Sun Java System Access Manager 7.1 - Versionshinweise für Microsoft Windows

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

Teilenr.: 820–1792–10
Februar 2007

070528@17466

Inhalt

◆ ◆ ◆ KAPITEL 1

Sun Java System Access Manager 7.1 Versionshinweise für Microsoft Windows

Die Versionshinweise zu Sun Java™ System Access Manager 7.1 enthalten wichtige Informationen über die Version Sun Java Enterprise System (Java ES), neue Funktionen von Access Manager und bekannte Probleme sowie Problemlösungen, falls verfügbar. Lesen Sie dieses Dokument, bevor Sie diese Version installieren.

Die Java ES-Produktdokumentation, einschließlich der Access Manager-Sammlung können Sie unter `http://docs.sun.com/prod/entsys.05q4` anzeigen.Schauen Sie auf dieser Website nach, bevor Sie die Software installieren und einrichten und dann in regelmäßigen Abständen, um die aktuellste Dokumentation einzusehen.

Die Access Manager 7.1 2006Q4 Versionshinweise enthalten die folgenden Abschnitte:

Info zu Sun Java System Access Manager 7.1

Sun Java System Access Manager ist Teil der Sun Identity Management-Infrastruktur, die es einem Unternehmen ermöglicht, sicheren Zugriff auf Webanwendungen und andere Ressourcen sowohl innerhalb eines Unternehmens als auch über B2B-Wertschöpfungsketten (Business-to-Business) hinweg zu verwalten. Access Manager bietet die folgenden Hauptfunktionen:

- Zentrale Authentifizierungs- und Genehmigungsdienste unter Verwendung einer rollen- und regelbasierten Zugriffssteuerung
- Single Sign-On (SSO) für den Zugriff auf die webbasierten Anwendungen eines Unternehmens
- Vereinigte Identitätsunterstützung mit Liberty Alliance Project und Security Assertions Markup Language (SAML)
- Protokollierung von wichtigen Informationen, einschließlich Administrator- und Benutzeraktivitäten durch Access Manager-Komponenten für nachfolgende Analysen, Berichterstellung und Prüfung.

Neue Funktionen in dieser Version

Diese Version bietet die folgenden neuen Funktionen:

- „Java ES Monitoring Framework-Integration" auf Seite 6
- „Web Service Security" auf Seite 7
- „Single Access Manager WAR-Dateibereitstellung. " auf Seite 7
- „Verbesserung der Kerndienste" auf Seite 7

Java ES Monitoring Framework-Integration

Access Manager 7.1 wird über Java Management Extensions (JMX) mit dem Java Enterprise System Monitoring Framework integriert. Die JMX-Technologie bietet Werkzeuge zum Erstellen von verteilten, webbasierten, modularen und dynamischen Lösungen für die Verwaltung und Überwachung von Geräten, Anwendungen und dienstgesteuerten Netzwerken. Zur typischen Verwendung der JMX-Technologie gehören die Konsultation und das Ändern der Anwendungskonfiguration, das Erfassen von Statistiken über das Anwendungsverhalten und Benachrichtigungen über Statusänderungen und fehlerhaftes Verhalten. Die Daten werden an eine zentrale Überwachungskonsole gesendet.

Access Manager 7.1 verwendet das Java ES Monitoring Framework, um Statistiken und dienstbezogene Daten zu erfassen, beispielsweise:

- Anzahl an versuchten, erfolgreichen und fehlgeschlagenen Authentifizierungen.
- Anzahl an aktiven Sitzungen, Statistiken aus der Sitzungs-Failover-Datenbank.
- Sitzungs-Failover-Datenbankstatistiken.
- Statistiken zum Richtlinien-Caching.
- Transaktionszeiten der Richtlinienbewertung.
- Anzahl an Assertionen für einen bestimmten Anbieter in einer SAML/Federation-Bereitstellung.

Web Service Security

Access Manager 7.1 erweitert die Authentifizierungsfähigkeiten für Webdienste in folgender Art und Weise:

- In ausgehende Nachrichten werden Token eingefügt.
- Eingehende Nachrichten werden auf Sicherheitstoken überprüft.
- Ermöglicht die Auswahl von Authentifizierungsanbietern durch Anklicken neuer Anwendungen.

Single Access Manager WAR-Dateibereitstellung.

Access Manager enthält eine einzelne WAR-Datei, die Sie verwenden können, um Access Manager-Dienste konsistent auf allen unterstützten Containern und Plattformen bereitzustellen. Die Access Manager WAR-Datei koexistiert neben dem Java Enterprise System-Installer, der viele JAR-, XML-, JSP-, HTML-, GIF- und verschiedene .properties-Dateien bereitstellt.

