Notes de version de Sun Java System Access Manager 7 2005Q4

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

Référence : 819–3478
19 août 2008

080915@20795

Table des matières

Notes de version de Sun Java System Access Manager 7 2005Q4 5
Contenu 5
Historique des révisions 6
À propos de Sun Java System Access Manager 7 2005Q4 9
Versions de patchs Access Manager 7 2005Q4 9
Access Manager 7 2005Q4 Patch 7 10
Remarques relatives à la pré-installation 12
Instructions d'installation du patch 15
Remarques relatives à la post-installation 20
Access Manager 7 2005Q4 Patch 6 23
Access Manager 7 2005Q4 Patch 5 28
Access Manager 7 2005Q4 Patch 4 45
Access Manager 7 2005Q4 Patch 3 47
Access Manager 7 2005Q4 Patch 2 58
Access Manager 7 2005Q4 Patch 1 63
Nouveautés de cette version 64
Modes d'Access Manager 65
Nouvelle console Access Manager 65
Référentiel d'identité 65
Arborescence d'informations d'Access Manager 66
Modifications liées au basculement de session 66
Notification de modification d'une propriété de session 67
Contraintes relatives aux quotas de session 67
Authentification distribuée 68
Prise en charge de plusieurs instances du module d'authentification 68
Espace de noms sous forme d'enchaînement ou de configuration nommée, associé à l'authentification 69
Améliorations du module de stratégie 69
Configuration du site 70

Fédération en bloc 70
Améliorations en termes de journalisation 70
Configurations matérielle et logicielle requises 71
Navigateurs pris en charge 72
Prise en charge de la virtualisation du système 73
Problèmes de compatibilité 73
Mode hérité d'Access Manager 73
Agents de stratégie Access Manager 75
Notes relatives à l'installation 76
Problèmes connus et restrictions 76
Problèmes de compatibilité 76
Problèmes relatifs à l'installation 78
Problèmes de mise à niveau 80
Problèmes de configuration 83
Problèmes liés à la console Access Manager 87
Problèmes liés au SDK et au client 89
Problèmes liés aux utilitaires de ligne de commande 91
Problèmes d'authentification 92
Problèmes de session et de connexion unique 93
Problèmes liés aux stratégies 95
Problèmes liés au démarrage du serveur 95
Problèmes concernant le système d'exploitation Linux 96
Problèmes liés à SAML et aux fédérations 96
Problèmes liés à la globalisation (g11n) 99
Problèmes liés à la documentation 101
Mises à jour de la documentation 108
Collection Sun Java System Access Manager 7 2005Q4 108
Collection Sun Java System Federation Manager 7.0 2005Q4 109
Collection Sun Java System Access Manager Policy Agent 2.2 109
Fichiers redistribuables 110
Comment signaler des problèmes et apporter des commentaires 110
Sun attend vos commentaires 110
Ressources Sun supplémentaires 111
Fonctions d'accessibilité destinées aux personnes handicapées 111
Sites Web complémentaires émanant de tiers 111

Notes de version de Sun Java System Access Manager 7 2005Q4

19 août 2008

Numéro de référence 819-2134-22

Ces notes de version contiennent des informations importantes disponibles au moment de la mise sur le marché de Sun Java™ Enterprise System (Java ES), notamment sur les nouvelles fonctions 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 plus d'informations sur la modification des notes de version, reportez-vous à la rubrique “Historique des révisions” à la page 6.

Pour consulter la documentation du produit Java ES, notamment la collection de manuels Access Manager, rendez-vous sur le 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.

Contenu

Les notes de version d'Access Manager 7 2005Q4 se composent des sections suivantes :

- “Historique des révisions” à la page 6
- “À propos de Sun Java System Access Manager 7 2005Q4” à la page 9
- “Versions de patchs Access Manager 7 2005Q4” à la page 9
- “ Nouveautés de cette version” à la page 64
- “ Configurations matérielle et logicielle requises” à la page 71
- “Problèmes de compatibilité” à la page 73
- “ Notes relatives à l'installation” à la page 76
- “ Problèmes connus et restrictions” à la page 76
- “Mises à jour de la documentation” à la page 108

- " Fichiers redistribuables" à la page 110
- "Comment signaler des problèmes et apporter des commentaires" à la page 110
- " Ressources Sun supplémentaires" à la page 111
- "Sites Web complémentaires émanant de tiers" à la page 111

Historique des révisions

Le tableau ci-après présente l'historique des révisions apportées aux notes de version d'Access Manager 7 2005Q4.

TABLEAU 1 Historique des révisions

Date	Description des modifications
19 août 2008	Ajout d'informations sur le patch 7 pour les systèmes Windows et HP-UX dans la section "Versions de patchs Access Manager 7 2005Q4" à la page 9.
12 mai 2008	■ Ajout d'informations sur le patch 7 dans la section "Versions de patchs Access Manager 7 2005Q4" à la page 9. ■ Ajout de la section "Prise en charge de la virtualisation du système" à la page 73.
16 octobre 2007	Les modifications apportées à cette révision sont les suivantes : ■ Ajout d'informations sur le patch 6 dans la section "Versions de patchs Access Manager 7 2005Q4" à la page 9. ■ Mise à jour de "CR# 6522720 : il est impossible d'effectuer une recherche de caractères multioctets dans l'aide en ligne de la console sous Windows et HP-UX" à la page 44. Le patch 6 résout ce problème sous Windows. Cependant, il persiste sur les systèmes HP-UX.
10 juillet 2007	Les modifications apportées à cette révision sont les suivantes : ■ Ajout d'informations sur le patch 126371-05 pour les systèmes HP-UX dans la section "Versions de patchs Access Manager 7 2005Q4" à la page 9. ■ Ajout du nouveau problème suivant : "La recherche LDAP d'attributs null renvoie une erreur lorsqu'Access Manager pointe vers Directory Proxy (6357975)" à la page 91.

TABLEAU 1 Historique des révisions *(Suite)*

Date	Description des modifications
16 mars 2007	Les modifications apportées à cette révision sont les suivantes : ■ Ajout d'informations sur le patch 5 dans la section "Versions de patchs Access Manager 7 2005Q4" à la page 9. ■ Ajout de clarifications et de nouvelles informations dans la section "Problèmes liés à la documentation" à la page 101. ■ Diverses autres modifications techniques et rédactionnelles apportées par les réviseurs et les demandes de modification.
30 octobre 2006	Les modifications apportées à la section "Versions de patchs Access Manager 7 2005Q4" à la page 9 comprennent : ■ Ajout d'informations sur le patch 4. ■ Correction de l'utilisation incohérente de *AccessManager-base* . ■ Révision de la description de "CR# 6440651 : la rediffusion de cookie requiert la propriété `com.sun.identity.session.resetLBCookie` ." à la page 55.
25 août 2006	Les modifications apportées à la section "Versions de patchs Access Manager 7 2005Q4" à la page 9 comprennent : ■ Ajout d'informations sur le patch 3. ■ Nouvelles informations révisées et ajoutées sur les patchs 1 et 2.

25 mai 2006	Les modifications apportées à cette révision sont les suivantes :
	■ Ajout de la section "Access Manager 7 2005Q4 Patch 2" à la page 58.
	■ Ajout d'informations sur la prise en charge des plates-formes HP-UX et Microsoft Windows dans le Tableau 4.
	■ Ajout des problèmes suivants dans la rubrique "Problèmes liés à la documentation" à la page 101 :
	  ■ "Les notes de version ne résolvent pas un problème connu (6422907)" à la page 106
	  ■ "Document `com.iplanet.am.session.protectedPropertiesList` dans `AMConfig.properties` (6351192)" à la page 106

9 février 2006	Section "Mises à jour de la documentation" à la page 108 révisée afin de répertorier les documents nouveaux et révisés relatifs à Access Manager 7 2005Q4 publiés depuis la version initiale.

TABLEAU 1 Historique des révisions *(Suite)*

Date	Description des modifications
7 février 2006	Les modifications apportées à cette révision sont les suivantes : ■ Ajout des problèmes suivants dans la section " Problèmes connus et restrictions" à la page 76 : ■ "Le service d'authentification n'est pas initialisé lorsque Access Manager et Directory Server sont installés sur des machines séparées (6229897)" à la page 80 ■ "Le script `ampre70upgrade` d'Access Manager ne supprime pas les packages localisés (6378444)" à la page 81 ■ Mise à jour de la section "Mises à jour de la documentation" à la page 108.
18 janvier 2006	Les modifications apportées à cette révision sont les suivantes : ■ Ajout de la section "Access Manager 7 2005Q4 Patch 1" à la page 63. ■ Clarification de la description de "Authentification distribuée" à la page 68. ■ Clarification de la prise en charge des zones Solaris 10 et ajout de la prise en charge du système d'exploitation Solaris 10 sur les plates-formes AMD64 dans la section " Configurations matérielle et logicielle requises" à la page 71. ■ Ajout des problèmes suivants dans la section " Problèmes connus et restrictions" à la page 76 : ■ "Échec de signature d'URL dans IBM WebSphere avec une clé RSA (6271087)" à la page 86 ■ "Des problèmes surviennent sur Java Virtual Machine (JVM) lors de l'exécution d'Access Manager sur Application Server (6223676)" à la page 96 ■ "L'exécution de l'exemple de services Web renvoie le message Resource offering not found (6359900)" à la page 97 ■ "Après l'application du patch 1, le fichier `/tmp/amsilent` offre un accès en lecture à tous les utilisateurs (6370691)" à la page 79 ■ "Ajout de l'attribut `ContainerDefaultTemplateRole` après la migration des données (4677779)" à la page 83 ■ "Documentation de la prise en charge des rôles et des rôles filtrés pour le plug-in LDAPv3 (6365196)" à la page 107 ■ "Documentation des propriétés non utilisées dans le fichier `AMConfig.properties` (6344530)" à la page 107 ■ "Documentation sur la façon d'activer le chiffrement XML (6275563)" à la page 108 ■ Ajout de la section "Mises à jour de la documentation" à la page 108.

TABLEAU 1 Historique des révisions *(Suite)*

Date	Description des modifications
8 novembre 2005	Révision de la section "Référentiel d'identité" à la page 65 pour les référentiels compatibles avec LDAP version 3 (LDAP v3) pris en charge.
3 octobre 2005	Version initiale.
30 juin 2005	Version Bêta.

À propos de Sun Java System Access Manager 7 2005Q4

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.

Versions de patchs Access Manager 7 2005Q4

Les dernières versions des patchs d'Access Manager 7 2005Q4 peuvent être téléchargées sur SunSolve Online à l'adresse suivante : `http://sunsolve.sun.com`. Les derniers ID de patch sont les suivants :

- Systèmes d'exploitation Solaris™ (Solaris OS) sur SPARC® : **120954-07**
- Solaris OS sur les plates-formes x86 : **120955-07**
- Systèmes Linux : **120956-07**
- Systèmes Microsoft Windows : **124296-07**
- Systèmes HP-UX : **126371-07**

Remarque – Les patchs d'Access Manager 7 2005Q4 peuvent être cumulés. Vous pouvez installer le patch 7 sans installer d'abord le patch 1, 2, 3, 4, 5 ou 6. Cependant, si vous n'avez pas installé un patch antérieur, vérifiez les nouvelles fonctions et problèmes dans les sections relatives aux patchs précédents pour déterminer si l'un d'eux s'appliquent à votre déploiement.

Les informations sur les patchs d'Access Manager 7 2005Q4 sont notamment :

- "Access Manager 7 2005Q4 Patch 7" à la page 10
- "Remarques relatives à la pré-installation" à la page 12
- "Instructions d'installation du patch" à la page 15
- "Remarques relatives à la post-installation" à la page 20
- "Access Manager 7 2005Q4 Patch 6" à la page 23
- "Access Manager 7 2005Q4 Patch 5" à la page 28
- "Access Manager 7 2005Q4 Patch 4" à la page 45
- "Access Manager 7 2005Q4 Patch 3" à la page 47
- "Access Manager 7 2005Q4 Patch 2" à la page 58
- "Access Manager 7 2005Q4 Patch 1" à la page 63

Access Manager 7 2005Q4 Patch 7

Le patch 7 (révision 7) d'Access Manager 7 résout de nombreux problèmes, répertoriés dans le fichier LISEZMOI accompagnant le patch.

Le patch 7 inclut les modifications suivantes :

- "CR# 6637806 : au redémarrage, Access Manager envoyait un jeton SSO d'application incorrect à un agent" à la page 10
- "CR# 6612609 : le basculement de session fonctionne si le câble réseau est débranché du serveur Message Queue" à la page 11
- "CR# 6570409 : le service Interaction derrière l'équilibreur de charge fonctionne correctement en tant que fournisseur d'identités" à la page 11
- "CR# 6545176 : les URL de redirection peuvent être définis de façon dynamique dans le plug-in de la SPI de traitement de la post-authentification" à la page 12

CR# 6637806 : au redémarrage, Access Manager envoyait un jeton SSO d'application incorrect à un agent

Après un redémarrage du serveur Access Manager, le SDK du client Access Manager envoie maintenant une exception significative à un agent afin que ce dernier puisse s'authentifier de nouveau pour obtenir une nouvelle session d'application. Auparavant, après l'application du patch 5 d'Access Manager 7 2005Q4, le SDK du client Access Manager envoyait un jeton SSO d'application incorrect au redémarrage du serveur Access Manager.

Ce problème a été résolu par le doublon CR 6496155. Le patch 7 inclut également une option (propriété `comp.iplanet.dpro.session.dnRestrictionOnly`) permettant d'envoyer le jeton SSO d'application dans un contexte restrictif. Par défaut, les agents envoient l'adresse IP du serveur où ils sont installés. Toutefois, si une vérification stricte du DN s'avère nécessaire, définissez cette propriété dans le fichier `AMConfig.properties` comme suit :

```
com.iplanet.dpro.session.dnRestrictionOnly=true
```

CR# 6612609 : le basculement de session fonctionne si le câble réseau est débranché du serveur Message Queue

Lors du déploiement d'un basculement de session, si chaque instance d'Access Manager et courtier Message Queue sont installés sur le même serveur, le basculement de session fonctionne si un câble réseau est débranché d'un des serveurs. Par défaut, l'attribut de fabrique de connexion `imqAddressListBehavior` de Message Queue est défini sur `PRIORITY`, ce qui amène Message Queue à essayer les adresses par ordre d'apparition dans la liste d'adresses du courtier (par exemple : `localhost:7777,server2:7777,server3:7777`). Si l'attribut est défini sur `RANDOM`, les adresses sont essayées dans le désordre.

Pour définir cet attribut sur RANDOM, définissez le paramètre suivant dans le script `amsessiondb` :

```
-DimqAddressListBehavior=RANDOM
```

Pour plus d'informations sur les attributs `PRIORITY` et `RANDOM` de Message Queue, reportez-vous à la section "Broker Address List" du *Sun Java System Message Queue 3.7 UR1 Administration Guide*.

CR# 6570409 : le service Interaction derrière l'équilibreur de charge fonctionne correctement en tant que fournisseur d'identités

Lors d'un déploiement impliquant deux serveurs connectés à un équilibreur de charge et fonctionnant en tant que fournisseur d'identités, vous devez définir les propriétés suivantes dans le fichier `AMConfig.properties` :

```
com.sun.identity.liberty.interaction.lbWspRedirectHandler
com.sun.identity.liberty.interaction.trustedWspRedirectHandlers
```

La classe `com.sun.identity.liberty.interaction.interactionConfigClass` est actuellement la seule prise en charge. Ainsi, par défaut, la classe de configuration de l'interaction intégrée à Federation Liberty est utilisée pour accéder aux paramètres de configuration de l'interaction.

CR# 6545176 : les URL de redirection peuvent être définis de façon dynamique dans le plug-in de la SPI de traitement de la post-authentification

Les URL de redirection peuvent être définis de façon dynamique dans les plug-ins de la SPI de traitement de la post-authentification pour la réussite et l'échec de connexion, ainsi que pour la déconnexion. Si un plug-in de post-traitement n'est pas exécuté, l'URL de redirection défini dans la SPI de post-traitement n'est pas utilisé et les URL de redirection définis par tout autre moyen seront exécutés comme auparavant.

Pour plus d'informations, reportez-vous à l'exemple `com.iplanet.am.samples.authentication.spi.postprocess.ISAuthPostProcessSample.java`.

Remarques relatives à la pré-installation

- "Sauvegarde de fichiers" à la page 12
- "Installation et configuration d'Access Manager" à la page 14

Sauvegarde de fichiers

Important Si vous avez personnalisé des fichiers de votre installation, sauvegardez-les avant d'installer le patch. Une fois le patch installé, comparez les fichiers sauvegardés avec les nouveaux fichiers installés par ce patch afin de repérer vos personnalisations. Fusionnez les fichiers personnalisés avec les nouveaux et enregistrez-les. Pour plus d'informations sur la gestion de fichiers personnalisés, lisez les informations suivantes.

Sauvegardez également les fichiers suivants avant d'installer un patch :

Systèmes Solaris	■ *AccessManager-base*/SUNWam/bin/amsfo ■ *AccessManager-base*/SUNWam/lib/amsfo.conf ■ Fichiers inclus dans le répertoire /etc/opt/SUNWam/config/xml/template/ : idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml, amAuth.xml , amSession.xml ■ Fichiers inclus dans le répertoire *AccessManager-base*/SUNWam/locale/ : amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties
Systèmes Linux et HP-UX	■ *AccessManager-base*/identity/bin/amsfo ■ *AccessManager-base*/identity/lib/amsfo.conf ■ Fichiers inclus dans le répertoire /etc/opt/sun/identity/config/xml/template/ : idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml , amAuth.xml, amSession.xml ■ Fichiers inclus dans le répertoire *AccessManager-base*/identity/locale/ : amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties

Systèmes Windows	■ *AccessManager-base*\identity\setup\AMConfigurator.properties ■ *AccessManager-base*\identity\bin\amsfo ■ *AccessManager-base*\identity\lib\amsfo.conf ■ Fichiers inclus dans le répertoire *AccessManager-base*\identity\config\xml\template : idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml , amAuth.xml, amSession.xml ■ Fichiers inclus dans le répertoire *AccessManager-base*\identity\locale : amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties

AccessManager-base correspond au répertoire d'installation de base. Le répertoire d'installation de base par défaut dépend de la plate-forme :

- Systèmes Solaris : /opt
- Systèmes Linux et HP-UX : /opt/sun
- Systèmes Windows : *javaes-install-directory*\AccessManager . Exemple : C:\Program Files\Sun\AccessManager

Installation et configuration d'Access Manager

Les patchs d'Access Manager décrits dans ce document n'installent pas Access Manager. Avant d'installer le patch, vous devez installer Access Manager 7 2005Q4 sur le serveur. Pour plus d'informations sur l'installation, reportez-vous au manuel *Guide d'installation de Sun Java Enterprise System 2005Q4 pour UNIX*.

Si vous installez le patch sous Windows, consultez le *Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows* .

Vous devez savoir exécuter le script amconfig pour déployer, redéployer et configurer Access Manager, comme décrit dans le Chapitre 1, "Access Manager 7 2005Q4 Configuration Scripts" du *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

Pour obtenir une liste des patchs d'Access Manager rendus obsolètes par ce patch et tout autre patch à installer avant celui-ci, consultez le fichier LISEZMOI fourni avec ce patch.

Attention – Les patchs d'Access Manager (ainsi que tout autre patch) doivent être testés sur un système intermédiaire ou de pré-déploiement avant de les installer dans un environnement de production. De plus, le programme d'installation du patch peut ne pas mettre à jour correctement vos fichiers JSP personnalisés. Vous devrez donc peut-être les modifier manuellement pour qu'Access Manager fonctionne correctement.

Instructions d'installation du patch

- "Instructions d'installation du patch pour les systèmes Solaris" à la page 15
- "Instructions d'installation du patch pour les systèmes Linux" à la page 17
- "Instructions d'installation du patch pour les systèmes Windows" à la page 18
- "Instructions d'installation du patch pour les systèmes HP-UX" à la page 19

Instructions d'installation du patch pour les systèmes Solaris

Avant d'installer le patch pour Solaris, n'oubliez pas de sauvegarder les fichiers répertoriés sous "Remarques relatives à la pré-installation" à la page 12.

Pour ajouter ou supprimer des patchs sur des systèmes Solaris, utilisez les commandes `patchadd` et `patchrm` fournies avec le système d'exploitation.

Commande patchadd

Utilisez la commande `patchadd` pour installer un patch sur un système autonome. Exemple :

```
# patchadd /var/spool/patch/120954-07
```

Remarque – Si vous installez le patch pour Solaris dans la zone globale de Solaris 10, appelez la commande `patchadd` avec l'argument `-G`. Exemple :

```
patchadd -G /var/spool/patch/120954-07
```

Le script `postpatch` affiche un message relatif au redéploiement des applications Access Manager, sauf sur un système sur lequel seul le composant SDK d'Access Manager est installé.

Le script `postpatch` crée le fichier `amsilent` dans le répertoire suivant :

- Systèmes Solaris : *AccessManager-base*`/SUNWam`
- Systèmes Linux : *AccessManager-base*`/identity`

AccessManager-base correspond au répertoire d'installation de base. Le répertoire d'installation de base par défaut est `/opt` sous Solaris et `/opt/sun` sous Linux.

Le fichier `amsilent` est basé sur le fichier `amsamplesilent`, mais certains paramètres requis sont définis en fonction des fichiers de configuration d'Access Manager sur le système. Les paramètres de mot de passe contiennent cependant des valeurs par défaut. Supprimez le commentaire et modifiez la valeur de chaque paramètre de mot de passe et vérifiez les autres paramètres du fichier en fonction de votre déploiement.

Le paramètre `COMMON_DEPLOY_URI`, le préfixe URI des applications Web de domaine communes, contient également une valeur par défaut. Si vous avez sélectionné une autre valeur que la valeur par défaut pour cette URI, n'oubliez pas de la mettre à jour. Dans le cas contraire, le redéploiement des applications Web avec `amconfig` et le fichier `amsilent` généré par le patch échouent.

Exécutez ensuite la commande suivante (Access Manager installé dans le répertoire par défaut) :

```
# cd /opt/SUNWam/bin
# ./amconfig -s /opt/SUNWam/amsilent
```

Attention – Comme le fichier `amsilent` contient des données sensibles (mots de passe administrateur en clair, etc.), veillez à le protéger de manière appropriée en fonction de votre déploiement.

Après avoir exécuté le script `amconfig`, exécutez le script `updateschema.sh` pour charger les fichiers XML et LDIF. Le script `updateschema.sh` est disponible une fois le patch 7 installé dans le répertoire suivant :

- Systèmes Solaris SPARC : *patch-home-directory* /120954-07
- Systèmes Solaris x86 : *patch-home-directory*/120955-07

Redémarrez les processus d'Access Manager une fois le script `updateschema` exécuté. Exemple :

```
# cd /opt/SUNWam/bin
# ./amserver stop
# ./amserver start
```

Redémarrez ensuite le conteneur Web d'Access Manager.

Commande patchrm

Utilisez la commande `patchrm` pour supprimer un patch d'un système autonome. Exemple :

```
# patchrm 120954-03
```

Le script `backout` affiche un message identique à la commande `patchadd`, sauf sur un système sur lequel seul le composant SDK d'Access Manager est installé.

Une fois le patch supprimé, redéployez les applications Access Manager à l'aide du fichier `amsilent` dans le répertoire *AccessManager-base* `/SUNWam`, où *AccessManager-base* correspond au répertoire d'installation de base. Le répertoire d'installation de base est `/opt` sous Solaris.

Définissez les paramètres du fichier `amsilent` en fonction de votre déploiement.

Exécutez ensuite la commande suivante, accessible dans le répertoire par défaut sous Solaris une fois Access Manager installé :

```
# cd /opt/SUNWam/bin
# ./amconfig -s /opt/SUNWam/amsilent
```

Pour plus d'informations et d'exemples sur les commandes `patchadd` et `patchrm`, reportez-vous aux pages de manuel `man` Solaris correspondantes.

Voir aussi "Remarques relatives à la post-installation" à la page 20 pour plus d'informations.

Zones Solaris 10

Le système d'exploitation Solaris 10 a introduit le nouveau concept de 'zones'. La commande patchadd inclut donc la nouvelle option `-G` qui permet d'ajouter un patch à la zone globale uniquement. Par défaut, la commande patchadd recherche la variable `SUNW_PKG_ALLZONES` dans le pkginfo des packages à fournir en patch. Pour tous les packages Access Manager, la variable `SUNW_PKG_ALLZONES` n'est cependant pas définie et l'option `-G` est nécessaire si Access Manager 7 2005Q4 est installé dans la zone globale. L'option `patchadd -G` ne s'applique pas si Access Manager est installé dans une zone locale.

Si vous installez les patchs Access Manager 7 2005Q4 sur un système Solaris, il est recommandé d'utiliser l'option `-G.` Exemple :

```
 # patchadd -G AM7_patch_dir
```

De même, si Access Manager est installé dans la zone globale, l'option `-G` est nécessaire pour exécuter la commande `patchrm.` Exemple :

```
# patchrm -G 120954-07
```

Instructions d'installation du patch pour les systèmes Linux

Avant d'installer le patch pour Linux, n'oubliez pas de sauvegarder les fichiers répertoriés sous "Remarques relatives à la pré-installation" à la page 12.

La commande `installpatch` installe un patch sur un système Linux autonome. Exemple :

```
# ./installpatch
```

Le script `postpatch` affiche des messages identiques à ceux d'un système Solaris. La procédure de sortie d'un patch sur un système Linux est cependant différente de celle sur un système Solaris. Il n'existe pas de script générique de sortie d'un patch Linux. Si une version antérieure du patch a été préalablement installée, vous pouvez réinstaller cette version puis suivre les instructions de postpatch afin de redéployer les applications Access Manager en exécutant le script `amconfig`.

