Notes de version de Sun Java System Access Manager 7.1

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Référence : 820–0362–10
juillet 2007

070802@18135

Table des matières

Notes de version Sun Java System Access Manager 7.1

Juillet 2007

Numéro de référence 819-4683-13

Ces notes de version contiennent des informations importantes disponibles au moment de la commercialisation de Sun Java™ Enterprise System (Java ES), notamment sur les nouvelles fonctionnalités d'Access Manager, sur les problèmes connus et sur leurs solutions éventuelles. Lisez attentivement ce document avant d'installer et d'utiliser cette version.

Pour consulter la documentation relative aux produits Java ES, notamment celle d'Access Manager, accédez au site `http://docs.sun.com/prod/entsys.05q4`.

Consultez ce site Web avant d'installer et de configurer votre logiciel, puis régulièrement par la suite pour vous procurer la documentation la plus récente concernant le produit.

Ces notes de version contiennent les rubriques suivantes :

Historique des révisions

Le tableau suivant présente l'historique des révisions apportées aux notes de version d'Access Manager 7.1.

TABLEAU 1 Historique des révisions

Date	Description des modifications
Juillet 2006	Version Bêta.
Mars 2007	Java Enterprise System version 5
Mai 2007	Mis à jour suite aux problèmes connus suivants : 6555040, 6550261, 6554379, 6554372, 6480354
Juin 2007	Mis à jour suite aux problèmes connus suivants : 6562076, 6490150
Juillet 2007	Mis à jour suite au problème connu 6485695

À propos de Sun Java System Access Manager 7.1

Sun Java System Access Manager fait partie de l'infrastructure Sun Identity Management permettant à une organisation de gérer les accès sécurisés aux applications Web et à d'autres ressources au sein de l'entreprise et aux différents niveaux des chaînes de valeurs interentreprises (B2B).

Les principales fonctions d'Access Manager sont les suivantes :

- des services d'authentification et d'autorisation centralisés ayant recours à un contrôle d'accès basé sur les rôles et les règles ;
- une connexion unique pour accéder aux applications Web d'une organisation ;
- la prise en charge d'une identité réseau fédérée avec le projet Liberty Alliance et le protocole d'authentification SAML (Security Assertions Markup Language) ;
- la consignation des informations critiques, telles que les activités des utilisateurs et des administrateurs via les composants Access Manager et ce, en vue de l'établissement d'analyses, de rapports et de contrôles ultérieurs.

Nouveautés de cette version

Cette version propose les nouvelles fonctions suivantes :

Intégration de la structure de contrôle Java ES

Access Manager 7.1 intègre la structure de contrôle Java Enterprise System par le biais de Java Management Extensions (JMX). La technologie JMX fournit des outils de mise en œuvre de solutions Web distribuées, dynamiques et modulaires permettant de gérer et contrôler des appareils, applications et réseaux dynamisés par les services. Exemples d'utilisations classiques de la technologie JMX : conseils et modification de la configuration de l'application, collecte de statistiques sur le comportement de l'application, notification de modifications d'état et comportements erronés. Les données sont transférées sur la console de contrôle centralisée.

Access Manager 7.1 utilise la structure de contrôle Java ES pour collecter des statistiques et des données de service, telles que :

- le nombre de tentatives d'authentifications, le nombre d'authentifications réussies et le nombre d'échecs d'authentification ;
- les statistiques de mise en cache des stratégies ;
- les temps de transaction pour l'évaluation des stratégies ;

Sécurité des services Web

Access Manager 7.1 étend les capacités d'authentification aux services Web comme suit :

- affectation de jetons aux messages sortants ;
- évaluation des jetons de sécurité affectés aux messages entrants ;
- activation de la sélection par pointer-cliquer des fournisseurs d'authentification pour les nouvelles applications.

Déploiement d'un fichier WAR unique Access Manager

Access Manager comprend un fichier WAR unique permettant de déployer de façon cohérente les services Access Manager sur n'importe quel conteneur ou plate-forme pris en charge. Le fichier WAR d'Access Manager coexiste avec le programme d'installation Java Enterprise System qui déploie plusieurs fichiers JAR, XML, JSP, HTML, GIF et de propriétés.

Améliorations apportées aux services de base

Conteneurs Web pris en charge

- Sun Java System Web Server 7.0
- Sun Java System Application Server 8.2
- BEA WL 8.1 SP4
- IBM WebSphere 5.1.1.6

Intégration de la structure de contrôle

Access Manager peut utiliser la structure de contrôle JES pour contrôler les éléments suivants :

1. Authentification
   - Nombre de tentatives d'authentification
   - Nombre de tentatives d'authentifications distantes (facultatif)
   - Nombre d'authentifications réussies
   - Nombre d'échecs d'authentification
   - Nombre d'opérations de déconnexion réussies
   - Nombre d'échecs d'opérations de déconnexion
   - Temps de transaction pour chaque module si possible (à l'état En cours d'exécution et En attente)
2. Sessions
   - Taille de la table des sessions (nombre maximal de sessions)
   - Nombre de sessions actives (compteur incrémentiel)
3. Service de profil
   - Taille de cache maximale
   - Temps de transaction pour les opérations (à l'état En cours d'exécution et En attente)
4. Stratégie
   - Demandes d'entrée et de sortie d'évaluation de stratégie
   - Statistiques de pool de connexions de stratégie pour le serveur LDAP du plug-in concerné

Module d'authentification

- Il n'est pas nécessaire que le service d'authentification distribuée s'associe à un serveur pour les déploiements d'équilibrage de charge.
- Il n'est pas nécessaire que le service d'authentification s'associe à un serveur pour les déploiements d'équilibrage de charge.

- Prise en charge de services composites, parmi lesquels le service d'authentification, les agents de stratégie et le service de stratégie. Comprend la condition `AuthenticateToRealm`, la condition AuthenticateToService et la qualification du domaine sur l'ensemble des conditions.
- Organisation des services (conditions d'authentification sur un domaine qualifié)
- Configurations d'authentification / chaînes d'authentification (`AuthServiceCondition`)
- L'authentification modulaire peut maintenant être désactivée si l'enchaînement d'authentification est mis en œuvre.
- Le service d'authentification distribuée prend en charge le mode d'authentification de certification.
- Ajout de `CertAuth` à l'interface d'authentification distribuée pour en faire une présentation d'extracteur d'informations d'identification complète
- Module d'authentification du nouveau magasin de données sous forme de module prêt à l'emploi qui authentifie le magasin de données configuré pour un domaine donné
- Configuration du verrouillage de compte désormais persistante sur plusieurs instances de serveurs AM
- Chaînage de classes SPI de post-traitement

Module de stratégie

- Une nouvelle condition de stratégie `AuthenticateToServiceCondition` est ajoutée, visant à obliger l'authentification de l'utilisateur à une chaîne de service d'authentification spécifique.
- Une nouvelle condition de stratégie `AuthenticateToRealmCondition` est ajoutée, visant à obliger l'authentification de l'utilisateur à un domaine spécifique.
- Une nouvelle condition de stratégie `LDAPFilterCondition` est ajoutée, visant à obliger la correspondance de l'utilisateur avec le fichier ldap indiqué.
- Prise en charge de la comparaison de caractères génériques de premier niveau permettant de faciliter la protection du contenu du répertoire sans avoir besoin de protéger le sous-répertoire.
- Les stratégies peuvent être créées en sous-domaines sans stratégie de référence explicite, à partir d'un domaine parent si la référence de l'alias d'organisation est activée dans la configuration de stratégie globale.
- `AuthLevelCondition` peut spécifier le nom de domaine en plus du niveau d'authentification.
- `AuthSchemeCondition` peut spécifier le nom de domaine en plus de celui du module d'authentification.

Module de gestion des services

- Prise en charge du stockage de la configuration des stratégies/de la gestion des services dans Active Directory

Access Manager SDK

- Prise en charge d'API permettant l'authentification d'utilisateurs sur une base de données de structure de référentiel d'identités par défaut

Prise en charge des services Web

- Fournisseur Liberty ID-WSF SOAP : Fournisseur d'authentification qui encapsule la liaison Liberty ID-WSF SOAP telle qu'elle est mise en œuvre par Access Manager. Il se compose d'un client et d'un fournisseur de services.
- Fournisseur de connexion unique utilisant une couche HTTP : Fournisseur d'authentification utilisant une couche HttpServlet qui encapsule la connexion unique basée sur Access Manager côté serveur

Module d'installation

- Reconditionnement d'Access Manager sous forme d'application J2EE résultant en un fichier WAR unique pour rendre son déploiement possible sur le Web
- Prise en charge de SJS Web Server 7.0 64 bits : prise en charge de JVM 64 bits

Module de délégation

- Prise en charge du groupement de privilèges de délégation

Mise à niveau

- Prend en charge la mise à niveau vers Access Manager 7.1 à partir des versions suivantes : Access Manager 7.0 2005Q4, Access Manager 6.3 2005Q1 et Identity Server 6.2 2004Q2.

Journalisation

- Prise en charge de la délégation dans le module de journalisation : contrôle des identités disposant d'autorisations en écriture ou en lecture depuis les fichiers journaux.
- Prise en charge de `SecureLogHelper` basé sur JCE : permet d'utiliser JCE (en plus de JSS) en tant que fournisseur de sécurité pour la mise en œuvre d'une journalisation sécurisée

Informations et notifications relatives aux fonctions abandonnées

Les API de gestion d'identité de Sun Java(TM) System Access Manager 7.1 et les modèles XML permettent aux administrateurs système de créer, supprimer et gérer des entrées d'identité dans Sun Java System Directory Server. Access Manager fournit également des API de gestion d'identité. Les développeurs utilisent les interfaces publiques et les classes définies dans le

package `com.iplanet.am.sdk` pour intégrer des fonctions de gestion dans des applications ou services externes devant être gérés par Access Manager. Les API d'Access Manager permettent de créer ou supprimer des objets relatifs aux identités ainsi que d'obtenir, modifier, ajouter ou supprimer les attributs des objets à partir de Directory Server.