Verbesserung der Kerndienste

Unterstützte Webcontainer

- 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

Monitoring Framework-Integration

Access Manager kann das JES Monitoring Framework zur Überwachung der folgenden Punkte verwenden:

- Authentifizierung
  - Anzahl an versuchten Authentifizierungen
  - Anzahl an versuchten entfernten Authentifizierungen (optional)
  - Anzahl an erfolgreichen Authentifizierungen
  - Anzahl an fehlgeschlagenen Authentifizierungen
  - Anzahl an erfolgreichen Abmeldevorgängen
  - Anzahl an fehlgeschlagenen Abmeldevorgängen (optional)
  - Transaktionszeit für jedes Modul, falls möglich, beim Ausführen und Wartestatus
  - Konnektivitätsfehler für Backend-Server.
- Sitzungen
  - Größe der Sitzungstabelle, die die maximale Anzahl angibt

    - Anzahl an aktiven Sitzungen bei Verwendung eines inkrementellen Zählers
    - Sitzungs-Failover, einschließlich der Anzahl der "gespeicherten" Sitzungen oder Sitzungszählung mit inkrementellem Zähler und Anzahl der durchgeführten Operationen, die für die Failover-DB durchgeführt wurden, einschließlich Lesen, Schreiben, Löschen und Anzahl der Operationen
- Benutzerverwaltung/Identitäts-Repository/Sitzungsverwaltungsdienst
    - Maximale Cachegröße
    - Cache-bezogene Statistiken wie die Anzahl an Treffern, Verhältnis, Höchstlast, aktuelle Größe usw.
    - Transaktionszeit für Vorgänge beim Ausführen und Warten
- Richtlinie
    - Anzahl an Richtlinien im Cache
    - Anzahl an `policyManagers` im Cache
    - Anzahl an Dienstnamen im `policyListener`-Cache
    - Anzahl an Diensten im `resultsCache`
    - Anzahl an `tokenIDs` in `sessionListernerRgistry`
    - Anzahl der Dienstnamen in `policyListenerRegistry`
    - Anzahl an `tokenIDs` im `role`/Cache
    - Anzahl an Dienstnamen im `resourceNames`-Cache
    - Anzahl an Einträgen für `SubjectEvaluationCache`
    - Anzahl an `PolicyEvaluators` im Cache
    - Anzahl an Richtlinienänderungs-Listenern im Cache
    - Transaktionszeit für die Verarbeitung der Richtlinienbewertung
- Verbindung
    - Anzahl an Produkten für einen bestimmten Anbieter
    - Anzahl der Assertionen in Tabelle für einen bestimmten Anbieter
    - Anzahl der Sitzungseinträge in eine bestimmte Tabelle für eine bestimmte Anbieter-ID
- SAML
    - Größe der Produktzuordnung
    - Größe der Assertionszuordnung

Authentifizierungsmodul

- Dienst für verteilte Authentifizierung für Bereitstellungen mit Load Balancer nicht auf einen einzigen Server beschränkt
- Dienst und Server für Authentifizierung für Bereitstellungen mit Load Balancer nicht auf einen einzigen Server beschränkt

- Unterstützt zusammengesetzte Advices neben Authentifizierungsdienst, Richtlinien-Agenten und Richtliniendienst. Diese Unterstützung enthält `AuthenticateToRealm` und AuthenticateToService sowie die Bereichsqualifizierung für alle Bedingungen.
- Advice-Organisation unter Verwendung von bereichsqualifizierten Authentifizierungsbedingungen.
- Authentifizierungskonfigurationen-Authentifizierungsketten (`AuthServiceCondition`)
- Bei aktivierter Authentifizierungsverkettung kann die modulbasierte Authentifizierung verweigert werden.
- Der Dienst für verteilte Authentifizierung unterstützt das Zertifikatauthentifizierungs-Modul.
- Zu Distributed Authentication UI wurde `CertAuth` hinzugefügt, um über die UI eine voll funktionsfähige Extractor-Präsentation für Anmeldeinformationen zu bieten.
- Neues Data Store-Authentifizierungsmodul, das die Authentifizierung anhand des konfigurierten Data Store für einen bestimmten Bereich durchführt.
- Die Konfiguration der Kontosperre ist nun über mehrere AM-Serverinstanzen hinweg persistent.
- Verkettung von Vorverarbeitungs-SPI-Klassen.

