Sun Java System Access Manager 7 2005Q4 Versionshinweise

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

Teilenr.: 819–3479
19. August 2008

080915@20795

Inhalt

Sun Java System Access Manager 7 2005Q4 Versionshinweise

19. August 2008

Teilenr. 819-3479

Die Sun Java™ System Access Manager (Access Manager) 7 2005Q4 Versionshinweise enthalten wichtige Informationen, die für die Herausgabe von Sun Java Enterprise System (Java ES) zur Verfügung stehen, einschließlich neuer Access Manager-Funktionen und bekannter Probleme mit Lösungen, falls vorhanden. Lesen Sie dieses Dokument, bevor Sie diese Version installieren und verwenden.

Informationen zu dieser Ausgabe der Versionshinweise finden Sie im "Änderungsprotokoll" auf Seite 6.

Die Produktdokumentation zu Java ES, einschließlich der Access Manager-Sammlung, finden Sie unter `http://docs.sun.com/prod/entsys.05q4`.

Schauen Sie auf dieser Website nach, bevor Sie die Software installieren und einrichten und dann in regelmäßigen Abständen, um die aktuellste Dokumentation einzusehen.

Inhalt

Die Access Manager 7 2005Q4 Versionshinweise enthalten die folgenden Abschnitte:

Änderungsprotokoll

Die folgende Tabelle enthält das Änderungsprotokoll der Access Manager 7 2005Q4 Versionshinweise.

TABELLE 1 Änderungsprotokoll

Datum	Beschreibung der Änderungen
19. August 2008	Informationen zu Patch 7 für Windows und HP-UX-Systeme in Abschnitt "Access Manager 7 2005Q4 Patch-Versionen" auf Seite 10 hinzugefügt.
12. Mai 2008	■ Informationen zu Patch 7 in Abschnitt "Access Manager 7 2005Q4 Patch-Versionen" auf Seite 10 hinzugefügt. ■ Abschnitt "Unterstützung für Systemvirtualisierung" auf Seite 76 hinzugefügt.
16. Oktober 2007	Bei dieser Überarbeitung vorgenommene Änderungen: ■ Informationen zu Patch 6 in Abschnitt "Access Manager 7 2005Q4 Patch-Versionen" auf Seite 10 hinzugefügt. ■ "CR# 6522720: Suchvorgänge in der Onlinehilfe der Konsole funktionieren unter Windows- und HP-UX-Systemen nicht für Multibyte-Zeichen." auf Seite 46 aktualisiert. Patch 6 behebt dieses Problem auf Windows-Systemen. Auf HP-UX-Systemen besteht das Problem weiterhin.
10. Juli 2007	Bei dieser Überarbeitung vorgenommene Änderungen: ■ Informationen zu Patch 126371-05 für HP-UX-Systeme in Abschnitt "Access Manager 7 2005Q4 Patch-Versionen" auf Seite 10 hinzugefügt. ■ Informationen zum folgenden neuen Problem hinzugefügt: "Die Suche nach Null-Attributen gibt einen Fehler zurück, wenn Access Manager auf Directory Proxy (6357975) verweist." auf Seite 94.

TABELLE 1 Änderungsprotokoll *(Fortsetzung)*

Datum	Beschreibung der Änderungen
16. März 2007	Bei dieser Überarbeitung vorgenommene Änderungen: ■ Informationen zu Patch 5 in Abschnitt "Access Manager 7 2005Q4 Patch-Versionen" auf Seite 10 hinzugefügt. ■ Erläuterungen und neue Informationen unter "Dokumentationsprobleme" auf Seite 104 hinzugefügt. ■ Verschiedene technische und redaktionelle Änderungen nach Review und entsprechend der Änderungsanfragen (Change Requests, CRs) vorgenommen.
30. Oktober 2006	Folgende Änderungen wurden im Abschnitt "Access Manager 7 2005Q4 Patch-Versionen" auf Seite 10 vorgenommen: ■ Informationen zu Patch 4 hinzugefügt. ■ Inkonsistente Verwendung von *AccessManager-base* korrigiert. ■ Beschreibung unter "Cookie-Wiedergabe erfordert Eigenschaft `com.sun.identity.session.resetLBCookie` (6440651)" auf Seite 57 überarbeitet.
25. August 2006	Folgende Änderungen wurden im Abschnitt "Access Manager 7 2005Q4 Patch-Versionen" auf Seite 10 vorgenommen: ■ Informationen zu Patch 3 hinzugefügt. ■ Informationen zu Patch 1 und 2 überarbeitet und neue Informationen zu diesen Patches hinzugefügt.

25. Mai 2006	Bei dieser Überarbeitung vorgenommene Änderungen:
	■ Neuer Abschnitt "Access Manager 7 2005Q4-Patch 2" auf Seite 60 hinzugefügt.
	■ Informationen zur Unterstützung der HP-UX- und Microsoft Windows-Plattformen zur Tabelle 4 hinzugefügt.
	■ Folgende Probleme wurden unter "Dokumentationsprobleme" auf Seite 104 hinzugefügt:
	  ■ "Versionshinweise enthalten falsche Lösung für ein bekanntes Problem (6422907)" auf Seite 110
	  ■ "Dokument `com.iplanet.am.session.protectedPropertiesList` in `AMConfig.properties` (6351192)" auf Seite 110

9. Februar 2006	Abschnitt "Dokumentationsaktualisierungen" auf Seite 112 um eine Liste mit den neuen und überarbeiteten Dokumenten zu Access Manager 7 2005Q4 erweitert, die seit der Erstausgabe veröffentlicht wurden.

TABELLE 1 Änderungsprotokoll *(Fortsetzung)*

Datum	Beschreibung der Änderungen
7. Februar 2006	Bei dieser Überarbeitung vorgenommene Änderungen: ■ Folgende Abschnitte unter "Bekannte Probleme und Einschränkungen" auf Seite 79 hinzugefügt: ■ "Der Authentifizierungsdienst wird nicht initialisiert, wenn Access Manager und Directory Server auf unterschiedlichen Computern installiert sind. (6229897)" auf Seite 83 ■ "Access Manager-Skript `ampre70upgrade` entfernt lokalisierte Pakete nicht (6378444)" auf Seite 84 ■ Abschnitt "Dokumentationsaktualisierungen" auf Seite 112 aktualisiert.

TABELLE 1 Änderungsprotokoll *(Fortsetzung)*

Datum	Beschreibung der Änderungen
18. Januar 2006	Bei dieser Überarbeitung vorgenommene Änderungen: ■ Neuer Abschnitt "Access Manager 7 2005Q4-Patch 1" auf Seite 66 hinzugefügt. ■ Beschreibung unter "Verteilte Authentifizierung" auf Seite 71 überarbeitet. ■ Beschreibung der Unterstützung für Solaris 10-Zonen überarbeitet und Beschreibung der Unterstützung für Solaris 10 OS auf AMD64-Plattformen unter "Hardware- und Software-Anforderungen" auf Seite 74 hinzugefügt. ■ Folgende Abschnitte unter "Bekannte Probleme und Einschränkungen" auf Seite 79 hinzugefügt: ■ "URL-Signierung in IBM WebSphere bei Verwendung des RSA-Schlüssels schlägt fehl (6271087)" auf Seite 90 ■ "JVM-Probleme treten auf, wenn Access Manager auf Application Server ausgeführt wird (6223676)." auf Seite 100 ■ "Ausführen des Webdienstes gibt Fehler "Ressourcenangebot nicht gefunden" zurück (6359900)" auf Seite 100 ■ "Nach Anwendung von Patch 1 haben alle Benutzer Lesezugriff auf die Datei `/tmp/amsilent` (6370691)" auf Seite 82 ■ "Attribut `ContainerDefaultTemplateRole` nach Datenmigration hinzufügen (4677779)" auf Seite 86 ■ "Beschreibung der Unterstützung für Rollen und gefilterte Rolle für das LDAPv3-Plugin (6365196)" auf Seite 110 ■ "Beschreibung nicht verwendeter Eigenschaften in der Datei `AMConfig.properties` (6344530)" auf Seite 111 ■ "Beschreibung der Aktivierung der XML-Verschlüsselung (6275563)" auf Seite 111 ■ Neuer Abschnitt "Dokumentationsaktualisierungen" auf Seite 112 hinzugefügt.
8. November 2005	Abschnitt "Identitätsrepository" auf Seite 68 überarbeitet und Informationen zu den unterstützten, mit der LDAP-Version 3 (LDAP v3) konformen Repositories hinzugefügt.
3. Oktober 2005	Erstausgabe.
30. Juni 2005	Beta-Release.

Informationen zu Sun Java System Access Manager 7 2005Q4

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.

Access Manager 7 2005Q4 Patch-Versionen

Die aktuellen Überarbeitungen der Access Manager 7 2005Q4-Patches stehen unter SunSolve Online zum Download bereit: `http://sunsolve.sun.com`. Die aktuellen Patch-IDs lauten:

- Solaris™-Betriebssystem (Solaris OS) auf SPARC®-basierten Systemen **120954-07**
- Solaris OS auf x86-Plattformen: **120955-07**
- Linux-Systeme: **120956-07**
- Microsoft Windows-Systeme: **124296-07**
- HP-UX-Systeme: **126371-07**

Hinweis – Access Manager 7 2005Q4-Patches sind kumulativ. Sie können Patch 7 installieren, ohne zunächst Patch 1, 2, 3, 4, 5 oder 6 installieren zu müssen. Wenn Sie jedoch einen der früheren Patches nicht installiert haben, sollten Sie die Informationen zu neuen Funktionen und Problemen in den entsprechenden Abschnitten lesen, um festzustellen, ob die neuen Funktionen bzw. Probleme für Sie relevant sind.

Folgende Informationen zu Access Manager 7 2005Q4-Patches sind enthalten:

Access Manager 7 2005Q4 Patch 7

Access Manager 7-Patch 7 (Überarbeitung 07) behebt eine Reihe von Problemen, die in der README-Datei zum Patch aufgeführt sind.

Patch 7 enthält folgende Änderungen:

CR# 6637806: Nach dem Neustart sendete Access Manager ein ungültiges Anwendungs-SSO-Token an einen Agenten

Nach einem Neustart eines Access Manager-Servers sendet das Access Manager-Client-SDK jetzt eine sinnvolle Ausnahme an einen Agenten, sodass der Agent sich selbst erneut authentifizieren kann und eine neue Anwendungssitzung gestartet werden kann. Bisher sendete das Access Manager-Client-SDK nach der Anwendung von Access Manager 7 2005Q4 Patch 5 im Anschluss an einen Neustart des Access Manager-Servers ein ungültiges Anwendungs-SSO-Token an den Agenten.

Dieses Problem wurde durch CR 6496155 behoben. Patch 7 bietet auch eine Option (Eigenschaft `comp.iplanet.dpro.session.dnRestrictionOnly`) zum Senden des Anwendungs-SSO-Token in einem eingeschränkten Kontext. Standardmäßig senden Agenten die IP-Adresse des Servers, auf dem sie installiert sind. Wenn jedoch strenge DN-Prüfungen erforderlich sind, legen Sie diese Eigenschaft in der Datei `AMConfig.properties` wie folgt fest:

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

CR# 6612609: Sitzungsfailover funktioniert, wenn das Netzwerkkabel vom Message Queue-Server getrennt ist

Wenn bei einer Sitzungsfailover-Bereitstellung jede Access Manager-Instanz und der Message Queue-Broker auf demselben Server installiert sind, funktioniert das Sitzungs-Failover jetzt, wenn ein Netzwerkkabel nicht an einen der Server angeschlossen ist. Standardmäßig ist das

Verbindungsfactory-Attribut `imqAddressListBehavior` der Nachrichtenwarteschlange auf `PRIORITY` gesetzt, was bewirkt, dass die Adressen in der Reihenfolge ausprobiert werden, in der Sie in der Broker-Adressenliste aufgeführt sind (Beispiel: `localhost:7777,server2:7777,server3:7777`). Wenn das Attribut auf `RANDOM` gesetzt ist, werden für in den Versuchen die Adressen in einer zufälligen Reihenfolge verwendet.

Um dieses Attribut auf RANDOM zu setzen, legen Sie im Skript `amsessiondb` folgenden Parameter fest:

```
-DimqAddressListBehavior=RANDOM
```

Informationen zu den Attributen `PRIORITY` und `RANDOM` der Nachrichtenwarteschlange finden Sie im "Broker Address List" in *Sun Java System Message Queue 3.7 UR1 Administration Guide*.

CR# 6570409: Der Interaktionsdienst hinter dem Load Balancer funktioniert ordnungsgemäß als Identity-Anbieter

Bei einer Bereitstellung mit zwei Servern, die mit einem Load Balancer verbunden sind und als einzelner Identity-Anbieter fungieren, müssen Sie in der Datei `AMConfig.properties` folgende Eigenschaften festlegen:

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

Derzeit wird lediglich die Klasse `com.sun.identity.liberty.interaction.interactionConfigClass` unterstützt. Daher wird standardmäßig die mit Federation Liberty gebündelte Interations-Konfigurationsklasse für den Zugriff auf die Interaktions-Konfigurationsparameter verwendet.

CR# 6545176: Umleitungs-URLs können im SPI-Plugin für die Verarbeitung nach der Authentifzierung dynamisch festgelegt werden.

Umleitungs-URLs können jetzt in SPI-Plugins für die Verarbeitung nach der Authentifizierung für erfolgreiche und fehlgeschlagene Anmeldungen sowie für die Abmeldung dynamisch festgelegt werden. Wird ein Plugin für die Nachbearbeitung nicht ausgeführt, wird die Umleitungs-URL im Nachbearbeitungs-SPI nicht verwendet, und auf andere Weise angegebene Umleitungs-URLs werden wie zuvor ausgeführt.

Informationen hierzu finden Sie im Beispiel `com.iplanet.am.samples.authentication.spi.postprocess.ISAuthPostProcessSample.java`.

Aufgaben vor der Installation

- "Sichern von Dateien" auf Seite 13
- "Installation und Konfiguration von Access Manager" auf Seite 14

Sichern von Dateien

Wichtig Wenn Sie Dateien in Ihrer aktuellen Installation angepasst haben, sichern Sie diese Dateien, bevor Sie den Patch installieren. Vergleichen Sie nach der Patch-Installation die gesicherten Dateien mit den neuen von diesem Patch installierten Dateien, um die Anpassungen zu ermitteln. Nehmen Sie die Anpassungen in den neuen Dateien vor und speichern Sie die Dateien. Weitere Informationen zum Umgang mit angepassten Dateien finden Sie im folgenden Abschnitt.

Sichern Sie vor der Installation eines Patches auch die folgenden Dateien:

Solaris-Systeme	■ *AccessManager-base*/SUNWam/bin/amsfo ■ *AccessManager-base*/SUNWam/lib/amsfo.conf ■ Dateien im Verzeichnis /etc/opt/SUNWam/config/xml/template/: idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml, amAuth.xml , amSession.xml ■ Dateien im Verzeichnis *AccessManager-base*/SUNWam/locale/: amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties
Linux and HP-UX Systems	■ *AccessManager-base*/identity/bin/amsfo ■ *AccessManager-base*/identity/lib/amsfo.conf ■ Dateien im Verzeichnis /etc/opt/sun/identity/config/xml/template/: idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml , amAuth.xml, amSession.xml ■ Dateien im Verzeichnis *AccessManager-base*/identity/locale/: amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties

Windows-Systeme	■ *AccessManager-base*\identity\setup\AMConfigurator.properties ■ *AccessManager-base*\identity\bin\amsfo ■ *AccessManager-base*\identity\lib\amsfo.conf ■ Dateien im Verzeichnis *AccessManager-base*\identity\config\xml\template: idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml , amAuth.xml, amSession.xml ■ Dateien im Verzeichnis *AccessManager-base*\identity\locale: amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties

AccessManager-base ist das Basisinstallationsverzeichnis. Das standardmäßige Basis-Installationsverzeichnis ist plattformabhängig.

- Solaris-Systeme:/opt
- Linux- und HP-UX-Systeme: /opt/sun
- Windows-Systeme: *javaes-install-directory*\AccessManager. Beispiel: C:\Program Files\Sun\AccessManager

Installation und Konfiguration von Access Manager

Access Manager wird mit den in diesem Dokument beschriebenen Access Manager-Patches nicht installiert. Bevor Sie ein Patch anwenden, muss Access Manager 7 2005Q4 bereits auf dem Server installiert sein. Informationen zur Installation finden Sie im *Sun Java Enterprise System 2005Q4 Installationshandbuch für UNIX*.

Wenn Sie den Patch auf einem Windows-System installieren, lesen Sie das *Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows* .

Des Weiteren sollten Sie mit der Ausführung des Skripts amconfig für die Bereitstellung, erneute Bereitstellung und Konfiguration von Access Manager vertraut sein, wie in Kapitel 1, "Access Manager 7 2005Q4 Configuration Scripts" in *Sun Java System Access Manager 7 2005Q4 Administration Guide* beschrieben .

Eine Liste der Access Manager-Patches, die durch Anwendung dieses Patches nicht mehr aktuell sind, sowie aller anderen Patches, die Sie vor der Installation dieses Patches installieren müssen finden Sie in der README-Datei zu diesem Patch.

Achtung – Access Manager-Patches (so wie alle anderen Patches) sollten auf einem Test- oder Vorabbereitstellungssystem getestet werden, bevor Sie in einer Produktionsumgebung eingesetzt werden. Darüber hinaus werden Ihre angepassten JSP-Dateien möglicherweise vom Patch-Installationsprogramm nicht ordnungsgemäß aktualisiert. Sie müssen daher unter Umständen Änderungen an diesen Dateien manuell vornehmen, damit Access Manager ordnungsgemäß ausgeführt werden kann.

Patch-Installationsanweisungen

Patch-Installationsanweisungen für Solaris-Systeme

Stellen Sie vor der Installation des Solaris-Patches sicher, dass Sie die unter "Aufgaben vor der Installation" auf Seite 12 aufgelisteten Dateien gesichert haben.

Um auf Solaris-Systemen Patches hinzuzufügen oder zu entfernen, verwenden Sie die Befehle `patchadd` und `patchrm`, die mit dem Betriebssystem bereitgestellt werden.

patchadd-Befehl

Verwenden Sie den Befehl `patchadd`, um ein Patch auf einem Standalone-System zu installieren. Beispiel:

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

Hinweis – Wenn Sie den Solaris-Patch in einer globalen Solaris 10-Zone installieren, rufen Sie den Befehl `patchadd` mit dem Argument `-G` auf. Beispiel:

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

Das Skript `postpatch` zeigt eine Meldung zur erneuten Bereitstellung der Access Manager-Anwendungen an, mit Ausnahme für ein System, auf dem lediglich die Access Manager-SDK-Komponente installiert ist.

Das Skript `postpatch` erstellt die Datei `amsilent` in folgendem Verzeichnis:

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

AccessManager-base ist das Basisinstallationsverzeichnis. Das standardmäßige Basisinstallationsverzeichnis lautet `/opt` auf Solaris-Systemen und `/opt/sun` auf Linux-Systemen.

Die Datei `amsilent` basiert auf der Datei `amsamplesilent`, einige erforderliche Parameter sind jedoch entsprechend der auf dem System vorhandenen Access Manager-Konfigurationsdateien festgelegt. Die Passwortparameter enthalten jedoch Standardwerte. Kommentieren Sie den Wert für jeden Passwortparameter aus und ändern Sie die Werte. Überprüfen Sie sorgfältig die Werte der übrigen Parameter in dieser Datei entsprechend der Anforderungen Ihrer Bereitstellung.

Der Parameter `COMMON_DEPLOY_URI` (das URI-Präfix der gemeinsam genutzten Domänen-Webanwendung) enthält ebenfalls einen Standardwert. Wenn Sie für diesen URI einen anderen als den Standardwert verwenden möchten, müssen Sie diesen Wert aktualisieren. Anderenfalls schlägt die erneute Bereitstellung der Webanwendungen mit `amconfig` und der vom Patch erzeugten Datei `amsilent` fehl.

Führen Sie anschließend folgenden Befehl aus (in diesem Beispiel ist Access Manager im Standardverzeichnis installiert):

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

Achtung – Die Datei `amsilent` enthält vertrauliche Daten (z. B. das Administratorpasswort in Klartext). Stellen Sie daher sicher, dass Sie die Datei entsprechend Ihrer Bereitstellung ausreichend schützen.

Führen Sie nach der Ausführung des Skripts `amconfig` das Skript `updateschema.sh` aus, um die XML- und LDIF-Dateien zu laden. Das Skript `updateschema.sh` ist nach der Installation von Patch 7 in folgendem Verzeichnis verfügbar:

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

Starten Sie nach der Ausführung des Skripts `updateschema` die Access Manager-Prozesse neu. Beispiel:

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

Starten Sie anschließend den Access Manager-Webcontainer neu.

patchrm-Befehl

Um ein Patch aus einem Standalone-System zu entfernen, verwenden Sie den Befehl `patchrm`. Beispiel:

```
# patchrm 120954-03
```

Das Skript `backout` zeigt eine Meldung an, die in etwa dem Befehl `patchadd` entspricht, mit Ausnahme auf Systemen, auf denen lediglich die Access Manager-SDK-Komponente installiert ist.

Stellen Sie nach dem Entfernen des Patches die Access Manager-Anwendungen unter Verwendung der Datei `amsilent` im Verzeichnis *AccessManager-base* `/SUNWam` erneut bereit, wobei *AccessManager-base* das Basisinstallationsverzeichnis ist. Auf Solaris-Systemen lautet das standardmäßige Installationsverzeichnis `/opt`.

Legen Sie die Parameter in der Datei `amsilent` entsprechend der Anforderungen für Ihre Bereitstellung fest.

Führen Sie anschließend folgenden Befehl aus. In diesem Beispiel ist Access Manager im Standardverzeichnis für Solaris-Systeme installiert:

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

Weitere Informationen sowie Beispiele zu den Befehlen `patchadd` und `patchrm` finden Sie in den entsprechenden Solaris-`man`-Pages.

Weiterführende Informationen finden Sie außerdem unter “Aufgaben nach der Installation“ auf Seite 20.

Solaris 10-Zonen

Mit dem Solaris 10-Betriebssystem wurde das neue Zonenkonzept eingeführt. Daher enthält der "patchadd"-Befehl die neue Option `-G`, mit der ein Patch ausschließlich einer globalen Zone hinzugefügt wird. Der "patchadd"-Befehl sucht in "pkginfo" von Paketen, auf die der Patch angewendet werden soll, standardmäßig nach der Variable `SUNW_PKG_ALLZONES`. Da die Variable `SUNW_PKG_ALLZONES` jedoch nicht für alle Access Manager-Pakete festgelegt ist, ist die Option `-G` erforderlich, wenn Access Manager 7 2005Q4 in der globalen Zone installiert ist. Wenn Access Manager in einer lokalen Zone installiert ist, hat die Option `patchadd -G` keine Auswirkungen.

Wenn Sie Access Manager 7 2005Q4-Patches auf einem Solaris-System installieren, wird die Verwendung der Option `-G` empfohlen. Beispiel:

```
# patchadd -G AM7_patch_dir
```

Ebenso ist die Option `-G` für die Ausführung des Befehls `patchrm` erforderlich, wenn Access Manager in der globalen Zone installiert ist. Beispiel:

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

Patch-Installationsanweisungen für Linux-Systeme

Stellen Sie vor der Installation des Linux-Patches sicher, dass Sie die unter "Aufgaben vor der Installation" auf Seite 12 aufgelisteten Dateien gesichert haben.

Um ein Patch auf einem Standalone-Linux-System zu installieren, verwenden Sie den Befehl `installpatch`. Beispiel:

```
# ./installpatch
```

Das Skript `postpatch` gibt Meldungen aus, die in etwa den Meldungen auf einem Solaris-System entsprechen. Das Verfahren zum Rückgängigmachen eines Patches auf einem Linux-System unterscheidet sich jedoch von dem Verfahren auf Solaris-Systemen. Zum Rückgängigmachen eines Linux-Patches steht kein allgemeines Skript zur Verfügung. Wenn zuvor eine Vorgängerversion des Patches installiert war, installieren Sie diese Version erneut. Folgen Sie anschließend den "postpatch"-Anweisungen, um die Access Manager-Anwendungen durch Ausführung des Skripts `amconfig` erneut bereitzustellen.

