Versionshinweise zu Sun Java™ System Access Manager

Version 6 2005Q1

2. Februar 2005

Teilenummer 819-1943

Diese Versionshinweise enthalten wichtige, zum Zeitpunkt der Veröffentlichung von Sun Java System Access Manager 6 2005Q1 (vormals Sun Java System Identity Server) verfügbare Informationen. In diesem Dokument werden neue Funktionen und Verbesserungen, bekannte Probleme und Einschränkungen und andere Informationen angesprochen, die Sie vor der Installation und Verwendung dieser Version lesen sollten.

Die Versionshinweise werden auf der Sun Java System Documentation-Website unter

`http://docs.sun.com/prod/entsys.05q1` veröffentlicht.

Besuchen Sie diese Website vor der Installation und Konfiguration Ihrer Software und später regelmäßig, um stets die neuesten Versionshinweise und Produktdokumentationen verfügbar zu haben.

In diesen Versionshinweisen werden die folgenden Themen behandelt:

Diese Dokumentation nimmt Bezug auf URLs zu Produkten von Drittanbietern und bietet weitere relevante Informationen.

HINWEIS Sun übernimmt keine Verantwortung für die Verfügbarkeit der in diesem Dokument erwähnten Websites von Drittanbietern. Sun unterstützt keine Inhalte, Werbung, Produkte oder andere Materialien, die auf oder mithilfe von solchen Sites oder Ressourcen erhältlich sind, und übernimmt keine Verantwortung diesbezüglich. Sun ist nicht verantwortlich oder haftbar für tatsächliche oder vermeintliche Schäden oder Verluste, die durch oder in Verbindung mit der Verwendung von über solche Websites oder Ressourcen verfügbaren Inhalten, Waren oder Dienstleistungen bzw. dem Vertrauen darauf entstanden sind.

Änderungsprotokoll der Versionshinweise

Tabelle 1 Änderungsprotokoll

Datum	Beschreibung der Änderungen
2. Februar 2005	Freigabe von Version 2005Q1. Erste Veröffentlichung dieser Versionshinweise.

Über Access Manager 6 2005Q1

Sun Java System Access Manager ist eine Identitätsverwaltungslösung, die für die Anforderungen rasch expandierender Unternehmen entwickelt wurde. Mit Access Manager können Sie Identitäten für Ihre Mitarbeiter, Ihre Partner und Lieferanten in einem einzigen Online-Verzeichnis zusammenstellen. So bietet es die Möglichkeit, Richtlinien aufzustellen und Berechtigungen für den Zugriff der einzelnen Identitäten auf bestimmte Informationen zu erteilen. Access Manager ist der Schlüssel zu all Ihren Daten, Ihren Diensten und die Vergabe der Zugriffsberechtigungen – es ist der Schlüssel zu Ihren gesamten internen und externen Geschäftsbeziehungen.

Neuheiten dieser Version

Access Manager 2005Q1 enthält die folgenden Funktionen. Eine ausführliche Beschreibung dieser Funktionen finden Sie im *Sun Java System Access Manager Technical Overview*.

- Der Produktname wurde von Identity Server in Access Manager geändert
- Unterstützung für Solaris 10
- Unterstützung für neuen Webcontainer: Sun Java System Application Server Enterprise Edition 8 2005Q1 (8.1)
- Neue bzw. überarbeitete Authentifizierungsmodule:
  - Java Database Connectivity (JDBC)
  - Mobile Station ISDN (MSISDN)
  - Active Directory
  - Security Assertion Markup Language (SAML): Die Unterstützung für die SAML-Authentifizierung wird in einem Authentifizierungsmodul bereitgestellt, über das die SAML-Authentifizierung in den Authentifizierungsprozess integriert ist.
- Sitzungs-Failover
  - Zwei oder mehr Access Manager 6 2005Q1-Instanzen, die jeweils auf einem unterstützten Webcontainer auf einem anderen Hostserver laufen.
  - Message Queue-Broker-Cluster, das die Sitzungsnachrichten zwischen den Access Manager-Instanzen und der Sitzungsspeicher-Datenbank verwaltet.
  - Berkeley DB von Sleepycat Software, Inc., (http://www.sleepycat.com/) als Sitzungsspeicher-Datenbank. Der Berkeley DB-Clientdämon ist „amsessiondb“.
- Die Richtlinienverwaltung enthält ein neues Ressourcennamen-Plugin: `HttpURLResourceName`.
- Verbesserungen der Konsole:
  - Möglichkeit, die Ansicht jedes Objekttyps im Navigationsfenster anzupassen (die angezeigten Objektattribute können ausgewählt werden).
  - Möglichkeit, dem Dropdown-Menü des Navigationsfensters neue Objekttypen hinzuzufügen (z. B. neue Einträge für Drucker oder Gebäude)

- Client-SDK:
  - Neu zusammengestelltes SDK (Komponenten für Authentifizierung, Dienstverwaltung, Benutzerverwaltung, SAML, Richtlinienclient und Sitzungen). Damit lässt sich Access Manager besser in die Java-Anwendungsentwicklung integrieren.
  - Keine Abhängigkeit mehr von der Datei `serverconfig.xml` und reduzierter Footprint der jar-Dateien.
- Verbindungsverwaltung:
  - Unterstützung des Liberty Alliance Project (LAP) Name Identifier Mapping Protocol
  - Unterstützung der LAP Identity Web Services Framework (ID-WSF) Discovery Service Specification, Version 1.1
  - Unterstützung der LAP ID-WSF Authentication Service Specification
  - Unterstützung der LAP Metadata Description and Discovery Specification
  - Unterstützung der erweiterten Profile des LAP Liberty Identity Federation Framework (ID-FF):
    - Dynamic Identity Provider Proxying (Dynamische Provideridentitäts-Proxyabfragen)
    - Affiliation Federation (Partnerverbindung)
    - One-time Federation (Einmalige Verbindung)
    - Name Identifier Mapping Profile (Zuordnungsprofil für Namensbezeichner)
    - Name Identifier Encryption Profile (Verschlüsselungsprofil für Namensbezeichner)
- Ein Leistungsoptimierungsskript zur Optimierung von Application Server Enterprise Edition 8 2005Q1 (8.1) als Webcontainer

Hardware- und Softwareanforderungen

Für diese Version von Access Manager müssen die folgenden Hardware- und Softwareanforderungen erfüllt sein.

Tabelle 2 Hardware- und Softwareanforderungen

Komponente	Anforderung
Betriebssystem	Solaris™ Operating System (OS), SPARC® Platform Edition, Version 8, 9 und 10
	Solaris™ OS, x86 Platform Edition, Version 9 und 10
	Red Hat™ Linux, Advanced Server 2.1 Update 2
	Red Hat™ Linux, Advanced Server 3.0 Update 1, Update 2 und Update 3
	Red Hat™ Linux, Advanced Server 3.0 Update 2 für AMD64
RAM	512 MB
Festplattenspeicher	250 MB für Access Manager und zugehörige Anwendungen

Unterstützte Browser

Diese Version von Access Manager unterstützt die folgenden Browser:

Browser	Plattformen
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000, Sun Linux, Red Hat™ Linux 8.0
Microsoft Internet Explorer 6.0	Windows 2000, Windows™ XP, Sun Linux, Red Hat Linux 8.0
Mozilla 1.7.1	Windows 2000, Sun Linux, Red Hat Linux 8.0, Solaris™ 9 und 10, Solaris™ OS x86 Platform Edition Version 9 und 10
Netscape™ 4.79	Windows NT, Solaris 8 und 9
Netscape™ 6.2.1	Windows NT, Windows 98, Sun Linux, Red Hat™ Linux Advanced Server 2.1, Solaris™ OS x86 Platform Edition Version 9 und 10
Netscape™ 7.0	Windows 2000, Sun Linux, Red Hat Linux 8.0, Solaris 9 und 10, Solaris™ OS x86 Platform Edition Version 9 und 10

