Notes de version de Sun Java System Access Manager 7.1 pour Microsoft Windows

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

Référence : 820–1794–10
Février 2007

070528@17466

Table des matières

◆ ◆ ◆ CHAPITRE 1

Notes de version de Sun Java System Access Manager 7.1 pour Microsoft Windows

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

Pour consulter la documentation relative aux produits Java ES, notamment celle d'Access Manager, accédez au site `http://docs.sun.com/prod/entsys.05q4`. Consultez ce site Web avant d'installer et de configurer votre logiciel, puis régulièrement par la suite pour vous procurer la documentation la plus récente concernant le produit.

Les notes de version d'Access Manager 7.1 se composent des sections suivantes :

À propos de Sun Java System Access Manager 7.1

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

- des services d'authentification et d'autorisation centralisés ayant recours à un contrôle d'accès basé sur les rôles et les règles ;

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

Nouveautés de cette version

Cette version propose les nouvelles fonctions suivantes :

Intégration de la structure de contrôle Java ES

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

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

- le nombre de tentatives d'authentifications, le nombre d'authentifications réussies et le nombre d'échecs d'authentification ;
- le nombre de sessions actives et les statistiques issues de la base de données de basculement de session ;
- les statistiques sur la base de données de basculement de session ;
- les statistiques de mise en cache des stratégies ;
- les temps de transaction pour l'évaluation des stratégies ;
- le nombre d'assertions d'un fournisseur donné dans un déploiement SAML/de fédération.

Sécurité des services Web

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

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

Déploiement d'un fichier WAR unique Access Manager

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

Améliorations apportées aux services de base

Conteneurs Web pris en charge

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

Intégration de la structure de contrôle

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

- Authentification
  - Nombre de tentatives d'authentification
  - Nombre de tentatives d'authentifications distantes (facultatif)
  - Nombre d'authentifications réussies
  - Nombre d'échecs d'authentification
  - Nombre d'opérations de déconnexion réussies
  - Nombre d'échecs d'opérations de déconnexion (facultatif)
  - Temps de transaction pour chaque module si possible (à l'état En cours d'exécution et En attente)
  - Échecs de connectivité pour les serveurs d'arrière-plan
- Sessions
  - Taille de la table des sessions (nombre maximal de sessions)

    - Nombre de sessions actives (compteur incrémentiel)
    - Basculement de session, notamment le nombre de sessions stockées, de sessions utilisant un compteur incrémentiel et d'opérations réalisées sur la base de données de basculement, notamment les opérations de lecture, écriture, suppression.
- Gestion des utilisateurs / Référentiel d'identité / Service de gestion de sessions
    - Taille de cache maximale
    - Statistiques relatives au cache telles que nombre d'occurrences, ratio, pointe, taille actuelle, etc.
    - Temps de transaction pour les opérations (à l'état En cours d'exécution et En attente)
- Stratégie
    - Nombre de stratégies en cache
    - Nombre de `policyManagers` en cache
    - Nombre de noms de services dans le cache `policyListeners`
    - Nombre de services dans le `resultsCache`
    - Nombre de `tokenIDs` dans `sessionListernerRegistry`
    - Nombre de noms de services dans `policyListenerRegistry`
    - Nombre de `tokenIDs` dans le cache `role`
    - Nombre de noms de services dans le cache `resourceNames`
    - Nombre d'entrées pour `SubjectEvaluationCache`
    - Nombre de `PolicyEvaluators` en cache
    - Nombre de listeners de modification de stratégie en cache
    - Temps de transaction pour le traitement de l'évaluation de la stratégie
- Fédération
    - Nombre d'artefacts dans le tableau pour un fournisseur donné
    - Nombre d'assertions dans le tableau pour un fournisseur donné
    - Nombre d'entrées de sessions dans un tableau pour un ID de fournisseur donné
- SAML
    - Taille du mappage d'artefact
    - Taille du mappage d'assertion

Module d'authentification

- Il n'est pas nécessaire que le service d'authentification distribuée s'associe à un seul serveur pour les déploiements à charges équilibrées.
- Il n'est pas nécessaire que le service d'authentification s'associe à un serveur pour les déploiements à charges équilibrées.
- Prise en charge de services composites, parmi lesquels le service d'authentification, les agents de stratégie et le service de stratégie. Comprend la condition `AuthenticateToRealm`, la condition AuthenticateToService et la qualification du domaine sur l'ensemble des conditions.
- Conseils sur l'organisation à l'aide de conditions d'authentification sur un domaine qualifié.