Führen Sie nach der Ausführung des Skripts `amconfig` das Skript `updateschema.sh` (Patch 5 und zukünftige Patches) aus, um die XML- und LDIF-Dateien zu laden. Das Skript `updateschema.sh` ist nach der Installation von Patch 7 im Verzeichnis *patch-home-directory*`/120956-07/scripts` verfügbar.

Starten Sie nach der Ausführung der Skripte `amconfig` und `updateschema.sh` den Access Manager-Webcontainer neu.

Wenn der Patch auf der Access Manager 7 2005Q4 RTM-Version installiert wurde und Sie den Patch entfernen und den RTM-Status des Systems wiederherstellen möchten, müssen Sie die Access Manager RTM-Bestandteile mithilfe des Skripts `reinstallRTM` erneut installieren. Das Skript verwendet den Pfad zu dem Verzeichnis, in dem die Access Manager RTM-RPMs gespeichert sind und installiert die RTM-RPMs über die gepatchten RPMs. Beispiel:

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

Stellen Sie nach der Ausführung des Skripts `reinstallRTM` die Access Manager-Anwendungen durch Ausführung des Skripts `amconfig` erneut bereit und starten Sie den Webcontainer neu.

Weiterführende Informationen finden Sie außerdem unter "Aufgaben nach der Installation" auf Seite 20.

Patch-Installationsanweisungen für Windows-Systeme

Voraussetzungen für die Windows-Patch-Installation:

- Access Manager 7 2005Q4 muss auf dem Windows-System installiert sein. Informationen zur Installation finden Sie im *Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows* .

- Um die Patch-Skripte ausführen zu können, muss ActivePerl 5.8 (oder höher) auf dem Windows-System ausgeführt werden.

Installation des Windows-Patches

Stellen Sie vor der Installation des Windows-Patches sicher, dass Sie die unter "Aufgaben vor der Installation" auf Seite 12 aufgelisteten Dateien gesichert haben.

Verwenden Sie im Basisverzeichnispfad für die Eingabe in die Patch-Skripte einen Schrägstrich (`/`). Beispiel: `c:/sun`

So installieren Sie den Windows-Patch

1. Melden Sie sich am Windows-System als Mitglied der Administratorgruppe an.
2. Erstellen Sie ein Verzeichnis für das Herunterladen und Entzippen der Windows-Patch-Datei. Beispiel: `AM7p7`
3. Laden Sie die Datei `124296-07.zip` herunter und entzippen Sie die Datei im oben angegebenen Verzeichnis.
4. Beenden Sie alle Java ES 2005Q4-Dienste.
5. Führen Sie das Skript `AM7p7\scripts\prepatch.pl` aus.
6. Führen Sie `AM7p7\124296-07.exe` aus, um den Patch zu installieren.
7. Führen Sie das Skript `AM7p7\scripts\postpatch.pl` aus.
8. Starten Sie die Java ES 2005Q4-Dienste neu.
9. Stellen Sie die Access Manager-Anwendungen erneut bereit. Weitere Informationen finden Sie unter "Aufgaben nach der Installation" auf Seite 20.
10. Führen Sie das Skript `AM7p7\scripts\updateschema.pl` aus, um das Directory Server-Dienstschema zu aktualisieren. Ihre Angaben werden überprüft und die Dateien geladen. Das Skript erstellt außerdem folgende Protokolldatei:

    javaes-install-directory`\AccessManager\AM70Patch-upgrade-schema-` *timestamp*
11. Starten Sie die Java ES 2005Q4-Dienste neu.

Rückgängigmachen des Windows-Patches

So machen Sie den Windows-Patch rückgängig

1. Melden Sie sich am Windows-System als Mitglied der Administratorgruppe an.
2. Führen Sie die Datei `Uninstall_124296-07.bat` aus.
3. Führen Sie das Skript `AM7p7\scripts\postbackout.pl` aus.
4. Stellen Sie die Access Manager-Anwendungen erneut bereit.
5. Starten Sie die Java ES 2005Q4-Dienste neu.

Hinweis: Wenn Sie das Patch rückgängig machen, werden die vom Skript `AM7p7\scripts\updateschema.pl` vorgenommenen Schemaänderungen nicht aus Directory

Server entfernt. Sie müssen diese Änderungen jedoch nicht manuell entfernen, da die Änderungen die Funktionalität und Bedienbarkeit von Access Manager nicht beeinträchtigen, nachdem das Patch entfernt wurde.

Anweisungen zur Patch-Installation für HP-UX-Systeme

Um den HP-UX-Patch zu installieren oder zu entfernen, verwenden Sie den Befehl `swinstall` und `swremove` So installieren Sie den Patch beispielsweise auf einem Standalone-System

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

So entfernen Sie den Patch von einem Standalone-System

```
# swremove 126371-07
```

Informationen zu den Befehlen `swinstall` und `swremove` finden Sie in der Online-Dokumentation unter `swinstall` und `swremove`.

Nachdem Sie den Patch installiert oder entfernt haben, müssen Sie die Access Manager-Anwendungen wie im Abschnitt “Aufgaben nach der Installation“ auf Seite 20 erneut bereitstellen.

Führen Sie nach der erneuten Bereitstellung der Access Manager-Anwendungen das Skript`updateschema.sh` (Patch 5 und höhere Patches) aus, um die XML- und LDIF-Dateien zu laden. Das Skript updateschema.sh ist nach der Installation von Patch 7 im Verzeichnis *patch-home-directory*`/120956-07/scripts` verfügbar. Starten Sie nach der Ausführung der Skripte `amconfig` und `updateschema.sh` den Access Manager-Webcontainer neu.

Hinweis Wenn Sie den Patch entfernen, werden die vom Skript `updateschema.sh` vorgenommenen Schemaänderungen nicht aus Directory Server entfernt. Sie müssen diese Änderungen jedoch nicht manuell entfernen, da die Änderungen die Funktionalität und Bedienbarkeit von Access Manager nicht beeinträchtigen, nachdem der Patch entfernt wurde.

Weitere Informationen zur Bereitstellung von Access Manager auf HP-UX-Systemen finden Sie in den *Sun Java System Access Manager 7 2005Q4 Release Notes for HP-UX*.

Aufgaben nach der Installation

Folgendes ist nach der Installation eines Access Manager 7 2005Q4-Patches zu beachten:

- “Access Manager-Patches stellen keine Access Manager-Anwendungen in "postpatch"-Skripten bereit (6254355)“ auf Seite 21
- “Erneutes Bereitstellen der WAR-Dateien für verteilte Authentifizierung und Client SDK (6436409)“ auf Seite 23

Access Manager-Patches stellen keine Access Manager-Anwendungen in "postpatch"-Skripten bereit (6254355)

Das Patch-Installationsprogramm behält unter Umständen einige der angepassten WAR-Dateien nicht bei, sondern ersetzt diese durch nicht angepasste Dateiversionen. Um den angepassten Inhalt in WAR-Dateien zu ermitteln und manuell zu aktualisieren, wenden Sie folgendes Verfahren an.

In den folgenden Beispielen ist *AccessManager-base* das Basisinstallationsverzeichnis. Das standardmäßige Basisinstallationsverzeichnis lautet `/opt` auf Solaris-Systemen und `/opt/sun` auf Linux-Systemen.

Auf Windows-Systemen ist *AccessManager-base* das Verzeichnis *javaes-install-directory*`\AccessManager`. Beispiel: `C:\Program Files\Sun\AccessManager`

Der Patch wird auf folgende WAR-Dateien angewendet:

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

Diese Dateien befinden sich auf Solaris-Systemen im Verzeichnis *AccessManager-base*`/SUNWam` und auf Linux-Systemen im Verzeichnis *AccessManager-base*`/identity`.

Auf Windows-Systemen: Die zu patchenden WAR-Dateien befinden sich im Verzeichnis *AccessManager-base*`\`.

Folgender Inhalt kann in WAR-Dateien angepasst werden:

- Eigenschaftsdateien:
  - Solaris-Systeme: *AccessManager-base*`/SUNWam/locale/*.properties`
  - Linux-Systeme: *AccessManager-base*`/identity/locale/*.properties`
  - Windows-Systeme: *AccessManager-base*`\locale\*.properties`
- Tag-Bibliotheksdeskriptoren:
  - Solaris-Systeme: *AccessManager-base*`/SUNWam/web-src/applications/WEB-INF/*.tld`
  - Linux-Systeme: *AccessManager-base*`/identity/web-src/applications/WEB-INF/*.tld`
  - Windows-Systeme: *AccessManager-base*`\web-src\applications\WEB-INF\*.tld`
- Die Datei `web.xml` sowie die Dateien, die für ihre Erstellung verwendet wurden (`WEB-INF/web.xml` und `WEB-INF/*.xml`).
- Anwendungsspezifische Dateien: JSP-Dateien (`*.jsp`), Bilddateien (`*.gif`) und Stylesheet-Dateien mit Hintergrundfarben, Schriftgrößen usw. (`*.css`)

Um sicherzustellen, dass alle benutzerdefinierten Änderungen beibehalten werden, gehen Sie wie folgt vor: Bevor Sie eine Datei ändern, sichern Sie zuerst die Datei.

1. Installieren Sie den Patch.

2. Erweitern Sie die WAR-Dateien in einem temporären Verzeichnis. Beispiel mit Installation von Access Manager im Standardverzeichnis für Solaris-Systeme:

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

3. Überprüfen Sie die erweiterten Dateien, um festzustellen, ob das Patch-Installationsprogramm Änderungen an den von Ihnen angepassten Dateien vorgenommen hat. Nehmen Sie Ihre ursprünglichen Anpassungen an den geänderten Dateien im temporären Verzeichnis vor. Anpassungen in Dateien, die sich im Verzeichnis *AccessManager-base*`/web-src/` befinden, jedoch nicht zu den WAR-Dateien gehören, auf die der Patch angewendet wurde, müssen Sie nicht erneut vornehmen.

4. Aktualisieren Sie die WAR-Dateien mit den geänderten Dateien: Beispiel mit Installation von Access Manager im Standardverzeichnis für Solaris-Systeme:

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

   Zum Beispiel für Schritt 2-4:

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

5. Verwenden Sie erneut die vom Patch generierte automatische Konfigurationsdatei (`amsilent`) oder erstellen Sie basierend auf der Vorlagendatei `amsamplesilent` eine neue Konfigurationsdatei und legen Sie die entsprechenden Konfigurationsvariablen in der Datei fest, einschließlich:

   - `DEPLOY_LEVEL=21`
   - `DIRECTORY_MODE=5`
   - Passwörter für `DS_DIRMGRPASSWD`, `ADMINPASSWD` und `AMLDAPUSERPASSWD`
   - Access Manager-Webontainer-Variablen

   Verwenden Sie auf Windows-Systemen erneut die vom Skript `postpatch.pl` generierte automatische Konfigurationsdatei (`amsilent`) und stellen Sie sicher, dass *AccessManager-base*`\setup\AMConfigurator.properties-tmp` gültige Werte enthält. Benennen Sie diese Datei anschließend in *AccessManager-base* `\setup\AMConfigurator.properties` um.

Weitere Informationen zu den Webcontainer-Variablen finden Sie in der Datei `amsamplesilent` im Verzeichnis `/opt/SUNWam/bin` (Solaris-Systeme) bzw. im Verzeichnis `/opt/sun/identity/bin` (Linux-Systeme).

Auf Windows-Systemen lautet die Konfigurationsdatei *AccessManager-base*`\setup\AMConfigurator.properties`.

6. Führen Sie das Skript `amconfig` wie im folgenden Beispiel aus. Bevor Sie `amconfig`, ausführen, muss der Directory Server und der Access Manager-Webcontainer ausgeführt werden. So führen Sie beispielsweise `amconfig` auf einem Solaris-System aus, auf dem Access Manager im standardmäßigen Basisinstallationsverzeichnis installiert ist

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

7. Starten Sie nach der Ausführung des Skripts `amconfig` die Access Manager-Prozesse neu. Beispiel:

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

8. Stellen Sie sicher, dass sich alle benutzerdefinierten JSP-Dateien in den richtigen untergeordneten Verzeichnissen im Verzeichnis *AccessManager-base*`/SUNWam/web-src/` (Solaris-Systeme) bzw. *AccessManager-base* `/identity/web-src/` (Linux-Systeme) befinden und dass Sie alle benutzerdefinierten Dateien gesichert haben.

   Auf Windows-Systemen befinden sich die Dateien in *AccessManager-base*`\web-src\`.

9. Starten Sie den Access Manager-Webcontainer neu.

Weitere Informationen zum Ausführen des Skripts `amconfig` finden Sie in: Kapitel 1, "Access Manager 7 2005Q4 Configuration Scripts" in *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

Erneutes Bereitstellen der WAR-Dateien für verteilte Authentifizierung und Client SDK (6436409)

Wenn Sie die verteilte Authentifizierung oder das Client SDK verwenden, erstellen Sie nach der Patch-Installation die WAR-Datei der verteilten Authentifizierung bzw. die Client SDK-WAR-Datei erneut und stellen Sie sie erneut bereit. Weitere Informationen finden Sie in folgendender Dokumentation:

- Erstellen der WAR-Datei für die verteilte Authentifizierung: *Technical Note: Using Access Manager Distributed Authentication*
- Erstellen der Client SDK-WAR-Datei: "Installing the Client SDK" in *Sun Java System Access Manager 7 2005Q4 Developer's Guide*
- Bereitstellen der Client SDK-WAR-Datei: "To Deploy amclientwebapps.war" in *Sun Java System Access Manager 7 2005Q4 Developer's Guide*

Access Manager 7 2005Q4 Patch 6

Access Manager 7-Patch 6 (Überarbeitung 06) behebt eine Reihe von Problemen, die in der README-Datei zum Patch aufgeführt sind. Patch 6 enthält außerdem die folgenden neuen Funktionen, Problemlösungen und Dokumentationsaktualisierungen.

Neue Funktionen in Patch 6

Bekannte Probleme und Einschränkungen in Patch 6

Hinweis – Es wird empfohlen, folgende Komponenten zu aktualisieren bzw. Patches für diese Komponenten anzuwenden, bevor Sie Patch 6 installieren:

- Wenn Sie Sun Java System Web Server 6.1 SP5 oder eine ältere Version verwenden, rüsten Sie auf Web Server 6.1 SP7 auf. Diese Version finden Sie unter folgender Adresse:

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

  Folgen Sie den Anweisungen zum Aufrüsten unter "Aktualisierung" in *Versionshinweise zu Sun Java System Web Server 6.1 SP8*.

- Laden Sie den aktuellen Sicherheitspatch für NSS, JSS und NSPR von SunSolve Online herunter: `http://sunsolve.sun.com`.

  - Solaris 8 SPARC-Plattformen: 119209
  - Solaris 8 x86-Plattformen: 119210
  - Solaris 9 SPARC-Plattformen: 119211
  - Solaris 9 x86-Plattformen: 119212
  - Solaris 10 SPARC-Plattformen: 119213
  - Solaris 10 x86- und AMD64-Plattformen: 119214

- Windows-Systeme: 124392
- HP-UX-Systeme: 124379

Access Manager unterstützt die JDK 1.5-Methode `HttpURLConnection setReadTimeout`

Zur Unterstützung der Methode `setReadTimeout` enthält die Datei `AMConfig.properties` die folgende neue Eigenschaft, sodass Sie den Wert für die Zeitüberschreitung für Lesevorgänge festlegen können:

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

Wenn der Webcontainer JDK 1.5 verwendet, legen Sie für diese Eigenschaft einen geeigneten Zeitüberschreitungswert für Verbindungen fest, um zu vermeiden, dass zu viele `HttpURLConnections` gleichzeitig aktiv sind, was zu einem Serverabsturz führen könnte. Der Standardwert ist 30.000 Millisekunden (30 Sekunden).

Die Methode `setReadTimeout` wird ignoriert, wenn `com.sun.identity.url.readTimeout` in der Datei `AMConfig.properties` nicht vorhanden oder auf eine leere Zeichenfolge gesetzt ist.

Access Manager-SDK verwendet den primären Directory-Server wieder, nachdem dieser erneut hochgefahren wurde

Wenn Sun Java System Directory Server für die Multi-Master-Replikation (MMR) konfiguriert ist, verwendet das Access Manager-SDK jetzt wieder den primären Directory-Server, nachdem dieser herunter- und wieder hochgefahren wurde. Zuvor griff das Access Manager-SDK weiterhin auf den sekundären Directory-Server zu, nachdem der primäre Server wieder hochgefahren wurde.

Zur Unterstützung dieses neuen Verhaltens verfügt die Datei `AMConfig.properties` von Access Manager über folgende neue Eigenschaft:

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

Mit dieser Eigenschaft wird die Zeit in Minuten festgelegt, die eine Instanz des sekundären Directory-Servers nach dem erneuten Hochfahren des primären Servers pausiert, bevor dieser wieder verwendet wird. Der Standardwert ist 15 Minuten.

Die Eigenschaft `com.sun.am.ldap.fallback.sleep.minutes` ist verborgen. Um für diese Eigenschaft einen anderen als den Standardwert (15 Minuten) festzulegen, fügen Sie sie der Datei `AMConfig.properties` explizit hinzu. Legen Sie für den Wert beispielsweise 7 Minuten fest:

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

Damit der neue Wert in Kraft tritt, starten Sie den Access Manager-Webcontainer neu.

Die Protokollierung für mehrere Access Manager-Instanzen erfolgt in separaten Protokolldateien.

Die Protokollierung für mehrere Access Manager-Instanzen, die auf demselben Hostserver ausgeführt werden, kann nun in verschiedenen Unterverzeichnissen erfolgen. Legen Sie hierzu die folgende neue Eigenschaft in der Datei `AMConfig.properties` fest:

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

Solange Sie das Standard-Protokollierungsverzeichnis in der Admin-Konsole nicht ändern, werden standardmäßig die folgenden Protokollierungsverzeichnisse verwendet:

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

Die Protokollierung für die erste Access Manager-Instanz erfolgt immer im Standard-Protokollierungsverzeichnis. Um für weitere Access Manager-Instanzen unterschiedliche Protokollierungs-Unterverzeichnisse anzugeben, legen Sie in der Datei `AMConfig.properties` für jede weitere Access Manager-Instanz die Eigenschaft `com.sun.identity.log.logSubdir` fest.

Wenn Sie beispielsweise drei Instanzen haben, `am-instance-1`, `am-instance-2` und `am-instance-3`, die auf demselben Solaris-Hostserver ausgeführt werden, legen Sie die Eigenschaft wie folgt fest:

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

Die Eigenschaft `com.sun.identity.log.logSubdir` ist verborgen. Sie müssen diese Eigenschaft der Datei `AMConfig.properties` bei Bedarf explizit hinzufügen und den Access Manager-Webcontainer neu starten, damit die Werte für die Unterverzeichnisse in Kraft treten.

Die Protokollierung für die Access Manager-Instanzen erfolgt dann in folgenden Verzeichnissen:

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

Access Manager 7 lässt mehrere Cookie-Domänen zu

Zur Unterstützung mehrerer Cookie-Domänen verfügt Access Manager über die folgende neue Eigenschaft:

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

Der Standardwert lautet `true`. Die neue Eigenschaft ist verborgen. Um für den Wert `false` festzulegen, fügen Sie die Eigenschaft der Datei `AMConfig.properties` explizit hinzu, und starten Sie den Access Manager-Webcontainer neu.

Post-Authentifizierungs-Plugin von Microsoft IIS 6.0 unterstützt SharePoint Server

Das Authentifizierungs-Plugin von Microsoft Internet Information Services (IIS) 6.0 unterstützt jetzt Microsoft Office SharePoint Server. Benutzer können sich bei Access Manager mit einer Benutzer-ID oder einem Anmeldenamen anmelden. SharePoint Server akzeptiert jedoch Anmeldenamen, was Probleme verursachen kann, wenn der Benutzer eine Benutzer-ID angibt.

Um eine Anmeldung bei SharePoint Server zu ermöglichen, verwendet das Post-Authentifizierungs-Plugin (`ReplayPasswd.java`) jetzt die folgende neue Eigenschaft:

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

Mit dieser neuen Eigenschaft wird das Benutzerattribut angegeben, das SharePoint Server für die Authentifizierung verwendet. Mit der folgenden Eigenschaft wird beispielsweise der gemeinsame Name (`cn`) für die Authentifizierung angegeben:

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

Das Post-Authentifizierungs-Plugin liest die Eigenschaft `com.sun.am.sharepoint_login_attr_name` und ruft den entsprechenden Attributwert für den Benutzer vom Directory-Server ab. Anschließend werden die Autorisierungskopfzeilen so definiert, dass der Benutzer auf SharePoint Server zugreifen kann.

Diese Eigenschaft ist verborgen. Um die Eigenschaft festzulegen, fügen Sie sie der Datei `AMConfig.properties` explizit hinzu, und starten Sie dann den Access Manager-Webcontainer neu, damit der Wert in Kraft tritt.

Access Manager unterstützt Internet Explorer 7

Access Manager 7 2005Q4 Patch 6 unterstützt jetzt Microsoft Windows Internet Explorer 7.

CR# 6379325 Der Zugriff auf die Konsole während eines Sitzungsfailovers löst eine Nullzeiger-Ausnahme aus

In diesem Szenario wurden mehrere Access Manager-Server im Sitzungsfailover-Modus hinter einem Load Balancer bereitgestellt, der für das cookiebasierte so genannte "Sticky Request Routing" (zähe Anforderungsweiterleitung) konfiguriert ist. Der Access Manager-Administrator greift über den Load Balancer auf die Access Manager-Konsole zu. Wenn der Administrator sich bei der Konsole anmeldet, wird die Sitzung auf einem der Access Manager-Server erstellt. Sollte dieser Server ausfallen, wird für die Konsolensitzung

erwartungsgemäß ein Failover auf einen anderen Access Manager-Server ausgeführt. Manchmal werden dem Administrator jedoch sporadisch Nullzeiger-Ausnahmen im Browser und im Fehlerprotokoll des Webcontainers angezeigt.

Dieses Problem betrifft nur die zum Zeitpunkt des Failovers aktive Access Manager-Konsolensitzung und wirkt sich nicht auf die Funktion der Access Manager-Server aus.

Umgehung: So vermeiden Sie sporadische Nullzeiger-Ausnahmen

- Als vorübergehende Lösung können Sie den Browser aktualisieren oder sich abmelden und dann erneut bei der Konsole anmelden.
- Um das Problem dauerhaft zu beseitigen, stellen Sie die Access Manager-Konsole auf einer separaten Access Manager-Instanz bereit, die nicht am Sitzungsfailover beteiligt ist.

CR# 6508103: Unter Windows wird durch Aufrufen der Hilfe in der Admin-Konsole ein Anwendungsfehler zurückgegeben

Wenn Access Manager unter Windows 2003 Enterprise Edition auf einem Sun Java System Application Server in anderen Gebietsschemata als Englisch bereitgestellt wird, wird durch Aufrufen der Hilfe in der Admin-Konsole im Realm-Modus ein Anwendungsfehler zurückgegeben.

Umgehung:

1. Kopieren Sie die Datei *javaes-install-dir*`\share\lib\jhall.jar` in das Verzeichnis `%JAVA_HOME%\jre\lib\ext`.

   javaes-install-dir steht hierbei für das Windows-Installationsverzeichnis.
2. Starten Sie die Anwendungsserver-Instanz neu.

CR# 6564877: Durch die Installation des Access Manager 7-Patches werden die SAML v2-Dateien überschrieben

Wenn das SAML v2-Plugin installiert ist, werden durch die Installation des Patches die SAML v2-bezogenen Dateien überschrieben, und das Skript `postpatch` zeigt die folgende Nachricht an:

```
The postpatch script detected that the SAML v2 plug-in is installed in your
environment. When you run the amconfig script to redeploy the Access Manager
applications, the script will recreate the amserver.war file and the SAML v2
related files will be lost. Therefore, after you run amconfig, recreate and
redeploy the amserver.war file, as described in the Sun Java System SAML v2
Plug-in for Federation Services User’s Guide.
```

Umgehung: Nachdem Sie den Patch installiert und das Skript `amconfig` ausgeführt haben, erstellen Sie die Datei `amserver.war` für die Federation Manager- oder Access Manager-Bereitstellungen, die das SAML v2-Plugin verwenden, und stellen Sie sie erneut bereit.

Die genaue Vorgehensweise entnehmen Sie Kapitel 2, "Installing the SAML v2 Plug-in for Federation Services" in *Sun Java System SAML v2 Plug-in for Federation Services User's Guide*.