Behobene Fehler in dieser Version

In der nachfolgenden Tabelle werden die in Access Manager 2005Q1 behobenen Probleme beschrieben:

Tabelle 3 In Access Manager 2005Q1 behobene Fehler

Fehlernummer	Beschreibung
5050332	Auf Linux-Systemen wird durch Anhalten von „amserver“ der amunixd-Prozess nicht angehalten
5049218	Fehler in der Konsole beim Suchen nach Benutzern, wenn die Benutzerverwaltung deaktiviert ist
5048378	Falsche SMTP-Serveranschlusseigenschaft in „AMConfig.properties“
5043752	Fehler beim Ausführen von „am2bak“
5042100	Der Richtlinien-Admin kann sein eigenes Profil nicht ändern
5041529	BasicEntitySearch-Filter für „uid“ ist hartkodiert
5038600	Benutzer können nicht mit dem SAML-Dienst erstellt werden
5037978	Beim Erstellen von Rollen mit definierten Zugriffsberechtigungen als Org-Admin wird ein Fehler gemeldet
5026635	Konsolenbeispiele werden nicht kompiliert
5016725	Änderungen an der Bezugsrichtlinienregel werden nicht in die Unterorganisation übernommen
5013994	Die Anmeldung auf Authentifizierungsebene schlägt in japanischen Browsern fehl
5008960	„amadmin“ gibt eine falsche Fehlermeldung zurück
4996479	Dienste mit einem Richtlinienschema werden einem Benutzer als „hinzufügbar“ angezeigt
4961370	„**“-Suchmaske funktioniert nicht
4959895	Der Suchfilter für Entity-Deskriptoren funktioniert nicht ordnungsgemäß
4959071	Im Leerlauf befindliche Sitzungen werden nicht bereinigt
4931907	Dienste verschwinden bei Anmeldung eines Benutzers der Diensttyp-Rolle
4931163	Benennungsattribute müssen in Kleinbuchstaben angegeben werden
4930610	„am2bak-“ und „bak2am“-Versionsmeldungen nur in Englisch
4922030	Konfliktlösungsebene bei festgelegter Ländereinstellung
4916683	Meldung für msgid-msgstr-Paare in „backup_restore.po“ nicht lokalisiert
4853809	Problem bei Dienstregistrierung
4853809	Bei der Registrierung aller Dienste werden eventuell nicht alle verfügbaren Dienste registriert

Installationshinweise

Das Skript `amconfig` unterstützt nun die Bereitstellung weiterer Access Manager-Instanzen mit Application Server Enterprise Edition 8 2005Q1 (8.1) als Webcontainer, nachdem die erste Instanz mit dem Java Enterprise System-Installationsprogramm installiert wurde.

Informationen zur Ausführung der Konfigurationsskripts finden Sie im *Access Manager 6 2005Q1 Administration Guide*.

Lesen Sie auch den Abschnitt Installation unter Bekannte Probleme und Einschränkungen.

Bekannte Probleme und Einschränkungen

In diesem Abschnitt werden die wichtigsten Probleme beschrieben, die zum Zeitpunkt der Freigabe von Access Manager 2005Q1 bekannt waren. In diesem Abschnitt werden folgende Themen behandelt:

- Installation
- Authentifizierung
- Access Manager-Beispiele
- Befehlszeilen-Tools
- Konfiguration
- Access Manager-Konsole
- Verbindung
- Protokolldienst
- Richtlinie
- Single Sign-On
- Access Manager-SDK
- Internationalisierung (i18n)
- Cookies
- Cookie-Raub

Installation

„amadmin“ auf SDK-Installationen mit sicherem Server meldet Ausnahmefehler (5107584)

Wenn Sie in Access Manager 2005Q1 eine vollständige Installation eines sicheren Access Manager und danach eine SDK-Installation installieren, um die vollständige Installation zu nutzen, können Ausnahmefehler gemeldet werden. Dies liegt an einer falschen Einstellung der Eigenschaft `com.iplanet.am.admin.sli.cerdb.prefix` für Web Server.

Umgehung

1. Bearbeiten Sie `AMConfig.properties`.
2. Ändern Sie die Eigenschaft `com.iplanet.am.admin.cli.certdb.prefix` in `https-<ws-instanz-name>-<ws-hostname>-`.
3. Starten Sie den Web Server neu.

AMSDK-Installation mit Webcontainern enthält beschädigte Links zu gemeinsam genutzten Linux-Komponenten (6199933)

Wenn Sie das Access Manager-SDK für Webcontainer auf der Plattform Linux installieren, werden mehrere Links zu gemeinsam genutzten Komponenten beschädigt.

Umgehung

Entfernen Sie die beschädigten Links und erstellen Sie die richtigen Links.

So entfernen Sie die Links:

```
cd ${AM_INSTALL_DIR}/identity/lib

rm -rf jaxrpc-spi.jar relaxngDatatype.jar xsdlib.jar
```

So erstellen Sie die neuen Links:

```
ln -s /opt/sun/private/share/lib/jaxrpc-spi.jar

ln -s /opt/sun/private/share/lib/relaxngDatatype.jar

ln -s /opt/sun/private/share/lib/xsdlib.jar
```

Tippfehler in einem Argument des Plugins für die referenzielle Integrität beeinträchtigt die Leistung (5029256)

Wenn Access Manager das Plugin für die referenzielle Integrität für Directory Server aktiviert, enthält Argument 11 des Plugins einen Attributnamen mit einem Tippfehler. Der Attributname wird als `iplanet-am-modifable-by` eingegeben. Aufgrund dieses Fehlers wird im Fehlerprotokoll des Verzeichnisses die Warnung `search not indexed` eingetragen, sobald eine Organisation gelöscht wird.

Alle Attribute, die in den Argumenten des Plugins für die referenzielle Integrität erwähnt werden, müssen indiziert sein. Der korrekt geschriebene Name des indizierten Attributs lautet `iplanet-am-modifiable-by`. Der Tippfehler kann sich auf die Leistung von Access Manager auswirken.

Die Datei „xercesImpl.jar“ von Application Server bewirkt, dass der Vorgang „To JVM“ abstürzt (6223676)

Die Datei `xercesImpl.jar` von Application Server 8.1 EE aus dem Verzeichnis `/opt/sun/appserver/lib` (für RedHat Linux) bzw. aus dem Verzeichnis `/opt/SUNWappserver/appserver/lib` (für Solaris) wird geladen, bevor die gemeinsam genutzte Komponentenversion von `xercesImpl.jar` aus `/opt/sun/share/lib` (für RedHat Linux) bzw. `usr/share/lib` (für Solaris) geladen wird.

Die Application Server-Version wird vom Klassenladeprogramm vor der gemeinsam genutzten Komponentenversion geladen. Die veraltete Version des Application Server kann aber nicht die tausende anstehenden JSPs verarbeiten. Der JVM bleibt entweder hängen oder er stürzt ab.

Umgehung

Benennen Sie die Datei `xercesImpl.jar` in `opt/sun/appserver/lib` (für Red Hat AS 2.1 oder 3.0) bzw. in `/opt/SUNWappserver/appserve/lib` (für Solaris 9 oder 10 sowohl auf SPARC- als auch auf x86-Plattformen) um. Das JVM-Klassenladeprogramm ist dann gezwungen, die Datei `xerceImpl.jar` der gemeinsam genutzten Komponenten aus dem Verzeichnis `/opt/sun/share/lib` (für Red Hat AS 2.1 oder 3.0) oder `/usr/share/lib` (für Solaris 9 oder 10) zu verwenden.