Richtlinienmodul

- Unterstützt Richtliniendefinitionen basierend auf der dienstbasierten Authentifizierung.
- Eine neue Richtlinienbedingung wurde hinzugefügt: AuthenticateToRealmCondition
- Unterstützung von Ein-Ebenen-Platzhalter-Vergleichen; hierdurch kann der Inhalt des Verzeichnisses geschützt werden, ohne das Unterverzeichnis zu schützen.
- Unterstützung für LDAP-Filterbedingung. Der Richtlinienadministrator kann beim Definieren einer Richtlinie einen LDAP-Filter in der Bedingung angeben.
- Richtlinien können ohne explizite Bezugsrichtlinien des übergeordneten Bereichs in Unterbereichen erstellt werden, wenn in der globalen Richtlinienkonfiguration Organisations-Aliasbezüge aktiviert wurden.
- `AuthLevelCondition` kann zusätzlich zur Authentifizierungsebene den Bereichsnamen angeben.
- `AuthSchemeCondition` kann zusätzlich zum Namen des Authentifizierungsmoduls den Bereichsnamen angeben.

Dienst-Verwaltungs-Modul

- Unterstützt das Speichern der Dienst-Verwaltungs-/Richtlinienkonfiguration in Active Directory.

Access Manager-SDK

- Unterstützt APIs zum Authentifizieren von Benutzern anhand einer standardmäßigen Identitäts-Repository-Framework-Datenbank.

Unterstützung von Webdiensten

- Liberty ID-WSF SOAP-Anbieter: Authentifizierungsanbieter, der die Liberty ID-WSF SOAP-Binding als Implementierung von Access Manager enthält. Dieser Anbieter ist ein Client- und Server-Anbieter.
- SSO-Anbieter auf HTTP-Ebene: Authentifizierungsanbieter auf `HttpServlet`-Ebene, der den Access Manager-basierten SSO auf der Serverseite enthält.

Installationsmodul

- Erneute Bereitstellung von Access Manager als J2EE Application, wobei eine einzelne WAR-Datei erzeugt wird, die im Web bereitgestellt werden kann.

Delegationsmodul

- Unterstützt die Gruppierung von Delegationsberechtigungen

Protokollierung

- Unterstützt die Delegation im Protokollierungsmodul und kontrolliert, welche Identitäten die Protokolldateien bearbeiten oder lesen können.
- Unterstützt JCE-basierte SecureLogHelper - auf diese Weise kann JCE (neben JSS) als Sicherheitsanbieter für die Implementierung der sicheren Protokollierung verwendet werden.

Hardware- und Software-Anforderungen

Die folgende Tabelle enthält eine Auflistung der für diese Version erforderlichen Hardware und Software.

TABELLE 1–1 Hardware- und Software-Anforderungen

Komponente	Anforderung
Betriebssystem (OS)	■ Windows 2000 Advance Server SP4 ■ Windows XP SP2 ■ Windows 2003 Enterprise Server SP1 (32 Bit) ■ Windows 2003 Enterprise Server SP1 (64 Bit)
Java 2 Standard Edition (J2SE™-Plattform)	J2SE-Plattform 6.0, 5.0 Update 7 und 1.4.2 Update 11

TABELLE 1–1 Hardware- und Software-Anforderungen *(Fortsetzung)*

Komponente	Anforderung
Directory Server	Access Manager-Informationsbaum: Sun Java System Directory Server 5.2
	Access Manager-Identitätsrepository: Sun Java System Directory Server 6.0 oder Microsoft Active Directory
Web-Container	Sun Java System Web Server7.0
	Sun Java System Application Server Enterprise Edition 8.2
RAM	Basistests: 512 MB
	Tatsächliche Bereitstellung: 1 GB für Threads, Access Manager SDK, HTTP-Server sowie andere interne Komponenten
Plattenspeicher	512 MB für Access Manager und die zugehörigen Anwendungen

Falls Sie Fragen zur Unterstützung von anderen Versionen dieser Komponenten haben, wenden Sie sich an die technischen Mitarbeiter von Sun Microsystems.

Unterstützte Browser

In der folgenden Tabelle sind die von der Sun Java Enterprise System 5-Version unterstützten Browser aufgelistet.

TABELLE 1–2 Unterstützte Browser

Browser	Plattform
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

Allgemeine Kompatibilitätsoptionen

Legacy-Modus von Access Manager

Wenn Sie Access Manager mit Sun Java System Portal Server installieren, müssen Sie den Access Manager Legacy (6.x)-Modus auswählen:Weitere Informationen zum Modus einer Access Manager 7.1-Installation finden Sie unter „Ermitteln des Access Manager-Modus” auf Seite 12.