Le package `com.iplanet.am.sdk` d'Access Manager, plus connu sous le nom AMSDK, ne sera pas inclus dans la prochaine version d'Access Manager. Il comprend tous les API et modèles XML. Aucune option de migration n'est disponible pour le moment et aucune n'est prévue ultérieurement. Les solutions d'approvisionnement de l'utilisateur fournies par Sun Java System Identity Manager sont des remplacements compatibles que vous pouvez commencer à utiliser maintenant. Pour plus d'informations sur Sun Java System Identity Manager, consultez la page `http://www.sun.com/software/products/identity_mgr/index.xml`.

Configurations matérielle et logicielle requises

Le tableau ci-dessous présente les équipements matériels et logiciels requis pour cette version.

TABLEAU 2 Configurations matérielle et logicielle requises

Composant	Configuration requise
Système d'exploitation	■ Solaris™10 SPARC, x86 et x64, avec prise en charge des zones locales et de secours racines. ■ Solaris 9 SPARC et x86. ■ Red Hat™ Enterprise Linux 3 et 4, toutes les mises à jour Advanced Server (versions 32 bits et 64 bits) et Enterprise Server (versions 32 bits et 64 bits) ■ Windows Windows 2000 Advanced Server, Data Center Server version SP4 sur x86 Windows 2003 Standard (versions 32 et 64 bits), Enterprise (versions 32 et 64 bits), Data Center Server (version 32 bits) sur systèmes x86 et x64 Windows XP Professional SP2 sur systèmes x86 HP-UX 11i v1 (11.11 à uname), 64 bits sur PA-RISC 2.0 Pour obtenir la dernière liste à jour des systèmes d'exploitation pris en charge, reportez-vous à "Platform Requirements and Issues" du *Sun Java Enterprise System 5 Release Notes for UNIX* du document *Notes de version de Sun Java Enterprise System 5 pour UNIX* ou à "Hardware and Software Platform Information" du *Sun Java Enterprise System 5 Release Notes for Microsoft Windows* du document *Notes de version de Sun Java Enterprise System 5 pour Windows*.
Java 2 Standard Edition (J2SE)	Plate-forme J2SE 6.0, 5.0 Mise à jour 9 (HP-UX : 1.5.0.03) et 1.4.2 Mise à jour 11
Directory Server	Arborescence d'informations d'Access Manager : Sun Java System Directory Server 6.0 ou Sun Java System Directory Server 5.2 2005Q4 Référentiel d'identités Access Manager : Sun Java System Directory Server 5.2 et 6.0 et Microsoft Active Directory

TABLEAU 2 Configurations matérielle et logicielle requises *(Suite)*

Composant	Configuration requise
Conteneurs Web	Sun Java System Web Server 7.0. Sur les combinaisons de systèmes d'exploitation/plates-formes prises en charge, vous pouvez choisir d'exécuter l'instance Web Server en JVM 64 bits. Plates-formes prises en charge : Solaris 9/SPARC, Solaris 10/SPARC, Solaris 10/AMD64, Red Hat AS ou ES 3.0/AMD64, Red Hat AS ou ES 4.0/AMD64
	Sun Java System Application Server Enterprise Edition 8.2
	BEA WebLogic 8.1 SP4
	IBM WebSphere Application Server 5.1.1.6
RAM	Test de base : 512 Mo
	Déploiement réel : 1 Go pour les threads, Access Manager SDK, le serveur HTTP et d'autres éléments internes
Espace disque	512 Mo pour Access Manager et les applications associées

Pour toute question sur la prise en charge d'autres versions de ces composants, contactez votre représentant technique Sun Microsystems.

Navigateurs pris en charge

Le tableau suivant présente les navigateurs pris en charge par Sun Java Enterprise System 5.

TABLEAU 3 Navigateurs pris en charge

Navigateur	Plate-forme
Firefox 1.0.7	Windows XP
	Windows 2000
	Système d'exploitation Solaris, versions 9 et 10
	Red Hat Linux 3 et 4
	Mac OS X
Microsoft Internet Explorer™ 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows™ 2000

TABLEAU 3 Navigateurs pris en charge *(Suite)*

Navigateur	Plate-forme
Mozilla™ 1.7.12	Système d'exploitation Solaris, versions 9 et 10
	Windows XP
	Windows 2000
	Red Hat Linux 3 et 4
	Mac OS X
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000
Netscape Communicator 7.1	Système d'exploitation Solaris, versions 9 et 10

Informations sur la compatibilité générale

Incompatibilité intersystème AMSDK avec le serveur Access Manager

Les combinaisons suivantes ne sont pas compatibles entre AMSDK et le serveur Access Manager dans les versions Java Enterprise System suivantes :

- Java Enterprise System 2004Q2 AMSDK n'est pas compatible avec le serveur Java Enterprise System 5 Access Manager (la présente version).
- Java Enterprise System 5 AMSDK (la présente version) n'est pas compatible avec le serveur Java Enterprise System Access Manager 2004Q2 (anciennement Identity Server).

Mise à niveau d' Access Manager version HPUX non prise en charge

La mise à niveau d'Access Manager 7 2005Q4 vers Access Manager 7.1 (la présente version) pour HPUX n'est pas prise en charge.

Mode hérité d'Access Manager

Si vous installez Access Manager avec l'un des produits ci-dessous, vous devez activer le mode hérité d'Access Manager (6.x) :

- Sun Java System Portal Server ;
- les serveurs Sun Java System Communications Services, notamment Messaging Server, Calendar Server, Instant Messaging ou Delegated Administrator ;

La méthode de sélection de ce mode dépend du type d'exécution du programme d'installation de Java ES :

- "Installation de Java ES en mode silencieux à l'aide d'un fichier d'état" à la page 15
- "Option d'installation Configurer maintenant en mode graphique" à la page 15
- "Option d'installation Configurer maintenant en mode texte" à la page 16
- "Option d'installation Configurer ultérieurement" à la page 16

Pour déterminer le mode dans lequel Access Manager 7.1 a été configuré, reportez-vous à la section "Détection du mode d'Access Manager" à la page 16.

Installation de Java ES en mode silencieux à l'aide d'un fichier d'état

Le mode silencieux du programme d'installation de Java ES est un mode non interactif qui vous permet d'installer les composants Java ES sur plusieurs serveurs hôtes dont les configurations sont similaires. Vous commencez par exécuter le programme d'installation pour générer un fichier d'état (sans procéder à l'installation des composants), puis vous modifiez une copie du fichier d'état pour chacun des serveurs hôtes sur lesquels vous envisagez d'installer Access Manager et d'autres composants.

Pour sélectionner le mode hérité (6.x) d'Access Manager, définissez le paramètre ci-dessous dans le fichier d'état avant d'exécuter le programme d'installation en mode silencieux :

```
...
AM_REALM = disabled
...
```

Pour obtenir plus d'informations sur l'exécution du programme d'installation de Java ES en mode silencieux à l'aide d'un fichier d'état, consultez le Chapitre 5, "Installing in Silent Mode" du *Sun Java Enterprise System 5 Installation Guide for UNIX*.

Option d'installation Configurer maintenant en mode graphique

Si vous exécutez le programme d'installation de Java ES en mode graphique avec l'option Configurer maintenant, dans l'écran Access Manager : Administration (1 sur 6), sélectionnez Mode hérité (style de version 6.x), qui constitue la valeur par défaut.

Option d'installation Configurer maintenant en mode texte

Si vous exécutez le programme d'installation de Java ES en mode texte avec l'option Configurer maintenant, choisissez la valeur par défaut `Hérité` dans `Mode d'installation (Domaine/Hérité)`.

Option d'installation Configurer ultérieurement

Si vous avez exécuté le programme d'installation de Java ES avec l'option Configurer ultérieurement, vous devez exécuter le script `amconfig` pour configurer Access Manager après son installation. Pour sélectionner le mode Hérité (6.x), définissez le paramètre ci-dessous dans le fichier de saisie du script de configuration (`amsamplesilent`) :

```
...
AM_REALM=disabled
...
```

Pour plus d'informations sur la configuration d'Access Manager via l'exécution du script `amconfig`, reportez-vous au manuel *Sun Java System Access Manager 7.1 Administration Guide* .

Détection du mode d'Access Manager

Pour déterminer le mode dans lequel Access Manager 7.1 a été configuré, appelez :

`http(s)://`*host*`:`*port*`/amserver/SMSServlet?method=isRealmEnabled`

Les résultats possibles sont les suivants :

- true : Mode Domaine
- false : Mode Hérité

Agents de stratégie Access Manager

Le tableau suivant présente la compatibilité des agents de stratégie avec les modes d'Access Manager 7.1.

TABLEAU 4 Compatibilité entre les agents de stratégie et les modes d'Access Manager 7.1

Agent et version	Mode compatible
Agents J2EE et Web, version 2.2	Modes Domaine et Hérité
Les agents Web et J2EE, version 2.1 ne sont pas pris en charge dans Access Manager 7.1	

Problèmes et restrictions connus

Cette section présente les différents problèmes connus au moment de la commercialisation d'Access Manager 7.1, ainsi que leurs solutions, le cas échéant.

Problèmes relatifs à l'installation

Vous trouverez des informations sur les problèmes d'installation de Java System Enterprise dans les notes de version de JES5. Reportez-vous à la section "Access Manager Installation Issues" du *Sun Java Enterprise System 5 Release Notes for UNIX*.