Das Installationsprogramm fragt den Benutzer während der Access Manager-SDK-Installation nicht nach dem Protokoll (6180090)

Bei der Installation des Access Manager-SDK wird der Benutzer im Fenster `Access Manager: Webcontainer zum Ausführen der Sun Java System Access Manager-Dienste` nicht nach dem Protokoll des Webcontainers gefragt, auf dem die Access Manager-Dienste ausgeführt werden. Das Installationsprogramm geht vielmehr davon aus, dass der Webcontainer das `http`-Protokoll verwendet. Für eine SDK-Installation, die eine SSL-aktivierte Access Manager-Installation verwendet, ist jedoch das `https`-Protokoll erforderlich.

Umgehung

Stellen Sie das Protokoll für eine Access Manager-Serverinstallation in der Datei `AMConfig.properties` auf `https` ein. Zum Beispiel:

```
com.iplanet.am.server.protocol=https
com.iplanet.am.console.protocol=https
```

Access Manager fügt dem CLASSPATH des Servers die Datei „servlet.jar“ hinzu (5016348)

Access Manager fügt in den Server-CLASSPATH seiner unterstützten Webcontainer die Datei `servlet.jar` ein. Diese Datei kann zu unerwünschten Ergebnissen führen, da jeder Webcontainer in seiner Implementierung eine `servlet.jar`-Datei bündelt.

Umgehung

Entfernen Sie die Datei `servlet.jar` aus dem CLASSPATH.

Access Manager-Beispiele

Bei der Kompilierung mit JDK 1.5 geben Beispiele Warnungen zurück (5102149)

Die in Access Manager enthaltenen Beispiele geben Warnungen zurück, wenn sie mit JDK 1.5 kompiliert werden.

Umgehung

Verhindern Sie die Ausgabe der Warnungen. Gehen Sie dazu wie folgt vor:

- Wenn Sie JDK 1.5 verwenden, fügen Sie der Kompilierungsbefehlszeile den Parameter `encoding="ISO-8859-1"` hinzu.

  Oder

- Verwenden Sie JDK 1.4 zur Kompilierung der Beispiele.

Auslassungen in den xmlsig-Beispielen für SAML führen zu Kompilierungsfehlern (5090925)

Auslassungen in den `xmlsig`-Beispielen für SAML führen bei der Kompilierung mit JDK 1.5 zu Kompilierungsfehlern. Bei der Kompilierung mit JDK 1.4.2 tritt dieses Problem nicht auf.

Umgehung

Wenn Sie JDK 1.5 zur Kompilierung verwenden, führen Sie die folgenden Schritte aus, um den LD_LIBRARY_PATH einzurichten:

1. Suchen Sie die Datei `Readme.html` oder `Readme.txt` der SAML-Beispiele im Verzeichnis `xmlsig`.
2. Befolgen Sie die Anleitungen in Abschnitt 3 „Instructions to set up the XMLSIG sample on Solaris“. In Schritt 4 geben Sie als LD_LIBRARY_PATH unter *web-server-install-directory* das Verzeichnis `/bin/https/lib` ein.
3. Fügen Sie dem LD_LIBRARY_PATH das Verzeichnis `/usr/lib/mps/secv1` hinzu, um auch die JSS-Bibliothek und ihre Abhängigkeiten zu erfassen.

Authentifizierung

E-Mail-Benachrichtigung über Benutzermodifizierung funktioniert nicht (6212964)

Der im Administrationsdienst integrierte Mechanismus zur E-Mail-Benachrichtigung über Benutzermodifizierungen funktioniert zurzeit nicht.

SafeWord-Verbindungen werden nicht getrennt (5073718)

Wenn Sie versuchen, sich bei Access Manager anzumelden, dabei zur Seite `Challenge/Response` von SafeWord gehen und kein Passwort eingeben, kommt es zu keiner Zeitüberschreitung. Wenn Sie anschließend den Browser schließen, wird die Verbindung mit dem SafeWord-Server nicht getrennt.

LDAP-Authentifizierung nimmt eine anonyme Bindung für die LDAP Directory Server-Verbindung vor (5090018)

Access Manager leitet den BIND-DN und das Passwort bei einer LDAP-Verbindung nicht an Directory Server weiter. Dies beeinträchtigt die Authentifizierung, wenn die anonyme Bindung auf dem LDAP Directory Server deaktiviert wird.

Umgehung

Aktivieren Sie die anonyme Bindung für Directory Server.

Eine Eigenschaft von „Modus für persistentes Cookie“ ist inkonsistent (5038544)

Im Modus für persistentes Cookie ist die im Token festgelegte UserID-Eigenschaft inkonsistent. Dadurch kann der Richtlinienagent fehlschlagen, der von der UserID-Eigenschaft abhängig ist.

Umgehung

Verwenden Sie `UserToken` für einen Nicht-DN-Wert und `Principal` für den DN-Wert.

Beim erneuten Laden der Zeitüberschreitungsseite wird der Benutzer mit einem gültigen Benutzernamen und Passwort authentifiziert (4697120)

Wenn ein Benutzer, der sich auf der Anmeldeseite befindet, wartet, bis die Seite eine Zeitüberschreitung erfährt, und dann einen gültigen Benutzernamen und ein Passwort eingibt, wird die Sitzungszeitüberschreitungsseite angezeigt. Der Benutzer wird für Access Manager authentifiziert, wenn er die Seite erneut lädt, ohne den Benutzernamen und das Passwort wieder eingeben zu müssen.

Verschiedene Verzeichnisse müssen für mehrere SafeWord-Server angegeben werden (4756295)

In einer Konfiguration, bei der mehrere Organisationen ihre eigenen SafeWord-Server verwenden, müssen diese ihre eigenen `.../serverVerification`-Verzeichnisse in ihren Dienstvorlagen für die SafeWord-Authentifizierung angeben. Falls Sie den Standardwert nicht ändern und alle Server dasselbe Verzeichnis verwenden, funktioniert nur die Organisation, die als erste mit ihrem SafeWord-Server authentifiziert wird.

Befehlszeilen-Tools

Die Dienstprogramme „ldapsearch“ und „ldapmodify“ aus dem Verzeichnis „/opt/SUNWam/bin“ funktionieren nicht einwandfrei (4954779)

Die Dienstprogramme `ldapsearch` und `ldapmodify` aus dem Verzeichnis `/opt/SUNWam/bin` geben schwerwiegende Fehler zurück.

Umgehung

Fügen Sie der Umgebungsvariablen LD_LIBRARY_PATH den Pfad *DirectoryServer-Basis*`/lib/` hinzu.

Die Skripts „am2bak“ und „bak2am“ funktionieren nicht unter Linux (5053866)

Die Wiederherstellungsskripts `am2bak` und `bak2am` funktionieren nicht, wenn Access Manager auf einem Linux-System läuft.

Umgehung

1. Korrigieren Sie den Pfad der folgenden Befehle:
   - `ECHO=/usr/bin/echo` muss in `ECHO=/bin/echo` geändert werden.
   - `uid='/usr/xpg4/bin/id -un'` muss in `uid='/usr/bin/id -un'` geändert werden.
   - `/usr/bin/tar` muss in `/bin/tar` geändert werden.
   - `/usr/bin/rm` muss in `/bin/rm` geändert werden.
   - `/usr/bin/grep` muss in `/bin/grep` geändert werden.
   - `/usr/bin/ps` muss in `/bin/ps` geändert werden.
   - `/usr/bin/ls` muss in `/bin/ls` geändert werden.

2. Ändern Sie die Funktion `check_for_invalid_chars()`. Zum Beispiel:

```
check_for_invalid_chars() {
echo "$1" | grep '[^/_.a-zA-Z0-9a-]' > /dev/null
if [ $? = 0 ]; then
return 1
else
return 0
fi
}
```

„amadmin“ gibt eine falsche Fehlermeldung aus (5008960)

Die Option `import` von `amadmin` gibt fälschlicherweise für alle Fehler dieselbe Fehlermeldung aus.

