des cellules différentes, vous devez effectuer des étapes manuelle afin d'activer la connexion unique (SSO). Par exemple, si vous utilisez plusieurs produits (WebSphere Business Compass, WebSphere Business Monitor, WebSphere Enterprise Service Bus ou WebSphere Process Server), que les serveurs se trouvent sur des noeuds différents et que vous souhaitez qu'ils puissent tous fonctionner avec le serveur Business Space, vous devez configurer SSO manuellement. Pour activer SSO, procédez comme suit :

a. Sur la console d'administration de chaque serveur, ouvrez la page Sécurité globale en cliquant sur **Sécurité** > **Sécurité globale**. Développez **Web et sécurité SIP** et cliquez sur **connexion unique (SSO)** pour vous assurer que la case **Activé** est cochée.

b. Vérifiez que tous les noeuds utilisent les mêmes informations **Référentiel de comptes utilisateur** (voir l'étape 3).

c. Sur la console d'administration du premier noeud, ouvrez la page Sécurité globale. Sous Authentification, cliquez sur **LTPA**.

d. Sous **Ouverture d'une session intercellulaire**, entrez un mot de passe pour le fichier de clés, ainsi qu'un nom qualifié complet désignant l'emplacement et le nom de fichier sous lequel vous souhaitez exporter le fichier de clés. Le nom qualifié complet du fichier de clés correspond au chemin d'accès absolu sur le système sur lequel votre serveur est exécuté.

e. Cliquez sur **Exporter les clés**. Le fichier de clés est sauvegardé sur le système sur lequel le serveur est exécuté.

f. Si les deux noeuds ne sont pas sur le même système, faites une copie physique du fichier de clés à destination des autres systèmes.

g. Importez le fichier de clés sur chaque autre noeud : connectez-vous à la console d'administration des autres noeuds et accédez à la page Sécurité globale > LTPA. Sous **Ouverture d'une session intercellulaire**, entrez le mot de passe du fichier de clés, ainsi que le nom qualifié complet (utilisez le même mot de passe pour le fichier de clés exporté que vous avez copié), puis cliquez sur **Importer les clés**.

h. Redémarrez le serveur après avoir importé les clés sur chaque système.

5. Si vous utilisez HTTPS dans le fichier d'enregistrement des points de contact, l'emplacement du point de contact est sur un noeud différent de celui de Business Space et que le certificat SSL (Secure Sockets Layer) est autosigné, vous devez l'importer.

   a. Ouvrez une session sur la console d'administration du serveur qui contient Business Space et importez le certificat SSL utilisé par le noeud éloigné sur lequel le produit est exécuté.

      1) Sous Sécurité, cliquez sur **Certificat SSL et gestion des clés**.

      2) Dans la page Certificat SSL et gestion des clés, sous Articles liés, cliquez sur **Magasins de clés et certificats**.

      3) Dans la page Magasins de clés et certificats, cliquez sur **NodeDefaultTrustStore** pour modifier ce type de fichier de clés certifiées.

      4) Dans la page NodeDefaultTrustStore, sous Propriétés supplémentaires, cliquez sur **Certificats de signataire**.

      5) Dans la page Certificats de signataire de **NodeDefaultTrustStore**, cliquez sur le bouton **Extraire d'un port**.

      6) Dans la page Extraire d'un port, sous Propriétés générales, tapez le nom d'hôte, le port et l'alias du noeud où votre produit est exécuté. Cliquez sur le bouton **Récupérer les informations du signataire**, puis sur **OK**.

      7) Redémarrez les deux serveurs.

   b. Ouvrez une session sur la console d'administration du noeud du produit et importez le certificat SSL utilisé par le noeud sur lequel Business Space est exécuté.

      1) Répétez les étapes i. à v.

2) Dans la page Extraire d'un port, sous Propriétés générales, tapez le nom d'hôte et le port où Business Space est exécuté. Cliquez sur le bouton **Récupérer les informations du signataire**, puis sur **OK**.
3) Redémarrez les deux serveurs.

Pour plus d'informations sur SSO et SSL, reportez-vous au centre de documentation de WebSphere Application Server.

Que faire ensuite

- Une fois la sécurité administrative et des applications activée, vous recevez un message demandant un ID utilisateur et un mot de passe lorsque vous vous connectez à Business Space. Vous devez utiliser un ID utilisateur et un mot de passe valides du registre d'utilisateurs sélectionné pour pouvoir vous connecter. Après avoir activé la sécurité administrative, vous devez vous connecter avec l'ID utilisateur ayant des droits d'administration chaque fois que vous revenez dans la console d'administration.
- Si vous voulez limiter les connexions à Business Space à un sous-ensemble d'utilisateurs et de groupes, vous pouvez changer le mappage du rôle J2EE de Business Space. Vous devez mettre à jour le mappage des utilisateurs/groupes de deux applications d'entreprise : **BSpaceEAR_*noeud_serveur*** et **mm.was_*noeud_serveur***. Cliquez sur **Applications** > **Types d'application** > **Applications d'entreprise WebSphere** et sélectionnez les deux applications. Dans le panneau droit, sous Detail Properties, sélectionnez **Security role to user/group mapping**. Remappez les rôles **businessspaceusers** et **Allauthenticated** des deux applications en supprimant d'abord le sujet spécial. Cliquez sur **Mappage des objets spéciaux** et sélectionnez **Aucun**. Cliquez ensuite sur **Mappage des utilisateurs** ou **Mappage des groupes** et affectez chaque rôle à vos utilisateurs ou groupes sélectionnés. Notez que la modification du mappage des rôles J2EE n'affecte pas la fonction de recherche des utilisateurs/groupes dans Business Space.
- Pour définir les autorisations d'accès aux pages et aux espaces dans Business Space, vous pouvez gérer les autorisations lorsque vous créez des pages et des espaces Business Space.

