

Tivoli Federated Identity Manager
Version 6.2.1

*Guide d'identification et de résolution
des problèmes*

IBM

Tivoli Federated Identity Manager
Version 6.2.1

*Guide d'identification et de résolution
des problèmes*

IBM

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 63.

Première édition - juin 2010

Réf. US : GC27-2715-00

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

© Copyright IBM France 2010. Tous droits réservés.

© **Copyright IBM Corporation 2006, 2010.**

Table des matières

Avis aux lecteurs canadiens v

A propos de ce document vii

Public ciblé	vii
Publications	vii
Bibliothèque IBM Tivoli Federated Identity Manager	vii
Publications prérequisées	viii
Documentation associée	viii
Accès à la terminologie en ligne	ix
Accès aux publications en ligne	ix
Commande de publications	ix
Accessibilité	x
Formation technique Tivoli	x
Informations de support	x
Conventions utilisées dans ce document	x
Conventions typographiques	x
Variables et chemins de système d'exploitation	xi

Chapitre 1. Identification des problèmes et support 1

Chapitre 2. En savoir plus sur les symptômes d'un problème. 3

A propos de l'identification et résolution des problèmes	3
A propos des problèmes de connectivité	5
A propos de Tivoli Federated Identity Manager.	6
A propos des correctifs et des mises à jour	6
A propos des messages	7
A propos des problèmes de performances et des blocages	8
A propos des interruptions, pannes et abandons	9

Chapitre 3. Liste d'identification des problèmes de Tivoli Federated Identity Manager 11

Chapitre 4. Problèmes connus et solutions. 13

Problèmes d'installation	13
Problèmes de désinstallation.	14
Problèmes de configuration de Tivoli Federated Identity Manager	16
Problèmes associés à Integrated Solutions Console	25
Affichage de plusieurs messages vous invitant à redémarrer WebSphere Application Server	25
Opérations incomplètes après la déconnexion de la console	26
Redémarrage de WebSphere Application Server après la reconfiguration des paramètres de sécurité dans la console de gestion	26

Arrêt de WebSphere Application Server à partir de la ligne de commande après le redémarrage de Tivoli Federated Identity Manager à partir de la console	26
Limitation dans le panneau Instances de module de gestion	27
Problèmes associés à la console WebSphere Application Server	27
WebSphere Application Server doit être installé séparément pour chaque instance de la console de gestion	27
L'environnement d'exécution ou le service de gestion ne s'affiche pas dans la console d'administration WebSphere	28
Les modifications de configuration ne sont pas propagées à chaque noeud de cluster tant que l'environnement d'exécution de Federated Identity Manager n'a pas redémarré	28
La console WebSphere indique que le service de gestion est indisponible	29
Obtention du statut du module d'exécution de Tivoli Federated Identity Manager.	29
Problèmes opérationnels	30
Impossible de se connecter à WebSphere lors de l'utilisation de l'adaptateur VMM Tivoli Access Manager	32
Problèmes de déploiement	33
Echec du déploiement de Tivoli Federated Identity Manager sous z/OS.	33
Erreur lors de l'opération de déploiement	34
Déploiement de Tivoli Federated Identity Manager dans un environnement en cluster vertical WebSphere	35
Le déploiement de Tivoli Federated Identity Manager dans un cluster requiert la reconnaissance des agents de noeud	35
Problèmes de personnalisation	36

Chapitre 5. Correctifs 39

Obtention de correctifs	39
Réception des notifications de correctifs	39

Chapitre 6. Recherche dans les bases de connaissances 41

Chapitre 7. Collecte de données. 43

Journaux de messages et de trace	44
Journaux de messages	44
Journaux de trace	45
Configuration des paramètres du journal	47
Configuration de la consignation des messages	47
Activation de la consignation de trace	48
Affichage des journaux	50
Utilisation du composant IBM Support Assistant	51
Utilisation d'IBM Support Assistant en mode graphique	51

Utilisation d'IBM Support Assistant en mode console	53	Définition de l'impact sur l'entreprise.	59
Chapitre 8. Analyse des données	55	Description d'un incident.	59
Chapitre 9. Comment contacter le support ?	57	Envoi de données	60
Présentation du composant ISA.	57	Remarques	63
Contrats de maintenance logicielle IBM	59	Marques	65
		Index	67

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.

A propos de ce document

IBM® Tivoli Federated Identity Manager version 6.2.1 implémente des solutions de connexion unique fédérée, de gestion de la sécurité des services Web et d'application des accès basées sur des normes ouvertes. IBM Tivoli Federated Identity Manager étend les solutions d'authentification et d'autorisation fournies par IBM Tivoli Access Manager afin de simplifier l'intégration de plusieurs solutions Web existantes.

Le présent manuel décrit la procédure d'identification et de résolution des problèmes survenus dans IBM Tivoli Federated Identity Manager.

Public ciblé

Ce guide s'adresse aux architectes de la sécurité des réseaux, aux administrateurs système, aux administrateurs de réseau et aux intégrateurs système. Les lecteurs doivent savoir gérer les aspects de la sécurité des réseaux, la technologie de chiffrement, les clés et les certificats. Ils doivent également avoir une bonne connaissance de la mise en oeuvre des règles d'authentification et d'autorisation dans un environnement réparti.

Le présent guide décrit une mise en oeuvre d'une solution de services Web qui prend en charge plusieurs normes des services Web. Les lecteurs doivent connaître les normes des services Web spécifiques, telles qu'elle sont extraites de la documentation diffusée par l'organisme de normalisation pour chacune des normes concernées.

Les lecteurs doivent avoir une bonne connaissance du développement et du déploiement des applications à utiliser dans un environnement de services Web. Cela inclut une expérience en déploiement d'applications dans un environnement IBM WebSphere Application Server.

Publications

Consultez les descriptions de la bibliothèque IBM Tivoli Federated Identity Manager, les publications prérequis et connexes afin de déterminer lesquelles vous seront utiles. Elle indique également comment accéder aux publications Tivoli en ligne et comment les commander.

Bibliothèque IBM Tivoli Federated Identity Manager

Les documents de la bibliothèque IBM Tivoli Federated Identity Manager sont les suivants :

- *IBM Tivoli Federated Identity Manager - Guide de démarrage rapide*
Fournit des instructions pour la mise en route de IBM Tivoli Federated Identity Manager.
- *IBM Tivoli Federated Identity Manager - Guide d'installation*
Fournit des instructions pour l'installation de IBM Tivoli Federated Identity Manager.
- *IBM Tivoli Federated Identity Manager - Guide de configuration*

Fournit des instructions pour la configuration de IBM Tivoli Federated Identity Manager.

- *IBM Tivoli Federated Identity Manager for z/OS Program Directory*
Fournit des instructions pour l'installation de IBM Tivoli Federated Identity Manager sur z/OS.
- *IBM Tivoli Federated Identity Manager Guide d'administration*
Fournit des instructions pour réaliser les tâches d'administration nécessaires à tous les déploiements.
- *IBM Tivoli Federated Identity Manager - Guide de gestion de la sécurité des services Web*
Fournit des instructions pour réaliser les tâches de configuration nécessaires à la gestion de la sécurité des services Web.
- *IBM Tivoli Federated Identity Manager - Guide d'audit*
Fournit des instructions pour effectuer un audit des événements IBM Tivoli Federated Identity Manager.
- *IBM Tivoli Federated Identity Manager Error Message Reference*
Fournit des explications sur les messages d'erreur de IBM Tivoli Federated Identity Manager.
- *IBM Tivoli Federated Identity Manager - Guide d'identification et de résolution des problèmes*
Fournit des informations pour l'identification des incidents et des instructions pour les résoudre.

Vous pouvez vous procurer les publications à partir du centre de documentation de IBM Tivoli Federated Identity Manager :

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml

Publications prérequis

Pour utiliser efficacement le présent guide, vous devez vous familiariser avec les logiciels associés en consultant les sources suivantes :

- Centre de documentation d'IBM Tivoli Access Manager for e-business :
<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.itame.doc/toc.xml>
- Centre de documentation de IBM WebSphere Application Server Version 6.1 :
<http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp>
Vous pouvez obtenir les versions PDF de la documentation IBM WebSphere Application Server à l'adresse :
<http://www.ibm.com/software/webservers/appserv/was/library/>

Documentation associée

Vous pouvez obtenir les publications connexes sur les sites Web d'IBM suivants :

- Le Centre de documentation d'IBM Tivoli Federated Identity Manager Business Gateway à l'adresse
- *Enterprise Security Architecture avec IBM Tivoli Security Solutions*. Ce guide est disponible au format PDF (Portable Document Format) à l'adresse <http://www.redbooks.ibm.com/redbooks/pdfs/sg246014.pdf> ou au format

HTML (Hypertext Markup Language) à l'adresse <http://www.redbooks.ibm.com/redbooks/SG246014/>

- *Federated Identity Management et Web Services Security avec IBM Tivoli Security Solutions* (SG24-6394-01). Ce manuel est disponible au format PDF à l'adresse <http://www.redbooks.ibm.com/redbooks/pdfs/sg246394.pdf> ou au format HTML à l'adresse <http://www.redbooks.ibm.com/redbooks/SG246394/>
- La bibliothèque de logiciels Tivoli offre une grande diversité de documents Tivoli tels que des livres blancs, des fiches techniques, des démonstrations, des livres rouges et des lettres d'annonces. La bibliothèque de logiciels Tivoli est disponible sur le Web à l'adresse suivante : <http://publib.boulder.ibm.com/tividd/td/tdprodlist.html>
- Le document *Tivoli Software Glossary* inclut des définitions pour de nombreux termes techniques liés au logiciel Tivoli. Le document *Tivoli Software Glossary* est disponible à l'adresse suivante : <http://publib.boulder.ibm.com/tividd/glossary/tivologlossarymst.htm>

Accès à la terminologie en ligne

Le site terminologique Web rassemble la terminologie relative aux bibliothèques des produits IBM à un seul emplacement pratique. Vous pouvez accéder au site Web de la terminologie à l'adresse suivante : <http://www.ibm.com/software/globalization/terminology>

Accès aux publications en ligne

IBM propose des publications sur ce produit et d'autres produits Tivoli à mesure de leur disponibilité et à chaque mise à jour sur le site Web du centre de documentation Tivoli à l'adresse <http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp>.

Remarque : Si vous imprimez des documents PDF sur du papier qui n'est pas au format commercial, définissez l'option de la fenêtre **Fichier** → **Imprimer** permettant à Adobe® Reader d'imprimer des pages au format commercial sur votre format de papier local.

Commande de publications

Vous pouvez commander de nombreuses publications Tivoli en ligne sur le site Web suivant :
<http://www.elink.ibm.com/public/applications/cgibin/pbi.cgi>

Vous pouvez également passer votre commande par téléphone en composant l'un des numéros suivants :

- Aux Etats-Unis : 800-879-2755
- Au Canada : 800-426-4968

Pour obtenir la liste des numéros de téléphone pour les autres pays, voir le site Web suivant : <http://www.ibm.com/software/tivoli/order-lit/>

Accessibilité

Les fonctions d'accessibilité permettent à un utilisateur souffrant d'un handicap physique, comme une mobilité réduite ou une vision limitée, d'utiliser plus facilement les logiciels. Ce logiciel permet d'utiliser des technologies d'assistance pour entendre les commandes et naviguer dans l'interface. Il permet également d'utiliser le clavier à la place de la souris pour activer toutes les fonctions de l'interface graphique.

Pour plus d'informations, voir la rubrique "Accessibilité" dans le centre de documentation à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml.

Formation technique Tivoli

Pour obtenir des informations sur la formation technique Tivoli, consultez le site Web de formation d'IBM Tivoli à l'adresse : <http://www.ibm.com/software/tivoli/education>.

Informations de support

Si vous rencontrez un problème avec votre logiciel IBM, vous souhaitez le résoudre rapidement. IBM vous propose différentes manières d'obtenir l'aide dont vous avez besoin :

En ligne

Accédez au site du service de support logiciel IBM à l'adresse <http://www.ibm.com/software/support/probsub.html> et suivez les instructions.

IBM Support Assistant

ISA (IBM Support Assistant) est un outil de maintenabilité logicielle local et gratuit conçu pour vous aider à résoudre les problèmes et à trouver des réponses aux questions liées à l'utilisation des produits logiciels IBM. L'assistant ISA fournit un accès rapide aux informations d'aide et aux outils de mise en service pour la détermination d'un problème. Pour installer le logiciel ISA, voir *IBM Tivoli Federated Identity Manager - Guide d'installation*. Voir également à l'adresse <http://www.ibm.com/software/support/isa>.

Guide d'identification et de résolution des problèmes

Pour plus d'informations sur la résolution des problèmes, voir *IBM Tivoli Federated Identity Manager - Guide d'identification et de résolution des problèmes*.

Conventions utilisées dans ce document

Ce document utilise plusieurs conventions typographiques pour signaler des actions et des termes particuliers, ainsi que des commandes et des chemins d'accès spécifiques du système d'exploitation.

Conventions typographiques

Cette publication utilise les conventions typographiques suivantes :

Gras

- Commandes en minuscules ou majuscules-minuscules combinées difficiles à distinguer du texte environnant

- Composants d'interface (cases à cocher, boutons de fonction, boutons radio, sélecteurs rotatifs, zones, dossiers, icônes, listes déroulantes, options des listes déroulantes, listes à colonnes multiples, conteneurs, options de menu, noms de menus, onglets et pages de propriétés) et intitulés de rubrique (tels que **Astuce** : ou **Spécificité liée au système d'exploitation** :)
- Mots clés et paramètres du texte

Italique

- Citations (exemple : titres des publications, disquettes et CD)
- Mots définis dans le texte (exemple : une ligne spécialisée est appelée une *ligne point-à-point*)
- Emphase mise sur les mots et les lettres (exemple : "Utilisez le mot *que* pour commencer une clause restrictive."; exemple de lettres comme des lettres : "l'adresse LUN doit commencer par la lettre *L*.")
- Nouveaux termes du texte (sauf dans une liste de définitions) : une *vue* est un cadre dans un espace de travail contenant des données.
- Variables et valeurs à saisir : ... où *valeur1* représente....

Espacement simple

- Exemples et exemples de code
- Noms de fichier, mots clés de programmation et autres éléments difficiles à distinguer du texte environnant
- Texte des messages et invites destinés à l'utilisateur
- Texte que l'utilisateur doit taper
- Valeurs des arguments ou des options de commande

Variables et chemins de système d'exploitation

Le présent document utilise la convention UNIX[®] pour la spécification des variables d'environnement et la notation des répertoires.

Lorsque vous utilisez la ligne de commande Windows[®] remplacez la variable \$ par la variable% % pour les variables d'environnement et remplacez chaque barre oblique (/) par une barre oblique inverse (\) dans les noms de chemin des répertoires. Le nom des variables d'environnement n'est pas toujours le même dans les environnements Windows et UNIX. Par exemple, %TEMP% dans les environnements Windows est équivalent à \$TMPDIR dans les environnements UNIX.

Remarque : Si vous utilisez le shell bash sur un système Windows, vous pouvez vous servir des conventions UNIX.

Chapitre 1. Identification des problèmes et support

Le processus d'identification des problèmes nécessite de manière générale que vous isoliez et identifiez un problème, puis que vous cherchiez à le résoudre. Pour Tivoli Federated Identity Manager, vous pouvez utiliser une liste d'identification des problèmes pour vous aider. Si cette liste ne vous permet pas de résoudre un incident, vous pouvez collecter des données de diagnostic supplémentaires et les analyser vous-même, ou encore envoyer les données au support logiciel IBM en vue d'une analyse.

Les rubriques d'identification et de résolution des problèmes de Tivoli Federated Identity Manager sont organisées selon la séquence d'étapes suivante :

1. Apprenez en plus sur un symptôme ou une fonctionnalité.

Avant de pouvoir correctement identifier un symptôme ou un incident avec une fonctionnalité de produit spécifique, vous devez avoir une compréhension de base de ce symptôme ou de cette fonctionnalité.

2. Suivez la liste d'identification des incidents pour la fonctionnalité ou le symptôme correspondant(e).

La liste d'identification des incidents propose une série de questions qui vous guident dans le processus d'isolation et d'identification de l'incident. Si IBM connaît l'incident, la liste vous guide vers un correctif, une solution ou une solution palliative publiés.

Si la liste d'identification des incidents ne vous a pas permis de résoudre le problème, poursuivez en appliquant l'étape suivante.

3. Collectez des données de diagnostic.

Ces informations expliquent comment recueillir les renseignements dont le support logiciel IBM ou vous-même devez disposer pour déterminer la source d'un incident.

4. Analysez les données de diagnostic.

Ces informations expliquent comment analyser les données de diagnostic que vous avez recueillies.

Chapitre 2. En savoir plus sur les symptômes d'un problème

La première étape du processus d'identification des incidents consiste à en savoir plus sur les symptômes du problème ou sur la fonctionnalité de produit concernée.

Les rubriques suivantes peuvent vous permettre d'acquérir les informations conceptuelles dont vous avez besoin pour résoudre efficacement les incidents susceptibles de se produire lorsque vous utilisez IBM Tivoli Federated Identity Manager :

- «A propos de l'identification et résolution des problèmes»
- «A propos des problèmes de connectivité», à la page 5
- «A propos de Tivoli Federated Identity Manager», à la page 6
- «A propos des correctifs et des mises à jour», à la page 6
- «A propos des messages», à la page 7
- «A propos des problèmes de performances et des blocages», à la page 8
- «A propos des interruptions, pannes et abandons», à la page 9

A propos de l'identification et résolution des problèmes

L'identification et résolution des problèmes est une approche systématique de la résolution d'un problème. L'objectif consiste à déterminer la raison pour laquelle quelque chose n'a pas fonctionné comme prévu et la façon de résoudre l'incident.

La première étape du processus d'identification des incidents consiste à décrire entièrement le problème. Sans cette description, ni vous ni IBM ne pourrez savoir par où commencer à chercher l'origine du problème. Cette étape consiste également à vous poser des questions de base, comme :

- Quels sont les symptômes de l'incident ?
- Quelle est l'origine de l'incident ?
- Quand l'incident a-t-il lieu ?
- Sous quelles conditions l'incident se produit-il ?
- L'incident peut-il être reproduit ?

Les réponses à ces questions permettent généralement d'obtenir une description satisfaisante de l'incident et c'est la meilleure façon de s'attaquer à la résolution du problème.

Quels sont les symptômes de l'incident ?

Lorsque vous commencez à décrire un incident, la question la plus évidente est "Quel est l'incident ?" Cela peut sembler être une question simple, mais vous pouvez la détailler en plusieurs questions plus spécifiques qui créent une description plus approfondie de l'incident. Ces questions peuvent comprendre :

- Qui ou qu'est-ce qui signale l'incident ?
- Quels sont les codes et les messages d'erreur ?
- De quelle façon le système échoue-t-il ? Par exemple, est-ce une boucle, un blocage, une panne, une dégradation des performances ou un résultat incorrect ?
- Quel est l'impact de l'incident sur votre entreprise ?

Quelle est l'origine de l'incident ?

Déterminer la source de l'incident n'est pas toujours tâche facile, mais c'est l'une des étapes les plus importantes de la résolution d'un problème. De nombreuses couches de technologie peuvent exister entre les composants de reporting et d'échec. Les réseaux, disques et pilotes sont quelques-uns des composants que vous devez prendre en compte lorsque vous examinez des incidents. Les questions suivantes peuvent vous permettre d'identifier la source d'un problème afin d'isoler la couche de l'incident :

- L'incident est-il spécifique à une plateforme ou un système d'exploitation ou est-il commun à plusieurs plates-formes et systèmes d'exploitation ?
- L'environnement et la configuration actuels sont-ils pris en charge ?