„amverifyarchive“ verfügt in Nur-Konsolen-Installationen über nicht ausgelagerte Tags (4993375)

Wenn Sie eine Nur-Konsolen-Installation von Access Manager durchführen, werden die folgenden Tags des Dienstprogramms `amverifyarchive` in diesem Skript nicht ausgelagert: JSSHOME, JDK_HOME, BASEDIR und PRODUCT_DIR.

Konfiguration

WebSphere Application Server 5.1 lässt sich nach erfolgreicher Konfiguration nicht unter Linux starten (6204646)

Wenn Sie die Access Manager-SDK-Komponente für WebSphere unter Linux installieren und danach `amwas51config` mit der richtigen `amsamplesilent`-Datei ausführen, startet WebSphere nicht.

Umgehung

Fügen Sie `LD_LIBRARY_PATH` das Verzeichnis `/opt/sun/private/lib` wie folgt hinzu:

```
LD_LIBRARY_PATH="$WAS_LIBPATH":$LD_LIBRARY_PATH:/opt/sun/private/lib

export LD_LIBRARY_PATH ;;
```

Entfernen Sie in der Datei `server.xml` die Zeichen „**/:**“ vor dem Eintrag `the -Djava.util.logging.config.class`.

Das certdb-Alias ist nicht richtig für Web Server eingestellt (6212532)

Wenn Sie SSL für Web Server mit Access Manager aktivieren und danach `amadmin` ausführen, wird der Fehler „namingservice not available“ zurückgegeben. Im Browser funktioniert das Dienstprogramm wie erwartet.

Für userRoot werden unabhängig vom Back-End-Namen immer Indizes erstellt (5002886)

`index.ldif` nimmt zur Erstellung eines Index für die Attribute eine Hartkodierung für userRoot vor. Daher kann Access Manager in einem Root-Suffix installiert werden, das sich in einem beliebigen Back-End-Datenbanknamen befinden kann. Der Back-End-Name kann durch `ldapsearch` mit der Basis `cn=config` unter Verwendung von `nsslapd-suffix=SUFFIX_NAME` als Filter abgerufen werden.

Verbindung

Die Kontaktperson der Verbindungsverwaltung meldet einen Ausnahmefehler (6213102)

Wenn Sie einen neuen Anbieter erstellen und diesem eine neue Kontaktperson hinzufügen, erhalten Sie unter Umständen den folgenden Fehler:

```
Der Server ist auf einen internen Fehler gestoßen (), aufgrund dessen er diese Anforderung
nicht erfüllen konnte.
```

Die Remote-Protokollierung funktioniert für amFederation.access-Protokolle nicht (6197608)

Wenn die Remote-Protokollierung konfiguriert ist, werden alle Protokolle mit Ausnahme von `amFederation.access` korrekt auf der Remote-Instanz von Access Manager aufgezeichnet. Nur dieser Protokolleintrag wird nicht aufgezeichnet.

Umgehung

Verwenden Sie in `LogUtils` die Option `AccessController.doPrivileged(AdminTokenAction.getInstance());`.

Der fedCookie-Status ändert sich nicht (6202574)

Wenn Sie unter SP und IDP eine Verbindungstrennung für föderierte Benutzer durchführen, wird als `fedCookie`-Status nach wie vor `YES` angezeigt. Der Status sollte aber `NO` lauten.

Persönliche Profilcontainer generieren bei einer Abfrage oder Änderung einen Fehler (6189808)

Die folgenden persönlichen Profilcontainer generieren bei einer Abfrage oder Änderung einen Fehler:

```
LegalIdentity/Geschlecht

EmploymentIdentity/AltO
```

Wenn der Attributwert leer ist, wird für „PP Modify“ ein Ausnahmefehler gemeldet (5047103)

Access Manager meldet einen Ausnahmefehler, wenn Sie `PP Modify` mit einem leeren Attributwert durchführen. Wenn Sie beispielsweise eine Einrichtung zum Testen des Beispiels `sis-ep` vornehmen und dann die EP Modify-Seite senden und auf die Schaltfläche klicken, ohne einen Wert für das Attribut einzugeben, wird fälschlicherweise ein Ausnahmefehler gemeldet.

Richtlinie wird erst bei Neustart des Servers wirksam (5045036)

Die Implementierung von Verbindungsrichtlinien erfolgt erst beim Neustart des Servers. Dies gilt sowohl für Application Server als auch für Web Server. Sie müssen den Server nur nach einer neuen Installation und zur erstmaligen Implementierung der Richtlinie neu starten.

Access Manager-Konsole

Bei sehr vielen Personen-Containern im DIT können keine neuen Benutzer erstellt werden (5079609)

Wenn Sie sehr viele Personen-Container (mehr als Tausend) erstellen und sich danach bei der Access Manager-Konsole anmelden und dort versuchen, einen neuen Benutzer zu erstellen, wird der Benutzer nicht erstellt, weil keine Personen-Container gefunden werden.

`UMCreateUserModelImpl.getPeopleContainers()` meldet während der Suche Zeitüberschreitungsfehler. Obwohl der Directory Server vor Erreichen des Zeitlimits zahlreiche Personen-Container findet, werden diese nicht an die Konsole übertragen.

Umgehung

Aktivieren Sie auf der Access Manager-Konsole die Option `Personen-Container anzeigen`, öffnen Sie den gewünschten Personen-Container und erstellen Sie die Benutzer dort.

Top-Level-Help-Desk-Admin-Rolle mit Nur-Lese-Zugriff kann neue Benutzer erstellen (5109348)

Zurzeit ist die Standardeinstellung für die Help-Desk-Admin-Rolle `Vollständiger Zugriff`. Wenn Sie die Zugriffsrechte auf `Ändern` einstellen, werden zwar die Schaltflächen `Neu` und `Löschen` im Navigationsbereich deaktiviert, der Administrator kann aber dennoch die Benutzereintragseigenschaften ändern.

Umgehung

Öffnen Sie die Eigenschaftenseite des Help-Desk-Administrators und zeigen Sie die verfügbaren Aktionen an. Suchen Sie die Benutzerzeile und stellen Sie dort statt `Vollständiger Zugriff` die Berechtigung `Ändern` ein.

Bei Auswahl der Ansicht „Partner“ auf der Seite „Partner-Entity“ wird ein Ausnahmefehler gemeldet (6203563)

Das Verbindungsverwaltungsmodul meldet einen Ausnahmefehler, wenn Sie auf der Seite `Partner-Entity` die Ansicht `Partner` auswählen.

Umgehung

Ändern Sie die JSP-Datei so, dass sich das Attribut `Height` außerhalb des schließenden JATO-Tags befindet. Ändern Sie dazu die Zeile 104 der Datei `FSAffiliateProfile.jsp` wie folgt:

```
<td width="1%"><img src="<%consoleImages%>/spacer.gif" width=<jato:text
name="defaultAttrNameWidth" /> height="1" alt=""></td>
```

Das Zeichen `/>` muss sich vor dem Attribut `Height` befinden.

Fehler in Partneranzeige-Option (6194139)

Access Manager gibt eine Fehlerseite zurück, wenn die Partneranzeige-Option im Verbindungsverwaltungsmodul die einzige Option im Menü ist und als Standardeinstellung festgelegt ist.

Personen-Admin-Rolle kann keine Dienste für Benutzer ändern (6174652)

Wenn Sie als Top-Level-Personen-Admin-Rolle angemeldet sind, können Sie für Benutzer zwar neue Dienste hinzufügen, die Dienste aber nicht ändern.

Umgehung

Fügen Sie dem Anzeigeprofil der Personen-Admin-Rolle die erforderlichen Ansichtmenüs und verfügbaren Aktionen hinzu.