Cette section regroupe les problèmes connus suivants :

Pour pouvoir effectuer le déploiement d'un fichier WAR unique Access Manager sur WebLogic, les fichiers JAX-RPC 1.0 JAR doivent communiquer avec le client SDK (6555040)

Il existe un problème connu avec le fichier WAR unique déployé sur Weblogic 8.1 avec l'initialisation JAX-RPC. Vous devez remplacer les fichiers jar JAX-RCP 1.1 par les fichiers jar JAX-RPC 1.0 pour que Access Manager puisse communiquer avec le client SDK.

Solution :

Il existe deux manières d'obtenir le fichier WAR : avec le programme d'installation de Java Enterprise System 5 avec Access Manager configuré sur l'option Configurer ultérieurement ou via le site de téléchargement Sun.

Si vous avez généré le fichier WAR via le programme d'installation de JES5 avec l'option Configurer ultérieurement :

1. Supprimez les fichiers `.jar` JAXRPC 1.1 suivants de *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib` :
   - `jaxrpc-api.jar`
   - `jaxrpc-spi.jar`
   - `jaxrpc-impl.jar`
2. Copiez les fichiers `.jar` suivants depuis leurs emplacements respectifs vers *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib` :
   - `jaxrpc-api.jar` depuis `/opt/SUNWam/lib/jaxrpc 1.0`
   - `jaxrpc_ri.jar` depuis `/opt/SUNWam/lib/jaxrpc 1.0`
   - `commons-logging.jar` depuis `/opt/SUNWmfwk/lib`
3. Accédez à *AccessManager-base*`/SUNWam/bin/` et exécutez la commande suivante :

   `amconfig –s` *samplesilent*

   Pour plus d'informations sur la configuration de Access Manager via le script amconfig, consultez la section Running the Access Manager amconfig Script du *Guide post-installation d'Access Manager*.

Si vous avez obtenu le fichier WAR via le site de téléchargement Sun (`http://www.sun.com/download/index.jsp`) :

1. Obtenez le fichier *ZIP_ROOT*`/applications/jdk14/amserver.war` et décompressez-le dans une zone de travail, par exemple, `/tmp/am-staging` .
2. Supprimez les fichiers `.jar` JAXRPC 1.1 suivants de `/tmp/am-staging/WEB-INF/lib` :
   - `jaxrpc-api.jar`
   - `jaxrpc-spi.jar`
   - `jaxrpc-impl.jar`

3. Copiez les fichiers `.jar` JAXRPC 1.0 suivants et le fichier journal commun `.jar`, situés dans le répertoire *ZIP_ROOT*`/applications/jdk14/jarFix`, vers `/tmp/am-staging/WEB-INF/lib` :
   - `jaxrpc-api.jar`
   - `jaxrpc-ri.jar`
   - `commons-logging.jar`
4. Reconstituez et déployez le fichier WAR d'Access Manager. Pour plus d'informations, reportez-vous à la section Deploying Access Manager as a Single WAR File du *Guide post-installation d'Access Manager*.

Un fichier .jar supplémentaire est requis pour le fichier WAR unique généré par le programme d'installation de JES 5 pour Websphere 5.1 (6550261)

Si le fichier WAR unique d'Access Manager est généré par le programme d'installation de JES 5 avec l'option Configurer ultérieurement, des fichiers `.jar` supplémentaires sont requis pour le déploiement de Websphere 5.1.

Solution :

1. Copiez `jsr173_api.jar` à partir de `/usr/share/lib` vers le répertoire *AcessManager-base*`/opt/SUNWam/web-src/WEB-INF/lib` .
2. Accédez à *AccessManager-base*`/SUNWam/bin/` et exécutez la commande suivante :

   `amconfig –s` *samplesilent*

   Pour plus d'informations sur la configuration de Access Manager via le script amconfig, consultez la section Running the Access Manager amconfig Script du *Guide post-installation de Access Manager*.

Pour pouvoir déployer un fichier WAR unique pour Webshpere, vous devez apporter des modifications au fichier server.xml pour qu'il puisse communiquer avec le client SDK (6554379)

Pour que le déploiement du fichier WAR unique d'Access Manager avec Websphere 5.1 puisse communiquer correctement avec le client SDK, vous devez apporter des modifications au fichier `server.xml`.

Solution :

Pour modifier le fichier `server.xml` comme il convient, procédez comme suit :

1. Obtenez le fichier `amserver.war`. Il existe deux moyens d'obtenir le fichier WAR unique : via le programme d'installation de JES5 avec l'option Configurer ultérieurement ou via le site de téléchargement Sun.

Remarque – Si vous avez généré le fichier WAR via le programme d'installation de JES5, veillez à effectuer les étapes décrites dans le problème connu n°6550261.

2. Décompressez le fichier WAR d'Access Manager dans une zone de travail, par exemple, `/tmp/am-staging`.
3. Copiez les fichiers `.jar` partagés suivants à partir de `/tmp/am-staging/WEB-INF/lib` vers un emplacement partagé, par exemple, `/export/jars` :

jaxrpc-api.jar	jaxrpc-spi.jar	jaxrpc-impl.jar	saaj-api.jar
saaj-impl.jar	xercesImpl.jar	namespace.jar	xalan.jar
dom.jar	jax-qname.jar	jaxb-api.jar	jaxb-impl.jar
jaxb-libs.jar	jaxb-xjc.jar	jaxr-api.jar	jaxr-impl.jar
xmlsec.jar	swec.jar	acmecrypt.jar	iaik_ssl.jar
iaik_jce_full.jar	mail.jar	activation.jar	relaxngDatatype.jar
xsdlib.jar	mfwk_instrum_tk.jar	FastInfoset.jar	jsr173_api.jar

4. Supprimez les mêmes fichiers `.jar` de `/tmp/am-staging/WEB-INF/lib` dans la zone de travail.
5. Mettez à jour le fichier `server.xml` de l'instance Websphere. Si l'emplacement d'instance par défaut est `/opt/WebSphere/AppServer/config/cells/`*node-name*`/nodes/`*node-name*`/servers/server1` , apportez les modifications à *jvmEntries* dans `server.xml`, comme indiqué ci-dessous :

```
<classpath>/export/jars/jaxrpc-api.jar:/export/jars/jaxrpc-spi.jar:
    /export/jars/jaxrpc-impl.jar:/export/jars/saaj-api.jar:
    /export/jars/saaj-impl.jar:/export/jars/xercesImpl.jar:
    /export/jars/namespace.jar:/export/jars/xalan.jar:/export/jars/dom.jar:
    /export/jars/jax-qname.jar:/export/jars/jaxb-api.jar:/export/jars/jaxb-impl.jar:
    /export/jars/jaxb-libs.jar:/export/jars/jaxb-xjc.jar:/export/jars/jaxr-api.jar:
    /export/jars/jaxr-impl.jar:/export/jars/xmlsec.jar:/export/jars/swec.jar:
    /export/jars/acmecrypt.jar:/export/jars/iaik_ssl.jar:
    /export/jars/iaik_jce_full.jar:/export/jars/mail.jar:
    /export/jars/activation.jar::/export/jars/relaxngDatatype.jar:
    /export/jars/xsdlib.jar:/export/jars/mfwk_instrum_tk.jar:
    /export/jars/FastInfoset.jar:/export/jars/jsr173_api.jar</classpath>
```

6. Redémarrez le conteneur.
7. Reconstituez et déployez le fichier WAR d'Access Manager à partir de /tmp/am-staging. Pour plus d'informations, reportez-vous à la section Deploying Access Manager as a Single WAR File du *Guide post-installation d'Access Manager*.

Modifications requises pour que Distributed Authentication fonctionne avec le fichier WAR unique d'Access Manager pour Weblogic et Websphere (6554372)

Le fichier WAR d'authentification distribuée requiert des fichiers jar supplémentaires pour l'analyse de Weblogic 8.1 et Websphere 5.1, car le conteneur fonctionne avec la version JDK14. Les fichiers `.jar` du JDK14 se trouvent dans le répertoire suivant du fichier `.zip` :

ZIP-ROOT`/applications/jdk14/jarFix`

Solution :

Pour Weblogic 8.1 :

1. Configurez l'authentification distribuée à l'aide des scripts de configuration. Consultez la section Deploying a Distributed Authentication UI Server du *Guide post-installation d'Access Manager*.
2. Décompressez le fichier WAR d'authentification distribuée dans un emplacement temporaire, par exemple, `/tmp/dist-auth`.
3. Copiez `xercesImpl.jar`, `dom.jar` et `xalan.jar` vers le répertoire `/tmp/dist_auth/WEB-INF/lib` à partir de *ZIP-ROOT*`/applications/jdk14/jarFix`.
4. Générez à nouveau le fichier WAR d'authentification distribuée à partir de l'emplacement temporaire et décompressez-le. Pour plus d'informations, consultez la section Deploying a Distributed Authentication UI Server WAR File du *Guide post-installation d'Access Manager*.

Pour Websphere 5.1 :

1. Configurez Distributed Authentication à l'aide des scripts de configuration. Consultez la section Deploying a Distributed Authentication UI Server du *Guide post-installation d'Access Manager*.
2. Décompressez le fichier WAR d'authentification distribuée dans un emplacement temporaire, par exemple, `/tmp/dist-auth`.
3. Copiez `xercesImpl.jar`, `dom.jar` et `xalan.jar` vers le répertoire `/tmp/dist_auth/WEB-INF/lib` à partir de *ZIP-ROOT*`/applications/jdk14/jarFix`.
4. Éditez `WEB-INF/web.xml file` et remplacez `jar://web-app_2_3.dtd` par `http://java.sun.com/dtd/web-app_2_3.dtd .`
5. Générez à nouveau le fichier WAR de Distributed Authentication à partir de l'emplacement temporaire et décompressez-le. Pour plus d'informations, consultez la section Deploying a Distributed Authentication UI Server WAR File du *Guide post-installation d'Access Manager*.