Access Manager 7 2005Q4-Patch 5

Access Manager 7-Patch 5 (Überarbeitung 05) behebt eine Reihe von Problemen, die in der README-Datei zum Patch aufgeführt sind. Patch 5 enthält außerdem die folgenden neuen Funktionen, Problemlösungen und Dokumentationsaktualisierungen.

Neue Funktionen in Patch 5

Bekannte Probleme und Einschränkungen in Patch 5

Globalisierungsprobleme (g11n)

Dokumentationsaktualisierungen

- "Fehlender Schritt in Onlinehilfe unter ?So erstellen Sie einen neuen Site-Namen" (2144543)" auf Seite 109
- "Konfigurationsparameter für Administrator-Passwort lautet auf Windows-Systemen `ADMIN_PASSWD` (6470793)" auf Seite 110

Unterstützung von HP-UX-Systemen

Patch **126371** bietet Unterstützung für HP-UX-Systeme. Weitere Informationen finden Sie hier:

- "Anweisungen zur Patch-Installation für HP-UX-Systeme" auf Seite 20
- "Aufgaben nach der Installation" auf Seite 20

Informationen zur Installation von HP-UX-Systemen finden Sie im *Sun Java Enterprise System 2005Q4 Installationshandbuch für UNIX*.

Unterstützung für Microsoft Windows-Systeme

Patch **124296** bietet Unterstützung für Windows-Systeme. Weitere Informationen finden Sie hier:

- "Patch-Installationsanweisungen für Windows-Systeme" auf Seite 18
- "Aufgaben nach der Installation" auf Seite 20
- "Optimierungsskripte für Windows-Systeme verfügbar" auf Seite 39

Informationen zur Installation von Windows-Systemen finden Sie im *Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows* .

Neues `updateschema.sh`-Skript zum Laden von LDIF- und XML-Dateien

Patch 5 (und höher) enthält das Skript `updateschema.sh`, um folgende Dateien für die Aktualisierung des Directory Server-Dienstschemas zu laden:

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

In vorherigen Access Manager-Patch-Versionen mussten diese Dateien manuell geladen werden.

So führen Sie das `updateschema.sh`-Skript aus

1. Melden Sie sich als Superuser (`root`) an.

2. Wechseln Sie in das Patch-Verzeichnis.
3. Führen Sie das Skript aus. Beispielsweise auf Solaris-Systemen:

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

   Auf Windows-Systemen lautet das Skript `updateschema.pl`.
4. Machen Sie folgende Angaben, wenn Sie dazu aufgefordert werden:
   - Hostname und Portnummer für Directory Server
   - Admin-Benutzer-DN und Passwort für Directory Server
   - DN und Passwort für `amadmin`
5. Ihre Angaben werden überprüft und die Dateien geladen. Das Skript erstellt außerdem folgende Protokolldatei:
   - Solaris-Systeme: `/var/opt/SUMWam/logs/AM70Patch.upgrade.schema.` *timestamp*
   - Linux-Systeme: `/var/opt/sun/identity/logs/AM70Patch.upgrade.schema.` *timestamp*
6. Nach Ausführung des Skripts wird der Access Manager-Webcontainer neu gestartet.

Hinweis Wenn Sie die Patch 5-Installation rückgängig machen, werden die vom `updateschema.sh`-Skript vorgenommenen Schemaänderungen nicht aus Directory Server entfernt. Sie müssen diese Änderungen jedoch nicht manuell entfernen, da die Änderungen die Funktionalität und Bedienbarkeit von Access Manager nicht beeinträchtigen, nachdem das Patch entfernt wurde.

Unterstützung für anwendungsspezifische Zeitüberschreitungswerte für Sitzungsleerlauf

Patch 5 ermöglicht die Einstellung unterschiedlicher Zeitüberschreitungswerte für den Sitzungsleerlauf in den verschiedenen Anwendungen. In einem Unternehmen erfordern manche Anwendungen möglicherweise kleinere Zeitüberschreitungswerte für den Sitzungsleerlauf als den im Sitzungsdienst angegebenen Zeitüberschreitungswert für den Sitzungsleerlauf. Zum Beispiel: Im Sitzungsdienst ist der Zeitüberschreitungswert auf 30 Minuten festgelegt, in einer HR-Anwendung soll jedoch eine Zeitüberschreitung eintreten, wenn sich die Benutzersitzung länger als 10 Minuten im Leerlauf befindet.

Voraussetzungen für die Verwendung dieser Funktion:

- Die zum Schutz der Anwendung eingesetzten Agenten müssen so konfiguriert sein, dass sie die URL-Richtlinienentscheidungen von Access Manager durchsetzen.
- Agenten müssen für die Ausführung eigener Richtlinienentscheidungen im Cachemodus konfiguriert sein. Siehe folgende Eigenschaften:
  - Für Webagenten: `com.sun.am.policy.am.fetch_from_root_resource`
  - Für J2EE-Agenten: `com.sun.identity.policy.client.cacheMode`

- In der Access Manager-Datei `AMConfig.properties` muss die Auswertungsreihenfolge für Richtlinienkomponenten so angegeben sein, dass die Bedingung (Condition) zuletzt ausgewertet wird. Siehe folgende Eigenschaft:

  `com.sun.identity.policy.Policy.policy_evaluation_weights`

- Der vom Agenten erlaubte Anwendungszugriff, der auf der im lokalen Cache enthaltenen Bedingung basiert, wird der Bedingung in Access Manager nicht bekannt gemacht. Daher liegt der tatsächliche Zeitüberschreitungswert zwischen dem Zeitüberschreitungswert der Anwendung und dem Zeitüberschreitungswert der Anwendung minus der Cachedauer.

So verwenden Sie diese Funktion

- Fügen Sie den Richtlinien, die die Anwendung schützen und für die ein bestimmter Zeitüberschreitungswert für den Sitzungsleerlauf erforderlich ist, eine Bedingung für das Authentifizierungsschema (Authentication Scheme Condition) hinzu.
- Geben Sie in der Bedingung für das Authentifizierungsschema einen Anwendungsnamen und einen Zeitüberschreitungswert an.
- Verwenden Sie in allen Richtlinien, die auf die Ressourcen für die Anwendung angewendet werden, denselben Anwendungsnamen und Zeitüberschreitungswert.
- Geben Sie den Zeitüberschreitungswert in Minuten an. Wenn der Wert 0 oder höher als der im Sitzungsdienst angegebene Zeitüberschreitungswert ist, wird der Wert ignoriert und der Zeitüberschreitungswert des Sitzungsdienstes angewendet.

Gehen Sie beispielsweise von einer Richtlinie `http://host.sample.com/hr/*` mit folgender Bedingung für das Authentifizierungsschema aus:

- Authentifizierungsschema: LDAP
- Anwendungsname: HR
- Zeitüberschreitungswert: 10

Wenn mehrere Richtlinien zum Schutz der Ressourcen der HR-Anwendung festgelegt wurden, müssen Sie die Bedingung allen Richtlinien hinzufügen.

Wenn ein Benutzer in einer Sitzung auf die vom Access Manager-Agenten geschützte HR-Anwendung zugreifen möchte, wird der Benutzer zur Authentifizierung mit dem LDAP-Schema aufgefordert (falls der Benutzer nicht bereits authentifiziert ist).

Ist der Benutzer bereits mit dem LDAP-Schema authentifiziert, wird dem Benutzer nur dann Zugriff auf die Anwendung gewährt, wenn seit der letzten Authentifizierung weniger als 10 Minuten vergangen sind oder der Benutzer zuletzt vor weniger als 10 Minuten auf die HR-Anwendung zugegriffen hat. Anderenfalls wird der Benutzer zur erneuten Authentifizierung mit dem LDAP-Schema aufgefordert, um auf die Anwendung zugreifen zu können.

Bereitstellung des CDC-Servlets auf einem Server mit Verteilter Authentifizierungsbenutzeroberfläche möglich

Das CDC-Servlet kann neben einem Server mit Verteilter Authentifizierungsoberfläche in der DMZ bestehen, um domänenübergreifendes Single Sign-On (Cross-Domain Single Sign-On, CDSSO) zu aktivieren. Access Manager kann hinter einer Firewall bereitgestellt werden und sämtlicher Zugriff auf Access Manager, der für CDSSO erforderlich ist, wird vom CDC-Servlet des Servers mit Verteilter Authentifzierungsbenutzeroberfläche verarbeitet. Um CDSSO zu aktivieren, lesen Sie in der Dokumentation zum Richtlinienagenten nach und führen Sie zusätzlich folgende Schritte durch:

- Ändern Sie die Datei `AMAgent.properties` des Agenten so, dass diese auf das CDS-Servlet auf der Seite der Verteilten Authentifizierung (Client) zeigt. Ändern Sie für Webagenten beispielsweise die folgende Eigenschaft:

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

- Geben Sie in Access Manager gegebenenfalls Richtlinien für Ressourcen an, die von dem Agenten geschützt werden sollen. Wenn der Agent beispielsweise an Port `host.example.com:80` liegt, legen Sie als Richtlinie für die Ressource `http://host.example.com:80/*` fest.

Ein Bereich kann festgelegt werden, wenn das CDC-Servlet auf die Access Manager-Anmelde-URL umleitet.

Sie können nun einen Bereichsnamen für das CDC-Servlet angeben, sodass bei der Umleitung auf die Access Manager-Anmelde-URL der Bereichsname mit eingeschlossen wird und sich der Benutzer im angegebenen Bereich anmelden kann. Beispiel:

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

Zertifikatsauthentifizierung kann UPN-Wert für Zuordnung von Benutzerprofilen verwenden

Bei der Zertifikatsauthentifzierung konnte bislang nur die `dn`-Komponente von `subjectDN` für die Zuordnung eines Benutzerprofils verwendet werden. Access Manager ermöglicht nun die Verwendung des Werts für den Benutzer-Principal-Namen (User Principal Name, UPN) im `SubjectAltNameExt` für die Profilzuordnung.

Verarbeitung der Abmeldung nach Authentifizierung in Umgebung mit mehreren Servern

Die Verarbeitung nach der Authentifizierung findet nun statt, wenn sich ein Benutzer von einem anderen Server abmeldet, als dem Server, bei dem er sich ursprünglich in einer Umgebung mit mehreren Servern (mit oder ohne Sitzungsfailover-Konfiguration) angemeldet hat.

SAML-Unterstützung für neues Namensbezeichner-SPI

SAML unterstützt nun eine neue Dienstanbieterschnittstelle (Service Provider Interface, SPI) für Namensbezeichner, sodass eine Site den Namensbezeichner in der SAML-Assertion anpassen kann. Eine Site kann die neue `NameIdentifierMapper`-Schnittstelle implementieren, um ein Benutzerkonto einem Namensbezeichner im Subjekt einer SAML-Assertion zuzuordnen.

Neue Konfigurationseigenschaften für Siteüberwachung

Die Siteüberwachungsfunktion von Access Manager enthält die folgenden neuen Eigenschaften, mit denen Sie das Verhalten der Sitestatusüberprüfung festlegen können.

Eigenschaft	Beschreibung
`com.sun.identity.urlchecker.invalidate.interval`	Zeitintervall in Millisekunden für das Erkennen einer Site, die nicht verfügbar ist oder nicht antwortet. Standard: 70000 Millisekunden (70 Sekunden).
`com.sun.identity.urlchecker.sleep.interval`	Zeitintervall in Millisekunden, in dem die Sitestatusüberprüfung pausieren soll. Standard: 30000 Millisekunden (30 Sekunden).
`com.sun.identity.urlchecker.targeturl`	Andere Ziel-URL zum Überprüfen des Prozess-Status von Access Manager. Standard: "`/amserver/namingservice`".

Der Patch fügt diese Eigenschaften der Datei `AMConfig.properties` nicht hinzu. So verwenden Sie diese neuen Eigenschaften mit anderen Werten als den Standardwerten

1. Fügen Sie die Eigenschaften und ihre Werte der Datei `AMConfig.properties` hinzu. Fügen Sie für Richtlinienagenten diese Eigenschaften der Datei `AMAgents.properties` hinzu.
2. Starten Sie den Access Manager-Webcontainer neu, damit die Werte in Kraft treten.

Zweifache Authentifizierung des Benutzers in Authentifizierungskette nicht mehr erforderlich

Bedenken Sie folgendes Szenario. Eine Site konfiguriert eine Authentifizierungskette mit drei LDAP-Modulen. Alle Module werden auf `SUFFICIENT` festgelegt und die Optionen `iplanet-am-auth-shared-state-enabled` und `iplanet-am-auth-store-shared-state-enabled` werden auf `true` gesetzt. Beispiel:

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

Patch 5 fügt den Moduloptionen die neue Option `iplanet-am-auth-shared-state-behavior-pattern` mit zwei möglichen Werten hinzu: `tryFirstPass` (Standard) und `useFirstPass`.

Um zu verhindern, dass ein Benutzer seine Benutzer-ID und sein Passwort für die Authentifizierung zweimal eingeben muss (wie im obigen Szenario beschrieben), setzen Sie die Option für alle Module in der Kette auf `useFirstPass`. Zuvor musste ein Benutzer, der nur in der dritten LDAP-Instanz vorhanden war, seine Benutzer-ID und sein Passwort zweimal eingeben, um sich zu authentifizieren.

Änderungen der Leistungsoptimierungsskripten

Patch 5 enthält folgende Änderungen der Skripten für die Leistungsoptimierung:

- "Optimierungsskripte unterstützen eine Passwortdatei" auf Seite 37
- "Das Optimierungsskript entfernt nicht benötigte ACIs aus Directory Server" auf Seite 37
- "Optimierungsskripte optimieren den Webcontainer des Servers mit Verteilter Authentifizierungsbenutzeroberfläche" auf Seite 37
- "Skript `amtune-os` optimiert sowohl Solaris OS als auch Linux OS" auf Seite 38
- "Optimierungsskripte in einer lokalen Solaris 10-Zone werden vollständig ausgeführt " auf Seite 39
- "Optimierungsskripte für Windows-Systeme verfügbar" auf Seite 39
- "Zu berücksichtigende Aspekte bei der Optimierung von Sun Fire T1000- und Sun Fire T2000-Server" auf Seite 39

Siehe auch "Standardwert für Eigenschaft `com.sun.identity.log.resolveHostName` sollte auf `false` und nicht auf `true` eingestellt sein (6527663)" auf Seite 41.

Optimierungsskripte unterstützen eine Passwortdatei

Patch 5 ermöglicht die Angabe eines Passworts für die Optimierungsskripte in einer Textdatei. Zuvor konnten Passwörter nur als Befehlszeilenargument eingegeben werden, wodurch unter Umständen Sicherheitsprobleme aufgetreten sind. Um eine Passwortdatei zu verwenden, legen Sie die folgenden Variablen entsprechend Ihrer Anforderungen fest:

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

So optimieren Sie beispielsweise Application Server 8

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

wobei *password-file* die auf das Administratorpasswort von Application Server 8 festgelegte Variable `AS_ADMIN_PASSWORD` enthält.

Die Optimierungsskripte verwenden die Option `-j` *password-file* beim Aufrufen der Directory Server-Dienstprogramme `ldapmodify`, `ldapsearch`, `db2index` und `dsconf`.

Das Optimierungsskript entfernt nicht benötigte ACIs aus Directory Server

Wenn Access Manager 7 2005Q4 im Realm-Modus installiert ist, werden für die Ermittlung der Zugriffsberechtigungen Übertragungsberechtigungen verwendet, sodass manche Directory Server-ACIs nicht benötigt werden. Access Manager 7 2005Q4-Patch 5 ermöglicht Ihnen, die nicht benötigten ACIs durch Ausführung des Skripts `amtune-prepareDSTuner` zu entfernen. Das Skript liest eine Liste mit ACIs in der Datei `remacis.ldif` und ruft anschließend das `ldapmodify`-Dienstprogramm auf, um die ACIs zu entfernen.

Sie können das Skript `amtune-prepareDSTuner` zum Entfernen nicht benötigter ACIs auf Solaris-, HP-UX- und Windows-Systemen ausführen. Weitere Informationen, unter anderem zur Ausführung des Skripts, finden Sie im *Technical Note: Sun Java System Access Manager ACI Guide* .

Optimierungsskripte optimieren den Webcontainer des Servers mit Verteilter Authentifizierungsbenutzeroberfläche

Nachdem Sie den Server mit Verteilter Authentifizierungsbenutzeroberfläche bereitgestellt haben, können Sie den Webcontainer optimieren, indem Sie die Access Manager-Optimierungsskripte ausführen. Die folgenden Optimierungsskripte legen die JVM-Option sowie weitere Optimierungsoptionen für den jeweiligen Webcontainer fest:

TABELLE 2 Access Manager-Optimierungsskripte für Webcontainer

Webcontainer	Optimierungsskript
`amtune-ws61`	Web Server 6.1
`amtune-as7`	Application Server 7
`amtune-as8`	Application Server Enterprise Edition 8.1

So optimieren Sie den Webcontainer eines Servers mit Verteilter Authentifizierungsbenutzeroberfläche

1. Da der Access Manager-Server nicht auf dem System installiert ist, auf dem der Server mit Verteilter Authentifizierungsbenutzeroberfläche bereitgestellt wird, kopieren Sie das entsprechende Webcontainer-Optimierungsskript (siehe Tabelle oben), die Konfigurationsdatei `amtune-env` und das Skript `amtune-utils` aus einer Access Manager-Serverinstallation. Wenn Sie das Solaris- oder Linuxbetriebssystem optimieren möchten, kopieren Sie zusätzlich das Skript `amtune-os`.
2. Bearbeiten Sie die Parameter in der Konfigurationsdatei `amtune-env`, um den Webcontainer und die Optimierungsoptionen anzugeben. Um das Skript im REVIEW-Modus auszuführen, legen Sie `AMTUNE_MODE=REVIEW` in der Datei `amtune-env` fest.
3. Führen Sie das Webcontainer-Optimierungsskript im REVIEW-Modus aus. Im REVIEW-Modus schlägt das Skript basierend auf den Werten in der Datei `amtune-env` Änderungen für die Optimierung des Webcontainers vor, führt jedoch keine Änderungen an der Bereitstellung aus.
4. Überprüfen Sie die Optimierungsempfehlungen in der Debug-Protokolldatei. Ändern Sie die Datei `amtune-env` gegebenenfalls entsprechend der empfohlenen Änderungen.
5. Um Optimierungsänderungen vorzunehmen, legen Sie `AMTUNE_MODE=CHANGE` in der Datei `amtune-env` fest.
6. Führen Sie das Skript im CHANGE-Modus aus, um Optimierungsänderungen an der Bereitstellung vorzunehmen.

Weitere Informationen zur Ausführung des Optimierungsskripts für die Optimierung des Access Manager-Webcontainers finden Sie in Kapitel Kapitel 2, "Access Manager Tuning Scripts" in *Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide*.

Skript `amtune-os` optimiert sowohl Solaris OS als auch Linux OS

Patch 5 enthält das Skript `amtune-os`, das sowohl das Solaris OS als auch das Linux OS optimiert. Das Skript bestimmt das Betriebssystem mit dem Befehl `uname -s`. Zuvor wurden in Access Manager separate `amtune-os`-Skripte für die Optimierung des jeweiligen Betriebssystems bereitgestellt.

Optimierungsskripte in einer lokalen Solaris 10-Zone werden vollständig ausgeführt

Wenn Access Manager in einer lokalen Solaris 10-Zone installiert ist, können alle Skripte, mit Ausnahme von `amtune-os`, in der lokalen Zone ausgeführt werden. In einer lokalen Zone zeigt das `amtune-os`-Skript eine Warnung an, führt die Optimierung des Betriebssystems jedoch nicht aus. Das Skript führt anschließend alle anderen von Ihnen angeforderten Optimierungsskripts aus. Zuvor wurde die Ausführung des `amtune-os` -Skripts in einer lokalen Zone abgebrochen und keines der nachfolgenden angeforderten Optimierungsskripte ausgeführt.

In einer globalen Solaris 10-Zone ruft das Skript `amtune` das Skript `amtune-os` aus, um das Betriebssystem zu optimieren, sowie alle übrigen zur Ausführung angeforderten Skripten.

Optimierungsskripte für Windows-Systeme verfügbar

Patch 5 enthält Optimierungsskripte für Windows-Systeme. Die Ausführung der Optimierungsskripte auf einem Windows-System entspricht mit Ausnahme der folgenden Unterschiede der Ausführung der Skripte auf einem Solaris- oder Linux-System:

- Windows-Skripte sind in Perl geschrieben und erfordern die Ausführung von Active Perl 5.8.
- Wenn Sie nach der Ausführung des Skripts `amtune-prepareDSTuner.pl` Directory Server optimieren, müssen Sie die Dateien `amtune-utils.pl`, `amtune-directory.pl`, `remacis.ldif` und `amtune-samplepassordfile` in das Directory Server-System kopieren, da das Skript diese Dateien nicht komprimieren kann.
- Es steht kein Skript für die Optimierung des Windows-Betriebssystems zur Verfügung.
- Zonen werden nicht unterstützt.
- Bevor Sie ein Skript ausführen, müssen Sie den Parameter `$BASEDIR` in der Datei `amtune-env.pl` auf das Access Manager-Installationsverzeichnis setzen.

Zu berücksichtigende Aspekte bei der Optimierung von Sun Fire T1000- und Sun Fire T2000-Server

Wenn Access Manager auf einem Sun Fire T1000- oder Sun Fire T2000-Server installiert ist, setzen die Skripte für Web Server 6.1 und Application Server 8 den Parameter `JVM GC ParallelGCThreads` auf 8:

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

Dieser Parameter reduziert die Anzahl der Garbage Collection-Threads, die auf einem 32–Thread-fähigen System unnötig hoch sein kann. Wenn die Aktivitäten der vollständigen Garbage Collection dadurch reduziert werden, können Sie den Wert jedoch auf 16 bzw. im Fall eines virtuellen 32 CPU-Rechners (z. B. ein Sun Fire T1000- oder Sun Fire T2000-Server) auf 20 erhöhen.

Es wird außerdem empfohlen, auf Solaris SPARC-Systemen mit einem CMT-Prozessor unter Verwendung der CoolThreads-Technologie folgende Eigenschaft an das Ende der Datei `/etc/opt/SUNWam/config/AMConfig.properties` anzufügen:

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

Der Standardwert für *value* ist 16. Sie können für diese Eigenschaft jedoch je nach Anzahl der Cores im Sun Fire T1000- bzw. Sun Fire T2000-Server einen kleineren Wert festlegen.

Basisauthentifizierung im Richtlinienagenten für IIS 6.0

Um die Basisauthentifizierung in Microsoft Internet Information Services (IIS) 6.0 zu aktivieren, muss der Richtlinienagent den Namen und das Passwort des Benutzers erhalten. Patch 5 enthält die folgenden neuen Klassen, um diese Funktionalität unter Verwendung der DES-Verschlüsselung des Benutzerpassworts zu aktivieren:

- `DESGenKey.java` generiert einen eindeutigen Schlüssel für die Ver- und Entschlüsselung des Benutzerpassworts.
- `ReplayPasswd.java` liest den Wert des Verschlüsselungsschlüssels aus der Eigenschaft `com.sun.am.replaypasswd.key` in der Datei `AMConfig.properties`, verschlüsselt das Passwort und weist es der Sitzungseigenschaft `sunIdentityUserPassword` zu.

Um die Basisauthentifizierung in IIS 6.0 zu verwenden, müssen Sie sowohl in Access Manager (serverseitig) als auch im Richtlinienagent für IIS 6.0 folgende Schritte durchführen.

In Access Manager:

1. Führen Sie `DESGenKey.java` aus, um einen eindeutigen Verschlüsselungsschlüssel für die Ver- und Entschlüsselung des Passworts zu generieren. Auf Solaris-Systemen befindet sich die Datei `DESGenKey.java` im Verzeichnis `com/sun/identity/common` , das sich in der Datei `am_sdk.jar` im Verzeichnis `/opt/SUNWam/lib` befindet. Der folgende Befehl generiert beispielsweise einen Verschlüsselungsschlüssel:

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

2. Weisen Sie den Wert des Verschlüsselungsschlüssels aus Schritt 1 der Eigenschaft `com.sun.am.replaypasswd.key` in der Datei `AMConfig.properties` zu.
3. Stellen Sie `ReplayPasswd.java` als ein der Authentifizierung nachgestelltes Plugin bereit. Verwenden Sie bei der Konfiguration des Plugins den vollständigen Klassennamen: `com.sun.identity.authentication.spi.ReplayPasswd` .