Beim Klicken auf die Schaltfläche „Zurück“ bleiben die Werte nicht erhalten (4992972)

Wenn ein Vorgang, beispielsweise das Erstellen einer Gruppe oder Rolle oder das Hinzufügen einer Bedingung zu einer Richtlinie, mehrere Seiten umfasst und Sie auf die Schaltfläche `Zurück` klicken, werden die Werte der vorhergehenden Seite nicht wiederhergestellt.

Aktualisierungsproblem für Host-Anbieter im Verbindungsverwaltungsmodul (4915894)

Wenn Sie im Verbindungsverwaltungsmodul in der Ansicht `Identity-Anbieter` eines Host-Anbieters Attribute ändern und speichern, werden die Änderungen gespeichert, aber nicht automatisch in der Anzeige aktualisiert.

Umgehung

Beenden Sie das Verbindungsverwaltungsmodul, indem Sie ein anderes Modul auswählen (z. B. das Dienstkonfigurationsmodul), und kehren Sie anschließend zum Verbindungsverwaltungsmodul zurück. Durch diesen Vorgang wird die Anzeige aktualisiert.

Die Konsole wird bei Änderungen der Benutzerattribute nicht aktualisiert (4931455)

Der Navigationsbereich der Access Manager-Konsole wird nicht aktualisiert, um Änderungen an den Benutzerattributwerten anzuzeigen, die im Datenbereich vorgenommen wurden. Aktualisieren Sie die Seite manuell, um die geänderten Werte anzuzeigen.

Anschlussprobleme mit Internet Explorer (4864133)

Aufgrund einer Inkompatibilität mit Internet Explorer sollten Sie Anschluss 80 nicht als Access Manager-Anschlussnummer beim Ausführen von http bzw. Anschluss 443 beim Ausführen von https verwenden.

Protokolldienst

Protokollierungsproblem bei aktivierter Java-Sicherheit (4926520)

`jdk_logging.jar` funktioniert möglicherweise nicht, wenn die Java-Sicherheit aktiviert ist.

Umgehung

Wenn die Java-Sicherheit aktiviert ist und Sie über eine frühere JDK-Version als 1.4 verfügen, sollten Sie folgende Berechtigung in die Java-Sicherheitsdatei einschließen:

```
permission java.lang.RuntimePermission shutdownHooks
```

Richtlinie

Es werden keine übereinstimmenden Einträge ausgegeben, wenn die nslookthrough-Begrenzung erreicht ist (5013538)

In der Access Manager-Konsole werden keine übereinstimmenden Einträge ausgegeben, selbst wenn die in `nslookthrough` definierten Admin-Begrenzungen erreicht sind.

Umgehung

Optimieren Sie den Parameter `nslookthroughlimit`, um die entsprechende Anzahl von Einträgen zu kompensieren.

Die Richtlinie für Alias-Tokens wurde nicht durchgesetzt (4985823)

Wenn Sie einen Benutzer-Alias verwenden, um sich über ein anderes Autorisierungsmodul als LDAP oder Membership bei Access Manager anzumelden, und dann versuchen, auf eine geschützte Ressource zuzugreifen, wird der Zugriff verweigert.

Problem mit Richtlinienbeispiel (4923898)

In der Datei `Readme.html`, die im Richtlinienbeispiel enthalten ist, fehlen Informationen, wodurch das Beispiel nicht ausgeführt werden kann.

Umgehung

Um das Beispiel ausführen zu können, muss die Umgebungsvariable `LD_LIBRARY_PATH` den Pfad zu den gemeinsam genutzten Bibliotheken `NSPR`, `NSS` und `JSS` enthalten. Fügen Sie der Variablen `LD_LIBRARY_PATH` das Verzeichnis `/usr/lib/mps/secv1` (für Solaris) oder das Verzeichnis `/opt/sun/private/lib` (für Linux) hinzu.

Access Manager-SDK

Die Eindeutigkeit von Attributen in der Top-Level-Organisation ist bei Namensattributen nicht gewährleistet (6204537)

In der Top-Level-Organisation funktioniert die Eindeutigkeit von Attributen nicht. Die Eindeutigkeit von Attributen auf Benutzer- und Organisationsebene ist jedoch gewährleistet.

Der EventService-Thread verursacht einen Tight Loop, wenn er keine dauerhafte Suchverbindung erhält (6205443)

Der EventService-Thread (ES) fügt die Listener erfolgreich hinzu (LDAP JDK fügt Listener erfolgreich hinzu), selbst wenn dauerhafte Suchen verbunden sind. Wenn ein ES-Thread jedoch versucht, eine Antwort abzurufen, meldet LDAPResponse (Fehlernummer 51), dass keine dauerhaften Suchverbindungen verfügbar sind. Der ES-Thread versucht daraufhin, die Listener erneut einzurichten. Dadurch entsteht ein Tight Loop.

Verwendung von „certutil“ für Access Manager-SDK-Installationen, die SSL-Server verwenden (5027614)

Bei Benutzern treten sicherheitsbezogene Fehler und Ausnahmen auf, wenn Sie versuchen, von Nur-SDK-Rechnern mit SSL-fähigen Access Manager-Servern zu kommunizieren. In diesem Szenario wird der Access Manager-SDK entweder auf keinem Webcontainer oder auf einem Webcontainer eines Drittanbieters bereitgestellt, wie BEA WebLogic Server oder IBM WebSphere Application Server.

Umgehung

Erstellen Sie eine Zertifikatdatenbank auf dem Nur-SDK-Rechner und installieren Sie das Stamm-Zertifizierungsstellenzertifikat für Access Manager in dieser Datenbank:

1. Melden Sie sich am Nur-SDK-Rechner als Superuser (`root`) an.

2. Überprüfen Sie, dass das erforderliche Netscape Security Services-Paket (NSS) installiert ist:
   - Auf Solaris-Systemen: SUNWtlsu
   - Auf Linux-Systemen: sun-nss RPM
3. Wenn das Paket nicht installiert ist, installieren Sie es. Zum Beispiel:

   Auf Solaris-Systemen:

   ```
   cd JavaEnterpriseSystem_Basis/Solaris_arch/Product/shared_components/Packages
   pkgadd -d . SUNWtlsu
   ```

   Auf Linux-Systemen:

   ```
   cd JavaEnterpriseSystem_Basis/Linux_x86/Product/shared_components/Packages
   rpm -Uvh sun-nss-3.3.10-1.i386.rpm
   ```

4. Erstellen Sie die Passwortdatei für das Tokenpasswort für diese Zertifikatdatenbank. Zum Beispiel:

   Auf Solaris-Systemen:

   ```
   echo "cert-database-password" > /etc/opt/SUNWam/config/.wtpass
   chmod 700 /etc/opt/SUNWam/config/.wtpass
   ```

   Auf Linux-Systemen:

   ```
   echo "cert-database-password" > /etc/opt/sun/identity/config/.wtpass
   chmod 700 /etc/opt/sun/identity/config/.wtpass
   ```

   wobei *cert-database-password* das Tokenpasswort ist.

5. Prüfen Sie die Variable LD_LIBRARY_PATH:

   Prüfen Sie auf Solaris-Systemen anhand der Variablen LD_LIBRARY_PATH, ob die Verzeichnisse `/usr/lib`, `/usr/lib/mps/secv1` und `/usr/lib/mps` vorhanden sind. Wenn nicht, fügen Sie die nicht vorhandenen Verzeichnisse hinzu.

   Prüfen Sie anhand der Variablen LD_LIBRARY_PATH, ob das Verzeichnis `/opt/sun/private/lib` vorhanden ist. Falls nicht, fügen Sie das Verzeichnis hinzu.