Échec de la configuration du fichier WAR unique sur DS (6562076)

Access Manager déployé en tant que fichier WAR unique ne peut être configuré sur Directory Server 6 avec un suffixe de racine de composant unique, par exemple. `dc=example`. La configuration fonctionne toutefois avec le suffixe de racine de composants multiples, par exemple, `dc=example,dc=com` .

Solution : Utilisez le suffixe de racine de composants multiples, par exemple, `dc=example,dc=com`.

La configuration multi-serveurs du fichier WAR unique d'AM sur le même hôte génère une exception (6490150)

Lors de la configuration de la seconde instance du fichier WAR unique d'Access Manager sur le même hôte de Directory Server, une exception est générée lors de la mise à jour de l'alias d'organisation. Ce problème ne se produi pas si la seconde instance configurée se trouve sur un hôte différent.

Problèmes relatifs à la mise à niveau

Des informations sur les problèmes de mise à niveau sont proposées dans la section “Upgrade Issues” du *Sun Java Enterprise System 5 Release Notes for UNIX* du document *Notes de version de Sun Java Enterprise System 5 pour UNIX*.

Problèmes de compatibilité

Échec de la connexion unique d'Access Manager sur Universal Web Client (6367058, 6429573)

Ce problème apparaît lorsque vous installez le patch JES5 120955-01après avoir installé Access Manager, Messaging Server et Calendar Server et les avoir configurés pour qu'ils fonctionnent

ensemble. L'utilisateur rencontre une erreur à la connexion. Cette erreur est due à une incompatibilité entre les propriétés de l'agent de stratégie 2.1 et AMSDK. Il n'existe aucune solution à l'heure actuelle.

Une erreur StackOverflowError se produit sur Web Server 7.0 lorsqu'il s'exécute en mode 64 bits (6449977)

Si Access Manager est configuré sur une instance de Web Server 7.0 avec JVM 64 bits, l'utilisateur rencontre un message d'erreur du serveur lorsqu'il accède à la page de connexion à la console. Le journal des erreurs de Web Server contient une exception `StackOverflowError`.

Solution : Modifiez la configuration de Web Server en procédant comme indiqué ci-après :

1. Connectez-vous à la console d'administration de Web Server en tant qu'administrateur Web Server.
2. Cliquez sur Modifier la configuration.

   Dans le champ Plate-forme, sélectionnez 64 puis cliquez sur Enregistrer.
3. Cliquez sur l'onglet Java puis sur l'onglet Paramètres JVM.
   - Sous Options, recherchez la taille de tas minimale (par exemple : -Xms). La valeur de la taille de tas minimale doit être d'au moins 512m. Par exemple, si la valeur de la taille de tas n'est pas d'au moins -Xms512m, modifiez-la pour qu'elle le soit.
   - La valeur de la taille de tas minimale doit être d'au moins 768m. Si la valeur de la taille de tas n'est pas d'au moins -Xmx768m, modifiez-la pour qu'elle le soit.
   - Définissez la taille de la pile Java sur 512k ou 768k à l'aide de `-Xss512k` ou `-Xss768k`. Vous pouvez conserver la taille par défaut pour JVM 64 bits sur Solaris Sparc (1024k) en laissant le champ vide.
4. Cliquez sur l'onglet Performance, puis sur le lien Paramètres du pool de threads."

   Modifiez la valeur de la taille de pile sur au moins 261144 puis cliquez sur Enregistrer.
5. Cliquez sur le lien En attente de déploiement dans le coin supérieur droit de l'écran.

   Dans la page Déploiement de la configuration, cliquez sur le bouton Déployer.
6. Dans la fenêtre Résultats, cliquez sur OK pour redémarrer l'instance de Web Server.

   Cliquez sur Fermer dans la fenêtre Résultats après le redémarrage de Web Server.

En mode Hérité, il existe des incompatibilités dans le module d'authentification principale (6305840)

Le mode Hérité d'Access Manager 7.1 présente les incompatibilités suivantes dans le module d'authentification principale d'Access Manager 6 2005Q1 :

- Les modules d'authentification des organisations sont supprimés en mode hérité.

- La présentation des configurations d'authentification des administrateurs et des organisations a été modifiée. Dans la console Access Manager 7.1, la liste déroulante est paramétrée par défaut sur `ldapService`. Dans la console Access Manager 6 2005Q1, le bouton Modifier apparaît et le module LDAP n'a pas été sélectionné par défaut.

Solution : aucune.

La commande `commadmin` de l'utilitaire Delegated Administrator ne parvient pas à créer un utilisateur (6294603)

La commande `commadmin` de l'utilitaire Delegated Administrator, utilisée avec l'option `-S mail,cal`, ne permet pas de créer un utilisateur dans le domaine par défaut.

Solution : Ce problème apparaît si vous effectuez une mise à niveau vers Access Manager version 7.1, mais que vous ne mettez pas à niveau Delegated Administrator.

Si vous ne souhaitez pas mettre à niveau Delegated Administrator, suivez la procédure ci-après :

1. Dans le fichier `UserCalendarService.xml`, définissez les attributs `mail`, `icssubcribed` et `icsfirstday` comme facultatifs au lieu de requis. Ce fichier se trouve par défaut dans le répertoire `/opt/SUNWcomm/lib/services/` des systèmes Solaris.
2. Dans Access Manager, supprimez le fichier XML existant en exécutant la commande `amadmin`, comme suit :

   ```
   # ./amadmin -u amadmin -w password -r UserCalendarService
   ```

3. Dans Access Manager, ajoutez le fichier XML mis à jour, comme suit :

   ```
   # ./amadmin -u amadmin -w password
   -s /opt/SUNWcomm/lib/services/UserCalendarService.xml
   ```

4. Redémarrez le conteneur Web d'Access Manager.

La commande `commadmin` de l'utilitaire Delegated Administrator ne parvient pas à créer une organisation (6292104)

La commande `commadmin` de l'utilitaire Delegated Administrator, utilisée avec l'option `-S mail,cal`, ne permet pas de créer une organisation.

Solution : Reportez-vous à la solution du précédent problème.

Problèmes de configuration

Redirection de console incorrecte derrière un équilibreur de charge (6480354)

Si vous avez déployé des instances Access Manager derrière un équilibreur de charge, vous risquez d'être redirigé vers une des instances Access Manager plutôt que vers l'équilibreur de charge lors de la connexion à la console Access Manager. L'URL dans le navigateur correspond également à l'instance Access Manager. Par exemple, ce problème peut se produire si vous vous connectez à la console via l'URL suivant :

```
http://loadbalancer.example.com/amserver/realm
```

Cette redirection peut se produire lors de déploiements en mode Domaine comme en mode Hérité.

Il existe deux solutions à ce problème. Vous pouvez utiliser indifféremment l'une ou l'autre :

1. Connectez-vous avec l'un des URL suivants :

   `http://` *loadbalancer*`/amserver/UI/Login`

   `http://` *loadbalancer*`/amserver`

2. Dans `AMConfig.properties`, définissez la propriété `com.sun.identity.loginurl` sur le nom de l'équilibreur de charge. Vous devez procéder à cette manipulation pour chaque instance d'Access Manager derrière l'équilibreur de charge.

L'URL de notification doit être mise à jour pour l'installation d'Access Manager SDK sans conteneur Web (6491977)

Si vous installez Access Manager SDK sans conteneur Web en exécutant le programme d'installation Java ES 5 via l'option Configurer maintenant, la propriété `com.iplanet.am.notification.url` du fichier AMConfig.properties est définie sur `NOTIFICATION_URL`. Si ne procédez à aucune autre configuration de conteneur Web, les utilisateurs ne recevront aucune notification du serveur Access Manager distant.

Solution : Réinitialisez cette propriété comme suit : `com.iplanet.am.notification.url=""`

Le service de réinitialisation du mot de passe signale des erreurs de notification lors de la modification d'un mot de passe (6455079)

Lors de la modification d'un mot de passe, Access Manager envoie la notification par e-mail en utilisant un nom d'expéditeur non qualifié `Identity-Server`, ce qui provoque des erreurs d'entrées dans les journaux `amPasswordReset`. Exemple :

```
07/19/2006 10:26:04:010 AM PDT: Thread[service-j2ee,5,main]
ERROR: Could not send email to user [Ljava.lang.String;@999262
com.sun.mail.smtp.SMTPSendFailedException: 553 5.5.4 <Identity-Server>...
Domain name required for sender address Identity-Server
```

Solution : Modifiez la configuration dans `/opt/SUNWam/locale/amPasswordResetModuleMsgs.properties.`

- Modifiez l'adresse de l'expéditeur. Modifiez `fromAddress.label=<Identity-Server>` en `fromAddress.label=<IdentityServer@myhost.company.com>`
- Modifiez la propriété `lockOutEmailFrom` pour assurer que les notifications de verrouillage utilisent l'adresse de correcte.

La liste des serveurs de plate-forme et l'attribut d'alias FQDN ne sont pas mis à jour (6309259, 6308649)

Dans le cadre d'un déploiement avec plusieurs serveurs, la liste des serveurs de plate-forme et l'attribut d'alias FQDN ne sont pas mis à jour si vous installez Access Manager sur le deuxième serveur et les suivants.