Remarque :

Si le fichier `SystemOut.log` contient les erreurs suivantes, il se peut que votre registre d'utilisateurs contienne des attributs en trop qui ne peuvent pas être traités :

```
00000046 SystemErr R Caused by: com.ibm.websphere.wim.exception.WIMSystemException: CWWIM1013E
    The value of the property secretary is not valid for entity uid=xxx,c=us,ou=yyy,o=ibm.com.
00000046 SystemErr R at com.ibm.ws.wim.adapter.ldap.LdapAdapter.setPropertyValue
(LdapAdapter.java:3338)
```

Définissez les attributs suivants dans le fichier `ConfigServices.properties` pour ignorer ces attributs :

```
com.ibm.mashups.user.userProfile = LIMITED
com.ibm.mashups.user.groupProfile = LIMITED
```

Le fichier `ConfigServices.properties` se trouve dans *racine_profil*`\BusinessSpace\`*nom_noeud*`\`*nom_serveur*`\mm.runtime.prof\config\ConfigService.properties` pour un serveur autonome ou *racine_profil_gestionnaire_déploiement*`\BusinessSpace\`*nom_cluster*`\mm.runtime.prof\config\ConfigService.properties` pour un cluster. Une fois que vous avez modifié le fichier `ConfigServices.properties`, exécutez la commande **`updatePropertyConfig`** à l'aide du client de script wsadmin, en désignant les

paramètres suivants : **-serverName** et **-nodeName** pour un serveur autonome ou **-clusterName** pour un cluster, **-propertyFileName** avec la valeur du chemin d'accès du fichier ConfigServices.properties et **-prefix** avec la valeur Mashups_.

Remarque :

Si la sécurité Java 2 est activée dans un cluster, envisagez de renforcer l'entrée dans les règles serveur appliquées à l'emplacement de l'aide de Business Space.

Les règles de l'emplacement de l'aide sont les suivantes :

```
grant codeBase "file:${was.install.root}/profiles/nom_profil/temp/
nom_noeud/-" {

    permission java.security.AllPermission;

};
```

Renforcez la règle en la remplaçant par :

```
grant codeBase "file:${was.install.root}/profiles/nom_profil/temp/
nom_noeud/nom_serveur/BusinessSpaceHelpEAR_nom_noeud_nom_serveur/
BusinessSpaceHelp.war/-" {

    permission java.security.AllPermission;

 };
```

Configuration de la sécurité des services REST système

Pour configurer en fonction des utilisateurs et des groupes la sécurité des données dans les widgets, vous devez modifier le mappage des utilisateurs avec l'application REST Services Gateway.

Pourquoi et quand exécuter cette tâche

Le mappage des utilisateurs à une application fournisseur de services REST affecte tous les services du fournisseur.

Pour voir les services qui sont affectés, sélectionnez **Services** > **Services REST** > **Fournisseurs de services REST** et sélectionnez l'application dans la liste des fournisseurs.

Procédure

Procédure

1. Sur la console d'administration, sélectionnez l'une des options suivantes :
   - Pour un environnement de serveur, sélectionnez **Applications** > **Types d'application** > **Applications d'entreprise WebSphere** > **REST Services Gateway**
   - Dans le cas d'un environnement de déploiement réseau, sélectionnez en plus **Applications** > **Types d'application** > **Applications d'entreprise WebSphere** > **REST Services Gateway Dmgr**
2. Dans le panneau de droite, sous Propriétés du détail, sélectionnez **Mappage rôle de sécurité-utilisateur/groupe**.

3. Pour contrôler l'accès aux données dans tous les widgets de services REST, ajoutez les utilisateurs et les groupes au rôle **RestServicesUser**.

Considérations sur la sécurisation des widgets Business Space

Selon les widgets que vous utilisez dans Business Space avec votre produit de gestion des processus métier, vous pouvez affectuer des rôles de groupes d'utilisateurs d'administration pour contrôler l'accès aux données dans un widget, ou vous pouvez affecter une couche supplémentaire d'accès à base de rôle pour votre widget.

Rôles de groupes d'administration et widgets

Le contrôle de l'accès aux données dans des widgets s'effectue grâce aux rôles de groupes d'administration et aux utilisateurs qui sont affectés à ces rôles. Pour voir qui est affecté à ces rôles, ouvrez la console d'administration, sélectionnez **Utilisateurs et groupes** > **Rôles des groupes d'administration** et sélectionnez un groupe. La liste des rôles s'affiche.

Règles métier et Variables métier sont deux exemples de widgets qui peuvent nécessiter des modifications dans les rôles de groupes d'administration.

Par exemple, pour le widget Etat du système, les rôles d'administration suivants disposent tous d'autorisations de contrôle, ont tous accès à la console d'administration et, par conséquent, permettent aux utilisateurs qui leur sont affectés d'accéder aux données du widget Etat du système :

- **Moniteur**
- **Configurateur**
- **Opérateur**
- **Administrateur**
- **Adminsecuritymanager**
- **Déployeur**
- **iscadmins**

Les utilisateurs mappés à ces rôles de groupe d'administration ont accès aux données du widget Etat du système. Les utilisateurs non mappés à ces rôles n'ont pas accès aux données du widget Etat du système.

Accès du widget à base de rôle

Certains widgets ont un accès à base de rôle pour leurs artefacts qu'ont créés des utilisateurs métier. Dans le widget Rôles de sécurité, vous pouvez affecter des utilisateurs et des groupes à des rôles système ou à des rôles module qui déterminent le niveau d'accès dont bénéficient ces membres pour les plannings du widget Agendas métier. Pour plus d'informations sur le widget Rôles de sécurité, voir widget Rôles de sécurité dans la documentation WebSphere Process Server for Multiplatforms.