Option "Automatisch während der Installation konfigurieren"

Wenn Java ES Installer im Grafikmodus mit der Option zum automatischen Konfigurieren während der Installation ausgeführt wird, wird Access Manager im Modus "Legacy (Version 6.x)" konfiguriert.

Option "Manuell nach der Installation konfigurieren"

Wenn Sie Java ES Installer mit der Installationsoption "Manuell nach der Installation konfigurieren" ausgeführt haben, müssen Sie die Datei `install-dir\identity\setup\amconfig.bat` ausführen, um Access Manager nach der Installation zu konfigurieren. Um den Legacy-Modus (6.x) auszuwählen, legen Sie den folgenden Parameter in der Konfigurationsdatei fest

```
AM_REALM = disabled

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

Ermitteln des Access Manager-Modus

Um zu ermitteln, ob eine ausgeführte Access Manager 7.1-Installation im Realm- oder Legacy-Modus konfiguriert wurde, geben Sie Folgendes ein:

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

Ein Rückgabewert `true` deutet auf den Realm-Modus hin. Ein Rückgabewert `false` deutet auf den Legacy-Modus hin.

Access Manager-Richtlinienagenten

In der folgenden Tabelle wird die Kompatibilität von Richtlinienagenten mit den Access Manager 7.1-Modi dargestellt.

TABELLE 1–3 Kompatibilität von Richtlinienagenten mit den Access Manager 7.1-Modi

Agent und Version	Kompatibler Modus
Web- und J2EE-Agenten, Version 2.2	Legacy- und Realm-Modus
Webagenten, Version 2.1	Legacy- und Realm-Modus
J2EE-Agenten, Version 2.1	Nur Legacy-Modus

Andere bekannte Probleme und Einschränkungen

In diesem Abschnitt werden die folgenden bekannten Probleme und ggf. Lösungen beschrieben, die zum Zeitpunkt der Veröffentlichung von Version 7.0 verfügbar waren.

Probleme bei der Installation

Die Installation von Access Manager in einer vorhandenen DIT erfordert den erneuten Aufbau der Directory Server-Indizes (6268096)

Um die Suchleistung zu verbessern, verfügt Directory Server über mehrere neue Indizes.

Lösung: Nachdem Sie Access Manager mit einer vorhandenen Verzeichnisinformationsstruktur Directory Information Tree (DIT) installiert haben, erstellen Sie die Directory Server-Indizes neu, indem Sie das `db2index.pl`-Skript ausführen. Zum Beispiel:

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

Das `db2index.pl`-Skript ist im Verzeichnis *DS-install-directory*`/`*slapd-hostname* verfügbar.

Der Authentifizierungsdienst wird nicht initialisiert, wenn Access Manager und Directory Server auf demselben Computer installiert werden (6229897)

Obwohl `classpath` und andere Access Manager-Web-Container-Umgebungsvariablen während der Installation aktualisiert wurden, wird der Web-Container durch den Installationsvorgang nicht neu gestartet. Wenn Sie versuchen, sich bei Access Manager anzumelden, nachdem der Web-Container gestartet wurde, wird der folgende Fehler zurückgegeben:

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

Lösung: Starten Sie den Web-Container neu, bevor Sie sich bei Access Manager anmelden. Außerdem muss Directory Server ausgeführt werden, bevor Sie sich anmelden.

Probleme bei der Aktualisierung

- „Portal Server und Web Console funktionieren nicht nach dem Upgrade von Java ES 4 Access Manager auf Java ES 5 Access Manager (6515054)" auf Seite 14

Portal Server und Web Console funktionieren nicht nach dem Upgrade von Java ES 4 Access Manager auf Java ES 5 Access Manager (6515054)

Nach dem Upgrade von Java ES 5 Access Manager auf Java ES 5 Access Manager funktionieren die installierten Anwendungen, Portal Server und die Web-Konsole nicht.

Lösung: Kopieren Sie die Datei `config.properties` aus dem Java ES 5-Installationsverzeichnis in das Java ES 4-Installationsverzeichnis:

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

Konfigurationsprobleme

Active Perl 5.8 oder höher ist erforderlich zum Konfigurieren bestimmter Access Manager-Module

Active Perl 5.8 oder höher muss installiert sein, um die folgenden Komponenten mit Access Manager zu konfigurieren:

- MFWK
- Sitzungs-Failover
- Bulk Federation
- Einstellungen zur Leistungsoptimierung

Sie können Active Perl herunterladen von `http://www.activestate.com/Products/ActivePerl/`.

Installer kann die verteilte Authentifizierung und die Client-SDK-Komponenten nicht konfigurieren

Im Modus "Automatisch während der Installation konfigurieren" werden die verteilte Authentifizierung und die Client-SDK-Komponenten nicht konfiguriert. Es wird keine Fehlermeldung angezeigt.

Lösung: Verwenden Sie die Option "Manuell nach der Installation konfigurieren" während der Installation und konfigurieren Sie die verteilte Authentifizierung und die SDK-Komponenten nach der Installation.

`am2bak.bat` und `bak2am.bat`-Dateien werden nicht richtig generiert (6491091)

Access Manager 7.1 unterstützt nicht die Dienstprogramme für die Sicherung (`am2bak.bat`) und die Wiederherstellung (`bak2am.bat`).

Lösung: Keine.

Benutzerkonto wird nach vielen aufeinander folgenden Anmeldungen nicht deaktiviert (6469200)

Benutzerkonto wird nach mehreren erfolglosen Anmeldungen bei Access Manager nicht deaktiviert.

Lösung: Verwenden Sie die Realm-Administrationskonsole (`\amserver\console`), um das Sperrdienstprogramm zu aktivieren oder deaktivieren. Um den Anmeldefehler-Sperrmodus zu aktivieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Access Manager-GUI.
2. Wählen Sie einen Bereich, um das Sperren zu ermöglichen.
3. Wählen Sie die Registerkarte "Authentifizierung".
4. Klicken Sie auf die Schaltfläche "Erweiterte Eigenschaften".
5. Wählen Sie das Attribut "Anmeldefehler Sperrmodus".
6. Speichern Sie die Eigenschaften, indem Sie auf die Schaltfläche "Speichern" klicken.

Probleme mit Access Manager Console

Die neue Access Manager-Konsole kann keine CoS-Vorlagenprioritäten festlegen (6309262)

Die neue Access Manager 7.1 Console kann keine Class of Service (CoS)-Vorlagenpriorität festlegen oder ändern.

Lösung: Melden Sie sich an der Access Manager 6 2005Q1 Console an, um eine CoS-Vorlagenpriorität festzulegen oder zu ändern.

Beim Hinzufügen von Portal Server-verwandten Diensten wird die alte Konsole angezeigt (6293299)

Portal Server und Access Manager werden auf demselben Server installiert. Bei der Installation von Access Manager im Legacy-Modus melden Sie sich unter Verwendung von `/amserver` an der neuen Access Manager Console an. Wenn Sie einen bereits vorhandenen Benutzer wählen und versuchen, Dienste (wie NetFile oder Netlet) hinzuzufügen, wird plötzlich die alte Access Manager Console (`/amconsle`) angezeigt.

Lösung: Keine. Für die aktuelle Version von Portal Server ist die Access Manager 6 2005Q1 Console erforderlich.

Console gibt nicht die Ergebnisse aus, die von Directory Server nach Erreichen des Ressourcenlimits festgelegt wurden (6239724)

In der folgenden Situation zeigt Console nicht die richtigen Informationen an: Installieren Sie Directory Server und dann Access Manager mit der bereits vorhandenen DIT-Option. Melden Sie sich an der Access Manager Console an und erstellen Sie eine Gruppe. Bearbeiten Sie Benutzer in der Gruppe. Fügen Sie z. B. Benutzer mit dem Filter `uid=*999*` hinzu. Das resultierende Listenfeld ist leer und die Konsole zeigt keinen Fehler, keine Informationen und keine Warnmeldungen an.

Lösung: Die Gruppenmitgliedschaft darf die Directory Server-Suchgrößenbeschränkung nicht überschreiten. Ist die Gruppenmitgliedschaft größer, müssen Sie die Suchgrößenbeschränkung entsprechend ändern.

SDK- und Client-Probleme

Über das Portal kann nicht derselbe gelöschte Benutzer erstellt werden (6479611)

Sie können nicht dasselbe gelöschte Benutzerprofil über das Portal erstellen. Die folgende Fehlermeldung wird angezeigt:

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

Lösung: Keine.

Die Clients erhalten nach dem Serverneustart keine Benachrichtigungen (6309161)

Anwendungen, die mit dem Client-SDK (`amclientsdk.jar`) geschrieben wurden, erhalten bei einem Serverneustart keine Benachrichtigungen.