Souvenez-vous que, même si une couche peut signaler un incident, cela ne signifie pas que la source de l'incident se trouve dans cette couche. L'identification de l'origine de l'incident consiste aussi à comprendre l'environnement dans lequel il se produit. Prenez quelques instants pour décrire complètement l'environnement du problème, notamment le système d'exploitation, sa version, tous les logiciels et leurs versions, ainsi que les informations relatives au matériel. Vérifiez que le produit s'exécute dans une configuration prise en charge. De nombreux incidents peuvent être attribués à des niveaux de logiciels incompatibles, non conçus pour s'exécuter ensemble ou qui n'ont pas été entièrement testés ensemble.

Quand l'incident a-t-il eu lieu ?

Créez un tableau chronologique des événements qui ont abouti à la panne, en particulier pour les cas qui sont des occurrences uniques. Cette opération est plus facile si vous remontez dans le temps : commencez au moment où l'erreur a été signalée (le plus précisément possible, à la milliseconde le cas échéant), puis revenez en arrière via les journaux et les informations disponibles. En règle générale, votre recherche doit aller jusqu'au premier événement suspect que vous trouvez dans un journal de diagnostic. Toutefois, il n'est pas toujours facile d'y parvenir et il faut de la pratique. Savoir à quel moment vous devez cesser de chercher est particulièrement difficile lorsque plusieurs couches de technologie sont concernées et que chacune d'entre elles a ses propres informations de diagnostic.

Pour développer un tableau chronologique détaillé des événements, essayez de répondre aux questions suivantes :

- L'incident se produit-il uniquement à un certain moment du jour ou de la nuit ?
- A quelle fréquence l'incident se produit-il ?
- Quelle séquence d'événements conduit-elle au moment où l'incident est signalé ?
- L'incident se produit-il après une modification d'environnement comme une mise à niveau ou une installation de logiciels ou de matériel ?

En répondant à de telles questions, vous obtenez un système de référence dans lequel vous pourrez rechercher l'incident.

Sous quelles conditions l'incident se produit-il ?

Le fait de savoir quels systèmes et applications sont en cours d'exécution au moment où un incident se produit est une étape importante de l'identification des incidents. Les questions suivantes et d'autres sur votre environnement peuvent vous permettre d'identifier la cause à l'origine de l'incident :

- L'incident se produit-il toujours lorsqu'une tâche identique est effectuée ?

- Une certaine séquence d'événements doit-elle se produire pour que l'incident apparaisse ?
- D'autres applications échouent-elles au même moment ?

L'incident peut-il être reproduit ?

Du point de vue de l'identification des incidents, le problème idéal est un problème qui peut être reproduit. En règle générale, avec des incidents qui peuvent être reproduits, vous disposez d'un ensemble d'outils ou de procédures plus important pour vous aider dans vos recherches. Par conséquent, les incidents que vous pouvez reproduire sont souvent plus faciles à déboguer et résoudre. Cependant, de tels incidents représentent un inconvénient : si le problème a un impact important sur l'entreprise, vous ne souhaitez pas qu'il se reproduise ! Si cela est possible, recréez l'incident dans un environnement de test ou de développement qui vous offre généralement davantage de flexibilité et de contrôle lors de vos recherches.

- Est-il possible de recréer l'incident sur une machine de test ?
- Plusieurs utilisateurs ou applications rencontrent-ils le même type d'incident ?
- L'incident peut-il être recréé en exécutant une seule commande, un groupe de commandes ou une application particulière ou autonome ?

A propos des problèmes de connectivité

Les problèmes de connectivité impliquent généralement plusieurs systèmes, notamment les logiciels, le matériel et les communications. Le meilleur moyen de résoudre des problèmes de connectivité consiste à appliquer un processus de suppression.

Tout d'abord, collectez les données pertinentes pour déterminer ce que vous savez, les données que vous n'avez pas encore recueillies et les possibilités que vous pouvez supprimer. Répondez au minimum aux questions suivantes :

- Les chemins de communication fonctionnent-ils ?
- La connexion initiale a-t-elle réussi ?
- L'incident est-il intermittent ou permanent ?
- Des modifications ont-elles été apportées au réseau de communication, qui pourraient invalider les éléments de répertoire précédents ?
- A quel niveau se situe la panne de communication ? Par exemple, a-t-elle eu lieu entre le client et un serveur ?
- L'incident rencontré se produit-il uniquement dans une application spécifique ?
- Que pouvez-vous déterminer par le contenu du message et les jetons qu'il renvoie ?
- Les autres systèmes peuvent-ils effectuer correctement des tâches semblables ? S'il s'agit d'une tâche à distance, réussit-elle si elle est effectuée en local ?

Enfin, essayez d'isoler l'incident en répondant aux questions répertoriées au Chapitre 3, «Liste d'identification des problèmes de Tivoli Federated Identity Manager», à la page 11.

A propos de Tivoli Federated Identity Manager

La première étape pour résoudre un problème consiste à en savoir plus sur la fonctionnalité concernée du logiciel.

Vous pouvez en savoir plus sur Tivoli Federated Identity Manager à partir des sources suivantes :

- Centre de documentation IBM Tivoli Federated Identity Manager :
http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml
- IBM Tivoli Education pour Tivoli Federated Identity Manager. Consultez le catalogue de formation Tivoli à l'adresse : http://www-306.ibm.com/software/tivoli/education/edu_prd.html
- *Federated Identity Management et Web Services Security avec IBM Tivoli Security Solutions* (SG24-6394-01). Ce manuel est disponible au format PDF à l'adresse <http://www.redbooks.ibm.com/redbooks/pdfs/sg246394.pdf> ou au format HTML à l'adresse <http://www.redbooks.ibm.com/redbooks/SG246394/>

A propos des correctifs et des mises à jour

Si vous rencontrez un problème avec le logiciel IBM Tivoli Federated Identity Manager, vérifiez d'abord la liste des mises à jour conseillées pour confirmer qu'il dispose du dernier niveau de maintenance. Vérifiez ensuite la liste des incidents résolus pour savoir si IBM a déjà publié un correctif permettant de résoudre le problème.

Ces listes se trouvent sur le site Web de support Tivoli pour Tivoli Federated Identity Manager, à l'adresse <http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliFederatedIdentityManager.html>

Des correctifs sont publiés aussi souvent que nécessaire afin de résoudre les défauts identifiés dans IBM Tivoli Federated Identity Manager. De plus, deux types d'ensembles de correctifs cumulatifs, appelés groupes de correctifs et groupes de mises à jour, sont publiés périodiquement pour le produit IBM Tivoli Federated Identity Manager afin de fournir aux utilisateurs le dernier niveau de maintenance. Vous devez installer ces groupes de mises à jour dès que possible pour empêcher l'apparition de problèmes.

Pour recevoir une notification hebdomadaire des correctifs et des mises à jour, abonnez-vous aux mises à jour par e-mail de My Support. Pour plus d'informations, voir «Réception des notifications de correctifs», à la page 39.

Le tableau ci-dessous décrit les caractéristiques des différents types de maintenance.

Tableau 1. Types de maintenance

Nom	Caractéristiques
Correctif	<ul style="list-style-type: none"> • Un correctif unique publié entre deux mises à jour pour résoudre un problème spécifique. • Une fois que vous avez installé le correctif, testez toutes les fonctions sur lesquelles le composant corrigé a un impact.
Groupe de correctifs	<ul style="list-style-type: none"> • Un groupe de correctifs cumulatifs qui contient tous les correctifs publiés depuis le groupe de correctifs ou de mises à jour précédent. Un groupe de correctifs peut également comprendre de nouveaux correctifs. • Les groupes de correctifs augmentent le niveau de modification du produit et sont nommés en conséquence, par exemple, 5.0.1 • Un groupe de correctifs peut mettre à jour des composants spécifiques ou l'intégralité de l'image du produit. • Lors de l'installation du groupe de correctifs, tous les correctifs préalablement appliqués sont automatiquement désinstallés. • Une fois que vous avez installé un groupe de correctifs, vous devez effectuer un test de régression de toutes les fonctions critiques. • Les deux derniers groupes de correctifs sont disponibles en téléchargement (par exemple, 5.0.2 et 5.0.1). Les groupes de correctifs antérieurs ne sont pas disponibles.
Groupe de mises à jour	<ul style="list-style-type: none"> • Un groupe de correctifs cumulatifs qui contient tous les correctifs publiés depuis le groupe de correctifs ou de mises à jour précédent ainsi que les nouveaux correctifs. • Outre les correctifs, un groupe de mises à jour contient généralement une nouvelle fonction et il met à jour l'intégralité de l'image du produit. • Les groupes de mises à jour augmentent le niveau de modification du produit et sont nommés en conséquence, par exemple, 5.0.1. • Lors de l'installation du groupe de mises à jour, tous les correctifs préalablement appliqués sont automatiquement désinstallés. • Une fois que vous avez installé un groupe de mises à jour, vous devez effectuer un test de régression de toutes les fonctions critiques.

A propos des messages

Lorsqu'IBM Tivoli Federated Identity Manager affiche un message, vous pouvez souvent résoudre le problème en prenant connaissance de l'intégralité du texte du message et des actions de reprise qui lui sont associées.

Vous trouverez le texte complet des messages, leurs explications et les actions de reprise recommandées en recherchant l'identificateur de message dans *IBM Tivoli Federated Identity Manager Error Message Reference*.

A propos des problèmes de performances et des blocages

Les problèmes de performances surviennent dans de nombreuses situations. Un blocage est un type de problème de performance où les utilisateurs attendent une réponse sur une période de temps indéfinie. Les techniques de résolution des problèmes de blocage s'apparentent aux techniques que vous utiliseriez pour les autres problèmes de performances.

Vous trouverez ci-dessous quelques exemples de situations dans lesquels les problèmes de performances sont évidents :

- L'exécution des requêtes est plus lente que prévu.
- La charge de travail ou un travail par lots ne se termine pas aussi vite que prévu, ou le taux de transaction ou le rendement diminue.
- Le système dans son ensemble ralentit.
- Un goulot d'étranglement est suspecté au niveau de l'une des ressources système comme l'unité centrale, les entrées-sorties ou la mémoire.
- Le traitement des requêtes ou des autres charges de travail consomme plus de ressources que prévu ou disponible.
- Un système fonctionne mieux qu'un autre.
- Une requête, une application ou un système se bloque.

Les blocages peuvent être particulièrement difficiles à résoudre car leurs symptômes semblent souvent correspondre aux symptômes d'autres problèmes. Par exemple, si un utilisateur attend longtemps une réponse à une requête, il peut penser que le système est bloqué. Souvent, la requête peut être très complexe et le système peut également être très utilisé à ce moment-là. Par conséquent, le système n'est pas réellement bloqué, mais il est tout simplement très lent à répondre. De plus, lors d'un arrêt grave du système, une intensification importante de l'activité peut entraîner le blocage de la plupart ou de toutes les commandes.

Outre l'interprétation correcte du problème en termes de nature des symptômes (lenteur, utilisation excessive des ressources, etc.) et de leur origine (dans une requête, une application, une ressource système, etc.), vous avez besoin de plusieurs autres informations pour mettre le problème en contexte.

Répondez aux questions suivantes pour déterminer rapidement le meilleur point de départ pour commencer à rechercher la cause du problème de performances :

1. Quand le problème s'est-il produit la première fois ?

S'il se produit depuis quelques temps, vous pouvez utiliser les données de l'historique pour trouver les différences. Ainsi, vous pouvez vous concentrer sur les modifications apportées au comportement du système et leurs raisons. Vous devez également vous demander si des modifications récentes ont été effectuées comme des mises à niveau matérielles ou logicielles, une nouvelle implémentation d'application, un ajout d'utilisateurs et ainsi de suite.

2. Le problème de performances est-il permanent ou intermittent ?

Si les performances médiocres sont permanentes, vérifiez si le système a commencé à gérer une charge de travail supérieure ou si une ressource de base de données partagée est devenue un goulot d'étranglement. D'autres causes éventuelles de dégradation des performances comprennent l'augmentation de l'activité utilisateur, plusieurs applications importantes ou la suppression de périphériques matériels. Si les performances sont médiocres uniquement sur de courtes périodes, commencez par rechercher les applications ou utilitaires courants qui s'exécutent à ce moment-là. Si les utilisateurs signalent qu'un

groupe d'applications rencontre des problèmes de performances, vous pouvez commencer votre analyse en visant ces applications.

3. Le problème semble-t-il concerner l'ensemble du système ou est-il limité à Tivoli Federated Identity Manager ou ses composants ?

Les problèmes de performances qui affectent l'ensemble du système suggèrent un problème extérieur à Tivoli Federated Identity Manager. Un incident a pu se produire au niveau du système d'exploitation et doit être résolu.

4. Si le problème est isolé sur un composant, une activité particulière semble-t-elle être à l'origine du problème ?

Si un composant semble provoquer le problème, vous pouvez évaluer si les utilisateurs qui signalent cette activité particulière rencontrent un ralentissement. Vous pouvez isoler l'incident sur un composant et une activité spécifique.

5. Remarquez-vous des caractéristiques communes entre les différentes performances médiocres ou les problèmes semblent-ils aléatoires ?

Vous devez déterminer si des fonctions communes sont impliquées. Si tel est le cas, ces fonctions sont peut-être un point de conflit.

A propos des interruptions, pannes et abandons

Les termes *interruption*, *panne* et fin anormale (*abandon*) sont souvent utilisés pour indiquer la même chose.

Si Tivoli Federated Identity Manager ne peut pas continuer le traitement suite à une interruption, une violation de segmentation ou une exception, il génère une erreur.

La plupart des interruptions, pannes et abandons pour Tivoli Federated Identity Manager génèrent une exception, qui est peut être incluse dans le journal des messages et n'exige pas que la trace soit activée pour être signalés. Ces erreurs peuvent toutefois être enregistrées dans un journal de trace si le personnel du service de support IBM vous demande d'activer la journalisation de trace. Si vous ouvrez un rapport d'incident auprès d'IBM, vous serez peut-être invité à fournir le journal de trace à des fins d'analyse.

Bien que Tivoli Federated Identity Manager puisse générer des journaux de trace à la demande, vous ne devez générer des fichiers de trace que si le support logiciel IBM vous le demande. Pour plus d'informations, voir «Journaux de trace», à la page 45.

Chapitre 3. Liste d'identification des problèmes de Tivoli Federated Identity Manager

Les questions suivantes vous permettent d'identifier la source d'un problème se produisant dans un environnement Tivoli Federated Identity Manager.

1. Vos correctifs et groupes de correctifs sont-ils à jour ?
Pour plus de détails, voir «Obtention de correctifs», à la page 39.
2. L'incident est-il répertorié dans la section *Tivoli Federated Identity Manager Release Information* ?
Consultez les informations sur l'édition dans le centre de documentation de Tivoli Federated Identity Manager : <http://publib.boulder.ibm.com/infocenter/tiv2help/index.jsp>
3. La base de connaissances d'IBM contient-elle des informations complémentaires sur l'incident en question ?
Pour plus d'informations, voir Chapitre 6, «Recherche dans les bases de connaissances», à la page 41.
4. Des messages d'erreur s'affichent-ils ?
Voir *IBM Tivoli Federated Identity Manager Error Message Reference* pour obtenir des informations sur les messages d'erreur.
5. Les journaux contiennent-ils des messages sur l'incident en question ?
Pour plus d'informations, voir «Journaux de messages», à la page 44 et «Journaux de trace», à la page 45.
6. L'incident se produit-il lors de l'installation ou de la désinstallation de l'une des fonctionnalités suivantes ?
 - Tivoli Federated Identity Manager ou composants associés
Voir *IBM Tivoli Federated Identity Manager - Guide d'installation*.
 - Common Auditing and Reporting Service
Voir *IBM Tivoli Federated Identity Manager - Guide d'audit*.
 - Tivoli Access Manager for e-business
Voir *IBM Tivoli Access Manager for e-business Problem Determination Guide*.
 - WebSphere Application Server
Consultez les rubriques d'identification et de résolution des problèmes liés à l'installation dans le centre de documentation d'IBM WebSphere Application Server à l'adresse <http://www.ibm.com/software/webservers/appserv/was/library/>.
7. L'incident se produit-il lorsque vous configurez Tivoli Federated Identity Manager ?
Voir «Problèmes de configuration de Tivoli Federated Identity Manager», à la page 16.
8. L'incident se produit-il lorsque vous essayez d'exécuter la console d'administration ?
Voir «Problèmes associés à Integrated Solutions Console», à la page 25, et «Problèmes associés à la console WebSphere Application Server», à la page 27.
9. L'incident implique-t-il un échec de déploiement ?
Voir «Erreur lors de l'opération de déploiement», à la page 34.

10. Si vous n'êtes pas parvenu à résoudre l'incident lors des étapes précédentes, vous devrez essayer d'obtenir des informations supplémentaires sur son origine ou les conditions sous lesquelles il s'est produit :

- L'incident s'est-il produit lors du traitement d'exécution ?
 - La connexion a-t-elle échoué ?
 - Un incident s'est-il produit ?
 - Un problème de performances comme un ralentissement de la réponse ou un "blocage" s'est-il produit ?
 - Une fin anormale, une interruption ou une exception Java™ s'est-elle produite ?
- L'incident a-t-il eu lieu lors de la configuration d'une fonction spécifique ?
- L'incident a-t-il lieu lorsque vous effectuez une tâche spécifique ?

Les réponses à ces questions peuvent vous aider à déterminer l'origine de l'incident et à rechercher des informations supplémentaires. Par exemple, si l'incident se produit lors de la configuration d'une fonction ou des performances spécifiques d'une tâche particulière, vous pouvez trouver une solution dans la documentation de ladite fonction ou tâche.

Si la liste ne vous guide pas dans la résolution du problème, vous pouvez recueillir d'autres données de diagnostic. Ces autres données peuvent s'avérer utiles pour le personnel du service de support IBM qui doit vous aider à poursuivre l'identification et la résolution du problème. Voir Chapitre 7, «Collecte de données», à la page 43.

Chapitre 4. Problèmes connus et solutions

Les problèmes connus et leurs solutions sont décrits dans les sections suivantes.

Problèmes d'installation

Cette rubrique décrit les problèmes liés à l'installation de Tivoli Federated Identity Manager.

Echec de l'installation de Federated Identity Manager sous Solaris

Dans de rares cas, le démon de gestion de volume Solaris (vold) peut empêcher l'installation de Tivoli Federated Identity Manager. Après avoir demandé les paramètres d'installation, le programme d'installation ne trouve pas la machine Java virtuelle appropriée.

Remarque : Ce problème ne se produit pas lors de l'installation de l'image ISO Tivoli Federated Identity Manager à l'aide d'un périphérique de bouclage.

Pour résoudre ce problème, redémarrez le démon de gestion de volume (vold) ou installez le CD-ROM manuellement.

Pour arrêter et redémarrer le démon vold :

1. Arrêtez le démon vold à l'aide de la commande suivante :
`/etc/init.d/volmgt stop`
2. Démarrez-le à l'aide de la commande suivante :
`/etc/init.d/volmgt start`
3. Exécutez l'installation de Tivoli Federated Identity Manager.

Pour installer manuellement le CD-ROM :

1. Arrêtez le démon vold à l'aide de la commande suivante :
`/etc/init.d/volmgt stop`
2. Recherchez le périphérique de CD-ROM à l'aide de la commande suivante :
`ls -la /dev/sr0`
Cette commande renvoie le périphérique `c##d#s2` pour le CD-ROM.
3. Installez le périphérique à l'aide de la commande suivante :
`mount -F hsfs /dev/c##d#s2 point_installation`
4. Exécutez l'installation de Tivoli Federated Identity Manager.
5. Désinstallez le périphérique après avoir installé Tivoli Federated Identity Manager et redémarrez le démon vold à l'aide des commandes suivantes :
`umount point_installation`
`/etc/init.d/volmgt start`

Les commandes de l'interface de ligne de commande Federated Identity Manager ne fonctionnent pas immédiatement après l'installation du produit

L'interface de ligne de commande (CLI) Tivoli Federated Identity Manager ne fonctionne pas immédiatement après l'installation du produit car le programme d'installation n'arrête ni ne redémarre WebSphere Application Server. Vous devez arrêter et redémarrer manuellement WebSphere Application Server avant de commencer à utiliser les commandes de l'interface de ligne de commande Tivoli Federated Identity Manager.