Pour WebSphere Business Compass, le widget Contrôle d'accès du serveur de publication gère les autorisations des utilisateurs qui peuvent effectuer des vérifications et les commenter. Pour plus d'informations, voir l'aide en ligne des widgets.

Configuration de Tivoli Access Manager WebSEAL pour Business Space

Si vous disposez de Tivoli Access Manager WebSEAL et que vous souhaitez l'utiliser avec Business Space, vous devez effectuer plusieurs étapes de configuration supplémentaires.

Pourquoi et quand exécuter cette tâche

Portée de la rubrique : Cette rubrique s'applique aux produits suivants :

- WebSphere Business Monitor
- WebSphere Enterprise Service Bus
- WebSphere Process Server

Si vous souhaitez utiliser Tivoli Access Manager WebSEAL avec Business Space, vous devez configurer la sécurité de Tivoli Access Manager avec un fournisseur JACC (Java Authorization Contract for Containers) externe, configurer WebSEAL avec Tivoli Access Manager, configurer WebSEAL avec le serveur d'applications de votre produit et configurer les jonctions hôte de votre environnement.

Procédure

Procédure

1. Configurez Tivoli Access Manager avec JACC.
   a. Effectuez l'une des étapes ci-après, selon que vous souhaitiez utiliser la console d'administration ou les commandes wsadmin.
      - Si vous voulez utiliser la console d'administration pour configurer Tivoli Access Manager avec JACC, procédez comme suit :
        1) Activez la sécurité globale.
           a) Sélectionnez **Sécurité** > **Sécurité globale**.
           b) Activez la **sécurité d'administration**, la **sécurité des applications** et la **sécurité Java 2** avec le serveur LDAP avec lequel Tivoli Access Manager est configuré.
           c) Sélectionnez **Sécurité globale** > **LDAP**, entrez les informations ci-après, puis cliquez sur **OK**.

Nom	Description
`ID utilisateur du serveur`	Entrez l'ID utilisateur que vous avez entré pour le nom distinctif de l'administrateur dans les paramètres Tivoli Access Manager. Exemple : `user1`
`Mot de passe de l'utilisateur du serveur`	`puser1`
`Hôte`	LDAP configuré avec Tivoli Access Manager
`Port`	Exemple : `389`
`Nom distinctif de base`	Exemple : `o=ibm,c=us`
`Nom distinctif de liaison`	Exemple : `cn=SecurityMaster,secAuthority=Default`
`Mot de passe de liaison`	Mot de passe de l'utilisateur SecurityMaster

           d) Sauvegardez la configuration et redémarrez le serveur.

2) Activez les autorisations externes avec Tivoli Access Manager et JACC.
   a) Sélectionnez **Sécurité** > **Sécurité globale** > **Fourniseurs d'autorisation externes**.
   b) Dans la liste **Fournisseur d'autorisations**, sélectionnez **Fournisseur JACC externe**, puis cliquez sur **Configurer**. Les propriétés par défaut de Tivoli Access Manager sont correctes. Pour utiliser les valeurs par défaut, ne les modifiez pas.
   c) Sous **Propriétés supplémentaires**, sélectionnez **Propriétés Tivoli Access Manager**. Sélectionnez **Activer le programme Tivoli Access Manager intégré**, entrez les informations ci-après, puis cliquez sur **OK**.

Nom	Valeur
Ensemble de ports d'écoute du client	La valeur par défaut est 8900 - 8999. Ne la modifiez que si vous souhaitez utiliser des ports différents.
Serveur de règles (name:port)	Spécifiez vos valeurs *serveur_règles*:*port*. Exemple : `windomain3.rtp.raleigh.ibm.com:7135`
Serveurs d'autorisations et priorité (name:port:priority)	Spécifiez vos valeurs *serveurs_autorisations*:*port*:*priorité*. Exemple : `windomain3.rtp.raleigh.ibm.com:7136:1`
Nom de l'administrateur	Conservez le nom d'utilisateur **sec_master (valeur par défaut)**, sauf si vous utilisez un nom d'administrateur différent sur le serveur Tivoli Access Manager.
Mot de passe de l'administrateur	`domino123`
Suffixe du nom distinctif du registre d'utilisateurs	Entrez le nom à utiliser pour votre serveur d'applications. Exemple : `o=ibm,c=us`
Domaine de sécurité	Conservez la **valeur par défaut** pour le domaine de sécurité. Modifiez cette valeur si vous n'utilisez pas le domaine par défaut sur le serveur Tivoli Access Manager. Modifiez cette valeur si plusieurs domaines ont été créés sur le serveur Tivoli Access Manager et que vous souhaitez utiliser ou vous connecter à un domaine autre que le domaine **par défaut**.
Nom distinctif de l'administrateur	Entrez le nom qualifié complet de l'utilisateur. Exemple : `cn=user1,o=ibm,c=us` **Remarque :** Cet utilisateur correspond à l'**ID utilisateur du serveur** configuré dans le panneau du registre d'utilisateurs LDAP.

Le serveur contacte le serveur Tivoli Access Manager et crée plusieurs fichiers de propriétés sous le serveur d'applications. Ce processus peut prendre quelques minutes. En cas d'erreur, consultez la `sortie système` et corrigez le problème.

- Si vous voulez utiliser l'utilitaire wsadmin pour configurer Tivoli Access Manager avec JACC, effectuez les étapes ci-après. Effectuez la procédure ci-après une seule fois sur le serveur du gestionnaire de déploiement. Les paramètres de configuration sont transmis aux serveurs gérés, et

notamment aux agents de noeud, lors d'une synchronisation. Les serveurs gérés doivent être eux-mêmes redémarrés pour que les modifications de la configuration soient appliquées.