- Configurations d'authentification / chaînes d'authentification (`AuthServiceCondition`).
- L'authentification modulaire peut maintenant être désactivée si le chaînage d'authentification est mis en œuvre.
- Le service d'authentification distribuée prend en charge le module d'authentification de certification.
- Ajout de `CertAuth` à l'interface d'authentification distribuée pour en faire une présentation d'extracteur d'informations d'identification complète.
- Le module d'authentification du nouveau magasin de données est un module prêt à l'emploi qui authentifie le magasin de données configuré pour un domaine donné.
- Configuration du verrouillage de compte désormais persistante sur plusieurs instances de serveurs AM.
- Chaînage de classes SPI de post-traitement.

Module de stratégie

- Prise en charge de la définition de stratégie en fonction de l'authentification de service.
- Ajout d'une nouvelle condition de stratégie : AuthenticateToRealmCondition.
- Prise en charge de la comparaison de caractères génériques de premier niveau permettant de faciliter la protection du contenu du répertoire sans protéger le sous-répertoire.
- Prise en charge de la condition de filtre LDAP. L'administrateur de stratégies peut spécifier un filtre LDAP comme condition lors de la définition d'une stratégie.
- Les stratégies peuvent être créées en sous-domaines sans stratégie de référence explicite, à partir d'un domaine parent si la référence de l'alias d'organisation est activée dans la configuration de stratégie globale.
- `AuthLevelCondition` peut spécifier le nom de domaine en plus du niveau d'authentification.
- `AuthSchemeCondition` peut spécifier le nom de domaine en plus de celui du module d'authentification.

Module de gestion des services

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

Access Manager SDK

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

Prise en charge des services Web

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

Module d'installation

- Reconditionnement d'Access Manager sous forme d'application J2EE résultant en un fichier WAR unique pour rendre son déploiement possible sur le Web

Module de délégation

- Prise en charge du groupement de privilèges de délégation

Journalisation

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

Configurations matérielle et logicielle requises

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

TABLEAU 1–1 Configurations matérielle et logicielle requises

Composant	Configuration requise
Système d'exploitation	■ Windows 2000 Advance Server SP4 ■ Windows XP SP2 ■ Windows 2003 Enterprise Server SP1 (32 bits) ■ Windows 2003 Enterprise Server SP1 (64 bits)
Java 2 Standard Edition (J2SE™ platform)	J2SE plate-forme 6.0, 5.0 Mise à jour 7 et 1.4.2 Mise à jour 11
Directory Server	Arborescence d'informations d'Access Manager : Sun Java System Directory Server 5.2 Référentiel d'identités Access Manager : Sun Java System Directory Server 6.0 ou Microsoft Active Directory

TABLEAU 1–1 Configurations matérielle et logicielle requises *(Suite)*

Composant	Configuration requise
Conteneurs Web	Sun Java System Web Server 7.0
	Sun Java System Application Server Enterprise Edition 8.2
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 5.

TABLEAU 1–2 Navigateurs pris en charge

Navigateur	Plate-forme
Firefox 1.0.7	Windows XP
	Windows 2000
Microsoft Internet Explorer™ 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows 2000
Mozilla 1.7.12	Windows XP
	Windows 2000
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000

Informations sur la compatibilité générale

Mode hérité d'Access Manager

Si vous installez Access Manager avec Sun Java System Portal Server, vous devez activer le mode hérité d'Access Manager (6.x) : Pour déterminer le mode dans lequel Access Manager 7.1 a été configuré, reportez-vous à la section "Détection du mode d'Access Manager" à la page 12.

Option Configurer automatiquement lors de l'installation

Si vous exécutez le programme d'installation de Java ES en mode graphique avec l'option Configurer automatiquement lors de l'installation, Access Manager est configuré en mode Hérité (similaire à la version 6.x).

Option Configurer manuellement après l'installation

Si vous avez exécuté le programme d'installation de Java ES avec l'option Configurer manuellement après l'installation, vous devez exécuter le fichier `install-dir\identity\setup\amconfig.bat` pour configurer Access Manager après l'installation. Pour sélectionner le mode Hérité (6.x), définissez le paramètre suivant dans votre fichier de configuration.

```
AM_REALM = disabled

...
install-dir\identity\setup\AMConfigurator.properties
...
```

Détection du mode d'Access Manager

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

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

Si la valeur `true` est renvoyée, cela indique qu'Access Manager 7.1 a été configuré en mode Domaine. Si la valeur `false` est renvoyée, cela indique qu'Access Manager 7.1 a été configuré en mode Hérité.

Agents de stratégie Access Manager

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

TABLEAU 1–3 Compatibilité entre les agents de stratégie et les modes d'Access Manager 7.1

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

Autres problèmes connus et restrictions

Cette section présente les différents problèmes connus au moment de la commercialisation de la version 7.0, ainsi que leurs solutions, le cas échéant.

Problèmes relatifs à l'installation

L'installation d'Access Manager sur 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`. Par 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*.

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.