Après avoir exécuté le script `amconfig`, exécutez le script `updateschema.sh` (patchs 5 et ultérieurs) pour charger les fichiers XML et LDIF. Le script `updateschema.sh` est disponible une fois le patch 7 installé dans le répertoire *patch-home-directory*`/120956-07/scripts` .

Redémarrez le conteneur Web d'Access Manager après avoir exécuté les scripts `amconfig` et `updateschema.sh` .

Si le patch est installé sur la version Access Manager 7 2005Q4 RTM et que vous souhaitez le supprimer et restaurer le système à l'état RTM, vous devez reinstaller Access Manager RTM à l'aide du script `reinstallRTM`. Ce script utilise le chemin d'accès au stockage des RPM Access Manager RTM et installe les RPM RTM sur les RPM du patch. Exemple :

```
# ./scripts/reinstallRTM path_of_AM7_RTM_RPM_directory
```

Après avoir exécuté le script `reinstallRTM`, redéployez les applications Access Manager en exécutant le script `amconfig` et redémarrez le conteneur Web.

Voir aussi "Remarques relatives à la post-installation" à la page 20 pour plus d'informations.

Instructions d'installation du patch pour les systèmes Windows

Conditions requises pour installer le patch pour Windows :

- Access Manager 7 2005Q4 doit être installé sous Windows. Pour plus d'informations sur l'installation, consultez le *Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows* .
- Pour exécuter les scripts du patch, ActivePerl 5.8 (ou version ultérieure) doit être installé sous Windows.

Installation du patch pour Windows

Avant d'installer le patch pour Windows, n'oubliez pas de sauvegarder les fichiers répertoriés sous "Remarques relatives à la pré-installation" à la page 12.

Utilisez une barre oblique (`/`) dans le chemin d'accès au répertoire de base de saisie des scripts de patchs. Exemple : `c:/sun`

Pour installer le patch pour Windows :

1. Connectez-vous à Windows en tant qu'administrateur.

2. Créez un répertoire où télécharger et décompresser le fichier de patch pour Windows. Par exemple : `AM7p7`
3. Téléchargez et décompressez le fichier `124296-07.zip` dans le répertoire créé lors de l'étape précédente.
4. Arrêtez tous les services Java ES 2005Q4.
5. Exécutez le script `AM7p7\scripts\prepatch.pl`.
6. Exécutez le fichier `AM7p7\124296-07.exe` pour installer le patch.
7. Exécutez le script `AM7p7\scripts\postpatch.pl`.
8. Redémarrez les services Java ES 2005Q4.
9. Redéployez les applications Access Manager. Voir "Remarques relatives à la post-installation" à la page 20 pour plus d'informations.
10. Exécutez le script `AM7p7\scripts\updateschema.pl` pour mettre à jour le schéma de service de Directory Server. Le script valide vos entrées et charge les fichiers. Le script écrit aussi le fichier journal suivant :

    javaes-install-directory`\AccessManager\AM70Patch-upgrade-schema-` *timestamp*
11. Redémarrez les services Java ES 2005Q4.

Suppression du patch pour Windows

Pour supprimer le patch pour Windows :

1. Connectez-vous à Windows en tant qu'administrateur.
2. Exécutez le fichier `Uninstall_124296-07.bat`.
3. Exécutez le script `AM7p7\scripts\postbackout.pl`.
4. Redéployez les applications Access Manager.
5. Redémarrez les services Java ES 2005Q4.

Remarque : Si vous retirez le patch, les modifications du schéma ajoutées par le script `AM7p7\scripts\updateschema.pl` ne sont pas supprimées de Directory Server. Vous n'avez, cependant, pas besoin de supprimer les modifications apportées manuellement au schéma car ces dernières n'affectent pas les fonctionnalités d'Access Manager ni son utilisation une fois le patch supprimé.

Instructions d'installation du patch pour les systèmes HP-UX

Pour installer ou supprimer le patch HP-UX, utilisez les commandes `swinstall` et `swremove`. Par exemple, pour installer le patch sur un système autonome :

```
# swinstall /var/spool/patch/126371-07
```

Ou, pour supprimer le patch d'un système autonome :

```
# swremove 126371-07
```

Pour plus d'informations sur les commandes `swinstall` et `swremove` , consultez l'aide en ligne de `swinstall` et `swremove` .

Après avoir installé ou supprimé le patch, vous devez redéployer les applications Access Manager comme décrit dans la section "Remarques relatives à la post-installation" à la page 20.

Après avoir redéployé les applications Access Manager, exécutez le script `updateschema.sh` (patch 5 et versions ultérieures) pour charger les fichiers XML et LDIF. Le script `updateschema.sh` est disponible après avoir installé le patch 7 dans le répertoire *patch-home-directory*`/120956-07/scripts` . Redémarrez le conteneur Web d'Access Manager après avoir exécuté les scripts `amconfig` et `updateschema.sh` .

Remarque : Si vous supprimez le patch, les modifications du schéma ajoutées au script `updateschema.sh` ne sont pas supprimées de Directory Server. Cependant, vous n'avez pas besoin de supprimer les modifications apportées manuellement au schéma, car ces dernières n'affectent ni les fonctionnalités d'Access Manager ni son utilisation une fois le patch supprimé.

Pour plus d'informations sur le déploiement d'Access Manager sous HP-UX, reportez-vous aux *Sun Java System Access Manager 7 2005Q4 Release Notes for HP-UX*.

Remarques relatives à la post-installation

Ces remarques après l'installation du patch Access Manager 7 2005Q4 sont :

- "CR# 6254355 : Les patchs d'Access Manager ne déploient pas les applications Access Manager dans des scripts postpatch." à la page 20
- "CR# 6436409 : Redéploiement des fichiers WAR d'authentification distribuée et de SDK client" à la page 23

CR# 6254355 : Les patchs d'Access Manager ne déploient pas les applications Access Manager dans des scripts postpatch.

Le programme d'installation du patch peut ne pas conserver certains fichiers personnalisés et les remplace par des versions standard. Pour vous aider à identifier, puis à mettre à jour le contenu personnalisé d'un fichier WAR, suivez la procédure suivante.

Dans les exemples suivants, *AccessManager-base* correspond au répertoire d'installation de base. Le répertoire d'installation de base par défaut est `/opt` sous Solaris et `/opt/sun` sous Linux.

Sous Windows, *AccessManager-base* est *javaes-install-directory*`\AccessManager`. Exemple : `C:\Program Files\Sun\AccessManager`

Les fichiers WAR mis en patch sont :

- `console.war`

- `password.war`
- `services.war`

Ces fichiers sont situés dans *AccessManager-base*`/SUNWam` sous Solaris et *AccessManager-base*`/identity` sous Linux.

Sur les systèmes Windows : les fichiers WAR appartenant au patch figurent dans *AccessManager-base*`\`.

Le contenu modifiable d'un fichier WAR inclut :

- Fichiers de propriétés :
  - Systèmes Solaris : *AccessManager-base*`/SUNWam/locale/*.properties`
  - Systèmes Linux : *AccessManager-base*`/identity/locale/*.properties`
  - Systèmes Windows : *AccessManager-base*`\locale\*.properties`
- Descripteurs de bibliothèque de balises :
  - Systèmes Solaris : *AccessManager-base*`/SUNWam/web-src/applications/WEB-INF/*.tld`
  - Systèmes Linux : *AccessManager-base*`/identity/web-src/applications/WEB-INF/*.tld`
  - Systèmes Windows : *AccessManager-base*`\web-src\applications\WEB-INF\*.tld`
- Le fichier `web.xml` et les fichiers utilisés pour le créer (`WEB-INF/web.xml` et `WEB-INF/*.xml`)
- Les fichiers spécifiques à l'application : Fichiers JSP (`*.jsp`), image (`*.gif`) et feuilles de styles (couleurs d'arrière-plan, tailles de police, etc.) (`*.css`)

Pour conserver toutes les personnalisations, suivez les étapes ci-dessous. Sauvegardez toujours un fichier avant d'y apporter des modifications.

1. Installez le patch.
2. Ouvrez les fichiers WAR dans un répertoire temporaire. Par exemple, lorsque Access Manager est installé dans le répertoire par défaut sous Solaris :

   ```
   # cd temporary-directory
   # jar -xvf /opt/SUNWam/console.war
   # jar -xvf /opt/SUNWam/services.war
   # jar -xvf /opt/SUNWam/password.war
   ```

3. Consultez les fichiers ouverts pour savoir si le programme d'installation a apporté des modifications à vos fichiers personnalisés et ajoutez vos personnalisations manuellement dans les fichiers modifiés du répertoire temporaire. Vous ne devez pas répéter les modifications des fichiers du répertoire *AccessManager-base*`/web-src/` mais non reproduites dans les fichiers WAR du patch.
4. Mettez à jour les fichiers WAR en fonction des fichiers modifiés : Par exemple, lorsque Access Manager est installé dans le répertoire par défaut sous Solaris :

```
# cd temporary-directory
# jar -uvf /opt/SUNWam/console.war $path/$modified file
# jar -uvf /opt/SUNWam/services.war $path/$modified file
# jar -uvf /opt/SUNWam/password.war $path/$modified file
```

Par exemple, pour les étapes 2 à 4 :

```
# mkdir /tmp/war.tmp
# cd /tmp/war.tmp
# jar -xvf /opt/SUNWam/services.war
# vi index.html
# jar -uvf /opt/SUNWam/services.war index.html
```

5. Réutilisez le fichier de configuration (`amsilent`) généré par le patch ou créez-en un nouveau basé sur le modèle `amsamplesilent`, puis définissez les variables de configuration appropriées du fichier, notamment :
   - `DEPLOY_LEVEL=21`
   - `DIRECTORY_MODE=5`
   - Les mots de passe pour `DS_DIRMGRPASSWD`, `ADMINPASSWD` et `AMLDAPUSERPASSWD`
   - Variables du conteneur Web d'Access Manager

   Sous Windows, réutilisez le fichier silencieux de configuration (`amsilent`) généré par le script `postpatch.pl` et assurez-vous que *AccessManager-base*`\setup\AMConfigurator.properties-tmp` possède des valeurs valides. Renommez ensuite ce fichier en *AccessManager-base* `\setup\AMConfigurator.properties`.

   Pour plus d'informations sur les variables du conteneur Web, consultez le fichier `amsamplesilent` du répertoire `/opt/SUNWam/bin` sur les systèmes Solaris ou du répertoire `/opt/sun/identity/bin` sur les systèmes Linux.

   Sous Windows, le fichier de configuration est *AccessManager-base*`\setup\AMConfigurator.properties`.

6. Exécutez le script `amconfig` comme illustré ci-dessous. Directory Server et le conteneur Web d'Access Manager doivent être en cours d'exécution avant d'exécuter `amconfig`. Par exemple, pour exécuter `amconfig` sur un système Solaris sur lequel Access Manager est installé dans le répertoire d'installation de base par défaut :

```
# cd /opt/SUNWam/bin
# ./amconfig -s /opt/SUNWam/amsilent
```

7. Redémarrez les processus d'Access Manager une fois le script `amconfig` exécuté. Exemple :

```
# cd /opt/SUNWam/bin
# ./amserver stop
# ./amserver start
```

8. Assurez-vous que tous les fichiers JSP personnalisés résident dans les sous-répertoires appropriés du répertoire *AccessManager-base*`/SUNWam/web-src/` sous Solaris ou *AccessManager-base* `/identity/web-src/` sous Linux et que vous les avez tous sauvegardés.

   Sous Windows, les fichiers figurent dans *AccessManager-base*`\web-src\` .
9. Redémarrez le conteneur Web d'Access Manager.

Pour plus d'informations sur l'exécution du script `amconfig`, reportez-vous à : Chapitre 1, "Access Manager 7 2005Q4 Configuration Scripts" du *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

CR# 6436409 : Redéploiement des fichiers WAR d'authentification distribuée et de SDK client

Si vous utilisez l'authentification distribuée ou le SDK client, recréez ou redéployez le fichier WAR d'authentification distribuée et/ou le fichier WAR de SDK client après avoir installé le patch. Pour plus d'informations, reportez-vous aux documents suivants :

- Création du fichier WAR d'authentification distribuée : *Technical Note: Using Access Manager Distributed Authentication*
- Création du fichier WAR de SDK client : "Installing the Client SDK" du *Sun Java System Access Manager 7 2005Q4 Developer's Guide*
- Déploiement du fichier WAR de SDK client : "To Deploy amclientwebapps.war" du *Sun Java System Access Manager 7 2005Q4 Developer's Guide*

Access Manager 7 2005Q4 Patch 6

Le patch 6 (révision 6) d'Access Manager 7 résout de nombreux problèmes, répertoriés dans le fichier LISEZMOI acompagnant le patch. Le patch 6 comprend également les nouvelles fonctionnalités, les problèmes et les mises à jour de la documentation ci-après.

Nouvelles fonctions du patch 6

- "Access Manager prend en charge la méthode `setReadTimeout` `HttpURLConnection` de JDK 1.5 " à la page 24
- "Access Manager SDK rétablit le serveur d'annuaire principal après une remise en service du noeud principal" à la page 25
- "Les instances multiples d'Access Manager sont consignées dans des fichiers journaux distincts" à la page 25
- "Access Manager 7 autorise plusieurs domaines de cookie" à la page 26
- "Le plug-in de post-authentification de Microsoft IIS 6.0 prend en charge SharePoint Server" à la page 26
- "Access Manager prend en charge Internet Explorer 7" à la page 27

Problèmes et restrictions connus du patch 6

- "CR# 6379325 Accéder à la console pendant le basculement de session renvoie une exception de pointeur null" à la page 27
- "CR# 6508103 : sous Windows, cliquer sur Aide dans la console d'administration renvoie une erreur d'application" à la page 27
- "CR# 6564877 : l'installation du patch 7 d'Access Manager entraîne l'écrasement des fichiers SAML v2" à la page 28

Remarque – Avant d'installer le patch 6, nous vous recommandons de mettre à niveau ou d'appliquer un patch aux composants suivants :

- Si vous utilisez Sun Java System Web Server 6.1 SP5 ou une version ultérieure, procédez à une mise à niveau vers Web Server 6.1 SP7, cette version étant disponible sur le site :

  `http://www.sun.com/download/products.xml?id=45c90ca9`

  Suivez la procédure de mise à niveau comme indiqué dans la section "Mise à niveau" du *Notes de version de Sun Java System Web Server 6.1 SP8*.
- Téléchargez et installez le dernier patch sur la sécurité pour NSS, JSS et NSPR depuis SunSolve Online :`http://sunsolve.sun.com`
  - Plates-formes Solaris 8 SPARC : 119209
  - Plates-formes Solaris 8 x86 : 119210
  - Plates-formes Solaris 9 SPARC : 119211
  - Plates-formes Solaris 9 x86 : 119212
  - Plates-formes Solaris 10 SPARC : 119213
  - Plates-formes Solaris 10 x86 et AMD64 : 119214
  - Systèmes Windows : 124392
  - Systèmes HP-UX : 124379

Access Manager prend en charge la méthode `setReadTimeout` `HttpURLConnection` de JDK 1.5

Pour prendre en charge la méthode `setReadTimeout`, le fichier `AMConfig.properties` inclut la nouvelle propriété suivante qui vous permet de définir la valeur du délai d'attente de lecture :

```
com.sun.identity.url.readTimeout
```

Si le conteneur Web utilise JDK 1.5, définissez cette propriété sur une valeur appropriée qui provoque le dépassement du délai des connexions, afin d'éviter qu'un trop grand nombre de `HttpURLConnections` ouvertes n'entraîne une suspension du serveur. La valeur par défaut est 30 000 millisecondes (30 secondes).

La méthode `setReadTimeout` est ignorée si `com.sun.identity.url.readTimeout` ne figure pas dans le fichier `AMConfig.properties` ou s'il est défini sur une chaîne vide.

Access Manager SDK rétablit le serveur d'annuaire principal après une remise en service du noeud principal

Si Sun Java System Directory Server est configuré pour une réplication multimaître (MMR), le SDK d'Access Manager rétablit le serveur d'annuaire principal après une panne et une remise en service immédiate du serveur principal. Auparavant, le SDK d'Access Manager continuait d'accéder au serveur d'annuaire secondaire, même après la remise en service du serveur principal.

Pour prendre en charge ce nouveau comportement, Access Manager inclut la nouvelle propriété suivante dans le fichier `AMConfig.properties` :

```
com.sun.am.ldap.fallback.sleep.minutes
```

Cette propriété définit la période en minutes pendant laquelle une instance de serveur d'annuaire secondaire est mise en veille avant de revenir au serveur principal une fois le serveur principal remis en service. La valeur par défaut est 15 minutes.

La propriété `com.sun.am.ldap.fallback.sleep.minutes` est masquée. Pour définir cette propriété sur une valeur différente de la valeur par défaut (15 minutes), ajoutez-la explicitement au fichier `AMConfig.properties`. Par exemple, pour définir la valeur sur 7 minutes :

```
com.sun.am.ldap.fallback.sleep.minutes=7
```

Pour que la nouvelle valeur soit validée, redémarrez le conteneur Web d'Access Manager.

Les instances multiples d'Access Manager sont consignées dans des fichiers journaux distincts

Les instances multiples d'Access Manager exécutées sur le même serveur hôte peuvent désormais être consignées dans des fichiers journaux distincts résidant dans différentes sous-répertoires de journalisation en définissant la nouvelle propriété suivante dans le fichier `AMConfig.properties` :

```
com.sun.identity.log.logSubdir
```

Si vous ne modifiez pas le répertoire de journalisation par défaut dans la console d'administration, les répertoires de journalisation par défaut sont les suivants :

- Systèmes Solaris : `/var/opt/SUNWam/logs`
- Systèmes Linux et HP-UX : `/var/opt/sun/identity/logs`
- Systèmes Windows : `C:\Sun\JavaES5\identity\logs`

La première instance d'Access Manager est toujours consignée dans le répertoire de journalisation par défaut. Pour spécifier d'autres sous-répertoires de journalisation pour des instances d'Access Manager supplémentaires, définissez la propriété `com.sun.identity.log.logSubdir` dans le fichier `AMConfig.properties` pour chaque nouvelle instance d'Access Manager.

Par exemple, si vous disposez de trois instances, `am-instance-1`, `am-instance-2`, et `am-instance-3`, toutes exécutées sur le même serveur hôte Solaris, définissez la propriété comme suit :

```
com.sun.identity.log.logSubdir=am-instance-2
com.sun.identity.log.logSubdir=am-instance-3
```

La propriété `com.sun.identity.log.logSubdir` est masquée. Vous devez ajouter explicitement cette propriété au fichier `AMConfig.properties` approprié et redémarrer le conteneur Web d'Access Manager pour que les valeurs de sous-répertoires soient validées.

Les instances d'Access Manager sont ensuite consignées dans les répertoires suivants :

`/var/opt/SUNWam/logs/`*log-files-for-am-instance-1*
`/var/opt/SUNWam/logs/am-instance-2/`*log-files-for-am-instance-2*
`/var/opt/SUNWam/logs/am-instance-3/`*log-files-for-am-instance-3*

Access Manager 7 autorise plusieurs domaines de cookie

Pour prendre en charge plusieurs domaines de cookie, Access Manager inclut la nouvelle propriété suivante :

```
com.sun.identity.authentication.setCookieToAllDomains
```

La valeur par défaut est `true`. Cette nouvelle propriété est masquée. Pour définir la valeur sur `false`, ajoutez explicitement la propriété au fichier `AMConfig.properties` et redémarrez le conteneur Web d'Access Manager.

Le plug-in de post-authentification de Microsoft IIS 6.0 prend en charge SharePoint Server

Le plug-in d'authentification de Microsoft Internet Information Services (IIS) 6.0 prend en charge Microsoft Office SharePoint Server. Un utilisateur peut se connecter à Access Manager à l'aide d'un ID utilisateur ou d'un nom de connexion. SharePoint Server accepte néanmoins un nom de connexion, ce qui pose problème lorsque l'utilisateur spécifie un ID utilisateur.

Pour permettre la connexion à SharePoint Server, le plug-in de post-authentification (`ReplayPasswd.java`) utilise maintenant la nouvelle propriété suivante :

```
com.sun.am.sharepoint_login_attr_name
```

Cette nouvelle propriété indique l'attribut utilisateur employé par SharePoint Server pour l'authentification. Par exemple, la propriété suivante spécifie le nom commun (`cn`) pour l'authentification :

```
com.sun.am.sharepoint_login_attr_name=cn
```

Le plug-in de post-authentification lit la propriété `com.sun.am.sharepoint_login_attr_name` et obtient la valeur d'attribut correspondante pour l'utilisateur de Directory Server. Le plug-in définit ensuite les en-têtes d'autorisation qui permettent à l'utilisateur d'accéder à SharePoint Server.

Cette propriété est masquée. Pour définir la propriété, ajoutez-la explicitement au fichier `AMConfig.properties`, puis redémarrez le conteneur Web d'Access Manager pour que la valeur soit validée.

Access Manager prend en charge Internet Explorer 7

Le patch 6 d'Access Manager 7 2005Q4 prend maintenant en charge Microsoft Windows Internet Explorer 7.

CR# 6379325 Accéder à la console pendant le basculement de session renvoie une exception de pointeur null

Dans ce scénario, plusieurs serveurs Access Manager sont déployés en mode basculement de session derrière un équilibreur de charge configuré pour le routage des demandes d'association basé sur des cookies. L'administrateur d'Access Manager accède à la console Access Manager via l'équilibreur de charge. Lorsque l'administrateur se connecte à la console, la session est créée sur l'un des serveurs Access Manager. Si ce serveur tombe en panne, la session de la console bascule comme prévu vers un autre serveur Access Manager. Cependant, l'administrateur rencontre parfois des exceptions de pointeur null intermittentes sur le navigateur et dans le journal d'erreurs du conteneur Web.

Ce problème ne concerne que la session active de la console Access Manager au moment du basculement et n'affecte pas le fonctionnement des serveurs Access Manager.

Solution : pour empêcher ces exceptions de pointeur null intermittentes de se produire :

- Pour une solution temporaire, actualisez le navigateur ou bien déconnectez-vous, puis reconnectez-vous à la console.
- Pour une solution permanente, déployez la console Access Manager sur une instance d'Access Manager distincte ne participant pas au basculement de session.

CR# 6508103 : sous Windows, cliquer sur Aide dans la console d'administration renvoie une erreur d'application

Sous Windows 2003 Édition Entreprise avec Access Manager déployé sur Sun Java System Application Server dans un environnement linguistique autre que l'anglais, cliquer sur Aide dans la console en mode Domaine d'administration renvoie une erreur d'application.

Solution :

1. Copiez le fichier *javaes-install-dir*`\share\lib\jhall.jar` dans le répertoire `%JAVA_HOME%\jre\lib\ext`.

où *javaes-install-dir* correspond au répertoire d'installation de Windows

2. Redémarrez l'instance du serveur d'application.

CR# 6564877 : l'installation du patch 7 d'Access Manager entraîne l'écrasement des fichiers SAML v2

Si le plug-in SAML v2 est installé, l'installation du patch entraîne l'écrasement des fichiers associés à SAML v2 et le script`postpatch` affiche le message suivant :

```
Le script postpatch a détecté que le plug-in SAML v2 est installé dans votre
environnement. Lorsque vous exécutez le script amconfig pour redéployer les
applications Access Manager, le script recrée le fichier amserver.war et les
fichiers associés à SAML v2 sont perdus. Par conséquent, une fois le script
amconfig exécuté, recréez et redéployez le fichier amserver.war, comme décrit
dans le Guide de l'utilisateur du plug-in Sun Java System SAML v2 pour les
services de fédération.
```

Solution : après avoir installé le patch et exécuté le script `amconfig`, recréez et redéployez le fichier `amserver.war` pour les déploiements de Federation Manager ou d'Access Manager qui utilisent le plug-in SAML v2.

Pour les étapes spécifiques, reportez-vous au Chapitre 2, “Installing the SAML v2 Plug-in for Federation Services” du *Sun Java System SAML v2 Plug-in for Federation Services User's Guide*.

Access Manager 7 2005Q4 Patch 5

Le patch 5 (révision 5) d'Access Manager 7 résout de nombreux problèmes, répertoriés dans le fichier LISEZMOI accompagnant le patch. Le patch 5 comprend également les nouvelles fonctionnalités, les problèmes et les mises à jour de la documentation ci-après.