1) Vérifiez que tous les serveurs gérés, y compris les agents de noeud, sont démarrés.
2) Démarrez le serveur.
3) Démarrez l'utilitaire de ligne de commande en exécutant la commande **wsadmin** à partir du répertoire *racine_install*/bin.
4) A l'invite de wsadmin, exécutez la commande **configureTAM**, en spécifiant les informations appropriées à partir du tableau suivant :

   Exemple Jacl :

   ```
   $AdminTask configureTAM -interactive
   ```

   Exemple Jython :

   ```
   AdminTask.configureTAM('-interactive')
   ```
   Entrez ensuite les informations suivantes :

Nom	Valeur
Nom de noeud du serveur de votre produit	Spécifiez un noeud unique ou entrez un astérisque (*) pour choisir tous les noeuds.
Serveur de règles Tivoli Access Manager	Entrez le nom du serveur de règles Tivoli Access Manager et le port de connexion. Utilisez le format, *serveur_règles*:*port*. Le port de communication du serveur de règles est défini lors de la configuration de Tivoli Access Manager. Le port par défaut est 7135.
Serveur d'autorisations Tivoli Access Manager	Entrez le nom du serveur d'autorisations Tivoli Access Manager. Utilisez le format, *serveur_autorisations*:*port*:*priorité*. Le port de communication du serveur d'autorisations est défini lors de la configuration de Tivoli Access Manager. Le port par défaut est 7136. Vous pouvez spécifier plusieurs serveurs d'autorisations en séparant les entrées par des virgules. Il est utile que plusieurs serveurs d'autorisations soient configurés à des fins de reprise en ligne et de performances. La valeur de la priorité correspond à l'ordre d'utilisation du serveur d'autorisations. Par exemple : `auth_server1:7136:1,auth_server2:7137:2`. La priorité 1 est tout de même requise lors de la configuration sur un seul serveur d'autorisations.
Nom distinctif de l'administrateur du serveur de votre produit	Entrez le nom distinctif complet correspondant à l'ID administrateur de la sécurité du serveur de votre produit. Par exemple : `cn=wasadmin,o=organization,c=country`. Pour plus d'informations, voir le lien correspondant.
Suffixe du nom distinctif du registre d'utilisateurs Tivoli Access Manager	Par exemple : o=organization, c=country

Nom	Valeur
Nom de l'administrateur Tivoli Access Manager	Entrez l'ID administrateur Tivoli Access Manager, tel qu'il a été créé lors de la configuration de Tivoli Access Manager. Cet ID est généralement sec_master.
Mot de passe utilisateur de l'administrateur Tivoli Access Manager	Entrez le mot de passe de l'administrateur Tivoli Access Manager.
Domaine de sécurité de Tivoli Access Manager	Entrez le nom du domaine de sécurité de Tivoli Access Manager utilisé pour stocker les utilisateurs et les groupes. Si aucun domaine de sécurité n'est encore établi au moment de la configuration de Tivoli Access Manager, cliquez sur **Retour** pour accepter la valeur par défaut.
Ensemble de ports d'écoute du programme Tivoli Access Manager intégré	Le serveur du produit écoute sur un port TCP/IP les mises à jour de la base de données d'autorisations du serveur de règles. Plusieurs processus pouvant être exécutés sur une machine et un noeud particulier, une liste de ports est requise pour les processus. Spécifiez les ports utilisés comme ports d'écoute par les clients Tivoli Access Manager, en les séparant par des virgules. Si vous spécifiez une plage de ports, séparez la valeur la plus faible de la valeur la plus élevée par un signe deux-points. Par exemple, 7999, 9990:9999.
Différer	Si cette option a la valeur `yes`, elle diffère la configuration du serveur de gestion jusqu'au prochain redémarrage. Si sa valeur est `no`, la configuration du serveur de gestion est immédiate. Les serveurs gérés sont configurés au prochain redémarrage.

5) Une fois que vous avez entrée toutes les informations requises, sélectionnez **F** pour sauvegarder les propriétés de configuration ou **C** pour annuler la procédure de configuration et effacer les informations entrées.

   Exemple avec le serveur SVTM TAM60 :

```
wsadmin>$AdminTask configureTAM -interactive
Configurer le programme Tivoli Access Manager intégré

Cette commande configure le serveur Tivoli Access Manager imbriqué sur le ou les noeuds WebSphere
Application Server spécifiés.

Nom du noeud WebSphere Application Server (nodeName) : *
*Serveur de règles Tivoli Access Manager (policySvr) :
 windomain3.rtp.raleigh.ibm.com:7135
*Serveurs d'autorisations Tivoli Access Manager (authSvrs) :
 windomain3.rtp.raleigh.ibm.com:7136:1
*Nom distinctif de l'administrateur WebSphere Application Server (wasAdminDN) :
 cn=was61admin,o=ibm,c=us
*Suffixe du nom distinctif du registre d'utilisateurs Tivoli Access Manager (dnSuffix) :
o=ibm,c=us
Nom d'utilisateur de l'administrateur Tivoli Access Manager (adminUid) :
 [sec_master]
*Mot de passe utilisateur de l'administrateur Tivoli Access Manager (adminPasswd) :
 domino123
Domaine de sécurité Tivoli Access Manager (secDomain) : [Valeur par défaut]
Ensemble de ports d'écoute du programme Tivoli Access Manager intégré (portSet) : [9900:9999]
Différer (defer) : [no]

Configurer le programme Tivoli Access Manager intégré

F (Terminer)
C (Annuler)

Sélectionnez [F, C] : [F] F
WASX7278I: Ligne de commande générée : $AdminTask configureTAM {-policySvr
 windomain3.rtp.raleigh.ibm.com:7135 -authSvrs
 windomain3.rtp.raleigh.ibm.com:7136:1 -wasAdminDN cn=wa
La sauvegarde des paramètres d'action de configuration du programme Tivoli Access Manager intégré a abouti.
 Redémarrez toutes les instances WebSphere Application Server en cours d'exécution sur le noeud ou les noeuds cible afin de mener à terme l'action de configuration.
wsadmin>
```