Lösung: Keine.

SDK-Clients müssen nach Dienstschemaänderung neu gestartet werden (6292616)

Beim Ändern eines Dienstschemas gibt `ServiceSchema.getGlobalSchema` das alte Schema, nicht das neue Schema zurück.

Lösung: Starten Sie den Client nach einer Dienstschemaänderung neu.

Sitzungs- und SSO-Probleme

Verwendung von `HttpSession` mit Webcontainern anderer Hersteller

Als Standardmethode für das Aufrechterhalten von Sitzungen für Authentifizierungen ist "interne Sitzung" und nicht `HttpSession` festgelegt. Der standardmäßige Wert von drei Minuten für die maximale Dauer einer Sitzung, bevor diese ungültig wird, ist ausreichend. Das Skript `amtune` legt für den Web Server und Application Server einen Wert von einer Minute fest. Wenn Sie jedoch einen Drittanbieter-Container (IBM WebSphere oder BEA WebLogic Server) und die Option `HttpSession` verwenden, müssen Sie die maximale `HttpSession`-Dauer des Webcontainers möglicherweise einschränken, um Leistungsprobleme zu vermeiden.

Richtlinienprobleme

Das Löschen der dynamischen Attribute im Policy Configuration Service führen zu Problemen beim Bearbeiten der Richtlinien (6299074)

Das Löschen der dynamischen Attribute im Policy Configuration Service führt zu Problemen beim Bearbeiten der Richtlinien für das folgende Szenario:

1. Erstellen Sie zwei dynamische Attribute im Policy Configuration Service.
2. Erstellen Sie eine Richtlinie und wählen Sie die neu erstellten dynamischen Attribute im Antwort-Anbieter aus.
3. Entfernen Sie die dynamischen Attribute im Policy Configuration Service und erstellen Sie zwei weitere Attribute.
4. Versuchen Sie, die in Schritt 2 erstellte Richtlinie zu bearbeiten.

Die folgende Fehlermeldung wird angezeigt: Fehlermeldung, dass eine ungültige dynamische Eigenschaft festgelegt wurdeEs werden standardmäßig keine Richtlinien in der Liste angezeigt. Nach einer Suche werden die Richtlinien angezeigt. Sie können die bereits vorhandenen Richtlinien jedoch nicht bearbeiten oder löschen oder eine neue Richtlinie erstellen.

Lösung: Bevor Sie die dynamischen Attribute aus dem Policy Configuration Service entfernen, müssen Sie die Verweise auf diese Attribute aus den Richtlinien entfernen.

Probleme beim Starten des Servers

Debug-Fehler tritt beim Starten von Access Manager auf (6309274, 6308646)

Beim Starten von Access Manager 7.1 werden in den Debug-Dateien `amDelegation` und `amProfile` Debug-Fehler ausgegeben:

- `amDelegation`: Kann keine Plugin-Instanz zur Delegation abrufen
- `amProfile`: Bekommt Delegationsausnahme

Lösung: Keine. Sie können diese Meldungen ignorieren.

Verbund- und SAML-Probleme

Der Verbund schlägt bei der Verwendung eines Artifact-Profils fehl (6324056)

Wenn Sie einen Identitätsanbieter (IDP) und einen Dienstanbieter (SP) einrichten, das Kommunikationsprotokoll für die Verwendung des Browser-Artifact-Profils ändern und dann versuchen, die Benutzer zwischen dem IDP und SP zu verbinden, schlägt dies fehl.

Lösung: Keine.

Im Verbund tritt ein Abmeldefehler auf (6291744)

Wenn Sie im Realm-Modus Benutzerkonten für einen Identitätsanbieter (IDP) und einen Dienstanbieter (SP) verbinden, den Verbund dann beenden und sich abmelden, wird die folgende Fehlermeldung angezeigt: Fehler: Es wurde keine untergeordnete Organisation gefunden.

Lösung: Keine.

Globalisierungsprobleme (g11n)

Ein Anwendungsfehler wird im linken Bereich der Online-Hilfe der Realm-Konsole angezeigt (6508103)

Wenn Access Manager auf Application Server installiert ist, wird im linken Bereich der Online-Hilfe auf der Realm-Konsole ein Anwendungsfehler angezeigt.

Lösung: Gehen Sie wie folgt vor:

1. Kopieren Sie die Datei `jhall.jar`.

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

2. Starten Sie Application Server neu.

Entfernen von UTF-8 schlägt in Client Detection fehl (5028779)

Die Client Detection-Funktion funktioniert nicht ordnungsgemäß. Änderungen an Access Manager 7.1 Console werden nicht automatisch im Browser übernommen.