Nouvelles fonctions du patch 5

- “Prise en charge des systèmes HP-UX ” à la page 30
- “Prise en charge des systèmes Microsoft Windows” à la page 30
- “Nouveau script `updateschema.sh` de chargement des fichiers LDIF et XML” à la page 30
- “Prise en charge des valeurs de délai d'attente de session inactive d'une application spécifique” à la page 32
- “Déploiement possible du servlet CDC sur un serveur d'interface utilisateur d'authentification distribuée” à la page 33
- “Spécification possible du domaine lors de la redirection vers l'URL de connexion d'Access Manager par le servlet CDC” à la page 33
- “Utilisation possible de la valeur UPN par l'authentification des certificats pour mapper le profil utilisateur ” à la page 34
- “Exécution du traitement post-authentification de la déconnexion dans un environnement de serveur multiple” à la page 34

- "Prise en charge d'une nouvelle interface SPI d'identificateur de nom par SAML" à la page 34
- "Nouvelles propriétés de configuration pour le contrôle de site" à la page 34
- "L'utilisateur n'a plus à s'authentifier deux fois dans la chaîne d'authentification" à la page 35
- "Modifications apportées aux scripts de réglage des performances" à la page 35
- "Authentification de base dans l'agent de stratégie IIS 6.0" à la page 39

Problèmes et restrictions connus du patch 5

- "CR# 6567746 : sous HP-UX, le patch 5 d'Access Manager renvoie une valeur errorCode incorrecte si le nombre de nouvelles tentatives de saisie du mot de passe est dépassé" à la page 40
- "CR# 6527663 : la valeur par défaut de la propriété `com.sun.identity.log.resolveHostName` doit être `false` au lieu de `true`" à la page 40
- "CR# 6527528 : la suppression du patch conserve le mot de passe `amldapuser` en clair dans les fichiers XML" à la page 40
- "CR# 6527516 : le serveur plein sur WebLogic exige que les fichiers JAR de JAX-RPC 1.0 communiquent avec le SDK client" à la page 40
- "CR # 6523499 : fichier `amsilent` du patch 5 lisible par tous les utilisateurs sous Linux" à la page 41
- "CR# 6520326 : l'application du patch 5 sur une deuxième instance d'Access Manager sur un serveur écrase le fichier `serverconfig.xml` de la première instance" à la page 42
- "CR# 6520016 : l'installation du patch 5 sur une machine SDK uniquement écrase les fichiers makefile échantillon" à la page 42
- "CR#6515502 : le plug-in de référentiel LDAPv3 ne gère pas toujours correctement l'attribut de recherche d'alias" à la page 43
- "CR# 6515383 : l'authentification distribuée et l'agent J2EE ne fonctionnent pas dans le même conteneur Web" à la page 43
- "CR# 6508103 : l'aide en ligne renvoie une erreur d'application si le serveur d'application fonctionne sous Windows" à la page 43
- "CR# 6507383 et CR# 6507377 : l'authentification distribuée nécessite un paramètre d'URL `goto` explicite" à la page 43
- "CR# 6402167 : LDAP JDK 4.18 provoque des problèmes au niveau du client LDAP/Directory Server" à la page 44
- "CR# 6352135 : les fichiers du serveur d'interface utilisateur d'authentification distribuée ne sont pas installés au bon emplacement" à la page 44
- "CR# 6513653 : la configuration de la propriété `com.iplanet.am.session.purgedelay` peut provoquer un problème" à la page 45

Problèmes liés à la globalisation (g11n)

- "CR# 6522720 : il est impossible d'effectuer une recherche de caractères multioctets dans l'aide en ligne de la console sous Windows et HP-UX" à la page 44
- "CR# 6524251 : les caractères multioctets des messages sortants sont tronqués pendant la configuration d'Access Manager sous Windows" à la page 44
- "CR# 6526940 : les touches de propriété apparaissent à la place du texte pendant l'installation du patch 5 dans une autre langue que l'anglais sous Windows" à la page 45

Mises à jour de la documentation

- "Access Manager ne peut pas rebasculer en mode Hérité à partir du mode Domaine (6508473)" à la page 101
- "Obtention de davantage d'informations sur la désactivation des recherches persistantes (6486927)" à la page 102
- "Documentation des privilèges d'Access Manager pris et non pris en charge (2143066)" à la page 103
- "Documentation du routage des demandes d'association basé sur des cookies (6476922)" à la page 103
- "Documentation de la configuration de Windows Desktop SSO pour Windows 2003 (6487361)" à la page 104
- "Documentation des étapes de configuration des mots de passe du serveur d'interface utilisateur d'authentification distribuée (6510859)" à la page 105
- "L'aide en ligne sur la création d'un nouveau nom de site demande plus d'informations (2144543)" à la page 106
- "Le paramètre de configuration du mot de passe administrateur est`ADMIN_PASSWD` sous Windows (6470793)" à la page 106

Prise en charge des systèmes HP-UX

Le patch **126371** prend en charge les systèmes HP-UX. Pour davantage d'informations, consultez les rubriques:

- "Instructions d'installation du patch pour les systèmes HP-UX" à la page 19
- "Remarques relatives à la post-installation" à la page 20

Pour plus d'informations sur l'installation sous HP-UX, consultez le *Guide d'installation de Sun Java Enterprise System 2005Q4 pour UNIX*.

Prise en charge des systèmes Microsoft Windows

Le patch **124296** prend en charge les systèmes Windows. Pour davantage d'informations, consultez les rubriques:

- "Instructions d'installation du patch pour les systèmes Windows" à la page 18
- "Remarques relatives à la post-installation" à la page 20
- "Disponibilité des scripts de réglage pour Windows" à la page 38

Pour plus d'informations sur l'installation sous Windows, consultez le *Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows* .

Nouveau script `updateschema.sh` de chargement des fichiers LDIF et XML

Le patch 5 (et version ultérieure) inclut le script `updateschema.sh` qui permet de charger les fichiers suivants pour mettre à jour le schéma du service Directory Server :

- `AddLDAPFilterCondition.xml`
- `amPolicyConfig_mod_ldfc.xml`
- `accountLockoutData.xml`
- `accountLockout.ldif`
- `idRepoServiceAddAttrSchemaRequest_Cache.xml`
- `wsf1.1_upgrade.xml`
- `amAuth_mod.xml`
- `amAuthCert_mod.xml`

Dans les précédentes versions de patch pour Access Manager, il était nécessaire de charger ces fichiers manuellement.

Pour exécuter le script `updateschema.sh` :

1. Connectez-vous en tant que superutilisateur (`root`).
2. Accédez au répertoire des patchs.
3. Exécutez le script. Par exemple, sur les systèmes Solaris :

   ```
   # cd /120954-07
   # ./updateschema.sh
   ```

   Sous Windows, le script est `updateschema.pl`.
4. Lorsque le script vous y invite, entrez les éléments suivants :
   - Nom d'hôte et numéro de port de Directory Server
   - DN utilisateur admin et mot de passe de Directory Server
   - DN `amadmin` et mot de passe
5. Le script valide vos entrées et charge les fichiers. Le script écrit aussi le fichier journal suivant :
   - Systèmes Solaris : `/var/opt/SUMWam/logs/AM70Patch.upgrade.schema.` *timestamp*
   - Systèmes Linux : `/var/opt/sun/identity/logs/AM70Patch.upgrade.schema.` *timestamp*
6. Une fois le script terminé, redémarrez le conteneur Web d'Access Manager.

Remarque Si vous supprimez le patch 5, les modifications apportées au schéma ajoutées au script `updateschema.sh` ne sont pas supprimées de Directory Server. Vous n'avez, cependant, pas besoin de supprimer les modifications apportées manuellement au schéma car ces dernières n'affectent pas les fonctionnalités d'Access Manager ni son utilisation une fois le patch supprimé.

Prise en charge des valeurs de délai d'attente de session inactive d'une application spécifique

Le patch 5 permet à différentes applications d'avoir différentes valeurs de délai d'attente de session inactive. Dans une entreprise, certaines applications peuvent nécessiter des valeurs de délai d'attente de session inférieures aux valeurs de délai d'attente de session spécifiées dans le service de la session. Vous avez, par exemple, spécifié une valeur de délai d'attente de session de 30 minutes dans le service de la session mais une application HR doit se déconnecter dès qu'un utilisateur est inactif pendant plus de 10 minutes.

Conditions requises pour utiliser cette fonctionnalité :

- Les agents protégeant l'application doivent être configurés pour appliquer les décisions concernant la stratégie relative aux URL depuis Access Manager.
- Les agents doivent être configurés pour s'exécuter en mode cache de décision de stratégie automatique. Consultez les propriétés suivantes :
  - Pour les agents Web : `com.sun.am.policy.am.fetch_from_root_resource`
  - Pour les agents J2EE : `com.sun.identity.policy.client.cacheMode`
- Le fichier `AMConfig.properties` d'Access Manager doit spécifier un ordre d'évaluation du composant de stratégie de sorte que la Condition soit évaluée en dernier. Consultez la propriété suivante :

  `com.sun.identity.policy.Policy.policy_evaluation_weights`
- La Condition sur Access Manager ne connaîtra pas l'accès à l'application autorisé par l'agent en fonction de la décision stockée en mémoire cache localement. Par conséquent, le délai d'attente réel d'inactivité de l'application se situera entre le délai d'attente d'inactivité de l'application et le délai d'attente d'inactivité de l'application moins la durée de stockage en mémoire cache de l'agent.

Pour utiliser cette fonctionnalité :

- Ajoutez la condition du plan d'authentification aux stratégies de protection de l'application nécessitant le délai d'attente d'inactivité de la session propre à l'application.
- Spécifiez le nom de l'application et la valeur du délai d'attente dans la condition du plan d'authentification.
- Utilisez le même nom d'application et la même valeur de délai d'attente dans toutes les stratégies applicables aux ressources de l'application.
- Spécifiez la valeur du délai d'attente en minutes. Si la valeur est égale à 0 ou supérieure à la valeur de délai d'attente d'inactivité de la session spécifié dans le service de la session, la valeur est ignorée et le délai d'attente du service de la session est appliqué.

Par exemple, imaginez une stratégie `http://host.sample.com/hr/*` avec la condition de plan d'authentification suivante :

- Schéma d'authentification : LDAP

- Nom de l'application : HR
- Valeur du délai d'attente : 10

Si plusieurs stratégies sont définies pour protéger les ressources de l'application HR, vous devez ajouter la condition à toutes les stratégies.

Lorsqu'un utilisateur d'une session distincte tente d'accéder à l'application HR protégée par l'agent d'Access Manager, il est invité à s'authentifier pour le plan LDAP (si ce n'est pas déjà fait).

Si l'utilisateur s'est déjà authentifié sur le plan LDAP, il dispose d'une autorisation d'accès à condition qu'il se soit écoulé moins de 10 minutes depuis sa dernière authentification ou depuis son dernier accès à l'application HR. Dans le cas contraire, il est invité à s'authentifier à nouveau sur le plan LDAP pour accéder à l'application.

Déploiement possible du servlet CDC sur un serveur d'interface utilisateur d'authentification distribuée

Le servlet CDC peut coexister avec un serveur d'interface utilisateur d'authentification distribuée dans la DMZ pour activer la connexion unique interdomaine (CDSSO). Il est possible de déployer le serveur Access Manager derrière un pare-feu. Par ailleurs, tous les accès à Access Manager dédiés à l'exécution d'une connexion unique interdomaine sont gérés par le servlet CDC dans le serveur d'interface utilisateur d'authentification distribuée. Pour activer la connexion unique interdomaine, consultez la documentation de l'agent de stratégie spécifique et exécutez la procédure complémentaire suivante :

- Modifiez le fichier `AMAgent.properties` pour pointer le servlet CDC sur le serveur d'authentification distribuée côté client. Par exemple, pour les agents Web, modifiez la propriété suivante :

  ```
  com.sun.am.policy.agents.config.cdcservlet.url=
      http://DAhost.DAdomain:DAport/DISTAUTH_DEPLOY_URI/cdcservlet
  ```

- Définissez les stratégies requises dans Access Manager pour les ressources que l'agent doit protéger. Par exemple, si l'agent se situe à l'emplacement `host.example.com:80` , définissez une stratégie pour la ressource comme suit : `http://host.example.com:80/*` .

Spécification possible du domaine lors de la redirection vers l'URL de connexion d'Access Manager par le servlet CDC

Vous pouvez à présent spécifier un nom de domaine sur le servlet CDC, de sorte à inclure le nom du domaine lors de la redirection vers l'URL de connexion d'Access Manager et à permettre à l'utilisateur de se connecter au domaine spécifique. Exemple :

```
com.sun.am.policy.agents.config.cdcservlet.url=
    http://lb.example.com/amserver/cdcservlet?org=realm1
```

Utilisation possible de la valeur UPN par l'authentification des certificats pour mapper le profil utilisateur

Auparavant, l'authentification des certificats n'utilisait que le composant `dn` dans le `subjectDN` pour mapper un profil utilisateur. Access Manager prend désormais en charge la valeur UPN (nom principal de l'utilisateur) dans `SubjectAltNameExt` pour mapper le profil.

Exécution du traitement post-authentification de la déconnexion dans un environnement de serveur multiple

Le traitement post-authentification est désormais exécuté lorsqu'un utilisateur se déconnecte d'un autre serveur que celui auquel il était initialement connecté dans un environnement de serveur multiple, qu'un basculement de session soit ou non configuré.

Prise en charge d'une nouvelle interface SPI d'identificateur de nom par SAML

SAML prend désormais en charge une nouvelle interface SPI d'identificateur de nom permettant à un site de personnaliser l'identificateur de nom dans l'assertion SAML. Un site peut mettre en œuvre la nouvelle interface `NameIdentifierMapper` pour mapper un compte utilisateur sur un identificateur de nom dans le cadre d'une assertion SAML.

Nouvelles propriétés de configuration pour le contrôle de site

La fonctionnalité de surveillance de site d'Access Manager intègre les nouvelles propriétés suivantes, afin que vous puissiez spécifier le comportement du contrôle d'état du site.

Propriété	Description
`com.sun.identity.urlchecker.invalidate.interval`	Intervalle de détection d'un site hors service ou qui ne répond pas exprimé en millisecondes. Par défaut : 70 000 millisecondes (70 secondes).
`com.sun.identity.urlchecker.sleep.interval`	Intervalle de temps en millisecondes pendant lequel le contrôle d'état du site est en sommeil. Par défaut : 30 000 millisecondes (30 secondes).
`com.sun.identity.urlchecker.targeturl`	Autre URL cible pour le contrôle de l'état du processus d'Access Manager. Par défaut : `"/amserver/namingservice"`.

Le patch n'ajoute pas ces propriétés au fichier `AMConfig.properties` . Pour utiliser ces nouvelles propriétés avec des valeurs autres que celles par défaut :

1. Ajoutez les propriétés et leurs valeurs au fichier `AMConfig.properties` . Pour les agents de stratégie, ajoutez ces propriétés au fichier `AMAgents.properties` .
2. Redémarrez le conteneur Web d'Access Manager pour appliquer les valeurs.

L'utilisateur n'a plus à s'authentifier deux fois dans la chaîne d'authentification

Étudiez le scénario suivant. Un site configure une chaîne d'authentification avec trois modules LDAP. Tous les modules sont configurés sur `SUFFICIENT` et les options `iplanet-am-auth-shared-state-enabled` et `iplanet-am-auth-store-shared-state-enabled` sont configurées sur `true`. Exemple :

```
<AttributeValuePair>
   <Value>A-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>B-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>C-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
</AttributeValuePair>
```

Le patch 5 ajoute la nouvelle option `iplanet-am-auth-shared-state-behavior-pattern` aux options du module. Cette option peut prendre deux valeurs : `tryFirstPass` (par défaut) et `useFirstPass`.

Pour empêcher un utilisateur d'avoir à saisir deux fois son identifiant et son mot de passe pour s'authentifier (comme indiqué dans le scénario précédent), configurez cette nouvelle option sur `useFirstPass` pour tous les modules de la chaîne. Auparavant, un utilisateur qui n'existait que dans la troisième instance LDAP devait saisir son identifiant et son mot de passe deux fois pour s'authentifier.

Modifications apportées aux scripts de réglage des performances

Dans le patch 5 les modifications suivantes ont été apportées aux scripts de réglage des performances :

- “Prise en charge d'un fichier de mots de passe par les scripts de réglage” à la page 36
- “Le script de réglage supprime les ACI inutiles de Directory Server” à la page 36
- “Réglage possible du conteneur Web du serveur d'interface utilisateur d'authentification distribuée par les scripts de réglage” à la page 36
- “Réglage des systèmes d'exploitation Solaris et Linux au moyen d'un script `amtune-os` unique” à la page 37
- “Exécution complète des scripts de réglages dans une zone locale de Solaris 10” à la page 38

- "Disponibilité des scripts de réglage pour Windows" à la page 38
- "Réglages à prendre en compte pour les serveurs Sun Fire T1000 et T2000" à la page 38

Voir aussi "CR# 6527663 : la valeur par défaut de la propriété `com.sun.identity.log.resolveHostName` doit être `false` au lieu de `true`" à la page 40.

Prise en charge d'un fichier de mots de passe par les scripts de réglage

Le patch 5 vous permet de spécifier des mots de passe dans un fichier texte pour les scripts de réglage. Auparavant, vous ne pouviez saisir de mots de passe que sous la forme d'un argument de ligne de commande, ce qui pouvait engendrer des problèmes de sécurité. Pour utiliser un fichier de mots de passe, configurez les variables suivantes dans le fichier, au besoin :

```
DS_ADMIN_PASSWORD=DirectoryServer-admin-password
AS_ADMIN_PASSWORD=ApplicationServer8-admin-password
```

Par exemple, pour régler Application Server 8 :

```
# ./amtune-as8 password-file
```

password-file contenant `AS_ADMIN_PASSWORD`, cette valeur étant définie sur le mot de passe administrateur d'Application Server 8.

Les scripts de réglage utilisent l'option `-j` *password-file* lorsqu'ils appellent les utilitaires `ldapmodify`, `ldapsearch`, `db2index` et `dsconf` de Directory Server.

Le script de réglage supprime les ACI inutiles de Directory Server

Si Access Manager 7 2005Q4 est installé en mode Domaine, les privilèges de délégation servent à déterminer les droits d'accès ; par conséquent, certains ACI de Directory Server ne sont pas requis. Le patch 5 d'Access Manager 7 2005Q4 vous permet de supprimer les ACI inutiles en exécutant le script `amtune-prepareDSTuner`. Ce script lit une liste d'ACI dans le fichier `remacis.ldif`, puis appelle l'utilitaire `ldapmodify` pour les supprimer.

Vous pouvez exécuter le script `amtune-prepareDSTuner` pour supprimer les ACI inutiles sous Solaris, Linux, HP-UX et Windows. Pour plus d'informations, y compris sur la manière d'exécuter le script, consultez le *Technical Note: Sun Java System Access Manager ACI Guide* .

Réglage possible du conteneur Web du serveur d'interface utilisateur d'authentification distribuée par les scripts de réglage

Une fois le serveur d'interface utilisateur d'authentification distribuée déployé sur un serveur Web, vous pouvez régler le conteneur Web en exécutant les scripts de réglage d'Access Manager. Les scripts de réglage suivants définissent la JVM, ainsi que d'autres options de réglage du conteneur Web concerné :

TABLEAU 2 Scripts de réglage du conteneur Web d'Access Manager

Conteneur Web	Script de réglage
`amtune-ws61`	Web Server6.1
`amtune-as7`	Application Server 7
`amtune-as8`	Application Server Enterprise Edition 8.1

Pour régler un conteneur Web pour un serveur d'interface utilisateur d'authentification distribuée :

1. Le serveur Access Manager n'étant pas installé sur le système sur lequel le serveur d'interface utilisateur d'authentification distribuée est déployé, copiez le script de réglage de conteneur Web approprié (indiqué dans le tableau précédent), le fichier de configuration `amtune-env` et le script `amtune-utils` depuis une installation du serveur Access Manager. Si vous souhaitez régler le système d'exploitation Solaris ou Linux, copiez également le script `amtune-os`.
2. Modifiez les paramètres dans le fichier de configuration `amtune-env` pour spécifier le conteneur Web et les options de réglage. Pour exécuter le script en mode REVIEW (de révision), configurez `AMTUNE_MODE=REVIEW` dans le fichier `amtune-env` .
3. Exécutez le script de réglage du conteneur Web en mode REVIEW. En mode REVIEW, le script suggère des modifications de réglage basées sur les valeurs contenues dans le fichier `amtune-env` mais n'apporte aucune modification réelle au déploiement.
4. Consultez les recommandations en matière de réglage dans le fichier journal de débogage. Modifiez le fichier `amtune-env` en fonction de cette exécution, au besoin.
5. Pour modifier les réglages, configurez le fichier `AMTUNE_MODE=CHANGE` dans `amtune-env`.
6. Exécutez le script de réglage en mode CHANGE (de modification) pour modifier les réglages du déploiement.

Pour plus d'informations sur l'exécution du script de réglage pour régler le conteneur Web d'Access Manager, consultez le Chapitre 2, “Access Manager Tuning Scripts” du *Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide*.

Réglage des systèmes d'exploitation Solaris et Linux au moyen d'un script `amtune-os` unique

Le patch 5 intègre un script `amtune-os` unique pour régler les systèmes d'exploitation Solaris et Linux. Le script détermine le type de système d'exploitation au moyen de la commande `uname -s`. Auparavant, Access Manager fournissait des scripts `amtune-os` distincts pour régler chaque système d'exploitation.

Exécution complète des scripts de réglages dans une zone locale de Solaris 10

Si Access Manager est installé dans une zone locale de Solaris 10, tous les scripts de réglage à l'exception du script `amtune-os` peuvent être exécutés dans la zone locale. Dans une zone locale, le script `amtune-os` affiche un message d'avertissement mais ne règle pas le système d'exploitation. Le script continue d'exécuter les autres scripts de réglage que vous avez demandés. Auparavant, dans une zone locale, l'exécution du script `amtune-os` était interrompue et aucun des scripts de réglage ultérieurs demandés ne s'exécutaient.

Dans une zone globale de Solaris 10, le script `amtune` appelle `amtune-os` pour régler le système d'exploitation, ainsi que les autres scripts que vous voulez exécuter.

Disponibilité des scripts de réglage pour Windows

Le patch 5 comprend des scripts de réglage de Windows. L'exécution des scripts de réglage sous Windows est similaire à l'exécution des scripts de réglage sous Solaris ou Linux, aux exceptions suivantes près :

- Les scripts pour Windows sont écrits en Perl et ne peuvent être exécutés sans Active Perl 5.8.
- Si vous réglez Directory Server, vous devez copier les fichiers `amtune-utils.pl`, `amtune-directory.pl`, `remacis.ldif` et `amtune-samplepassordfile` sur Directory Server après avoir exécuté le script `amtune-prepareDSTuner.pl` car ce dernier ne peut pas compresser ces fichiers.
- Aucun script de réglage de Windows n'est disponible.
- Aucune prise en charge des zones n'est fournie.
- Avant d'exécuter un script, vous devez configurer le paramètre `$BASEDIR` pour accéder au répertoire d'installation d'Access Manager dans le fichier `amtune-env.pl`.

Réglages à prendre en compte pour les serveurs Sun Fire T1000 et T2000

Si Access Manager est installé sur un serveur Sun Fire T1000 ou T2000, les scripts de réglage pour Web Server 6.1 et Application Server 8 fournis avec le patch 5 configurent le paramètre `JVM GC ParallelGCThreads` sur 8 :

```
-XX:ParallelGCThreads=8
```

Ce paramètre réduit le nombre de threads de libération de la mémoire qui pourrait être inutilement élevé sur un système prenant en charge 32 threads. Vous pouvez toutefois augmenter la valeur à 16, voire à 20, pour une machine CPU virtuelle 32 bits comme un serveur Sun Fire T1000 ou T2000, si cela permet de réduire les activités complètes de libération de la mémoire.

Par ailleurs, pour les systèmes Solaris SPARC intégrant un processeur CMT doté de la technologie CoolThreads, nous vous recommandons d'ajouter la propriété suivante à la fin du fichier `/etc/opt/SUNWam/config/AMConfig.properties` :

`com.sun.am.concurrencyRate=`*value*

La *value* par défaut est de 16, mais vous pouvez attribuer une valeur inférieure à cette propriété en fonction du nombre de composants de base que contient le serveur Sun Fire T1000 ou T2000.

Authentification de base dans l'agent de stratégie IIS 6.0

Pour activer l'authentification de base dans Microsoft Internet Information Services (IIS) 6.0, l'agent de stratégie doit obtenir le nom et le mot de passe de l'utilisateur. Le patch 5 intègre les nouvelles classes suivantes pour activer cette fonctionnalité à l'aide du chiffrement DES du mot de passe de l'utilisateur :

- `DESGenKey.java` génère une touche unique utilisée pour chiffrer et déchiffrer le mot de passe de l'utilisateur.
- `ReplayPasswd.java` lit la valeur de chiffrement à partir de la propriété `com.sun.am.replaypasswd.key` dans le fichier `AMConfig.properties`, chiffre le mot de passe et l'affecte à la propriété de session `sunIdentityUserPassword`.

Pour utiliser l'authentification de base dans IIS 6.0, vous devez exécuter la procédure suivante sur le serveur Access Manager et l'agent de stratégie IIS 6.0.

Sur le serveur Access Manager :

1. Exécutez `DESGenKey.java` pour générer une clé de chiffrement unique pour le chiffrement et le déchiffrement du mot de passe. Sous Solaris, le fichier `DESGenKey.java` figure dans le répertoire `com/sun/identity/common` présent dans `am_sdk.jar` dans le répertoire `/opt/SUNWam/lib`. Par exemple, la commande suivante génère une clé de chiffrement :

   ```
   # cd /opt/SUNWam/lib
   # java -cp am_sdk.jar com.sun.identity.common.DESGenKey
   ```

2. Attribuez la valeur de clé de chiffrement de l'étape 1 à la propriété `com.sun.am.replaypasswd.key` dans le fichier `AMConfig.properties`.
3. Déployez `ReplayPasswd.java` comme plug-in de post-authentification. Utilisez le nom de classe complet lors de la configuration du plug-in : `com.sun.identity.authentication.spi.ReplayPasswd .`

Sur l'agent de stratégie IIS 6.0 :

1. Attribuez la valeur de clé de chiffrement du côté serveur à la propriété `com.sun.am.replaypasswd.key` dans le fichier `AMAgent.properties` . Le serveur Access Manager et l'agent de stratégie IIS 6.0 doivent utiliser la même clé de chiffrement.
2. Activez l'authentification de base dans le gestionnaire d'IIS 6.0.

L'agent de stratégie IIS 6.0 lit le mot de passe chiffré de la réponse de session, déchiffre le mot de passe à partir de la propriété`com.sun.am.replaypasswd.key` et configure les en-têtes d'authentification pour permettre le fonctionnement de l'authentification de base.

Pour plus d'informations sur l'agent de stratégie IIS 6.0, consultez le *Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0* .

CR# 6567746 : sous HP-UX, le patch 5 d'Access Manager renvoie une valeur errorCode incorrecte si le nombre de nouvelles tentatives de saisie du mot de passe est dépassé

Lorsqu'un compte d'utilisateur est bloqué, le patch 5 d'Access Manager 7 2005Q4 sous HP-UX renvoie `errorCode = null` au lieu de `errorCode = 107` si le nombre de tentatives de saisie du mot de passe est dépassé.

Solution. aucune.