6. Erstellen Sie mit dem Zertifikatdatenbank-Tool (`certutil`) die Zertifikat- und Schlüsseldatenbank. Informationen über `certutil` finden Sie auf der folgenden Website:

   `http://mozilla.org/projects/security/pki/nss/tools/certutil.html`

   Zum Beispiel:

   `certutil-home``/certutil -N -d` *`cert-database-dir`* `-f` *`config-home`*`/.wtpass`

   Wobei:

   certutil-home der Speicherort von `certutil` ist:

   - Auf Solaris-Systemen: `/usr/sfw/bin`
   - Auf Linux-Systemen: `/opt/sun/private/bin`

   cert-database-dir das Datenbankverzeichnis für die Zertifikat- und Schlüsseldatenbank ist.

   config-home der Speicherort der Access Manager-Konfigurationsdateien ist:

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

7. Fügen Sie in der neu erstellten Zertifikatdatenbank das Stamm-Zertifizierungsstellenzertifikat für das SSL-Zertifikat hinzu, das auf dem Access Manager-Server installiert ist. Zum Beispiel:

   `certutil-home``/certutil -A -n "`*`certificate-nickname`*`" -t "TCu,TCu,TCuw" -d` *`cert-database-dir`* `-a -i` *`path-to-file-containing-cert`* `-f` *`config-home`*`/.wtpass`

8. Zeigen Sie die Datei `AMConfig.properties` mit einem Editor an und prüfen Sie folgende Werte:

   - Zertifikatdatenbankverzeichnis: `com.iplanet.am.admin.cli.certdb.dir`
   - Präfix: `com.iplanet.am.admin.cli.certdb.prefix`
   - Passwortdatei: `com.iplanet.am.admin.cli.certdb.passfile`

     Bearbeiten Sie die Einstellungen, falls erforderlich. Die Präfixeinstellung sollte beispielsweise leer sein (d. h. „“ entsprechen).

9. Wenn Änderungen an der Datei `AMConfig.properties` vorgenommen wurden und Access Manager-SDK in einem Webcontainer bereitgestellt wird, starten Sie den Webcontainer neu.

SSL-Handshake schlägt bei DNSAlias mit JCE Provider fehl (5038876)

Der SSL-Handshake schlägt fehl, wenn Zertifikate mit gültigen `DNSAlias`-Namen im `subjectaltname` mit einem JCE Provider verwendet werden.

Identity-Methoden in Init() von Filtern verursachen den Absturz von WebLogic (5016283)

Ein WebLogic-Server kann nicht gestartet werden, wenn die `init()`-Methoden der Filter Access Manager-bezogenen Code enthalten. Die Access Manager-API wird in der `init`-Methode des ServletFilter-Servlet aufgerufen.

Access Manager verwendet JSS als Sicherheitsanbieter, WebLogic hingegen standardmäßig JCE. Wenn die `init`-Methode aufgerufen wird, versucht WebLogic, die Lizenz mit JCE zu überprüfen. Es wird jedoch JSS initialisiert.

Umgehung

Ändern Sie die Standard-Sicherheitsverschlüsselung in der Datei `AMConfig.properties` von `JSSEncryption` in `JCEEncryption`.

Passwörter, die mit „{SSHA}“-Symbolen beginnen, können nicht verwendet werden (4966191)

Access Manager unterstützt nicht die Verwendung von Hash-{SSHA}-Symbolen in Passwörtern.

Option für die Gruppenerstellung fügt nur ein memberURL-Attribut hinzu (4931958)

Wenn Sie eine Gruppe mit der Option für mehrere LDAP-Filter (`-f`) erstellen, wird die Gruppe fälschlicherweise mit nur einem `memberURL`-Attribut erstellt.

Optimierung

Das Skript „amtune“ und die zugehörigen Dateien werden für Solaris-x86 nicht bereitgestellt (6213019)

In dieser Version werden das Skript `amtune` und die ihm zugeordneten Dateien unter Solaris-x86 nicht im richtigen Verzeichnis installiert.

Umgehung

Verwenden Sie die für Sparc-Solaris bereitgestellten `amtune`-Dateien.

Das Skript „amtune-as8“ generiert eine fehlerhafte Passwortdatei (6212380)

Die automatische Optimierung von Application Server 8 (`amtune-as8`) mit dem Skript `amtune` funktioniert nicht, weil eine temporäre Passwort-Datei mit dem Passwort `asadmin` generiert wird, die zurzeit nur das Passwort enthält.

Umgehung

Verwenden Sie in `amtune-as8` die folgende Syntax, um die Zeichenfolge korrekt einzugeben:

```
"TOKEN=Wert"
```

Zum Beispiel:

```
"AS_ADMIN_PASSWORD=11111111"
```

Geben Sie die folgende Änderung in `amtune-env` ein:

```
#ASADMIN=$CONTAINER_BASE_DIR/bin/asadmin

ASADMIN=/opt/SUNWappserver/appserver/bin/asadmin
```

Single Sign-On

SSO kann nicht mit verschiedenen Bereitstellungs-URIs durchgeführt werden (4770271)

Falls die Bereitstellungs-URIs zweier verschiedener Instanzen von Access Manager unterschiedlich sind, funktioniert Single Sign-On nicht ordnungsgemäß.

Internationalisierung (i18n)

Gruppenmitglieder werden nicht aufgelistet, wenn der Gruppenname aus Multibyte-Zeichen besteht (6197041)

In der internationalen Version von Access Manager 6 2005Q1 werden Gruppenmitglieder nicht auf der Access Manager-Konsole aufgelistet, wenn der Gruppenname aus Multibyte-Zeichen besteht.

Die Start- und Endmeldungen sind unter Linux nicht lesbar (6207421)

Die Start- und Endmeldungen von Access Manager sind im Zeichensatz `zh/zh_TW` nicht lesbar. Dieser Fehler tritt nur unter Linux auf.

Die Anmeldung ist nicht möglich, wenn „HTTPBasic“ und „WindowsDesktopSSO“ in einem nichtenglischen Gebietsschema vorliegen (6209324)

Bei nichtenglischen Gebietsschemen können Sie sich nicht bei den Authentifizierungsmodulen `HTTPBasic` und `WindowsDesktopSSO` anmelden.

Umgehung

Setzen Sie die folgenden Parameter in den XML-Dateien auf Englisch zurück:

```
HTTPBasic.xml: <HttpHeader>Authorization</HttpHeader>

WindowsDesktopSSO.xml: HttpHeader>Authorization</HttpHeader>
```

Diese Dateien werden bei der Bereitstellung von Access Manager in Application Server normalerweise im folgenden Verzeichnis installiert:

```
/var/opt/sun/appserver/domains/domain1/applications/j2ee-modules/amserver/config/auth/defa
ult_<lang>
```

Bei der Bereitstellung von Access Manager in Web Server werden diese Dateien normalerweise im folgenden Verzeichnis installiert:

```
/opt/sun/webserver/https-<host>/is-web-apps/services/config/auth/default_<lang>
```

Die japanische Online-Hilfe wird falsch angezeigt (5024138)

Wenn Sie die japanische Version von Access Manager ausführen und die Sprache in en_US ändern, wird nach wie vor die japanische Kontexthilfe angezeigt.

Umgehung

Erstellen Sie einen Sym-Verweis von `docs_en` zu `docs_en_US`.

Die Client-Erkennungsfunktion funktioniert nicht ordnungsgemäß (5028779)

Das Entfernen des UTF-8-Zeichensatzes funktioniert im Client-Erkennungsdienst nicht ordnungsgemäß.

Umgehung

Wenn Sie den UTF-8-Zeichensatz entfernen, müssen Sie den Webcontainer anschließend neu starten.