Problèmes de désinstallation

Cette rubrique décrit les problèmes liés à la désinstallation de Tivoli Federated Identity Manager.

Les fichiers JAR de la version imbriquée de WebSphere Application Server sont supprimés après un redémarrage système

Sur les plateformes Windows uniquement, si vous installez Tivoli Federated Identity Manager et que vous le désinstallez et le réinstallez ensuite, le redémarrage du système entraîne la suppression des fichiers JAR de la version imbriquée de WebSphere Application Server dans le répertoire `ewas\java\jre\lib` et de tous les autres fichiers non supprimés au cours du processus de désinstallation après le redémarrage du système.

Remarque : Cela se produit uniquement dans les conditions suivantes :

- Tivoli Federated Identity Manager est installé au même emplacement que les fichiers verrouillés ;
- ET-
- l'emplacement du répertoire est marqué pour suppression.

Ces fichiers JAR doivent être supprimés au cours de la désinstallation, mais ils ne l'ont pas été car un processus les a verrouillés. Ils sont donc marqués en vue d'une suppression ultérieure par le système d'exploitation ; celle-ci a lieu lors du redémarrage d'un système.

Vous devez redémarrer le système une fois la désinstallation de Tivoli Federated Identity Manager terminée.

Echec de la désinstallation de Federated Identity Manager sous AIX

Sous AIX, si un échec se produit au cours de l'installation de Federated Identity Manager, l'exécutable du programme de désinstallation n'est pas toujours placé dans le répertoire Federated Identity Manager. Si cet exécutable n'est pas installé au cours de l'installation du produit, suivez la procédure décrite dans cette section pour désinstaller manuellement Federated Identity Manager sous AIX. Après l'installation du produit, la liste de l'ensemble de fichiers AIX contient l'entrée suivante :

```
FIM620 6.2.0.0 C P ISMP installed entry (/opt/IBM/FIM)
```

Remarque : La désinstallation du produit peut échouer également si vous n'employez pas le même utilitaire pour installer et désinstaller Federated Identity Manager. Par exemple, si vous installez le produit par le biais d'ISMP et tentez ensuite de le désinstaller à l'aide de `smitty` ou `installp`, l'erreur suivante peut se produire :

```
A lexical error occurred for 0e0febbe7616f2ea257999d5d7f41e9b 0.0.0.0
```

Pour supprimer les entrées Federated Identity Manager de l'ensemble de fichiers AIX, vous devez utiliser les commandes qui administrent la base de données Object Data Manager (ODM). ODM est le registre logiciel AIX utilisé pour suivre les installations logicielles. Les étapes à suivre pour supprimer les entrées Federated Identity Manager d'ODM sont décrites ci-dessous. Elles doivent être exécutées par un administrateur AIX. Pour obtenir de l'aide sur la suppression des entrées ODM, contactez le service de support logiciel IBM.

1. Déterminez quelles entrées lexicales de l'installation ISMP sont conservées dans ODM à l'aide de la commande `lslpp`, par exemple :

```
lslpp -l > /tmp/out.txt
```

2. Recherchez dans la sortie les entrées similaires aux chaînes alphanumériques comportant 32 caractères suivants (valeurs lexicales). Exemples de valeurs lexicales :

```
11317ad90fc7a29df5c0bb762f59634e
                                0.0.0.0 COMMITTED ISMP installed entry
1188c43b206f32f0aefda112c87f1ea1
                                0.0.0.0 COMMITTED ISMP installed entry
1db8e322a4c716d975d865f055754736
                                0.0.0.0 COMMITTED For the Configuration
...
1e2bb97d8e16691143874a5410a42701
                                0.0.0.0 COMMITTED ISMP installed entry
27a07408c198e30e990f03da160c11f4
                                0.0.0.0 COMMITTED ISMP installed entry
2c1e1f7d0a0bd2da6975d31d9fc5e446
                                0.0.0.0 COMMITTED ISMP installed entry
335d2c0fd3c337c1b360a5e67df1a4ff
                                0.0.0.0 COMMITTED ISMP installed entry
3362ee349a200978dc4e1d262a00a304
                                0.0.0.0 COMMITTED ISMP installed entry
35e0d7afda41130690897b3e3e26fe1c
                                0.0.0.0 COMMITTED ISMP installed entry
36acdf900b4761a4571c2ba54e78281
                                0.0.0.0 COMMITTED ISMP installed entry
36defc93f537a680a64504555c8a3ab7
                                0.0.0.0 COMMITTED ISMP installed entry
```

3. Sauvegardez le répertoire `/usr` ODM, par exemple :

```
#cd /
#tar -cvf /tmp/odm.tar ./usr/lib/objrepos ./etc/objrepos
```

4. Supprimez les entrées du sous-répertoire `/usr` d'ODM, comme suit, à l'aide des commandes `odmget` et `odmdelete`. Lors de la spécification de la commande `odmget`, notez la valeur `lpp_id#` qui est renvoyée car vous devrez la spécifier pour les paramètres d'inventaire et d'historique dans la commande `odmdelete`. Dans certains cas, aucun objet (0) n'est supprimé, ce qui est correct car les entrées ISMP peuvent ne pas faire partie d'ODM.

```
#export ODMDIR=/usr/lib/objrepos
#odmget -q name=val_lex_32_chiffres lpp
#odmdelete -q name=val_lex_32_chiffres -o lpp
#odmdelete -q lpp_name=val_lex_32_chiffres -o product
#odmdelete -q lpp_id=# -o inventory
#odmdelete -q lpp_id=# -o history
```

- Supprimez les entrées du sous-répertoire /etc d'ODM, comme suit, à l'aide des commandes `odmget` et `odmdelete`. Lors de la spécification de la commande `odmget`, notez la valeur `lpp_id#` qui est renvoyée car vous devrez la spécifier pour les paramètres d'inventaire et d'historique dans la commande `odmdelete`.

```
#export ODMDIR=/etc/objrepos
#odmget -q name=val_lex_32_chiffres lpp
#odmdelete -q name=val_lex_32_chiffres -o lpp
#odmdelete -q lpp_name=val_lex_32_chiffres -o product
#odmdelete -q lpp_id=# -o inventory
#odmdelete -q lpp_id=# -o history
```

- Exécutez à nouveau la commande `ls|lpp`. Plus aucune entrée ISMP ne doit apparaître dans la sortie `ls|lpp`. S'il en reste encore, vérifiez que vous avez exécuté correctement toutes les opérations `odmget` et `odmdelete`. Vous devez exécuter ces commandes pour *chaque* entrée à supprimer.

Problèmes de configuration de Tivoli Federated Identity Manager

Les problèmes ci-dessous et leurs solutions concernent la configuration de Tivoli Federated Identity Manager.

Ne pas ajouter de fichiers ni de sous-répertoires à la bibliothèque partagée ITFIM_WSSM

N'ajoutez pas de fichiers ni de sous-répertoires au répertoire ITFIM_WSSM. Les fichiers et sous-répertoires apparaîtraient alors dans le chemin d'accès aux classes, ce qui peut avoir des effets indésirables. La bibliothèque partagée ITFIM_WSSM affecte le chemin d'accès aux classes de toutes les applications qui s'exécutent sur le serveur. Le chemin d'accès aux classes de la bibliothèque partagée inclut le répertoire d'installation ITFIM_WSSM.

Des paramètres de propriété SSL du service d'audit remplacent d'autres paramètres de propriété SSL

Les propriétés SSL utilisées pour une connexion HTTPS sortante à partir d'un serveur d'applications vers un serveur Common Auditing and Reporting Service peuvent remplacer les propriétés SSL dans des requêtes HTTPS sortantes à partir d'autres applications déployées sur le même serveur WebSphere Application Server.

Si le client Common Auditing and Reporting Service WebSphere définit les propriétés système du fichier de clés sécurisées, ces paramètres remplacent les autres clients SSL qui s'exécutent sur la machine Java virtuelle s'ils requièrent l'utilisation des mêmes paramètres de propriétés système. Par exemple, si Tivoli Federated Identity Manager est configuré pour utiliser une connexion HTTPS à un serveur Common Auditing and Reporting Service, le fichier de clés sécurisées spécifié pour cette connexion sera utilisé sur toutes les connexions HTTPS sortantes à partir de ce serveur WebSphere Application Server. Les requêtes HTTPS sortantes ultérieures peuvent alors échouer et renvoyer l'exception suivante :

```
javax.net.ssl.SSLHandshakeException: Received fatal alert: certificate_unknown
```

Pour corriger ce problème dans WebSphere Application Server Version 6.0.2, ajoutez le certificat de CA pour d'autres requêtes HTTPS sortantes à partir du serveur d'applications vers le fichier de clés sécurisées utilisé pour la connexion HTTPS au serveur Common Auditing and Reporting Service. Par exemple, si une application de service Web qui s'exécute sur un serveur d'applications configuré

pour établir une connexion sortante à un service sécurisé Tivoli Federated Identity Manager par le biais de HTTPS, ajoutez le certificat de CA pour cette connexion HTTPS au fichier de clés sécurisées utilisé pour la connexion au serveur Common Auditing and Reporting Service.

Pour corriger ce problème dans WebSphere Application Server 6.1, définissez les configurations SSL de noeud final sortant dynamique. A partir de la console d'administration WebSphere, cliquez sur **Sécurité -> Certificat SSL et gestion des clés -> Configurations SSL du noeud final de communication sortante dynamique**. Cette fenêtre permet de définir une connexion sortante basée sur le nom d'hôte cible, le port et le protocole et indique la configuration SSL à utiliser. Vous pouvez définir des propriétés SSL uniques pour les connexions sortantes établies au serveur Common Auditing and Reporting Service et aux autres systèmes cible des requêtes SSL sortantes.

N'utilisez pas de caractère en langue nationale dans les noms de fédération

Tivoli Federated Identity Manager risque de ne pas fonctionner correctement lorsque des caractères en langue nationale sont inclus dans le nom d'une fédération. L'utilisation de caractères en langue nationale dans les noms de fédération n'est pas autorisée. Les noms de fédération sont inclus dans des adresses URL et des serveurs Web différents, et les navigateurs prennent en charge des conventions d'attribution de nom pour la conversion des caractères en langue nationale en composants URL.

Seuls les caractères suivants peuvent être utilisés dans les noms de fédération :

- Caractères alphabétiques : A-Z, a-z
(Utilisez des caractères alphanumériques US-ASCII.)
- Chiffres : 0-9

Limitations du mappage d'alias

Un alias est créé lorsque vous fédérez le compte d'un fournisseur de services avec un compte associé sur un fournisseur d'identité. A la fin de l'action de fédération, le service d'alias sur le fournisseur d'identité inclut un attribut secSelfAlias (valeur de l'alias utilisateur attribuée à un partenaire) et comporte un attribut secPartnerAlias (valeur de l'alias utilisateur reçu d'un partenaire).

Un seul compte d'un fournisseur de services peut être fédéré avec un compte d'un fournisseur d'identité. Plusieurs comptes sur différents fournisseurs de services peuvent être fédérés avec le même compte sur le fournisseur d'identité. L'attribut secSelfAlias généré pour un partenaire contient la valeur ProviderId du partenaire (fournisseur de services) à laquelle il est associé. Le reste de la valeur de l'attribut secSelfAlias est l'alias généré de manière aléatoire. Ainsi, si plusieurs alias sont affectés au même ProviderId, il n'existe aucun mécanisme pour déterminer l'alias à fournir dans une assertion générée pour être consommée par ce partenaire.

Par exemple, l'utilisateur John Smith possède les comptes jsmith et jsmith1 sur le fournisseur de services 1, johns sur le fournisseur de services 2 et JohnSmith sur le fournisseur d'identité. Les comptes jsmith et johns peuvent être fédérés avec le compte JohnSmith, mais seul jsmith ou jsmith1 peut être fédéré avec le compte JohnSmith. Cependant, le principal spécifié dans l'assertion générée par le fournisseur d'identité est indéterminé car plusieurs comptes du même fournisseur de services sont fédérés avec le même compte du fournisseur d'identité.

Vous pouvez mettre à jour les valeurs d'alias en effectuant une mise à jour de l'attribut NameID. La mise à jour modifie l'attribut secSelfAlias du fournisseur d'identité et l'attribut secPartnerAlias du fournisseur de services. Vous pouvez lancer cette action sur le fournisseur d'identité ou le fournisseur de services.

Solutions en cas de présence d'espaces dans le chemin d'accès au fichier de clés SPNEGO

Si WebSphere Application Server est installé dans un répertoire dont le nom contient un espace, comme le répertoire d'installation par défaut sur une plateforme Windows, l'authentification SPNEGO ne peut pas être configurée correctement. Ce problème concerne la version imbriquée et la version autonome de WebSphere Application Server.

Ce problème peut être corrigé de deux manières, comme indiqué ci-dessous.

Si l'authentification SPNEGO est déjà configurée dans la console de gestion Tivoli Federated Identity Manager :

Après avoir configuré l'authentification SPNEGO à l'aide de la console de gestion Tivoli Federated Identity Manager, mettez à jour le fichier krb5.ini pour modifier le chemin d'accès au fichier de clés Kerberos à un format qui ne contient pas d'espace (par exemple, le format Windows 8.3). Le chemin d'accès au fichier krb5.ini peut être décrit comme suit :

```
WAS_HOME/profiles/WAS_PROFILE/config/itfim/ FIM_DOMAIN/etc/  
krb5.ini
```

Le fichier krb5.ini contient une ligne similaire à celle-ci :

```
nom_fichier_de_clés_par_défaut = C:/Program Files/ IBM/WebSphere/  
AppServer/profiles/AppSrv01/config/itfim/default/etc/krb5.keytab
```

Il suffit généralement de remplacer "Program Files" par "Progra~1", par exemple :

```
nom_fichier_de_clés_par_défaut = C:/Progra~1/ IBM/WebSphere/  
AppServer/profiles/AppSrv01/config/itfim/default/etc/krb5.keytab
```

Après avoir effectué cette mise à jour, redémarrez WebSphere Application Server. Vous devez réappliquer cette modification à chaque fois que vous modifiez les paramètres de configuration du fournisseur d'identité dans la console de gestion Tivoli Federated Identity Manager.

Si l'authentification SPNEGO n'est PAS déjà configurée dans la console de gestion Tivoli Federated Identity Manager :

Indiquez le chemin formaté 8.3 du fichier krb5.ini.template *avant* de configurer l'authentification SPNEGO dans la console de gestion Tivoli Federated Identity Manager. Le chemin peut varier en fonction du répertoire d'installation de WebSphere Application Server.

Le répertoire suivant contient le fichier krb5.ini.template :

```
racine_install_FIM/etc/krb5.ini.template
```

Remplacez la ligne suivante dans le fichier krb5.ini.template :

```
nom_fichier_de_clés_par_défaut = @KEYTAB@
```

par le nom de fichier qualifié complet 8.3, par exemple :

```
nom_fichier_de_clés_par_défaut = C:/Progra~1/ IBM/WebSphere/  
AppServer/profiles/AppSrv01/config/itfim/default/etc/krb5.keytab
```

Le nom de fichier est ainsi préservé à chaque fois que vous configurez les paramètres de configuration du fournisseur d'identité dans la console de gestion Tivoli Federated Identity Manager.

Mise à jour des droits d'accès pour l'enregistrement de fichiers journaux dans le répertoire log

Cette rubrique s'adresse uniquement aux clients qui utilisent le plug-in Tivoli Federated Identity Manager for IIS sur les systèmes Windows.

Dans des environnements locaux autres que l'anglais, des fichiers journaux ne peuvent pas être ajoutés au répertoire *rép_install_FIM\fimpi\log*.

En utilisant la commande *cacls.exe* et le nom de l'environnement local spécifique pour le groupe "NETWORK SERVICE", accordez les droits d'accès appropriés afin que le fichier journal puisse être enregistré dans le répertoire *rép_install_FIM\fimpi\log*.

Utilisez la commande suivante :

```
cacls.exe rép_install_FIM\fimpi\log /t /e /g nom_du_groupe_de_service_réseau:F
```

où *nom_du_groupe_de_service_réseau* correspond au nom traduit du groupe NETWORK SERVICE de votre environnement local.

La sécurité Java 2 ne peut pas être activée sur un système Tivoli Federated Identity Manager

La sécurité Java 2 ne peut pas être activée sur un système Tivoli Federated Identity Manager. Le produit Tivoli Federated Identity Manager ne fonctionnera pas et cette configuration n'est pas prise en charge.

Quelques symptômes :

- Erreur indiquant que la console ne peut pas communiquer avec le service de gestion.
FBTC0N257E Une erreur s'est produite lors de l'accès au service de gestion. Pour plus d'informations, consultez les fichiers journaux du serveur.
- Erreurs dans les journaux signalant un problème de droits d'accès au démarrage.

Pile de trace :

```
ava.security.AccessControlException:  
Access denied (java.util.PropertyPermission * read,write)  
at java.security.AccessController.checkPermission(AccessController.java:108)
```

- Exceptions d'exécution de la console :

```
javax.management.RuntimeOperationsException:  
The "name" parameter cannot be null. at  
com.ibm.ws.management.AdminClientImpl.assertObjectNameValid(AdminClientImpl.java:287)
```

Remarque :

- L'objectif principal de la sécurité Java 2 est de protéger le conteneur WebSphere Application Server contre les codes Java non sécurisés. Le client considérant IBM comme étant sécurisé, il n'y a aucune raison d'un point de vue technique d'activer la sécurité.
- L'utilisation de cette fonction a un impact important sur les performances. Déterminez si le niveau de risque auquel est exposé le code justifie cette opération.

Utilisation des éléments et ServiceName et PortType pour sélectionner une chaîne de modules STC spécifiques

Selon les valeurs utilisées par les éléments ServiceName et PortType, il existe des risques de non concordance avec l'erreur suivante dans la trace :

```
FBTSTM015E Aucune variable XPath configurée n'a sélectionné un noeud à partir de la requête, ou bien les données TokenType ou AppliesTo
```

De plus, différentes requêtes peuvent être mappées vers la même chaîne si le caractère "*" est utilisé de manière générique dans les deux zones.

Il est nécessaire que la partie située à gauche du signe deux-points dans l'élément Service Name et Port Type :

- corresponde au NSURI de l'espace de nom WS-Addressing utilisé pour les éléments PortType et ServiceName dans la demande ;
- et que la partie située à droite corresponde à la valeur.

Appel des classes Java à partir de XSLT dans ITFIM 6.2

ITFIM 6.2 a été développé à l'aide du modèle d'infrastructure OSGI. ITFIM 6.2 a modifié le mode de recherche des autres classes par chaque module. L'appel Java à partir de XSLT repose sur des détails d'implémentation qui échappent au contrôle d'ITFIM. Cette contrainte est une limitation et elle n'est pas officiellement prise en charge. La méthode d'utilisation des classes Java personnalisées correcte et prise en charge consiste à développer un module personnalisé. Ce dernier est utilisé en mode mappage dans une chaîne STS.

Paramètres de configuration DirectoryIntegratorSTSModule

Cette rubrique fournit des informations sur la configuration des paramètres suivants :

- Taille du pool de gestionnaires de chaîne d'assemblage
- Nombre d'unités d'exécution en attente
- Durée d'attente des unités d'exécution avant qu'un gestionnaire de chaîne d'assemblage devienne disponible

Les gestionnaires de chaîne d'assemblage Tivoli Directory Integrator sont synchrones et n'autorisent pas les unités d'exécution multiples. C'est en raison de cette limitation qu'un pool de gestionnaires de chaîne d'assemblage est créé. Cette rubrique fournit plus de détails sur la configuration WebSEAL et WebSphere Application Server.

Définissez la taille du pool en fonction du nombre prévu de clients simultanés attendus pour le système. La spécification d'une valeur élevée ne change rien si la ligne d'assemblage effectue des appels bloquants.