CR# 6527663 : la valeur par défaut de la propriété `com.sun.identity.log.resolveHostName` doit être `false` au lieu de `true`

Avant d'exécuter le script de réglage `amtune-identity`, nous vous recommandons d'ajouter la propriété suivante, configurée sur `false`, dans le fichier `AMConfig.properties` :

```
com.sun.identity.log.resolveHostName=false
```

La valeur `false` réduit l'incidence de la résolution des noms d'hôte et peut, en conséquence, améliorer les performances. Cependant, si vous souhaitez imprimer le nom d'hôte de la machine cliente dans le journal `amAuthentication.access`, configurez cette valeur sur `true`.

CR# 6527528 : la suppression du patch conserve le mot de passe `amldapuser` en clair dans les fichiers XML

Si vous supprimez le patch 5 d'une installation complète du serveur Access Manager, les fichiers `amAuthLDAP.xml` et `amPolicyConfig.xml` contiennent le mot de passe `amldapuser` en clair. Ces fichiers figurent 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`

Solution : Modifiez les fichiers `amAuthLDAP.xml` et `amPolicyConfig.xml`, puis supprimez le mot de passe en clair.

CR# 6527516 : le serveur plein sur WebLogic exige que les fichiers JAR de JAX-RPC 1.0 communiquent avec le SDK client

Dans les patchs d'Access Manager 7 2005Q4, le script de configuration d'Access Manager pour BEA WebLogic Server (`amwl81config`) ajoute les fichiers JAR de JAX-RPC 1.1 au `classpath` de l'instance WebLogic. Alors que cette modification est intéressante pour les produits comme Sun

Java System Portal Server, une installation de serveur complète (`DEPLOY_LEVEL=1`) déployée sur WebLogic Server ne peut pas communiquer avec une installation de SDK client. Le cas échéant, des exceptions se produiront ultérieurement.

Si le serveur Access Manager 7 2005Q4 est installé sur BEA WebLogic Server, le `CLASSPATH` dans le script `startWebLogic.sh` doit être configuré à l'emplacement des fichiers JAR de JAX-RPC 1.0 pour communiquer avec le SDK client d'Access Manager.

Solution : avant d'appliquer le patch d'Access Manager, configurez le `CLASSPATH` dans le script `startWebLogic.sh` de l'instance de WebLogic Server pour utiliser les fichiers JAR de JAX-RPC 1.0 plutôt que les fichiers JAR de JAX-RPC 1.1 :

1. Connectez-vous au serveur Access Manager en tant que superutilisateur(`root`).
2. Modifiez le script `startWebLogic.sh` et remplacez le `CLASSPATH` pour utiliser les fichiers JAR de JAX-RPC 1.0. Exemple :

Valeur actuelle :

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-spi.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-impl.jar:
```

Nouvelle valeur :

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc_1.0/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-ri.jar:
```

où *AccessManager-base* correspond au répertoire d'installation de base. La valeur par défaut est `/opt` sous Solaris et `/opt/sun` sous Linux et HP-UX. *AccessManager-package-dir* correspond au répertoire du package d'Access Manager.

5. Redémarrez l'instance de WebLogic Server.

CR # 6523499 : fichier `amsilent` du patch 5 lisible par tous les utilisateurs sous Linux

Sous Linux. Le script `postpatch` crée le fichier `/opt/sun/identity/amsilent` avec des permissions de 644, qui offrent un accès en lecture à tous les utilisateurs.

Solution : Une fois le script `installpatch` exécuté, modifiez les permissions dans le fichier `amsilent` pour accorder un accès en lecture et en écriture au propriétaire uniquement. Exemple :

```
# chmod 600 /opt/sun/identity/amsilent
```

CR# 6520326 : l'application du patch 5 sur une deuxième instance d'Access Manager sur un serveur écrase le fichier `serverconfig.xml` de la première instance

Dans ce scénario de déploiement, deux instances d'Access Manager sont déployées sur le même serveur hôte, chaque instance figurant sur une instance de conteneur Web différente. Procédez ensuite comme suit :

1. Appliquez le patch 5.
2. Modifiez le fichier `amsilent` et redéployez la première instance d'Access Manager.
3. Modifiez à nouveau `amsilent` pour la seconde instance d'Access Manager, puis redéployez cette instance.

Si `NEW_INSTANCE=false` dans le fichier `amsilent`, le fichier `serverconfig.xml` de la première instance d'Access Manager est écrasé par les données de la seconde instance d'Access Manager. Un redémarrage ultérieur de la première instance d'Access Manager échoue. Le fichier `serverconfig.xml` figure dans le répertoire suivant en fonction de votre plate-forme :

- Systèmes Solaris : `/etc/opt/SUNWam/config`
- Systèmes Linux : `/etc/opt/sun/identity/config`

Solution : lorsque vous déployez la seconde instance d'Access Manager, configurez `NEW_INSTANCE=true` dans le fichier `amsilent.` Le fichier `serverconfig.xml` de la seconde instance d'Access Manager est ensuite mis à jour avec les données correctes et le fichier `serverconfig.xml` de la première instance d'Access Manager n'est pas écrasé.

CR# 6520016 : l'installation du patch 5 sur une machine SDK uniquement écrase les fichiers makefile échantillon

L'application du patch 5 sur une machine SDK uniquement écrase les fichiers makefile échantillon.

Solution : L'application du patch 5 sur une machine SDK uniquement ne nécessite pas de reconfiguration ; cependant, si vous souhaitez utiliser les fichiers makefile échantillon, observez la procédure suivante pour mettre à jour les fichiers LDIF et de propriétés (effectuez le remplacement des balises) des fichiers makefile échantillon :

1. Exécutez le script `amconfig` avec `DEPLOY_LEVEL=14` pour désinstaller le SDK et annuler la configuration du conteneur Web.
2. Exécutez le script `amconfig` avec `DEPLOY_LEVEL=4` pour réinstaller le SDK et reconfigurer le conteneur Web.

CR#6515502 : le plug-in de référentiel LDAPv3 ne gère pas toujours correctement l'attribut de recherche d'alias

Ce problème a été résolu pour la plupart des recherches. Faites toutefois attention lors de la configuration de l'attribut de recherche d'alias. La valeur des attributs de recherche d'alias doit être unique au sein d'une organisation. Si plus d'un attribut de recherche d'alias est configuré, il est possible qu'une entrée du magasin de données corresponde à un attribut et qu'une autre entrée corresponde à l'autre attribut. Le cas échéant, le serveur Access Manager renvoie l'erreur suivante :

```
An internal authentication error has occurred. Contact your system administrator.
```

Solution : aucune

CR# 6515383 : l'authentification distribuée et l'agent J2EE ne fonctionnent pas dans le même conteneur Web

Un serveur d'interface utilisateur d'authentification distribuée et un agent de stratégie J2EE ne fonctionnent pas s'ils sont installés dans le même conteneur Web.

Solution : créez une seconde instance pour le conteneur Web et déployez le serveur d'interface utilisateur d'authentification distribuée et l'agent de stratégie sur une instance différente du conteneur.

CR# 6508103 : l'aide en ligne renvoie une erreur d'application si le serveur d'application fonctionne sous Windows

Si vous déployez Access Manager sur un serveur d'application Sun Java System sous Windows, cliquer sur Aide dans le panneau gauche de l'écran d'aide de la console en mode Domaine renvoie une erreur d'application.

Solution : copiez le fichier *javaes-install-dir*`\share\lib\jhall.jar` dans le répertoire `JAVA_HOME\jre\lib\ext`, puis redémarrez Application Server.

CR# 6507383 et CR# 6507377 : l'authentification distribuée nécessite un paramètre d'URL `goto` explicite

Si aucun paramètre d'URL `goto` explicite n'est spécifié, un serveur d'interface utilisateur d'authentification distribuée tente de rediriger le paramètre `goto` sur un URL opérationnel spécifié dans Access Manager. Cette redirection peut échouer pour les motifs suivants :

- L'URL est relatif et aucune page correspondante n'est disponible sur le serveur d'interface utilisateur d'authentification distribuée.
- L'URL est absolu et le navigateur ne peut pas y accéder.

Solution : spécifiez toujours un paramètre d'URL `goto` explicite pour un serveur d'interface utilisateur d'authentification distribuée.

CR# 6402167 : LDAP JDK 4.18 provoque des problèmes au niveau du client LDAP/Directory Server

Dans Access Manager 7 2005Q4, LDAP JDK 4.18 est intégré à Java ES 2005Q4, d'où l'apparition de plusieurs problèmes de connexions avec Access Manager et Directory Server.

Solution : Appliquez l'un des patchs Sun Java System LDAP Java Development Kit suivants :

- Plates-formes SE Solaris, SPARC et x86 : 119725-04
- SE Linux 120834-02

Ces patchs sont accessibles sur le site Web de SunSolve : `http://sunsolve.sun.com`.

CR# 6352135 : les fichiers du serveur d'interface utilisateur d'authentification distribuée ne sont pas installés au bon emplacement

Sous Solaris, le programme d'installation de Java ES n'installe pas les fichiers du serveur d'interface utilisateur d'authentification distribuée `Makefile.distAuthUI`, `README.distAuthUI` et `amauthdistui.war` au bon emplacement : `/opt/SUNComm/SUNWam`.

Solution : copiez ces fichiers au bon emplacement : `/opt/SUNWam`.

Remarque : tout problème relatif au serveur d'interface utilisateur d'authentification distribuée qui a été résolu dans un patch est inséré dans le fichier `/opt/SUNComm/SUNWam/amauthdistui.war` . En conséquence, chaque fois que vous appliquez un patch sur le serveur Access Manager, puis que vous reconstruisez et déployez le fichier WAR, vous devez également copier ces fichiers dans le répertoire `/opt/SUNWam`.

CR# 6522720 : il est impossible d'effectuer une recherche de caractères multioctets dans l'aide en ligne de la console sous Windows et HP-UX

Si Access Manager est installé dans un environnement linguistique utilisant des caractères multioctets (comme le japonais) sous Windows ou HP-UX, il est impossible d'effectuer une recherche par saisie de mots-clés utilisant des caractères multioctets dans l'aide en ligne de la console.

Solution : aucune

Mise à jour du patch 6 : le patch 6 d'Access Manager 7 2005Q4 résout ce problème sous Windows. Cependant, il persiste sur les systèmes HP-UX.

CR# 6524251 : les caractères multioctets des messages sortants sont tronqués pendant la configuration d'Access Manager sous Windows

Si Access Manager est installé dans un environnement linguistique utilisant des caractères multioctets (comme le japonais ou le chinois) sous Windows, les mots sont tronqués dans les messages sortants apparaissant dans la fenêtre de terminal pendant sa configuration.

Solution : aucune, mais ce problème n'affecte pas la configuration en elle-même.

CR# 6526940 : les touches de propriété apparaissent à la place du texte pendant l'installation du patch 5 dans une autre langue que l'anglais sous Windows

Si vous installez le patch 5 (124296-05) dans une autre langue que l'anglais sous Windows, certaines chaînes apparaissent dans les panneaux d'installation sous la forme de touches de propriété au lieu de s'afficher sous forme de texte. Exemples de touches de propriété : `PRODUCT_NAME`, `JES_Patch_FinishPanel_Text1` et `JES_Patch_FinishPanel_Text2`.

Solution : aucune

CR# 6513653 : la configuration de la propriété `com.iplanet.am.session.purgedelay` peut provoquer un problème

Le script `amtune` configure la propriété `com.iplanet.am.session.purgedelay` sur 1 pour autoriser autant de sessions Access Manager que possible. Cette propriété spécifie, en minutes, le délai pendant lequel l'opération de session de purge est repoussée. Pour les clients comme Sun Java System Portal Server, cependant, une valeur de 1 peut s'avérer trop faible.

Solution : réinitialisez la propriété `com.iplanet.am.session.purgedelay` après avoir exécuté le script `amtune` :

1. Dans le fichier `AMConfig.properties`, configurez la propriété sur la nouvelle valeur. Exemple :

   ```
   com.iplanet.am.session.purgedelay=5
   ```

2. Redémarrez le conteneur Web d'Access Manager pour appliquer la nouvelle valeur.

Access Manager 7 2005Q4 Patch 4

Access Manager 7 2005Q4 patch 4 (révision 04) résout les problèmes suivants :

- CR# 6463796 : la désactivation du service `iPlanetAMClientDetection` pour `genericHTML` bloque l'accès à toutes les pages HTML d'Access Manager
- CR# 6463779 : l'authentification distribuée `amProfile_Client` et le serveur Access Manager Server `amProfile_Server` répertorient les exceptions inoffensives
- CR# 6463730 : les paramètres `goto` et `gx-charset` présentent une vulnérabilité de script de site croisé (XSS)
- CR# 6435889 : la méthode `Session.getSession` échoue car `RestrictedTokenContext` n'est pas configuré

Problèmes et restrictions connus du patch 4

- "CR# 6470055 : amélioration des performances du serveur d'interface utilisateur d'authentification distribuée" à la page 46
- "CR# 6455079 : le service de réinitialisation des mots de passe signale des erreurs de notification lors de la modification d'un mot de passe" à la page 46

CR# 6470055 : amélioration des performances du serveur d'interface utilisateur d'authentification distribuée

Pour améliorer les performances de lecture, de recherche et de comparaison des attributs utilisateur d'un utilisateur du serveur d'interface utilisateur d'authentification distribuée, procédez comme suit :

1. Dans le fichier `Makefile.distAuthUI`, remplacez le nom d'utilisateur de l'application `anonymous` par un autre utilisateur. Exemple :

   ```
   APPLICATION_USERNAME=user1
   ```

2. Dans Directory Server, ajoutez le nouveau nom (`user1` dans l'exemple) et l'ACI pour pouvoir lire, rechercher et comparer les attributs utilisateur. Le nouvel ACI est ajouté dans l'exemple suivant :

   ```
   dn:ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com
   changetype:modify add:aci
   aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com")
   (targetattr = *")(version 3.0;
   acl "SunAM client data access to a Distributed Auth App User";
   allow (read, search, compare)
   userdn =  "ldap:///uid=user1,ou=people,dc=example,dc=com";)
   ```

CR# 6455079 : le service de réinitialisation des mots de passe signale des erreurs de notification lors de la modification d'un mot de passe

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 entrées d'erreur 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 l'adresse de l'expéditeur pour ajouter le nom de domaine complet du serveur hôte dans le fichier `amPasswordResetModuleMsgs.properties` :

1. Modifiez l'étiquette de l'adresse de l'expéditeur. Exemple :

   ```
   fromAddress.label=<Identity-Server@amhost.example.com>
   ```

2. Modifiez la propriété `lockOutEmailFrom` pour assurer que les notifications de verrouillage utilisent l'adresse correcte de l'expéditeur. Exemple :

   ```
   lockOutEmailFrom=<Identity-Server@amhost.example.com>
   ```

   Le fichier `amPasswordResetModuleMsgs.properties` réside dans le répertoire *AccessManager-base*`/SUNWam/locale` sous Solaris et dans le répertoire *AccessManager-base*`/identity/locale` sous Linux.

   AccessManager-base correspond au répertoire d'installation de base. Le répertoire d'installation de base par défaut est `/opt` sous Solaris et `/opt/sun` sous Linux.

Access Manager 7 2005Q4 Patch 3

Le patch 3 (révision 3) d'Access Manager 7 résout de nombreux problèmes, répertoriés dans le fichier LISEZMOI accompagnant le patch. Le patch 3 inclut également les nouvelles fonctions et problèmes connus suivants :

Nouvelles fonctions du patch 3

- "Nouvelles propriétés de configuration pour le contrôle de site" à la page 48
- "Prise en charge de Liberty Identity Web Services Framework (ID-WSF) 1.1" à la page 49

Problèmes et restrictions connus du patch 3

- "CR# 6463779 : Le journal `amProfile_Client` d'authentification distribuée et le journal `amProfile_Server` du serveur Access Manager répertorient les exceptions inoffensives." à la page 50
- "CR# 6460974 : L'utilisateur de l'application d'authentification distribuée par défaut ne doit pas être `amadmin`" à la page 50
- "CR# 6460576 : Aucun lien vers le service utilisateur dans Rôle filtré dans l'aide en ligne de la console" à la page 51
- "CR# 6460085 : Le serveur sur WebSphere est inaccessible après l'exécution de `reinstallRTM` et le redéploiement d'applications Web." à la page 51
- "CR# 6455757 : La classe de marqueurs `sunISManagerOrganization` doit être ajoutée à une organisation avant une mise à niveau." à la page 52
- "CR# 6454489 : La mise à niveau en Access Manager 7 2005Q4 Patch 2 entraîne une erreur dans l'onglet des sessions en cours de la console" à la page 52
- "CR# 6452320 : Les exceptions sont rejetées en cas d'interrogation avec SDK client." à la page 53
- "CR# 6442905 : Le `SSOToken` de l'utilisateur authentifié doit être indiqué pour les sites malveillants." à la page 53
- "CR# 6441918 : Intervalle de contrôle de site et propriétés du délai d'expiration" à la page 54
- "CR# 6440697 : L'authentification distribuée doit être exécutée en tant qu'utilisateur non administratif." à la page 54

- “CR# 6440695 : Serveurs d'interface utilisateur d'authentification distribuée avec équilibreur de charge” à la page 54
- “CR# 6440651 : la rediffusion de cookie requiert la propriété `com.sun.identity.session.resetLBCookie` .” à la page 55
- “CR# 6440648 : La propriété `com.iplanet.am.lbcookie.name` implique une valeur par défaut de `amlbcookie`” à la page 55
- “CR# 6440641 : La propriété `com.iplanet.am.lbcookie.value` est désapprouvée.” à la page 55
- “CR# 6429610 : Impossible de créer le jeton SSO en cas d'utilisation d'ID-FF SSO.” à la page 55
- “CR# 6389564 : Plusieurs requêtes successives sur les membres du rôle d'un magasin de données LDAP v3 lors de la connexion à Access Manager” à la page 56
- “CR# 6385185 : Le module d'authentification ne peut pas remplacer l'URL 'aller à' et en spécifier une autre” à la page 56
- “CR# 6385184 : La redirection depuis un module d'authentification personnalisé lorsque le jeton SSO est toujours à l'état non valide. ” à la page 56
- “CR# 6324056 : La fédération échoue en cas d'utilisation d'un profil d'artefact.” à la page 57

Nouvelles propriétés de configuration pour le contrôle de site

La fonction de contrôle de site d'Access Manager inclut les nouvelles propriétés suivantes :

Propriété	Description
`com.sun.identity.sitemonitor.interval`	Intervalle de contrôle de site exprimé en millisecondes. La fonction de contrôle de site vérifie la disponibilité de chaque site dans l'intervalle de temps spécifié. Par défaut : 6 0000 millisecondes (1 minute).
`com.sun.identity.sitemonitor.timeout`	Délai de vérification de la disponibilité du site exprimé en millisecondes. La fonction de contrôle de site attend une réponse du site pendant le délai spécifié. Par défaut : 5 000 millisecondes (5 secondes).

Le patch n'ajoute pas ces propriétés au fichier `AMConfig.properties` . Pour utiliser ces nouvelles propriétés avec des valeurs autres que celles par défaut :

1. Ajoutez les propriétés et leurs valeurs au fichier `AMConfig.properties` dans le répertoire suivant, en fonction de votre plate-forme :
   - Systèmes Solaris : `/etc/opt/SUNWam/config`
   - Systèmes Linux : `/etc/opt/sun/identity/config`

   Pour les agents de stratégie, ajoutez ces propriétés au fichier `AMAgents.properties` .
2. Redémarrez le conteneur Web d'Access Manager pour appliquer les valeurs.

Mise en œuvre personnalisée. La classe `com.sun.identity.sitemonitor.SiteStatusCheck` vous permet en outre de personnaliser votre mise en œuvre de vérification de la disponibilité du site à l'aide de l'interface suivante :

```
package com.iplanet.services.naming.WebtopNaming$SiteStatusCheck
```

Chaque classe de mise en œuvre doit utiliser la méthode `doCheckSiteStatus`.

```
public interface SiteStatusCheck {
public boolean doCheckSiteStatus(URL siteurl);
}
```

Prise en charge de Liberty Identity Web Services Framework (ID-WSF) 1.1

La version par défaut de ID-WSF dans le patch 3 d'Access Manager 7 est WSF1.1. Aucune autre configuration n'est nécessaire pour déclencher ID-WSF, à l'exception des exemples, qui doivent doivent utiliser les nouveaux mécanismes de sécurité. Les nouveaux mécanismes de sécurité pour ID-WSF1.1 sont :

```
urn:liberty:security:2005-02:null:X509
urn:liberty:security:2005-02:TLS:X509
urn:liberty:security:2005-02:ClientTLS:X509
urn:liberty:security:2005-02:null:SAML
urn:liberty:security:2005-02:TLS:SAML
urn:liberty:security:2005-02:ClientTLS:SAML
urn:liberty:security:2005-02:null:Bearer
urn:liberty:security:2005-02:TLS:Bearer
urn:liberty:security:2005-02:ClientTLS:Bearer
```

Nouvelle propriété pour la prise en charge de Liberty ID-WSF

La propriété `com.sun.identity.liberty.wsf.version` détermine la structure de Liberty ID-WSF lorsque celle-ci n'est pas en mesure de déterminer à partir du message entrant ou des ressources disponibles si Access Manager fait office de WSC. Les valeurs peuvent être 1.0 ou 1.1. La valeur par défaut est 1.1.

Remarque : l'installation du patch n'ajoute pas la propriété `com.sun.identity.liberty.wsf.version` au fichier `AMConfig.properties` (CR# 6458184). Pour utiliser cette nouvelle propriété, ajoutez-la au fichier `AMConfig.properties` avec la valeur appropriée après l'installation du patch, puis redémarrez le conteneur Web d'Access Manager.

Une fois Access Manager 7 patch 3 installé, exécutez la commande suivante, pour charger les modifications apportées au schéma. Cette commande est illustrée avec Access Manager installé dans le répertoire par défaut sous Solaris :

```
# /opt/SUNWam/bin/amadmin -u amadmin -w amadmin_password
-t /etc/opt/SUNWam/wsf1.1_upgrade.xml
```

L'enregistrement de découverte ID-WSF peut utiliser ces nouveaux mécanismes de sécurité lors de l'enregistrement. Les WSC détecteront également automatiquement la version à utiliser lors d'une communication avec des WSP. Pour configurer pour ID-WSF1.1, consultez les fichiers LisezMoi de Liberty ID-FF sample1 et les exemples ID-WSF fournis avec le produit.

CR# 6463779 : Le journal `amProfile_Client` d'authentification distribuée et le journal `amProfile_Server` du serveur Access Manager répertorient les exceptions inoffensives.

Les demandes faites au serveur Access Manager via une interface utilisateur d'authentification distribuée entraîne la consignation d'exceptions dans le journal `distAuth/amProfile_Client` et dans le journal `debug/amProfile_Server` du serveur Access Manager. Après plusieurs sessions, le journal `amProfile_Client` peut atteindre plusieurs gigaoctets et le journal `amProfile_Server` du serveur Access Manager peut atteindre plusieurs mégaoctets. Ces exceptions n'entraînent aucune perte de fonctionnalité dans les journaux, mais peuvent provoquer une fausse alarme pour les utilisateurs et les journaux peuvent éventuellement saturer le disque dur.

Solution. Exécutez des tâches `cron` qui annuleront le contenu des fichiers journaux. Exemple :

- Sur la machine client de l'interface utilisateur d'authentification distribuée, exécutez "`cat /dev/null > distAuth/amProfile_Client`" à des intervalles de quelques heures en fonction du trafic.
- Sur le serveur Access Manager, exécutez "`cat /dev/null > /var/opt/SUNWam/debug/amProfile_Server`" à des intervalles de quelques jours plutôt que quelques heures.

CR# 6460974 : L'utilisateur de l'application d'authentification distribuée par défaut ne doit pas être `amadmin`

Si vous déployez un serveur d'interface utilisateur d'authentification distribuée, l'administrateur correspondant ne doit pas être `amadmin`. L'utilisateur de l'application d'authentification distribuée par défaut indiqué dans le fichier `Makefile.distAuthUI` est `amadmin`, et donc dans le fichier `AMConfig.properties`, une fois que le fichier `distAuth.war` est déployé côté client. L'utilisateur `amadmin` dispose d'un `AppSSOToken` expirant à la fin de la session `amadmin`, pouvant ainsi entraîner la consignation d'une ERREUR FATALE dans le fichier journal `amSecurity` (situé, par défaut, dans le répertoire `/tmp/distAuth`).

Solution. Spécifiez `UrlAccessAgent` comme utilisateur de l'application d'authentification distribuée. Exemple :

Avant de déployer le fichier `distAuth.war` du conteneur Web client, modifiez les paramètres suivants du fichier `Makefile.distAuthUI` :

```
APPLICATION_USERNAME=UrlAccessAgent
APPLICATION_PASSWORD=shared-secret-password or amldapuser-password
```

eur

Après avoir déployé le fichier `distAuth.war` du conteneur Web client, modifiez les propriétés suivantes du fichier `AMConfig.properties` pour chaque serveur Access Manager :

```
com.sun.identity.agents.app.username=UrlAccessAgent
com.iplanet.am.service.password=shared-secret-password or amldapuser-password
```

Voir aussi "CR# 6440697 : L'authentification distribuée doit être exécutée en tant qu'utilisateur non administratif." à la page 54.

CR# 6460576 : Aucun lien vers le service utilisateur dans Rôle filtré dans l'aide en ligne de la console

L'aide en ligne de la console Access Manager ne comprend pas de lien vers le service utilisateur dans Rôle filtré. Dans l'aide en ligne, accédez au sommaire, à Rôle filtré, puis à la procédure de création d'un rôle filtré. Faites défiler la page vers le bas puis, en fonction du type d'identité sélectionné, une liste de services s'affiche mais aucun lien de service utilisateur n'est disponible.

Solution. aucune

CR# 6460085 : Le serveur sur WebSphere est inaccessible après l'exécution de `reinstallRTM` et le redéploiement d'applications Web.