Solution : Ajoutez manuellement les alias DNS et de domaine, ainsi que les entrées de la liste des serveurs de plate-forme. Pour connaître la procédure, consultez la section “Adding Additional Instances to the Platform Server List and Realm/DNS Aliases” du *Sun Java System Access Manager 7.1 Postinstallation Guide*.

Validation de données d'attributs requis dans les services (6308653)

Avec Access Manager 7.1, les attributs requis dans les fichiers XML des services doivent utiliser les valeurs par défaut.

Solution : Si un service comporte des attributs sans valeur, ajoutez des valeurs à ces attributs, puis relancez le service.

Exception lors du déploiement sur une instance WebLogic 8.1 sécurisée (6295863)

Si vous déployez Access Manager 7.1 sur une instance BEA WebLogic 8.1 SP4 sécurisée (SSL activé), une exception est générée au cours du déploiement de chacune des applications Web d'Access Manager.

Solution : Procédez comme suit :

1. Appliquez le patch de WebLogic 8.1 SP4, `CR210310_81sp4.jar`, disponible auprès de BEA.
2. Dans le script `/opt/SUNWam/bin/amwl81config` (système Solaris) ou `/opt/sun/identity/bin/amwl81config` (système Linux), mettez à jour les fonctions `doDeploy` et `undeploy_it` de manière à ajouter le chemin d'accès au fichier JAR du patch à la variable `wl8_classpath` , qui contient la variable `classpath` utilisée pour déployer et annuler le déploiement des applications Web d'Access Manager.

   Trouvez la ligne contenant la variable `wl8_classpath` :

   ```
   wl8_classpath= ...
   ```
3. Immédiatement à la suite de la ligne trouvée à l'étape 2, ajoutez la ligne suivante :

   ```
   wl8_classpath=path-to-CR210310_81sp4.jar:$wl8_classpath
   ```

Le script `amconfig` ne met pas à jour les alias DNS et de domaine, ni les entrées de la liste des serveurs de plate-forme (6284161)

Dans le cadre d'un déploiement sur plusieurs serveurs, le script `amconfig` ne met pas à jour les alias DNS et de domaine, ni les entrées de la liste des serveurs de plate-forme pour les instances Access Manager supplémentaires.

Solution : Ajoutez manuellement les alias DNS et de domaine, ainsi que les entrées de la liste des serveurs de plate-forme. Pour connaître la procédure, consultez la section “Adding Additional Instances to the Platform Server List and Realm/DNS Aliases” du *Sun Java System Access Manager 7.1 Postinstallation Guide*.

Dans le modèle de fichier d'état de configuration, le mode Domaine est le mode par défaut d'Access Manager (6280844)

Par défaut, le mode Domaine (variable `AM_REALM`), d'Access Manager est activé dans le modèle de fichier d'état de configuration.

Solution : Pour installer ou configurer Access Manager en mode hérité, vous devez réinitialiser la variable dans le fichier d'état :

```
AM_REALM = disabled
```

Problèmes de performance

En mode Domaine, lorsque vous créez un nouveau groupe, un administrateur de groupe avec des listes de contrôle d'accès qui ne seront jamais utilisées est créé (6485695)

Si vous installez Access Manager en mode Domaine, dès qu'un nouveau groupe est créé, Access Manager crée de manière dynamique un nouvel administrateur de groupe, disposant des listes de contrôle d'accès nécessaires à la gestion du groupe. En mode Domaine, ces listes de contrôle d'accès de l'administrateur de groupe ne sont pas utilisées. Cependant, Directory Server analyse ces listes lors du traitement d'entrées avec suffixe. Cela risque de faire baisser les performances d'Access Manager, notamment lorsqu'un nombre important de groupes est généré au cours d'un déploiement.

Solution : La résolution de ce problème s'effectue en deux étapes :

- empêcher Access Manager de créer un administrateur de groupe et les listes de contrôle d'accès correspondantes chaque fois qu'un groupe est créé
- supprimer toutes les listes de contrôle d'accès existantes de Directory Server

Empêcher la création de listes de contrôle d'accès pour les administrateurs de groupe

La procédure suivante vous permet d'empêcher Access Manager de créer un administrateur de groupe et les listes de contrôle d'accès correspondantes chaque fois qu'un groupe est créé.

Remarque – En suivant cette procédure, aucun administrateur de groupe ou liste de contrôle correspondante ne sera générée lors de la création d'un groupe. N'utilisez cette procédure que si elle est appropriée à votre déploiement.

---

1. Sauvegardez le fichier `amAdminConsole.xml`. Ce fichier figure dans le répertoire suivant, en fonction de votre plate-forme :
   - Systèmes Solaris : `/etc/opt/SUNWam/config/xml`
   - Systèmes Linux et HP-UX : `/etc/opt/sun/identity/config/xml`
   - Systèmes Windows : *javaes-install-dir*`\identity\config\xml`

     javaes-install-dir correspond au répertoire d'installation Java ES 5. La valeur par défaut est `C:\Program Files\Sun\JavaES5`.
2. Dans le fichier `amAdminConsole.xml`, supprimez l'entrée suivante, délimitée par les lignes de commentaires :

```
<AttributeSchema name="iplanet-am-admin-console-dynamic-aci-list"
    type="list"
    syntax="string"
    i18nKey="g111">
```

```
    <DefaultValues>
...
# Début de l'entrée à supprimer
                <Value>Group Admin|Group Admin Description|ORGANIZATION:aci:
(target="ldap:///GROUPNAME")(targetattr = "*")
(version 3.0; acl "Group and people container admin role";
allow (all) roledn = "ldap:///ROLENAME";)##ORGANIZATION:aci:
(target="ldap:///ORGANIZATION")
(targetfilter=(&amp;FILTER(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Policy Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Organization Admin Role,ORGANIZATION)
(nsroledn=cn=Container Admin Role,ORGANIZATION)
(nsroledn=cn=Organization Policy Admin Role,ORGANIZATION)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members"; allow (read,write,search)
roledn = "ldap:///ROLENAME";)</Value>
# Fin de l'entrée à supprimer
...
    </DefaultValues>
</AttributeSchema>
```

3. Utilisez `amadmin` pour supprimer le service Admin Console d'Access Manager. Par exemple, sur les systèmes Solaris :

   ```
   # cd /opt/SUNWam/bin
   # ./amadmin -u amadmin -w amadmin_password
   --deleteService iPlanetAMAdminConsoleService
   ```

4. Utilisez `amadmin` pour recharger le service Admin Console dans Access Manager à partir du fichier `amAdminConsole.xml` de l'étape 2. Par exemple :

   ```
   # ./amadmin -u amadmin -w amadmin_password
   -t /etc/opt/SUNWam/config/xml/amAdminConsole.xml
   ```

5. Redémarrez le conteneur Web d'Access Manager. (Comme décrit dans la procédure suivante, si vous prévoyez de supprimer les listes de contrôle d'accès de Directory Server, patientez et redémarrez le conteneur Web à la fin de cette procédure.)

Supprimer des listes de contrôles d'administrateurs de groupe existantes

Remarque – La procédure suivante utilise les utilitaires `ldapsearch` et `ldapmodify` pour rechercher et supprimer les listes de contrôle d'accès. Si votre déploiement utilise Directory Server 6.0, vous pouvez également utiliser Directory Server Control Center (DSCC) ou la commande `dsconf` pour effectuer ces actions. Pour plus d'informations, reportez-vous à la documentation de Directory Server 6.0 :

`http://docs.sun.com/app/docs/coll/1224.1`

La procédure suivante permet de supprimer toutes les listes de contrôle d'accès de Directory Server.

1. Créez un fichier LDIF à utiliser avec `ldapmodify` pour supprimer les listes de contrôle des administrateurs de groupe. Pour trouver ces listes, utilisez `ldapsearch` (ou un autre outil de recherche de répertoire).

   Par exemple, les entrées suivantes du fichier LDIF type nommé `Remove_Group_ACIs.ldif` supprimeront les listes de contrôle d'un groupe nommé New Group :

```
dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///cn=New Group,ou=Groups,o=isp")(targetattr = "*")
(version 3.0; acl "Group and people container admin role"; allow (all)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///ou=People,o=isp")(targetattr="nsroledn")
(targattrfilters="add=nsroledn:(!(nsroledn=*)),
del=nsroledn:(!(nsroledn=*))") (version 3.0;
acl "Group admin's right to add user to people container"; allow (add)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///o=isp")
(targetfilter=(&(|(memberof=*cn=New Group,ou=Groups,o=isp)
(iplanet-am-static-group-dn=*cn=New Group,ou=Groups,o=isp))
(!(|(nsroledn=cn=Top-level Admin Role,o=isp)
(nsroledn=cn=Top-level Help Desk Admin Role,o=isp)
(nsroledn=cn=Top-level Policy Admin Role,o=isp)
(nsroledn=cn=Organization Admin Role,o=isp)(
nsroledn=cn=Container Admin Role,o=isp)
(nsroledn=cn=Organization Policy Admin Role,o=isp)))))
```

```
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list ||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members";
allow (read,write,search)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)
aci: (target="ldap:///o=isp")(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the root suffix";
allow (all) userdn = "ldap: ///cn=dsameuser,ou=DSAME Users,o=isp"; )
```

2. Utilisez `ldapmodify` avec le fichier LDIF de l'étape précédente pour supprimer les listes de contrôle d'accès Group de Directory Server. Exemple :

```
# ldapmodify -h ds-host -p 389 -D "cn=Directory Manager"
-w ds-bind-password -f Remove_Group_ACIs.ldif
```

3. Redémarrez le conteneur Web d'Access Manager.

Problèmes liés à la console Access Manager

La nouvelle console Access Manager ne permet pas de définir les priorités du modèle CoS (6309262)

La nouvelle console Access Manager 7.1 ne peut pas définir ou modifier la priorité d'un modèle de classe de service (COS).