De même, la spécification d'une taille de pool supérieure au nombre maximal d'unités d'exécution dans WebSphere ou WebSEAL ne présente aucun bénéfice. Le nombre d'unités d'exécution en attente indique combien d'unités d'exécution seront bloquées dans Tivoli Federated Identity Manager en attendant qu'un gestionnaire de chaîne d'assemblage devienne disponible pour appeler Tivoli Directory Integrator. Si la valeur zéro est indiquée, les unités d'exécution n'entraînent pas de blocage si un gestionnaire de chaîne d'assemblage n'est pas disponible immédiatement et une erreur est renvoyée. Si une valeur inférieure à zéro est

indiquée, les unités d'exécution entraînent un blocage d'une durée illimitée. Si une valeur supérieure à zéro est indiquée, elles entraînent un blocage d'une durée correspondant au nombre de secondes indiqué. Evitez d'affecter une valeur négative à l'unité d'exécution en attente pour ne pas générer d'autres problèmes comme le blocage de toutes les unités d'exécution dans WebSEAL.

Erreur lors de l'utilisation de l'option Tester la connexion pour le service ITFIM

Lorsque vous utilisez ITFIM 6.2 sous Linux®, un problème peut survenir lors de la création d'un domaine. Après avoir installé Tivoli Federated Identity Manager 6.2 et sélectionné l'option Tester la connexion, l'erreur suivante peut se produire :

```
FBTCON313E Une erreur s'est produite lors de l'appel du service de gestion ITFIM. Il se peut que le service de gestion soit indisponible.
```

Cette erreur peut être due à de multiples itérations d'installation et de désinstallation dans l'environnement.

Pour résoudre le problème, désinstallez manuellement ITFIM de l'environnement. Toutes les commandes suivantes s'exécutent à partir de l'invite de commande wsadmin.

Pour désinstaller manuellement ITFIM de l'environnement :

1. Vérifiez que WebSphere Application Server est démarré avant de lancer wsadmin.
2. Lancez wsadmin à l'aide de la commande suivante :

```
 /<RACINE_INSTALL_WAS>/profiles/<nom_serveur>/bin/wsadmin.sh -user  
<utilisateur> -password <mot_de_passe>
```

par exemple : /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/
wsadmin.sh -user wasadmin -password passw0rd
3. Affichez la liste des applications installées dans WebSphere Application Server à l'aide de la commande suivante :

```
wsadmin>$AdminApp list
```

Remarque : La console Tivoli Federated Identity Manager n'apparaît pas dans cette liste car elle est installée en tant qu'application système dans WebSphere.

4. Désinstallez une application.
 - Pour désinstaller une application (comme ITFIMManagementService et ITFIMRuntime) de la version autonome de WebSphere Application Server, lancez les commandes dans l'ordre suivant :

```
wsadmin>$AdminApp uninstall <nom_application>
```

```
wsadmin>$AdminConfig save
```

Le <nom_application> peut être déterminé à l'aide de la commande \$AdminApp list.
 - Pour désinstaller une application d'un cluster WebSphere Application Server, exécutez la même commande mais à partir de l'invite wsadmin du gestionnaire de déploiement.
5. Il est nécessaire de synchroniser les noeuds d'un cluster afin de propager les modifications de configuration aux noeuds concernés. Par défaut, cette situation se produit périodiquement tant que le noeud peut communiquer avec le

gestionnaire de déploiement. Vous pouvez propager les modifications de manière explicite à partir de l'invite wsadmin du gestionnaire de déploiement à l'aide de la commande suivante :

```
wsadmin>set Sync1 [$AdminControl completeObjectName  
type=NodeSync,node=myNodeName,*] wsadmin>$AdminControl invoke $Sync1  
sync
```

6. Désinstallez fimconsole de WebSphere Application Server à l'aide de la commande suivante :

```
wsadmin>$AdminApp update isclite modulefile {-operation delete  
-contenturi itfim-fimconsole-e.war} wsadmin>$AdminConfig save
```

7. Après avoir supprimé ITFIMManagementService, ITFIMRuntime et Fimconsole de WebSphere à l'aide des commandes wsadmin, supprimez les répertoires suivants de votre système de fichiers :

```
/opt/IBM/FIM /opt/IBM/WebSphere/AppServer/systemApps/isclite.ear/itfim-  
fimconsole-*.war
```

Exception dans SystemOut.log lors du démarrage du serveur ITFIM

Lors du démarrage d'un noeud sur lequel le module d'exécution ITFIM est déployé, l'opération peut échouer et renvoyer l'exception suivante :

```
com.tivoli.am.fim.rte.config.impl.RuntimeConfigurationImpl setThreadSubject  
java.lang.NullPointerException
```

L'exception de trace de pile complète dans le fichier SystemOut.log du serveur contient les informations suivantes :13/11/09 13.24.25:502 CET] 00000036
RuntimeConfig I com.tivoli.am.fim.rte.config.impl.RuntimeConfigurationImpl
setThreadSubject java.lang.NullPointerException at
com.ibm.ws.security.auth.ContextManagerImpl.isWSSubject

Le problème est dû à une configuration erronée du domaine ITFIM qui utilise SSL pour se connecter au gestionnaire de déploiement. Cependant, la sécurité WebSphere Application Server n'est pas activée dans la cellule de ce serveur de sorte que le trafic vers le port 8879 (port SOAP du gestionnaire de déploiement) n'utilise pas SSL.

Pour résoudre ce problème, désactivez l'option "La sécurité globale WebSphere est désactivée". Cette configuration peut s'effectuer dans la configuration du noeud final du service de gestion du domaine ITFIM de la console ISC si la sécurité WebSphere Application Server n'est pas activée dans la cellule.

Erreur de fonctionnement de la déconnexion unique ITFIM

Le problème est dû à une configuration de jonction incorrecte. La meilleure manière de configurer WebSEAL consiste à utiliser l'outil tfimcfg.jar qui crée la jonction avec la configuration appropriée et apporte les modifications de configuration nécessaires pour EAI.

Une jonction se présente comme suit :

```
object show /WebSEAL/ip-ip/FIM/  
Name: /WebSEAL/ip-ip/FIM  
Description: Object from host sam120sp3.  
Type: 16 (Management Object)  
Is Policy Attachable: Yes  
Attributs étendus  
Name: HTTP-Tag-Value
```

```
Value(s): ssn=ssn
name=name
email=email
user_session_id=user_session_id
Attached ACL: itfim_saml20ip2_nobody
Fichier POP attaché :
Règle AuthzRule attachée :
```

```
Attributs étendus effectifs
Protected Object Location: /WebSEAL/ip-ip/FIM
Name: HTTP-Tag-Value
Value(s): ssn=ssn
name=name
email=email
user_session_id=user_session_id
Effective ACL: itfim_saml20ip2_nobody
Fichier POP effectif :
Règle AuthzRule effective :
```

Assurez-vous que l'ID session est transmis par la jonction.

L'outil itfimcfg.jar active également EAI pour l'instance SOAP WebSEAL

Lors de la configuration de l'instance SOAP WebSEAL à l'aide de l'utilitaire de configuration de Tivoli Federated Identity Manager, itfimcfg.jar active également l'authentification EAI.

EAI est activé sur SOAP car la même instance WebSEAL peut être utilisée pour le canal de retour SOAP et le point de contact de connexion unique. Une amélioration a été apportée à WebSEAL pour l'autoriser à accepter une demande d'arrêt de session directement à partir d'un serveur Tivoli Federated Identity Manager. WebSEAL peut accepter une demande d'arrêt de session au lieu de passer par l'interface de programme d'application PDAdmin. Cette fonction exige que la fonctionnalité WebSEAL soit configurée pour la configuration EAI.

Un déclencheur EAI doit être configuré sur toutes les adresses URL pouvant recevoir une demande de déconnexion. La déconnexion pouvant être lancée par le biais de SOAP, l'outil de configuration définit un déclencheur EAI sur le noeud final SOAP.

Si le noeud final SOAP est hébergé sur un serveur WebSEAL différent de celui qui gère les sessions utilisateur, Tivoli Federated Identity Manager détecte que des serveurs différents sont utilisés. Tivoli Federated Identity Manager fait à nouveau appel à l'interface de programme d'application PDAdmin pour procéder à la déconnexion. Dans ce cas, la configuration EAI sur le noeud final SOAP n'est pas utile et peut être désactivée manuellement.

La console n'affiche pas le nouveau membre de cluster dans la table Noeuds d'exécution

La console n'affiche pas le nouveau membre de cluster dans la table Noeuds d'exécution une fois que celui-ci a été ajouté au cluster.

Pour afficher le nouveau membre du cluster :

1. Editez le fichier software.properties dans le sous-répertoire /pkg où Tivoli Federated Identity Manager est installé.

2. Mettez à jour le fichier `com.tivoli.am.fim.rte.software.serialId` en lui affectant une valeur différente.
Par exemple, remplacez :
`com.tivoli.am.fim.rte.software.serialId=1197396816285` par
`com.tivoli.am.fim.rte.software.serialId=1197396816286`
3. Connectez-vous à la console de gestion.
4. Cliquez sur **Tivoli Federated Identity Manager -> Gestion des domaines -> Gestion des noeuds d'exécution**. Lorsque le portlet est ouvert, il vérifie si `software.properties serialId` a été mis à jour.
5. Cliquez sur le bouton Déployer l'environnement d'exécution.

Une fois le déploiement terminé, le noeud apparaît dans la table.

Le type de valeur BinarySecurityToken LTPA Version 2 n'est pas pris en charge par WebSphere Application Server Versions 6.0.2 et 6.1

Si vous configurez un module de jeton LTPA Version 2, la couche de services Web ne fait de distinction entre LTPA V1 et LTPA V2 si vous utilisez WebSphere Application Server Version 6.0.2 ou 6.1. Si vous envoyez un jeton LTPA ayant le nom qualifié (Qname) `http://www.ibm.com/websphere/appserver/tokentype#LTPAv2` comme type de valeur, le jeton est rejeté dans WebSphere Application Server Versions 6.0.2 et 6.1.

WebSphere Application Server Versions 6.0.2 et 6.1 n'établit pas de distinction entre un jeton LTPA V1 ou LTPA V2 dans la couche de services Web. Un seul type de valeur BinarySecurityToken est pris en charge pour les jetons LTPA et le nom qualifié (QName) du type de valeur est : `http://www.ibm.com/websphere/appserver/tokentype/5.0.2#LTPA`.

Comme solution palliative temporaire, vous pouvez continuer à utiliser un jeton LTPA V1 ou LTPA V2. Veuillez cependant à affecter au nom qualifié le type de valeur suivant, quel que soit le contenu du jeton : `http://www.ibm.com/websphere/appserver/tokentype/5.0.2#LTPA`.

Pour activer le type `http://www.ibm.com/websphere/appserver/tokentype/5.0.2#LTPA` pour les jetons LTPAv2, la propriété personnalisée du module d'exécution est la suivante :

- Pour activer le jeton à l'échelle globale :
 - Clé : `ltpa.enable.compat.mode`
 - Type : valeur booléenne : `true` ou `false`
 - Description : la valeur par défaut est `false`. Si cette valeur est activée, cela permet de s'assurer que le module STS LTPA émet des jetons compatibles avec WAS 6.0.2 et WAS 6.1.
- Pour activer le jeton sur un chaîne STS unique :
 - Clé : `ltpa.enable.compat.mode.[chainId]`
 - Exemple de clé : `ltpa.enable.compat.mode.[uuid3778696c-0124-1fa7-9b85-be0cd9adb32a]`
 - Type : booléen
 - Valeur : `true` ou `false`

- Description : la valeur par défaut est false. Si cette valeur est activée, cela permet de s'assurer que le module STS LTPA émet des jetons compatibles avec WAS 6.0.2 et WAS 6.1. Cette propriété permet de définir la configuration sur une chaîne spécifique.

La création d'un domaine Tivoli Federated Identity Manager peut nécessiter le redémarrage de WebSphere Application Server

Lors de la création d'un domaine Tivoli Federated Identity Manager (ou d'une connexion à un domaine), si vous spécifiez des informations incorrectes dans le panneau des paramètres de sécurité, il peut s'avérer nécessaire de redémarrer WebSphere Application Server. Si vous entrez des données correctes et que la connexion à la console Tivoli Federated Identity Manager a été établie au service de gestion (utilisez l'option **Tester la connexion** pour tester la connexion), il n'est pas nécessaire de se reconnecter à WebSphere Application Server. Si la console Tivoli Federated Identity Manager ne peut pas se connecter au service de gestion, même si des informations de sécurité correctes sont fournies, il est nécessaire de redémarrer WebSphere Application Server.

Problèmes associés à Integrated Solutions Console

Les problèmes ci-dessous et leurs solutions concernent l'utilisation de la console de gestion de Tivoli Federated Identity Manager qui s'exécute en tant que plug-in d'IBM Integrated Solutions Console.

Affichage de plusieurs messages vous invitant à redémarrer WebSphere Application Server

Une fois que vous avez effectué une opération sur la console, vous pouvez être invité à redémarrer plusieurs fois le serveur d'applications WebSphere.

A propos de cette tâche

Si vous redémarrez WebSphere Application Server à l'invite et que vous essayez de réutiliser la console avant que le redémarrage ne soit totalement terminé, vous pouvez à nouveau être invité à redémarrer le serveur WebSphere.

Procédure

1. Patientez quelques instants après le redémarrage du serveur d'applications WebSphere pour permettre au redémarrage de se terminer correctement. Vous pouvez consulter les journaux du serveur d'applications WebSphere afin de vous assurer de la fin du redémarrage.
2. Une fois le redémarrage terminé, vous pouvez continuer à utiliser la console.

Opérations incomplètes après la déconnexion de la console

Si vous vous déconnectez de la console avant la fin d'une opération, un résultat incomplet peut se produire.

A propos de cette tâche

Pour exécuter certaines opérations, telles que la création d'une fédération, il convient de compléter une série de panneaux d'information dans la console. Si vous vous déconnectez avant d'avoir cliqué sur le bouton **Terminer** dans le panneau final, l'opération en cours s'effectue à l'aide des données entrées. Ainsi, l'opération, comme une définition de fédération, peut s'avérer incomplète. Les étapes suivantes peuvent empêcher d'obtenir des opérations complètes.

Procédure

1. Terminez l'opération en cours.
2. Déconnectez-vous ensuite de la console. Si vous devez vous déconnecter de la console en cours d'opération, procédez comme suit :
 - a. Connectez-vous à la console.
 - b. Vérifiez que l'opération est bien terminée.
 - c. Dans le cas contraire, modifiez les valeurs, le cas échéant.

Redémarrage de WebSphere Application Server après la reconfiguration des paramètres de sécurité dans la console de gestion

Vous devez redémarrer WebSphere Application Server si vous définissez de nouvelles valeurs de sécurité dans la console de gestion.

La console d'administration Tivoli Federated Identity Manager fonctionne comme un plug-in d'IBM Integrated Solutions Console qui s'exécute comme une application dans WebSphere Application Server. WebSphere Application Server peut en option être configuré pour activer la sécurité. Lorsque la sécurité WebSphere Application Server est activée, IBM Integrated Solutions Console et la console de gestion Tivoli Federated Identity Manager doivent être configurés pour utiliser les valeurs de sécurité WebSphere Application Server appropriées (par exemple, l'emplacement des fichiers de chiffrement et les mots de passe nécessaires pour accéder aux fichiers).

Arrêt de WebSphere Application Server à partir de la ligne de commande après le redémarrage de Tivoli Federated Identity Manager à partir de la console

Cette rubrique s'applique uniquement aux systèmes Windows. Si vous sélectionnez le redémarrage dans la console de gestion Tivoli Federated Identity Manager, arrêtez le service WebSphere Application Server à l'aide de la ligne de commande.

Sur les systèmes Windows sur lesquels WebSphere Application Server s'exécute en tant que service, si vous cliquez sur Redémarrer dans la console de gestion Tivoli Federated Identity Manager, le panneau Windows Services indique que le service perd le contact avec WebSphere Application Server. Le redémarrage de WebSphere Application Server aboutit, mais le panneau Services peut ne pas l'indiquer.

Dans ce cas, vous ne pouvez pas arrêter le service WebSphere Application Server par le biais du panneau Services et la console de gestion Tivoli Federated Identity Manager peut perdre sa connexion à WebSphere Application Server. Pour arrêter le service WebSphere Application Server, utilisez la ligne de commande. Pour plus de détails sur la procédure à suivre, consultez le centre de documentation de WebSphere Application Server.

Pour apporter une solution palliative, procédez comme suit :

1. Redémarrez WebSphere Application Server à partir de la console de gestion Tivoli Federated Identity Manager.
2. Déconnectez-vous de la console de gestion Tivoli Federated Identity Manager.
3. Connectez-vous à celle-ci.

Pour une solution palliative plus durable, vous pouvez installer WebSphere Application Server sous Windows sans l'enregistrer en tant que service. Dans ce cas, la console de gestion Tivoli Federated Identity Manager peut le redémarrer à l'aide des commandes appropriées.

Limitation dans le panneau Instances de module

Lors de la configuration du service d'accréditation dans Tivoli Federated Identity Manager, le panneau Instances de module utilise la langue de l'environnement local du serveur.

Le domaine Tivoli Federated Identity Manager est créé sur la base de l'environnement local du serveur. La langue utilisée sur le serveur est basée sur l'environnement local de ce dernier. La langue utilisée sur le serveur est implémentée quelle que soit celle utilisée sur le navigateur qui se connecte au serveur.

Par exemple, un navigateur en langue anglaise se connecte à une console Tivoli Federated Identity Manager dans une langue autre que l'anglais. La langue affichée dans le panneau Instances de module est une langue autre que l'anglais.

Problèmes associés à la console WebSphere Application Server

Les problèmes suivants et leurs solutions concernent l'utilisation de la console d'administration WebSphere Application Server.

WebSphere Application Server doit être installé séparément pour chaque instance de la console de gestion

Vous ne pouvez installer qu'un seul composant de console de gestion dans chaque installation WebSphere Application Server.

Le composant de console de gestion de IBM Tivoli Federated Identity Manager ne peut être installé que sur un profil unique d'une installation WebSphere Application Server. Si vous devez installer ce composant plusieurs fois sur la même machine, vous devez créer une installation de WebSphere Application Server pour chaque instance de la console de gestion.

L'environnement d'exécution ou le service de gestion ne s'affiche pas dans la console d'administration WebSphere

Si la console d'administration du serveur d'applications WebSphere n'affiche pas l'application d'exécution ou de gestion, fermez, puis rouvrez la session.

A propos de cette tâche

Cliquez sur le lien Déconnexion dans la console pour fermer correctement la session. Vous n'obtenez pas le résultat correct en fermant l'explorateur. Si cette opération ne résout pas le problème, procédez comme suit :

Procédure

1. Recherchez les fichiers EAR appropriés :

Composant	Nom de fichier
Service de gestion	ITFIMManagementService.ear
Environnement d'exécution	ITFIMRuntime.ear

Selon l'environnement de serveur d'applications WebSphere, ces fichiers se trouvent à l'un des emplacements suivants :

Configuration de serveur	Chemin par défaut
Serveur unique	\$WAS_PROFILE_HOME/installedApps/ nom_cellule/nom_noeud/
Cluster	\$WAS_PROFILE_HOME/installedApps/ nom_cellule

2. Si vous ne parvenez pas à localiser les fichiers EAR, vous rencontrez peut-être un problème d'installation. Pour plus d'informations, voir *Tivoli Federated Identity Manager - Guide d'installation*.

Les modifications de configuration ne sont pas propagées à chaque noeud de cluster tant que l'environnement d'exécution de Federated Identity Manager n'a pas redémarré

L'environnement d'exécution de Federated Identity Manager redémarre avant que les modifications de configuration spécifiées soient propagées à chaque noeud du cluster.