Après l'application du patch 3 d'Access Manager 7 pour un déploiement `DEPLOY_LEVEL=1` sur IBM WebSphere Application Server 5.1.1.6 sur Red Hat Linux AS 3.0 Update 4, le script `reinstallRTM` a été exécuté pour restaurer les RPM RTM. Les applications Web ont alors été redéployées après modification du fichier `amsilent` généré par le script `reinstallRTM`. WebSphere a été redémarré à l'aide des scripts `stopServer.sh` et `startServer.sh`. Toutefois, lors de l'accès à la page de connexion, WebSphere a affiché une erreur 500 liée au filtre `amlcontroller`.

Ce problème est survenu car le nouveau fichier `server.xml` généré par le script `reinstallRTM` était corrompu.

Solution. Le fichier `server.xml` sauvegardé à l'aide du script `amconfig` est toujours valide. Utilisez cette copie précédente, comme suit :

1. Arrêtez le serveur.
2. Remplacez le fichier `server.xml` corrompu par la copie sauvegardée à l'aide du script `amconfig`.

   Le fichier `server.xml` sauvegardé à l'aide du script `amconfig` sera nommé `server.xml-orig-` *pid*, où *pid* correspond à l'ID de processus du script `amwas51config`. Le fichier se trouve dans le répertoire suivant :

   WebSphere-home-directory`/config/cells/`*WebSphere-cell*
   `/nodes/`*WebSphere-node*`/servers/`*server-name*

3. Redémarrez le serveur.

CR# 6455757 : La classe de marqueurs `sunISManagerOrganization` doit être ajoutée à une organisation avant une mise à niveau.

Une organisation dans une arborescence d'informations d'annuaire (DIT) Access Manager créée avant Access Manager version 7 risque de ne pas disposer de la classe d'objet `sunISManagerOrganization`. La définition d'une organisation créée par un produit autre qu'Access Manager ne comprendra pas non plus la classe d'objet `sunISManagerOrganization`.

Solution. Avant de mettre à niveau en Access Manager 7 2005Q4, vérifiez que la définition de toutes les organisations de l'arborescence d'informations d'annuaire (DIT) comprend la classe d'objet `sunISManagerOrganization`. Si nécessaire, ajoutez manuellement cette classe d'objet avant la mise à niveau.

CR# 6454489 : La mise à niveau en Access Manager 7 2005Q4 Patch 2 entraîne une erreur dans l'onglet des sessions en cours de la console

Une mise à niveau a entraîné l'erreur suivante dans l'onglet des sessions en cours de la console Access Manager :

```
Failed to get valid Sessions from the Specified server
```

Ce problème s'applique aux déploiements mis à niveau des versions Access Manager 6 ne disposant pas de suffixe racine sous la forme `o=orgname`.

Solution. Après l'installation d'Access Manager 7 2005Q4, appliquez le patch 3 d'Access Manager 7 puis exécutez le script `amupgrade` pour migrer les données comme suit :

1. Sauvegardez votre arborescence d'informations d'annuaire (DIT) Access Manager 6.
2. Exécutez le script `ampre70upgrade`.
3. Installez Access Manager 7 2005Q4 avec l'option de configuration ultérieure.
4. Annulez le déploiement des applications Web d'Access Manager.
5. Déployez les applications Web d'Access Manager.
6. Appliquez le patch 3 d'Access Manager 7, mais pas les changements XML/LDIF. Les changements XML/LDIF doivent être appliqués après l'exécution du script `amupgrade` à l'étape suivante.
7. Exécutez le script `amupgrade`.
8. Redéployez les applications Web d'Access Manager en raison des changements du patch 3 d'Access Manager 7.
9. Accédez à la console Access Manager.

CR# 6452320 : Les exceptions sont rejetées en cas d'interrogation avec SDK client.

Lorsque vous déployez le SDK client d'Access Manager (`amclientsdk.jar`) et que vous activez l'interrogation, des erreurs comme la suivante peuvent se produire :

```
ERROR: Send Polling Error:
com.iplanet.am.util.ThreadPoolException:
amSessionPoller thread pool's task queue is full.
```

De telles erreurs peuvent se produire après avoir déployé un serveur d'interface utilisateur d'authentification distribuée, des agents J2EE ou dans toute autre situation de déploiement du SDK client d'Access Manager sur une machine client.

Solution. Si vous disposez de quelques centaines de sessions simultanées uniquement, ajoutez les propriétés et valeurs suivantes au fichier `AMConfig.properties` ou au fichier `AMAgents.properties` :

```
com.sun.identity.session.polling.threadpool.size=10
com.sun.identity.session.polling.threadpool.threshold=10000
```

Pour des centaines ou des milliers de sessions, les valeurs doivent être identiques à celles données à titre d'exemple dans le fichier `AMConfig.properties` d'Access Manager après exécution du script `amtune-identity`. Par exemple, pour une machine disposant de 4 Go de RAM, le script `amtune-identity` d'Access Manager définit les valeurs suivantes :

```
com.sun.identity.session.notification.threadpool.size=28
com.sun.identity.session.notification.threadpool.threshold=76288
```

Définissez des valeurs identiques côté client dans le fichier `AMAgent.properties` ou `AMConfig.properties` lors du déploiement du serveur d'interface utilisateur d'authentification distribuée ou du SDK client d'Access Manager sur une machine client avec 4 Go de RAM.

CR# 6442905 : Le `SSOToken` de l'utilisateur authentifié doit être indiqué pour les sites malveillants.

Un utilisateur Access Manager authentifié peut révéler sans le vouloir le `SSOToken` d'un site malveillant en cliquant sur une URL du site.

Solution. Créez toujours un profil d'utilisateur d'agent unique dans Access Manager pour tous les agents de stratégie participant afin de s'assurer que le site n'est pas erroné. Vérifiez également qu'aucun de ces utilisateurs d'agent n'utilise un mot de passe identique au mot de passe secret partagé ou au mot de passe `amldapuser` . Par défaut, les agents de stratégie sont authentifiés dans le module d'authentification d'Access Manager comme l'utilisateur `UrlAccessAgent`.

Pour plus d'informations sur la création d'un agent à l'aide la console d'administration d'Access Manager, reportez-vous à "Agents" du *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

CR# 6441918 : Intervalle de contrôle de site et propriétés du délai d'expiration

Le basculement de site Access Manager inclut les nouvelles propriétés suivantes :

```
com.sun.identity.sitemonitor.interval
com.sun.identity.sitemonitor.timeout
```

Pour plus d'informations, reportez-vous à "Nouvelles propriétés de configuration pour le contrôle de site" à la page 48.

CR# 6440697 : L'authentification distribuée doit être exécutée en tant qu'utilisateur non administratif.

Pour créer un administrateur d'authentification distribuée autre que l'utilisateur administratif par défaut (`amadmin`) pour l'authentification d'application, suivez la procédure ci-dessous :

1. Créez un utilisateur LDAP comme administrateur de l'authentification distribuée. Exemple :

   ```
   uid=DistAuthAdmin,ou=people,o=am
   ```

2. Ajoutez l'administrateur de l'authentification distribuée à la liste d'utilisateurs spéciaux. Exemple :

   ```
   com.sun.identity.authentication.special.users=cn=dsameuser,
   ou=DSAME Users,o=am|cn=amService-UrlAccessAgent,ou=DSAME Users,
   o=am|uid=DistAuthAdmin,ou=People,o=am
   ```

   Ajoutez cette propriété au fichier `AMConfig.properties` de tous les serveurs Access Manager afin que le `AppSSOToken` de l'administrateur de l'authentification distribuée n'expire pas à la fin de la session.

CR# 6440695 : Serveurs d'interface utilisateur d'authentification distribuée avec équilibreur de charge

Si votre déploiement comprend un équilibreur de charge et plusieurs serveurs d'interface utilisateur d'authentification distribuée, définissez les propriétés suivantes dans le fichier `AMConfig.properties` après avoir déployé le fichier WAR.

`com.iplanet.am.lbcookie.name=`*DistAuthLBCookieName*
`com.iplanet.am.lbcookie.value=`*DistAuthLBCookieValue*

CR# 6440651 : la rediffusion de cookie requiert la propriété `com.sun.identity.session.resetLBCookie .`

Pour que la rediffusion de cookie fonctionne correctement dans le basculement de session d'Access Manager, ajoutez la propriété `com.sun.identity.session.resetLBCookie` définie sur `true` pour l'agent de stratégie et le serveur Access Manager. Exemple :

```
com.sun.identity.session.resetLBCookie='true'
```

- Pour l'agent de stratégie, ajoutez la propriété au fichier `AMAgent.properties` .
- Pour le serveur Access Manager, ajoutez la propriété au fichier `AMConfig.properties`.

Remarque : Cette propriété n'est requise que si vous avez implémenté le basculement de session d'Access Manager.

CR# 6440648 : La propriété `com.iplanet.am.lbcookie.name` implique une valeur par défaut de `amlbcookie`

Par défaut, un agent de stratégie et des serveurs Access Manager impliquent le nom de cookie d'équilibreur de charge `amlbcookie`. Si vous renommez le cookie du serveur d'arrière-plan, utilisez le même nom dans le fichier `AMAgent.properties` de l'agent de stratégie. De même, si vous utilisez le SDK client Access Manager, utilisez également le même nom de cookie que celui utilisé par le serveur d'arrière-plan.

CR# 6440641 : La propriété `com.iplanet.am.lbcookie.value` est désapprouvée.

Access Manager ne prend plus en charge la propriété `com.iplanet.am.lbcookie.value` sur les serveurs afin de personnaliser le cookie d'équilibreur de charge. Access Manager utilise désormais, pour la valeur de cookie et le nom donné par l'agent, l'ID du serveur défini dans la configuration de la session.

CR# 6429610 : Impossible de créer le jeton SSO en cas d'utilisation d'ID-FF SSO.

Après la définition de l'exemple 1 du Liberty Identity Federation Framework (ID-FF), la fédération réussit mais SSO échoue.

Solution. Ajoutez `uuid` de `dsameuser` à la propriété `com.sun.identity.authentication.special.users` dans le fichier `AMConfig.properties`. Pour l'authentification d'applications, `dsameuser` requiert un jeton SSO sans date d'expiration pour le serveur Access Manager.

CR# 6389564 : Plusieurs requêtes successives sur les membres du rôle d'un magasin de données LDAP v3 lors de la connexion à Access Manager

Lorsqu'un utilisateur se connecte à Access Manager, plusieurs recherches LDAP se produisent sur l'attribut `nsRoleDN` de l'utilisateur.

Solution. Une fois Access Manager 7 patch 3 installé, exécutez la commande suivante, illustrée avec Access Manager installé dans le répertoire par défaut sous Solaris :

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/idRepoServiceAddAttrSchemaRequest_Cache.xml
```

CR# 6385185 : Le module d'authentification ne peut pas remplacer l'URL 'aller à' et en spécifier une autre

Un module d'authentification peut remplacer l'URL 'aller à' et demander la redirection vers une autre URL d'un site Web externe afin de valider le statut de l'utilisateur.

Pour remplacer l'URL 'aller à' une fois l'authentification terminée, définissez la propriété de l'exemple suivant du `SSOToken`. Pour cela, utilisez la méthode `onLoginSuccess` de la classe `PostProcess` mettant en œuvre `AMPostAuthProcessInterface`. Par exemple, *OverridingURL* représente l'URL remplaçant l'URL 'aller à' :

```
public class <..> implements AMPostAuthProcessInterface {
...
    public void onLoginSuccess(...) {
        try {
            ssoToken.setProperty("PostProcessSuccessURL", OverridingURL);
         } catch (Exception ...) {
         ...         }
...
}
```

CR# 6385184 : La redirection depuis un module d'authentification personnalisé lorsque le jeton SSO est toujours à l'état non valide.

La nouvelle propriété `RedirectCallback` pour module d'authentification personnalisé permet de rediriger vers un site Web externe via l'interface utilisateur d'authentification afin de valider un utilisateur. Si l'authentification réussit, l'utilisateur est alors redirigé vers l'URL du serveur Access Manager d'origine. Les fichiers d'exemple incluent :

- `LoginModuleSample.java`
- `LoginModuleSample.xml`
- `testExtWebSite.jsp`

Pour mettre en œuvre cette fonction :

1. Créez un module d'authentification personnalisé basé sur l'exemple `LoginModuleSample.java`.
2. Chargez le module sur un serveur Access Manager.
3. Définissez `RedirectCallback` dans le fichier XML à l'aide de l'exemple `LoginModuleSample.xml`.
4. Pour tester le module, utilisez le fichier d'exemple `testExtWebSite.jsp` pour le site Web externe.
5. Connectez-vous via l'URL suivante :

```
http://example.com/amserver/UI/Login?module=LoginModuleSample
```

Le nom d'utilisateur et le mot de passe sont redirigés vers le site Web externe pour validation. Si le nom et le mot de passe sont valides, l'authentification réussit et l'utilisateur est redirigé vers l'URL du serveur Access Manager d'origine.

Prenons un exemple dans lequel le déploiement utilise un module d'authentification personnalisé pour accéder à un site d'approvisionnement/carte bancaire :

1. Un utilisateur ouvre la page de traitement d'authentification/de connexion du module d'authentification personnalisé.
2. L'utilisateur entre les informations d'authentification (nom d'utilisateur et mot de passe) et envoie une requête au module d'authentification personnalisé.
3. Le module d'authentification personnalisé redirige l'utilisateur vers un site d'approvisionnement/carte bancaire externe ainsi que les informations utilisateur nécessaires fournies avec la requête.
4. Le site d'approvisionnement/carte de crédit externe vérifie le statut de l'utilisateur et renvoie la requête comme étant réussie ou en échec.
5. Le module d'authentification personnalisé valide l'utilisateur en fonction du statut renvoyé à l'étape 4 et le renvoie au service d'authentification.
6. L'authentification utilisateur se termine et est soit réussie, soit en échec.

CR# 6324056 : La fédération échoue en cas d'utilisation d'un profil d'artefact.

Solution : Pour résoudre ce problème, appliquez la dernière version du patch 'Core Mobile Access', en fonction de votre plate-forme :

- Solaris OS sur les systèmes SPARC : 119527
- Solaris OS sur les plates-formes x86 : 119528
- Systèmes Linux : 119529

Redémarrez le conteneur Web après application du patch.

Access Manager 7 2005Q4 Patch 2

Le patch 2 (révision 02) d'Access Manager 7 2005Q4 a résolu de nombreux problèmes, répertoriés dans le fichier LISEZMOI accompagnant le patch. Le patch 2 inclut également les nouvelles fonctions et problèmes connus suivants :

Nouvelles fonctions du patch 2

- "Nouvelles propriétés des caches User Management, Identity Repository et Service Management" à la page 58
- "Nouvelle propriété pour le fournisseur de services de fédération" à la page 60
- "Prise en charge de la condition de filtre LDAP " à la page 60

Problèmes et restrictions connus du patch 2

- "CR# 6283582 : Le nombre d'échecs de connexion n'est pas réparti entre les instances d'Access Manager." à la page 61
- "CR# 6293673 : Les informations de session d'origine doivent être conservées pendant l'envoi de la notification du délai d'expiration de session." à la page 61
- "CR# 6244578 : Access Manager doit avertir l'utilisateur que la prise en charge de cookie/l'activation des cookies de navigateur est désactivée/indisponible." à la page 61
- "CR# 6236892 : Substituant d'image/texte pendant que CDCServlet traite AuthNResponse après la connexion" à la page 62
- "CR# 6363157 : la nouvelle propriété désactive les recherches persistantes si cela est absolument nécessaire" à la page 62
- "CR# 6385696 : Les IDP et SP existants et nouveaux n'apparaissent pas." à la page 63

Nouvelles propriétés des caches User Management, Identity Repository et Service Management

Le patch 2 inclut également les nouvelles propriétés suivantes pour les caches User Management (Access Manager SDK), Identity Repository (IdRepo) et Service Management. Ces propriétés vous permettent d'activer et de désactiver les différents caches indépendamment, en fonction de vos besoins de déploiement et de définir la durée de vie des entrées de cache.

TABLEAU 3 Nouvelles propriétés des caches User Management, Identity Repository et Service Management

Propriété	Description
Nouvelles propriétés d'activation/désactivation de caches	
`com.iplanet.am.sdk.caching.enabled`	Propriété globale activant (vrai) ou désactivant (faux) les caches Identity Repository (IdRepo), User Management et Service Management. Si cette propriété est réglée sur vrai ou absente du fichier `AMConfig.properties` , les trois caches sont activés.

TABLEAU 3 Nouvelles propriétés des caches User Management, Identity Repository et Service Management *(Suite)*

Remarque Les trois propriétés suivantes pour activer ou désactiver les caches spécifiques ne s'appliquent que si la propriété globale ci-dessus est réglée sur faux.	
`com.sun.identity.amsdk.cache.enabled`	Active (vrai) ou désactive (faux) le cache User Management (Access Manager SDK) uniquement.
`com.sun.identity.idm.cache.enabled`	Active (vrai) ou désactive (faux) le cache Identity Repository (IdRepo) uniquement.
`com.sun.identity.sm.cache.enabled`	Active (vrai) ou désactive (faux) le cache Service Management uniquement.
Nouvelles propriétés du cache User Management de durée de vie	
`com.iplanet.am.sdk.cache.entry.expire.enabled`	Active (vrai) ou désactive (faux) le délai d'expiration (défini par les deux propriétés suivantes) du cache User Management.
`com.iplanet.am.sdk.cache.entry.user.expire.time`	Définit la durée de validité en minutes des entrées utilisateur du cache User Management après leur dernière modification. A savoir, après la durée spécifiée écoulée (après la dernière modification ou lecture dans le répertoire), les données de l'entrée mise en cache expirent. De nouvelles demandes de données pour ces entrées doivent alors être lues depuis le répertoire.
`com.iplanet.am.sdk.cache.entry.default.expire.time`	Définit la durée de validité en minutes des entrées non-utilisateur du cache User Management après leur dernière modification. A savoir, après la durée spécifiée écoulée (après la dernière modification ou lecture dans le répertoire), les données de l'entrée mise en cache expirent. De nouvelles demandes de données pour ces entrées doivent alors être lues depuis le répertoire. Nouvelles propriétés de durée de vie du cache Identity Repository
`com.sun.identity.idm.cache.entry.expire.enabled`	Active (vrai) ou désactive (faux) le délai d'expiration (défini par les deux propriétés suivantes) du cache IdRepo.
`com.sun.identity.idm.cache.entry.default.expire.time`	Définit la durée de validité en minutes des entrées non-utilisateur du cache IdRepo après leur dernière modification. A savoir, après la durée spécifiée écoulée (après la dernière modification ou lecture dans le référentiel), les données de l'entrée mise en cache expirent. De nouvelles demandes de données pour ces entrées doivent alors être lues depuis le référentiel.

Utilisation des nouvelles propriétés de cache

Les patchs Access Manager 7 2005Q4 n'ajoutent pas automatiquement les nouvelles propriétés de cache au fichier `AMConfig.properties`.

Pour utiliser les nouvelles propriétés de cache :

1. A l'aide d'un éditeur de texte, ajoutez les propriétés et leurs valeurs au fichier `AMConfig.properties` dans le répertoire suivant, en fonction de votre plate-forme :
   - Systèmes Solaris : `/etc/opt/SUNWam/config`
   - Systèmes Linux : `/etc/opt/sun/identity/config`
2. Redémarrez le conteneur Web d'Access Manager pour appliquer les valeurs.

Nouvelle propriété pour le fournisseur de services de fédération

La nouvelle propriété `com.sun.identity.federation.spadapter` définit la classe de mise en œuvre de `com.sun.identity.federation.plugins.FederationSPAdapter` qui permet d'ajouter le traitement spécifique à l'application pendant le traitement de fédération côté fournisseur de services.

Voir aussi "CR# 6385696 : Les IDP et SP existants et nouveaux n'apparaissent pas." à la page 63.

Prise en charge de la condition de filtre LDAP

La prise en charge de la condition de filtre LDAP est ajoutée dans le patch 2. Un administrateur de stratégies peut désormais spécifier un filtre LDAP dans la condition lors de la définition d'une stratégie. La stratégie ne s'applique à l'utilisateur que si l'entrée LDAP de l'utilisateur est conforme au filtre LDAP spécifié dans la condition. L'entrée LDAP de l'utilisateur est recherchée dans le répertoire indiqué dans le service de configuration de la stratégie.

Pour enregistrer et utiliser la condition de filtre LDAP, exécutez les commandes suivantes une fois Access Manager 7 patch 2 installé. Elles sont illustrées avec Access Manager installé dans le répertoire par défaut sous Solaris :

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-s /etc/opt/SUNWam/AddLDAPFilterCondition.xml
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/amPolicyConfig_mod_ldfc.xml
```

Remarque sur le patch 5 Si vous avez ajouté Access Manager 7 2005Q4 Patch 5 et exécuté le script `updateschema.sh`, vous n'avez pas besoin de charger ces fichiers à l'aide de `amadmin`. Pour plus d'informations, consultez la section "Nouveau script `updateschema.sh` de chargement des fichiers LDIF et XML" à la page 30.

CR# 6283582 : Le nombre d'échecs de connexion n'est pas réparti entre les instances d'Access Manager.

Une fois Access Manager 7 patch 2 installé, exécutez les commandes suivantes, illustrées avec Access Manager installé dans le répertoire par défaut sous Solaris :

```
# cd DirectoryServer-base/shared/bin
# ./ldapmodify -h DirectoryServerHost -p DirectoryServerPort
-D "cn=Directory Manager" -w DirectoryMangerPassword
-a -f /etc/opt/SUNWam/accountLockout.ldif
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/accountLockoutData.xml
```

La valeur par défaut de *DirectoryServer-base* est `/var/opt/mps/serverroot` sous Solaris et `/var/opt/sun/directory-server` sous Linux.

Remarque sur le patch 5 Si vous avez ajouté Access Manager 7 2005Q4 Patch 5 et exécuté le script `updateschema.sh`, vous n'avez pas besoin de charger ces fichiers à l'aide de `amadmin`. Pour plus d'informations, consultez la section "Nouveau script `updateschema.sh` de chargement des fichiers LDIF et XML" à la page 30.

CR# 6293673 : Les informations de session d'origine doivent être conservées pendant l'envoi de la notification du délai d'expiration de session.

La nouvelle propriété `com.sun.identity.session.property.doNotTrimList` du fichier `AMConfig.properties` peut contenir une liste des noms de propriétés de session séparés par une virgule. Une fois qu'une session a expiré, les propriétés définies dans cette liste ne seront pas supprimées afin de pouvoir y accéder avant la purge de la session. Exemple :

```
com.sun.identity.session.property.doNotTrimList=UserId,HostName
```

CR# 6244578 : Access Manager doit avertir l'utilisateur que la prise en charge de cookie/l'activation des cookies de navigateur est désactivée/indisponible.

La nouvelle propriété `com.sun.identity.am.cookie.check` du fichier `AMConfig.properties` indique si le serveur doit vérifier la prise en charge de cookie/l'activation des cookies dans le navigateur. La valeur `true` amène le serveur à vérifier la prise en charge de cookie/l'activation des cookies dans le navigateur et à renvoyer une page d'erreur si le navigateur ne prend pas en charge les cookies ou s'ils ne sont pas activés. Cette valeur doit être paramétrée sur false (valeur par défaut) si le serveur doit prendre en charge un mode sans cookies pour l'authentification.

CR# 6236892 : Substituant d'image/texte pendant que CDCServlet traite AuthNResponse après la connexion

Les nouvelles propriétés suivantes sont ajoutées au fichier `AMConfig.properties` et lues par CDCServlet :

- `com.iplanet.services.cdc.WaitImage.display` entraîne l'affichage d'une image dans le navigateur pendant que l'utilisateur attend la page sécurisée d'un scénario, si cette propriété est paramétrée sur true. La valeur par défaut est faux.
- `com.iplanet.services.cdc.WaitImage.name` indique le nom de l'image. La valeur par défaut est `waitImage.gif`. Cette image peut être copiée du répertoire `login_images`.
- `com.iplanet.services.cdc.WaitImage.width` indique la largeur de l'image. La valeur par défaut est 420.
- `com.iplanet.services.cdc.WaitImage.height` indique la hauteur de l'image. La valeur par défaut est 120.

CR# 6363157 : la nouvelle propriété désactive les recherches persistantes si cela est absolument nécessaire

La nouvelle propriété `com.sun.am.event.connection.disable.list` du fichier `AMConfig.properties` indique la connexion d'événement pouvant être désactivée. Les valeurs (sensibles à la casse) peuvent être :

`aci` - Modifications de l'attribut `aci`, la recherche utilisant le filtre LDAP (`aci=*`)

`sm` - Modifications de l'arborescence d'informations d'Access Manager (ou du nœud de gestion du service) qui comprend les objets appartenant à la classe d'objet marqueur `sunService` ou `sunServiceComponent`. Vous pouvez, par exemple, créer une stratégie visant à définir les privilèges d'accès à une ressource protégée ou modifier les règles, objets, conditions ou fournisseurs de réponse d'une stratégie existante.

`um` - Modifications dans le répertoire utilisateur (ou nœud de gestion des utilisateurs). Vous pouvez, par exemple, modifier le nom ou l'adresse de l'utilisateur.

Par exemple, pour désactiver des recherches persistantes de modifications de l'arborescence d'informations d'Access Manager (ou du nœud de gestion du service) :

```
com.sun.am.event.connection.disable.list=sm
```

Pour spécifier plusieurs valeurs, séparez chaque valeur par une virgule.

Attention – Les recherches persistantes provoquent quelques dépassements de performances sur Directory Server. Si vous déterminez que la suppression d'une partie de ce dépassement de performances est absolument indispensable dans un environnement de production, vous pouvez désactiver une ou plusieurs recherches persistantes à l'aide de la propriété `com.sun.am.event.connection.disable.list`.