Problèmes de mise à niveau

- "Portal Server et la console Web ne fonctionnent pas après la mise à niveau de Java ES 4 Access Manager vers Java ES 5 Access Manager (6515054)" à la page 14

Portal Server et la console Web ne fonctionnent pas après la mise à niveau de Java ES 4 Access Manager vers Java ES 5 Access Manager (6515054)

Après la mise à niveau de Java ES 5 Access Manager vers Java ES 5 Access Manager, les applications déployées, Portal Server et la console Web ne fonctionnent pas.

Solution : copiez le fichier `config.properties` depuis l'emplacement d'installation de Java ES 5 vers l'emplacement d'installation de Java ES 4 :

`copy` *install-Dir*`\share\MobileAccess\config\config.properties`
JavaES4–install-dir`\PortalServer\`*https-host-name*`\portal\web-apps\WEB-INF\classes\`

Problèmes de configuration

- "Active Perl 5.8 (ou version ultérieure) doit être installé pour configurer certains modules d'Access Manager" à la page 15
- "Le programme d'installation ne peut pas configurer l'authentification distribuée et les composants du SDK client" à la page 15
- "`am2bak.bat` et `bak2am.bat` Les fichiers ne sont pas générés correctement (6491091)" à la page 15

- "Le compte utilisateur n'est pas désactivé après plusieurs échecs successifs de connexion (6469200)" à la page 15

Active Perl 5.8 (ou version ultérieure) doit être installé pour configurer certains modules d'Access Manager

Active Perl 5.8 (ou version ultérieure) doit être installé pour configurer les composants suivants avec Access Manager :

- MFWK
- Basculement de session
- Fédération en bloc
- Réglage des performances

Vous pouvez télécharger Active Perl à partir de l'URL suivant : `http://www.activestate.com/Products/ActivePerl/`.

Le programme d'installation ne peut pas configurer l'authentification distribuée et les composants du SDK client

Dans l'option Configurer automatiquement lors de l'installation, l'authentification distribuée et les composants du SDK client ne sont pas configurés. Aucun message d'erreur n'est affiché.

Solution : au moment de l'installation, utilisez l'option Configurer manuellement après l'installation puis, une fois l'installation effectuée, configurez manuellement l'authentification distribuée et les composants du SDK client.

`am2bak.bat` et `bak2am.bat` Les fichiers ne sont pas générés correctement (6491091)

Access Manager 7.1 ne prend pas en charge les utilitaires de sauvegarde (`am2bak.bat`) et de restauration (`bak2am.bat`).

Solution : Aucune.

Le compte utilisateur n'est pas désactivé après plusieurs échecs successifs de connexion (6469200)

Le compte utilisateur n'est pas désactivé après plusieurs échecs de connexion à Access Manager.

Solution : utilisez la console d'administration du domaine (`\amserver\console`) pour activer ou désactiver l'utilitaire de verrouillage. Pour définir l'attribut Mode de verrouillage en cas d'échec de connexion, procédez comme suit :

1. Ouvrez l'interface graphique utilisateur d'Access Manager.
2. Sélectionnez un domaine pour activer le verrouillage.

3. Sélectionnez l'onglet Authentification.
4. Cliquez sur le bouton Propriétés avancées.
5. Sélectionnez l'attribut Mode de verrouillage en cas d'échec de connexion.
6. Enregistrez les propriétés en cliquant sur le bouton Enregistrer.

Problèmes liés à la console Access Manager

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

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

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

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

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

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

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

Dans la situation suivante, la console affiche des informations inexactes : Installez Directory Server, puis Access Manager avec l'option d'arborescence d'informations d'annuaire 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 créer le même utilisateur supprimé via le portail (6479611)

Vous ne pouvez pas créer le même profil utilisateur supprimé via le portail. Le message d'erreur suivant s'affiche :

```
An error occurred while storing the user profile.
```

Solution : Aucune.

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.

Les clients SDK doivent être redémarrés 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.

Problèmes de session et de connexion unique

Utilisation de `HttpSession` avec des conteneurs Web tiers

La méthode par défaut de maintenance de sessions pour l'authentification est la session interne et non pas `HttpSession`. La valeur maximale de session non valide par défaut de trois minutes est suffisante. Le script `amtune` définit la valeur sur une minute pour Web Server ou Application

Server. Toutefois, si vous utilisez un conteneur Web tiers (IBM WebSphere ou BEA WebLogic Server) et l'option `HttpSession`, il se peut que vous deviez limiter le temps `HttpSession` maximum du conteneur Web pour éviter les problèmes de performances.

Problèmes liés aux stratégies

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

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 créés à l'étape précédente 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.

Le message d'erreur suivant s'affiche : “Erreur. Tentative de définition d'une propriété dynamique non valide.”Aucune stratégie n'est affichée dans la liste par défaut. Si vous effectuez une recherche, les stratégies s'affichent, mais vous ne pouvez pas modifier ou supprimer les stratégies existantes, ni en créer une autre.