6) Sur la console d'administration, sélectionnez **Sécurité** > **Sécurité globale** > **Fourniseurs d'autorisation externes**. Sélectionnez ensuite **Autorisation externe utilisant un fournisseur JACC**, puis cliquez sur **OK**.

7) Accédez à l'écran principal de la sécurité, puis cliquez sur **OK**. Enregistrez et synchronisez vos modifications.
8) Redémarrez tous les processus de votre cellule.

b. Si vous avez installé des applications avant d'activer Tivoli Access Manager (par exemple, vous avez activé la sécurité LDAP, installé des applications sécurisées et mappé des utilisateurs et des groupes à des rôles de sécurité), propagez les informations de mappage des rôles de sécurité des descripteurs de déploiement vers le serveur de règles Tivoli Access Manager. Effectuez l'une des étapes ci-après, selon que vous souhaitiez utiliser la console d'administration ou les commandes wsadmin.
   - Si vous souhaitez utiliser la commande wsadmin **propagatePolicyToJACCProvider**, consultez la rubrique Transmission des règles de sécurité des applications installées à un fournisseur JACC à l'aide de wsadmin.
   - Si vous souhaitez utiliser la console d'administration, consultez la rubrique Transmission des règles de sécurité et des rôles des applications déjà déployées.

2. Configurez WebSEAL avec Tivoli Access Manager.
   a. Vérifiez que WebSEAL est installé et configuré correctement.
   b. Créez la jonction entre WebSEAL et le serveur d'applications de votre produit à l'aide de l'option **-c iv_creds** pour TAI++ et de l'option **-c iv_user** pour TAI. Entrez l'une des commandes suivantes sur une même ligne, en utilisant les variables correspondant à votre environnement :

      Pour TAI++

      ```
      server task webseald-server create -t tcp -b supply -c iv_creds
      -h nom_hôte -p numéro_port_app_websphere nom_jonction
      ```

   c. Pour créer un compte utilisateur sécurisé dans Tivoli Access Manager, qui peut être utilisé pour configurer TAI, exécutez les commandes suivantes :

      ```
      pdadmin -a sec_master -p domino123
      pdadmin sec_master> user create -gsouser -no-password-policy taiuser
      "cn=taiuser,ou=websphere,o=ibm,c=us" taiuser taiuser ptaiuser
      pdadmin sec_master> user modify taiuser password-valid yes
      pdadmin sec_master> user modify taiuser account-valid yes
      ```

   d. Dans le fichier de configuration de WebSEAL, *répertoire_installation_webseal*/etc/webseald-default.conf, définissez le paramètre suivant :

      ```
      basicauth-dummy-passwd=mot_de_passe_id_utilisateur_webseal
      ```

      Par exemple, si vous avez défini taiuser/ptaiuser dans Tivoli Access Manager, définissez le paramètre suivant :`basicauth-dummy-passwd = ptaiuser`

      Si vous utilisez une authentification par formulaire, définissez les paramètres suivants :

      ```
      forms-auth=both
      ba-auth=none
      ```

3. Configurez WebSEAL avec le serveur d'applications de votre produit en activant l'intercepteur TAI++ sur le serveur.
   a. Sur la console d'administration, sélectionnez **Sécurité globale** > **Mécanismes d'authentification et d'expiration**.
   b. Développez **Web et sécurité SIP**, puis sélectionnez **Relations de confiance**. Cochez la case et cliquez sur **Appliquer**.

c. Sélectionnez **Intercepteurs** > **TAMTrustAssociationInterceptorPlus** > **propriétés personnalisées** et ajoutez les propriétés suivantes :

Nom	Valeur
com.ibm.websphere.security.webseal.configURL	${WAS_INSTALL_ROOT}/java/jre/PdPerm.properties
com.ibm.websphere.security.webseal.id	iv-creds
com.ibm.websphere.security.webseal.loginId	taiuser (si l'utilisateur taiuser/ptaiuser a été créé dans Tivoli Access Manager)

d. Redémarrez la cellule.

e. Pour accéder au client, accédez à https://*nom_serveur_webseal*:*port_webseal*/*nom_jonction*/*uri_web_client*.

4. Configurez les jonctions hôte pour votre environnement, de sorte que les widgets Business Space apparaissent. Effectuez l'une des étapes ci-après, selon que vous utilisiez des jonctions hôte ou des jonctions hôte transparentes.

   • Si vous utilisez des jonctions hôte virtuelles, créez une jonction hôte virtuelle. Une jonction hôte virtuelle élimine la nécessité de créer des jonctions distinctes.

     a. Assurez-vous qu'un hôte virtuel a été configuré. Les jonctions hôte virtuelles correspondent à un hôte et un numéro de port et acheminent les adresses à l'hôte cible. Aucun filtrage d'URL n'est effectué et toutes les demandes correspondantes sont acheminées vers l'hôte cible.

     b. Assurez-vous que les applications ci-après sont disponibles pour le même hôte virtuel. La liste ci-après peut contenir l'intégralité des applications ou certaines d'entre elles, suivant les produits que vous utilisez avec Business Space.