Im Richtlinienagent für IIS 6.0:

1. Weisen Sie den serverseitigen Verschlüsselungsschlüssel der Eigenschaft `com.sun.am.replaypasswd.key` in der Datei `AMAgent.properties` zu. Access Manager und der Richtlinienagent für IIS 6.0 müssen denselben Verschlüsselungsschlüssel verwenden.

2. Aktivieren Sie die Basisauthentifizierung in IIS 6.0 Manager.

Der Richtlinienagent für IIS 6.0 liest das verschlüsselte Passwort aus der Sitzungsantwort, entschlüsselt das Passwort aus der Eigenschaft `com.sun.am.replaypasswd.key` und legt die Authentifizierungs-Header fest, um die Basisauthentifizierung zuzulassen.

Informationen zum Richtlinienagenten für IIS 6.0 finden Sie im *Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0* .

CR# 6567746: Auf HP-UX-Systemen meldet Access Manager Patch 5 einen falschen Wert für errorCode, wenn die maximale Anzahl an versuchten Passworteingaben überschritten wird

Wenn das Konto eines Benutzer gesperrt wird, meldet Access Manager 7 2005Q4 Patch 5 `errorCode = null` statt `errorCode = 107`, wenn die maximale Anzahl an versuchten Passworteingaben überschritten wird.

Lösung. Keine.

Standardwert für Eigenschaft `com.sun.identity.log.resolveHostName` sollte auf `false` und nicht auf `true` eingestellt sein (6527663)

Es wird empfohlen, vor der Ausführung des Optimierungsskripts `amtune-identity` die folgende Eigenschaft mit der Einstellung `false` der Datei `AMConfig.properties` hinzuzufügen:

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

Mit `false` wird der Aufwand für das Auflösen von Hostnamen minimiert, wodurch die Leistung verbessert werden kann. Wenn jedoch der Hostname des Clientcomputers in das Protokoll `amAuthentication.access` geschrieben werden soll, setzen Sie den Wert auf `true`.

Nach Entfernung des Patches verbleiben XML-Dateien, die das `amldapuser`-Passwort in Klartext enthalten (6527528)

Wenn Sie Patch 5 aus einer vollständigen Access Manager-Serverinstallation entfernen, enthalten die Dateien `amAuthLDAP.xml` und `amPolicyConfig.xml` das Passwort für `amldapuser` in Klartext. Diese Dateien befinden sich je nach Plattform im folgenden Verzeichnis:

- Solaris-Systeme: `/etc/opt/SUNWam/config/xml`
- Linux- und HP-UX-Systeme: `/etc/opt/sun/identity/config/xml`

Umgehung: Bearbeiten Sie die Dateien `amAuthLDAP.xml` und `amPolicyConfig.xml` und löschen Sie das in Klartext enthaltene Passwort.

Vollständiger Server auf WebLogic erfordert Kommunikation der JAR-Dateien von JAX-RPC 1.0 mit Client-SDK (6527516)

In Access Manager 7 2005Q4-Patches fügt das Access Manager-Konfigurationsskript für BEA WebLogic Server (`amwl81config`) die JAR-Dateien von JAX-RPC 1.1 dem `classpath` für die WebLogic-Instanz hinzu. Diese Änderung ist zwar für Produkte wie Sun Java System Portal Server vorteilhaft, eine vollständige auf einem WebLogic-Server bereitgestellte Serverinstallation (`DEPLOY_LEVEL=1`), kann jedoch nicht mit einer Client-SDK kommunizieren, sodass es zu Ausnahmefehlern kommt.

Wenn der Access Manager 7 2005Q4-Server auf einem BEA WebLogic-Server installiert ist, muss der `CLASSPATH` im Skript `startWebLogic.sh` auf den Speicherort der JAR-Dateien von JAX-RPC 1.0 JAR festgelegt werden, um mit dem Access Manager-Client-SDK kommunizieren zu können.

Umgehung: Legen Sie vor der Anwendung des Access Manager-Patches den `CLASSPATH` im Skript `startWebLogic.sh` so fest, dass die WebLogic-Serverinstanz die JAR-Dateien von JAX-RPC 1.0 und nicht die JAR-Dateien von JAX-RPC 1.1 verwendet:

1. Melden Sie sich beim Access Manager-Server als Superuser (`root`) an oder wechseln Sie zum Superuser.
2. Bearbeiten Sie das Skript `startWebLogic.sh` und ersetzen Sie den `CLASSPATH`, sodass die JAR-Dateien von JAX-RPC 1.0 verwendet werden. Beispiel:

Aktueller Wert:

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

Neuer Wert:

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

wobei *AccessManager-base* das Basisinstallationsverzeichnis ist. Auf Solaris-Systemen lautet der Standardwert `/opt`, auf Linux- und HP-UX-Systemen `/opt/sun`. *AccessManager-package-dir* ist das Access Manager-Paketverzeichnis.

5. Starten Sie die WebLogic-Serverinstanz neu.

Datei `amsilent` in Patch 5 kann auf Linux-Systemen von allen Benutzern gelesen werden (6523499)

Auf Linux-Systemen. Das Skript `postpatch` erstellt die Datei `/opt/sun/identity/amsilent` mit der Berechtigung 644, die allen Benutzern Lesezugriff gewährt.

Umgehung: Ändern Sie nach Ausführung des Skripts `installpatch` die Berechtigungen in der Datei `amsilent`, sodass nur der Eigentümer Lese- und Schreibzugriff erhält. Beispiel:

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

Anwendung von Patch 5 auf eine zweite Access Manager-Instanz auf einem Server überschreibt `serverconfig.xml` der ersten Instanz (6520326)

In diesem Bereitstellungsszenario werden zwei Access Manager-Instanzen auf demselben Hostserver bereitgestellt, wobei sich die Instanzen auf verschiedenen Webcontainer-Instanzen befinden. Führen Sie folgende Schritte aus:

1. Wenden Sie Patch 5 an.
2. Bearbeiten Sie die Datei `amsilent` und stellen Sie die erste Access Manager-Instanz erneut bereit.
3. Bearbeiten Sie die Datei `amsilent` erneut für die zweite Access Manager-Instanz und stellen Sie diese Instanz erneut bereit.

Wenn in der Datei `amsilent` die Eigenschaft `NEW_INSTANCE=false` festgelegt ist, wird die Datei `serverconfig.xml` der ersten Access Manager-Instanz mit den Informationen für die zweite Access Manager-Instanz überschrieben. Ein anschließender Neustart der ersten Access Manager-Instanz schlägt fehl. Die Datei `serverconfig.xml` befindet sich je nach Plattform im folgenden Verzeichnis:

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

Umgehung: Legen Sie bei der Bereitstellung der zweiten Access Manager-Instanz in der Datei `amsilent` die Eigenschaft `NEW_INSTANCE=true` fest. Die Datei `serverconfig.xml` der zweiten Access Manager-Instanz wird so mit den richtigen Informationen aktualisiert, und die Datei `serverconfig.xml` der ersten Access Manager-Instanz wird nicht überschrieben.

Bei der Patch 5-Installation auf einem Rechner, der nur SDK enthält, werden die Beispiel-Makefiles überschrieben (6520016)

Wenn Sie Patch 5 auf einem Rechner anwenden, der nur SDK enthält, werden die Beispiel-Makefiles überschrieben.

Umgehung: Bei der Anwendung von Patch 5 auf einen Rechner, der nur SDK enthält, ist keine Neukonfiguration erforderlich. Wenn Sie jedoch die Beispiel-Makefiles verwenden möchten, führen Sie folgende Schritte durch, um die LDIF- und Eigenschaftsdateien für die Beispiel-Makefiles zu aktualisieren (Tag-Swapping):

1. Führen Sie das Skript `amconfig` mit `DEPLOY_LEVEL=14` aus, um das SDK zu deinstallieren und die Konfiguration des Webcontainers aufzuheben.
2. Führen Sie das Skript `amconfig` mit `DEPLOY_LEVEL=4` aus, um das SDK erneut zu installieren und den Webcontainer erneut zu konfigurieren.

LDAPv3-Repository-Plugin verarbeitet Alias-Suchattribut nicht immer korrekt (6515502)

Für die Mehrzahl der Suchläufe wurde das Problem behoben. Bedenken Sie jedoch folgende Problematik beim Festlegen des Alias-Suchattributs. Der Wert des Alias-Suchattributs muss über die gesamte Organisation hinweg eindeutig sein. Wenn mehrere Alias-Suchattribute festgelegt werden, besteht die Möglichkeit, dass ein Eintrag im Datenspeicher mit einem Attribut übereinstimmt und ein anderer Eintrag mit dem anderen Attribut übereinstimmt. In diesem Fall gibt Access Manager folgenden Fehler aus:

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

Umgehung: Kein

Verteilte Authentifizierung und J2EE-Agent können nicht im selben Webcontainer ausgeführt werden (6515383)

Ein Server mit Verteilter Authentifizierungsbenutzeroberfläche und ein J2EE-Richtlinienagent können nicht zusammen ausgeführt werden, wenn diese im selben Webcontainer installiert sind.

Umgehung: Erstellen Sie eine zweite Webcontainer-Instanz und stellen Sie den Server mit Verteilter Authentifizierungsbenutzeroberfläche und den J2EE-Richtlinienagenten auf verschiedenen Instanzen des Containers bereit.

Die Onlinehilfe gibt Anwendungsfehler aus, wenn Application Server auf einem Windows-System ausgeführt wird (6508103)

Wenn Access Manager auf einem Sun Java System Application Server auf einem Windows-System bereitgestellt wird und Sie im linken Bereich des Hilfebildschirms der Konsole im Realm-Modus auf die Hilfeschaltfläche klicken, wird ein Fehler ausgegeben.

Umgehung: Kopieren Sie die Datei *javaes-install-dir*`\share\lib\jhall.jar` in das Verzeichnis `JAVA_HOME\jre\lib\ext`, und starten Sie den Anwendungsserver neu.

Verteilte Authentifizierung erfordert expliziten `goto`-URL-Parameter (6507383 und 6507377)

Wenn kein expliziter `goto`-URL-Parameter angegeben ist, versucht ein Server mit verteilter Authentifizierungsbenutzeroberfläche auf den `goto` eines in Access Manager angegebenen Erfolgs-URLs (Success URL) umzuleiten. Diese Umleitung kann aus folgenden Gründen fehlschlagen:

- Die URL ist relativ und es ist keine entsprechende Seite beim Server mit Verteilter Authentifizierungsbenutzeroberfläche verfügbar.
- Die URL ist absolut und der Browser kann die URL nicht finden.

Umgehung: Geben Sie für einen Server mit Verteilter Authentifizierungsbenutzeroberfläche immer einen expliziten `goto`-URL-Parameter an.

LDAP JDK 4.18 verursacht Probleme in LDAP-Client/Directory Server (6402167)

Access Manager 7 2005Q4 wurde mit LDAP JDK 4.18 als Bestandteil der Java ES 2005Q4-Version ausgegeben, wodurch eine Reihe von Verbindungsproblemen mit Access Manager und Directory Server aufgetreten sind.

Umgehung: Wenden Sie nur eines der folgenden Sun Java System LDAP Java Development Kit-Patches an:

- Solaris OS-, SPARC- und x86-Plattformen: 119725-04
- Linux OS: 120834-02

Die Patches stehen unter SunSolve Online zur Verfügung.`http://sunsolve.sun.com`.

Dateien des Servers mit Verteilter Authentifizierungsbenutzeroberfläche werden im falschen Verzeichnis installiert (6352135)

Auf Solaris-Systemen installiert Java ES die Datei `Makefile.distAuthUI`, `README.distAuthUI` und `amauthdistui.war` des Servers mit Verteilter Authentifizierungsbenutzeroberfläche im falschen Verzeichnis: `/opt/SUNComm/SUNWam`.

Umgehung: Kopieren Sie diese Dateien in das richtige Verzeichnis: `/opt/SUNWam`.

Hinweis: Alle in einem Patch behobenen Probleme bezüglich des Servers mit Verteilter Authentifizierungsbenutzeroberfläche werden in die Datei `/opt/SUNComm/SUNWam/amauthdistui.war` aufgenommen. Sie müssen daher diese Dateien auch jedes Mal dann in das Verzeichnis `/opt/SUNWam` kopieren, wenn Sie einen Patch auf den Access Manager-Server anwenden und anschließend die WAR-Datei neu erstellen und bereitstellen.

CR# 6522720: Suchvorgänge in der Onlinehilfe der Konsole funktionieren unter Windows- und HP-UX-Systemen nicht für Multibyte-Zeichen.

Wenn Access Manager auf einem Windows- oder HP-UX-System in einem Gebietsschema installiert ist, das Multibyte-Zeichen verwendet (z. B. Japanisch), schlägt die Suche in der Konsolen-Onlinehilfe fehl, wenn Schlüsselwörter in Multibyte-Zeichen eingegeben werden.

Umgehung: Kein

Patch 6-Aktualisierung: Access Manager 7 2005Q4 Patch 6 behebt dieses Problem auf Windows-Systemen. Auf HP-UX-Systemen besteht das Problem weiterhin.

Unleserliche Multibyte-Zeichen in Ausgabemeldungen während der Access Manager-Konfiguration auf Windows-Systemen (6524251)

Wenn Access Manager auf einem Windows-System in einem Gebietsschema installiert ist, das Multibyte-Zeichen verwendet (z. B. Japanisch oder Chinesisch), sind die während der Access Manager-Konfiguration im Terminal-Fenster angezeigten Ausgabemeldungen nicht lesbar.

Umgehung: Keine; dieses Problem hat jedoch keine Auswirkungen auf die Konfiguration selbst.

Bei der Patch 5-Installation auf Windows-Systemen in nicht englischen Gebietsschemata werden Eigenschaftsschlüssel anstelle von Textmeldungen angezeigt (6526940)

Wenn Sie Patch 5 (124296-05) auf einem Windows-System in einem nicht englischen Gebietsschema installieren, werden manche Zeichenfolgen in der Installationsanzeige als Eigenschaftsschlüssel anstelle von Meldungstext angezeigt. Beispiele der Eigenschaftsschlüssel: `PRODUCT_NAME`, `JES_Patch_FinishPanel_Text1` und `JES_Patch_FinishPanel_Text2`.

Umgehung: Kein

Problem mit Eigenschaftseinstellung `com.iplanet.am.session.purgedelay` (6513653)

Das Access Manager-Skript `amtune` legt die Eigenschaft `com.iplanet.am.session.purgedelay` auf 1 fest, um so viele Access Manager-Sitzungen wie möglich zuzulassen. Diese Eigenschaft gibt die Anzahl der Minuten an, um die die Bereinigung der Sitzung verzögert wird. Der Wert 1 ist jedoch für manche Clients (z. B. Sun Java System Portal Server) unter Umständen nicht ausreichend.

Umgehung: Setzen Sie die Eigenschaft `com.iplanet.am.session.purgedelay` nach der Ausführung des Skripts `amtune` zurück:

1. Legen Sie in der Datei `AMConfig.properties` den neuen Wert für die Eigenschaft fest. Beispiel:

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

2. Starten Sie den Access Manager-Webcontainer neu, damit der neue Wert in Kraft tritt.

Access Manager 7 2005Q4-Patch 4

Access Manager 7 2005Q4-Patch 4 (Überarbeitung 04) behebt folgende Probleme:

- CR# 6463796: Deaktivierung des `iPlanetAMClientDetection`-Dienstes für `genericHTML` verhindert Zugriff auf Access Manager-HTML-Seiten
- CR 6463779: `amProfile_Client` der verteilten Authentifizierung und `amProfile_Server` des Access Manager-Servers enthalten unbedenkliche Ausnahmefehler
- CR 6463730: Cross-Site Scripting-(XSS-)Sicherheitslücke mit Parameter `goto` und `gx-charset`
- CR 6435889: Methode `Session.getSession` schlägt fehl, da `RestrictedTokenContext` nicht festgelegt ist

Bekannte Probleme und Einschränkungen in Patch 4

- "Leistungsoptimierung des Servers mit Verteilter Authentifizierungsbenutzeroberfläche (6470055)" auf Seite 47
- "Dienst zum Zurücksetzen von Passwörtern meldet Benachrichtigungsfehler bei einer Passwortänderung (6455079)" auf Seite 48

Leistungsoptimierung des Servers mit Verteilter Authentifizierungsbenutzeroberfläche (6470055)

Um die Leistung beim Lesen, Suchen und Vergleichen von Benutzerattributen für einen Server mit Verteilter Authentifizierungsbenutzeroberfläche zu optimieren, gehen Sie wie folgt vor:

1. Ändern Sie in der Datei `Makefile.distAuthUI` den Anwendungsbenutzernamen `anonymous` in einen anderen Benutzernamen um. Beispiel:

   ```
   APPLICATION_USERNAME=user1
   ```

2. Fügen Sie in Directory Server den neuen Benutzer (in diesem Beispiel `user1`) und die neue ACI hinzu, um das Lesen, Suchen und Vergleichen von Benutzerattributen zuzulassen. Im folgenden Beispiel wird die neue ACI hinzugefügt:

   ```
   dn:ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com
   changetype:modify add:aci
   aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com")
   (targetattr = *")(version 3.0;
   ```

```
acl "SunAM client data access to a Distributed Auth App User";
allow (read, search, compare)
userdn =  "ldap:///uid=user1,ou=people,dc=example,dc=com";)
```

Dienst zum Zurücksetzen von Passwörtern meldet Benachrichtigungsfehler bei einer Passwortänderung (6455079)

Wenn ein Passwort geändert wird, sendet Access Manager die E-Mail-Benachrichtigung mithilfe des nicht qualifizierten Sendernamens `Identity-Server`, was zu Fehlereinträgen in den `amPasswordReset`-Protokollen führt. Beispiel:

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

Umgehung: Ändern Sie die from-Adresse, sodass der vollständige Domänenname des Hostservers in der Datei `amPasswordResetModuleMsgs.properties` enthalten ist:

1. Ändern Sie die Angabe für die from-Adressbezeichnung. Beispiel:

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

2. Ändern Sie die Eigenschaft `lockOutEmailFrom`, um sicherzustellen, dass Sperrbenachrichtigungen die richtige from-Adresse verwenden. Beispiel:

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

   Die Datei `amPasswordResetModuleMsgs.properties` befindet sich im Verzeichnis *AccessManager-base*`/SUNWam/locale` (Solaris-Systeme) bzw. im Verzeichnis *AccessManager-base*`/identity/locale` (Linux-Systeme).

   AccessManager-base ist das Basisinstallationsverzeichnis. Das standardmäßige Basisinstallationsverzeichnis lautet `/opt` auf Solaris-Systemen und `/opt/sun` auf Linux-Systemen.

Access Manager 7 2005Q4-Patch 3

Access Manager 7-Patch 3 (Überarbeitung 03) behebt eine Reihe von Problemen, die in der README-Datei zum Patch aufgeführt sind. Des Weiteren enthält Patch 3 folgende neue Funktionen und bekannte Probleme:

Neue Funktionen in Patch 3

- "Neue Konfigurationseigenschaften für Siteüberwachung" auf Seite 49
- "Unterstützung für Liberty Identity Web Services Framework (ID-WSF) 1.1" auf Seite 50

Bekannte Probleme und Einschränkungen in Patch 3

Neue Konfigurationseigenschaften für Siteüberwachung

Die Siteüberwachungsfunktion von Access Manager enthält folgende neue Eigenschaften:

Eigenschaft	Beschreibung
`com.sun.identity.sitemonitor.interval`	Intervallzeit in Millisekunden für Siteüberwachung. Die Siteüberwachungsfunktion überprüft die Verfügbarkeit der einzelnen Sites im angegebenen Zeitintervall. Standard: 60000 Millisekunden (1 Minute).
`com.sun.identity.sitemonitor.timeout`	Zeitüberschreitung in Millisekunden für Überprüfung der Siteverfügbarkeit. Die Siteüberwachungsfunktion wartet auf eine Antwort von der Site, bis der angegebene Zeitüberschreitungswert erreicht wurde. Standard: 5000 Millisekunden (5 Sekunden).

Der Patch fügt diese Eigenschaften der Datei `AMConfig.properties` nicht hinzu. So verwenden Sie diese neuen Eigenschaften mit anderen Werten als den Standardwerten

1. Fügen Sie die Eigenschaften und deren Werte zur Datei `AMConfig.properties` im folgenden Verzeichnis (abhängig von der Plattform) hinzu:
   - Solaris-Systeme: `/etc/opt/SUNWam/config`
   - Linux-Systeme: `/etc/opt/sun/identity/config`

   Fügen Sie für Richtlinienagenten diese Eigenschaften der Datei `AMAgents.properties` hinzu.
2. Starten Sie den Access Manager-Webcontainer neu, damit die Werte in Kraft treten.

Benutzerdefinierte Implementierung. Die Klasse `com.sun.identity.sitemonitor.SiteStatusCheck` ermöglicht Ihnen zusätzlich, Ihre eigene Implementierung für die Überprüfung der Siteverfügbarkeit über folgende Schnittstelle anzupassen:

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

Alle Implementierungsklassen müssen die Methode `doCheckSiteStatus` verwenden.

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

Unterstützung für Liberty Identity Web Services Framework (ID-WSF) 1.1

WSF1.1 ist die in Access Manager 7-Patch 3 verwendete Standardversion von ID-WSF. Zum Auslösen von ID-WSF ist keine gesonderte Konfiguration erforderlich, die Beispiele müssen jedoch die neuen Sicherheitsmechanismen verwenden. Die neuen Sicherheitsmechanismen für ID-WSF1.1 lauten:

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

Neue Eigenschaft für Liberty ID-WSF-Unterstützung

Die Eigenschaft `com.sun.identity.liberty.wsf.version` legt das Liberty ID-WSF-Framework fest, wenn das Framework nicht von der eingehenden Nachricht oder vom Ressourcenangebot festgelegt werden kann und Access Manager als WSC agiert. Gültige Werte sind 1.0 und 1.1. Der Standardwert lautet 1.1.

Hinweis Bei der Patch-Installation wird die Eigenschaft `com.sun.identity.liberty.wsf.version` der Datei `AMConfig.properties` nicht hinzugefügt (6458184). Um diese neue Eigenschaft zu verwenden, fügen Sie sie der Datei `AMConfig.properties` mit dem enstprechenden Wert hinzu, nachdem Sie den Patch installiert und den Access Manager-Webcontainer neu gestartet haben.

Führen Sie nach der Installation von Access Manager 7-Patch 3 den folgenden Befehl aus, um die Schemaänderungen zu laden. Im folgenden Beispiel ist Access Manager im Standardverzeichnis für Solaris-Systeme installiert:

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

Die Erkennungsregistrierung von ID-WSF kann diese neuen Sicherheitsmechanismen bei der Registrierung verwenden. Darüber hinaus erkennen WSCs automatisch, welche Version bei der Kommunikation mit WSPs verwendet werden muss. Um die Konfiguration für ID-WSF1.1 vorzunehmen, folgen Sie den Anweisungen in den im Produkt enthaltenen Readme-Dateien für Liberty ID-FF Beispiel 1 und ID-WSF-Beispiele.

Protokoll `amProfile_Client` der verteilten Authentifizierung und Access Manager-Serverprotokoll `amProfile_Server` enthalten unbedenkliche Ausnahmefehler (6463779)

Anfragen bei Access Manager über die "Verteilte Authentifizierungsbenutzeroberfläche" lösen Ausnahmefehler im Protokoll `distAuth/amProfile_Client` und im Access Manager-Serverprotokoll `debug/amProfile_Server` aus. Nach mehreren Sitzungen kann das Protokoll `amProfile_Client` auf mehrere Gigabyte und das Access Manager-Serverprotokoll `amProfile_Server` auf mehrere Megabyte anwachsen. Die Funktionalität wird durch die

Ausnahmefehler in diesen Protokollen nicht beeinträchtigt. Die Ausnahmefehler können jedoch unnötigerweise Benutzer alarmieren und dazu führen, dass die Protokolle den gesamten Festplattenspeicherplatz einnehmen.

Lösung. Führen Sie `cron`-Aufträge aus, die den Inhalt der Protokolldateien auf null setzen. Beispiel:

- Führen Sie auf dem Client mit der "Verteilten Authentifizierungsoberfläche" in Abständen von einigen Stunden (je nach Datenverkehr) den Auftrag "`cat /dev/null > distAuth/amProfile_Client`" aus.
- Führen Sie auf dem Access Manager-Server in Abständen von einigen Tagen (anstatt in Abständen von einigen Stunden) "`cat /dev/null > /var/opt/SUNWam/debug/amProfile_Server`" aus.