Cependant, avant de désactiver une recherche persistante, vous devez comprendre les restrictions présentées ci-après. Nous vous recommandons fortement de ne pas modifier cette propriété à moins que cela ne soit absolument nécessaire. Cette propriété a été initialement introduite pour éviter tout dépassement sur Directory Server lorsque plusieurs agents 2.1 J2EE sont utilisés car chacun de ces agents crée ces recherches persistantes. Les agents 2.2 J2EE ne créant plus ces recherches persistantes, il n'est pas nécessaire d'utiliser cette propriété.

Pour plus d'informations, consultez la section "Obtention de davantage d'informations sur la désactivation des recherches persistantes (6486927)" à la page 102.

CR# 6385696 : Les IDP et SP existants et nouveaux n'apparaissent pas.

La nouvelle propriété `com.sun.identity.federation.spadapter` du fichier `AMConfig.properties` spécifie la mise en œuvre par défaut de l'adaptateur de fournisseur de services de fédération dans laquelle l'application peut obtenir des assertions et des informations de réponse. Exemple :

```
com.sun.identity.federation.spadapter=com.sun.identity.federation.plugins.FSDefaultSPAdapter
```

Access Manager 7 2005Q4 Patch 1

Le patch 1 (révision 1) d'Access Manager 7 2005Q4 a résolu de nombreux problèmes, répertoriés dans le fichier LISEZMOI accompagnant le patch. Le patch 1 inclut également les nouvelles fonctions et problèmes connus suivants :

- "Création de fichiers de débogage" à la page 63
- "Prise en charge des rôles et des rôles filtrés dans le plug-in LDAPv3" à la page 64
- "CR# 6320475 : La propriété `com.iplanet.am.session.client.polling.enable` côté serveur ne doit pas être paramétrée sur true." à la page 64
- "CR# 6358751 : L'application du patch 1 d'Access Manager 7 échoue si des espaces sont insérés dans la clé de chiffrement." à la page 64

Création de fichiers de débogage

Par défaut, les fichiers de débogage d'Access Manager sont créés dans le répertoire de débogage, même si la propriété `com.iplanet.services.debug.level` du fichier `AMConfig.properties` est paramétrée sur error. Avant la sortie du patch 1 d'Access Manager 7, un fichier de débogage n'était créé que lors de la première consignation d'un message de débogage dans le fichier.

Prise en charge des rôles et des rôles filtrés dans le plug-in LDAPv3

Le patch 1 d'Access Manager 7 ajoute la prise en charge des rôles et des rôles filtrés dans le plug-in LDAPv3, si les données sont stockées dans Sun Java System Directory Server. Pour plus d'informations, reportez-vous à la section "Documentation de la prise en charge des rôles et des rôles filtrés pour le plug-in LDAPv3 (6365196)" à la page 107.

CR# 6320475 : La propriété `com.iplanet.am.session.client.polling.enable` côté serveur ne doit pas être paramétrée sur true.

La propriété `com.iplanet.am.session.client.polling.enable` du fichier `AMConfig.properties` côté serveur est paramétrée sur false par défaut et ne doit jamais être reparamétrée sur true.

CR# 6358751 : L'application du patch 1 d'Access Manager 7 échoue si des espaces sont insérés dans la clé de chiffrement.

L'application du patch échoue si la clé de chiffrement du mot de passe contient des espaces.

Solution. Utilisez une nouvelle clé de chiffrement sans espaces. Pour connaître les étapes de changement de clé de chiffrement, reportez-vous à : Annexe B, "Changing the Password Encryption Key" du *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Nouveautés de cette version

La liste des nouvelles fonctionnalités des différentes versions de patch d'Access Manager sont disponibles dans les "Versions de patchs Access Manager 7 2005Q4" à la page 9. La version initiale d'Access Manager 7 2005Q4 intégrait les nouvelles fonctionnalités suivantes :

- "Modes d'Access Manager" à la page 65
- "Nouvelle console Access Manager" à la page 65
- "Référentiel d'identité" à la page 65
- "Arborescence d'informations d'Access Manager" à la page 66
- "Modifications liées au basculement de session" à la page 66
- "Notification de modification d'une propriété de session" à la page 67
- "Contraintes relatives aux quotas de session" à la page 67
- "Authentification distribuée" à la page 68
- "Prise en charge de plusieurs instances du module d'authentification" à la page 68
- "Espace de noms sous forme d'enchaînement ou de configuration nommée, associé à l'authentification" à la page 69
- "Améliorations du module de stratégie" à la page 69
- "Configuration du site" à la page 70
- "Fédération en bloc" à la page 70

- "Améliorations en termes de journalisation" à la page 70

Modes d'Access Manager

Access Manager 7 2005Q4 propose les modes Domaine et Hérité. Ces deux modes prennent en charge :

- les nouvelles fonctionnalités d'Access Manager 7 2005Q4 ;
- les fonctions d'Access Manager 6 2005Q1, à l'exception des points suivants :
  - Lors de la création de domaines, les organisations correspondantes ne sont pas créées dans Sun Java System Directory Server.
  - La nouvelle console Access Manager 7 2005Q4 ne peut pas définir la priorité d'un modèle de classe de service. Voir le bogue "La nouvelle console Access Manager ne permet pas de définir les priorités du modèle CoS (6309262)" à la page 88.
- les référentiels d'identité dans Sun Java System Directory Server et d'autres magasins de données.

Le mode hérité est requis pour :

- Sun Java System Portal Server ;
- les serveurs Sun Java System Communications Services, notamment Messaging Server, Calendar Server, Instant Messaging ou Delegated Administrator ;
- les déploiements avec coexistence lorsque Access Manager 6 2005Q1 et Access Manager 7 2005Q4 accèdent au même serveur Directory Server.

Nouvelle console Access Manager

La console Access Manager a été repensée de manière à être adaptée à cette version. Cependant, si Access Manager est déployé avec Portal Server, Messaging Server, Calendar Server, Instant Messaging ou Delegated Administrator, vous devez installer Access Manager en mode hérité et utiliser la console Access Manager 6 2005Q1 :

Pour de plus amples informations, reportez-vous à la section "Problèmes de compatibilité" à la page 73.

Référentiel d'identité

Les référentiels d'identité d'Access Manager contiennent des informations pertinentes sur les identités, notamment celles des utilisateurs, des groupes et des rôles. Vous pouvez créer et mettre à jour un référentiel d'identité via Access Manager ou un autre produit de provisioning, tel que Sun Java System Identity Manager.

Dans la version actuelle, un référentiel d'identité peut résider dans Sun Java System Directory Server ou dans Microsoft Active Directory. Access Manager peut accéder à un référentiel d'identité en mode lecture/écriture ou en mode lecture seule.

Arborescence d'informations d'Access Manager

L'arborescence d'informations d'Access Manager contient des informations pertinentes en termes d'accès au système. Chaque instance d'Access Manager crée et met à jour une arborescence distincte dans Sun Java System Directory Server. Vous pouvez lui attribuer n'importe quel nom (suffixe). Elle est constituée de domaines (et de sous-domaines, si nécessaire), comme décrit dans la section suivante.

Domaines d'Access Manager

Les domaines, et sous-domaines le cas échéant, sont des éléments de l'arborescence d'informations d'Access Manager. Ils peuvent contenir des informations de configuration qui définissent un ensemble d'utilisateurs et/ou de groupes, le type d'authentification des utilisateurs, les ressources auxquelles les utilisateurs peuvent accéder et les informations disponibles pour les applications, une fois les utilisateurs autorisés à accéder aux ressources. Les domaines et sous-domaines peuvent également contenir d'autres informations de configuration, notamment sur la configuration de globalisation, la configuration de la réinitialisation de mot de passe, la configuration de session, la configuration de console et les préférences utilisateur. Un domaine ou sous-domaine peut également être vide.

Vous pouvez créer un domaine à l'aide de la console Access Manager ou de l'utilitaire CLI `amadmin`. Pour plus d'informations, reportez-vous à l'aide en ligne de la console ou au Chapitre 14, “The amadmin Command Line Tool” du *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

Modifications liées au basculement de session

Access Manager permet l'implémentation d'un basculement de session indépendant du conteneur Web en utilisant Sun Java System Message Queue (Message Queue) comme courtier de communications et Berkeley DB (de Sleepycat Software, Inc.) comme base de données de stockage des sessions. Avec Access Manager 7 2005Q4, l'une des nouveautés repose sur la prise en charge du script `amsfoconfig` pour configurer l'environnement de basculement de session et du script `amsfo` pour démarrer et arrêter le courtier Message Queue et le client Berkeley DB.

Pour obtenir plus d'informations, reportez-vous à la section “Implementing Access Manager Session Failover” du *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Notification de modification d'une propriété de session

Avec la fonction de notification de modification de propriété de session, Access Manager peut envoyer une notification à des listeners spécifiques lorsqu'une modification est apportée à une propriété de session spécifique. Cette fonction prend effet lorsque l'attribut Activer les notifications de modification de propriété est activé dans la console d'administration d'Access Manager. Par exemple, dans un environnement de connexion unique, une session Access Manager peut être partagée par plusieurs applications. Lors de la modification d'une propriété de session spécifique définie dans la liste Propriétés de notification, Access Manager envoie une notification à tous les listeners enregistrés.

Pour obtenir plus d'informations, reportez-vous à la section "Enabling Session Property Change Notifications" du *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Contraintes relatives aux quotas de session

La fonction de contraintes de quota de session permet à l'administrateur d'Access Manager (`amadmin`) de définir l'attribut Sessions utilisateur actives de manière à limiter le nombre de sessions utilisées simultanément par un même utilisateur. L'administrateur peut définir une contrainte de quota de session au niveau global pour tous les utilisateurs ou pour une entité, par exemple une organisation, un domaine, un rôle ou un utilisateur qui s'applique à un ou plusieurs utilisateurs spécifiques.

Par défaut, ces contraintes sont désactivées, mais l'administrateur peut les activer en paramétrant l'attribut Activer les contraintes liées aux quotas dans la console d'administration d'Access Manager.

L'administrateur peut également configurer le comportement adopté si un utilisateur épuise le quota de sessions en paramétrant l'attribut Comportement observé en cas d'épuisement du quota de sessions :

- DENY_ACCESS. Access Manager rejette la demande de connexion pour une nouvelle session.
- DESTROY_OLD_SESSION. Access Manager détruit la prochaine session arrivant à expiration pour l'utilisateur donné et accepte la nouvelle demande de connexion.

L'attribut Exempter les administrateurs de niveau supérieur de la vérification des contraintes détermine si les quotas s'appliquent également aux administrateurs de niveau supérieur.

Pour plus d'informations, reportez-vous à la section "Setting Session Quota Constraints" du *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*

Authentification distribuée

Access Manager 7 2005Q4 comprend l'interface utilisateur d'authentification distribuée, un composant d'interface utilisateur d'authentification à distance offrant une authentification distribuée et sécurisée sur deux pare-feu dans un déploiement. Sans le composant d'interface utilisateur d'authentification distribuée, les URL de service Access Manager peuvent se trouver exposées aux utilisateurs finaux. Cette exposition peut être évitée par l'utilisation d'un serveur proxy ; toutefois, un serveur proxy n'est pas nécessairement une solution acceptable pour un grand nombre de déploiements.

Le composant d'interface utilisateur d'authentification distribuée est installé sur un ou plusieurs serveurs dans la couche (DMZ) non sécurisée d'un déploiement Access Manager. Un serveur d'interface utilisateur d'authentification distribuée n'exécute pas Access Manager ; il n'existe que pour fournir l'interface d'authentification aux utilisateurs finaux par le biais d'un navigateur Web.

L'utilisateur final envoie une requête HTTP à l'interface utilisateur d'authentification distribuée, qui présente à son tour une page de connexion à l'utilisateur. Le composant d'authentification distribuée envoie ensuite la requête de l'utilisateur par le biais du second pare-feu vers un serveur Access Manager, ce qui permet d'éviter d'ouvrir des trous dans les pare-feu entre les utilisateurs finaux et le serveur Access Manager.

Pour plus d'informations, reportez-vous au manuel *Technical Note: Using Access Manager Distributed Authentication* .

Prise en charge de plusieurs instances du module d'authentification

Tous les modules d'authentification ont été étendus de manière à prendre en charge le sous-schéma avec l'interface utilisateur de la console. Il est possible de créer plusieurs instances de module d'authentification pour chaque type de module (classe de module chargée). Par exemple, s'il existe deux instances appelées `ldap1` et `ldap2` pour un type de module LDAP, chacune des instances peut désigner un serveur d'annuaire LDAP différent. Les instances dotées du même nom que leur type de module sont prises en charge à des fins de compatibilité ascendante. L'appel requis est le suivant :

server_deploy_uri`/UI/Login?module=`*module-instance-name*

Espace de noms sous forme d'enchaînement ou de configuration nommée, associé à l'authentification

Un espace de noms séparé est créé sous une organisation/un domaine, qui correspond à une chaîne d'instances de module d'authentification. La même chaîne peut être réutilisée et assignée à une organisation/un domaine, un rôle ou un utilisateur. L'instance du service d'authentification correspond à la chaîne d'authentification. L'appel requis est le suivant :

server_deploy_uri`/UI/Login?service=`*authentication-chain-name*

Améliorations du module de stratégie

Attributs de personnalisation

Outre les règles, les objets et les conditions, les stratégies disposent désormais d'attributs de personnalisation (`IDResponseProvider`). La décision de stratégie envoyée au client à partir de l'évaluation de stratégie comporte désormais des attributs de personnalisation de réponse basés sur la stratégie. Deux types d'attributs de personnalisation sont pris en charge :

- Les attributs statiques. Vous définissez le nom et la valeur de l'attribut dans la stratégie.
- Les attributs dynamiques. Vous répertoriez les noms des attributs dans les stratégies, et les valeurs sont récupérées dans les magasins de données du référentiel d'identité au moment de l'évaluation de la stratégie.

Les points d'application de stratégie (agents) transfèrent généralement ces valeurs d'attribut à l'application protégée, sous forme d'en-tête HTTP, de cookies ou d'attributs de requête.

Access Manager 7 2005Q4 ne prend pas en charge les implémentations personnalisées de l'interface du fournisseur de réponse, effectuées par les utilisateurs.

Condition de propriété de session

L'implémentation d'une condition de propriété de session (`SessionPropertyCondition`) permet de déterminer si une stratégie s'applique à une requête, en fonction de la valeur des propriétés définies dans la session Access Manager d'un utilisateur. Au moment de l'évaluation de la stratégie, la condition renvoie la valeur “true” uniquement si la session Access Manager de l'utilisateur comporte toutes les valeurs de propriété définies dans la condition. Lorsque les propriétés sont définies avec plusieurs valeurs dans la condition, il suffit que la session de l'utilisateur dispose d'au moins une des valeurs répertoriées pour la propriété dans la condition.

Objet de stratégie

L'implémentation d'un objet de stratégie (objet d'identité Access Manager) vous permet d'utiliser, comme valeurs d'objet, des entrées du référentiel d'identité configuré.

Exportation de stratégie

Vous pouvez exporter des stratégies au format XML à l'aide de la commande `amadmin`. Cette fonction est prise en charge par les nouveaux éléments `GetPolices` et `RealmGetPolicies` du fichier `amAdmin.dtd`.

État de la stratégie

Les stratégies disposent désormais d'un attribut d'état, indiquant si elles sont actives ou inactives. Les stratégies inactives sont ignorées durant la phase d'évaluation de stratégie.

Configuration du site

Access Manager 7 2005Q4 introduit le concept de "site" qui implique une gestion centralisée de la configuration associée au déploiement d'Access Manager. Lorsque Access Manager est configuré en tant que site, les requêtes des clients transitent toujours par l'équilibreur de charge, ce qui simplifie le déploiement et permet de résoudre certains problèmes, notamment lors de la présence d'un pare-feu entre le client et les serveurs d'arrière-plan Access Manager.

Pour obtenir plus d'informations, reportez-vous à la section "Configuring an Access Manager Deployment as a Site" du *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Fédération en bloc

Access Manager 7 2005Q4 propose une fonction de fédération en bloc des comptes d'utilisateur pour les applications externalisées auprès de partenaires commerciaux. Auparavant, pour fédérer des comptes entre un fournisseur de services et un fournisseur d'identités, chaque utilisateur devait accéder aux sites respectifs des deux fournisseurs, créer des comptes le cas échéant et fédérer les deux comptes via un lien Web. Ce processus prenait un certain temps et n'était pas toujours approprié, notamment lorsqu'il s'agissait d'effectuer le déploiement avec des comptes existants ou lorsque le site intervenait lui-même en tant que fournisseur d'identités ou qu'il utilisait l'un de ses partenaires comme fournisseur d'authentification.

Pour plus d'informations, reportez-vous au manuel *Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide*.

Améliorations en termes de journalisation

Access Manager 7 2005Q4 intègre plusieurs améliorations en termes de journalisation :

- Nouveaux champs (ou colonnes) : le champ `MessageID` contient l'identificateur de message de l'événement consigné. Le champ `ContextID` contient l'identificateur de contexte, qui est semblable à un identificateur de session et qui s'applique à tous les événements de la session d'un utilisateur particulier. Dans le cadre d'une session spécifique d'un utilisateur, la valeur `ContextID` sera la même pour tous les événements consignés dans les fichiers journaux.

- API de journalisation : l'API comporte des nouveautés relatives à la lecture des enregistrements de journal, notamment à partir d'une base de données, lorsque la fonction de journalisation dans la base de données est configurée. Reportez-vous à l'élément `LogReaderSample.java` du répertoire `/opt/SUNWam/samples/logging`, qui présente la récupération des enregistrements de journal à partir d'un fichier plat ou d'un référentiel de table de base de données.

Attention – Les tables de base de données ont tendance à être plus volumineuses que les journaux de fichiers plats. Par conséquent, dans une requête donnée, évitez de récupérer tous les enregistrements d'une table de base de données, car une telle quantité de données risquerait d'utiliser toutes les ressources du serveur Access Manager.

Configurations matérielle et logicielle requises

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

TABLEAU 4 Configurations matérielle et logicielle requises

Composant	Configuration requise
Système d'exploitation	Système d'exploitattion Solaris sur les systèmes SPARC™, versions 8, 9 et 10, avec prise en charge des zones locales racines sur Solaris 10
	Système d'exploitation Solaris sur les plates-formes x86, versions 9 et 10, avec prise en charge des zones locales racines sur Solaris 10
	Système d'exploitation Solaris sur les plates-formes AMD64, version 10, avec prise en charge des zones locales racines
	Red Hat™ Linux, WS/AS/ES 2.1 Update 6 ou ultérieur
	Red Hat Linux, WS/AS/ES 3.0
	Red Hat Linux, WS/AS/ES 3.0 Updates 1, 2, 3 et 4
	HP-UX. Reportez-vous à la documentation Sun Java Enterprise System 2005Q4 pour HP-UX : `http://docs.sun.com/coll/1258.2`
	Windows. Reportez-vous à la documentation Sun Java Enterprise System 2005Q4 pour Microsoft Windows : `http://docs.sun.com/coll/1259.2`
Java 2 Standard Edition (J2SE)	Plate-forme J2SE 1.5.0_04, 1.5_01, 1.5 et 1.4.2

TABLEAU 4 Configurations matérielle et logicielle requises *(Suite)*

Composant	Configuration requise
Directory Server	Arborescence d'informations d'Access Manager : Sun Java System Directory Server 5 2005Q4
	Référentiel d'identités Access Manager : Sun Java System Directory Server 5 2005Q4 ou Microsoft Active Directory
Conteneurs Web	Sun Java System Web Server 6.1 2005Q4 SP5
	Sun Java System Application Server Enterprise Edition 8.1 2005Q2
	BEA WebLogic Server 8.1 SP4
	IBM WebSphere Application Server 5.1 et 5.1.1 (et correctifs associés)
Mémoire vive	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 2005Q4.

TABLEAU 5 Navigateurs pris en charge

Navigateur	Plate-forme
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000
Microsoft Internet Explorer 6.0	Windows 2000
	Windows XP

TABLEAU 5 Navigateurs pris en charge *(Suite)*

Navigateur	Plate-forme
Mozilla 1.7.1	Système d'exploitation Solaris, versions 9 et 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0
Netscape™ 7.0	Système d'exploitation Solaris, versions 9 et 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0

Prise en charge de la virtualisation du système

La virtualisation du système est une technologie qui permet d'exécuter plusieurs instances de système d'exploitation (SE) indépendamment sur du matériel partagé. D'un point de vue fonctionnel, les logiciels déployés sur un SE hébergé dans un environnement virtuel ignorent généralement que la plate-forme sous-jacente a été virtualisée. Sun teste ses produits Sun Java System en fonction d'une virtualisation de système et des combinaisons de SE sélectionnées pour s'assurer que les produits Sun Java System continuent de fonctionner dans des environnements virtuels correctement dimensionnés et configurés de la même façon que sur des systèmes non virtuels. Pour plus d'informations sur la prise en charge par Sun des produits Sun Java System dans des environnements virtuels, rendez-vous sur http://docs.sun.com/doc/820-4651.

Problèmes de compatibilité

- "Mode hérité d'Access Manager" à la page 73
- "Agents de stratégie Access Manager" à la page 75

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 74
- "Option d'installation Configurer maintenant en mode graphique" à la page 74
- "Option d'installation Configurer maintenant en mode texte" à la page 74
- "Option d'installation Configurer ultérieurement" à la page 74

Pour déterminer le mode dans lequel Access Manager 7 2005Q4 a été configuré, reportez-vous à la section "Détection du mode d'Access Manager" à la page 75.

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, "Installation en mode Silencieux" du *Guide d'installation de Sun Java Enterprise System 2005Q4 pour 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
...
```

Sous Windows, le fichier de configuration est *AccessManager-base* `\setup\AMConfigurator.properties`.

Pour plus d'informations sur la configuration d'Access Manager par le biais de l'exécution du script `amconfig`, reportez-vous au manuel *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

Détection du mode d'Access Manager

Pour déterminer le mode dans lequel Access Manager 7 2005Q4 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 2005Q4.

TABLEAU 6 Compatibilité entre les agents de stratégie et les modes d'Access Manager 7 2005Q4

Agent et version	Mode compatible
Agents J2EE et Web, version 2.2	Modes Domaine et Hérité
Agents Web, version 2.1	Modes Domaine et Hérité
Agents J2EE, version 2.1	Mode hérité uniquement

Notes relatives à l'installation

Les notes relatives à l'installation d'Access Manager comprennent les informations suivantes :

- "Mode hérité d'Access Manager" à la page 73
- "Problèmes relatifs à l'installation" à la page 78

Problèmes connus et restrictions

Cette section présente les différents problèmes connus au moment de la mise sur le marché de cette version, ainsi que leurs solutions, le cas échéant.

- "Problèmes de compatibilité" à la page 76
- "Problèmes relatifs à l'installation" à la page 78
- "Problèmes de mise à niveau" à la page 80
- "Problèmes de configuration" à la page 83
- "Problèmes liés à la console Access Manager" à la page 87
- "Problèmes liés au SDK et au client" à la page 89
- "Problèmes liés aux utilitaires de ligne de commande" à la page 91
- "Problèmes d'authentification" à la page 92
- "Problèmes de session et de connexion unique" à la page 93
- "Problèmes liés aux stratégies" à la page 95
- "Problèmes liés au démarrage du serveur" à la page 95
- "Problèmes concernant le système d'exploitation Linux" à la page 96
- "Problèmes liés à SAML et aux fédérations" à la page 96
- "Problèmes liés à la globalisation (g11n)" à la page 99
- "Problèmes liés à la documentation" à la page 101

Problèmes de compatibilité

- "Incompatibilité entre les serveurs Java ES 2004Q2 et Instant Messaging sous Java ES 2005Q4 (6309082)" à la page 77
- "En mode Hérité, il existe des incompatibilités dans le module d'authentification principale (6305840)" à la page 77
- "Un agent ne peut pas se connecter, car son profil n'existe pas dans l'organisation (6295074)" à la page 77
- "La commande `commadmin` de l'utilitaire Delegated Administrator ne parvient pas à créer un utilisateur (6294603)" à la page 77
- "La commande `commadmin` de l'utilitaire Delegated Administrator ne parvient pas à créer une organisation (6292104)" à la page 78

Incompatibilité entre les serveurs Java ES 2004Q2 et Instant Messaging sous Java ES 2005Q4 (6309082)

Le scénario de déploiement ci-dessous a provoqué le problème suivant :

- server-1 : Java ES 2004Q2 : Directory Server
- serveur-2 : Java ES 2004Q2 : Application Server, Access Manager et Portal Server
- serveur-3 : Java ES 2004Q2 : Calendar Server et Messaging Server
- serveur-4 : Java ES 2005Q4 : Application Server, Instant Messaging et Access Manager SDK

Lors de l'exécution de l'utilitaire `imconfig` pour configurer Instant Messaging sur le serveur-4, la configuration a échoué. Le SDK d'Access Manager 7 2005Q4, utilisé par Instant Messaging (IM) sur le serveur 4, n'est pas compatible avec la version Java ES 2004Q2.

Solution : Idéalement, le serveur et le SDK Access Manager doivent tous deux être de la même version. Pour obtenir plus d'informations, consultez le *Guide de mise à niveau de Sun Java Enterprise System 2005Q4*.

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

Le mode Hérité d'Access Manager 7 2005Q4 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 2005Q4, 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.

Un agent ne peut pas se connecter, car son profil n'existe pas dans l'organisation (6295074)

Dans la console Access Manager, vous avez créé un agent en mode Domaine. Si vous vous déconnectez, puis vous reconnectez à l'aide du nom de l'agent, Access Manager renvoie une erreur car l'agent ne dispose pas des privilèges requis pour accéder au domaine.

Solution : Modifiez les droits de manière à autoriser les accès en lecture/écriture pour cet agent.

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 se produit si vous effectuez une mise à niveau vers Access Manager version 7 2005Q4, mais que vous ne mettez pas à niveau Delegated Administrator. Pour obtenir plus d'informations sur la mise à niveau de Delegated Administrator, consultez le *Guide de mise à niveau de Sun Java Enterprise System 2005Q4*.

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 relatifs à l'installation

- "Après l'application du patch 1, le fichier `/tmp/amsilent` offre un accès en lecture à tous les utilisateurs (6370691)" à la page 79
- "Lors de l'installation du SDK avec la configuration du conteneur, l'URL de notification est incorrect (6327845)" à la page 79
- "La valeur `classpath` d'Access Manager fait référence au package JCE 1.2.1 qui a expiré (6297949)" à la page 79
- "L'installation d'Access Manager dans une arborescence d'informations d'annuaire existante requiert la reconstruction des index de Directory Server (6268096)" à la page 79
- "Les droits associés aux répertoires de débogage et de journaux sont incorrects pour les utilisateurs non root (6257161)" à la page 80
- "Le service d'authentification n'est pas initialisé lorsque Access Manager et Directory Server sont installés sur des machines séparées (6229897)" à la page 80
- "Le programme d'installation n'ajoute pas d'entrée de plate-forme pour un serveur d'annuaire existant (6202902)" à la page 80

Après l'application du patch 1, le fichier `/tmp/amsilent` offre un accès en lecture à tous les utilisateurs (6370691)

Après l'application du patch 1, le fichier `/tmp/amsilent` offre un accès en lecture à tous les utilisateurs.

Solution : Après avoir appliqué le patch, réinitiailisez les permissions du fichier pour n'autoriser l'accès en lecture que par l'administrateur Access Manager.

Lors de l'installation du SDK avec la configuration du conteneur, l'URL de notification est incorrect (6327845)

Si vous effectuez une installation du SDK avec la configuration du conteneur (DEPLOY_LEVEL=4), l'URL de notification est incorrect.

Solution :

1. Définissez la propriété ci-dessous dans le fichier `AMConfig.properties` :

   ```
   com.iplanet.am.notification.url=
   protocol://fqdn:port/amserver/servlet/com.iplanet.services.comm.client.
   PLLNotificationServlet
   ```

2. Redémarrez Access Manager afin que la nouvelle valeur soit prise en compte.

La valeur `classpath` d'Access Manager fait référence au package JCE 1.2.1 qui a expiré (6297949)

La valeur `classpath` d'Access Manager fait référence au package Java Cryptography Extension (JCE) 1.2.1 (certificat de signature), qui a expiré le 27 juillet 2005.

Solution : aucune. Bien que la référence au package figure dans la variable `classpath`, Access Manager n'utilise pas ce package.

L'installation d'Access Manager dans une arborescence d'informations d'annuaire existante requiert la reconstruction des index de Directory Server (6268096)

Afin d'améliorer les performances de recherche, Directory Server a été doté de nouveaux index.

Solution : Après avoir installé Access Manager dans une arborescence d'informations d'annuaire existante, vous devez recréer les index Directory Server en exécutant le script `db2index.pl`. Exemple :