Après avoir effectué un changement de configuration dans Federated Identity Manager par le biais de la console WebSphere, le message et le bouton de sélection suivant s'affichent :

FBTCON197W Les modifications récentes apportées à la configuration doivent être rechargées vers l'environnement d'exécution de Tivoli Federated Identity Manager...

Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager

Lorsque vous sélectionnez ce bouton, l'environnement d'exécution Federated Identity Manager redémarre sur chaque serveur d'applications du cluster.

Les changements de configuration effectués sont récupérés dans l'environnement d'exécution Federated Identity Manager dans un délai d'une à deux secondes. Cependant, en raison des délais d'attente du réseau, il peut s'avérer nécessaire de cliquer sur ce bouton et de démarrer les environnements d'exécution

pour que tous les changements soient propagés vers chaque noeud de la cellule WebSphere. Dans ce cas, vous pouvez démarrer à nouveau l'environnement d'exécution Federated Identity Manager à partir de la console d'administration WebSphere en sélectionnant la séquence d'options suivante : **Tivoli Federated Identity Manager-> Gestion de domaines-> Gestion des noeuds d'exécution-> Recharger les configurations.**

La console WebSphere indique que le service de gestion est indisponible

Il se peut que la console d'administration WebSphere Application Server indique de façon incorrecte que le service de gestion de IBM Tivoli Federated Identity Manager n'est pas disponible.

A propos de cette tâche

Le service de gestion de IBM Tivoli Federated Identity Manager s'exécute en tant qu'application WebSphere. La page Applications d'entreprise de la console d'administration WebSphere Application Server est utilisée pour afficher la disponibilité des applications WebSphere. Dans un environnement (en clusters) de déploiement réseau du serveur d'applications WebSphere, la page des applications d'entreprise peut afficher l'état du service de gestion comme étant indisponible même si l'application est en cours d'exécution. L'état est indiqué par une icône grise contenant une barre oblique.

Procédure

1. Pour vérifier l'état de l'application, arrêtez celle-ci, puis redémarrez-la à l'aide de l'une des méthodes suivantes :
 - Utilisez la commande `wsadmin` de l'interface de ligne de commande.
 - Utilisez la console WebSphere Application Server.
2. Examinez la console pour vérifier que le service de gestion s'affiche comme étant disponible.

Obtention du statut du module d'exécution de Tivoli Federated Identity Manager

Il n'est pas possible d'obtenir le statut du module d'exécution de IBM Tivoli Federated Identity Manager à partir de la console eWAS. Les commandes `wsadmin` suivantes indiquent comment obtenir le statut du module d'exécution de IBM Tivoli Federated Identity Manager et comment démarrer et arrêter ce module à partir de la ligne de commande. Ces commandes considèrent que l'instance WebSphere Application Server est nommée "server1".

- Déterminez si le module d'exécution de IBM Tivoli Federated Identity Manager est installé ("ITFIMRuntime" apparaît si c'est le cas) :

```
wsadmin>$AdminApp list
```
- Vérifiez si le module d'exécution de IBM Tivoli Federated Identity Manager est en cours d'exécution (si aucune sortie n'est renvoyée, il ne l'est pas) :

```
wsadmin>$AdminControl queryNames  
type=Application,process=server1,name=ITFIMRuntime,*
```
- Arrêtez le module d'exécution de IBM Tivoli Federated Identity Manager :

```
wsadmin>set appManager [$AdminControl queryNames  
type=ApplicationManager,process=server1,*]  
wsadmin>$AdminControl invoke $appManager stopApplication ITFIMRuntime
```

- Démarrez le module d'exécution de IBM Tivoli Federated Identity Manager :

```
wsadmin>set appManager [$AdminControl queryNames
type=ApplicationManager,process=server1,*]
wsadmin>$AdminControl invoke $appManager startApplication ITFIMRuntime
```

Problèmes opérationnels

Cette rubrique décrit les problèmes liés au fonctionnement du système.

Echec de la connexion unique (SSO) fédérée bien que l'utilisateur soit défini dans le répertoire du point de contact

Lorsque vous utilisez Tivoli Access Manager, une tentative de connexion unique peut échouer si WebSphere Application Server est spécifié comme étant le serveur de point de contact et si le serveur d'autorisation Tivoli Access Manager (pdacld) n'est pas synchronisé avec le répertoire utilisateur WebSphere Application Server.

Si vous spécifiez WebSphere Application Server comme étant le point de contact et que le répertoire n'est pas synchronisé avec le registre d'utilisateurs Tivoli Access Manager, un fournisseur de services, tout en essayant de connecter un utilisateur au cours d'une opération de connexion unique, appelle le serveur d'autorisation Tivoli Access Manager (pdacld) pour extraire le principal de l'utilisateur (pour une fédération SAML11, par exemple). Bien que l'utilisateur soit défini dans le répertoire utilisateur WebSphere Application Server, si Tivoli Access Manager utilise un répertoire différent et si l'utilisateur ne se trouve pas dans ce répertoire, la tentative d'établissement de connexion unique échoue avec le message suivant :

```
HPDIA0202W Un nom d'utilisateur inconnu a été présenté à Access Manager.
```

Solution :

Lors de la création d'un domaine pour la connexion unique fédérée, l'assistant vous demande si vous voulez effectuer la configuration dans un environnement Tivoli Access Manager. Vous ne devez choisir cette possibilité que si vous utilisez WebSEAL comme serveur de point de contact ou si le registre d'utilisateurs Tivoli Access Manager est synchronisé avec le répertoire utilisateur du point de contact indiqué.

Echecs intermittents lors de la validation des messages reçus

Des échecs intermittents de la validation des messages reçus peuvent se produire dans l'environnement Federated Identity Manager si le correctif IY93387 n'est pas installé pour la machine virtuelle Java.

Des erreurs dans le fichier de trace indiquent l'échec de la validation du XML reçu. L'entrée de trace suivante est un exemple :

```
[9/7/07 17:05:27:807 EST] 0000002d KessServiceJk 3 \
com.tivoli.am.fim.kess.service.jks.worker.impl.\
  KessServiceJksWorkerImpl validateXML The certificate\
    retrieved for xml signature validation was: [
[
  Version: V3
  Subject: CN=Centrelink Test Cert :7100000475, \
    O=Centrelink, L=CANBERRA, ST=ACT, C=AU
  Signature Algorithm: SHA1withRSA, OID = \
    1.2.840.113549.1.1.5

  Key: IBMJCE RSA Public Key:
  modulus:
```

```
14189859499861991556759666278919062796750170353960474643269\  
64828281839944736663117523328393135352278107418418307586142\  
87325943234755701308264277933574423686572764845396587200330\  
99438097967197848101728967308745194178118178620477841810867\  
01145700565261600463539503091277695238640382185227225322270\  
78677140534763  
public exponent:  
65537
```

```
Validity: [From: Wed Nov 01 14:28:26 EST 2006,  
To: Sun Mar 30 11:46:30 EST 2008]  
Issuer: CN=TEST SecureNet Health OCA, O=SecureNet Limited,\  
C=AU  
SerialNumber: [1162351707]  
<...removed for brevity ...>  
[9/7/07 17:05:27:813 EST] 0000002d KessServiceJk 3 \  
com.tivoli.am.fim.kess.service.jks.worker.impl\  
KessServiceJksWorkerImpl validateXML  
Signature was NOT valid on the XML document.  
Core Validity: false  
SignedInfo: false  
Msg: SignatureValue mismatched.
```

Ce problème est résolu par l'APAR IY93387 et corrigé dans la JVM 1.4.2 SR9 et la JVM 5.0 SR4.

Le niveau de correctif Java SDK 1.4.2 SR9 peut être téléchargé à partir du site Web suivant :

<http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24011104>

Le niveau de correctif Java SDK 1.5 SR5 peut être téléchargé à partir du site Web suivant :

<http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24015843>

Désactivation de la détection de validation de réexécution dans un mot de passe associé (passticket)

Un horodatage est imbriqué dans un mot de passe associé (passticket), mais la granularité de l'intervalle horaire est à la seconde pleine. Si deux mots de passe associés (passticket) sont générés pour le même objet (utilisateur, application cible, clé secrète) au cours de la même seconde, ceux-ci sont identiques, c'est-à-dire qu'ils apparaîtront comme étant de type "attaque de réexécution" pour le valideur. Pour gérer ce problème, RACF autorise l'option "disable replay detection" et cet APAR autorise IBM Tivoli Federated Identity Manager pour prendre en charge cette fonctionnalité. Pour désactiver la réexécution, définissez l'une des propriétés d'exécution suivantes ou les deux :

```
passticket.disable.replay.check.[uuid_chaine]=true
```

```
passticket.disable.replay.check=true
```

où *uuid_chaine* correspond à la valeur de l'identificateur unique universel de chaîne. Par exemple :

```
passticket.disable.replay.check.[uuideb42e428-011b-1ebc-a0cb-  
9e6c4b35c1c7]=true
```

Pour déterminer la valeur de l'identificateur unique universel de chaîne, sélectionnez **Trust Service Chains-> Select Action**, puis **Show Chain ID in**

column in table dans la console d'administration. Lorsque cette action est sélectionnée, une nouvelle colonne apparaît dans la table qui affiche l'ID de chaîne unique.

Impossible de se connecter à WebSphere lors de l'utilisation de l'adaptateur VMM Tivoli Access Manager

Symptôme : impossible de se connecter en tant qu'administrateur WebSphere ou d'autoriser l'arrêt de WebSphere Application Server. Un message d'erreur signale un problème lié à l'initialisation ou à la communication avec le registre de l'adaptateur VMM (Virtual Member Management) Tivoli Access Manager. Cette erreur peut survenir lorsque la sécurité WebSphere Application Server est activée et que l'adaptateur est configuré pour utiliser les référentiels fédérés WebSphere.

A propos de cette tâche

L'adaptateur VMM Tivoli Access Manager utilise les registres pris en charge Tivoli Access Manager. Il convient pour cela que le registre Tivoli Access Manager soit disponible à chaque fois que l'adaptateur est utilisé. Le fichier de configuration Tivoli Access Manager qui est requis par l'adaptateur VMM Tivoli Access Manager doit également exister. Il doit se trouver à l'emplacement que vous avez spécifié lors de la configuration de l'adaptateur.

Le problème lié à la connexion WebSphere peut se produire si l'une des conditions suivantes se vérifie (true) :

- La propriété de configuration de l'adaptateur VMM Tivoli Access Manager est supprimée
- Le serveur de registre Tivoli Access Manager n'est pas en cours d'exécution
- Tivoli Access Manager est configuré.

Lorsque ce problème se produit, vous devez rétablir l'accès à WebSphere Application Server.

Remarque : Consultez d'abord le journal de WebSphere Application Server et déterminez si le serveur de registre Tivoli Access Manager sous-jacent n'est pas en cours d'exécution. Si c'est le cas, redémarrez le serveur de registre et vérifiez que vous pouvez y accéder à partir de l'environnement WebSphere. Si vous y parvenez, il n'est pas nécessaire d'exécuter les étapes de tâches décrites dans cette rubrique.

Les étapes suivantes indiquent comment rétablir l'accès à WebSphere Application Server. Cette procédure s'applique uniquement aux configurations dans lesquelles deux conditions se vérifient (true) :

1. Les référentiels fédérés WebSphere Application Server sont configurés pour contenir plusieurs adaptateurs. Sachez qu'un adaptateur est requis pour chaque type de registre configuré.
2. L'adaptateur VMM Tivoli Access Manager est l'un des adaptateurs configurés dans les référentiels fédérés WebSphere Application Server.

Procédure

1. Arrêtez WebSphere Application Server.

Si vous ne parvenez pas à vous connecter, vous pouvez être amené à utiliser une commande du système d'exploitation pour interrompre le processus.

2. Connectez-vous à WebSphere Application Server :

```
wsadmin -conntype none
```

3. Si une entrée de base est configurée pour l'adaptateur VMM Tivoli Access Manager, supprimez-la du domaine.
Par exemple, si le nom du domaine est defaultWIMFileBasedRealm et l'entrée de base de l'adaptateur est o=ibm,c=us :

```
$AdminTask deleteIdMgrRealmBaseEntry {-name defaultWIMFileBasedRealm
-baseEntry o=ibm,c=us}
```
4. Supprimez l'entrée de référentiel de l'adaptateur VMM Tivoli Access Manager.
Par exemple, si l'ID de registre de l'adaptateur VMM Tivoli Access Manager est TAMRegistryAdapter :

```
$AdminTask deleteIdMgrRepository {-id TAMRegistryAdapter}
```
5. Sauvegardez la configuration.

```
$AdminConfig save
```
6. Redémarrez le serveur WebSphere Application Server.
7. Si nécessaire, reconfigurez l'adaptateur VMM Tivoli Access Manager.

Problèmes de déploiement

Les problèmes et solutions suivants concernent les opérations de déploiement dans IBM Tivoli Federated Identity Manager.

Echec du déploiement de Tivoli Federated Identity Manager sous z/OS

Lors du déploiement de Tivoli Federated Identity Manager sous z/OS, les actions se bloquent et échouent après un certain délai.

Une limitation de la plateforme z/OS peut entraîner le blocage et l'échec des actions Tivoli Federated Identity Manager. L'erreur peut se produire avec le déploiement de l'environnement d'exécution Federated Identity Manager. Vous pouvez diagnostiquer l'erreur en examinant le fichier journal de WebSphere Application Server et en recherchant un message d'AVERTISSEMENT tel que le suivant :

```
Trace: 2008/02/20 15:30:48.909 01 t=9BE748 c=UNK key=P8 \
(13007002)
ThreadId: 00000044
FunctionName: com.ibm.ws.runtime.component.\
ThreadMonitorImpl
SourceId: com.ibm.ws.runtime.component.ThreadMonitorImpl
Category: WARNING
ExtendedMessage: BB000221W: WSVR0605W: Thread "WebSphere:\
ORB.thread.pool t=009c22b8" (00000022) has been active \
for 181010 milliseconds and may be hung. There is/are 1\
thread(s) in total in the server that may be hung.
```

Pour résoudre le problème, définissez une variable d'environnement WebSphere Application Server qui augmente la taille du pool d'unités d'exécution essentiel.

Pour définir la variable d'environnement pour un serveur d'applications autonome dans la console d'administration, sélectionnez **Serveurs -> Serveurs d'applications -> nom_serveur -> Infrastructure du serveur -> Administration -> Propriétés personnalisées**. Ajoutez la propriété `private_bboo_internal_work_thread_pool_size` associée à la valeur 5.

Pour définir la variable d'environnement pour une configuration de déploiement réseau dans la console d'administration, sélectionnez **Administration système ->**

Gestionnaire de déploiement -> Services d'administration -> Propriétés personnalisées. Ajoutez la propriété `private_bboo_internal_work_thread_pool_size` associée à la valeur 5.

Redémarrez le serveur WebSphere Application Server dont l'environnement a été modifié. Pour vérifier que la nouvelle valeur a été prise en compte, recherchez ce message dans la sortie du serveur lors du démarrage de ce dernier :

```
BBOM0001I private_bboo_internal_work_thread_pool_size: 5
```

Remarque : Cette erreur a été signalée uniquement au cours du déploiement de l'environnement d'exécution Federated Identity Manager et a été corrigée par la spécification de la valeur 5. Toutefois, si des messages d'erreur similaires sont générés lors de l'exécution d'autres activités Federated Identity Manager, la variable d'environnement `pool-size` peut être définie sur une valeur plus élevée.

Erreur lors de l'opération de déploiement

FBTCON137E: An error occurred during the deploy operation.

Ce message est une description générique de tous les échecs de déploiement. Il s'affiche même en cas de succès de l'opération lorsque la durée d'exécution de cette dernière a dépassé le délai d'expiration défini pour la demande SOAP.

Ce message peut s'afficher une fois que vous avez créé le domaine et cliqué sur **Déployer** dans le panneau Gestion des noeuds d'exécution. Pour valider le déploiement, suivez la procédure ci-dessous.

1. Fermez le panneau Gestion des noeuds d'exécution.
2. Ouvrez à nouveau ce panneau.

L'environnement d'exécution apparaît comme étant déployé (il est coché dans la colonne d'état). Vous pouvez alors le configurer.

Expiration du délai SOAP

Pour éviter que le connecteur client SOAP n'expire au cours d'une opération, augmentez la valeur du paramètre `com.ibm.SOAP.requestTimeout` afin qu'elle soit supérieure de 45 secondes à la durée d'exécution de l'opération. Pour déterminer le paramètre de délai d'expiration approprié, suivez la procédure ci-dessous.

1. Désactivez la valeur de délai d'expiration en attribuant au paramètre `com.ibm.SOAP.requestTimeout` la valeur 0.
2. Déployez l'application et enregistrez la durée du processus.
3. Définissez la valeur de délai d'expiration en attribuant au paramètre `com.ibm.SOAP.requestTimeout` une valeur correspondant à la durée enregistrée, à laquelle vous ajouterez 45.

Par exemple, si le déploiement de l'application a duré 3 minutes et 45 secondes, définissez le paramètre `com.ibm.SOAP.requestTimeout` sur la valeur 270 (4 minutes et 30 secondes).

Pour définir la valeur du paramètre `com.ibm.SOAP.requestTimeout`, procédez comme suit :

1. Arrêtez le noeud WebSphere Application Server sur lequel la console d'administration est installée.
2. Editez le fichier `$ISC/AppServer/properties/soap.client.props`.

3. Modifiez la valeur du paramètre `com.ibm.SOAP.requestTimeout`.
4. Enregistrez, puis fermez le fichier.
5. Démarrez le noeud WebSphere Application Server sur lequel la console d'administration est installée.

Déploiement de Tivoli Federated Identity Manager dans un environnement en cluster vertical WebSphere

Lors du déploiement de Tivoli Federated Identity Manager dans un environnement en cluster vertical, l'opération aboutit sur la première instance de WebSphere Application Server, mais elle échoue sur l'instance de serveur suivante.

Un environnement en cluster vertical WebSphere Application Server est créé en hébergeant plusieurs instances de serveur d'applications sur la même machine physique (noeud). Toutes les instances de WebSphere Application Server utilisent le même environnement de machine virtuelle Java.

Si vous tentez de déployer le serveur Tivoli Federated Identity Manager sur plusieurs instances de WebSphere Application Server sur le même système, l'opération échoue sur la deuxième instance car le serveur est déjà configuré dans la machine virtuelle Java.

Pour éviter que ce problème se produise, sauvegardez et supprimez les fichiers suivants avant de configurer le serveur IBM Tivoli Federated Identity Manager sur la deuxième instance de WebSphere Application Server :

`WAS_HOME/java/jre/PolicyDirector/PD.properties`

`WAS_HOME/java/jre/PolicyDirector/PDCA.ks`

Répétez cette procédure à chaque fois que vous déployez le serveur Tivoli Federated Identity Manager sur une instance distincte de WebSphere Application Server sur le même noeud.

Le déploiement de Tivoli Federated Identity Manager dans un cluster requiert la reconnaissance des agents de noeud

Dans un déploiement en cluster de WebSphere Application Server, l'environnement d'exécution Federated Identity Manager requiert la reconnaissance d'un agent de noeud pour s'initialiser correctement.

Bien que l'environnement d'exécution de Federated Identity Manager requiert la reconnaissance d'un agent de noeud pour s'initialiser correctement, ce dernier peut ne pas être disponible sur le serveur de noeuds gérés lors du démarrage. La liste suivante inclut les raisons clés expliquant les raisons pour lesquelles l'agent de noeud n'est pas reconnu lors du démarrage :

L'agent de noeud n'a pas été démarré

L'agent de noeud n'a pas été démarré avant le démarrage des noeuds gérés. Les agents de noeud doivent être démarrés avant le démarrage des noeuds gérés, sinon ils ne seront pas reconnus par l'application lors du démarrage.

Problèmes de performance

L'environnement d'exécution Federated Identity Manager utilise un événement de reconnaissance d'agent de noeud pour réinitialiser ses composants. Si le système ou le réseau fait face à une forte charge ou à un temps d'attente de réponse élevé pour d'autres raisons, cet événement peut ne pas être émis par WebSphere Application Server. L'environnement d'exécution peut ainsi rester indûment à l'état initialisé.