        – BPMAdministrationWidgets_*nomnoeud_nomserveur* (pour WebSphere Enterprise Service Bus et WebSphere Process Server)
        – BusinessSpaceHelpEAR_*nomnoeud_nomserveur* (pour tous les produits)
        – BSpaceEAR_*nomnoeud_nomserveur* (pour tous les produits)
        – BSpaceWebformsEnabler_*nomnoeud_nomserveur* (pour tous les produits)
        – HumanTaskManagementWidgets_*nomnoeud_nomserveur* (pour WebSphere Process Server et WebSphere Business Monitor)
        – REST Services Gateway (pour tous les produits)
        – REST Services Gateway Dmgr (pour WebSphere Enterprise Service Bus et WebSphere Process Server)
        – mm.was_*nomnoeud_nomserveur* (pour tous les produits)
        – WBMDashboardWeb_*nomnoeud_nomserveur* (pour WebSphere Business Monitor)
        – wesbWidgets_*nomnoeud_nomserveur* (pour WebSphere Enterprise Service Bus)
        – widgets_busleader_*nomnoeud_nomserveur* (pour WebSphere Business Compass)
        – widgets_pubserver_*nomnoeud_nomserveur* (pour WebSphere Business Compass)
        – widgets_fabric_*nomnoeud_nomserveur* (pour WebSphere Business Services Fabric)

        Remarque : Cette liste d'applications ne couvre que les applications requises par Business Space. Il se peut que vous deviez ajouter d'autres

applications à cette liste pour les scénarios autres que des scénarios Business Space, qui utilisent Tivoli Access Manager WebSEAL.

c. Exécutez la commande suivante en utilisant pdadmin : `server task` *`serveur_webseal`* `virtualhost create -t` *`transport`* `-h` *`hôte_cible`* `[-p` *`port`*`] [-v` *`nom_hôte_virtuel`*`]` *`libellé_hôte_virtuel`*

   Utilisez les information suivantes :

   – *serveur_webseal* correspond au nom du serveur WebSEAL sur lequel vous créerez l'entrée d'hôte virtuel.
   – *transport* correspond au type de transport. Les entrées valides sont `tcp`, `ssl`, `tcpproxy` et `sslproxy`.
   – *hôte_cible* correspond à l'hôte de l'application requise.
   – *nom_hôte_virtuel* permet d'associer les demandes HTTP à une jonction d'hôte virtuel. Si aucune valeur n'est entrée, cette valeur est composée de l'hôte cible et du port par défaut. Par exemple, si vous spécifiez pour *nom_hôte_virtuel* la valeur `myvirthost.ibm.com:80`, WebSEAL recherche les URL contenant `myvirthost.ibm.com:80` et les achemine vers l'hôte spécifié dans la commande pdadmin.
   – *nom_hôte_virtuel* correspond au libellé permettant d'identifier l'entrée dans WebSEAL. Ce libellé doit être unique.

   Pour que Business Space fonctionne correctement, les entrées `ssl` et `tcp` doivent être toutes deux crées pour le type de transport. Si SSL (Secure Sockets Layer) et TCP (Transmission Control Protocol) (TCP) doivent être tous deux pris en charge dans une même jonction d'hôte virtuel, vous devez utiliser l'option -g *libellé_hôte_virtuel*, *libellé_hôte_virtuel* correspondant au libellé d'hôte virtuel d'origine, pour partager la configuration. Cette option recherche une jonction d'hôte virtuel déjà créée (une jonction créée précédemment, où *nom_hôte_virtuel* correspond au libellé spécifié dans l'option -g) et partage cette configuration. La seconde entrée a cependant toujours besoin de sa propre valeur *nom_hôte_virtuel*, mais elle peut partager l'hôte cible, le port et les autres valeurs. Si vous ne spécifiez pas cette option -g, il n'est pas possible de créer un second hôte virtuel car WebSEAL considère l'hôte cible et le port comme étant identiques à ceux d'une jonction créée précédemment (ce qui n'est pas autorisé).

- Si vous utilisez des jonctions hôte transparentes, créez une série de jonctions de chemin transparentes pour les widgets de chaque produit.

  a. Exécutez la commande suivante en utilisant pdadmin : `server task` *`serveur_webseal`* `create -t` *`type_transport (ssl) ou (tcp)`* `-x -h hostname` *`chemin`*

     Par exemple, entrez : `server task webseald-default create -t tcp -x -h monServer.ibm.com /BusinessSpace`.

  b. Créez les racines de contexte suivantes pour votre produit : Mappage des adresses URL Business Space pour un serveur proxy inverse.

5. Effectuez des étapes de configuration supplémentaires pour résoudre les incidents relatifs aux cookies de programme de navigateur et aux hôtes virtuels.

   a. Pour résoudre le nouveau nom du cookie Business Space, ajoutez le contenu suivant au fichier de configuration de WebSEAL :

   ```
   [preserve-cookie-names]
   name = com.ibm.bspace.UserName
   name = com.ibm.wbimonitor.UserName
   ```

b. Facultatif : Si vous utilisez des hôtes virtuels autres que ceux par défaut avec une racine de contexte, vous risquez de rencontrez des erreurs dans les pages Business Space. Il se peut que vous deviez empêcher la jonction de réécrire le JavaScript dans les pages Business Space en ajoutant la jonction -j à la racine de contexte. Exécutez la commande suivante : `server task default-webseald create -f -h nomhôte -p numéroport -t tcp -b supply -c iv-user,iv-creds,iv-groups -x -s -j -J trailer/contexte_racine`

Affectation du rôle de superutilisateur Business Space

Dans Business Space, vous pouvez octroyer à des utilisateurs des droits de superutilisateur (ou d'administrateur de Business Space). Un superutilisateur peut afficher, éditer et supprimer tous les espaces et les pages, peut gérer et créer des modèles et modifier le propriétaire d'un espace en modifiant l'ID propriétaire.