Standardmäßiger Anwendungsbenutzer der verteilten Authentifizierung darf nicht `amadmin` sein (6460974)

Wenn Sie einen Server mit der "Verteilten Authentifizierungsbenutzeroberfläche" bereitstellen, darf der Administrator der verteilten Authentifizierung nicht `amadmin` sein. Der standardmäßige Anwendungsbenutzer der verteilten Authentifizierung in der Datei `Makefile.distAuthUI` lautet `amadmin` und somit auch in der Datei `AMConfig.properties`, nachdem die Datei `distAuth.war` auf Clientseite bereitgestellt wurde. Der Benutzer `amadmin` verfügt über ein `AppSSOToken`, das nach Zeitüberschreitung der `amadmin`-Sitzung abläuft. Dies kann zu einem SCHWEREN FEHLER in der Protokolldatei `amSecurity` führen, die sich standardmäßig im Verzeichnis `/tmp/distAuth` befindet.

Lösung. Geben Sie `UrlAccessAgent` als Anwendungsbenutzer der verteilten Authentifizierung an. Beispiel:

Ändern Sie vor der Bereitstellung der Datei `distAuth.war` im Client-Webcontainer folgende Parameter in der Datei `Makefile.distAuthUI` :

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

oder

Ändern Sie nach der Bereitstellung der Datei `distAuth.war` im Client-Webcontainer die folgenden Eigenschaften in der Datei `AMConfig.properties` für jeden Access Manager-Server:

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

Siehe auch "Die "Verteilte Authentifizierung" sollte nicht als amadmin-Benutzer ausgeführt werden (6440697)" auf Seite 56.

Fehlender Link für Benutzerdienst unter "Gefilterte Funktion" in Konsolenonlinehilfe (6460576)

In der Konsolenonlinehilfe zu Access Manager fehlt unter "Gefilterte Funktion" der Link zum Benutzerdienst. Navigieren Sie in der Onlinehilfe zu "Inhalt", "Gefilterte Funktion" und "So erstellen Sie eine gefilterte Rolle". Wenn Sie weiterblättern, wird je nach ausgewähltem Identitätstyp eine Liste mit Diensten angezeigt, ein Link zum Benutzerdienst ist jedoch nicht verfügbar.

Lösung. Kein

Zugriff auf den Server auf WebSphere nach Ausführung von `reinstallRTM` und der erneuten Bereitstellung von Webanwendungen nicht möglich (6460085)

Nach der Anwendung von Access Manager 7-Patch 3 in einer `DEPLOY_LEVEL=1`-Bereitstellung auf IBM WebSphere Application Server 5.1.1.6 unter Red Hat Linux AS 3.0 Update 4 wurde das Skript `reinstallRTM` ausgeführt, um die RTM-RPMs wiederherzustellen. Die Webanwendungen wurden anschließend erneut bereitgestellt, nachdem die vom Skript `reinstallRTM` generierte Datei `amsilent` bearbeitet wurde. WebSphere wurde dann mit den Skripten `stopServer.sh` und `startServer.sh` neu gestartet. Beim Zugriff auf die Anmeldeseite hat WebSphere jedoch einen 500-Fehler mit Verweis auf Filter `amlcontroller` angezeigt.

Dieses Problem trat auf, da die neue vom Skript `reinstallRTM` generierte Datei `server.xml` fehlerhaft war.

Lösung. Die vom Skript `amconfig` erstellte Kopie der Datei `server.xml` ist nach wie vor gültig. Verwenden Sie diese Kopie wie folgt:

1. Halten Sie den Server an.
2. Ersetzen Sie die fehlerhafte Datei `server.xml` durch die vom Skript `amconfig` erstellte Kopie der Datei.

   Die vom Skript `amconfig` erstellte Kopie der Datei `server.xml` hat den Namen `server.xml-orig-` *pid*, wobei *pid* die Prozess-ID des Skripts `amwas51config` ist. Die Datei befindet sich im folgenden Verzeichnis:

   WebSphere-home-directory`/config/cells/`*WebSphere-cell*
   `/nodes/`*WebSphere-node*`/servers/`*server-name*
3. Starten Sie den Server neu.

Markerklasse `sunISManagerOrganization` muss vor dem Aufrüsten zu Organisationen hinzugefügt werden (6455757)

Organisationen in einem Access Manager-Informationsverzeichnisbaum (Directory Information Tree, DIT), der mit einer Vorgängerversion von Access Manager 7 erstellt wurde, verfügen möglicherweise nicht über die Objektklasse `sunISManagerOrganization`. Ebenso ist in der Definition von Organisationen, die von einem anderen Produkt als Access Manager erstellt wurden, die Objektklasse `sunISManagerOrganization` nicht enthalten.

Lösung. Stellen Sie vor dem Aufrüsten auf Access Manager 7 2005Q4 sicher, dass alle Organisation im DIT in ihrer Definition über die Objektklasse `sunISManagerOrganization` verfügen. Fügen Sie die Objektklasse vor dem Aufrüsten gegebenenfalls manuell hinzu.

Aufrüsten auf Access Manager 7 2005Q4-Patch 2 verursacht Fehler auf der Registerkarte "Aktuelle Sitzungen" der Konsole (6454489)

Das Aufrüsten hat folgenden Fehler auf der Registerkarte "Aktuelle Sitzungen" der Access Manager-Konsole verursacht:

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

Dieses Problem betrifft Bereitstellungen, die von Access Manager 6-Versionen aufgerüstet werden und ein Root-Suffix im Format `o=orgname` aufweisen.

Lösung. Wenden Sie nach der Installation von Access Manager 7 2005Q4 den Access Manager 7-Patch 3 an und führen Sie anschließend das Skript `amupgrade` aus, um die Daten zu migrieren. Gehen Sie wie folgt vor:

1. Sichern Sie Ihren Access Manager 6-DIT.
2. Führen Sie das Skript `ampre70upgrade` aus.
3. Installieren Sie Access Manager 7 2005Q4 mit der Option "Später konfigurieren".
4. Heben Sie die Bereitstellung der Access Manager-Webanwendungen auf.
5. Stellen Sie die Access Manager-Webanwendungen bereit.
6. Wenden Sie den Access Manager 7-Patch 3 an, ohne dabei die XML/LDIF-Änderungen anzuwenden. Die XML/LDIF-Änderungen müssen nach der Ausführung des Skripts `amupgrade` im nächsten Schritt angewendet werden.
7. Führen Sie das Skript `amupgrade` aus.
8. Stellen Sie die Access Manager-Webanwendungen erneut bereit. Dies ist aufgrund der Änderungen durch den Access Manager 7-Patch 3 erforderlich.
9. Greifen Sie auf die Access Manager-Konsole zu.

Ausnahmefehler bei Verwendung der Abruffunktion zusammen mit dem Client-SDK (6452320)

Wenn Sie das Access Manager Client-SDK (`amclientsdk.jar`) bereitstellen und die Abruffunktion aktivieren, können beispielsweise folgende Fehler auftreten:

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

Fehler dieser Art können auftreten, wenn Sie einen Server mit Verteilter Authentifizierungsbenutzeroberfläche oder J2EE-Agenten bereitstellen bzw. wenn Sie das Access Manager Client-SDK auf einem Client bereitstellen.

Lösung. Beschränkt sich die Anzahl der gleichzeitigen Sitzungen auf einige hundert Sitzungen, fügen Sie folgende Eigenschaften und deren Werte entweder der Datei `AMConfig.properties` oder der Datei `AMAgents.properties` hinzu:

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

Handelt es sich um Tausende oder Zehntausende von Sitzungen, sollten die Werte mit den Werten für die Benachrichtigung in der Access Manager-Datei `AMConfig.properties` übereinstimmen, nachdem das Skript `amtune-identity` ausgeführt wurde. Für einen Rechner mit 4 GB RAM werden vom Access Manager-Skript `amtune-identity` beispielsweise folgende Werte festgelegt.

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

Legen Sie ähnliche Werte auf Clientseite in der Datei `AMAgent.properties` oder `AMConfig.properties` fest, wenn der Server mit der "Verteilten Authentifizierungsoberfläche" oder das Access Manager Client-SDK auf einem Client-Rechner mit 4 GB RAM bereitgestellt wird.

`SSOToken` eines authentifizierten Benutzers wird ungewollt auf Rogue-Websites angezeigt (6442905)

Durch Klicken auf einen URL auf einer Rogue-Website ist es möglich, dass ein authentifizierter Access Manager-Benutzer ungewollt den `SSOToken` auf der Rogue-Website anzeigt.

Lösung. Erstellen Sie für alle teilnehmenden Richtlinienagenten immer ein eindeutiges Agent-Benutzerprofil in Access Manager, um sicherzustellen, dass die Website keine Rogue-Website ist. Stellen Sie außerdem sicher, dass keiner der eindeutigen Agent-Benutzer dasselbe Passwort als gemeinsames geheimes Passwort bzw. `amldapuser` -Passwort verwendet. Richtlinienagenten werden beim Access Manager-Anwendungsauthentifizierungsmodul standardmäßig als `UrlAccessAgent`-Benutzer authentifiziert.

Weitere Informationen zum Erstellen eines Agenten unter Verwendung der Access Manager Administration Console finden Sie unter "Agents" in *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

Site-Überwachungsintervall und Eigenschaften der Zeitüberschreitung (6441918)

Access Manager-Sitefailover enthält folgende neue Eigenschaften:

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

Weitere Informationen finden Sie unter "Neue Konfigurationseigenschaften für Siteüberwachung" auf Seite 49.

Die "Verteilte Authentifizierung" sollte nicht als amadmin-Benutzer ausgeführt werden (6440697)

Um einen anderen Administrator als den standardmäßigen Administrator (`amadmin`) der Anwendungsauthentifizierung für die verteilte Authentifizierung zu erstellen, gehen Sie wie folgt vor:

1. Erstellen Sie einen LDAP-Benutzer für den Administrator der verteilten Authentifizierung. Beispiel:

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

2. Fügen Sie den Administrator der verteilten Authentifzierung der Liste der besonderen Benutzer hinzu. Beispiel:

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

   Fügen Sie diese Eigenschaft der Datei `AMConfig.properties` auf allen Access Manager-Servern hinzu, damit das `AppSSOToken` des Administrators der verteilten Authentifzierung bei Ablauf der Sitzung nicht abläuft.

Server mit Verteilter Authentfizierungsbenutzeroberfläche und Load Balancer (6440695)

Wenn in Ihrer Bereitstellung mehreren Servern mit verteilter Authentifizierungsbenutzeroberfläche ein Load Balancer vorgeschaltet ist, legen Sie nach Bereitstellung der WAR-Datei die folgenden Eigenschaften in der Datei `AMConfig.properties` fest.

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

Cookie-Wiedergabe erfordert Eigenschaft `com.sun.identity.session.resetLBCookie` (6440651)

Damit die Cookie-Wiedergabe für das Access Manager-Sitzungsfailover ordnungsgemäß ausgeführt wird, fügen Sie die Eigenschaft `com.sun.identity.session.resetLBCookie` mit dem Wert `true` sowohl für den Richtlinienagenten als auch für den Access Manager-Server hinzu. Beispiel:

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

- Fügen Sie für den Richtlinienagenten die Eigenschaft der Datei `AMAgents.properties` hinzu.
- Fügen Sie für Access Manager-Server die Eigenschaft der Datei `AMConfig.properties` hinzu.

Hinweis: Diese Eigenschaft ist nur erforderlich, wenn Sie das Access Manager-Sitzungsfailover implementiert haben.

`com.iplanet.am.lbcookie.name`-Eigenschaft übernimmt den Standardwert `amlbcookie` (6440648)

Der Richtlinienagent und der Access Manager-Server übernehmen standardmäßig den Load Balancer-Cookie-Namen `amlbcookie`. Wenn Sie den Cookie-Namen auf dem Back-End-Server ändern, müssen Sie denselben Namen in der Datei `AMAgent.properties` für den Richtlinienagenten verwenden. Ebenso müssen Sie denselben Cookie-Namen wie den vom Back-End-Server verwendeten Namen verwenden, wenn Sie das Access Manager Client-SDK verwenden.

Eigenschaft `com.iplanet.am.lbcookie.value` ist veraltet (6440641)

Access Manager unterstützt nicht mehr die Servereigenschaft `com.iplanet.am.lbcookie.value` zum Anpassen des Load Balancer-Cookies. Access Manager verwendet nun stattdessen für den vom Agenten wiedergegebenen Wert und Namen des Cookies die bei der Sitzungskonfiguration konfigurierte Server-ID.

SSO-Token im ID-FF-SSO-Anwendungsfall kann nicht erstellt werden (6429610)

Nach dem Einrichten von Liberty Identity Federation Framework (ID-FF) Beispiel 1 ist Federation erfolgreich, SSO schlägt jedoch fehl.

Lösung. Fügen Sie die `uuid` des Benutzers `dsameuser` der Eigenschaft `com.sun.identity.authentication.special.users` in der Datei `AMConfig.properties` hinzu. Für die Anwendungsauthentifzierung benötigt `dsameuser` ein nicht ablaufendes SSO-Token für den Access Manager-Server.

Wiederholte erfolgreiche Abfragen der Rollenmitgliedschaften eines Benutzers in einem LDAP v3-Datenspeicher bei Access Manager-Anmeldung (6389564)

Bei der Anmeldung eines Benutzers in Access Manager treten wiederholte LDAP-Suchabfragen des Benutzerattributs `nsRoleDN` auf.

Lösung. Führen Sie nach der Installation von Access Manager 7-Patch 3 den folgenden Befehl aus. Im folgenden Beispiel ist Access Manager im Standardverzeichnis für Solaris-Systeme installiert:

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

Das Authentifizierungsmodul muss in der Lage sein, den "goto"-URL zu überschreiben und einen anderen URL anzugeben (6385185)

Ein Authentifzierungsmodul kann den "goto"-URL überschreiben und die Umleitung zu einem anderen URL auf einer externen Website anfordern, um den Benutzerstatus zu bestätigen.

Um den "goto"-URL nach Abschluss der Authentifizierung zu überschreiben, legen Sie die im folgenden Beispiel gezeigte Eigenschaft im `SSOToken.` fest. Verwenden Sie zum Festlegen der Eigenschaft die `onLoginSuccess`-Methode der Klasse `PostProcess`, die das `AMPostAuthProcessInterface` implementiert. *OverridingURL* ist in diesem Beispiel der URL, der den "goto"-URL überschreibt:

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

Umleitung von einem benutzerdefinierten Authentifizierungsmodul aus bei noch ungültigem SSO-Token (6385184)

Die neue Funktion `RedirectCallback` für benutzerdefinierte Authentifizierungsmodule ermöglicht zum Überprüfen eines Benutzers die Umleitung auf eine externe Website über die Authentifizierungsbenutzeroberfläche. Bei erfolgreicher Authentifizierung wird der Benutzer zurück zum ursprünglichen Access Manager-Server-URL umgeleitet. Folgende Beispieldateien gehören dazu:

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

So implementieren Sie diese Funktion

1. Erstellen Sie mithilfe des Beispiels `LoginModuleSample.java` ein benutzerdefiniertes Authentifizierungsmodul.
2. Laden Sie das Modul auf einen Access Manager-Server.
3. Erstellen Sie `RedirectCallback` in der XML-Datei mithilfe des Beispiels `LoginModuleSample.xml`.
4. Um das Modul zu testen, verwenden Sie die Beispieldatei `testExtWebSite.jsp` als externe Website.
5. Melden Sie sich unter Verwendung des folgenden URLs an:

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

Der Benutzername und das Passwort werden zur Überprüfung auf die externe Website umgeleitet. Wenn Name und Passwort gültig sind, ist die Authentifizierung erfolgreich und der Benutzer wird zurück zum ursprünglichen Access Manager-Server-URL umgeleitet.

Im folgenden Beispielszenario wird in der Bereitstellung ein benutzerdefiniertes Authentifizierungsmodul für den Zugriff auf eine Geld-/Kreditkarten-Website verwendet:

1. Ein Benutzer ruft die Authentifizierungs-/Anmeldeseite für das benutzerdefinierte Authentifizierungsmodul auf.
2. Der Benutzer gibt seine Anmeldedaten (Benutzername und Passwort) ein und übermittelt eine Anforderung an das benutzerdefinierte Authentitfizierungsmodul.
3. Das benutzerdefinierte Authentifizierungsmodul leitet den Benutzer zusammen mit den erforderlichen Benutzerangaben und der Anforderung auf eine externe Geld-/Kreditkarten-Website um.
4. Die externe Geld-/Kreditkarten-Website überprüft den Benutzerstatus und gibt die Anforderung entweder als erfolgreich oder als nicht erfolgreich zurück. Der Status ist in der zurückgegebenen Anforderung festgelegt.

5. Das benutzerdefinierte Authentifizierungsmodul überprüft den Benutzer basierend auf dem in Schritt 4 zurückgegebenen Status und gibt den Status an den Authentifizierungsdienst zurück.
6. Die Benutzerauthentifizierung wird als erfolgreich oder als nicht erfolgreich abgeschlossen.

Federation schlägt bei Verwendung des Artefaktprofils fehl (6324056)

Umgehung: Um dieses Problem zu beheben, wenden Sie die für Ihre Plattform enstprechende aktuelle Version des Patches "Core Mobile Access" an:

- Solaris OS auf SPARC-basierten Systemen: 119527
- Solaris OS auf x86-Plattformen: 119528
- Linux-Systeme: 119529

Starten Sie nach Anwendung des Patches den Webcontainer neu.

Access Manager 7 2005Q4-Patch 2

Access Manager 7 2005Q4-Patch 2 (Überarbeitung 02) hat eine Reihe von Problemen behoben, die in der README-Datei zum Patch aufgeführt sind. Patch 2 enthält darüber hinaus folgende neue Funktionen und bekannte Probleme:

Neue Funktionen in Patch 2

- "Neue Eigenschaften für die Benutzerverwaltungs-, Identitäts-Repository- und Dienst-Verwaltungszwischenspeicher" auf Seite 61
- "Neue Eigenschaft für Federation-Dienstanbieter" auf Seite 63
- "Unterstützung für LDAP-Filterbedingung " auf Seite 63

Bekannte Probleme und Einschränkungen in Patch 2

- "Die Anzahl fehlgeschlagener Anmeldungen wird nicht an die Access Manager-Instanzen weitergegeben (6283582)" auf Seite 63
- "Ursprüngliche Sitzungsinformationen können beim Senden der Benachrichtigung zum Sitzungs-Timeout beibehalten werden (6293673)" auf Seite 64
- "Access Manager sollte den Benutzer darüber informieren, dass die Cookie-Unterstützung des Browsers deaktiviert/nicht verfügbar ist (6244578)" auf Seite 64
- "Bild-/Textplatzhalter während der Verarbeitung durch CDCServlet von "AuthNResponse" nach Anmeldung (6236892)" auf Seite 64
- "Neue Eigenschaft zum Deaktivieren persistenter Suchabfragen zur Anwendung in Ausnahmefällen (6363157)" auf Seite 65
- "Vorhandene und neue IDPs und SPs sind nicht sichtbar (6385696)" auf Seite 66

Neue Eigenschaften für die Benutzerverwaltungs-, Identitäts-Repository- und Dienst-Verwaltungszwischenspeicher

Patch 2 umfasst außerdem die folgenden neuen Eigenschaften für die Benutzerverwaltung (Access Manager-SDK), Identitäts-Repository- (IdRepo) und Dienst-Verwaltungszwischenspeicher. Diese Eigenschaften ermöglichen es Ihnen, die verschiedenen Zwischenspeicher in Abhängigkeit der Bereitstellungsanforderungen unabhängig voneinander zu aktivieren und zu deaktivieren sowie die Time to Live (TTL) für die Zwischenspeichereinträge festzulegen.

TABELLE 3 Neue Eigenschaften für die Benutzerverwaltungs-, Identitäts-Repository- und Dienst-Verwaltungszwischenspeicher

Eigenschaft	Beschreibung
Neue Eigenschaften zum Aktivieren und Deaktivieren von Zwischenspeichern	
`com.iplanet.am.sdk.caching.enabled`	Globale Eigenschaft, die die Identitäts-Repository- (IdRepo), Benutzerverwaltungs- und Dienst-Verwaltungszwischenspeicher aktiviert (true) oder deaktiviert (false). Falls der Wert mit true festgelegt oder die Eigenschaft nicht in der Datei `AMConfig.properties` vorhanden ist, sind alle drei Zwischenspeicher aktiviert.
Hinweis Die folgenden drei Eigenschaften zum Aktivieren bzw. Deaktivieren der jeweiligen Zwischenspeicher treffen nur zu, wenn der Wert der vorhergehenden globalen Eigenschaft mit false festgelegt ist.	
`com.sun.identity.amsdk.cache.enabled`	Aktiviert (true) bzw. deaktiviert (false) nur den Benutzerverwaltungszwischenspeicher (Access Manager-SDK).
`com.sun.identity.idm.cache.enabled`	Aktiviert (true) bzw. deaktiviert (false) nur den Identitäts-Repository (IdRepo)-Zwischenspeicher.
`com.sun.identity.sm.cache.enabled`	Aktiviert (true) bzw. deaktiviert (false) nur den Dienst-Verwaltungszwischenspeicher.
Neue Eigenschaften des Benutzerverwaltungszwischenspeichers für TTL	
`com.iplanet.am.` `sdk.cache.entry.expire.enabled`	Aktiviert (true) bzw. deaktiviert (false) die durch die folgenden beiden Eigenschaften definierte Ablaufzeit des Benutzerverwaltungszwischenspeichers.

TABELLE 3 Neue Eigenschaften für die Benutzerverwaltungs-, Identitäts-Repository- und Dienst-Verwaltungszwischenspeicher *(Fortsetzung)*

`com.iplanet.am.sdk.cache.entry.user.expire.time`	Gibt die Zeit in Minuten an, die Benutzereinträge für den Benutzerverwaltungszwischenspeicher nach ihrer letzten Bearbeitung gültig bleiben. Dies bedeutet, dass die Daten für den zwischengespeicherten Eintrag nach dieser bestimmten Zeit (nach der letzten Bearbeitung oder dem letzten Lesevorgang vom Verzeichnis) ablaufen. Neue Anforderungen für Daten dieser Einträge müssen dann vom Verzeichnis gelesen werden.
`com.iplanet.am.sdk.cache.entry.default.expire.time`	Gibt die Zeit in Minuten an, die Einträge, die nicht von Benutzern stammen, für den Benutzerverwaltungszwischenspeicher nach ihrer letzten Bearbeitung gültig bleiben. Dies bedeutet, dass die Daten für den zwischengespeicherten Eintrag nach dieser bestimmten Zeit (nach der letzten Bearbeitung oder dem letzten Lesevorgang vom Verzeichnis) ablaufen. Neue Anforderungen für Daten dieser Einträge müssen dann vom Verzeichnis gelesen werden. Neue Eigenschaften des Identitäts-Repository-Zwischenspeichers für TTL
`com.sun.identity.idm.cache.entry.expire.enabled`	Aktiviert (true) bzw. deaktiviert (false) die durch die folgende Eigenschaft definierte Ablaufzeit des Benutzerverwaltungszwischenspeichers.
`com.sun.identity.idm.cache.entry.default.expire.time`	Gibt die Zeit in Minuten an, die Einträge, die nicht von Benutzern stammen, für den IdRepo-Zwischenspeicher nach ihrer letzten Bearbeitung gültig bleiben. Dies bedeutet, dass die Daten für den zwischengespeicherten Eintrag nach dieser bestimmten Zeit (nach der letzten Bearbeitung oder dem letzten Lesevorgang vom Repository) ablaufen. Neue Anforderungen für Daten dieser Einträge müssen dann vom Repository gelesen werden.

Verwenden der neuen Eigenschaften beim Zwischenspeichern

Die Access Manager 7 2005Q4-Patches fügen die neuen Eigenschaften beim Zwischenspeichern nicht automatisch zur Datei `AMConfig.properties` hinzu.

So verwenden Sie die neuen Eigenschaften beim Zwischenspeichern

1. Fügen Sie die Eigenschaften und deren Werte mit einem Texteditor zur Datei `AMConfig.properties` im folgenden Verzeichnis (abhängig von der Plattform) hinzu:
   - Solaris-Systeme: `/etc/opt/SUNWam/config`
   - Linux-Systeme: `/etc/opt/sun/identity/config`

2. Starten Sie den Access Manager-Webcontainer neu, damit die Werte in Kraft treten.

Neue Eigenschaft für Federation-Dienstanbieter

Die neue Eigenschaft `com.sun.identity.federation.spadapter` definiert die Implementierungsklasse für `com.sun.identity.federation.plugins.FederationSPAdapter`, der zum Hinzufügen anwendungsspezfischer Prozesse während der Federation-Verarbeitung auf Dienstanbieterseite verwendet wird.