Solution : Connectez-vous à la console Access Manager 6 2005Q1 pour définir ou modifier la priorité du modèle CoS.

L'ancienne console apparaît lors de l'ajout de services associés à Portal Server (6293299)

Portal Server et Access Manager sont installés sur le même serveur. En mode hérité, vous vous connectez à la nouvelle console Access Manager en utilisant `/amserver`. Si vous choisissez un utilisateur existant et que vous essayez d'ajouter des services (tels que NetFile ou Netlet), l'ancienne console Access Manager (`/amconsle`) apparaît.

Solution : aucune. La version actuelle de Portal Server requiert la console Access Manager 6 2005Q1.

La console ne renvoie pas les résultats de Directory Server, une fois la limite des ressources atteinte (6239724)

Installez Directory Server, puis Access Manager avec l'option d'arborescence d'informations d'annuaire (DIT) existante. Connectez-vous à la console Access Manager et créez un groupe. Modifiez les utilisateurs du groupe. Par exemple, ajoutez des utilisateurs avec le filtre `uid=*999*`. La zone de liste qui en résulte est vide, mais la console n'affiche aucune erreur ou information, ni aucun message d'avertissement.

Solution : La taille du groupe ne doit pas dépasser la taille limite de la recherche Directory Server. Si la taille du groupe est supérieure, modifiez la taille limite de la recherche en conséquence.

Ajout de l'attribut `ContainerDefaultTemplateRole` après la migration des données (4677779)

En mode Hérité, le rôle de l'utilisateur n'apparaît pas sous une organisation qui n'a pas été créée dans Access Manager. En mode de débogage, le message suivant apparaît :

```
ERROR: DesktopServlet.handleException()
com.iplanet.portalserver.desktop.DesktopException:
DesktopServlet.doGetPost(): no privilige to execute desktop
```

Cette erreur devient évidente après l'exécution des scripts de migration du programme d'installation de Java ES. L'attribut `ContainerDefaultTemplateRole` n'est pas ajouté automatiquement à l'organisation lorsque cette dernière est migrée depuis une arborescence d'informations d'annuaire existante ou depuis une autre source.

Solution : Utilisez la console Directory Server pour copier l'attribut `ContainerDefaultTemplateRole` depuis une autre organisation Access Manager, puis ajoutez-le à l'organisation affectée.

Problème de ligne de commande

Échec de création d'un nouvel utilisateur via le rôle d'administration de l'organisation à l'aide de l'utilitaire de ligne de commande amadmin (6480776)

Un administrateur doté du rôle d'administration de l'organisation ne peut pas créer un nouvel utilisateur à l'aide de l'utilitaire de ligne de commande amadmin en raison de privilèges de connexion incorrects.

Solution: L'administrateur de l'organisation et l'administrateur de niveau supérieur peuvent définir les autorisations. Pour cela, via la console d'administration :

1. Accédez à l'organisation à laquelle l'administrateur de l'organisation appartient.
2. Cliquez sur l'onglet Privilèges.
3. Cliquez sur le lien du rôle d'administration de l'organisation.
4. Sélectionnez `Read and write access to all log files` ou `Write access to all log files`.
5. Cliquez sur Enregistrer.

Problèmes liés au SDK et au client

Les clients ne reçoivent pas de notifications après le redémarrage du serveur (6309161)

Les applications écrites à l'aide du SDK client (`amclientsdk.jar`) ne reçoivent pas de notifications lorsque le serveur redémarre.

Solution : aucune.

Redémarrer les clients SDK après une modification du schéma de service (6292616)

Si vous modifiez un schéma de service, `ServiceSchema.getGlobalSchema` renvoie l'ancien schéma et non le nouveau.

Solution : Redémarrez le client après avoir modifié un schéma de service.

Ce problème est résolu dans le patch 1.

Problèmes d'authentification

Les performances du serveur d'interface d'authentification distribuée baissent lorsque l'utilisateur ne dispose pas de privilèges suffisants (6470055)

Lorsque vous déployez le serveur d'interface utilisateur d'authentification distribuée à l'aide de l'utilisateur de l'application par défaut, les performances baissent de façon significative en raison des privilèges restreints de l'utilisateur de l'application.

Solution : Créez un nouvel utilisateur disposant des privilèges appropriés.

Création d'un nouvel utilisateur avec les ACI appropriées

1. Dans la console Access Manager, créez un nouvel utilisateur. Par exemple, créez un utilisateur nommé `AuthUIuser`.
2. Dans la console Directory Server, ajoutez l'ACI suivante.

   ```
   dn:ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>
   changetype:modifyadd:aci
   aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>")
   (targetattr = "*"(version 3.0; acl "SunAM client data anonymous access";
   allow (read, search, compare) userdn = "ldap:///<AuthUIuser's DN>";)
   ```

   Notez que `userdn` est défini sur `"ldap:///<AuthUIuser's DN>"`.
3. Consultez les instructions dans la section “To Install and Configure a Distributed Authentication UI Server” du *Sun Java System Access Manager 7.1 Postinstallation Guide* pour modifier le fichier `amsilent` et exécuter la commande `amadmin`.
4. Dans le fichier `amsilent`, définissez les propriétés suivantes :

APPLICATION_USER	Saisissez `AuthUIuser`.
APPLICATION_PASSWD	Saisissez un mot de passe pour `AuthUIuser`.

5. Enregistrez le fichier.
6. Exécutez le script `amconfig` à l'aide du nouveau fichier de configuration. Par exemple, sur un système Solaris avec Access Manager installé dans le répertoire par défaut.

   ```
   # cd /opt/SUNWam/bin
   # ./amconfig -s ./DistAuth_config
   ```
7. Redémarrez le conteneur Web sur le serveur d'interface utilisateur d'authentification distribuée.

Incompatibilité entre la configuration par défaut du service des statistiques et le mode hérité d'Access Manager (6286628)

À l'issue de l'installation d'Access Manager en mode hérité, la configuration par défaut du service des statistiques a été modifiée :

- Le service est activé par défaut (`com.iplanet.services.stats.state=file`). Auparavant, il était désactivé.
- L'intervalle par défaut (`com.iplanet.am.stats.interval`) est passé de 3600 à 60.
- Le répertoire de statistiques par défaut (`com.iplanet.services.stats.directory`), `/var/opt/SUNWam/debug`, a été remplacé par `/var/opt/SUNWam/stats`.

Solution : aucune.

Principe d'unicité des attributs non appliqué aux attributs de dénomination dans l'organisation de niveau supérieur (6204537)

Après avoir installé Access Manager, connectez-vous en tant qu'utilisateur `amadmin` et ajoutez les attributs `o`, `sunPreferredDomain`, `associatedDomain`, `sunOrganizationAlias`, `uid` et `mail` à la liste des attributs uniques. Si vous créez deux nouvelles organisations avec le même nom, l'opération échoue, mais Access Manager affiche le message “L'organisation existe déjà.” au lieu du message “Unicité d'attribut violée”.

Solution : aucune. Ignorez le message. Access Manager fonctionne correctement.

Problèmes de session et de connexion unique

Le système crée un nom d'hôte de service non valide lorsque l'équilibreur de charge dispose d'une terminaison SSL (6245660)

Si vous déployez Access Manager en utilisant Web Server comme conteneur Web avec un équilibreur de charge doté d'une terminaison SSL, les clients ne sont pas dirigés vers la page Web Server appropriée. Si vous cliquez sur l'onglet Sessions dans la console Access Manager, une erreur est renvoyée, car l'hôte n'est pas valide.

Solution : Dans les exemples suivants, Web Server écoute sur le port 3030. L'équilibreur de charge écoute sur le port 80 et redirige les requêtes vers Web Server.

Dans le fichier *web-server-instance-name*`/config/server.xml`, vous devez modifier l'attribut `servername` de sorte qu'il désigne l'équilibreur de charge, en fonction de la version Web Server utilisée.

Avec les versions Web Server 6.1 Service Pack (SP), modifiez l'attribut `servername`, de la manière suivante :

```
<LS id="ls1" port="3030" servername="loadbalancer.example.com:80"
defaultvs="https-sample" security="false" ip="any" blocking="false"
acceptorthreads="1"/>
```

Les versions Web Server 6.1 SP2 (ou ultérieures) peuvent modifier le protocole `http` en `https` ou `https` en `http`. Par conséquent, modifiez l'attribut `servername` comme suit :

```
<LS id="ls1" port="3030"
servername="https://loadbalancer.example.com:443" defaultvs="https-sample"
security="false" ip="any" blocking="false" acceptorthreads="1"/>
```

Utilisation de `HttpSession` avec des conteneurs Web tiers

La méthode par défaut de maintenance de sessions pour l'authentification est la session interne et non pas `HttpSession`. La valeur maximale de session non valide par défaut de trois minutes est suffisante. Le script `amtune` définit la valeur sur une minute pour Web Server ou Application Server. Toutefois, si vous utilisez un conteneur Web tiers (IBM WebSphere ou BEA WebLogic Server) et l'option `HttpSession`, il se peut que vous deviez limiter le temps `HttpSession` maximum du conteneur Web pour éviter les problèmes de performances.

Problèmes liés aux stratégies

- "La suppression des attributs dynamiques dans le service de configuration des stratégies entraîne des problèmes de modification des stratégies (6299074)" à la page 36

La suppression des attributs dynamiques dans le service de configuration des stratégies entraîne des problèmes de modification des stratégies (6299074)

La suppression des attributs dynamiques dans le service de configuration des stratégies entraîne des problèmes de modification des stratégies dans le scénario suivant :

1. Vous créez deux attributs dynamiques dans le service de configuration des stratégies.
2. Vous créez une stratégie et sélectionnez les attributs dynamiques de l'étape 1 dans le fournisseur de réponses.
3. Vous supprimez les attributs dynamiques du service de configuration des stratégies et créez deux autres attributs.
4. Vous essayez ensuite de modifier la stratégie créée à l'étape 2.