Lösung: Versuchen Sie die folgende Lösung:

1. Starten Sie den Access Manager-Webcontainer neu, nachdem Sie im Client Detection-Abschnitt eine Änderung vorgenommen haben.
2. Führen Sie die folgenden Schritte durch in Access Manager Console:
   a. Klicken Sie auf der Registerkarte `Konfiguration` auf `Client-Erkennung`.
   b. Klicken Sie auf den Link `Bearbeiten` für `genericHTML`.
   c. Klicken Sie auf der Registerkarte "HTML" auf den Link `genericHTML`.
   d. Nehmen Sie in der Zeichensatzliste den folgenden Eintrag vor: `UTF-8;q=0.5` (Stellen Sie sicher, dass der UTF-Faktor `q` niedriger als die anderen Zeichensätze für Ihr Gebietsschema ist.)
   e. Klicken Sie auf "Speichern„.
   f. Melden Sie sich ab und wieder an.

Mehrfachbyte-Zeichen werden in den Protokolldateien als Fragezeichen angezeigt (5014120)

Mehrfachbyte-Nachrichten in Protokolldateien im Verzeichnis `install_dir\identity\logs` werden als Fragezeichen (?) angezeigt. Die Protokolldateien liegen in der nativen Codierung und nicht immer als UTF-8 vor. Wenn eine Webcontainerinstanz unter einer bestimmten Ländereinstellung gestartet wird, liegen die Protokolldateien für diese Ländereinstellung in der nativen Codierung vor. Wenn Sie zu einer anderen Ländereinstellung wechseln und die Webcontainerinstanz neu starten, liegen alle weiteren Nachrichten für die aktuelle Ländereinstellung in der nativen Codierung vor, die Nachrichten aus früheren Codierungen werden jedoch als Fragezeichen angezeigt.

Lösung: Stellen Sie sicher, dass Sie die Webcontainerinstanzen immer mit derselben nativen Codierung starten.

Dokumentationsprobleme

Beschreibung der Unterstützung für Rollen und gefilterte Rolle für das LDAPv3-Plugin (6365196)

Nach Anwendung des entsprechenden Patches können Sie Rollen und gefilterte Rollen für das LDAPv3-Plugin konfigurieren, wenn die Daten in Sun Java System Directory Server gespeichert sind.

1. Öffnen Sie die Access Manager 7.1 Administrator Console.
2. Wählen Sie LDAPv3-Konfiguration.
3. Geben Sie im Feld "LDAPv3 Plugin Supported Types and Operations" die folgenden Werte abhängig von den Rollen und gefilterten Rollen ein, die Sie in der LDAPv3-Konfiguration verwenden möchten:

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

Beschreibung nicht verwendeter Eigenschaften in der Datei `AMConfig.properties` (6344530)

Die folgenden Eigenschaften in der Datei `AMConfig.properties` werden nicht verwendet:

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

Beschreibung der Aktivierung der XML-Verschlüsselung (6275563)

Um die XML-Verschlüsselung zu aktivieren, führen Sie die folgenden Schritte aus:

1. (Optional) Wenn Sie eine ältere JDK-Version als 1.5 verwenden:,
   a. laden Sie den Bouncy Castle JCE-Anbieter von der Bouncy Castle-Site herunter (`http://www.bouncycastle.org/`).

      Wenn Sie beispielsweise JDK 1.4 verwenden, laden Sie die Datei `bcprov-jdk14-131.jar` herunter.

   b. Kopieren Sie die Datei in das Verzeichnis *jdk_root*`\jre\lib\ext` herunter.
2. Laden Sie die JCE Unlimited Strength Jurisdiction Policy-Dateien für Ihre JDK-Version herunter.
   - Laden Sie für Sun Systems die Dateien von der Sun-Website (`http://java.sun.com`) für Ihre JDK-Version herunter.
   - Laden Sie für IBM WebSphere die erforderlichen Dateien von der IMB-Website herunter.
3. Kopieren Sie die heruntergeladenen `US_export_policy.jar`/ und `local_policy.jar`-Dateien in das Verzeichnis *jdk_root*`\jre\lib\security`.
4. Wenn Sie eine ältere JDK-Version als JDK 1.5 verwenden, bearbeiten Sie die Datei *jdk_root*`\jre\lib\security\java.security` und fügen Sie Bouncy Castle als einen der Anbieter hinzu. Zum Beispiel:

   ```
   security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider
   ```
5. Legen Sie in der Datei `AMConfig.properties` folgende Eigenschaft als true fest:

   ```
   com.sun.identity.jss.donotInstallAtHighestPriority=true
   ```