Weitere Informationen finden Sie unter "Vorhandene und neue IDPs und SPs sind nicht sichtbar (6385696)" auf Seite 66.

Unterstützung für LDAP-Filterbedingung

Die Unterstützung der LDAP-Filterbedingung wird in Patch 2 hinzugefügt. Ein Richtlinien-Administrator kann jetzt bei der Definition einer Richtlinie einen LDAP-Filter in der Bedingung angeben. Die Richtlinie wird nur dann auf den Benutzer angewendet, wenn der LDAP-Eintrag des Benutzers das in der Bedingung angegebenen LDAP-Filterkriterium erfüllt. Der LDAP-Eintrag des Benutzers wird in dem im Richtlinienkonfigurationsdienst angegebenen Verzeichnis gesucht.

Um die LDAP-Filterbedingung zu registrieren und zu verwenden, führen Sie nach der Installation von Access Manager 7-Patch 2 folgenden Befehl aus. Im folgenden Beispiel ist Access Manager im Standardverzeichnis für Solaris-Systeme installiert:

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

Hinweis zu Patch 5 Wenn Sie Access Manager 7 2005Q4-Patch 5 installiert und das Skript `updateschema.sh` ausgeführt haben, müssen Sie diese Dateien unter Verwendung von `amadmin` laden. Weitere Informationen finden Sie unter "Neues `updateschema.sh`-Skript zum Laden von LDIF- und XML-Dateien" auf Seite 31.

Die Anzahl fehlgeschlagener Anmeldungen wird nicht an die Access Manager-Instanzen weitergegeben (6283582)

Führen Sie nach der Installation von Access Manager 7-Patch 2 folgende Befehle aus. Im folgenden Beispiel ist Access Manager im Standardverzeichnis für Solaris-Systeme installiert:

```
# cd DirectoryServer-base/shared/bin
# ./ldapmodify -h DirectoryServerHost -p DirectoryServerPort
-D "cn=Directory Manager" -w DirectoryMangerPassword
```

```
-a -f /etc/opt/SUNWam/accountLockout.ldif
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/accountLockoutData.xml
```

Der Standardwert für *DirectoryServer-base* lautet `/var/opt/mps/serverroot` (Solaris-Systeme) bzw. `/var/opt/sun/directory-server` (Linux-Systeme).

Hinweis zu Patch 5 Wenn Sie Access Manager 7 2005Q4-Patch 5 installiert und das Skript `updateschema.sh` ausgeführt haben, müssen Sie diese Dateien unter Verwendung von `amadmin` laden. Weitere Informationen finden Sie unter "Neues `updateschema.sh`-Skript zum Laden von LDIF- und XML-Dateien" auf Seite 31.

Ursprüngliche Sitzungsinformationen können beim Senden der Benachrichtigung zum Sitzungs-Timeout beibehalten werden (6293673)

Die neue Eigenschaft `com.sun.identity.session.property.doNotTrimList` in der Datei `AMConfig.properties` kann eine kommagetrennte Liste mit Sitzungseigenschaftsnamen enthalten. Die in dieser Liste definierten Eigenschaften werden nach Ablauf einer Sitzung nicht entfernt, sodass auf die Eigenschaften zugegriffen werden kann, bevor die Sitzung bereinigt wird. Beispiel:

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

Access Manager sollte den Benutzer darüber informieren, dass die Cookie-Unterstützung des Browsers deaktiviert/nicht verfügbar ist (6244578)

Die neue Eigenschaft `com.sun.identity.am.cookie.check` in der Datei `AMConfig.properties` gibt an, ob der Server überprüfen soll, ob Cookies vom Browser unterstützt werden bzw. die Cookie-Unterstützung im Browser aktiviert ist. Wenn der Wert als `true` festgelegt ist, überprüft der Server, ob der Browser Cookies unterstützt bzw. ob die Cookie-Unterstützung aktiviert ist. Werden keine Cookies unterstützt bzw. ist die Cookie-Unterstützung nicht aktiviert, wird eine Fehlerseite ausgegeben. Dieser Wert muss als "false" (Standard) festgelegt werden, wenn der Server für die Authentifizierung einen Modus ohne Cookies unterstützen soll.

Bild-/Textplatzhalter während der Verarbeitung durch CDCServlet von "AuthNResponse" nach Anmeldung (6236892)

Die folgenden neuen Eigenschaften wurden der Datei `AMConfig.properties` hinzugefügt und werden vom CDCServlet gelesen:

- Mit `com.iplanet.services.cdc.WaitImage.display` wird im Browser ein Bild angezeigt, solange ein Benutzer in einem CDSSO-Szenario auf die Anzeige der geschützten Seite wartet. Hierzu muss die Eigenschaft auf "true" festgelegt sein. Der Standardwert ist "false".
- `com.iplanet.services.cdc.WaitImage.name` gibt den Bildnamen an. Der Standardwert ist `waitImage.gif`. Dieses Bild wird aus dem Verzeichnis `login_images` kopiert.
- `com.iplanet.services.cdc.WaitImage.width` gibt die Bildbreite an. Der Standardwert ist "420".
- `com.iplanet.services.cdc.WaitImage.height` gibt die Bildhöhe an. Der Standardwert ist "120".

Neue Eigenschaft zum Deaktivieren persistenter Suchabfragen zur Anwendung in Ausnahmefällen (6363157)

Die neue Eigenschaft `com.sun.am.event.connection.disable.list` in der Datei `AMConfig.properties` gibt an, welche Ereignisverbindung deaktiviert werden kann. Gültige Werte (Groß-/Kleinschreibung beachten):

`aci` - Änderungen des Attributs `aci`, wobei bei der Suche der LDAP-Filter (`aci=*`) angewendet wird.

`sm` - Änderungen des Access Manager-Informationsbaums (oder des Dienstverwaltungskontens), der Objekte mit der Markerobjektklasse `sunService` oder `sunServiceComponent` enthält. Sie können beispielsweise eine Richtlinie erstellen, um Zugriffsberechtigungen für eine geschützte Ressource festzulegen, oder die Regeln, Subjekte, Bedingungen oder Antwortanbieter für eine bestehende Richtlinie ändern.

`um` - Änderungen des Benutzerverzeichnisses (oder des Benutzerverwaltungsknotens). Sie können beispielsweise den Namen oder die Adresse eines Benutzers ändern.

So deaktivieren Sie beispielsweise die persistente Suche für Änderungen des Access Manager-Informationsbaums (oder des Dienstverwaltungsknotens)

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

Wenn Sie mehrere Werte angeben möchten, verwenden Sie als Trennzeichen ein Komma.

Achtung – Persistente Suchabfragen verursachen Performance-Overhead in Directory Server. In diesem Fall ist das Entfernen diese Performance-Overheads in einer Produktionsumgebung dringend erforderlich. Sie können eine oder mehrere persistente Suchabfragen mit der Eigenschaft `com.sun.am.event.connection.disable.list` deaktivieren.

Bevor Sie jedoch eine persistente Suche deaktivieren, sollten Sie mit den oben beschriebenen Einschränkungen vertraut sein. Es wird dringend empfohlen, diese Eigenschaft nur im absoluten Bedarfsfall zu ändern. Diese Eigenschaft wurde in erster Linie eingeführt, um Overhead auf Directory Server bei Einsatz mehrerer J2EE-Agenten zu vermeiden, da persistente Suchabfragen von jedem Agenten eingerichtet werden. Da die 2.2 J2EE-Agenten diese persistenten Suchabfragen nicht mehr einrichten, müssen Sie die Eigenschaft unter Umständen nicht verwenden.

Weitere Informationen finden Sie unter "Weitere Informationen zum Deaktivieren von persistenten Suchabfragen (6486927)" auf Seite 105.

Vorhandene und neue IDPs und SPs sind nicht sichtbar (6385696)

Die neue Eigenschaft `com.sun.identity.federation.spadapter` in der Datei `AMConfig.properties` gibt die standardmäßige Implementierung des Federation-Dienstanbieteradapters an, an dem die Anwendung Bestätigungsanweisungen und Antwortinformationen erhält. Beispiel:

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

Access Manager 7 2005Q4-Patch 1

Access Manager 7 2005Q4-Patch 1 (Überarbeitung 01) hat eine Reihe von Problemen behoben, die in der README-Datei zum Patch aufgeführt sind. Des Weiteren enthält Patch 1 folgende neue Funktionen und bekannte Probleme:

Erstellen von Debug-Dateien

Access Manager-Debug-Dateien werden standardmäßig im Debug-Verzeichnis erstellt, auch wenn die Eigenschaft `com.iplanet.services.debug.level` in der Datei `AMConfig.properties` auf false festgelegt ist. Vor der Herausgabe von Access Manager 7-Patch 1 wurden Debug-Dateien nur dann erstellt, wenn die erste Debug-Meldung in der Datei protokolliert wurde.

Unterstützung für Rollen und gefilterte Rollen im LDAPv3-Plugin

Access Manager 7-Patch 1 fügt Unterstützung für Rollen und gefilterte Rollen für das LDAPv3-Plugin hinzu, vorausgesetzt, die Daten sind in Sun Java System Directory Server gespeichert. Weitere Informationen finden Sie unter "Beschreibung der Unterstützung für Rollen und gefilterte Rolle für das LDAPv3-Plugin (6365196)" auf Seite 110.

`com.iplanet.am.session.client.polling.enable` auf Serverseite darf nicht true sein (6320475)

Die Eigenschaft `com.iplanet.am.session.client.polling.enable` in der Datei `AMConfig.properties` auf Serverseite wird standardmäßig auf false festgelegt und sollte niemals erneut auf true festgelegt werden.

Anwendung von Access Manager 7-Patch 1 schlägt fehl, wenn der Verschlüsselungsschlüssel eingebettete Leerzeichen enthält (6358751)

Wenn der Passwortverschlüsselungsschlüssel Leerzeichen enthält, schlägt die Anwendung des Patches fehl.

Lösung. Verwenden Sie einen neuen Verschlüsselungsschlüssel ohne Leerzeichen. Detailierte Anweisungen zum Ändern des Verschlüsselungsschlüssels finden Sie in: Anhang B, "Changing the Password Encryption Key" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Neue Funktionen in dieser Version

Eine Liste mit neuen Funktionen der Access Manager-Patch-Versionen finden Sie in "Access Manager 7 2005Q4 Patch-Versionen" auf Seite 10. Die ursprüngliche Version von Access Manager 7 2005Q4 enthält die folgenden neuen Eigenschaften:

- "Stapelverbund" auf Seite 73
- "Protokollierungserweiterungen" auf Seite 73

Access Manager-Modusarten

Access Manager 7 2005Q4 bietet sowohl Realm- als auch Legacy-Modus. Beide Modusarten unterstützen Folgendes:

- Die Funktionen von New Access Manager 7 2005Q4
- Die Funktionen von Access Manager 6 2005Q1 mit Ausnahme der folgenden Einschränkungen:
  - Beim Erstellen von Bereichen werden die entsprechenden Organisationen in Sun Java System Directory Server nicht erstellt.
  - Die neue Access Manager 7 2005Q4 Console kann keine CoS-Vorlagenpriorität (Class of Service) festlegen. Weitere Informationen finden Sie unter "Die neue Access Manager-Konsole kann keine CoS-Vorlagenprioritäten festlegen (6309262)" auf Seite 91.
- Identitätsrepositories in Sun Java System Directory Server und anderen Datenspeichern

Der Legacy-Modus ist erforderlich für:

- Sun Java System Portal Server
- Sun Java System Communications Services-Server, u.a. Messaging Server, Calendar Server, Instant Messaging oder Delegated Administrator
- Koexistenzbereitstellungen, wenn Access Manager 6 2005Q1 und Access Manager 7 2005Q4 auf denselben Directory Server zugreifen

Neue Access Manager-Konsole

Die Access Manager Console wurde für diese Version neu entworfen. Wenn Access Manager jedoch mit Portal Server, Messaging Server, Calendar Server, Instant Messaging oder Delegated Administrator bereitgestellt wird, muss Access Manager im Legacy-Modus installiert und die Access Manager 6 2005Q1 Console verwendet werden:

Weitere Informationen finden Sie unter "Kompatibilitätsprobleme" auf Seite 77.

Identitätsrepository

Ein Access Manager-Identitätsrepository enthält Informationen zu Identitäten, wie Benutzern, Gruppen und Rollen. Sie können ein Identitätsrepository unter Verwendung von Access Manager oder einem anderen Bereitstellungsprodukt, wie Sun Java System Identity Manager, erstellen und verwalten.

In der aktuellen Version kann ein Identitätsrepository entweder in Sun Java System Directory Server oder in Microsoft Active Directory vorhanden sein. Access Manager kann über Lese-/Schreibzugriff oder schreibgeschützten Zugriff auf ein Identitätsrepository verfügen.

Access Manager-Informationsbaum

Der Access Manager-Informationsbaum enthält Informationen zum Systemzugriff. Jede Access Manager-Instanz erstellt und verwaltet einen separaten Informationsbaum in Sun Java System Directory Server. Ein Access Manager-Informationsbaum kann einen beliebigen Namen (Suffix) haben. Der Access Manager-Informationsbaum umfasst Bereiche (sowie untergeordnete Bereiche, falls erforderlich), wie im folgenden Abschnitt beschrieben.

Access Manager-Realms

Ein Bereich sowie alle untergeordneten Bereiche sind Teil des Access Manager-Informationsbaums und können Konfigurationsinformationen enthalten, die eine Reihe von Benutzern und/oder Gruppen sowie die Authentifizierung von Benutzern definieren oder auf welche Ressourcen die Benutzer zugreifen können sowie die Informationen, die Anwendungen zur Verfügung stehen, nachdem den Benutzern Zugriff auf die Ressourcen gewährt wurde. Ein Bereich oder ein untergeordneter Bereich kann auch andere Konfigurationsinformationen enthalten, u. a. die Globalisierungskonfiguration, die Passwortrücksetzungskonfiguration, die Sitzungskonfiguration, die Konsolenkonfiguration und die Benutzervoreinstellungen. Ein Bereich oder ein untergeordneter Bereich kann auch leer sein.

Sie können einen Bereich mit Access Manager Console oder dem `amadmin`-CLI-Dienstprogramm erstellen. Weitere Informationen erhalten Sie in der Console-Onlinehilfe oder in Kapitel 14, “The amadmin Command Line Tool“ in *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

Änderungen des Sitzungsfailovers

Access Manager bietet eine webcontainer-unabhängige Sitzungsfailover-Implementierung, bei der Sun Java System Message Queue (Message Queue) als Kommunikationsvermittler und die Berkeley DB von Sleepycat Software, Inc. als Sitzungsspeicherdatenbank verwendet werden. Zu den Access Manager 7 2005Q4-Erweiterungen gehören u. a. das `amsfoconfig`-Skript zur Konfiguration der Sitzungsfailover-Umgebung sowie das `amsfo`-Skript zum Starten und Anhalten des Message Queue-Brokers und des Berkeley DB-Clients.

Weitere Informationen finden Sie unter “Implementing Access Manager Session Failover“ in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Benachrichtigung über eine Änderung der Sitzungseigenschaft

Mithilfe der Funktion zur Benachrichtigung über eine Änderung der Sitzungseigenschaft kann Access Manager eine Benachrichtigung an bestimmte Empfänger senden, wenn eine Änderung einer bestimmten Sitzungseigenschaft auftritt. Diese Funktion tritt in Kraft, wenn das Attribut "Enable Property Change Notifications" in der Access Manager Administrator Console aktiviert ist. In einer SSO-Umgebung (Single Sign-On) kann z. B. eine Access Manager-Sitzung von mehreren Anwendungen gemeinsam verwendet werden. Wenn für eine bestimmte Sitzungseigenschaft, die in der Liste "Notification Properties" definiert ist, eine Änderung auftritt, sendet Access Manager an alle registrierten Empfänger eine Benachrichtigung.

Weitere Informationen finden Sie unter "Enabling Session Property Change Notifications" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Beschränkungen der Sitzungsanzahl

Mit der Funktion der Beschränkungen der Sitzungsanzahl kann der Access Manager-Administrator (`amadmin`) das "Active User Sessions"-Attribut so festlegen, dass die maximale Anzahl gleichzeitiger Sitzungen für einen Benutzer beschränkt wird. Der Administrator kann eine Beschränkung der Sitzungsanzahl für alle Benutzer oder für eine Entität, z. B. ein Unternehmen, ein Bereich, eine Rolle oder einen Benutzer, festlegen, die für mindestens einen bestimmten Benutzer gilt.

Die Beschränkungen der Sitzungsanzahl sind standardmäßig deaktiviert (OFF), der Administrator kann sie jedoch aktivieren, indem er das Attribut "Enable Quota Constraints" in der Access Manager Administrator Console festlegt.

Der Administrator kann auch das Verhalten konfigurieren, wenn ein Benutzer die Beschränkung der Sitzungsanzahl ausgeschöpft hat, indem er das Attribut "Resulting Behavior If Session Quota Exhausted" festlegt:

- DENY_ACCESS. Access Manager weist die Anmeldeanforderung für eine neue Sitzung zurück.
- DESTROY_OLD_SESSION. Access Manager zerstört die nächste auslaufende vorhandene Sitzung für denselben Benutzer und ermöglicht eine erfolgreiche neue Anmeldeanforderung.

Das Attribut "Exempt Top-Level Admins From Constraint Checking" gibt an, ob die Sitzungsbeschränkungsquoten für die Administratoren der "Top-level Admin Role" gelten.

Weitere Informationen finden Sie unter "Setting Session Quota Constraints" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*

Verteilte Authentifizierung

Access Manager 7 2005Q4 enthält die Verteilte Authentifizierungsbenutzeroberfläche. Hierbei handelt es sich um eine UI-Komponente für Remote-Authentifizierung, die eine sichere, verteilte Authentifizierung bei zwei Firewalls in einer Bereitstellung ermöglicht. Ohne die Komponente für die Verteilte Authentifizierungsbenutzeroberfläche sind die Access Manager-Dienst-URLs unter Umständen für Endbenutzer sichtbar. Dieses Problem kann durch die Verwendung eines Proxy-Servers verhindert werden. Ein Proxy-Server ist jedoch für zahlreiche Bereitstellungen keine annehmbare Lösung.

Die Komponente für die Verteilte Authentifizierungsbenutzeroberfläche wird auf einem oder mehreren Servern innerhalb der nicht sicheren Schicht (DMZ-Schicht) einer Access Manager-Bereitstellung installiert. Access Manager wird auf einem Server für die Verteilte Authentifizierungsbenutzeroberfläche nicht ausgeführt, sondern ist lediglich vorhanden, um eine Authentifizierungsschnittstelle für Endbenutzer über einen Webbrowser bereitzustellen.

Der Endbenutzer sendet eine HTTP-Anforderung an die Komponente für die Verteilte Authentifizierungsbenutzeroberfläche, die wiederum eine Anmeldeseite für den Benutzer anzeigt. Die Komponente für verteilte Authentifizierung leitet die Anforderung des Benutzers durch die zweite Firewall an den Access Manager-Server weiter. Dadurch wird vermieden, dass die Firewall für die Kommunikation zwischen Endbenutzern und Access Manager-Server ?geöffnet“ werden muss.

Weitere Informationen finden Sie im Handbuch *Technical Note: Using Access Manager Distributed Authentication*.

Unterstützung von mehreren Authentifizierungsmodulinstanzen

Alle Authentifizierungsmodule (Standard) bieten Erweiterungsfunktionen zur Unterstützung des untergeordneten Schemas mit der Console UI-Unterstützung. Für jeden Modultyp (geladene Modulklasse) können mehrere Authentifizierungsmodulinstanzen erstellt werden. So kann z. B. für Instanzen mit Namen wie `ldap1` und `ldap2` für einen LDAP-Modultyp jede Instanz auf einen anderen LDAP-Verzeichnisserver verweisen. Modulinstanzen mit demselben Namen wie ihre Typen werden zur Rückwärtskompatibilität unterstützt. Der Aufruf lautet:

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

Authentifizierung "Named Configuration" oder Namespace "Chaining"

In einer Organisation bzw. in einem Bereich wird ein separater Namensraum erstellt, der eine Kette von Authentifizierungsmodulinstanzen darstellt. Dieselbe Kette kann erneut verwendet werden und einer Organisation/einem Bereich, einer Rolle oder einem Benutzer zugeordnet werden. Die Authentifizierungsdienst-Instanz entspricht der Authentifizierungskette. Der Aufruf lautet:

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

Richtlinienmodulerweiterungen

Personalisierungsattribute

Zusätzlich zu Regeln, Themen und Bedingungen können Richtlinien nun auch Personalisierungsattribute (`IDResponseProvider`) besitzen. Die von der Richtlinienprüfung gesendete Richtlinienentscheidung umfasst nun auch richtlinienbasierte Antwortpersonalisierungsattribute in den Anwendungsrichtlinien. Es werden zwei Arten von Personalisierungsattributen unterstützt:

- Statische Attribute. Sie definieren den Attributnamen und den Wert in der Richtlinie.
- Dynamische Attribute. Sie listen die Attributnamen in den Richtlinien auf. Die Werte werden zum Zeitpunkt der Richtlinienprüfung aus den Identitätsrepository-Datenspeichern abgerufen.

Policy Enforcement Points (Agents) leiten diese Attributwerte in der Regel als HTTP-Header, Cookies oder Anforderungsattribute an die geschützte Anwendung weiter.

Access Manager 7 2005Q4 unterstützt keine benutzerdefinierten Implementierungen der Antwortdienstanbieter-Schnittstelle, die von den Kunden durchgeführt werden.

Session Property Condition

Die Implementierung der Sitzungsrichtlinie (`SessionPropertyCondition`) entscheidet darüber, ob eine Richtlinie für die Anforderung gilt, basierend auf den Werten der Eigenschaften, die in der Access Manager-Sitzung eines Benutzers festgelegt werden. Zum Zeitpunkt der Richtlinienprüfung gibt die Bedingung den Wert "true" nur dann aus, wenn die Access Manager-Sitzung des Benutzers über jeden in der Bedingung definierten Eigenschaftswert verfügt. Für Eigenschaften, die mit mehreren Werten in der Bedingung definiert sind, ist es ausreichend, wenn die Benutzersitzung mindestens einen für die Eigenschaft in der Bedingung aufgelisteten Wert besitzt.

Richtlinienthema

Mit der Richtlinienthemaimplementierung (Access Manager Identity Subject) können Sie Einträge aus dem konfigurierten Identity Repository als Richtlinienthemawerte verwenden.

Richtlinienexport

Sie können Richtlinien mit dem Befehl `amadmin` im XML-Format exportieren. Die neuen `GetPolices`- und `RealmGetPolicies`-Elemente in der Datei `amAdmin.dtd` unterstützen diese Funktion.

Richtlinienstatus

Eine Richtlinie hat jetzt ein Statusattribut, das auf aktiv oder inaktiv festgelegt werden kann. Während der Richtlinienprüfung werden die inaktiven Richtlinien ignoriert.

Seitenkonfiguration

Access Manager 7 2005Q4 führt das "Sitekonzept" ein, das eine zentrale Konfigurationsverwaltung für eine Access Manager-Bereitstellung liefert. Wenn Access Manager als Site konfiguriert wird, werden die Clientanforderungen immer durch den Load Balancer geleitet, was die Bereitstellung vereinfacht und die Probleme, wie eine Firewall zwischen dem Client und den Access Manager-Backend-Servern, löst.

Weitere Informationen finden Sie unter "Configuring an Access Manager Deployment as a Site" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Stapelverbund

Access Manager 7 2005Q4 bietet einen Stapelverbund von Benutzerkonten für Anwendungen, die an Geschäftspartner ausgelagert werden. Zuvor musste bei einem Verbund von Konten zwischen einem Service Provider (SP) und einem Identity Provider (IDP) jeder Benutzer sowohl auf die SP- als auch auf die IDP-Sites zugreifen, Konten erstellen, falls keine vorhanden waren, und diese beiden Konten über einen Weblink miteinander verbinden. Dieser Vorgang war zeitaufwändig. Er war für eine Bereitstellung mit bereits vorhandenen Konten oder für eine Site, die selbst als Identitätsanbieter fungierte oder für die Verwendung einer seiner Partner als Authentifizierungsanbieter nicht immer geeignet.