Les scénarios suivants indiquent comment un agent de noeud peut être détecté :

- L'environnement d'exécution Federated Identity Manager est configuré sans erreur à l'aide de la console d'administration ou le noeud d'exécution s'affiche comme étant à la fois déployé et configuré par le biais de la page Gestion des noeuds d'exécution.
- Lorsque la fonction de trace de Federated Identity Management est activée, vous trouverez une entrée journalisée par la méthode `handleNotification()` de `com.tivoli.am.fim.fedmgr2.servlet.SSOPSServlet` indiquant :
`received mbean notification: <message_de_notification>`

où `message_de_notification` indique un type d'événement `com.ibm.websphere.management.NotificationConstants`.

Solution :

Si l'agent de noeud ne peut pas être détecté, réinitialisez l'environnement d'exécution de Federated Identity Manager en redémarrant le fichier EAR ITFIMRuntime ou le noeud géré. Vérifiez que l'agent de noeud et le gestionnaire de déploiement (dmgr) s'exécutent avant de démarrer ou de redémarrer l'environnement d'exécution Federated Identity Manager.

Problèmes de personnalisation

Les problèmes ci-dessous et leurs solutions concernent la personnalisation de Tivoli Federated Identity Manager comme le développement ou la modification de plug-ins.

Résolution de `ClassDefNotFoundErrors` ou `ClassNotFoundExceptions`

Si vous recevez une erreur `class-not-found` ou `class-definition-not-found` dans une classe fournie par le conteneur J2EE WebSphere, comme `ClassDefNotFoundErrors` et `ClassNotFoundExceptions`, vérifiez que le package manquant de la classe est répertorié dans la section `Export-Package` du fichier `MANIFEST.MF` de `com.tivoli.am.fim.osgi.connector`. Vous pouvez modifier le fichier `MANIFEST.MF` qui se trouve dans `$WAS_PROFILE/config/itfim/com.tivoli.am.fim.osgi.connector_6.2.1/META-INF/`. Lorsque vous appelez des méthodes du conteneur WebSphere J2EE, il peut s'avérer nécessaire de commuter le chargeur de classes de contexte.

Débogage des problèmes de résolution et de démarrage de l'offre groupée OSGi

Les modules d'exécution Eclipse de Federated Identity Manager peuvent être lancés en mode débogage, ce qui ouvre un port d'accès à la console OSGi (`osgiConsole`). Vous pouvez utiliser `telnet` pour vous connecter à `osgiConsole`. Le composant `osgiConsole` vous permet d'obtenir le statut de toutes les offres

groupées dans le répertoire des plug-ins Federated Identity Manager et d'exécuter des opérations de gestion du cycle de vie dans les offres groupées, comme le démarrage, l'arrêt, l'installation et la désinstallation. Exécutez les étapes suivantes pour lancer un module d'exécution Eclipse Federated Identity Manager en mode débogage :

1. Accédez au répertoire dans lequel le fichier `launch.ini` est installé pour `com.tivoli.am.fim.war.management.war` :
`PROFIL_WAS/installedApps/noeud/ITFIMManagementService.ear/com.tivoli.am.fim.war.management.war/WEB-INF/eclipse/launch.ini`
ou accédez à `com.tivoli.am.fim.war.runtime.war` :
`PROFIL_WAS/installedApps/noeud/ITFIMRuntime.ear/com.tivoli.am.fim.war.runtime.war/WEB-INF/eclipse/launch.ini`
2. Editez le fichier `launch.ini` et indiquez une valeur pour la propriété `osgi.console.port` (par exemple, `osgi.console.port=8888`), puis sauvegardez le fichier. Si vous activez le débogage à la fois pour le service de gestion et le mode d'exécution sur la même machine, veillez à utiliser des valeurs de port différentes.
3. Redémarrez le fichier EAR `ITFIMManagementService` ou `ITFIMRuntime`.
4. A partir d'une invite de commande (ou d'un shell), exécutez `telnet localhost 8888` pour accéder à la console OSGi pour le module d'exécution Eclipse particulier de Federated Identity Manager. Une invite `osgi>` apparaît une fois qu'une connexion telnet a été établie à ce port.
5. A partir de l'invite `osgi>`, exécutez la commande `ss` pour répertorier les offres groupées dans le module d'exécution Eclipse et le statut de chaque offre groupée. Exécutez `help` pour afficher une liste des options de commande possibles.
6. Recherchez l'offre groupée que vous avez ajoutée et le numéro indiqué en regard de celle-ci. Si le statut de l'offre groupée est `INSTALLED` et non pas `RESOLVED` ni `STARTED`, vous pouvez tenter d'exécuter la commande `start numéro` pour imprimer une trace de pile d'exception Java qui est associée au démarrage de l'offre groupée personnalisée.
7. Pour quitter la console OSGi, exécutez `disconnect` pour vous déconnecter du port.

Localisation du répertoire temp des journaux d'erreurs OSGi

Pour déboguer une erreur OSGi de Federated Identity Manager, il peut s'avérer nécessaire de consulter les journaux d'erreurs OSGi. Lors du démarrage de Federated Identity Manager, les répertoires des plug-ins, de la configuration et des fonctions sont copiés du référentiel de configuration vers un emplacement sous le répertoire temp de WebSphere Application Server où est lancée l'instance OSGi de Federated Identity Manager. Cet emplacement se trouve généralement dans l'un des répertoires suivants :

```
WAS_APPSERVER/profiles/nom_profil/temp/noeud/serveur/  
ITFIMManagementService/com.tivoli.am.fim.war.management.war/itfim/
```

```
WAS_APPSERVER/profiles/nom_profil/temp/noeud/serveur/ITFIMRuntime/  
com.tivoli.am.fim.war.runtime.war/itfim/
```

Les journaux d'erreurs d'OSGi se trouvent dans le répertoire `itfim/configuration` sous le répertoire temp.

Appel d'une méthode d'API WebSphere à partir d'un module personnalisé

Cette rubrique indique comment utiliser `J2EEContainerAction` dans un module personnalisé pour appeler une méthode d'API WebSphere (comme recherche JNDI, recherche RMI ou SOAP MessageFactory).

Un mécanisme de rappel permettant à une partie du code du plug-in Federated Identity Manager de s'exécuter comme s'il fonctionnait dans le conteneur J2EE est disponible. Il est utile car certains appels de méthode reposent sur des ressources visibles uniquement par les chargeurs de classes dans le conteneur J2EE. Exemples d'appels de méthode contenus dans Federated Identity Manager : recherche JNDI, recherche de noeud final RMI, création de MessageFactory SOAP et connexion JAAS.

Pour utiliser ce mécanisme, créez d'abord une classe implémentant `com.tivoli.am.fim.osgi.J2EEContainerAction` qui contient une méthode `run()` :

```
J2EEContainerAction myAction = new J2EEContainerAction(){
    public Object run() throws Exception{
        //do something that needs to run within a J2EE container
    }
};
```

Appelez ensuite la classe action avec `com.tivoli.am.fim.osgi.J2EEContainerFactory` :
`J2EEContainerFactory.runInJ2EEContainer(myAction);`

`J2EEContainerFactory` gère `contextclassloader` en passant du module Eclipse au conteneur J2EE. Il appelle ensuite la méthode `run()` dans la classe action puis rétablit `contextclassloader` à l'original. Les trois éléments `J2EEContainActions` d'usage commun sont déjà définis et sont réutilisables :

```
com.tivoli.am.fim.j2eeactions.CreateMessageFactoryAction
\\creates a SOAP Message Factory
com.tivoli.am.fim.j2eeactions.JndiLookupAction
\\performs a JNDI lookup in WAS
com.tivoli.am.fim.j2eeactions.RmiLookupAction
\\performs a RMI lookup in WAS
```

Chapitre 5. Correctifs

Vous pouvez obtenir des correctifs à partir du site Web du support produit et vous inscrire aux notifications d'informations du support produit, notamment concernant les correctifs.

Obtention de correctifs

Un correctif de produit peut être disponible pour résoudre votre incident. Vous pouvez vérifier les correctifs disponibles pour votre logiciel Tivoli Federated Identity Manager en accédant au site Web de support logiciel IBM :

Procédure

1. Accédez au site Web de support logiciel IBM du logiciel Tivoli Federated Identity Manager : <http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliFederatedIdentityManager.html>. Une liste des derniers correctifs est répertoriée dans la section Download de cette page.
2. Cliquez sur le nom d'un correctif pour afficher sa description et le télécharger si nécessaire.

Réception des notifications de correctifs

Pour recevoir par courrier électronique des notifications sur les correctifs et d'autres informations actualisées sur les produits IBM, procédez comme suit :

Procédure

1. Accédez au site Web de support logiciel IBM du logiciel Tivoli Federated Identity Manager : <http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliFederatedIdentityManager.html>.
2. Dans le coin supérieur droit de la page, cliquez sur **My Support**. Une page d'ouverture de session s'affiche.
3. Si vous êtes déjà enregistré, passez à l'étape suivante. Si ce n'est pas le cas, cliquez sur l'option **enregistrer maintenant** afin de définir votre ID utilisateur et votre mot de passe.
4. Connectez-vous à la page **My support**.
5. Cliquez sur l'onglet **Edit profile**.
6. Sélectionnez **Software** → **Security** → **Access** dans les zones qui s'affichent.
7. Sélectionnez **IBM Tivoli Federated Identity Manager** dans la liste des produits.
8. Cliquez sur **Add products**.
9. Pour activer la notification par courrier électronique, cliquez sur **Subscribe to email** en haut de la page.
10. Dans la liste, cliquez sur **Software**.
11. Cochez les cases qui décrivent le mieux les notifications que vous souhaiteriez recevoir par courrier électronique.
12. Cliquez sur **Update**.
13. Fermez la session en cliquant sur **Sign out** ou sur **Go to my personalized page** pour afficher votre page de support personnalisée.

Chapitre 6. Recherche dans les bases de connaissances

Le service de support IBM de Tivoli Federated Identity Manager dispose d'une base de connaissances contenant des articles techniques, des incidents et des solutions palliatives.

A propos de cette tâche

IBM Support Assistant inclut un outil de recherche hiérarchique destiné à vous aider à centrer votre recherche sur les informations liées à un produit, plateforme ou anomalie spécifique. Pour plus d'informations, voir «Présentation du composant ISA», à la page 57.

La procédure suivante indique comment effectuer une recherche manuelle d'information.

Procédure

1. Accédez au site Web de support logiciel IBM du logiciel Tivoli Federated Identity Manager : <http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliFederatedIdentityManager.html>
2. Sous **Solve a problem**, cliquez sur :
 - **Technotes**, qui répertorie les informations sur le produit par le titre d'article, ou sur
 - **APARs**, qui répertorie les incidents connus par leur numéro de rapport officiel d'analyse de programme.
3. Vous pouvez rechercher, de façon facultative, des termes spécifiques, des codes d'erreur ou des APAR à l'aide de la zone de recherche présente sur la page du support logiciel ou sur les pages Technotes ou APARs.

Chapitre 7. Collecte de données

Parfois, vous ne pouvez pas résoudre un problème simplement en résolvant les symptômes. Dans ce cas, vous devez recueillir davantage de données de diagnostic.

Avant de commencer à collecter les données pour un rapport d'incident, il est vivement conseillé d'installer et d'exécuter IBM Support Assistant. Cet outil d'identification et de résolution des problèmes inclut une console qui autorise la soumission en ligne d'un PMR (problem management record). Dans le cadre de ce processus, les informations propres au système, à l'environnement et au produit sont rassemblées dans un fichier utilisé par le service de support IBM. Pour plus d'informations sur IBM Support Assistant, voir «Présentation du composant ISA», à la page 57.

Une collecte de données anticipée, même avant d'ouvrir un enregistrement de gestion d'incidents, peut vous aider à répondre aux questions suivantes :

1. Les symptômes correspondent-ils à un incident connu ?
2. Dans ce cas, un correctif ou une solution palliative a-t-il(elle) été publié(e) ?
3. Est-ce un incident qui n'est pas axé sur un défaut et qui peut être identifié et résolu sans aucun correctif de code ?
4. Quelle est l'origine de l'incident ?

Les données de diagnostic dont vous avez besoin pour la collecte et les sources à partir desquelles vous avez recueilli ces données dépendent du type d'incident que vous examinez. Par exemple, si vous examinez une erreur disque potentielle dans un environnement AIX, la sortie de la commande `errpt` .

Pour identifier le composant à l'origine de l'incident, suivez les questions de la liste d'identification des incidents de Tivoli Federated Identity Manager.

Collecte de données générales

Lorsque vous soumettez un incident au service de support logiciel IBM, vous avez généralement besoin d'un ensemble d'informations de base pour fournir des détails sur le ou les systèmes affectés, comme :

- la version de Tivoli Federated Identity Manager et les niveaux des correctifs sur les systèmes affectés,
- le nom et la version du système d'exploitation,
- des détails d'ordre général sur la structure de votre environnement comme le nombre de serveurs et de logiciels installés, les domaines et les fédérations configurés et ainsi de suite.

Collecte de données spécifiques à un incident

Pour les symptômes spécifiques ou pour les incidents présents dans une partie particulière du produit, vous devrez peut-être recueillir d'autres données comme les informations de message et de trace. Pour plus d'informations, consultez les rubriques de ce chapitre. Une fois que vous avez recueilli les données de diagnostic appropriées, vous pouvez essayer de les analyser vous-même ou encore les fournir au service de support logiciel IBM.

Journaux de messages et de trace

Les journaux de messages et de trace de Tivoli Federated Identity Manager sont gérés et enregistrés par le serveur d'applications WebSphere.

Consultez les rubriques d'identification des incidents du centre de documentation WebSphere Application Server pour obtenir des informations détaillées sur les journaux et la journalisation.

Journaux de messages

Les journaux de messages sont des fichiers texte dans lesquels les opérations du système sont enregistrées.

Les types de message suivants sont enregistrés par défaut :

Messages d'information

Indiquent des conditions qui présentent un intérêt mais qui ne vous obligent pas à prendre des précautions ou à intervenir.

Messages d'avertissement

Indiquent qu'une condition à prendre en compte mais n'exigeant pas nécessairement votre intervention a été détectée.

Messages d'erreur

Indiquent qu'une condition s'est produite nécessitant une action de votre part.

Fichiers journaux de messages

Tous les messages Tivoli Federated Identity Manager sont enregistrés dans les journaux de messages par défaut suivants de WebSphere Application Server.

Tableau 2. Journaux de messages

Journal	Nom du fichier par défaut	Contenu
Journaux de la machine virtuelle Java	SystemOut.log	Messages au format texte pour l'instance du serveur d'applications.
Journal de maintenance IBM	activity.log	Messages au format d'événement de base commun binaire pour l'installation du serveur d'applications. Remarque : les outils d'affichage de ce format sont fournis avec WebSphere Application Server. Pour plus d'informations, consultez le centre de documentation WebSphere Application Server.

A l'aide de la console d'administration du WebSphere Application Server, vous pouvez configurer certains paramètres des journaux comme l'emplacement, le nom, la taille maximale des fichiers journaux et les niveaux de gravité que vous souhaitez enregistrer (comme Avertissement et Grave). Pour plus d'informations, voir «Configuration des paramètres du journal», à la page 47.

Emplacements des journaux de messages

Par défaut, les journaux de messages se trouvent dans les répertoires suivants.

Tableau 3. Emplacements des journaux de messages par défaut du serveur d'applications

Journal	Chemin
Journaux de la machine virtuelle Java	UNIX et Linux : /opt/IBM/WebSphere/AppServer/profiles/nom_profil/logs/nom_serveur/SystemOut.log z/OS : /usr/lpp/WebSphere/V6R0/profiles/nom_profil/logs/nom_serveur/SystemOut.log Windows : C:\Program Files\IBM\WebSphere\AppServer\profiles\nom_profil\logs\nom_serveur\SystemOut.log
Journal de maintenance IBM	UNIX et Linux : /opt/IBM/WebSphere/AppServer/profiles/nom_profil/logs/activity.log z/OS : /usr/lpp/WebSphere/V6R0/profiles/nom_profil/logs/activity.log Windows : C:\Program Files\IBM\WebSphere\AppServer\profiles\nom_profil\logs\nom_serveur\activity.log

Les journaux de messages de la console sont sauvegardés dans les répertoires de journal de messages du noeud WebSphere Application Server sur lequel la console d'administration est installée.

Journaux de trace

La consignation de trace (ou fonction de trace) fournit au personnel du service de support logiciel d'IBM des informations complémentaires relatives à l'état du système au moment où un incident s'est produit.

Contrairement aux journaux de messages, qui enregistrent les événements notables qui se sont produits, les journaux de trace enregistrent les informations transitoires relatives à l'environnement d'exploitation en cours lorsqu'un composant ou une application ne fonctionne pas comme prévu. Les journaux de trace sont uniquement disponibles en anglais.

L'activation de la journalisation de trace n'est pas effectuée par défaut car parfois, elle peut entraîner la collecte de grandes quantités de données dans un court délai et risque de dégrader considérablement les performances. C'est pourquoi vous devez uniquement activer la consignation de trace lorsque le personnel du support logiciel IBM vous le demande. Pour plus d'informations, voir le support logiciel.

Les entrées des journaux de trace peuvent fournir le niveau de détail suivant :

Fin Détail minimal.

Plus fin
 Détail modéré.

Le plus fin
 Détail maximal.

Fichier journal de trace

Si le traçage est activé pour un serveur d'applications, les informations de trace de Tivoli Federated Identity Manager sont enregistrées dans le journal de trace par défaut suivant de WebSphere Application Server.

Tableau 4. Journal de trace

Nom du journal par défaut	Nom du fichier par défaut	Contenu
Trace de diagnostic	trace.log	Informations de trace au format texte pour l'instance du serveur d'applications.

A l'aide de la console d'administration de WebSphere Application Server, vous pouvez configurer certains paramètres des journaux comme l'emplacement, le nom, la taille maximale des fichiers journaux et le niveau de gravité que vous souhaitez enregistrer (comme Fin, Plus fin, Le plus fin). Pour plus d'informations, voir «Configuration des paramètres du journal», à la page 47.

Emplacements du journal de trace

Par défaut, le journal de trace se trouve dans les répertoires suivants :

Tableau 5. Emplacements du journal de trace par défaut du serveur d'applications

Journal	Chemin
Trace de diagnostic	UNIX et Linux : /opt/IBM/WebSphere/AppServer/profiles/nom_profil/logs/nom_serveur/trace.log z/OS : /usr/lpp/WebSphere/V6R0/profiles/nom_profil/logs/nom_serveur/trace.log Windows : C:\Program Files\IBM\WebSphere\AppServer\profiles\nom_profil\logs\nom_serveur\trace.log

Les journaux de trace de la console sont sauvegardés dans les répertoires de journal de trace du nœud WebSphere Application Server sur lequel la console d'administration est installée.

Configuration des paramètres du journal

Les paramètres des journaux de messages et de trace peuvent être configurés à l'aide de la console d'administration. La consignation des messages est activée par défaut. La consignation de trace doit être activée uniquement sur demande du personnel de support IBM.

Configuration de la consignation des messages

La consignation des messages dans le journal de la machine virtuelle Java et le journal de maintenance IBM est activée par défaut. Les deux journaux sont configurés pour enregistrer les messages de tous niveaux de gravité, de tous les composants Tivoli Federated Identity Manager. Vous pouvez modifier les noms, l'emplacement, la taille de fichier et le niveau de gravité qui seront enregistrés.

Configuration du journal de la machine virtuelle Java

Vous pouvez modifier le nom de fichier, l'emplacement, le format de fichier, la taille de fichier, le début de la journalisation et l'heure de fin, le nombre de journaux à conserver et le niveau de gravité qui seront enregistrés dans le journal de la machine virtuelle Java.