```
# ./db2index.pl -D "cn=Directory Manager" -w password -n userRoot
```

Le script `db2index.pl` est accessible à partir du répertoire *DS-install-directory/slapd-hostname/*.

Les droits associés aux répertoires de débogage et de journaux sont incorrects pour les utilisateurs non root (6257161)

Lorsqu'un utilisateur non root est spécifié dans le fichier de configuration de l'installation silencieuse, les autorisations liées au débogage, aux journaux et aux répertoires de démarrage ne sont pas définies correctement.

Solution : Modifiez les droits associés à ces répertoires de manière à autoriser l'accès d'un utilisateur non root.

Le service d'authentification n'est pas initialisé lorsque Access Manager et Directory Server sont installés sur des machines séparées (6229897)

Bien que la variable `classpath` et les autres variables d'environnement de conteneur Web d'Access Manager soient mises à jour pendant l'installation, le processus d'installation ne redémarre pas le conteneur Web. Si vous essayez de vous connecter à Access Manager après l'installation et avant le redémarrage du conteneur Web, l'erreur suivante est renvoyée :

```
Authentication Service is not initialized.
Contact your system administrator.
```

Solution : Redémarrez le conteneur Web avant de vous connecter à Access Manager. Directory Server doit également être en cours d'exécution au moment de la connexion.

Le programme d'installation n'ajoute pas d'entrée de plate-forme pour un serveur d'annuaire existant (6202902)

Le programme d'installation de Java ES n'ajoute pas d'entrée de plate-forme pour un serveur d'annuaire existant (DIRECTORY_MODE=2).

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 2005Q4 Deployment Planning Guide*.

Problèmes de mise à niveau

- "Le script `ampre70upgrade` d'Access Manager ne supprime pas les packages localisés (6378444)" à la page 81
- "Le fichier `AMConfig.properties` dispose d'une ancienne version du conteneur Web (6316833)" à la page 81
- "Le fichier `server.policy` de l'agent de nœud n'est pas mis à jour lors de la mise à niveau d'Access Manager (6313416)" à la page 81

- "À l'issue d'une mise à niveau, la condition de propriété de session ne figure pas dans la liste des conditions (6309785)" à la page 82
- "Après une mise à niveau, le type Objet d'identité ne figure pas dans la liste des objets de stratégie (6304617)" à la page 82
- "Échec de la mise à niveau d'Access Manager, du fait de l'absence de migration de la variable `classpath` (6284595)" à la page 82
- "À l'issue d'une mise à niveau, la commande `amadmin` renvoie une version incorrecte (6283758)" à la page 83
- "Ajout de l'attribut `ContainerDefaultTemplateRole` après la migration des données (4677779)" à la page 83

Le script `ampre70upgrade` d'Access Manager ne supprime pas les packages localisés (6378444)

Si vous procédez à une mise à niveau depuis Access Manager vers Access Manager 7 2005Q4, le script `ampre70upgrade` ne supprime aucun package Access Manager localisé présent sur votre système.

Solution : Avant de procéder à la mise à niveau vers Access Manager 7 2005Q4, utilisez la commande `pkgrm` pour supprimer manuellement tous les packages Access Manager localisés installés sur votre système.

Le fichier `AMConfig.properties` dispose d'une ancienne version du conteneur Web (6316833)

Après la mise à niveau d'Access Manager et d'Application Server vers Java ES 2005Q4, le fichier `AMConfig.properties` d'Access Manager dispose d'une ancienne version d'Application Server.

Solution : Avant d'exécuter le programme de configuration de Delegated Administrator (`config-commda`), modifiez la propriété ci-dessous dans le fichier `AMConfig.properties` :

```
com.sun.identity.webcontainer=IAS8.1
```

Le fichier `server.policy` de l'agent de nœud n'est pas mis à jour lors de la mise à niveau d'Access Manager (6313416)

À l'issue de la mise à niveau d'Access Manager, le fichier `server.policy` de l'agent de nœud n'est pas mis à jour.

Solution : Remplacez le fichier `server.policy` de l'agent de nœud par le fichier suivant :

```
/var/opt/SUNWappserver/domains/domain1/config/server.policy
```

À l'issue d'une mise à niveau, la condition de propriété de session ne figure pas dans la liste des conditions (6309785)

Après une mise à niveau d'Access Manager version 2005Q1 vers la version 2005Q4, la condition de propriété de session n'est pas proposée comme choix dans la liste des conditions de stratégie si vous tentez d'ajouter une condition à une stratégie.

Solution : Sélectionnez le type de la condition de propriété de session dans le modèle du service de configuration de stratégie, au niveau du domaine correspondant.

Après une mise à niveau, le type Objet d'identité ne figure pas dans la liste des objets de stratégie (6304617)

À l'issue de la mise à niveau d'Access Manager version 2005Q1 vers la version 2005Q4, le type Objet d'identité, nouveau type d'objet de stratégie, n'est pas proposé comme choix dans la liste des objets de stratégie.

Solution : Sélectionnez le type Objet d'identité comme type d'objet par défaut dans le modèle du service de configuration de stratégie.

Échec de la mise à niveau d'Access Manager, du fait de l'absence de migration de la variable `classpath` (6284595)

Lors de la mise à niveau d'Access Manager, de Java ES 2004Q2 vers Java ES 2005Q4, la mise à niveau de Java ES 2004Q2 vers Java ES 2005Q4 a échoué. Access Manager a été déployé sur Application Server, ce dernier ayant également été mis à niveau de Java ES 2004Q2 vers Java ES 2005Q4. Le `classpath` dans le fichier `domain.xml` ne contenait pas de chemins d'accès aux fichiers JAR Access Manager.

Solution : Procédez comme indiqué ci-dessous.

1. Avant d'exécuter le script `amupgrade`, vous devez réindexer Directory Server, en raison d'un problème avec le script `comm_dssetup.pl`.
2. Ajoutez des entrées associées à Access Manager dans le fichier `server.policy` de l'agent de nœud. Il vous suffit de copier le fichier `server.policy` à partir du fichier par défaut (`/var/opt/SUNWappserver/domains/domain1/config/server.policy`).
3. Mettez à jour la variable `classpath` dans le fichier `domain.xml` de l'agent de nœud, de la manière suivante : Copiez les éléments `classpath-suffix` et `classpath` appropriés à partir des attributs `server-classpath` de l'élément `java-config` du fichier `server.xml` et utilisez-les pour les attributs correspondants, dans l'élément `java-config` du fichier`domain.xml`. L'élément `java-config` se trouve sous l'élément `config` du fichier `domain.xml`.

À l'issue d'une mise à niveau, la commande `amadmin` renvoie une version incorrecte (6283758)

À l'issue de la mise à niveau d'Access Manager version 6 2005Q1 vers la version 7 2005Q4, la commande `amadmin --version` a renvoyé une version incorrecte : Sun Java System Access Manager version 2005Q1.

Solution : Après avoir mis à niveau Access Manager, exécutez le script `amconfig` pour configurer Access Manager. Lors de l'exécution de `amconfig`, spécifiez le chemin d'accès complet au fichier de configuration (`amsamplesilent`). Par exemple, sous un système Solaris :

```
# ./amconfig -s ./config-file
```

eur

```
# ./amconfig -s /opt/SUNWam/bin/config-file
```

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

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.

Problèmes de configuration

- "Le fichier `server.policy` d'Application Server 8.1doit être modifié lors de l'utilisation d'URI autres que ceux par défaut (6309759)" à la page 84
- "La liste des serveurs de plate-forme et l'attribut d'alias FQDN ne sont pas mis à jour (6309259, 6308649)" à la page 85
- "Validation de données d'attributs requis dans les services (6308653)" à la page 85
- "Exception lors du déploiement sur une instance WebLogic 8.1 sécurisée (6295863)" à la page 85

- "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)" à la page 86
- "Dans le modèle de fichier d'état de configuration, le mode Domaine est le mode par défaut d'Access Manager (6280844)" à la page 86
- "Échec de signature d'URL dans IBM WebSphere avec une clé RSA (6271087)" à la page 86

Le fichier server.policy d'Application Server 8.1doit être modifié lors de l'utilisation d'URI autres que ceux par défaut (6309759)

Si vous déployez Access Manager 7 2005Q4 sur Application Server 8.1 et que vous utilisez des URI autres que ceux par défaut pour les services, la console et les applications Web avec mot de passe qui disposent des URI par défaut amserver, amconsole et ampassword, vous devez modifier le fichier server.policy correspondant au domaine du serveur d'application avant de tenter d'accéder à Access Manager via un navigateur Web.

Solution : Modifiez le fichier server.policy de la manière suivante :

1. Arrêtez l'instance Application Server sur laquelle Access Manager est déployé.
2. Accédez au répertoire /config. Exemple :

   ```
   cd /var/opt/SUNWappserver/domains/domain1/config
   ```

3. Effectuez une copie de sauvegarde du fichier server.policy. Exemple :

   ```
   cp server.policy server.policy.orig
   ```

4. Dans le fichier server.policy, recherchez les stratégies suivantes :

   ```
   grant codeBase "file:\${com.sun.aas.instanceRoot}/
   applications/j2ee-modules/amserver/-" { ...
   };
   grant codeBase "file:\${com.sun.aas.instanceRoot}/
   applications/j2ee-modules/amconsole/-" { ...
   };
   grant codeBase "file:\${com.sun.aas.instanceRoot}/
   applications/j2ee-modules/ampassword/-" { ...
   };
   ```

5. Dans la ligne ci-dessous, remplacez l'URI par défaut amserver par l'URI qui est utilisé pour l'application Web des services :

   ```
   grant codeBase "file:\${com.sun.aas.instanceRoot}/
   applications/j2ee-modules/amserver/-" {
   ```

6. Pour les installations en mode Hérité, remplacez l'URI par défaut amconsole par l'URI qui est utilisé pour l'application Web de la console (et qui est différent de celui par défaut) dans la ligne suivante :

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amconsole/-" {
```

7. Remplacez l'URI par défaut `ampassword` par l'URI utilisé pour l'application Web avec mot de passe dans la ligne ci-dessous:

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/ampassword/-" {
```

8. Démarrez l'instance Application Server sur laquelle Access Manager est déployé.

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 2005Q4 Deployment Planning Guide*.

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

Avec Access Manager 7 2005Q4, 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 2005Q4 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 indiqué ci-dessous.

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 2005Q4 Deployment Planning 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
```

Échec de signature d'URL dans IBM WebSphere avec une clé RSA (6271087)

Avec une clé RSA dans IBM WebSphere, la signature de la chaîne URL échoue avec l'exception suivante :

```
ERROR: FSSignatureUtil.signAndReturnQueryString: FSSignatureException
occured while signing query string: no such provider: SunRsaSign
```

Solution : Le fournisseur SunRsaSign est manquant dans le JDK intégré WebSphere. Pour résoudre ce problème, modifiez le fichier *websphere_jdk_root*`/jre/lib/security/java.security` et ajoutez la ligne suivante pour activer SunRsaSign en tant que fournisseur :

```
security.provider.6=com.sun.rsajca.Provider
```

Problèmes liés à la console Access Manager

- "Pour SAML, erreurs d'édition de doublon Trusted Partner (6326634)" à la page 87
- "La journalisation à distance ne fonctionne pas pour `amConsole.access` et `amPasswordReset.access` (6311786)" à la page 87
- "L'ajout de propriétés `amadmin` supplémentaires dans la console entraîne la modification du mot de passe de l'utilisateur `amadmin` (6309830)" à la page 88
- "La nouvelle console Access Manager ne permet pas de définir les priorités du modèle CoS (6309262)" à la page 88
- "Une exception est générée lors de l'ajout d'un groupe à un utilisateur en tant qu'administrateur de stratégies (6299543)" à la page 88
- "En mode hérité, vous ne pouvez pas supprimer tous les utilisateurs d'un rôle (6293758)" à la page 88
- "Impossible d'ajouter, de supprimer ou de modifier des offres de ressources du service de découverte (6273148)" à la page 88
- "Un mot de passe incorrect pour la liaison LDAP devrait générer une erreur lors de la recherche d'objet (6241241)" à la page 89
- "Access Manager ne peut pas créer une organisation sous un conteneur en mode hérité (6290720)" à la page 89
- "L'ancienne console apparaît lors de l'ajout de services associés à Portal Server (6293299)" à la page 89
- "La console ne renvoie pas les résultats de Directory Server, une fois la limite des ressources atteinte (6239724)" à la page 89

Pour SAML, erreurs d'édition de doublon Trusted Partner (6326634)

Dans la console Access Manager, vous avez créé un partenaire de confiance SAML sous l'onglet Fédération > SAML. Si vous tentez de le dupliquer, des erreurs se produisent.

Solution : aucune. Ce problème est résolu dans le patch 1. Pour plus d'informations sur l'application du patch à votre plate-forme spécifique, reportez-vous à la section "Access Manager 7 2005Q4 Patch 1" à la page 63.

La journalisation à distance ne fonctionne pas pour `amConsole.access` et `amPasswordReset.access` (6311786)

Lorsque la fonction de journalisation à distance est activée, tous les journaux sont écrits dans l'instance Access Manager distante, à l'exception des journaux `amConsole.access`et `amPasswordReset.access` regroupant les informations de réinitialisation de mot de passe. L'enregistrement de journal n'est écrit nulle part.

Solution : aucune.

L'ajout de propriétés `amadmin` supplémentaires dans la console entraîne la modification du mot de passe de l'utilisateur `amadmin` (6309830)

L'ajout ou la modification de certaines propriétés de l'utilisateur `amadmin` dans la console d'administration entraîne la modification du mot de passe de l'utilisateur `amadmin`.

Solution : aucune. Ce problème est résolu dans le patch 1. Pour plus d'informations sur l'application du patch à votre plate-forme spécifique, reportez-vous à la section "Access Manager 7 2005Q4 Patch 1" à la page 63.

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

La nouvelle console Access Manager 7 2005Q4 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.

Une exception est générée lors de l'ajout d'un groupe à un utilisateur en tant qu'administrateur de stratégies (6299543)

La console Access Manager renvoie une exception lorsque vous ajoutez un groupe à un utilisateur en tant qu'administrateur de stratégies.

Solution : aucune.

En mode hérité, vous ne pouvez pas supprimer tous les utilisateurs d'un rôle (6293758)

En mode hérité, si vous essayez de supprimer tous les utilisateurs d'un rôle, il reste un utilisateur.

Solution : Essayez de nouveau de supprimer l'utilisateur du rôle.

Impossible d'ajouter, de supprimer ou de modifier des offres de ressources du service de découverte (6273148)

La console d'administration d'Access Manager ne vous permet pas d'ajouter, de supprimer ou de modifier les offres de ressources d'un utilisateur, d'un rôle ou d'un domaine.

Solution : aucune. Ce problème est résolu dans le patch 1. Pour plus d'informations sur l'application du patch à votre plate-forme spécifique, reportez-vous à la section "Access Manager 7 2005Q4 Patch 1" à la page 63.

Un mot de passe incorrect pour la liaison LDAP devrait générer une erreur lors de la recherche d'objet (6241241)

La console d'administration d'Access Manager ne renvoie pas d'erreur lors de l'utilisation d'un mot de passe incorrect pour la liaison LDAP.

Solution : aucune.

Access Manager ne peut pas créer une organisation sous un conteneur en mode hérité (6290720)

Si vous créez un conteneur, puis essayez de créer une organisation sous ce conteneur, Access Manager signale une violation de contrainte d'unicité.

Solution : aucune.

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.

Problèmes liés au SDK et au client

- "Impossible de supprimer la configuration du service de session d'un sous-domaine (6318296)" à la page 90

- "Le servlet CDC redirige l'utilisateur vers une page de connexion non valide lorsque la condition de stratégie est indiquée (6311985)" à la page 90
- "Les clients ne reçoivent pas de notifications après le redémarrage du serveur (6309161)" à la page 90
- "Redémarrer les clients SDK après une modification du schéma de service (6292616)" à la page 90

Impossible de supprimer la configuration du service de session d'un sous-domaine (6318296)

Après l'ajout d'un sous-domaine au domaine supérieur, puis l'ajout d'un service de session à ce sous-domaine, si vous tentez de supprimer la configuration du service de session, un message d'erreur apparaît.

Solution : Supprimez le référentiel d'identités supérieur par défaut, AMSDK1, puis ajoutez-le à nouveau dans la configuration.

Ce problème est résolu dans le patch 1. Pour plus d'informations sur l'application du patch à votre plate-forme spécifique, reportez-vous à la section "Access Manager 7 2005Q4 Patch 1" à la page 63.

Le servlet CDC redirige l'utilisateur vers une page de connexion non valide lorsque la condition de stratégie est indiquée (6311985)

Avec l'agent Apache 2.2 en mode d'authentification unique interdomaines (CDSSO), lors de l'accès à la ressource protégée par l'agent, le servlet CDC redirige l'utilisateur vers une page d'authentification anonyme, au lieu de la page de connexion par défaut.

Solution : aucune. Ce problème est résolu dans le patch 1. Pour plus d'informations sur l'application du patch à votre plate-forme spécifique, reportez-vous à la section "Access Manager 7 2005Q4 Patch 1" à la page 63.

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. Pour plus d'informations sur l'application du patch à votre plate-forme spécifique, reportez-vous à la section “Access Manager 7 2005Q4 Patch 1” à la page 63.

Problèmes liés aux utilitaires de ligne de commande

- “La recherche LDAP d'attributs null renvoie une erreur lorsqu'Access Manager pointe vers Directory Proxy (6357975)” à la page 91
- “Les nouveaux fichiers de schéma ne figurent pas dans le script `amserveradmin` (6255110)” à la page 91
- “Impossible d'enregistrer des documents XML avec un caractère d'échappement dans Internet Explorer 6.0 (4995100)” à la page 91

La recherche LDAP d'attributs null renvoie une erreur lorsqu'Access Manager pointe vers Directory Proxy (6357975)

Si vous utilisez Sun Java System Directory Proxy Server, une recherche LDAP d'attributs null renvoie une erreur. Exemple :

```
# ldapsearch -b base-dn uid=user ""
```

Si Access Manager pointe directement vers le serveur d'annuaire LDAP, la même recherche aboutit.

Solution : si vous utilisez Directory Proxy Server, activez les recherches d'attributs null ou saisissez un nom d'attribut pour la recherche.

Les nouveaux fichiers de schéma ne figurent pas dans le script `amserveradmin` (6255110)

Après l'installation, lorsque vous devez exécuter le script `amserveradmin` pour charger les services dans Directory Server, le script ne contient pas les fichiers de schéma `defaultDelegationPolicies.xml` et `idRepoDefaults.xml`.

Solution : Chargez manuellement les fichiers `defaultDelegationPolicies.xml` et `idRepoDefaults.xml` à l'aide de la commande `amadmin` dotée de l'option `-t`.

Impossible d'enregistrer des documents XML avec un caractère d'échappement dans Internet Explorer 6.0 (4995100)

Si vous ajoutez un caractère d'échappement (tel que la chaîne `amp;` à côté du caractère &) dans un fichier XML, le fichier est correctement enregistré. Cependant, si par la suite vous récupérez le profil XML via Internet Explorer 6.0, le fichier ne s'affichera pas correctement. Si vous essayez de réenregistrer le profil, une erreur est renvoyée.

Solution : aucune.

Problèmes d'authentification

- "Le jeton SSO `UrlAccessAgent` arrive à expiration (6327691)" à la page 92
- "Impossible de se connecter au sous-domaine avec un profil dynamique/plug-in LDAPV3, après avoir corrigé le mot de passe (6309097)" à la page 92
- "Incompatibilité entre la configuration par défaut du service des statistiques et le mode hérité d'Access Manager (6286628)" à la page 92
- "Principe d'unicité des attributs non appliqué aux attributs de dénomination dans l'organisation de niveau supérieur (6204537)" à la page 93

Le jeton SSO `UrlAccessAgent` arrive à expiration (6327691)

Le jeton SSO `UrlAccessAgent` arrive à expiration, car le module d'application ne renvoie pas le `DN` de l'utilisateur spécial, ce qui entraîne l'échec de la correspondance du `DN` et celui du jeton.

Solution : aucune. Ce problème est résolu dans le patch 1. Pour plus d'informations sur l'application du patch à votre plate-forme spécifique, reportez-vous à la section "Access Manager 7 2005Q4 Patch 1" à la page 63.

Impossible de se connecter au sous-domaine avec un profil dynamique/plug-in LDAPV3, après avoir corrigé le mot de passe (6309097)

En mode Domaine, si vous créez un magasin de données LDAPv3 dans un domaine avec un certain mot de passe et que, par la suite, vous modifiez le mot de passe en tant qu'utilisateur `amadmin` parce qu'il ne vous convient pas, lorsque vous tentez de vous reconnecter avec le compte de l'utilisateur dont vous avez modifié le mot de passe, la connexion échoue, indiquant que ce profil n'existe pas.

Solution : aucune.

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

- “L'installation d'instances Access Manager avec différents fuseaux horaires entraîne l'expiration d'autres sessions utilisateur (6323639)” à la page 93
- “Le script de reprise de session (`amsfoconfig`) comporte des droits incorrects sous un système Linux 2.1 (6298433)” à la page 93
- “Échec du script de reprise de session (`amsfoconfig`) sous Linux 2.1 (6298462)” à la page 94
- “Le système crée un nom d'hôte de service non valide lorsque l'équilibreur de charge dispose d'une terminaison SSL (6245660)” à la page 94
- “Utilisation de `HttpSession` avec des conteneurs Web tiers (pas de numéro CR)” à la page 95

L'installation d'instances Access Manager avec différents fuseaux horaires entraîne l'expiration d'autres sessions utilisateur (6323639)

L'installation d'instances Access Manager avec différents fuseaux horaires et un même cercle de confiance entraîne l'expiration des sessions utilisateur.

Le script de reprise de session (`amsfoconfig`) comporte des droits incorrects sous un système Linux 2.1 (6298433)

Le script de configuration de reprise de session (`/opt/sun/identity/bin/amsfoconfig`) comporte des droits incorrects et ne peut pas être exécuté sous un système Linux 2.1.

Solution : Modifiez les droits de sorte que le script `amsfoconfig` devienne exécutable (par exemple, 755).

Ce problème est résolu dans le patch 1. Pour plus d'informations sur l'application du patch à votre plate-forme spécifique, reportez-vous à la section “Access Manager 7 2005Q4 Patch 1” à la page 63.

Échec du script de reprise de session (`amsfoconfig`) sous Linux 2.1 (6298462)

Le script de configuration de reprise de session (`amsfoconfig`) échoue sur un serveur Linux 2.1, car le caractère de tabulation (`\t`) n'est pas correctement interprété.

Solution : Configurez la reprise de session manuellement. Pour obtenir la procédure, consultez la section "Configuring Session Failover Manually" du *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Ce problème est résolu dans le patch 1. Pour plus d'informations sur l'application du patch à votre plate-forme spécifique, reportez-vous à la section "Access Manager 7 2005Q4 Patch 1" à la page 63.