G11NSetting kann Leerzeichen im Faktor Q nicht verarbeiten (5008860)

Wenn die Client-Daten in oder neben dem Faktor `q` ein Leerzeichen aufweisen, kann der G11NSettings-Code sie nicht korrekt analysieren und gibt folgenden Fehler aus:

```
FEHLER: G11NSettings::Fetchcharset() Analyse konnte nicht durchgeführt werden:
Zeichensatzeintrag ungültig Q q
```

Fehler bei der Anmeldeseite mit dem Multibyte-Rollenparameter auf URL für Ja-Zeichensatz (4905708)

Falls Sie eine Multibyte-Rolle erstellen und anschließend eine URL-Anmeldung mit einem Benutzer versuchen, der bei der Multibyte-Rolle registriert ist, gibt die Anmeldeseite eine Fehlermeldung aus.

Umgehung

Damit das Authentifizierungs-Framework einen im URL angegebenen Wert für eine Multibyte-Rolle entschlüsseln kann, müssen Sie `gx_charset` zusammen mit dem Parameter angeben. Zum Beispiel:

```
http://hostname:port/amserver/UI/Login?role=manager?role=%E3%81%82%&gx_charset=utf-8
```

In der Ja-Ländereinstellung sind die Protokolldateien unleserlich (4882286)

Die folgende Protokolldateien enthalten beim Öffnen japanische Zeichen und unleserlichen Text:

Alle Dateien im Verzeichnis `/var/opt/SUNWam/debug` mit Ausnahme der Dateien `deploy.log` und `undeploy.log`.

Ländereinstellungsparameter in URL zeigt eine mehrsprachige Anmeldeseite an (4915137)

Wenn Sie einen nichtenglischen Browser mit einer Instanz von Access Manager installieren, die auf Web Server installiert ist, und sich bei `http://`*host*`:`*anschluss*`/amserver/UI/Login?locale=en` anmelden, werden auf der Anmeldeseite sowohl englische als auch anderssprachige Zeichen angezeigt.

Umgehung

Ändern Sie den folgenden symbolischen Verweis:

AccessManager-Basis`/SUNWam/web-apps/services/config/auth/default`

in

AccessManager-Basis`/SUNWam/web-apps/services/config/auth/default_en`

Mehrere Sprachen im Anmeldefenster, wenn Application Server auf „ja“ gesetzt ist (4932089)

Das Access Manager-Anmeldefenster wird nicht auf die Standardeinstellung Englisch zurückgesetzt, wenn die Einstellung für die Browsersprache `en` lautet und die Ländereinstellung von Application Server auf `ja` eingestellt ist.

Umgehung

Führen Sie Application Server mit der Ländereinstellung `en` aus.

Sperrbenachrichtigungsfunktion sendet nicht lesbare E-Mail (4938511)

Wenn Sie Access Manager mit einem Webcontainer ausführen, für den die bevorzugte Ländereinstellung nicht `C` ist, und ein Benutzer für den Server gesperrt wird, erhalten Sie eine Sperrbenachrichtigung, die jedoch nicht lesbar ist.

Umgehung

Legen Sie für das Attribut „E-Mail-Adresse für das Versenden der Sperrbenachrichtigung“ `email|ländereinstellung|zeichensatz` (und nicht nur den `email`-Parameter) fest. Zum Beispiel:

```
user1@example.com|zh|GB2312
```

Multibyte-Namen funktionieren nicht bei Selbstregistrierung (4732470)

Wenn Sie im Selbstregistrierungsmodul (Mitgliedschafts-Authentifizierungsdienst) einen Benutzer erstellen, dessen Benutzer-ID doppelt vorhanden ist und der einen Multibyte-Vornamen und -Nachnamen aufweist, tritt ein Fehler auf. Multibyte-Benutzer-IDs werden nicht unterstützt.

Umgehung

Wenn sich ein Benutzer mithilfe der Selbstregistrierung in einer Multibyte-Umgebung anmeldet, muss der Administrator sicherstellen, dass das Attribut für den Benutzererstellungsmodus in der Kern-Authentifizierung nicht ausgewählt ist.

Oder

Der Benutzer kann auf der Anmeldeseite `Selbstregistrierung` die Option `Selbst erstellen` auswählen.

Japanische Version von Access Manager funktioniert nicht mit Netscape 6.22 oder 6.23 (4902421)

In der japanischen Version von Access Manager können Sie sich nicht mit Netscape 6.22 oder 6.23 bei der Konsole anmelden.

Zeitbedingungsformat ändert sich nicht (4888416)

In den Zeitbedingungen für Richtliniendefinitionen wird die Zeit unabhängig von der Ländereinstellung in folgendem Format angezeigt:

```
Stunde:Minute AM/PM
```

Bildschirm für Client-Erkennung nicht lokalisiert (4922013)

Teile des Bildschirms für die aktuellen Stileigenschaften der Oberfläche für die Client-Erkennung wurden in dieser Version nicht lokalisiert.

Aktualisierte genericHTM-Client-Eigenschaft wird nicht angewendet (4922348)

Wenn Sie UTF-8 aus der Zeichensatzliste in der genericHTML-Client-Eigenschaft im Client-Erkennungsdienst entfernen, die Änderungen speichern und die Client-Erkennung anschließend aktivieren und sich daraufhin ab- und wieder anmelden, weist die Anmeldeseite nach wie vor den UTF-8-Zeichensatz auf.

Umgehung

Starten Sie den Server manuell mithilfe von `amserver` neu.

Kopfzeilen der Protokolldateien nicht lokalisiert (4923536)

Die ersten beiden Zeilen aller Protokolldateien, genau genommen die Abschnitte `Version` und `Fields` und ihre zugehörigen Feldlisten, wurden nicht lokalisiert.

Datenfeldwerte in „amSSO.access“ nicht lokalisiert (4923549)

In der Protokolldatei `amSSO.access` wurden sämtliche Werte im Feld für die Daten nicht lokalisiert.

„Exception.jsp“ enthält hartkodierte Meldungen (4772313)

`Exception.jsp` wurde nicht lokalisiert und enthält hartkodierte Titel, Fehlermeldungen und Copyright-Informationen. Diese Ausnahmefehlerseite wird nur in extremen Fällen aufgerufen. Beispiele hierfür sind, wenn Directory Server ausgefallen ist oder keine Access Manager-Dienste hochgefahren werden können. Für diese JSP-Seite ist keine lokalisierte Version verfügbar.

Cookies

Der Modus ohne Cookies funktioniert nicht (4967866)

Wenn ein Browser, der Cookies unterstützt, auf Access Manager zugreift, und die Cookie-Unterstützung deaktiviert ist, sendet der Browser weiterhin das ältere Access Manager-Cookie. Dadurch wird der Zugriff auf die Access Manager-Ressourcen verweigert.

Umgehung

Wählen Sie eine der folgenden Lösungen:

- Leeren Sie den Cookie-Cache des Browsers, um alle Access Manager-Cookies zu entfernen.
- Deaktivieren Sie Cookies im Browser.

Cookie-Raub

Die Sicherheit kann beeinträchtigt werden, wenn Sitzungs-Cookies von Anwendungen verwendet werden, die nicht vertrauenswürdig sind.

Wenn in Ihrer Access Manager-Bereitstellung Single Sign-On (SSO) oder domänenübergreifendes Single Sign-On (CDSSO) aktiviert ist, werden die `http(s)`-Sitzungs-Cookies im Browser des Benutzers eingerichtet. Diese Cookies werden von mehreren Anwendungen überprüft. Wenn sich die Access Manager-Bereitstellung über mehrere DNS-Domänen hinweg erstreckt, überträgt das Liberty-Protokoll die `http(s)`-Sitzungs-Cookies von der authentifizierten DNS-Domäne an die Zieldomäne der Webanwendung.