A propos de cette tâche

Le journal de la machine virtuelle Java, également appelé SystemOut.log, est un journal WebSphere Application Server standard, utilisé pour les messages. Pour des informations détaillées, consultez les rubriques du journal de la machine virtuelle Java dans le centre de documentation du serveur d'applications WebSphere.

Procédure

1. Démarrez la console d'administration WebSphere Application Server, puis connectez-vous si nécessaire.
2. Cliquez sur **Identification et résolution des incidents** → **Journaux et trace** pour ouvrir la page Consignation et traçage.
3. Cliquez sur le nom du serveur que vous souhaitez configurer, server1 par exemple.
4. Cliquez sur **Journaux de la JVM** pour afficher les options de configuration.
5. Sélectionnez l'onglet **Configuration**.
6. Faites défiler l'écran pour afficher les attributs à configurer.
7. Modifiez les attributs de configuration, puis cliquez sur **Appliquer**.
8. Sauvegardez les modifications apportées à votre configuration.

Configuration du journal de maintenance IBM

Le journal de maintenance IBM est activé par défaut. Vous pouvez modifier ce paramètre ou les noms, l'emplacement, la taille de fichier et le niveau de gravité qui seront enregistrés dans le journal.

A propos de cette tâche

Le journal de maintenance, également appelé activity.log, est un journal WebSphere Application Server standard utilisé pour les messages. Pour des informations détaillées sur ce journal, consultez les rubriques correspondantes dans le centre de documentation du serveur d'applications WebSphere.

Procédure

1. Démarrez la console d'administration WebSphere Application Server, puis connectez-vous si nécessaire.
2. Cliquez sur **Identification et résolution des incidents** → **Journaux et trace** pour ouvrir la page Consignation et traçage.
3. Cliquez sur le nom du serveur que vous souhaitez configurer, server1 par exemple.
4. Cliquez sur **Journaux des services IBM** pour afficher les options de configuration.
5. Sélectionnez ou désélectionnez la case à cocher **Activer le journal des services** pour activer ou désactiver la journalisation. Le journal de maintenance est activé par défaut.
6. Définissez le nom du journal de maintenance dans la zone **Nom du fichier**. Le nom par défaut est : activity.log. Si ce nom est modifié, l'exécutable nécessite un accès en écriture au nouveau fichier, et le fichier doit utiliser l'extension .log.
7. Spécifiez le nombre maximal de mégaoctets que la taille d'un fichier peut atteindre dans la zone **Taille maximale du fichier**. Lorsque le fichier atteint cette taille, il boucle au début en remplaçant les données les plus anciennes par les plus récentes.
8. Cliquez sur **Appliquer** pour sauvegarder les modifications de configuration.
9. Redémarrez le serveur pour que les modifications de configuration soient prises en compte.

Activation de la consignation de trace

Vous pouvez activer la consignation de trace au démarrage du serveur ou sur un serveur en cours d'exécution.

A propos de cette tâche

Remarque : Pour préserver les performances du système, vous ne devez activer la journalisation de trace que lorsque le personnel du support IBM vous le demande.

Activation de la trace au démarrage du serveur

La journalisation de trace peut être activée au démarrage du serveur.

A propos de cette tâche

Le journal de trace est un journal WebSphere Application Server standard, utilisé pour les informations de trace. Pour plus d'informations sur ce journal, consultez le centre de documentation WebSphere Application Server.

Procédure

1. Démarrez la console d'administration WebSphere Application Server, puis connectez-vous si nécessaire.
2. Cliquez sur **Identification et résolution des incidents** → **Journaux et trace** pour ouvrir la page Consignation et traçage.
3. Cliquez sur le nom du serveur que vous souhaitez configurer, server1 par exemple.
4. Cliquez sur **Trace de diagnostic** pour afficher les options de configuration.
5. Cliquez sur l'onglet **Configuration**.
6. Sélectionnez ou désélectionnez la case à cocher **Activer le journal** pour activer ou désactiver la journalisation. Le journal de trace est activé par défaut.

7. Terminez la configuration en suivant les instructions du personnel du support IBM. Pour des informations supplémentaires sur les paramètres de configuration, consultez les rubriques du journal d'identification des problèmes et de trace dans le centre de documentation de WebSphere Application Server.
8. Cliquez sur **Appliquer** pour sauvegarder les modifications de configuration.
9. Pour entrer une chaîne de trace afin de définir la spécification de trace sur l'état souhaité, procédez comme suit :
 - a. Cliquez sur **Identification et résolution des incidents** → **Journaux et trace** pour ouvrir la page Consignation et traçage.
 - b. Cliquez sur le serveur que vous souhaitez configurer, server1 par exemple.
 - c. Cliquez sur **Modifier les niveaux de détail de journalisation**.
 - d. Si l'option **Tous les composants** a été activée, vous pouvez la désactiver, puis activer les composants spécifiques.
10. Cliquez sur un nom de composant ou de groupe. Pour obtenir une liste des composants Tivoli Federated Identity Manager, voir «Composants de trace», à la page 50. **Remarque** : Si le serveur sélectionné n'est pas en cours d'exécution, il ne s'affichera pas dans la liste.
11. Entrez une chaîne de trace dans la zone de chaîne de trace. Par exemple, pour définir le traçage uniquement pour le serveur d'accréditation, entrez : `*=info:com.tivoli.am.fim.trustserver.*=all` Pour plus d'informations sur les chaînes de trace, consultez le centre de documentation du serveur d'applications WebSphere.
12. Cliquez sur **OK**.
13. Cliquez sur **Sauvegarder** pour sauvegarder vos modifications. Il peut être nécessaire de redémarrer WebSphere Application Server pour que les modifications prennent effet.

Activation de la trace sur un serveur en cours d'exécution

La journalisation de trace peut être activée sur un serveur en cours d'exécution.

A propos de cette tâche

Le journal de trace est un journal WebSphere Application Server standard, utilisé pour les informations de trace. Pour plus d'informations sur ce journal, consultez le centre de documentation WebSphere Application Server.

Procédure

1. Démarrez la console d'administration WebSphere Application Server, puis connectez-vous si nécessaire.
2. Cliquez sur **Identification et résolution des incidents** → **Journaux et trace** pour ouvrir la page Consignation et traçage.
3. Cliquez sur le nom du serveur que vous souhaitez configurer, server1 par exemple.
4. Cliquez sur **Trace de diagnostic**.
5. Cliquez sur l'onglet **Exécution**.
6. Sélectionnez la zone **Enregistrer les modifications d'exécution dans la configuration également** si vous souhaitez écrire vos modifications dans la configuration de serveur.
7. Modifiez l'état de la chaîne de trace existante en modifiant la spécification de trace sur l'état souhaité.

8. Configurez la sortie de trace si vous souhaitez apporter une modification à partir de la sortie existante.
9. Cliquez sur **Appliquer**.

Composants de trace

Le tableau suivant décrit une liste partielle des composants que vous pouvez définir pour la consignation de trace. **Remarque** : Activez le traçage uniquement pour les composants que vous demande le personnel du support IBM. Selon les symptômes de votre incident, le personnel du support IBM peut vous conseiller d'activer le traçage pour d'autres composants qui ne sont pas décrits dans le tableau ci-dessous.

Tableau 6. Nom et description des composants de trace

Composant de trace	Description du composant
com.tivoli.am.fim	Tous les composants de Tivoli Federated Identity Manager
com.tivoli.am.fim.audit	Audit
com.tivoli.am.fim.fedmgr2	Service de protocole de connexion unique (SPS)
com.tivoli.am.fim.kess	Service de clés
com.tivoli.am.fim.liberty	Protocole de connexion unique Liberty
com.tivoli.am.fim.management	Gestion de la console
com.tivoli.am.fim.mgmt	Gestion de la console
com.tivoli.am.fim.saml	Protocole de connexion unique SAML
com.tivoli.am.fim.saml20	Protocole de connexion unique SAML 2.0
com.tivoli.am.fim.soap	Connexions SOAP
com.tivoli.am.fim.sps	Structure du service de protocole de connexion unique
com.tivoli.am.fim.trust	Client du service d'accréditation
com.tivoli.am.fim.trustserver	Service d'accréditation
com.tivoli.am.fim.wsfederation	Protocole de connexion unique WS-Federation
com.tivoli.am.fim.wssm	gestion de la sécurité des services Web

Affichage des journaux

Le format des journaux détermine leur affichage.

Journaux de la machine virtuelle Java

Pour afficher les journaux de la machine virtuelle Java, vous pouvez utiliser la console d'administration du serveur d'applications WebSphere, qui prend en charge l'affichage à partir d'une machine distante, ou utiliser un éditeur sur la machine qui contient les fichiers journaux. Pour plus d'informations, recherchez "affichage des journaux JVM" dans le centre de documentation de WebSphere Application Server.

Journaux de maintenance IBM

Les journaux de maintenance sont écrits au format binaire. Pour afficher un journal, vous pouvez utiliser les outils fournis avec WebSphere Application Server. Pour plus d'informations, recherchez "affichage du journal de service" dans le centre de documentation de WebSphere Application Server.

Journaux de trace

Les données de trace sont générées en texte en clair au format de base, avancé ou d'analyseur de journal. Sur un serveur d'applications, les données de trace peuvent être dirigées vers un fichier ou dans une mémoire tampon circulaire. Si une mémoire tampon circulaire est utilisée, les données devront être exportées dans un fichier avant de pouvoir être affichées.

Sur un client d'application ou dans un processus autonome, les données de trace peuvent être dirigées vers un fichier ou vers la fenêtre de la console du processus. Pour plus d'informations, recherchez "sortie de trace" dans le centre de documentation de WebSphere Application Server.

Utilisation du composant IBM Support Assistant

L'outil IBM Support Assistant Lite for Tivoli Federated Identity Manager facilite l'identification et la résolution des problèmes liés à Tivoli Federated Identity Manager. Utilisez cet outil pour collecter automatiquement les données relatives aux problèmes.

Vous devez installer le plug-in Tivoli Federated Identity Manager for IBM Support Assistant dans le cadre de l'installation de Tivoli Federated Identity Manager. Si vous n'avez pas spécifié le composant IBM Support Assistant lors de l'installation du produit, installez-le maintenant.

Pour savoir comment utiliser l'outil, voir :

- «Utilisation d'IBM Support Assistant en mode graphique»
- «Utilisation d'IBM Support Assistant en mode console», à la page 53

Utilisation d'IBM Support Assistant en mode graphique

Vous pouvez utiliser une interface graphique pour collecter les données avec IBM Support Assistant.

A propos de cette tâche

Pour accéder à l'interface graphique, exécutez un script à partir de la ligne de commande.

Procédure

1. Vérifiez que l'environnement Java est configuré correctement :
 - a. Vérifiez que l'environnement d'exécution Java est au niveau 1.4.2 ou supérieur.
 - b. Déterminez si l'emplacement de l'environnement d'exécution Java est inclus dans le paramètre d'environnement PATH. Si ce n'est pas le cas, définissez la variable JAVA_HOME de manière à ce qu'elle pointe vers l'environnement d'exécution Java.

Tableau 7. Spécification de la variable JAVA_HOME pour votre environnement

Système d'exploitation	Exemple de commande
Windows	Par exemple, si Java Development Kit est installé dans c:\jre1.4.2, utilisez la commande suivante : SET JAVA_HOME=c:\jre1.4.2
UNIX ou Linux	Par exemple, si vous utilisez le shell bash et que Java Development Kit est installé dans /opt/jre142, utilisez la commande suivante : export JAVA_HOME=/opt/jre142

- Démarrez l'outil IBM Support Assistant :
Ouvrez une fenêtre de commande et placez-vous dans le répertoire d'installation ISALite. Ce dernier est l'emplacement dans lequel vous avez décompressé le fichier TFIMISALite.zip. Entrez la commande correspondant à votre environnement :

Tableau 8. Exécution d'IBM Support Assistant

Type du système d'exploitation	Commande
Windows	runISALite.bat
UNIX ou Linux	runISALite.sh Remarque : Vérifiez que le script est exécutable. Si nécessaire, utilisez la commande suivante pour modifier les droits d'accès au fichier : chmod 755 runISALite.sh

IBM Support Assistant démarre maintenant une interface graphique.

- Dans la fenêtre Problem Type, sélectionnez un type de problème.
Développez les dossiers pour afficher tous les types de problème.
Recherchez-en un et sélectionnez-le.
- Indiquez un nom de fichier pour le fichier ZIP de collecte des données.
N'importe quel nom de fichier peut être utilisé. L'outil ajoute automatiquement l'extension de fichier ZIP. Par exemple, si vous entrez le nom de fichier Install_problem, le fichier est nommé Install_problem.zip.
- Cliquez sur **Collect Data**.
Le script de collecte s'exécute et vous invite à fournir des informations supplémentaires. Ces dernières peuvent inclure des informations de configuration ou la séquence d'événements à l'origine du problème. Le script peut également vous demander vos préférences pour la collecte des données.
Lorsque les scripts ont fini de collecter les informations de configuration, il collecte les données nécessaires. L'outil crée un fichier ZIP que vous pouvez envoyer au service de support IBM.
- A l'invite, entrez un nom de fichier dans la zone **Output Filename/Path**.
L'outil ajoute le nom d'hôte du serveur et l'horodatage en cours au nom de fichier que vous avez indiqué.
- Envoyez le fichier ZIP au service de support IBM
Vous pouvez choisir FTP ou HTTPS pour le transfert du fichier. Sachez que FTP n'est pas chiffré, contrairement à HTTPS.

Utilisation d'IBM Support Assistant en mode console

Vous pouvez collecter des données avec IBM Support Assistant en mode console.

A propos de cette tâche

Le mode console permet de contrôler, par le biais de la ligne de commande, les scripts de collecte IBM Support Assistant Lite. Par le biais de cet outil, vous enregistrez vos réponses à partir d'une session en mode console dans un fichier de réponses. Utilisez ensuite ce dernier pour lancer les exécutions ultérieures d'un même script de collecte.

Procédure

1. Vérifiez que l'environnement Java est configuré correctement :
 - a. Vérifiez que l'environnement d'exécution Java est au niveau 1.4.2 ou supérieur.
 - b. Déterminez si l'emplacement de l'environnement d'exécution Java est inclus dans le paramètre d'environnement PATH. Si ce n'est pas le cas, définissez la variable JAVA_HOME de manière à ce qu'elle pointe vers l'environnement d'exécution Java.

Tableau 9. Spécification de la variable JAVA_HOME pour votre environnement

Système d'exploitation	Exemple de commande
Windows	Par exemple, si Java Development Kit est installé dans c:\jre1.4.2, utilisez la commande suivante : SET JAVA_HOME=c:\jre1.4.2
UNIX ou Linux	Par exemple, si vous utilisez le shell bash et que Java Development Kit est installé dans /opt/jre142, utilisez la commande suivante : export JAVA_HOME=/opt/jre142

2. Démarrez l'outil IBM Support Assistant :

Ouvrez une fenêtre de commande et placez-vous dans le répertoire d'installation ISALite. Ce dernier est l'emplacement dans lequel vous avez décompressé le fichier TFIMISALite.zip. Entrez la commande correspondant à votre environnement :

Tableau 10. Exécution d'IBM Support Assistant

Type du système d'exploitation	Commande
Windows	runISALiteConsole.bat
UNIX ou Linux	runISALiteConsole.sh Remarque : Vérifiez que le script est exécutable. Si nécessaire, utilisez la commande suivante pour modifier les droits d'accès au fichier : chmod 755 runISALite.sh

IBM Support Assistant démarre maintenant en mode console.

3. Créez un fichier de réponses.

Tableau 11. Syntaxe pour l'enregistrement de l'entrée de données pour IBM Support Assistant

Type du système d'exploitation	Commande
Windows	runISALiteConsole.bat -record <i>response.txt</i>
UNIX ou Linux	runISALiteConsole.sh -record <i>response.txt</i>

Vous pouvez spécifier le nom de fichier de votre choix pour *response.txt*.

Lors de l'exécution dans ce mode, l'entrée des données s'effectue au cours d'une session interactive. L'outil enregistre vos réponses dans le fichier que vous spécifiez.

4. Exécutez l'outil à l'aide du fichier de réponses.

Tableau 12. Syntaxe pour l'utilisation d'IBM Support Assistant avec un fichier de réponses

Type du système d'exploitation	Commande
Windows	runISALiteConsole.bat <i>response.txt</i>
UNIX ou Linux	runISALiteConsole.sh <i>response.txt</i>

Remarques :

- Le fichier de réponses est un fichier en texte clair. Vous pouvez l'éditer pour modifier les valeurs comme il convient. Par exemple, vous pouvez utiliser le fichier sur un autre ordinateur après avoir ajusté les valeurs du fichier de réponses pour refléter les paramètres de l'ordinateur local.
- Sachez que des informations confidentielles telles les noms d'utilisateur et les mots de passe peuvent être enregistrées dans le fichier de réponses. Prenez les précautions nécessaires lors de la gestion du fichier afin d'éviter l'accès non autorisé aux informations importantes.
- Certaines sessions de collecte de données requièrent l'intervention de l'utilisateur et ne peuvent donc pas s'effectuer en mode silencieux. Par exemple, le service de support IBM peut vous demander de recréer un problème au cours de la collecte des données afin de collecter les fichiers journaux et de trace. Dans ce cas, la collecte en mode silencieux ne peut pas enregistrer ni reproduire toutes les étapes.

Chapitre 8. Analyse des données

Après avoir recueilli des données de différentes sources, vous devez déterminer de quelle manière elles peuvent vous aider à résoudre votre problème particulier.

Pour analyser les données, choisissez l'une des actions suivantes :

- Déterminez quelles sources de données sont les plus susceptibles de contenir des informations sur l'incident, puis commencez votre analyse. Par exemple, si l'incident est lié à l'installation, commencez votre analyse avec les fichiers journaux de l'installation (le cas échéant) plutôt qu'avec les fichiers journaux du produit général ou du système d'exploitation.
- Cernez précisément la façon dont les différents groupes de données sont liés. Par exemple, si les données s'étendent sur plusieurs systèmes, organisez-les de manière à pouvoir connaître la source d'origine de tel groupe de données.
- Assurez-vous de la pertinence des différents groupes de données de diagnostic par rapport à la chronologie de l'incident en vérifiant les horodatages. Notez que des données de sources différentes peuvent avoir des formats d'horodatage différents. Assurez-vous que vous comprenez bien la séquence des différents éléments de chaque format d'horodatage de façon à pouvoir expliquer quand les différents événements se sont produits.

La méthode d'analyse spécifique varie selon les sources de données, mais il est généralement conseillé, pour la plupart des traces et des fichiers journaux, de commencer par identifier le point dans les données où l'incident s'est produit. Une fois ce point identifié, vous pouvez revenir en arrière dans les données pour trouver l'origine de l'incident.

Si vous examinez un incident pour lequel vous disposez de données comparatives pour un environnement actif et inactif, commencez par comparer les détails du système d'exploitation et de la configuration du produit pour chaque environnement.

Chapitre 9. Comment contacter le support ?

Le service de support logiciel IBM fournit une assistance pour les produits défectueux.

Vous pouvez contacter le service de support IBM de plusieurs manières :

- **IBM Support Assistant** : Cette application Web vous permet de rechercher des informations sur un problème, de collecter les informations consignées nécessaires à l'identification et à la résolution d'un problème et d'ouvrir un PMR (problem management report) en ligne. IBM Support Assistant est la méthode recommandée pour signaler un problème au service de support logiciel IBM. Vous avez besoin d'un ID de compte utilisateur et d'un mot de passe pour soumettre un PMR par le biais d'IBM Support Assistant. Le client IBM Support Assistant est inclus sur le CD du produit et les mises à jour peuvent être téléchargées à partir du site Web suivant : <http://www.ibm.com/software/support/isa/>
- **En ligne** : cliquez sur l'onglet **Submit** et **track problems** sur le site Web du service de support logiciel IBM à l'adresse <http://www.ibm.com/software/support/probsub.html>. Entrez les informations requises dans l'outil de soumission d'incident.
- **Par téléphone** : Pour connaître le numéro de téléphone à composer en fonction de votre pays, accédez à la page de contacts du document *IBM Software Support Handbook*, à l'adresse <http://techsupport.services.ibm.com/guides/contacts.html>, puis cliquez sur le nom de votre région géographique.