Les résultats possibles sont les suivants : "Erreur. Tentative de définition d'une propriété dynamique non valide."Aucune stratégie n'a été affichée dans la liste par défaut. Si vous effectuez une recherche, les stratégies s'affichent, mais vous ne pouvez pas modifier ou supprimer les stratégies existantes, ni en créer une autre.

Solution : Avant de supprimer les attributs dynamiques du service de configuration des stratégies, supprimez les références à ces attributs dans les stratégies.

Problèmes liés au démarrage du serveur

Débogage d'erreur au démarrage d'Access Manager (6309274, 6308646)

Lors du démarrage d'Access Manager 7.1, les erreurs de débogage sont renvoyées dans les fichiers de débogage `amDelegation` et `amProfile` :

- `amDelegation` : Impossible d'obtenir une instance de plug-in pour la délégation
- `amProfile` : Exception de délégation

Solution : aucune. Ne tenez pas compte de ces messages.

Problèmes AMSDK

Erreur affichée lors de l'exécution de AMIdentity.modifyService (6506448)

Si vous utilisez `AMIdentity.modifyService` pour définir un attribut dynamique de service de bureau sur un domaine, Access Manager renvoie une exception de pointeur nul.

Solution : Ajoutez la propriété suivante au fichier `AMConfig.properties` et redémarrez le serveur.:

```
com.sun.am.ldap.connnection.idle.seconds=7200
```

Les membres du groupe ne s'affichent pas dans la liste sélectionnée (6459598)

Ce problème apparaît dans les circonstances ci-dessous.

1. Définissez un domaine avec la configuration suivante :
   - `amroot` est le domaine supérieur. `example.com` est un sous-domaine.
   - Le sous-domaine `example.com` dispose de deux magasins de données : `exampleDB` et `exampledminDB`.
   - Le magasin de données `exampleDB` contient tous les utilisateurs démarrant à `dc=example,dc=com`. Les opérations LDAPv3 prises en charge sont définies sur `user=read,write,create,delete,service.`
   - Le magasin de données `exampleadminDB` contient un groupe d'administration du domaine. Ce groupe d'administration est `DN: cn=example.com Realm Administrators,ou=Groups,dc=example,dc=com`. Ce groupe dispose d'un membre unique, `scarter`. Les opérations LDAPv3 prises en charge sont définies sur `group=read,write,create,delete`.
2. Cliquez sur l'onglet Objets, sur l'onglet Groupes, puis sur l'entrée correspondant à `example.com Realm Administrators`.
3. Cliquez sur l'onglet Utilisateur.

Tous les utilisateurs du magasin de données `exampleDB` s'affichent comme étant disponibles, mais `scarter` ne s'affiche pas dans le champ Sélectionné.

Solution : Ajoutez l'opération `user=read` aux opérations LDAPv3 prises en charge dans le magasin de données `exampleadminDB` .

L'URL de connexion à Access Manager renvoie le message « Aucune organisation de ce type n'a été trouvée » (6430874)

Le problème est peut-être dû à la présence de caractères en casse mixte (mélange de majuscules et minuscules) dans le nom de domaine complet (FQDN).

Exemple : `HostName.PRC.Example.COM`

Solution : Après l'installation, n'utilisez pas l'URL de connexion à Access Manager. À la place, dans l'URL de connexion, indiquez l'emplacement LDAP de l'organisation par défaut. Exemple :

```
http://HostName.PRC.Example.COM/amserver/UI/Login?org=dc=PRC,dc=Example,dc=COM
```

Une fois que vous êtes connecté à Access Manager, vous n'avez plus besoin de saisir le chemin complet de l'organisation de l'utilisateur à chaque connexion à Access Manager. Procédez comme suit :

1. Accédez à l'onglet Domaine en mode Domaine ou accédez à l'onglet Organisation en mode Hérité.
2. Cliquez sur le nom du domaine ou de l'organisation par défaut.

   Dans cet exemple, cliquez sur `prc`.
3. Modifiez tous les caractères majuscules dans la valeur `Realm/DNS Alias` en caractères minuscules.

   Dans cet exemple, ajoutez la valeur en minuscules uniquement `hostname.prc.example.com` à la liste, puis supprimez de la liste la valeur en casse mixte `HostName.PRC.Example.COM` .
4. Cliquez sur Enregistrer puis déconnectez-vous de la console Access Manager.

Vous pouvez désormais vous connecter en utilisant l'un des URL suivants :

- `http://hostname.PRC.Example.COM/amserver/UI/Login`
- `http://hostname.PRC.Example.COM/amserver`
- `http://hostname.PRC.Example.COM/amserver/console`

Impossible de créer une sous-organisation à partir d'Access Manager à l'aide d'`amadmin` (5001850)

Ce problème apparaît lorsque la réplication multimaître est activée entre deux Directory Server et que vous tentez de créer une sous-organisation à l'aide de l'utilitaire `amadmin`.

Solution : Dans les deux Directory Servers, définissez la propriété `nsslapd-lookthroughlimit` sur -1.

Problème concernant SSL

- "Échec du script amconfig lors de l'expiration du certificat SSL (6488777)" à la page 39

Échec du script amconfig lors de l'expiration du certificat SSL (6488777)

Si le conteneur Access Manager s'exécute en mode SSL et que le certificat SSL du conteneur est expiré, `amconfig` échoue et risque de provoquer une corruption de classpath.

Solution : Si vous avez déjà exécuté `amconfig` avec un certificat expiré et que le classpath est corrompu, obtenez tout d'abord un certificat SSL valide. Reprenez le fichier `domain.xml` d'origine ou une copie du fichier `domain.xml` dans lequel le classpath n'est pas corrompu. Réexécutez ensuite la commande `amconfig` :

```
/opt/SUNWam/bin/amconfig -s $PWD/amsamplesilent
```

Exemples de problèmes

Le répertoire d'exemples Clientsdk contient un fichier makefile indésirable (6490071)

Des exemples de fichiers sont inclus dans le SDK Client. Ils illustrent comment écrire des programmes indépendants et des applications Web. Les exemples se trouvent dans le répertoire dans lequel vous avez généré le fichier `Makefile.clientsdk`, ainsi que dans les sous-répertoires suivants :

```
.../clientsdk-samples/

.../clientsdk-webapps/
```

Clientsdk-samples inclut des exemples de programmes d'authentification, de journalisation, de stratégie et SAML indépendants. Clientsdk-webapps inclut des exemples de programmes de gestion des utilisateurs, de gestion de services et de stratégie. Chaque exemple comporte un fichier Readme.html contenant des instructions sur la compilation et l'exécution du programme en exemple.

Pour compiler les exemples, exécutez le fichier makefile du sous-répertoire correspondant. Le fichier makefile de niveau supérieur ne permet pas de compiler les exemples des sous-répertoires.

Problèmes concernant le système d'exploitation Linux

Des problèmes surviennent sur Java Virtual Machine (JVM) lors de l'exécution d'Access Manager sur Application Server (6223676)

Si vous exécutez Application Server 8.1 sous Red Hat Linux, la taille de la pile des threads créés par le système d'exploitation Red Hat pour Application Server est de 10 Mo, ce qui peut entraîner des problèmes de ressources JVM lorsque le nombre de sessions utilisateur Access Manager atteint 200.

Solution : Définissez la taille de la pile de fonctionnement du système d'exploitation Red Hat sur une valeur inférieure, telle que 2 048 ou même 256 Ko en exécutant la commande `ulimit`

avant de démarrer Application Server. Exécutez la commande `ulimit` sur la même console que celle utilisée pour démarrer Application Server. Exemple :

```
# ulimit -s 256;
```

Problèmes Windows et HP-UX

Échec de configuration automatique d'Access Manager lors de l'installation dans des environnements linguistiques zh_TW et es (6515043)

Solution : Dans des environnements linguistiques `zh_TW` et `es` sur plate-forme HP-UX, Access Manager doit être configuré en mode de configuration ultérieure uniquement. Lancez le programme d'installation JavaES, installez Access Manager et quittez le programme d'installation. Invoquez ensuite le configurateur Access Manager tel qu'illustré ci-dessous :

1. `LANG=C`
2. `export LANG`
3. Modifiez *accessmanager-base*`/bin/amsamplesilent file`
4. Exécutez *accessmanager-base*`/bin/amconfig -s amsamplesilent`

HP-UX requiert un binaire gettext avec AM lors de l'installation de la pile JES complète (6497926)

Il n'existe actuellement pas de solution à ce problème.

Problèmes liés à SAML et aux fédérations

Une erreur de déconnexion se produit dans la fédération (6291744)

En mode Domaine, si vous fédérez des comptes utilisateur sur un fournisseur d'identités et un fournisseur de services, que vous arrêtez la fédération, puis que vous vous déconnectez, une erreur se produit : Erreur : Aucune sous-organisation n'a été trouvée.

Solution : aucune.

Problèmes liés à la globalisation (g11n)

Composants de la console d'administration affichés en anglais dans l'environnement linguistique zh (6470543)

Si vous définissez l'environnement linguistique du navigateur sur `zh`, les composants de la console d'administration s'affichent en anglais, les boutons Version, Aide et Déconnexion par exemple.

Solution : Définissez l'environnement linguistique sur `zh-cn` au lieu de `zh`.

Les valeurs actuelle et nouvelle ne s'affichent pas correctement dans la console (6476672)

Dans la version localisée de la console d'administration, les intitulés des attributs de valeur actuelle et nouvelle ne s'affichent pas correctement sous la forme label.current.value et label.new.value, respectivement.