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"/>
```

Web Server 6.1 SP2 (ou version ultérieure) peut 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 (pas de numéro CR)

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)

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)” à la page 96
- “Utilisation de BEA WebLogic Server comme conteneur Web” à la page 96

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

Lors du démarrage d'Access Manager 7 2005Q4, 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. Vous pouvez ignorer ces messages.

Utilisation de BEA WebLogic Server comme conteneur Web

Si vous déployez Access Manager en utilisant BEA WebLogic Server comme conteneur Web, Access Manager risque de ne pas être accessible.

Solution : Redémarrez WebLogic Server une deuxième fois pour qu'Access Manager devienne accessible.

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 : 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 liés à SAML et aux fédérations

- "L'exécution de l'exemple de services Web renvoie le message Resource offering not found (6359900)" à la page 97
- "Échec de la fédération lors de l'utilisation du profil d'artéfact (6324056)" à la page 97
- "Les caractères spéciaux (&) des instructions SAML doivent être codés (6321128)" à la page 98

- "Une exception se produit lors de la tentative d'ajout du service de découverte à un rôle (6313437)" à la page 98
- "Les attributs de contexte d'authentification ne peuvent pas être configurés tant que les autres attributs n'ont pas été configurés et enregistrés (6301338)" à la page 98
- "L'exemple de profil d'employé ne fonctionne pas si le suffixe racine comporte le caractère & (6300163)" à la page 98
- "Une erreur de déconnexion se produit dans la fédération (6291744)" à la page 98

L'exécution de l'exemple de services Web renvoie le message Resource offering not found (6359900)

Lorsqu'Access Manager est configuré pour accéder aux échantillons de services Web dans le répertoire *AccessManager-base*`/SUNWam/samples/phase2/wsc` sous Solaris ou dans le répertoire *AccessManager-base* `/identity/samples/phase2/wsc` sous Linux, interroger le service de découverte ou modifier l'offre de ressources renvoie le message d'erreur suivant : 'Offre de ressources introuvable'.

AccessManager-base correspond au répertoire d'installation de base. Le répertoire d'installation de base par défaut est `/opt` sous Solaris et `/opt/sun` sous Linux.

Solution :

1. Accédez au répertoire d'exemples suivant : *AccessManager-base* `/SUNWam/samples/phase2/wsc`) sous Solaris ou *AccessManager-base*`/identity/samples/phase2/wsc` sous Linux
2. Dans le fichier `index.jsp`, recherchez la chaîne suivante :

   ```
   com.sun.org.apache.xml.security.utils.XMLUtils.outputDOM
   ```

3. Immédiatement avant la ligne contenant la chaîne trouvée dans l'étape précédente, insérez la nouvelle ligne suivante :

   ```
   com.sun.org.apache.xml.security.Init.init();
   ```

4. Exécutez de nouveau l'exemple. (Il n'est pas nécessaire de redémarrer Access Manager.)

Échec de la fédération lors de l'utilisation du profil d'artéfact (6324056)

Si vous configurez un fournisseur d'identités et un fournisseur de services, que vous modifiez le protocole de communication pour utiliser le profil d'artéfact du navigateur, puis que vous essayez de fédérer les utilisateurs entre les deux fournisseurs, la fédération échoue.

Solution : aucune.

Les caractères spéciaux (&) des instructions SAML doivent être codés (6321128)

Lorsque Access Manager fait office de site source et de site de destination et que la connexion unique est configurée, une erreur se produit dans le site de destination, car le caractère spécial (&) n'est pas codé dans les instructions SAML et par conséquent, l'analyse de l'assertion échoue.

Solution : aucune. Ce problème est résolu dans le patch 1. Pour plus d'informations sur l'application du patch à votre plate-forme spécifique, reportez-vous à la section "Access Manager 7 2005Q4 Patch 1" à la page 63.

Une exception se produit lors de la tentative d'ajout du service de découverte à un rôle (6313437)

Dans la console Access Manager, si vous essayez d'ajouter une offre de ressource au service de découverte, une exception inconnue se produit.

Solution : aucune.

Les attributs de contexte d'authentification ne peuvent pas être configurés tant que les autres attributs n'ont pas été configurés et enregistrés (6301338)

Les attributs de contexte d'authentification ne peuvent pas être configurés tant que les autres attributs n'ont pas été configurés et enregistrés.

Solution : Configurez et enregistrez un profil de fournisseur avant de configurer les attributs de contexte d'authentification.

L'exemple de profil d'employé ne fonctionne pas si le suffixe racine comporte le caractère & (6300163)

Si Directory Server dispose d'un suffixe racine contenant le caractère & et que vous essayez d'ajouter une offre de ressource du service de profil d'employé, une exception est générée.

Solution : aucune.

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)

- "Les préférences d'environnement linguistique de l'utilisateur ne sont pas appliquées à l'ensemble de la console d'administration (6326734)" à la page 99
- "L'aide en ligne n'est pas entièrement disponible pour les langues européennes si Access Manager est déployé sur IBM WebSphere (6325024)" à la page 99
- "Les informations sur la version n'apparaissent pas lorsque Access Manager est déployé sur IBM WebSphere (6319796)" à la page 100
- "La suppression de UTF-8 ne fonctionne pas avec la fonction Détection de client (5028779)" à la page 100
- "Les caractères multioctets sont affichés sous forme de points d'interrogation dans les fichiers journaux (5014120)" à la page 100

Les préférences d'environnement linguistique de l'utilisateur ne sont pas appliquées à l'ensemble de la console d'administration (6326734)

Certaines parties de la console d'administration d'Access Manager ne suivent pas les préférences linguistiques de l'utilisateur, mais utilisent celles définies dans le navigateur. Ce problème concerne les boutons Version et Déconnexion et ceux de l'aide en ligne, ainsi que le contenu auquel ils permettent d'accéder.

Solution : Modifiez les paramètres du navigateur de manière à définir les mêmes paramètres linguistiques que ceux définis dans les préférences de l'utilisateur.

L'aide en ligne n'est pas entièrement disponible pour les langues européennes si Access Manager est déployé sur IBM WebSphere (6325024)

Pour tous les paramètres linguistiques européens (espagnol, allemand et français), l'aide en ligne n'est pas disponible dans son intégralité lorsque Access Manager est déployé sur une instance IBM WebSphere Application Server. L'aide en ligne affiche un message indiquant une erreur d'application dans les cadres suivants :

- le cadre supérieur, là où les boutons Aide et Fermer devraient apparaître ;
- le cadre de gauche, là où les boutons Sommaire, Index et Rechercher devraient apparaître.

Solution : Choisissez l'anglais comme préférence linguistique dans le navigateur, puis actualisez la page pour accéder au cadre de gauche. Le cadre supérieur, cependant, continuera d'indiquer une erreur d'application.

Les informations sur la version n'apparaissent pas lorsque Access Manager est déployé sur IBM WebSphere (6319796)

Quelle que soit la préférence linguistique, si Access Manager est déployé sur une instance IBM WebSphere Application Server, la version du produit n'apparaît pas lorsque vous cliquez sur le bouton Version. Une page vide est affichée.

Solution : aucune.

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 2005Q4 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.

  eur

- 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 suivante : `UTF-8;q=0.5` (veillez à ce que le facteur UTF-8 `q` soit inférieur à celui des autres jeux de caractères de votre environnement linguistique).
  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 utilisent le codage natif et pas toujours UTF-8. Lorsqu'une instance de conteneur Web démarre dans un environnement linguistique donné, les fichiers journaux utilisent le codage natif pour cet environnement. 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 liés à la documentation

- "Access Manager ne peut pas rebasculer en mode Hérité à partir du mode Domaine (6508473)" à la page 101
- "Obtention de davantage d'informations sur la désactivation des recherches persistantes (6486927)" à la page 102
- "Documentation des privilèges d'Access Manager pris et non pris en charge (2143066)" à la page 103
- "Documentation du routage des demandes d'association basé sur des cookies (6476922)" à la page 103
- "Documentation de la configuration de Windows Desktop SSO pour Windows 2003 (6487361)" à la page 104
- "Documentation des étapes de configuration des mots de passe du serveur d'interface utilisateur d'authentification distribuée (6510859)" à la page 105
- "L'aide en ligne sur la création d'un nouveau nom de site demande plus d'informations (2144543)" à la page 106
- "Le paramètre de configuration du mot de passe administrateur est`ADMIN_PASSWD` sous Windows (6470793)" à la page 106
- "Les notes de version ne résolvent pas un problème connu (6422907)" à la page 106
- "Document `com.iplanet.am.session.protectedPropertiesList` dans `AMConfig.properties` (6351192)" à la page 106
- "Documentation de la prise en charge des rôles et des rôles filtrés pour le plug-in LDAPv3 (6365196)" à la page 107
- "Documentation des propriétés non utilisées dans le fichier `AMConfig.properties` (6344530)" à la page 107
- "La propriété `com.iplanet.am.session.client.polling.enable` côté serveur ne doit pas être paramétrée sur true (6320475)" à la page 107
- "L'URL par défaut de connexion réussie est incorrecte dans l'aide en ligne de la console (6296751)" à la page 107
- "Documentation sur la façon d'activer le chiffrement XML (6275563)" à la page 108

Access Manager ne peut pas rebasculer en mode Hérité à partir du mode Domaine (6508473)

Si vous installez Access Manager 7 2005Q4 en mode Domaine, vous ne pouvez pas rebasculer en mode Hérité.

Si vous installez Access Manager 7 2005Q4 en mode Hérité, vous pouvez basculer en mode Domaine à l'aide de la commande `amadmin` associée à l'option `-M`. Exemple :

```
amadmin -u cn=amAdmin,ou=People,dc=example,dc=com -w amadmin-password
-M dc=example,dc=com
```

Obtention de davantage d'informations sur la désactivation des recherches persistantes (6486927)

Access Manager utilise les recherches persistantes pour recevoir des informations sur la modification des entrées de Sun Java System Directory Server. Access Manager crée par défaut les connexions de recherche persistante suivantes pendant le démarrage du serveur :

`aci` - Modifications de l'attribut `aci`, la recherche utilisant le filtre LDAP (`aci=*`)

`sm` - Modifications de l'arborescence d'informations d'Access Manager (ou du nœud de gestion du service) qui comprend les objets appartenant à la classe d'objet marqueur `sunService` ou `sunServiceComponent`. Vous pouvez, par exemple, créer une stratégie visant à définir les privilèges d'accès à une ressource protégée ou modifier les règles, objets, conditions ou fournisseurs de réponse d'une stratégie existante.

`um` - Modifications dans le répertoire utilisateur (ou nœud de gestion des utilisateurs). Vous pouvez, par exemple, modifier le nom ou l'adresse de l'utilisateur.

Attention – Il n'est pas recommandé de désactiver les recherches persistantes de l'un de ces composants. De fait, lorsqu'une recherche persistante d'un composant est désactivée, ce dernier ne reçoit pas de notification de Directory Server. Par conséquent, les modifications apportées dans Directory Server pour ce composant particulier ne seront pas notifiées au cache du composant et le cache du composant sera bloqué.

Par exemple, si vous désactivez les recherches persistantes des modifications dans le répertoire utilisateur (`um`), le serveur Access Manager ne recevra plus les notifications de Directory Server. Par conséquent, un agent ne recevra pas les notifications d'Access Manager l'avertissant de mettre à jour son cache utilisateur local vers les nouvelles valeurs de l'attribut utilisateur. Si ensuite une application demande à l'agent de lui fournir les attributs utilisateur, elle recevra les anciennes valeurs.

N'utilisez cette propriété que dans des circonstances spéciales et lorsque cela est absolument nécessaire. Par exemple, si vous savez que les modifications de la configuration du service (en rapport avec la modification des valeurs de n'importe quel service comme le service de session ou les services d'authentification) ne seront pas mises en œuvre dans l'environnement de production, vous pouvez désactiver la recherche persistante sur le composant Service Management (`sm`). Cependant, en cas de modification d'un service quelconque, vous devrez redémarrer le serveur. La même condition s'applique aux recherches persistantes spécifiées par les valeurs `aci` et `um`.

Pour plus d'informations, consultez la section "CR# 6363157 : la nouvelle propriété désactive les recherches persistantes si cela est absolument nécessaire" à la page 62.

Documentation des privilèges d'Access Manager pris et non pris en charge (2143066)

Les privilèges définissent les droits d'accès dont bénéficient les administrateurs appartenant aux rôles ou groupes existant dans un domaine. Access Manager vous autorise à configurer les autorisations des types d'administrateurs suivants :

- Les administrateurs de domaine peuvent exécuter toutes les tâches liées au domaine, y compris la définition des référentiels d'identité (magasins de données), la configuration de l'authentification et la définition des stratégies.
- Les administrateurs de stratégie peuvent configurer des stratégies dans les domaines existants.

Les privilèges suivants sont pris en charge :

- Accès en lecture et écriture à toutes les propriétés de stratégie et de domaine Définit les privilèges d'accès en lecture et écriture des administrateurs de domaine.
- Accès en lecture et écriture aux propriétés de stratégie uniquement Définit les privilèges d'accès en lecture et écriture des administrateurs de stratégie.
- Combinaison de privilèges pris en charge : Accès en lecture et écriture uniquement pour les propriétés de stratégie et accès en lecture seule aux magasins de données. Les autres combinaisons de privilèges ne sont pas prises en charge.

Documentation du routage des demandes d'association basé sur des cookies (6476922)

Lorsque les serveurs Access Manager sont déployés derrière un équilibreur de charge, le routage des demandes d'association basé sur les cookies empêche une requête cliente d'être acheminée vers un serveur Access Manager incorrect (c'est-à-dire vers un serveur n'hébergeant pas la session). Cette fonctionnalité a été implémentée dans Access Manager 7 2005Q4 patch 3.

Auparavant, en l'absence d'un tel routage, les requêtes des clients non basés sur un navigateur (comme les agents de stratégie et les clients utilisant le SDL client distant d'Access Manager) étaient souvent acheminées vers un serveur Access Manager sur lequel la session n'était pas hébergée. Pour envoyer la requête au serveur approprié, le serveur Access Manager devait alors valider la session au moyen d'une communication par canal retour, ce qui engendrait une dégradation des performances. Le routage des demandes d'association basé sur des cookies permet de ne pas recourir aux communications par canal retour et contribue donc à améliorer les performances d'Access Manager.

Pour mettre en œuvre le routage des demandes d'association basé sur des cookies, le déploiement d'Access Manager doit être configuré comme un site. Pour obtenir plus d'informations, reportez-vous à la section "Configuring an Access Manager Deployment as a Site" du *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Pour configurer le routage des demandes d'association basé sur des cookies :

1. Pour spécifier un nom de cookie, configurez la propriété `com.iplanet.am.lbcookie.name` dans le fichier `AMConfig.properties`. Access Manager génère ensuite le cookie d'équilibreur de charge à l'aide d'un ID de serveur à 2 octets (comme 01, 02 et 03). Si vous ne spécifiez pas de nom de cookie, Access Manager génère la valeur du cookie d'équilibreur de charge à l'aide du nom par défaut `amlbcookie` plus l'ID de serveur à 2 octets.

   Si vous configurez le nom du cookie du serveur Access Manager, utilisez le même nom dans le fichier `AMAgent.properties` de l'agent de stratégie. De même, si vous utilisez le SDK client Access Manager, utilisez également le même nom de cookie que celui utilisé par le serveur Access Manager.

   Remarque : Ne configurez pas la propriété `com.iplanet.am.lbcookie.value` car Access Manager définit la valeur du cookie à l'aide de l'ID de serveur à 2 octets.
2. Configurez l'équilibreur de charge avec le nom de cookie de l'étape 1. Vous pouvez utiliser un équilibreur de charge matériel ou logiciel avec votre déploiement Access Manager.
3. Si un basculement de session est implémenté, activez la propriété `com.sun.identity.session.resetLBCookie` pour l'agent de stratégie et le serveur Access Manager.
   - Pour un agent de stratégie, ajoutez la propriété au fichier `AMAgent.properties` et activez-la.
   - Pour un serveur Access Manager, ajoutez la propriété au fichier `AMConfig.properties` et activez-la.

   Exemple :

   ```
   com.sun.identity.session.resetLBCookie='true'
   ```

   En cas de basculement, la session est acheminée vers un serveur Access Manager secondaire et la valeur du cookie d'équilibreur de charge est configurée sur l'ID de serveur du serveur Access Manager secondaire. Toute requête ultérieure de la session est acheminée vers le serveur Access Manager secondaire.

Documentation de la configuration de Windows Desktop SSO pour Windows 2003 (6487361)

Pour configurer Windows Desktop SSO sous Windows 2003, comme indiqué dans la section "Configuring Windows Desktop SSO" du *Sun Java System Access Manager 7 2005Q4 Administration Guide*, utilisez la commande `ktpass` suivante :

```
ktpass /out filename /mapuser username
/princ HTTP/hostname.domainname /crypto encryptiontype /rndpass
/ptype principaltype /target domainname
```

Exemple :

```
ktpass /out demo.HTTP.keytab
/mapuser http /princ HTTP/demo.identity.sun.com@IDENTITY.SUN.COM
/crypto RC4-HMAC-NT /rndpass /ptype KRB5_NT_PRINCIPAL /target IDENTITY.SUN.COM
```

La syntaxe est décrite sur le site suivant :

`http://technet2.microsoft.com/WindowsServer/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true`

Documentation des étapes de configuration des mots de passe du serveur d'interface utilisateur d'authentification distribuée (6510859)

La procédure suivante décrit comment configurer les mots de passe chiffrés d'un serveur d'interface utilisateur d'authentification distribuée communiquant avec un serveur Access Manager.

Pour configurer les mots de passe d'un serveur d'interface utilisateur d'authentification distribuée :

1. Sur le serveur Access Manager :
   a. Chiffrez le mot de passe `amadmin` à l'aide de l'utilitaire `ampassword -e`. Par exemple, sur les systèmes Solaris :

      ```
      # cd /opt/SUNWam/bin
      # ./ampassword -e amadmin-password
      AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      ```

      Enregistrez la valeur chiffrée.
   b. Copiez et enregistrez la valeur de la propriété `am.encryption.pwd` à partir du fichier `AMConfig.properties` du serveur Access Manager. Exemple :

      ```
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```
2. Sur le serveur d'interface utilisateur d'authentification distribuée, apportez les modifications suivantes au fichier `AMConfig.properties` :
   a. Commentez la propriété `com.iplanet.am.service.password`.
   b. Configurez la propriété `com.iplanet.am.service.secret` sur le mot de passe chiffré `amadmin` à l'étape 1a.
   c. Ajoutez `am.encryption.pwd` et la valeur chiffrée que vous avez copiés à l'étape 1b. Exemple :

      ```
      com.sun.identity.agents.app.username=username
      #com.iplanet.am.service.password=password
      com.iplanet.am.service.secret=AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```
3. Redémarrez le serveur d'interface utilisateur d'authentification distribuée.

L'aide en ligne sur la création d'un nouveau nom de site demande plus d'informations (2144543)

Dans l'aide en ligne d'Access Manager Console, il manque l'état de sauvegarde de la procédure de création d'un nouveau nom de site sous Configuration>Propriétés du système>Plate-forme. Si vous ne cliquez pas sur Enregistrer après avoir ajouté un nouveau nom de site et que vous essayez ensuite d'ajouter un nom d'instance, la procédure échoue. Par conséquent, vous devez toujours cliquer sur Enregistrer après avoir ajouté le nom du site, puis ajouter le nom de l'instance.

Le paramètre de configuration du mot de passe administrateur est`ADMIN_PASSWD` sous Windows (6470793)

Sous Solaris et Linux, le paramètre de configuration du mot de passe (`amadmin`) administrateur d'Access Manager dans le fichier `amsamplesilent` est `ADMINPASSWD`. Sous Windows, le paramètre dans le fichier `AMConfigurator.properties` est `ADMIN_PASSWD` .

Si vous exécutez `amconfig.bat` sous Windows, définissez le mot de passe `amadmin` dans le fichier `AMConfigurator.properties` à l'aide du paramètre `ADMIN_PASSWORD` et non du paramètre `ADMINPASSWD`.

Les notes de version ne résolvent pas un problème connu (6422907)

L'étape 3 de la procédure "L'exécution de l'exemple de services Web renvoie le message Resource offering not found (6359900)" à la page 97 n'est pas corrigée.

Document `com.iplanet.am.session.protectedPropertiesList` dans `AMConfig.properties` (6351192)

Le paramètre `com.iplanet.am.session.protectedPropertiesList` ne vous permet pas de protéger certaines propriétés essentielles ou de session interne contre des mises à jour à distance via la méthode `SetProperty` de Session Service. Le réglage de ce paramètre de sécurité clé " masqué " vous permet de personnaliser des attributs de session en vue d'une autorisation et dans le cadre d'autres fonctionnalités d'Access Manager. Pour utiliser ce paramètre :

1. À l'aide d'un éditeur de texte, ajoutez le paramètre au fichier `AMConfig.properties` .
2. Réglez le paramètre pour les propriétés de session que vous souhaitez protéger. Exemple :

   ```
   com.iplanet.am.session.protectedPropertiesList =
   PropertyName1 , PropertyName2 , PropertyName3
   ```

3. Redémarrez le conteneur Web d'Access Manager pour appliquer les valeurs.

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 CR 6349959). Au niveau de la console d'administration Access Manager 7 2005Q4, 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
```

La propriété `com.iplanet.am.session.client.polling.enable` côté serveur ne doit pas être paramétrée sur true (6320475)

La propriété `com.iplanet.am.session.client.polling.enable` dans le fichier `AMConfig.properties` ne doit jamais être paramétrée sur true côté serveur.

Solution : Par défaut, cette propriété est paramétrée sur false. Elle ne doit jamais être paramétrée sur true.

L'URL par défaut de connexion réussie est incorrecte dans l'aide en ligne de la console (6296751)

L'URL par défaut de connexion réussie est incorrecte dans le fichier `service.scserviceprofile.iplanetamauthservice.html` de l'aide en ligne. Le champ URL par défaut de connexion réussie accepte une liste de valeurs multiples indiquant l'URL vers lequel les utilisateurs sont redirigés à l'issue d'une authentification réussie. Le format de cet attribut est `clientType|URL`, bien que vous puissiez ne spécifier que la valeur de l'URL, qui suppose un type HTML par défaut.

La valeur par défaut `/amconsole` est incorrecte.

Solution : La valeur par défaut appropriée est `/amserver/console`.

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 de JDK antérieure à la version 1.5, téléchargez le fournisseur JCE Bouncy Castle depuis le site Web de 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

- "Collection Sun Java System Access Manager 7 2005Q4" à la page 108
- "Collection Sun Java System Federation Manager 7.0 2005Q4" à la page 109
- "Collection Sun Java System Access Manager Policy Agent 2.2" à la page 109

Collection Sun Java System Access Manager 7 2005Q4

Le tableau suivant répertorie les nouveaux documents et les documents révisés relatifs à Access Manager 7 2005Q4, publiés depuis la version initiale. Pour accéder à ces documents, reportez-vous à la collection Access Manager 7 2005Q4 :

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

TABLEAU 7 Historique des mises à jour de la documentation Access Manager 7 2005Q4

Titre	Date de publication
Notes de version de Sun Java System Access Manager 7 2005Q4	Reportez-vous au Tableau 1.
Sun Java System Access Manager 7 2005Q4 Administration Guide	Février 2006
Sun Java System Access Manager 7 2005Q4 Developers Guide	Février 2006
Sun Java System Access Manager Policy Agent 2.2 User's Guide	Février 2006
Sun Java System Access Manager 7 2005Q4 C API Reference	Février 2006
Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide	Février 2006
Technical Note: Using Access Manager Distributed Authentication	Février 2006
Technical Note: Installing Access Manager to Run as a Non-Root User	Février 2006
Sun Java System SAML v2 Plug-in for Federation Services User's Guide	Février 2006
Sun Java System SAML v2 Plug-in for Federation Services Release Notes	Février 2006
Sun Java System SAMLv2 Plug-in for Federation Services Java API Reference	Février 2006
Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide	Janvier 2006
Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide	Décembre 2005
Sun Java System Access Manager 7 2005Q4 Technical Overview	Décembre 2005

Collection Sun Java System Federation Manager 7.0 2005Q4

Pour accéder aux documents de la collection Federation Manager 7.0 2005Q4, reportez-vous à l'adresse suivante :

http://docs.sun.com/coll/1321.1

Collection Sun Java System Access Manager Policy Agent 2.2

La collection Access Manager Policy Agent 2.2 est révisée de manière continue afin de vous fournir des renseignements sur les nouveaux agents. Pour accéder aux documents de cette collection, reportez-vous à l'adresse suivante :

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

Fichiers redistribuables

Sun Java System Access Manager 7 2005Q4 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.
- En composant le numéro de téléphone indiqué sur votre contrat de maintenance.

Afin de vous aider au mieux à résoudre votre problème, nous vous suggérons de réunir les informations suivantes lorsque vous contactez le support technique de Sun :

- 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.
- la procédure détaillée 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. Ce numéro est constitué de sept ou neuf chiffres et figure sur la page de titre du manuel ou en haut du document. Par exemple, le numéro de référence des notes de version d'Access Manager est 819-2134-22.

Ressources Sun supplémentaires

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

- Documentation 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/`
- Ressources de support : `http://sunsolve.sun.com/`
- Informations pour les développeurs : `http://developers.sun.com/`
- Services de support pour les 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. Des versions mises à jour des applications sont disponibles à l'adresse suivante : `http://sun.com/software/javaenterprisesystem/get.html`.

Pour plus d'informations sur l'engagement de Sun en faveur de l'accessibilité, rendez-vous sur `http://sun.com/access`.

Sites Web complémentaires émanant de tiers

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

Remarque – Sun ne peut être tenu responsable de la disponibilité des sites Web des tiers qui sont mentionnés dans le présent document Sun ne garantit pas le contenu, la publicité, les produits et autres matériaux disponibles sur ces sites ou dans ces ressources, ou accessibles par leur intermédiaire, et ne saurait en être tenu pour responsable. Par ailleurs, la responsabilité de Sun ne saurait être engagée en cas de dommages ou de pertes, réels ou supposés, occasionnés par, ou liés à l'utilisation du contenu, des produits ou des services disponibles sur ces sites ou dans ces ressources, ou accessibles par leur biais, ou encore à la confiance qui a pu leur être accordée.