Avant de commencer

Si la sécurité administrative est activée lorsque vous configurez Business Space, étudiez les informations suivantes sur les groupes et les superutilisateurs :

- Les utilisateurs appartenant au groupe d'utilisateurs spécial, **administrateurs**, possède le rôle de superutilisateur par défaut. Par conséquent, l'affectation du rôle de superutilisateur est gérée par l'appartenance au groupe d'utilisateurs.
- Dans un environnement à un serveur, le serveur Business Space crée le groupe d'utilisateurs **administrateurs** dans le registre d'utilisateurs par défaut. L'ID administrateur fourni lors de la configuration est automatiquement ajouté comme membre de ce groupe.
- Dans un environnement de déploiement réseau, le groupe d'utilisateurs **administrateurs** n'est pas créé automatiquement. Utilisez le script `createSuperUser.py` pour créer le groupe d'utilisateurs et y ajouter des membres, dans le registre d'utilisateurs par défaut.
- Si un autre registre d'utilisateurs (par exemple, LDAP) est utilisé à la place du registre d'utilisateurs par défaut ou que le registre d'utilisateurs par défaut est utilisé, mais que vous ne souhaitez pas utiliser le groupe d'utilisateurs **administrateurs**, vous devez identifier le groupe d'utilisateurs que vous utilisez pour les superutilisateurs Business Space. Assurez-vous que la valeur que vous spécifiez peut être comprise par le registre d'utilisateurs. Par exemple, pour LDAP, vous pouvez spécifier un nom tel que `cn=administrators,dc=company,dc=com`. Pour plus d'informations sur l'identification de ce groupe d'utilisateurs, reportez-vous aux instructions de modification du groupe des administrateurs, dans la section Que faire ensuite.
- Pour Business Space dans WebSphere Portal, le groupe par défaut **wpsadmins** est également utilisé pour le rôle de superutilisateur. Les membres de ce groupe reçoivent le rôle de superutilisateur de Business Space.

  Remarque : La sécurité doit être activée si vous souhaitez utiliser Business Space dans WebSphere Portal.

Si la sécurité administrative n'est pas activée lorsque vous configurez Business Space, seul l'ID utilisateur spécial **BPMAdministrator** possède le rôle de superutilisateur Business Space.

Si vous possédez un environnement de déploiement réseau, vous devez exécuter le script `createSuperUser.py` pour affecter le rôle de superutilisateur : pour créer le groupe d'utilisateurs et ajouter des membres. Avant d'exécuter ce script, effectuez les étapes suivantes :

- Assurez-vous que le nom par défaut du groupe **administrateurs** n'a pas été modifié.
- Utilisez le référentiel par défaut pour le registre d'utilisateurs.
- Démarrez le serveur ou le gestionnaire de déploiement de votre environnement Business Space pour le profil où Business Space est installé.

Procédure

Procédure

1. Recherchez le script *racine_install*`\BusinessSpace\scripts\createSuperUser.py` pour affecter le rôle de superutilisateur à un utilisateur.
2. Ouvrez une invite de commande et accédez au répertoire suivant : *racine_profil*`\bin`, *racine_profil* représentant le répertoire du profil où Business Space est installé.
3. Entrez la commande suivante : `wsadmin -lang jython -f` *racine_install*`\BusinessSpace\scripts\createSuperUser.py` *nom_abrégé_utilisateur mot_de_passe* Où *nom_abrégé_utilisateur* correspond à l'identificateur unique d'un utilisateur de VMM (Virtual Member Manager) et *mot_de_passe*, au mot de passe VMM de cet utilisateur. Si cet utilisateur existe dans VMM, l'utilisateur est ajouté au groupe des administrateurs.

   Remarque : Si le chemin contient un espace (par eemple, si *racine_install* correspond à `Mon répertoire d'installation`, vous devez le placer entre guillemets. Par exemple, entrez la commande suivante : `wsadmin -lang jython -f "\My install dir\BusinessSpace\scripts\createSuperUser.py"` *nom_abrégé_utilisateur_dans_VMM*.

Que faire ensuite

Pour ouvrir Business Space, utilisez l'URL suivant : http://*hôte:port*/BusinessSpace, où *hôte* est le nom d'hôte sur lequel votre serveur s'exécute et *port*, le numéro de port de votre serveur.

Vous pouvez modifier le groupe d'utilisateurs spéciaux par défaut intitulé **administrateurs**. Pour vérifier le nom de groupe actuel ou le renommer, effectuez les étapes ci-après.

Inspectez la valeur `com.ibm.mashups.adminGroupName` dans le fichier de configuration :

- *racine_profil*`\BusinessSpace\`*nom_noeud*`\`*nom_serveur*`\mm.runtime.prof\config\ConfigService.properties` sur un serveur autonome ou
- *racine_profil_gestionnaire_déploiement*`\BusinessSpace\`*nom_cluster*`\mm.runtime.prof\config\ConfigService.properties` sur un cluster.

Pour modifier un groupe d'utilisateurs, effectuez les étapes suivantes sur un serveur autonome :

1. Modifiez la valeur `com.ibm.mashups.adminGroupName` dans le fichier de configuration *racine_profil*`\BusinessSpace\`*nom_noeud*`\`*nom_serveur*`\mm.runtime.prof\config\ConfigService.properties`.