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

Problèmes liés au démarrage du serveur

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

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

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

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

Problèmes liés à SAML et aux fédérations

Échec de la fédération lors de l'utilisation du profil d'artefact (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'artefact du navigateur, puis que vous essayez de fédérer les utilisateurs entre les deux fournisseurs, la fédération échoue.

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, le message d'erreur suivant s'affiche : Erreur : Aucune sous-organisation n'a été trouvée.

Solution : Aucune.

Problèmes liés à la globalisation (g11n)

Erreur d'application affichée dans le panneau de gauche de l'aide en ligne dans la console du domaine (6508103)

Lorsqu'Access Manager est déployé dans Application Server, le panneau de gauche dans l'aide en ligne de la console du domaine affiche une erreur d'application.

Solution : Procédez comme suit :

1. Copiez le fichier `jhall.jar`.

   ```
   copy install-dir\share\lib\jhall.jar %JAVA_HOME%\jre\lib\ext
   ```

2. Redémarrez Application Server.

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

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

Solution :vous avez deux possibilités :

1. Redémarrez le conteneur Web d'Access Manager, après avoir effectué une modification dans la section Détection de client.
2. Suivez la procédure ci-dessous dans la console Access Manager :
   a. Cliquez sur `Détection de client` sous l'onglet `Configuration`.
   b. Cliquez sur le lien `Modifier` correspondant au client `genericHTML`.
   c. Sous l'onglet HTML, cliquez sur le lien `genericHTML`.
   d. Dans la liste des jeux de caractères, entrez la valeur : `UTF-8;q=0.5` (Veillez à ce que le facteur UTF-8 `q` soit inférieur à celui des autres jeux de caractères de vos paramètres linguistiques.)
   e. Cliquez sur Enregistrer.
   f. Déconnectez-vous, puis reconnectez-vous.

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

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

- "Documentation sur la façon d'activer le chiffrement XML (6275563)" à la page 21

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. In , in for

1. Accédez à la console d'administration d'Access Manager 7.1.
2. Sélectionnez la configuration LDAPv3.
3. Dans le champ Types et opérations pris en charge du plug-in LDAPv3, saisissez les valeurs suivantes, en fonction des rôles et rôles filtrés que vous prévoyez d'utiliser dans votre configuration LDAPv3 :

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

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

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

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

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

Pour activer le chiffrement XML, procédez comme suit :

1. (facultatif) Si vous utilisez une version de JDK antérieure à JDK 1.5,
   a. téléchargez le fournisseur JCE Bouncy Castle depuis le site Web Bouncy Castle (`http://www.bouncycastle.org/`).

      Par exemple, pour JDK 1.4, téléchargez le fichier `bcprov-jdk14-131.jar` .
   b. Copiez le fichier dans le répertoire *jdk_root*`\jre\lib\ext`.
2. Téléchargez les fichiers JCE Unlimited Strength Jurisdiction Policy correspondant à votre version de JDK.
   - Pour les systèmes Sun, téléchargez les fichiers à partir du site de Sun (`http://java.sun.com`) correspondant à votre version de JDK.
   - Pour IBM WebSphere, rendez-vous sur le site IBM correspondant pour télécharger les fichiers requis.
3. Copiez les fichiers `US_export_policy.jar` et `local_policy.jar` téléchargés dans le répertoire *jdk_root*`\jre\lib\security`.

4. Si vous utilisez une version de JDK antérieure à JDK 1.5, modifiez le fichier *jdk_root*`\jre\lib\security\java.security` et ajoutez Bouncy Castle en tant que fournisseur. Par exemple :

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

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

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

6. Redémarrez le conteneur Web d'Access Manager.

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

Mises à jour de la documentation

Pour accéder à ces documents, reportez-vous à la collection Access Manager 7.1 : `http://docs.sun.com/coll/1292.1`

La collection Sun Java System Access Manager Policy Agent 2.2 a également été révisée pour documenter de nouveaux agents : `http://docs.sun.com/coll/1322.1`

Fichiers redistribuables

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

Comment signaler des problèmes et apporter des commentaires

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

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

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

- 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 :

- la description du problème, en particulier les situations dans lesquelles il se produit et son impact sur vos opérations ;
- 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 ;
- tous les journaux d'erreur ou core dumps.

Vos commentaires sont les bienvenus

Dans le souci d'améliorer notre documentation, nous vous invitons à nous faire parvenir vos commentaires et vos 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. Dans le cas présent, le numéro de référence des *Access Manager Notes de version* est 819-5686.

Ressources Sun supplémentaires

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

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

Fonctions d'accessibilité destinées aux personnes handicapées

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

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

Sites Web complémentaires émanant de tiers

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

Remarque – Sun décline toute responsabilité quant à la disponibilité des sites tiers mentionnés. 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.