Weitere Informationen finden Sie im *Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide* .

Protokollierungserweiterungen

Access Manager 7 2005Q4 bietet mehrere neue Protokollierungserweiterungen:

- Neue Felder (oder Spalten): Das Feld `MessageID` enthält die Nachrichten-ID für das protokollierte Ereignis. Das Feld `ContextID` enthält die Kontextkennung, die einer Sitzungskennung entspricht und für alle Ereignisse für die Anmeldesitzung eines bestimmten Benutzers gilt. Für eine bestimmte Anmeldesitzung eines Benutzers ist die `ContextID` in allen Protokolldateien für die protokollierten Ereignisse identisch.
- Protokollierungs-API. Die API bietet Zusätze zum Lesen von Protokolleinträgen, u. a. von einer Datenbank (DB), wenn die DB-Protokollierung konfiguriert ist. Weitere Informationen finden Sie unter `LogReaderSample.java` im `/opt/SUNWam/samples/logging`-Verzeichnis, das den Abruf von Protokolldatensätzen aus einer unstrukturierten Datei oder einem DB-Tabellenrepository zeigt.

Achtung – Datenbanktabellen sind in der Regel größer als Protokolle aus unstrukturierten Dateien. Deshalb sollten Sie bei einer bestimmten Anforderung nicht alle Datensätze in einer Datentabelle abrufen, da die Datenmenge alle Access Manager-Serverressourcen verbrauchen kann.

Hardware- und Software-Anforderungen

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

TABELLE 4 Hardware- und Software-Anforderungen

Komponente	Anforderung
Betriebssystem (OS)	Solaris OS auf SPARC™ basierenden Systemen, Version 8, 9 und 10, einschließlich Unterstützung für lokale root-Zonen der Version Solaris 10
	Solaris OS auf x86-Plattformen, Version 9 and 10, einschließlich Unterstützung für lokale root-Zonen der Version Solaris 10
	Solaris OS auf AMD64-Plattformen, Version 10, einschließlich Unterstützung für lokale root-Zonen
	Red Hat™ Linux, WS/AS/ES 2.1 Update 6 oder höher
	Red Hat Linux, WS/AS/ES 3.0
	Red Hat Linux, WS/AS/ES 3.0 Updates 1, 2, 3 und 4
	HP-UX-BS. Siehe Sun Java Enterprise System 4Q1258,2 Dokumentsammlung für HP-UX`http://docs.sun.com/coll/1258.2`
	Windows-BS. Siehe Sun Java Enterprise System 4Q1258,2 Document Collection for HP-UX`http://docs.sun.com/coll/1259.2`
Java 2 Standard Edition (J2SE)	J2SE-Plattform 1.5.0_04, 1.5_01, 1.5 und 1.4.2
Directory-Server	Access Manager-Informationsbaum: Sun Java System Directory Server 5 2005Q4
	Access Manager-Identitätsrepository: Sun Java System Directory Server 5 2005Q4 oder Microsoft Active Directory
Webcontainer	Sun Java System Web Server 6.1 2005Q4 SP5
	Sun Java System Application Server Enterprise Edition 8.1 2005Q2
	BEA WebLogic Server 8.1 SP4
	IBM WebSphere Application Server 5.1 und 5.1.1 (sowie die zugehörigen kumulativen Fixes)
RAM	Basistests: 512 MB
	Tatsächliche Bereitstellung: 1 GB für Threads, Access Manager SDK, HTTP-Server sowie andere interne Komponenten
Festplattenkapazität	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 2005Q4-Version unterstützten Browser aufgelistet.

TABELLE 5 Unterstützte Browser

Browser	Plattform
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000
Microsoft Internet Explorer 6.0	Windows 2000
	Windows XP
Mozilla 1.7.1	Solaris OS, Versionen 9 und 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0
Netscape™ 7.0	Solaris OS, Versionen 9 und 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0

Unterstützung für Systemvirtualisierung

Die Systemvirtualisierung ist eine Technologie, mit der mehrere Betriebssysteminstanzen unabhängig auf gemeinsam genutzter Hardware ausgeführt werden können. Funktionsgemäß ignoriert die Software, die unter einem in einer virtualisierten Umgebung gehosteten Betriebssystem bereitgestellt wird, dass die zugrunde liegende Plattform virtualisiert wurde. Sun testet seine Sun Java System-Produkte bezüglich ausgewählter Systemvirtualisierung und Betriebssystemkonfigurationen, um sicherzustellen, dass die Sun Java System-Produkte weiterhin in ordnungsgemäß dimensionierten und konfigurierten Umgebungen ebenso funktionieren wie in nicht virtualisierten Systemen. Informationen zu Sun-Support zu Sun Java System-Produkten finden Sie unter http://docs.sun.com/doc/820-4651.

Kompatibilitätsprobleme

Legacy-Modus von Access Manager

Wenn Sie Access Manager mit einem der folgenden Produkte installieren, müssen Sie den Access Manager Legacy (6.x)-Modus auswählen:

- Sun Java System Portal Server
- Sun Java System Communications Services-Server, u.a. Messaging Server, Calendar Server, Instant Messaging oder Delegated Administrator

Die Auswahl des Access Manager Legacy (6.x)-Modus richtet sich danach, wie das Java ES-Installationsprogramm ausgeführt wurde:

Weitere Informationen zum Modus einer Access Manager 7 2005Q4-Installation finden Sie unter “Ermitteln des Access Manager-Modus“ auf Seite 78.

Automatische Java ES-Installation mit einer Statusdatei

Die automatische Installation des Java ES-Installationsprogramms ist ein nicht interaktiver Modus, mit dem Sie Java ES-Komponenten auf mehreren Hostservern installieren können, die ähnliche Konfigurationen aufweisen. Zuerst führen Sie das Installationsprogramm aus, um eine Statusdatei zu generieren (ohne tatsächlich Komponenten zu installieren) und dann bearbeiten Sie eine Kopie der Statusdatei für jeden Hostserver, auf dem Sie die Installation von Access Manager und anderen Komponenten planen.

Um Access Manager im Legacy (6.x)-Modus auszuwählen, legen Sie den folgenden Parameter (zusammen mit anderen Parametern) in der Statusdatei fest, bevor Sie das Installationsprogramm im automatischen Modus ausführen:

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

Weitere Informationen zum Ausführen des Java ES-Installationsprogramms im automatischen Modus mithilfe einer Statusdatei finden Sie in Kapitel 5, “Installieren im stillen Modus“ in *Sun Java Enterprise System 2005Q4 Installationshandbuch für UNIX*.

Installationsoption "Configure Now" im grafischen Modus

Wenn Sie das Java ES-Installationsprogramm mit der Option "Configure Now" im grafischen Modus ausführen, müssen Sie im Fenster "Access Manager: Administration (1 of 6)" die Option "Legacy (version 6.x style)" auswählen, also den Standardwert.

Installationsoption "Configure Now" im textbasierten Modus

Wenn Sie das Java ES-Installationsprogramm im textbasierten Modus mit der Option "Configure Now" ausführen, wählen Sie für `Install type (Realm/Legacy) [Legacy]` die Option `Legacy`, also den Standardwert.

Installationsoption "Configure Later"

Wenn Sie das Java ES-Installationsprogramm mit der Option "Configure Later" ausgeführt haben, müssen Sie nach der Installation das `amconfig`-Skript zur Konfiguration von Access Manager ausführen. Um den Legacy (6.x)-Modus auszuwählen, legen Sie den folgenden Parameter in der Konfigurationsskript-Eingabedatei (`amsamplesilent`) fest:

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

Auf Windows-Systemen lautet die Konfigurationsdatei *AccessManager-base* `\setup\AMConfigurator.properties`.

Weitere Informationen zur Konfiguration von Access Manager durch Ausführen des `amconfig`-Skripts erhalten Sie im *Sun Java System Access Manager 7 2005Q4 Administration Guide* .

Ermitteln des Access Manager-Modus

Um zu ermitteln, ob eine ausgeführte Access Manager 7 2005Q4-Installation im Realm- oder Legacy-Modus installiert wurde, führen Sie folgenden Aufruf durch:

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

Die Ergebnisse lauten:

- wahr: Bereichsmodus
- false: Legacy-Modus

Access Manager-Richtlinienagenten

In der folgenden Tabelle wird die Kompatibilität von Richtlinienagenten mit den Access Manager 7 2005Q4-Modusarten dargestellt.

TABELLE 6 Kompatibilität von Richtlinienagenten mit den Access Manager 7 2005Q4-Modusarten

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

Installationshinweise

Die Access Manager-Installationshinweise enthalten die folgenden Informationen:

- "Legacy-Modus von Access Manager" auf Seite 77
- "Probleme bei der Installation" auf Seite 81

Bekannte Probleme und Einschränkungen

In diesem Abschnitt werden die folgenden bekannten Probleme und Lösungen beschrieben, die zum Zeitpunkt der Herausgabe verfügbar waren.

- "Kompatibilitätsprobleme" auf Seite 79
- "Probleme bei der Installation" auf Seite 81
- "Probleme bei der Aktualisierung" auf Seite 84
- "Konfigurationsprobleme" auf Seite 87
- "Probleme mit Access Manager Console" auf Seite 90
- "SDK- und Client-Probleme" auf Seite 93
- "Probleme mit den Befehlszeilendienstprogrammen" auf Seite 94
- "Authentifizierungsprobleme" auf Seite 95
- "Sitzungs- und SSO-Probleme" auf Seite 96
- "Richtlinienprobleme" auf Seite 98
- "Probleme beim Starten des Servers" auf Seite 99
- "Probleme auf Linux OS" auf Seite 100
- "Verbund- und SAML-Probleme" auf Seite 100
- "Globalisierungsprobleme (g11n)" auf Seite 102
- "Dokumentationsprobleme" auf Seite 104

Kompatibilitätsprobleme

- "Inkompatibilität zwischen Java ES 2004Q2-Servern und IM auf Java ES 2005Q4 (6309082)" auf Seite 80
- "Im Kernauthentifizierungsmodul gibt es Inkompatibilitäten für den Legacy-Modus (6305840)." auf Seite 80

Inkompatibilität zwischen Java ES 2004Q2-Servern und IM auf Java ES 2005Q4 (6309082)

Folgendes Bereitstellungsszenario verursachte dieses Problem:

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

Beim Ausführen des Dienstprogramms `imconfig` zur Konfiguration von Instant Messaging auf server-4 war die Konfiguration nicht erfolgreich. Das Access Manager 7 2005Q4 SDK, das von Instant Messaging (IM) auf server-4 verwendet wird, ist nicht mit Java ES 2004Q2 kompatibel.

Umgehung: Idealerweise sollten der Access Manager-Server und das Access Manager-SDK dieselbe Version aufweisen. Weitere Informationen finden Sie im *Sun Java Enterprise System 2005Q4 Aufrüstungshandbuch*.

Im Kernauthentifizierungsmodul gibt es Inkompatibilitäten für den Legacy-Modus (6305840).

Der Access Manager 7 2005Q4-Legacy-Modus weist die folgenden Inkompatibilitäten im Kernauthentifizierungsmodus von Access Manager 6 2005Q1 auf:

- Im Legacy-Modus werden die Organisationsauthentifizierungsmodule entfernt.
- Die Darstellung der "Administrator Authentication Configuration" und "Organization Authentication Configuration" hat sich geändert. In der Dropdown-Liste der Access Manager 7 2005Q4 Console ist standardmäßig `ldapService` ausgewählt. In der Access Manager 6 2005Q1 Console wurde die Schaltfläche zum Bearbeiten (Edit) bereitgestellt und das LDAP-Modul wurde nicht standardmäßig ausgewählt.

Umgehung: Keine.

Agent kann sich nicht anmelden, weil in der Organisation kein Profil vorhanden ist (6295074)

Erstellen Sie in der Access Manager Console einen Agenten im Realm-Modus. Wenn Sie sich abmelden und dann erneut mithilfe des Agentennamens anmelden, gibt Access Manager einen Fehler aus, da der Agent nicht über die Berechtigungen für den Realm-Zugriff verfügt.

Umgehung: Ändern Sie die Berechtigungen, um den Lese-/Schreibzugriff für den Agenten zu ermöglichen.

Das Dienstprogramm `commadmin` von Delegated Administrator erstellt keinen Benutzer (6294603)

Das Dienstprogramm `commadmin` von Delegated Administrator mit der Option `-S mail,cal` erstellt keinen Benutzer in der Standarddomäne.

Umgehung: Dieses Problem tritt auf, wenn Sie Access Manager auf Version 7 2005Q4 aktualisieren, Delegated Administrator jedoch nicht aktualisieren. Weitere Informationen zum Aktualisieren von Delegated Administrator finden Sie im *Sun Java Enterprise System 2005Q4 Aufrüstungshandbuch*.

Wenn Sie nicht vorhaben, Delegated Administrator zu aktualisieren, gehen Sie wie folgt vor:

1. Markieren Sie in der Datei `UserCalendarService.xml` die Attribute `mail`, `icssubcribed` und `icsfirstday` als optional und nicht als erforderlich. Diese Datei befindet sich auf Solaris-Systemen standardmäßig im Verzeichnis `/opt/SUNWcomm/lib/services/`.
2. Entfernen Sie in Access Manager die bereits vorhandene XML-Datei, indem Sie den Befehl `amadmin` wie folgt ausführen:

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

3. Fügen Sie in Access Manager die aktualisierte XML-Datei wie folgt hinzu:

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

4. Starten Sie den Access Manager-Webcontainer neu.

Das Dienstprogramm `commadmin` von Delegated Administrator erstellt keine Organisation (6292104)

Das Dienstprogramm `commadmin` von Delegated Administrator mit der Option `-S mail,cal` erstellt keine Organisation.

Umgehung: Die Lösung entspricht der des oben beschriebenen Problems.

Probleme bei der Installation

- "Für die Installation von Access Manager auf einem bereits vorhandenen DIT ist eine Wiederherstellung der Directory Server-Indizes erforderlich (6268096)" auf Seite 83
- "Die Protokollierungs- und Debug-Verzeichnisberechtigungen sind für Nicht-Root-Benutzer fehlerhaft (6257161)" auf Seite 83
- "Der Authentifizierungsdienst wird nicht initialisiert, wenn Access Manager und Directory Server auf unterschiedlichen Computern installiert sind. (6229897)" auf Seite 83
- "Das Installationsprogramm fügt für die bereits vorhandene Verzeichnisinstallation keinen Plattformeintrag hinzu (6202902)" auf Seite 83

Nach Anwendung von Patch 1 haben alle Benutzer Lesezugriff auf die Datei `/tmp/amsilent` (6370691)

Nachdem Sie Patch 1 angewendet haben, verfügen alle Benutzer über Lesezugriff auf die Datei `/tmp/amsilent`.

Umgehung: Setzen Sie nach Anwendung des Patches die Berechtigungen für die Datei so zurück, dass nur der Access Manager-Administrator über Lesezugriff verfügt.

Bei der SDK-Installation mit der Containerkonfiguration ist der Benachrichtigungs-URL fehlerhaft (6327845)

Wenn Sie eine SDK-Installation mit der Containerkonfiguration (DEPLOY_LEVEL=4) durchführen, ist der Benachrichtigungs-URL fehlerhaft.

Umgehung:

1. Legen Sie in der Datei `AMConfig.properties` die folgende Eigenschaft fest:

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

2. Starten Sie Access Manager neu, damit der neue Wert in Kraft tritt.

Access Manager `classpath` verweist auf das abgelaufene JCE 1.2.1-Paket (6297949)

Access Manager `classpath` verweist auf das Java Cryptography Extension (JCE) 1.2.1-Paket (Signing Certificate), das am 27. Juli 2005 abgelaufen ist.

Umgehung: Keine. Obwohl sich der Paketverweis im `classpath` befindet, verwendet Access Manager dieses Paket nicht.

Für die Installation von Access Manager auf einem bereits vorhandenen DIT ist eine Wiederherstellung der Directory Server-Indizes erforderlich (6268096)

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

Umgehung: Nachdem Sie Access Manager mit einem bereits vorhandenen Directory Information Tree (DIT) installiert haben, müssen Sie die Directory Server-Indizes neu erstellen, indem Sie das `db2index.pl`-Skript ausführen. Beispiel:

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

Das `db2index.pl`-Skript steht im Verzeichnis *DS-install-directory/slapd-hostname/* zur Verfügung.

Die Protokollierungs- und Debug-Verzeichnisberechtigungen sind für Nicht-Root-Benutzer fehlerhaft (6257161)

Wenn in der automatischen Installationskonfigurationsdatei ein Nicht-root-Benutzer angegeben ist, wurden die Berechtigungen für die Debug-, Protokoll- und Startverzeichnisse nicht ordnungsgemäß festgelegt.

Umgehung: Ändern Sie die Berechtigungen für diese Verzeichnisse, um den Zugriff für einen Nicht-root-Benutzer zu erlauben.

Der Authentifizierungsdienst wird nicht initialisiert, wenn Access Manager und Directory Server auf unterschiedlichen Computern installiert sind. (6229897)

Obwohl die `classpath`-Variablen sowie andere Access Manager-Webcontainervariablen während der Installation aktualisiert, beim Installationsvorgang wird jedoch kein Neustart des Webcontainers durchgeführt. Wenn Sie versuchen, sich nach der Installation jedoch vor dem Neustart des Webcontainers bei Access Manager anzumelden, wird folgender Fehler ausgegeben:

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

Umgehung: Starten Sie den Webcontainer neu, bevor Sie sich bei Access Manager anmelden. Directory Server muss ebenfalls ausgeführt werden, bevor Sie sich anmelden.

Das Installationsprogramm fügt für die bereits vorhandene Verzeichnisinstallation keinen Plattformeintrag hinzu (6202902)

Das Java ES-Installationsprogramm fügt für eine vorhandene Verzeichnisserverinstallation keinen Plattformeintrag hinzu (DIRECTORY_MODE=2).

Umgehung: Fügen Sie die Realm/DNS-Aliasnamen und Plattform-Serverlisteneinträge manuell hinzu. Anweisungen zu diesen Schritten finden Sie unter "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Probleme bei der Aktualisierung

Access Manager-Skript `ampre70upgrade` entfernt lokalisierte Pakete nicht (6378444)

Wenn Sie Access Manager auf Access Manager 7 2005Q4 aktualisieren, entfernt das Skript `ampre70upgrade` keine auf Ihrem System vorhandenen lokalisierten Access Manager-Pakete.

Umgehung: Bevor Sie die Aktualisierung auf Access Manager 7 2005Q4 durchführen, verwenden Sie den Befehl `pkgrm`, um sämtliche auf Ihrem System installierten, lokalisierten Access Manager-Pakete manuell zu entfernen.

Die Datei `AMConfig.properties` enthält eine alte Version des Webcontainers (6316833)

Nachdem Access Manager und Application Server auf Java ES 2005Q4-Versionen aktualisiert wurden, enthält die `AMConfig.properties`-Datei von Access Manager eine alte Version von Application Server.

Umgehung: Bevor Sie das Delegated Administrator-Konfigurationsprogramm (`config-commda`) ausführen, ändern Sie die folgende Eigenschaft in der Datei `AMConfig.properties`:

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

Die Datei `server.policy` des Knotenagenten wird nicht als Teil einer Access Manager-Aktualisierung aktualisiert (6313416)

Nachdem Sie Access Manager aktualisiert haben, wird die Datei `server.policy` des Knotenagenten nicht aktualisiert.

Umgehung: Ersetzen Sie die Datei `server.policy` des Knotenagenten durch die folgende Datei:

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

Nach der Aktualisierung fehlt "Session Property Condition" in der Bedingungsliste (6309785)

Nachdem Sie Access Manager von Version 2005Q1 auf Version 2005Q4 aktualisiert haben, wird die Session Property Condition in der Richtlinienbedingungsliste nicht als Option angezeigt, wenn Sie versuchen, einer Richtlinie eine Bedingung hinzuzufügen.

Umgehung: Wählen Sie den Typ "Session Property Condition" in der Dienstvorlage zur Richtlinienkonfiguration im entsprechenden Realm.

Nach der Aktualisierung fehlt der Typ "Identity Subject" in der Richtlinienthemaliste (6304617)

Nachdem Sie Access Manager von Version 2005Q1 auf Version 2005Q4 aktualisiert haben, wird "Identity Subject", ein neuer Richtlinienthematyp, nicht als Option in der Richtlinienthemaliste angezeigt.

Umgehung: Wählen Sie den Typ "Identity Subject" als Standardthematyp in der Vorlage für den Richtlinienkonfigurationsdienst aus.

Die Access Manager-Aktualisierung ist fehlgeschlagen, weil keine `classpath`-Migration stattgefunden hat (6284595)

Während der Aktualisierung von Access Manager von Java ES 2004Q2 auf Java ES 2005Q4, ist die Aktualisierung von Java ES 2004Q2 auf Java ES 2005Q1 fehlgeschlagen. Access Manager wurde auf einem Application Server bereitgestellt, der ebenfalls von Java ES 2004Q2 auf Java ES 2005Q4 aufgerüstet wurde. Der `classpath` in der Datei `domain.xml` enthielt jedoch nicht die Pfadangaben für die Access Manager-JAR-Dateien.

Umgehung: Führen Sie diese Schritte durch:

1. Bevor Sie das `amupgrade`-Skript ausführen, indizieren Sie Directory Server aufgrund eines Problems mit dem `comm_dssetup.pl`-Skript neu.

2. Fügen Sie der Datei `server.policy` des Knotenagenten Einträge für Access Manager hinzu. Eine Kopie von `server.policy` aus der Standardserverrichtlinie (`/var/opt/SUNWappserver/domains/domain1/config/server.policy`) ist ausreichend.
3. Aktualisieren Sie `classpath` in der `domain.xml` -Datei des Knotenagenten wie folgt. Kopieren Sie das `classpath-suffix` und den entsprechenden `classpath` aus den `server-classpath`-Attributen des `java-config`-Elements aus der Datei `server.xml` in die entsprechenden Attribute des `java-config`-Elements von `domain.xml`. Das `java-config`-Element ist unter dem `config`-Element in `domain.xml` zu finden.

Nach der Aktualisierung gibt der `amadmin`-Befehl eine falsche Version aus (6283758)

Nachdem Access Manager von Version 6 2005Q1 auf Version 7 2005Q4 aktualisiert wurde, gab der `amadmin --version`-Befehl die falsche Version aus: Sun Java System Access Manager Version 2005Q1.

Umgehung: Nachdem Sie Access Manager aktualisiert haben, führen Sie zur Konfiguration von Access Manager das `amconfig`-Skript aus. Wenn Sie `amconfig` ausführen, geben Sie den vollständigen Pfad der Konfigurationsdatei (`amsamplesilent`) an. Auf einem Solaris-System zum Beispiel:

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

oder

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

Attribut `ContainerDefaultTemplateRole` nach Datenmigration hinzufügen (4677779)

Die Rolle eines Benutzers wird nicht in einer Organisation angezeigt, die nicht in Access Manager erstellt wurde. Im Debug-Modus wird folgende Meldung angezeigt:

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

Dieser Fehler tritt auf, nachdem die Migrationsskripte des Java ES-Installationsprogramms ausgeführt wurden. Das Attribut `ContainerDefaultTemplateRole` wird der Organisation nicht automatisch hinzugefügt, wenn die Organisation aus einem vorhandenen Informationsverzeichnisbaum (Directory Information Tree, DIT) oder aus einer anderen Quelle migriert wurde.

Umgehung: Verwenden Sie die Directory Server-Konsole, um das Attribut `ContainerDefaultTemplateRole` aus einer anderen Access Manager-Organisation zu kopieren und es anschließend der betreffenden Organisation zuzuweisen.

Konfigurationsprobleme

Die Datei `server.policy` von Application Server 8.1 muss bei der Verwendung von nicht standardmäßigen URIs bearbeitet werden (6309759)

Wenn Sie Access Manager 7 2005Q4 auf Application Server 8.1 bereitstellen und Sie keine Standard-URIs für die Dienst-, Konsolen- und Passwortwebanwendungen verwenden, die die Standard-URI-Werte `amserver`, `amconsole` und `ampassword` aufweisen, müssen Sie die Datei `server.policy` der Anwendungsserverdomäne bearbeiten, bevor Sie versuchen, auf Access Manager über einen Webbrowser zuzugreifen.