Si l'incident soumis concerne un défaut logiciel ou une documentation manquante ou imprécise, le service de support logiciel IBM crée un rapport officiel d'analyse de programme (APAR). Cet APAR décrit l'incident de manière détaillée. Dans la mesure du possible, le centre de support IBM fournit une solution palliative que vous pouvez mettre en oeuvre jusqu'à ce que l'APAR soit résolu et qu'une solution soit apportée. IBM publie quotidiennement les APAR résolus sur le site Web de support logiciel, afin que les utilisateurs qui rencontrent le même incident puissent bénéficier des mêmes solutions.

Avant de soumettre un incident au support logiciel IBM, répondez aux questions suivantes :

1. Possédez-vous un contrat de maintenance logicielle IBM ?
2. Comprenez-vous l'impact de l'incident sur votre entreprise ?
3. Pouvez-vous décrire cet incident ?

Présentation du composant ISA

Le composant IBM Support Assistant simplifie le processus de recherche et de soumission de problèmes logiciels.

Le composant IBM Support Assistant facilite l'accès aux informations de support et aux outils de maintenabilité qui vous aideront à identifier les problèmes. Il est constitué de trois outils :

Rechercher

Offre un accès rapide aux informations du référentiel d'identification et de résolution des problèmes en utilisant un grand nombre de filtres pour

rendre vos recherches plus précises. L'outil de recherche simultanée balaie la masse des documents IBM et renvoie des résultats classés par source pour en faciliter la consultation.

Liens d'accès aux infos produit

Ces liens d'auto-assistance incluent :

- Pages de support du produit
- Pages d'accueil du produit
- Guide d'identification et de résolution des problèmes du produit
- Feuilles de route sur la formation au produit et au composant IBM Education Assistant
- Mises à jour recommandées du produit
- Forums sur le produit

Fonction de maintenance

La fonction de maintenance est un outil de collecte système automatique et de collecte basée sur les symptômes. La collecte système rassemble des informations générales auprès du système d'exploitation, du registre et d'autres sources. La collecte basée sur les symptômes rassemble des informations produit spécifiques liées au problème auquel vous êtes confronté. La fonction de maintenance permet également de définir automatiquement la trace afin d'aider le service de support IBM lors de la collecte des données.

Par ailleurs, elle offre la possibilité de soumettre un problème en ligne au service de support IBM. Entrez vos données d'autorisation d'utilisation une seule fois et celles-ci seront sauvegardées pour les sessions ultérieures. Vous pouvez ensuite créer un rapport d'incident pour IBM et associer les données collectées dans le fichier de collecteur.

Le composant IBM Support Assistant fournit un guide d'utilisation complet pour vous aider à configurer et à utiliser cet outil. Les étapes suivantes indiquent la procédure de base à suivre pour configurer votre système en vue de l'utilisation d'IBM Support Assistant :

1. Installez l'outil IBM Support Assistant à partir du CD du produit ou à partir du site Web suivant :
<http://www.ibm.com/software/support/isa/>
2. Dans un référentiel logiciel IBM, recherchez le plug-in IBM Support Assistant pour connaître la version de WebSphere Application Server que vous exécutez. Le plug-in Tivoli Federated Identity Manager utilise le plug-in WebSphere Application Server comme code de base.

Remarque : Le téléchargement de ce dernier peut prendre beaucoup de temps selon le trafic réseau et la disponibilité des ressources système.

3. Installez le plug-in WebSphere Application Server dans le sous-répertoire \plugin du répertoire d'installation d'IBM Support Assistant.
4. Recherchez le plug-in IBM Support Assistant de Tivoli Federated Identity Manager sur le CD du produit ou dans un référentiel logiciel IBM.
5. Installez le plug-in IBM Support Assistant dans le sous-répertoire \plugin du répertoire d'installation du produit.
6. Démarrez IBM Support Assistant en cliquant sur l'icône bureau. Pour obtenir des informations sur les différentes tâches disponibles, sélectionnez l'onglet **User Guide**.

Contrats de maintenance logicielle IBM

Avant de prendre contact avec le service de support logiciel IBM pour soumettre un incident, votre entreprise doit avoir conclu un contrat de maintenance logicielle et vous devez disposer d'une autorisation de soumission d'incident à IBM.

Si vous n'êtes pas certain du type de contrat de maintenance logicielle requis, téléphonez au 0801 835 426 ou 801 TEL IBM, ou à partir d'autres pays, accédez à la page de contacts d'*IBM Software Support Handbook* à l'adresse <http://techsupport.services.ibm.com/guides/contacts.html>, puis cliquez sur votre région pour obtenir les numéros de téléphone du service de support présent dans votre région.

Définition de l'impact sur l'entreprise

Lorsque vous signalez un incident à IBM, il vous est demandé d'indiquer son niveau de gravité. Par conséquent, vous devez comprendre et évaluer l'impact de l'incident sur vos activités.

Utilisez pour cela les critères suivants :

Tableau 13. Niveaux de gravité

Gravité 1	L'incident a un impact <i>critique</i> : vous ne pouvez pas utiliser le programme, ce qui a des conséquences graves sur le déroulement de vos opérations. Cette condition requiert une solution immédiate.
Gravité 2	Cet incident a un impact <i>significatif</i> : le programme peut être utilisé, mais de façon très limitée.
Gravité 3	L'incident a un impact <i>relatif</i> : le programme peut être utilisé, mais certaines fonctions, non préjudiciables au déroulement des opérations, ne sont pas disponibles.
Gravité 4	L'incident a un impact <i>minime</i> : l'incident a peu d'impact sur le déroulement de vos opérations, ou une solution satisfaisante a été mise en oeuvre.

Description d'un incident

Lorsque vous décrivez le problème à IBM, soyez le plus précis possible. Incluez toutes les informations possibles afin que les spécialistes du support logiciel IBM puissent vous aider à résoudre efficacement l'incident.

Pour gagner du temps, préparez les réponses aux questions ci-dessous.

- Quelles versions des logiciels étaient exécutées lorsque l'incident s'est produit ?
- Existe-t-il des journaux, des traces et des messages liés aux symptômes de l'incident ?
- Pouvez-vous recréer l'incident ? Si la réponse est oui, quelles étapes appliquez-vous pour le recréer ?
- Avez-vous apporté des modifications au système ? Par exemple, avez-vous modifié le matériel, le système d'exploitation, le logiciel réseau ou tout autre composant du système ?
- Appliquez-vous actuellement une solution palliative à cet incident ? Dans ce cas, préparez-vous à décrire la solution palliative lorsque vous signalez l'incident.

Envoi de données

Vous pouvez envoyer des données de diagnostic comme des fichiers journaux et de configuration, au support logiciel IBM.

Appliquez l'une des méthodes suivantes :

- IBM Support Assistant
- Le protocole FTP (EcuRep)
- L'outil ESR

IBM Support Assistant

Le composant IBM Support Assistant inclut une fonction de maintenance comportant un outil de collecte système automatique et un outil de collecte basée sur les symptômes. La collecte système rassemble des informations générales auprès du système d'exploitation, du registre et d'autres sources. La collecte basée sur les symptômes rassemble des informations produit spécifiques liées au problème auquel vous êtes confronté. La fonction de maintenance permet également de définir automatiquement la trace afin d'aider le service de support IBM lors de la collecte des données. Pour plus d'informations sur IBM Support Assistant, voir «Présentation du composant ISA», à la page 57.

Le protocole FTP (EcuRep)

Pour envoyer des fichiers à l'aide du service FTP appelé EcuRep, regroupez les fichiers de données que vous avez collectés au format ZIP ou TAR, puis nommez cet ensemble en fonction de votre identificateur PMR (Problem Management Record). Le fichier obtenu doit utiliser la convention d'attribution de nom suivante pour qu'il soit correctement associé au PMR :

xxxxx.bbb.ccc.yyy.yyy

où :

Tableau 14. Convention d'attribution de nom aux fichiers

xxxxx	Numéro PMR
bbb	Succursale, à partir de l'identificateur PMR
ccc	Code pays, à partir de l'identificateur PMR
yyy.yyy	Type de fichier (format ZIP ou TAR)

Pour transférer vos fichiers par FTP, procédez comme suit :

1. A l'aide d'un utilitaire FTP, connectez-vous au serveur emea.ibm.com (par exemple, ftp.emea.ibm.com).
2. Connectez-vous de façon anonyme, puis entrez votre adresse électronique comme mot de passe.
3. Placez-vous dans le répertoire toibm (par exemple, cd toibm).
4. Placez-vous dans l'un des sous-répertoires spécifiques à la plateforme : aix, cae, hw, linux, lotus, mvs, os2, os400, swm, tivoli, unix, vm, vse et windows.
5. Mettez-vous en mode binaire (bin) (par exemple, bin).

6. Téléchargez votre fichier sur le serveur. Vous pouvez envoyer des fichiers sur le serveur FTP, mais vous ne pouvez pas les mettre à jour. Par conséquent, si vous devez ensuite modifier le fichier, vous devez créer un nouveau fichier avec un nom unique.

Pour plus d'informations sur le service EcuRep, voir IBM EMEA Centralized Customer Data Store Service à l'adresse : <http://www.ibm.com/de/support/ecurep/index.html>.

Si votre produit s'exécute dans un environnement z/OS et que vous souhaitez compresser vos fichiers, vous pouvez utiliser l'utilitaire TRSMMAIN, disponible en téléchargement à partir de la page Web suivante : <ftp://ftp.software.ibm.com/s390/mvs/tools/packlib>.

Outil ESR

Les utilisateurs enregistrés répertoriés dans une liste de demandeurs autorisés peuvent envoyer des données de diagnostic à l'aide de l'outil ESR (Electronic Service Request). L'outil ESR vous permet d'envoyer et de gérer les PMR (Problem Management Records) à la demande, 24 heures sur 24, 7 jours sur 7 et 365 jours par an.

Pour envoyer des données à l'aide de l'outil ESR, procédez comme suit :

1. Ouvrez une session sur l'outil ESR.
2. Dans la page d'accueil, entrez votre numéro PMR dans la zone **Enter a report number**, puis cliquez sur **Go**.
3. Faites défiler vers la zone **Attach Relevant File**.
4. Cliquez sur **Browse** pour rechercher le journal, la trace ou tout autre fichier de diagnostic que vous souhaitez envoyer au support logiciel IBM.
5. Cliquez sur **Submit**. Votre fichier est transféré au support logiciel IBM par FTP, et est associé à votre PMR.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, un programme ou un service IBM n'implique pas que seul ce produit, programme ou service IBM puisse être utilisé. Tout produit, programme ou service fonctionnellement équivalent qui n'enfreint aucun droit de propriété intellectuelle IBM peut être utilisé. Toutefois, il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM est susceptible de posséder des brevets ou des applications brevetées en attente qui couvrent le sujet décrit dans ce document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

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

Pour le Canada, veuillez adresser votre courrier à :

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

Pour les demandes de licence concernant les informations à deux octets (DBCS), contactez le Département des propriétés intellectuelles IBM de votre pays ou envoyez vos demandes, par courrier, à :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd
3-3-12, Roppongi, Minato-ku, Tokyo 106-8711 Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun autre pays dans lequel il serait contraire aux lois locales : LE PRESENT DOCUMENT EST LIVRE «EN L'ETAT». IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS ET DE FACON NON LIMITATIVE, TOUTE GARANTIE IMPLICITE DE NON-CONTREFACON OU D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

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

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

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

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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

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

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

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

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

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

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

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes.

Marques

IBM, , le logo IBM et [ibm.com](http://www.ibm.com) sont des marques d'International Business Machines aux Etats-Unis et/ou dans certains autres pays. Les autres noms de produit ou service sont des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur le Web dans le document "Copyright and trademark information" à <http://www.ibm.com/legal/copytrade.shtml>

Adobe, Acrobat, PostScript® et l'ensemble des marques incluant Adobe sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Intel®, le logo Intel, Intel Inside®, le logo Intel Inside, Intel® Centrino®, le logo Intel Centrino, Celeron®, Intel® Xeon®, Intel SpeedStep®, Itanium® et Pentium® sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

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

Microsoft®, Windows, Windows NT® et le logo Windows sont des marques de Microsoft Corporation aux Etats unis et/ou dans d'autres pays.

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



Java et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux États-Unis et/ou dans certains autres pays.

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

Index

A

- accessibilité x
- activity.log 44, 47
- affichage des journaux 50
- analyse des données de journal 55
- APAR 41
- appel d'une méthode d'API
 - WebSphere 38
- application de gestion ne s'affichant pas 28
- arrêt de WebSphere Application Server après le redémarrage de Federated Identity Manager 26

B

- bases de connaissances, recherche 41

C

- cacls.exe, commande 19
- caractères en langue nationale 17
- changements de configuration ne se propageant pas 28
- CLI non fonctionnelle après l'installation 14
- cluster vertical WebSphere, déploiement 35
- cluster WebSphere, agent de noeud non reconnu 35
- collecte de données pour un problème 43
- commande de publications ix
- consignation de trace, activation 48
- console d'administration WebSphere n'affichant pas l'application d'exécution 28
- contrats de maintenance 59
- contrats de maintenance logicielle 59
- conventions
 - typographiques x
- conventions typographiques x
- correctifs, obtention 39
- correctifs du produit 6

D

- déconnexion, opérations incomplètes 26
- dépannage
 - configuration
 - caractères en langue nationale 17
 - enregistrement de fichiers journaux 19
 - erreurs de chargement de classe 36
 - espaces dans le chemin du fichier de clés 18
 - ITFIM_WSSM, répertoire 16
 - paramètres de propriété SSL 16

- dépannage (*suite*)
 - déploiement
 - agent de noeud non reconnu 35
 - erreur 34
 - Expiration du délai SOAP 34
 - Tivoli Federated Identity Manager 33
 - WebSphere, cluster vertical 35
 - désinstallation 14
 - exploitation
 - échec de validation des messages 30
 - installation 13, 14
 - limitations
 - service d'alias 17
 - liste de contrôle 1, 11
 - personnalisation
 - journaux d'erreurs OSGi 37
 - méthode d'API WebSphere 38
 - offre groupée OSGi, résolution 36
 - problèmes liés à la console
 - changements de configuration 28
 - opérations incomplètes 26
 - redémarrage de WebSphere Application Server 25
 - WebSphere Application Server 26
 - process 1
 - symptômes 3
 - WebSphere Application Server
 - console d'administration 28
 - plusieurs instances de la console de gestion 27
 - service de gestion 29
- désinstallation générant une erreur
 - lexicale 14
- données, collecte pour un problème 43
- données spécifiques du problème 43

E

- échec de l'installation sous Solaris 13
- échec de validation des messages dans la JVM 30
- EcuRep, service 60
- Electronic Service Request 61
- enregistrement de fichiers journaux 19
- erreur lexicale dans la désinstallation 14
- erreurs de chargement de classe
 - ClassDefNotFoundErrors 36
 - ClassNotFoundExceptions 36
- errpt, commande 43
- espaces dans le chemin du fichier de clés 18
- Expiration du délai SOAP 34
- exploitation
 - échec de validation des messages 30

F

- fichier, journal de messages 44
- fichiers EAR, emplacement 28
- fichiers JAR supprimés après le redémarrage 14
- fins anormales 9
- formation
 - Voir Formation technique à Tivoli
- formation, technique à Tivoli x
- formation sur le produit 6
- Formation technique à Tivoli x
- FTP EcuRep, service 60

G

- groupe de correctifs 7
- groupe de mises à jour 7

I

- IBM Support Assistant 43, 57, 60
- interface de ligne de commande non fonctionnelle après l'installation 14
- Internet, recherches pour la résolution d'incidents logiciels 39
- interruptions 9
- ITFIM_WSSM, répertoire 16
- ITFIMManagementService.ear 28
- ITFIMRuntime.ear 28
- IY93387 30

J

- journal de la machine virtuelle Java
 - chemin 45
 - étapes de configuration 47
- journal de maintenance IBM
 - chemin d'accès 45
- journal des services IBM
 - étapes de configuration 48
- journaux
 - activation de la trace au démarrage du serveur 48
 - activation de la trace sur un serveur en cours d'exécution 49
 - affichage 50
 - analyse des données 55
 - emplacements 45, 46
 - message 45
 - noms de fichier 44, 45
 - trace 45, 46
 - types de message 44
- journaux d'erreurs OSGi 37
- journaux de messages 44
- journaux de trace 45
- JVM, correctif IY93387 30

L

- limitations
 - service d'alias 17
- limitations du service d'alias 17
- liste de contrôle pour l'identification et résolution des problèmes 1, 11

M

- messages 7
- messages d'erreur 7
- méthodes de soumission des données à IBM 60
- mises à jour du produit 6

N

- niveaux de gravité des problèmes 59
- noms de chemin, notation xi
- noms de fédération, caractères valides 17
- noms de fichier des journaux de messages 45
- noms de fichier des journaux de trace 46
- noms de répertoire, notation xi
- noms des composants de trace 50
- notation
 - noms de chemin xi
 - typographiques xi
 - variables d'environnement xi
- notes techniques 41
- notification sur les correctifs, configuration 39

O

- offre groupée OSGi, résolution 36
- opérations incomplètes après déconnexion 26
- Outil ESR 61

P

- pannes 9
- paramètres de propriété SSL 16
- personnalisation
 - journaux d'erreurs OSGi 37
 - méthode d'API WebSphere 38
 - offre groupée OSGi, résolution 36
- plusieurs consoles 27
- pool d'unités d'exécution
 - augmentation 33
- prise de contact avec le service de support logiciel IBM 57
- problèmes
 - collecte de données 43
 - connectivité 5
 - performance 8
 - rapport 59
 - symptômes 3
- problèmes de configuration
 - caractères en langue nationale 17
 - enregistrement de fichiers
 - journaux 19

- problèmes de configuration (*suite*)
 - espaces dans le chemin du fichier de clés 18
 - ITFIM_WSSM, répertoire 16
 - paramètres de propriété SSL 16
- problèmes de connectivité 5
- problèmes de déploiement
 - agent de noeud non reconnu 35
 - erreur 34
 - Expiration du délai SOAP 34
 - Tivoli Federated Identity Manager 33
 - WebSphere, cluster vertical 35
- problèmes de performance 8
- problèmes liés à la console
 - changements de configuration 28
 - opérations incomplètes 26
 - redémarrage de WebSphere
 - Application Server 25
 - WebSphere Application Server 26
- produit, correctifs 6

R

- redémarrage de WebSphere Application Server 25
- redémarrage de WebSphere Application Server après la reconfiguration des paramètres de sécurité 26

S

- sécurité, reconfiguration des paramètres 26
- service de gestion non disponible 29
- site Web des correctifs 6
- Solaris, échec de l'installation 13
- soumission des données à IBM, méthodes 60
- SPNEGO, espaces dans le chemin du fichier de clés 18
- support handbook 59
- support logiciel, contact 57
- symptômes, identification et résolution des problèmes 3
- SystemOut.log 44

T

- trace, noms des composants 50
- trace.log 46
- TRSMAN, utilitaire 61
- types de message 44

V

- variables, notation pour xi
- variables d'environnement, notation xi

W

- WebSphere Application Server dépannage
 - console d'administration 28
 - plusieurs instances de la console de gestion 27

- WebSphere Application Server (*suite*)
 - dépannage (*suite*)
 - service de gestion 29
 - installation pour plusieurs consoles 27
- WebSphere Application Server, arrêté à partir de la ligne de commande 26
- WebSphere Application Server, redémarrage 25
- wsadmin, commande 29

Z

- z/OS, échec du déploiement de Tivoli Federated Identity Manager 33



GC11-6782-00