2. Exécutez la commande updatePropertyConfig dans l'environnement wsadmin du profil :$AdminTask updatePropertyConfig {-serverName *nom_serveur* -nodeName *nom_noeud* -propertyFileName"*racine_profil*\BusinessSpace*nom_noeud**nom_serveur*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} et exécutez$AdminConfig save.
3. Redémarrez le serveur.

Pour modifier un groupe d'utilisateurs, effectuez les étapes suivantes sur un cluster :

1. Vérifiez que le groupe existe dans le référentiel d'utilisateurs.
2. Modifiez la valeur com.ibm.mashups.adminGroupName dans le fichier de configuration *racine_profil_gestionnaire_déploiement*\BusinessSpace*nom_cluster*\mm.runtime.prof\config\ConfigService.properties.
3. Exécutez la commande updatePropertyConfig dans l'environnement wsadmin du profil de l'environnement de déploiement :$AdminTask updatePropertyConfig {-clusterName *nom_cluster* -propertyFileName "*racine_profil_gestionnaire_déploiement*\BusinessSpace*nom_cluster*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} et exécutez $AdminConfig save.
4. Redémarrez le gestionnaire de déploiement.

Pour modifier le superutilisateur lorsque la sécurité n'est pas activée, effectuez les étapes suivantes sur un serveur autonome :

1. Vérifiez que le groupe existe dans le référentiel d'utilisateurs.
2. Modifiez la valeur noSecurityAdminInternalUserOnly dans le fichier de configuration *racine_profil*\BusinessSpace*nom_noeud**nom_serveur*\mm.runtime.prof\config\ConfigService.properties.
3. Exécutez la commande updatePropertyConfig dans l'environnement wsadmin du profil :$AdminTask updatePropertyConfig {-serverName *nom_serveur* -nodeName *nom_noeud* -propertyFileName"*racine_profil*\BusinessSpace*nom_noeud**nom_serveur*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} et exécutez$AdminConfig save.
4. Redémarrez le serveur.

Pour modifier le superutilisateur lorsque la sécurité n'est pas activée, effectuez les étapes suivantes sur un cluster :

1. Modifiez la valeur noSecurityAdminInternalUserOnly dans le fichier de configuration *racine_profil_gestionnaire_déploiement*\BusinessSpace*nom_cluster*\mm.runtime.prof\config\ConfigService.properties.
2. Exécutez la commande updatePropertyConfig dans l'environnement wsadmin du profil de l'environnement de déploiement :$AdminTask updatePropertyConfig {-clusterName *nom_cluster* -propertyFileName "*racine_profil_gestionnaire_déploiement*\BusinessSpace*nom_cluster*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} et exécutez $AdminConfig save.
3. Redémarrez le gestionnaire de déploiement.

Création 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

Ces scénarios supposent tous que la sécurité administrative est activée.

Procédure

Procédure

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

Exemple

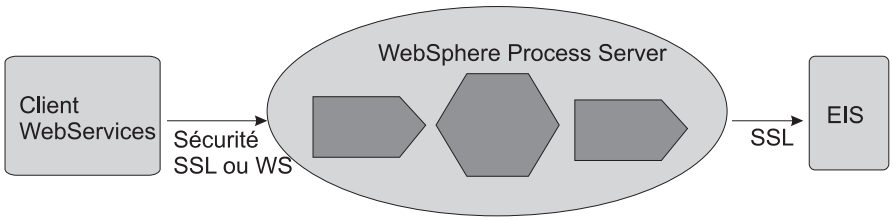
Scénario d'intégration classique - Adaptateurs entrants et sortants

Une demande entrante provient d'un adaptateur WebSphere Business Integration Adapter. L'architecture SCA (Service Component Architecture) appelle une mappe d'interface basée sur l'exportation SCA. La demande est acheminée par un composant de processus et une deuxième mappe d'interface, puis est transmise à un deuxième EIS (B), à l'aide 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 de service Web

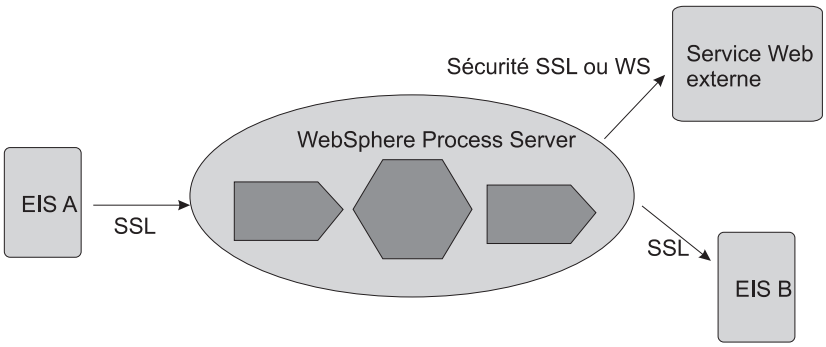
Dans ce scénario, un client de services Web appelle un composant WebSphere Process Server. La demande transite par plusieurs composants de l'environnement WebSphere Process Server avant d'être transmise à un EIS via un adaptateur.



Vous pouvez authentifier le client de services Web comme étant un client SSL, en utilisant une authentification HTTP de base ou une authentification WS-Security. Lorsque le client est authentifié, le contrôle d'accès est appliqué en définissant le 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 entrante de service Web

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



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

Demande entrante Application Web - HTTP vers WebSphere Process Server

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

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

En outre, pour protéger votre intranet de toute intrusion, vous pouvez placer le serveur Web dans la zone démilitarisée (DMZ) et WebSphere Process Server à l'intérieur du pare-feu interne. Dans cet exemple, WebSEAL est le proxy inverse

qui procède à l'authentification. Il est dans une relation de confiance avec WebSphere Process Server derrière le pare-feu et peut réacheminer les demandes authentifiées.