La date de la condition de stratégie doit être spécifiée selon les normes anglaises (6390856)

Les étiquettes de format de date de la condition de stratégie en version chinoise ne sont pas affichées selon les normes chinoises. Les étiquettes proposent un format de date similaire au format de date anglais. Les champs connexes acceptent également les valeurs au format de date anglais.

Solution : Pour chaque champ, suivez l'exemple de format de date donné dans cette étiquette de champ.

La suppression de UTF-8 ne fonctionne pas avec la fonction Détection de client (5028779)

La fonction Détection de client ne fonctionne pas correctement. Les modifications effectuées dans la console Access Manager 7.1 ne sont pas automatiquement appliquées dans le navigateur.

Solution : Vous avez deux possibilités :

- Redémarrez le conteneur Web d'Access Manager, après avoir effectué une modification dans la section Détection de client.

  ou

- Suivez la procédure ci-dessous dans la console Access Manager :

  1. Cliquez sur `Détection de client` sous l'onglet `Configuration`.
  2. Cliquez sur le lien `Modifier` correspondant au client `genericHTML`.
  3. Sous l'onglet HTML, cliquez sur le lien `genericHTML`.
  4. Dans la liste des jeux de caractères, entrez la valeur : `UTF-8;q=0.5` (Veillez à ce que le facteur UTF-8 `q` soit inférieur à celui des autres jeux de caractères de vos paramètres linguistiques.)
  5. Enregistrez l'opération, déconnectez-vous, puis reconnectez-vous.

Les caractères multioctets sont affichés sous forme de points d'interrogation dans les fichiers journaux (5014120)

Les messages multioctets des fichiers journaux du répertoire `/var/opt/SUNWam/logs` sont affichés sous forme de points d'interrogation (`?`). Les fichiers journaux ont recours à un codage natif et n'utilisent pas toujours UTF-8. Lors du démarrage d'une instance de conteneur Web dans un certain environnement linguistique, les fichiers journaux apparaissent avec le codage natif correspondant à cet environnement linguistique. Si vous changez d'environnement linguistique et que vous redémarrez l'instance du conteneur Web, les messages ultérieurs utiliseront le codage natif correspondant aux paramètres linguistiques actifs, mais les messages antérieurs sont affichés avec des points d'interrogation.

Solution : Veillez à démarrer les instances du conteneur Web en utilisant toujours le même codage natif.

Problèmes détectés dans la documentation

- "Documentation de la prise en charge des rôles et des rôles filtrés pour le plug-in LDAPv3 (6365196)" à la page 44

Documentation de la prise en charge des rôles et des rôles filtrés pour le plug-in LDAPv3 (6365196)

Après avoir appliqué le patch respectif, vous pouvez configurer les rôles et les rôles filtrés pour le plug-in LDAPv3, si les données sont stockées dans Sun Java System Directory Server (résout le problème ayant pour ID 6349959). Au niveau de la console d'administration Access Manager 7.1, dans la configuration LDAPv3, saisissez les valeurs suivantes pour le champ Types et opérations pris en charge du plug-in LDAPv3 :

```
role: read,edit,create,delete
filteredrole: read,edit,create,delete
```

Vous pouvez saisir une ou plusieurs des entrées ci-dessus, en fonction des rôles et des rôles filtrés que vous prévoyez d'utiliser dans votre configuration LDAPv3.

Documentation des propriétés non utilisées dans le fichier `AMConfig.properties` (6344530)

Les propriétés suivantes du fichier `AMConfig.properties` ne sont pas utilisées :

```
com.iplanet.am.directory.host
com.iplanet.am.directory.port
```

Documentation sur la façon d'activer le chiffrement XML (6275563)

Pour activer le chiffrement XML pour Access Manager ou Federation Manager à l'aide du fichier JAR Bouncy Castle afin de générer une clé de transport, appliquez les étapes suivantes :

1. Si vous utilisez une version JDK antérieure à JDK 1.5, téléchargez le fournisseur JCE Bouncy Castle depuis le site Web Bouncy Castle (`http://www.bouncycastle.org/`). Par exemple, pour JDK 1.4, téléchargez le fichier `bcprov-jdk14-131.jar` .
2. Si vous avez téléchargé un fichier JAR lors de l'étape précédente, copiez le fichier dans le répertoire *jdk_root*`/jre/lib/ext`.
3. Pour la version domestique de JDK, téléchargez les fichiers JCE Unlimited Strength Jurisdiction Policy correspondant à votre version de JDK depuis le site Web de Sun (`http://java.sun.com`). Pour IBM WebSphere, rendez-vous sur le site IBM correspondant pour télécharger les fichiers requis.
4. Copiez les fichiers `US_export_policy.jar` et `local_policy.jar` téléchargés dans le répertoire *jdk_root*`/jre/lib/security` .

5. Si vous utilisez une version de JDK inférieure à JDK 1.5, modifiez le fichier *jdk_root*`/jre/lib/security/java.security` et ajoutez Bouncy Castle en tant que fournisseur. Exemple :

   ```
   security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider
   ```

6. Définissez la propriété suivante du fichier `AMConfig.properties` sur true :

   ```
   com.sun.identity.jss.donotInstallAtHighestPriority=true
   ```

7. Redémarrez le conteneur Web d'Access Manager.

Pour de plus amples informations, reportez-vous au problème ayant pour ID 5110285 (le chiffrement XML requiert un fichier JAR Bouncy Castle).

Mises à jour de la documentation

Pour accéder à ces documents, reportez-vous à la collection Access Manager 7.1 :

`http://docs.sun.com/coll/1292.1`

Un nouveau document nommé Chapitre 1, “Technical Note: Deploying Access Manager Instances to an Application Server Cluster” du *Technical Note: Deploying Access Manager to an Application Server Cluster* a été ajouté à la documentation d'Access Manager 7 2005Q4.

La collection Sun Java System Access Manager Policy Agent 2.2 a également été révisée pour documenter de nouveaux agents :

`http://docs.sun.com/coll/1322.1`

Fichiers redistribuables

Sun Java System Access Manager 7.1 ne contient aucun fichier redistribuable auprès d'utilisateurs ne disposant pas d'une licence du produit.

Comment signaler des problèmes et apporter des commentaires

Si vous rencontrez des problèmes avec Access Manager ou Sun Java Enterprise System, contactez le support client de Sun de l'une des manières suivantes :

- En faisant appel aux services de support Sun (SunSolve) (`http://sunsolve.sun.com/`).

Ce site contient des liens vers la base de connaissances, le centre d'assistance en ligne et ProductTracker, ainsi que vers des programmes de maintenance et des coordonnées pour l'assistance.

- Le numéro de téléphone indiqué sur votre contrat de maintenance.

Afin que nous puissions vous aider au mieux à résoudre vos problèmes, munissez-vous des informations suivantes lorsque vous contactez le support :

- Description du problème, notamment les conditions dans lesquelles le problème se produit et sa répercussion sur l'opération effectuée.
- Le type de machine, les versions du système d'exploitation et du produit, y compris les patchs et autres logiciels pouvant avoir un lien avec le problème.
- Étapes détaillées des méthodes utilisées pour reproduire le problème.
- Journaux des erreurs ou core dumps éventuels.

Sun attend vos commentaires

Afin d' améliorer sa documentation, Sun vous encourage à faire des commentaires et à apporter des suggestions. Pour ce faire, accédez au site `http://docs.sun.com/` et cliquez sur Envoyer des commentaires.

Indiquez le titre complet du document ainsi que son numéro de référence dans les champs appropriés. Le numéro de référence est constitué de sept ou neuf chiffres et figure sur la page de titre du manuel ou en haut du document. Dans le cas présent, le numéro de référence des *Access Manager Notes de version* est 819-4683-13.

Ressources Sun supplémentaires

Vous pouvez trouver des informations et des ressources utiles sur Access Manager sur les sites Internet suivants :

- Documentation de Sun Java Enterprise System : `http://docs.sun.com/prod/entsys.05q4`
- Services Sun : `http://www.sun.com/service/consulting/`
- Produits et services logiciels : `http://wwws.sun.com/software/`
- Services de support : `http://sunsolve.sun.com/`
- Informations pour les développeurs : `http://developers.sun.com/`
- Services de support pour développeurs Sun : `http://www.sun.com/developers/support/`

Fonctions d'accessibilité destinées aux personnes handicapées

Pour obtenir la liste des fonctions d'accessibilité mises à disposition depuis la publication de ce média, consultez les évaluations de produit de la Section 508, disponibles sur demande auprès de Sun, afin de déterminer les versions les mieux adaptées au déploiement des solutions accessibles. Les mises à jour des applications sont disponibles à l'adresse `http://sun.com/software/javaenterprisesystem/get.html`.

Pour obtenir plus d'informations sur l'engagement de Sun en matière d'accessibilité, visitez le site `http://sun.com/access`.

Sites Web complémentaires émanant de tiers

Des URL de sites tiers, qui renvoient à des informations complémentaires connexes, sont référencés dans ce document.

Remarque – Sun décline toute responsabilité quant à la disponibilité des sites Web de tiers mentionnés dans ce document. Sun ne garantit pas le contenu, la publicité, les produits et autres documents disponibles sur ces sites ou dans ces ressources, ou accessibles par leur intermédiaire, et ne saurait en être tenu pour responsable. Sun ne pourra en aucun cas être tenu responsable, directement ou indirectement, de tous dommages ou pertes, réels ou invoqués, causés par ou liés à l'utilisation des contenus, biens ou services disponibles dans ou par l'intermédiaire de ces sites ou ressources.