Obwohl der Benutzer automatisch bei den Webressourcen angemeldet wird, besteht ein gewisses Sicherheitsrisiko, wenn die Sitzungs-Cookies von Anwendungen verwendet werden, die nicht vertrauenswürdig sind. Dieses Risiko besteht vor allem bei der Bereitstellung von Authentifizierungs-, Autorisierungs- und Profilinformationen von Benutzern für Anwendungen (oder Dienstanbieter), die von Drittanbietern oder nicht autorisierten Gruppen innerhalb des Unternehmens entwickelt wurden. Mögliche Sicherheitsprobleme:

- Alle Anwendungen verwenden dasselbe `http`-Sitzungs-Cookie. Dadurch kann eine böswillige Anwendung das Sitzungs-Cookie rauben und sich in einer anderen Anwendung als diesen Benutzer ausgeben.
- Wenn die Anwendung das `https`-Protokoll nicht verwendet, ist das Sitzungs-Cookie anfällig für Netzwerk-Lauschangriffe.
- Wenn auch nur eine Anwendung gehackt werden kann, ist die Sicherheit der gesamten Infrastruktur gefährdet.
- Eine böswillige Anwendung kann das Sitzungs-Cookie verwenden, um die Profilattribute eines Benutzers abzurufen und eventuell zu ändern. Wenn der Benutzer über Administratorrechte verfügt, wäre die Anwendung dann in der Lage, noch viel größeren Schaden anzurichten.

Umgehung

Führen Sie die folgenden Schritte aus:

1. Verwenden Sie die Access Manager-Verwaltungskonsole, um für jeden Agenten einen Eintrag zu erstellen.
    a. Wählen Sie in der Organisation, die den zu erstellenden Agenten enthält, im Menü `Ansicht` die Option `Agenten` und klicken Sie dann auf `Neu`.

b. Geben Sie die folgenden Informationen ein:

Name: Geben Sie den Namen oder die Identität des Agenten ein. Beispiel: `agent123`

Passwort: Geben Sie das Agentenpasswort ein. Beispiel: `agent123`

Passwort bestätigen: Bestätigen Sie das Passwort.

Beschreibung: Geben Sie eine kurze Beschreibung des Agenten ein. Sie können beispielsweise den Instanzennamen des Agenten oder den Namen der Anwendung eingeben, die dieser schützt.

Agent-Schlüsselwert. Legen Sie die Agenteneigenschaften über ein Schlüssel/Wert-Paar fest. Diese Eigenschaft verwendet Access Manager für den Empfang von Agentenanforderungen für Benutzerberechtigungsbestätigungen.

Geben Sie einen Eigenschaftswert für `agentRootURL` ein, der dem Agenten-URL und seiner Anschlussnummer entspricht. Beachten Sie, dass der `agentRootURL`-Wert zwischen Groß- und Kleinschreibung unterscheidet.

Beispiel: `agentRootURL=http://`*Servername:99*`/`

Gerätestatus: Geben Sie den Gerätestatus des Agenten ein. Bei Einstellung `Aktiv` wird dem Agenten die Authentifizierung und Kommunikation mit Access Manager ermöglicht. Bei Einstellung `Inaktiv` kann sich der Agent nicht bei Access Manager authentifizieren.

c. Klicken Sie auf `OK`.

2. Führen Sie den folgenden Befehl mit dem Passwort aus, das Sie in Schritt 1b eingegeben haben.

AccessManager-Basis`/SUNWam/agents/bin/crypt_util agent123`

Dies bewirkt folgende Ausgabe:

```
WnmKUCg/y3l404ivWY6HPQ==
```

3. Geben Sie in die Datei `AMAgent.properties` den neuen Wert ein und starten Sie den Agenten danach neu. Beispiel:

```
# The username and password to use for the Application authentication module.


com.sun.am.policy.am.username = agent123
com.sun.am.policy.am.password = WnmKUCg/y3l404ivWY6HPQ==


# Cross-Domain Single Sign On URL

# Is CDSSO enabled.

com.sun.am.policy.agents.cdsso-enabled=true


# This is the URL the user will be redirected to after successful login

# in a CDSSO Scenario.

com.sun.am.policy.agents.cdcservletURL =
http://server.example.com:port/amserver/cdcservlet
```

4. Geben Sie in die Datei `AMConfig.properties` die neuen Werte ein und starten Sie Access Manager danach neu. Beispiel:

```
com.sun.identity.enableUniqueSSOTokenCookie=true

com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer


com.sun.identity.authentication.uniqueCookieDomain=example.com
```

5. Wählen Sie in der Access Manager-Verwaltungskonsole die Option `Dienstkonfiguration> Plattform`.

6. Ändern Sie den Cookie-Domänennamen in der Liste `Cookie-Domänen`:
   a. Wählen Sie die Standarddomäne `iplanet.com` aus und klicken Sie auf `Entfernen`.
   b. Geben Sie den Hostnamen der Access Manager-Installation ein und klicken Sie auf `Hinzufügen`.

   Beispiel: server.`example.com`

   Nun sollten im Browser zwei Cookies zu sehen sein:

Cookie	Hostname
`iPlanetDirectoryPro`	`server.example.com`
`sunIdentityServerAuthNServer`	`example.com`

Dateien für Neuverteilung

Sun Java System Access Manager 2005Q1 enthält keine Dateien für die Neuverteilung für nicht lizenzierte Produktbenutzer.

Problemmeldungen und Feedback

Wenn Sie mit Sun Java System Access Manager Probleme haben, wenden Sie sich an die Kundenunterstützung von Sun. Dazu stehen Ihnen folgende Möglichkeiten zur Verfügung:

- Sun-Softwaresupport unter:
  `http://www.sun.com/supportraining`

  Auf dieser Website finden Sie Links zur Knowledge Base, zum Online Support Center, zum ProductTracker wie auch zu Wartungsprogrammen und Kontaktinformationen für den Kundendienst.
- Die auf Ihrem Wartungsvertrag angegebene Telefonnummer.

Damit wir Sie optimal beraten können, halten Sie bitte die folgenden Informationen bereit, wenn Sie sich an die Kundenunterstützung wenden:

- Beschreibung des Problems einschließlich der Situation, in der das Problem auftrat, sowie seine Auswirkungen auf Ihre Arbeit.
- Rechnertyp, Betriebssystem- und Produktversion einschließlich sämtlicher Patches und anderer Software, die mit dem Problem in Zusammenhang stehen können.
- Detaillierte Beschreibung der von Ihnen für die Reproduktion des Problems verwendeten Methoden.
- Sämtliche Fehlerprotokolle oder Kernspeicherauszüge.

Kommentare sind willkommen

Sun möchte seine Dokumentation laufend verbessern. Ihre Kommentare und Vorschläge sind daher immer willkommen. Verwenden Sie das webbasierte Formular, um uns Ihr Feedback mitzuteilen:

http://www.sun.com/hwdocs/feedback/

Tragen Sie den vollständigen Titel der Dokumentation und die vollständige Teilenummer in die entsprechenden Felder ein. Die Teilenummer ist eine 7-stellige oder 9-stellige Zahl, die Sie auf der Titelseite des Handbuchs oder am Anfang des Dokuments finden. Die Teilenummer dieser Versionshinweise lautet beispielsweise 819-1943.

Weitere Informationen über Sun

Nützliche Informationen über Sun Java System finden Sie unter den folgenden Internet-Adressen:

- Sun Java System-Dokumentation
  http://docs.sun.com/prod/entsys.05q1
- Professionelle Dienste für Sun Java System
  http://www.sun.com/service/products/software/javaenterprisesystem/
- Sun Java System-Softwareprodukte und -Dienste
  http://wwws.sun.com/software/
- Sun Java System-Softwaresupport
  http://www.sun.com/supportraining
- Sun Java System-Support und -Knowledge Base
  http://sunsolve.sun.com

- Sun Java System-Beratung und professionelle Dienste
  http://www.sun.com/service/products/software/javaenterprisesystem
- Sun Java System-Informationen für Entwickler
  http://developers.sun.com/
- Supportdienste für Sun-Entwickler
  http://www.sun.com/developers/support