6. Starten Sie den Access Manager-Webcontainer neu.

Weitere Informationen erhalten Sie unter der Problemnummer 5110285 (XML-Verschlüsselung erfordert Bouncy Castle-JAR-Datei).

Dokumentationsaktualisierungen

Diese Dokumente finden Sie in der Access Manager 7.1-Sammlung unter `http://docs.sun.com/coll/1292.1`

Die Sun Java System Access Manager Richtlinien-Agenten 2.2-Sammlung beinhaltet nun auch eine Dokumentation zu den neuen Agenten: `http://docs.sun.com/coll/1322.1`

Weitervertreibbare Dateien

Sun Java System Access Manager 7.1 enthält keine Dateien, die Sie an nicht lizenzierte Benutzer des Produkts weitervertreiben können.

So melden Sie Probleme und liefern Feedback

Wenn Sie mit Access Manager oder Sun Java Enterprise System Probleme haben, wenden Sie sich an den Kundensupport von Sun. Dazu stehen folgende Möglichkeiten zur Auswahl:

- Sun Support Resources-Dienste (SunSolve) unter `http://sunsolve.sun.com/`.

  Diese Site bietet Links zur Knowledge Base, zum Online Support Center und ProductTracker sowie zu Wartungsprogrammen und Supportkontaktnummern.
- Die Telefonnummer aus Ihrem Wartungsvertrag

Damit wir Ihnen unmittelbar Hilfe anbieten können, halten Sie die folgenden Informationen bereit, wenn Sie sich an den Support wenden:

- Beschreibung des Problems, u. a. der Situation, in der das Problem auftrat, und seiner Auswirkungen auf den Betrieb
- Computertyp, Betriebssystem- und Produktversion, u. a. Patches und andere Software, die eventuell das Problem verursachten
- Detaillierte Schritte zu den von Ihnen verwendeten Methoden, um das Problem zu reproduzieren
- Sämtliche Fehlerprotokolle oder Kernspeicher

Sun freut sich über Ihre Kommentare

Sun ist immer interessiert an Vorschlägen oder Kommentaren zur Dokumentationsverbesserung. Klicken Sie unter `http://docs.sun.com/` auf "Send Comments".

Geben Sie in den entsprechenden Feldern den vollständigen Dokumenttitel sowie die Teilenummer ein. Die Teilenummer besteht aus einer sieben- oder neunstelligen Zahl, die sich auf der Titelseite des Buchs oder oben im Dokument befindet. Die Teilenummer von *Access Manager Versionshinweise* lautet z. B. 819-5686.

Weitere Quellen von Sun

Unter folgenden Adressen finden Sie nützliche Access Manager-Informationen und Ressourcen:

- Sun Java Enterprise System Documentation: `http://docs.sun.com/prod/entsys.05q4`
- Sun Services: `http://www.sun.com/service/consulting/`
- Software Products and Service: `http://wwws.sun.com/software/`
- Support Resources `http://sunsolve.sun.com/`
- Developer Information: `http://developers.sun.com/`
- Sun Developer Support Services: `http://www.sun.com/developers/support/`

Zugriffsfunktionen für Personen mit Einschränkungen

Um Eingabehilfen zu erhalten, die seit der Veröffentlichung dieses Dokuments auf den Markt gekommen sind, lesen Sie Abschnitt 508 der Produktbewertungen, die Sie bei Sun anfordern können, um zu ermitteln, welche Versionen am besten geeignet sind. Die aktualisierten Versionen von Anwendungen finden Sie unter `http://sun.com/software/javaenterprisesystem/get.html`.

Informationen zum Engagement von Sun für Eingabehilfen finden Sie unter `http://sun.com/access`.

Verwandte Websites von Drittanbietern

In diesem Dokument wird auf Drittanbieter-URLs verwiesen, die zusätzliche verwandte Informationen liefern.

Hinweis – Sun ist nicht verantwortlich für die Verfügbarkeit von Drittpartei-Websites, die in diesem Dokument genannt werden. Sun unterstützt keinen Inhalt, keine Werbung, Produkte oder andere Materialien, die auf oder über solche Websites oder Ressourcen zur Verfügung stehen, und ist dafür weder verantwortlich noch haftbar. Sun ist für keinen tatsächlichen oder angeblichen Schaden oder Verlust verantwortlich oder haftbar, der verursacht wird durch oder in Verbindung steht mit der Verwendung oder der Verlässlichkeit auf solchen Inhalt, solche Waren oder Dienstleistungen, die auf oder über solche Websites oder Ressourcen zur Verfügung stehen.