Umgehung: Bearbeiten Sie die Datei `server.policy` wie folgt:

1. Halten Sie die Application Server-Instanz, auf der Access Manager bereitgestellt wird, an.
2. Wechseln Sie in das `/config`-Verzeichnis. Beispiel:

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

3. Erstellen Sie eine Sicherungskopie der Datei `server.policy`. Beispiel:

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

4. Suchen Sie in der Datei `server.policy` nach folgenden Richtlinien:

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

```
applications/j2ee-modules/ampassword/-" { ...
};
```

5. Ersetzen Sie `amserver` durch die Nicht-Standard-URI, die für die Dienstwebanwendung verwendet wird, in der folgenden Zeile:

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

6. Ersetzen Sie für Installationen im Legacy-Modus `amconsole` durch die Nicht-Standard-URI, die für die Konsolenwebanwendung verwendet wird, in der folgenden Zeile:

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

7. Ersetzen Sie amserver durch die Nicht-Standard-URI, die für die Passwortwebanwendung verwendet wird, in der folgenden Zeile:

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

8. Starten Sie die Application Server-Instanz, auf der Access Manager bereitgestellt wird.

Die Plattformserverliste und das FQDN-Aliasattribut werden nicht aktualisiert (6309259, 6308649)

Bei einer Mehrfachserverbereitstellung werden die Plattformserverliste und das FQDN-Aliasattribut nicht aktualisiert, wenn Sie Access Manager auf den sekundären (und nachfolgenden) Servern installieren.

Umgehung: Fügen Sie die Realm/DNS-Aliasnamen und Plattform-Serverlisteneinträge manuell hinzu. Anweisungen zu diesen Schritten finden Sie unter "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Datenvalidierung für erforderliche Attribute in Diensten (6308653)

Access Manager 7 2005Q4 erzwingt für die erforderlichen Attribute in XML-Dateien von Diensten Standardwerte.

Umgehung: Falls Sie über Dienste mit erforderlichen Attributen verfügen, die keine Werte aufweisen, fügen Sie für die Attribute Werte hinzu und laden Sie den Dienst dann erneut.

Dokumentieren der Abhilfe für die Bereitstellung auf einer sicheren WebLogic 8.1-Instanz (6295863)

Wenn Sie Access Manager 7 2005Q4 in einer sicheren (SSL-fähigen) BEA WebLogic 8.1 SP4-Instanz bereitstellen, tritt während der Bereitstellung der einzelnen Access Manager-Webanwendungen eine Ausnahme auf.

Umgehung: Führen Sie diese Schritte durch:

1. Wenden Sie das WebLogic 8.1 SP4-Patch JAR `CR210310_81sp4.jar` an, das Sie von BEA beziehen können.
2. Aktualisieren Sie im `/opt/SUNWam/bin/amwl81config`-Skript (Solaris-Systeme) oder im `/opt/sun/identity/bin/amwl81config`-Skript (Linux-Systeme) die `doDeploy`-Funktion und die `undeploy_it`-Funktion, um den Pfad der Patch-JAR `wl8_classpath` voranzustellen, wobei es sich um die Variable handelt, die den `classpath` enthält, der zum Bereitstellen und zum Aufheben der Bereitstellung der Access Manager-Webanwendungen verwendet wird.

   Suchen Sie die folgende Zeile, die den `wl8_classpath` enthält:

   ```
   wl8_classpath= ...
   ```

3. Fügen Sie unmittelbar nach der Zeile, die Sie in Schritt 2 gefunden haben, die folgende Zeile hinzu:

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

Das `amconfig`-Skript aktualisiert die Realm-/DNS-Aliasnamen und Plattformserver-Listeneinträge nicht (6284161)

Bei einer Mehrfachserverbereitstellung aktualisiert das `amconfig`-Skript die Realm-/DNS-Aliasnamen und Plattformserver-Listeneinträge für zusätzliche Access Manager-Instanzen nicht.

Umgehung: Fügen Sie die Realm/DNS-Aliasnamen und Plattform-Serverlisteneinträge manuell hinzu. Anweisungen zu diesen Schritten finden Sie unter "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Der Access Manager-Standardmodus ist der Realm in der Konfigurationsstatus-Dateivorlage (6280844)

Der Access Manager-Modus (`AM_REALM`-Variable) ist in der Konfigurationsstatus-Dateivorlage aktiviert.

Umgehung: Um Access Manager im Legacy-Modus zu installieren oder zu konfigurieren, legen Sie die Variable in der Statusdatei neu fest:

```
AM_REALM = disabled
```

URL-Signierung in IBM WebSphere bei Verwendung des RSA-Schlüssels schlägt fehl (6271087)

Wenn Sie einen RSA-Schlüssel in IBM WebSphere verwenden, schlägt der Signiervorgang der URL-Zeichenfolge mit folgender Ausnahme fehl:

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

Umgehung: Der Anbieter ?SunRsaSign“ fehlt in dem in WebSpere enthaltenen JDK. Um dieses Problem zu lösen, bearbeiten Sie die Datei *websphere_jdk_root*`/jre/lib/security/java.security` und fügen Sie folgende Zeile hinzu, um ?SunRSASign“ als einen der Anbieter zu aktivieren:

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

Probleme mit Access Manager Console

Bei SAML treten beim Trusted Partner-Duplizieren in der Konsole Bearbeitungsfehler auf (6326634)

Erstellen Sie unter der Access Manager Console einen SAML Trusted Partner unter der Registerkarte "Federation > SAML". Wenn Sie versuchen, den Trusted Partner zu duplizieren, treten Fehler auf.

Umgehung: Keine. Dieses Problem wurde in Patch 1 behoben. Informationen zur Anwendung des Patches für Ihre Plattform finden Sie unter "Access Manager 7 2005Q4-Patch 1" auf Seite 66.

Die Remote-Protokollierung funktioniert für `amConsole.access` und `amPasswordReset.access` nicht (6311786)

Wenn die Remote-Protokollierung konfiguriert wird, werden alle Protokolle in die Access Manager-Remoteinstanz geschrieben, mit Ausnahme von `amConsole.access` und `amPasswordReset.access` für die Passwortrücksetzinformationen. Der Protokolldatensatz wird nirgendwo geschrieben.

Umgehung: Keine.

Das Hinzufügen von weiteren `amadmin`-Eigenschaften in der Konsole ändert das Benutzerpasswort `amadmin` (6309830)

Wenn einige der Eigenschaften für den `amadmin`-Benutzer in der Verwaltungskonsole hinzugefügt oder bearbeitet werden, ändert sich das `amadmin`-Benutzerpasswort.

Umgehung: Keine. Dieses Problem wurde in Patch 1 behoben. Informationen zur Anwendung des Patches für Ihre Plattform finden Sie unter "Access Manager 7 2005Q4-Patch 1" auf Seite 66.

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

Die neue Access Manager 7 2005Q4 Console kann keine CoS-Vorlagenpriorität festlegen oder ändern.

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

Es tritt ein Ausnahmefehler auf, wenn einem Benutzer eine Gruppe als Richtlinienadminbenutzer hinzugefügt wird (6299543)

Die Access Manager Console gibt einen Ausnahmefehler zurück, wenn Sie einem Benutzer eine Gruppe als Richtlinienadminbenutzer hinzufügen.

Umgehung: Keine.

Im Legacy-Modus können nicht alle Benutzer aus einer Rolle gelöscht werden (6293758)

Wenn Sie im Legacy-Modus alle Benutzer aus einer Rolle löschen möchten, bleibt ein Benutzer übrig.

Umgehung: Versuchen Sie erneut, den Benutzer aus der Rolle zu löschen.

Discovery Service-Ressourcenangebote können nicht hinzugefügt, gelöscht oder geändert werden (6273148)

Mit der Access Manager Administration Console können Sie die Ressourcenangebote für einen Benutzer, eine Rolle oder einen Realm nicht hinzufügen, löschen oder ändern.

Umgehung: Keine. Dieses Problem wurde in Patch 1 behoben. Informationen zur Anwendung des Patches für Ihre Plattform finden Sie unter "Access Manager 7 2005Q4-Patch 1" auf Seite 66.

Das falsche LDAP-Bindungspasswort sollte Fehler für die Themensuche ausgeben (6241241)

Die Access Manager Administration Console gibt keinen Fehler aus, wenn ein falsches LDAP-Bindungspasswort verwendet wird.

Umgehung: Keine.

Access Manager kann keine Organisation unter einem Container im Legacy-Modus erstellen (6290720)

Wenn Sie einen Container erstellen und dann versuchen, eine Organisation unter dem Container zu erstellen, gibt Access Manager einen Fehler aus, dass die Eindeutigkeit verletzt wurde.

Umgehung: Keine.

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.

Umgehung: 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)

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 die Benutzer in der Gruppe. Fügen Sie zum Beispiel Benutzer mit dem Filter `uid=*999*` hinzu. Das resultierende Listenfeld ist leer und die Konsole zeigt keinen Fehler, keine Informationen und keine Warnmeldungen an.

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

SDK- und Client-Probleme

Die Session Service-Konfiguration für einen untergeordneten Realm kann nicht entfernt werden (6318296)

Nachdem Sie einen untergeordneten Realm des obersten Realms erstellt und ihm den Session Service hinzugefügt haben, führte der nachfolgende Versuch, die Session Service-Konfiguration zu entfernen, zu einer Fehlermeldung.

Umgehung: Entfernen Sie das oberste ID-Standardrepository AMSDK1 und fügen Sie dann dieses Repository wieder der Konfiguration hinzu.

Dieses Problem wurde in Patch 1 behoben. Informationen zur Anwendung des Patches für Ihre Plattform finden Sie unter "Access Manager 7 2005Q4-Patch 1" auf Seite 66.

CDC-Servletumleitung an die ungültige Anmeldeseite, wenn die Richtlinienbedingung angegeben ist (6311985)

Wenn sich der Apache-Agent 2.2 beim Zugriff auf die Agent-geschützte Ressource im CDSSO-Modus befindet, leitet das CDC-Servlet den Benutzer auf die anonyme Authentifizierungsseite und nicht auf die Standardanmeldeseite um.

Umgehung: Keine. Dieses Problem wurde in Patch 1 behoben. Informationen zur Anwendung des Patches für Ihre Plattform finden Sie unter "Access Manager 7 2005Q4-Patch 1" auf Seite 66.

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.

Umgehung: Keine.

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

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

Umgehung: Starten Sie den Client nach einer Dienstschemaänderung neu.

Dieses Problem wurde in Patch 1 behoben. Informationen zur Anwendung des Patches für Ihre Plattform finden Sie unter "Access Manager 7 2005Q4-Patch 1" auf Seite 66.

Probleme mit den Befehlszeilendienstprogrammen

Die Suche nach Null-Attributen gibt einen Fehler zurück, wenn Access Manager auf Directory Proxy (6357975) verweist.

Wenn Sie Sun Java System Directory Proxy Server verwenden, gibt die LDAP-Suche einen Fehler zurück. Beispiel:

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

Wenn Access Manager direkt auf den LDAP Directory Server verweist, ist dieselbe Suche erfolgreich.

Umgehung: Wenn Sie Directory Proxy Server verwenden, aktivieren Sie entweder Null-Attribut-Suchen, oder geben Sie einen Attributnamen für die Suche an.

Im `amserveradmin`-Skript fehlen neue Schemadateien (6255110)

Wenn Sie nach der Installation das `amserveradmin`Skript zum Laden der Dienste in Directory Server ausführen möchten, fehlen im Skript die `defaultDelegationPolicies.xml`- und `idRepoDefaults.xml`-Schemadateien.

Umgehung: Laden Sie die `defaultDelegationPolicies.xml`- und `idRepoDefaults.xml`-Dateien unter Verwendung des `amadmin`-CLI-Tools mit der Option `-t` manuell.

XML-Dokumente mit Escape-Zeichen können in Internet Explorer 6.0 nicht gespeichert werden (4995100)

Wenn Sie ein Sonderzeichen (z. B. die Zeichenfolge "`amp;`" neben ein "`&`") in einer XML-Datei hinzufügen, wird die Datei ordnungsgemäß gespeichert. Wenn Sie das XML-Profil jedoch zu einem späteren Zeitpunkt mit Internet Explorer 6.0 abrufen, wird die Datei nicht ordnungsgemäß angezeigt. Wenn Sie dann erneut versuchen, das Profil zu speichern, wird ein Fehler ausgegeben.

Umgehung: Keine.

Authentifizierungsprobleme

`UrlAccessAgent`-SSO-Token läuft ab (6327691)

Der `UrlAccessAgent`-SSO-Token läuft ab, da das Anwendungsmodul den speziellen Benutzer-`DN` nicht zurückgibt, was dazu führt, dass der spezielle Benutzer-`DN` und ein nicht ablaufendes Token fehlschlagen.

Umgehung: Keine. Dieses Problem wurde in Patch 1 behoben. Informationen zur Anwendung des Patches für Ihre Plattform finden Sie unter "Access Manager 7 2005Q4-Patch 1" auf Seite 66.

Anmeldung am untergeordneten Realm mit LDAPV3-Plugin/dynamischen Profil ist nach Korrigieren des Passworts nicht möglich (6309097)

Wenn Sie im Realm-Modus einen ldapv3-Datenspeicher in einem Realm mit einem "falschen" Passwort erstellen und Sie das Passwort zu einem späteren Zeitpunkt als `amadmin` ändern, schlägt die Anmeldung bei dem Versuch, sich erneut als Benutzer mit dem geänderten Passwort anzumelden, fehlt mit dem Hinweis, dass kein Profil vorhanden ist.

Umgehung: Keine.

Inkompatibilität für die Access Manager-Standardkonfiguration des Statistikdienstes für den Legacy-(kompatiblen)Modus (6286628)

Nach der Installation mit Access Manager im Legacy-Modus hat sich die Standardkonfiguration für den Statistikdienst geändert:

- Der Dienst wird standardmäßig aktiviert (`com.iplanet.services.stats.state=file`). Zuvor war er deaktiviert.
- Das Standardintervall (`com.iplanet.am.stats.interval`) hat sich von 3600 zu 60 geändert.
- Das Standardstatusverzeichnis (`com.iplanet.services.stats.directory`) hat sich von `/var/opt/SUNWam/debug` zu `/var/opt/SUNWam/stats` geändert.

Umgehung: Keine.

Attributeindeutigkeit in der obersten Organisation für Namensattribute nicht eingehalten (6204537)

Melden Sie sich nach der Installation von Access Manager als `amadmin` an und fügen Sie die `o`-, `sunPreferredDomain`-, `associatedDomain`-, `sunOrganizationAlias`-, `uid`- und `mail`-Attribute der Liste eindeutiger Attribute hinzu. Wenn Sie zwei neue Organisationen mit demselben Namen erstellen, schlägt die Operation fehl, Access Manager zeigt jedoch die Meldung "organization already exists" (Organisation bereits vorhanden) statt der erwarteten Meldung "attribute uniqueness violated" (Attributeindeutigkeit verletzt) an.

Umgehung: Keine. Ignorieren Sie die falsche Meldung. Access Manager wird ordnungsgemäß ausgeführt.

Sitzungs- und SSO-Probleme

- "Die Access Manager-Instanzen über verschiedene Zeitzonen hinweg führen zu Zeitüberschreitungen anderer Benutzersitzungen (6323639)" auf Seite 97
- "Das (`amsfoconfig`)-Sitzungsfailoverskript enthält fehlerhafte Berechtigungen auf dem Linux 2.1-System (6298433)" auf Seite 97

Die Access Manager-Instanzen über verschiedene Zeitzonen hinweg führen zu Zeitüberschreitungen anderer Benutzersitzungen (6323639)

Access Manager-Instanzen, die über verschiedene Zeitzonen hinweg und im selben Trustkreis installiert wurden, führen zu einer Zeitüberschreitung anderer Benutzersitzungen.

Das (`amsfoconfig`)-Sitzungsfailoverskript enthält fehlerhafte Berechtigungen auf dem Linux 2.1-System (6298433)

Das Sitzungsfailover-Konfigurationsskript (`/opt/sun/identity/bin/amsfoconfig`) enthält fehlerhafte Berechtigungen und kann auf dem Linux 2.1-System nicht ausgeführt werden.

Umgehung: Ändern Sie die Berechtigungen so, dass das `amsfoconfig`-Skript ausgeführt werden kann (zum Beispiel 755).

Dieses Problem wurde in Patch 1 behoben. Informationen zur Anwendung des Patches für Ihre Plattform finden Sie unter "Access Manager 7 2005Q4-Patch 1" auf Seite 66.

Das Sitzungsfailover-Skript (`amsfoconfig`) schlägt auf dem Linux 2.1-System fehl (6298462)

Das Sitzungsfailover-Konfigurationsskript (`amsfoconfig`) schlägt auf dem Linux 2.1-Server fehl, weil das Tabulatorzeichen (`\t`) nicht ordnungsgemäß interpretiert wird.

Umgehung: Konfigurieren Sie den Sitzungsfailover manuell. Eine Beschreibung der einzelnen Schritte finden Sie unter "Configuring Session Failover Manually" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Dieses Problem wurde in Patch 1 behoben. Informationen zur Anwendung des Patches für Ihre Plattform finden Sie unter "Access Manager 7 2005Q4-Patch 1" auf Seite 66.

System erstellt einen ungültigen Diensthostnamen bei SSL-Anschluss des Load Balancer (6245660)

Wenn Access Manager mit dem Web Server als der Webcontainer verwendet wird, der einen Load Balancer mit SSL-Anschluss verwendet, werden die Clients nicht auf die richtige Web Server-Seite geleitet. Wenn Sie auf die Registerkarte "Sessions" in der Access Manager Console klicken, wird ein Fehler ausgegeben, da der Host ungültig ist.

Umgehung: In folgenden Beispielen hört Web Server Port 3030 ab. Der Load Balancer hört Port 80 ab und leitet alle Anforderungen an Web Server um.

Bearbeiten Sie in der Datei *web-server-instance-name*`/config/server.xml` das Attribut `servername`, um auf den Load Balancer zu verweisen, je nach der verwendeten Version des Web Servers.

Bearbeiten Sie für die Versionen von Web Server 6.1 Service Pack (SP) das Attribut `servername` wie folgt:

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

Web Server 6.1 SP2 (oder höher) kann das Protokoll von `http` zu `https` oder von `https` zu `http` wechseln. Bearbeiten Sie deshalb `servername` wie folgt:

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

Verwenden von `HttpSession` mit Drittanbieter-Containern (keine CR-Nummer)

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 führen 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 dynamischen Attribute (aus Schritt 1) im Antwortanbieter 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 Ergebnisse lauten: "Error Invalid Dynamic property being set" (Fehler: Es wurde eine ungültige dynamische Eigenschaft festgelegt). Es wurden 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.

Umgehung: 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 2005Q4 werden in den Debug-Dateien `amDelegation` und `amProfile` Debug-Fehler ausgegeben:

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

Umgehung: Keine. Sie können diese Meldungen ignorieren.

Verwenden von BEA WebLogic Server als Webcontainer

Wenn Sie Access Manager mit BEA WebLogic Server als Webcontainer bereitstellen, kann Access Manager unter Umständen nicht aufgerufen werden.

Umgehung: Starten Sie WebLogic Server ein zweites Mal, damit Sie Access Manager aufrufen können.

Probleme auf Linux OS

JVM-Probleme treten auf, wenn Access Manager auf Application Server ausgeführt wird (6223676).

Wenn Sie Application Server 8.1 unter Red Hat Linux ausführen, ist die vom Red Hat OS für Application Server festgelegte Stackgröße für Threads 10 MB. Dadurch kann es zu JVM-Ressourcenproblemen kommen, wenn die Anzahl der Access Manager-Benutzersitzungen 200 erreicht.

Umgehung: Legen Sie als anzuwendende Stackgröße unter Red Hat OS einen niedrigeren Wert fest, z. B. 2048 oder 256 KB. Führen Sie hierfür den Befehl `ulimit` aus, bevor Sie Application Server starten. Führen Sie den Befehl `ulimit` auf derselben Konsole aus, auf der Sie auch Application Server starten. Beispiel:

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

Verbund- und SAML-Probleme

Ausführen des Webdienstes gibt Fehler "Ressourcenangebot nicht gefunden" zurück (6359900)

Wenn Access Manager für den Zugriff auf die Beispiele für den Webdienst im Verzeichnis *AccessManager-base*`/SUNWam/samples/phase2/wsc` (Solaris-Systeme) bzw. im Verzeichnis *AccessManager-base* `/identity/samples/phase2/wsc` (Linux-Systeme) konfiguriert wurde, wird beim Abfragen des Erkennungsdienstes und beim Bearbeiten des Ressourcenangebots folgende Fehlermeldung zurückgegeben: "Ressourcenangebot nicht gefunden".

AccessManager-base ist das Basisinstallationsverzeichnis. Das standardmäßige Basisinstallationsverzeichnis lautet `/opt` auf Solaris-Systemen und `/opt/sun` auf Linux-Systemen.

Umgehung:

1. Wechseln Sie in das folgende Beispielverzeichnis: *AccessManager-base* `/SUNWam/samples/phase2/wsc` auf Solaris-Systemen und *AccessManager-base*`/identity/samples/phase2/wsc` auf Linux-Systemen
2. Suchen Sie in der Datei `index.jsp` folgende Zeichenfolge:

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

3. Fügen Sie unmittelbar vor der Zeile mit der im vorherigen Schritt gesuchten Zeichenfolge folgende Zeile ein:

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

4. Führen Sie das Beispiel erneut aus. (Sie müssen Access Manager nicht neu starten.)

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.

Umgehung: Keine.

Die Sonderzeichen (&) in SAML-Anweisungen sollten codiert sein (6321128)

Wenn Access Manager als die Quellsite und die Zielsite und SSO konfiguriert sind, tritt auf der Zielsite ein Fehler auf, weil das Sonderzeichen (&) in den SAML-Anweidungen nicht codiert ist und deshalb die Analyse der Prüfung fehlschlägt.

Umgehung: Keine. Dieses Problem wurde in Patch 1 behoben. Informationen zur Anwendung des Patches für Ihre Plattform finden Sie unter "Access Manager 7 2005Q4-Patch 1" auf Seite 66.

Fehler beim Hinzufügen des Disco Service zu einer Rolle (6313437)

Wenn Sie versuchen, in der Access Manager Console ein Ressourcenangebot zum Disco Service hinzuzufügen, tritt eine unbekannte Ausnahme auf.

Umgehung: Keine.

Die Auth Context-Attribute können nicht konfiguriert werden, solange Sie keine anderen Attribute konfiguriert und gespeichert haben (6301338)

Die Auth Context-Attribute können nicht konfiguriert werden, solange Sie keine anderen Attribute konfiguriert und gespeichert haben

Umgehung: Konfigurieren und speichern Sie ein Anbieterprofil, bevor Sie die Auth Context-Attribute konfigurieren.

EP Sample funktioniert nicht, wenn das Root-Suffix ein " &"-Zeichen enthält (6300163)

Wenn Directory Server einen Root-Suffix mit dem "& "-Zeichen enthält und Sie versuchen, ein Employee Profile Service Resource Offering hinzuzufügen, wird eine Ausnahme ausgelöst.

Umgehung: 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, tritt ein Fehler auf: Fehler: Es wurde keine untergeordnete Organisation gefunden.

Umgehung: Keine.

Globalisierungsprobleme (g11n)

Die Benutzerländereinstellungen werden nicht auf die Administrationskonsole angewandt (6326734)

Teile der Access Manager-Administrationskonsole stimmen nicht mit den Benutzerländereinstellungen überein, sondern verwenden stattdessen die Browserländereinstellungen. Dieses Problem betrifft die Versions-, Abmelde- und Onlinehilfeschaltflächen sowie den Inhalt der Versions- und Onlinehilfe.

Umgehung: Ändern Sie die Browsereinstellungen in dieselbe Ländereinstellung wie die Benutzereinstellungen.

Die Onlinehilfe steht für europäische Sprachen nicht vollständig zur Verfügung, wenn Access Manager auf IBM WebSphere bereitgestellt wird (6325024)

Bei allen europäischen Ländereinstellungen (Spanisch, Deutsch und Französisch) kann auf die Onlinehilfe nicht vollständig zugegriffen werden, wenn Access Manager in einer IBM WebSphere Application Server-Instanz bereitgestellt wird. Die Onlinehilfe zeigt für die folgenden Rahmen einen Anwendungsfehler an:

- Oberer Rahmen, wo sich die Hilfeschaltflächen und die Schaltflächen zum Schließen befinden sollten.
- Linker Rahmen, wo sich die Inhalts-, Index- und Suchschaltflächen befinden sollten.

Umgehung: Legen Sie als Browsersprache Englisch fest und aktualisieren Sie die Seite, um auf den linken Rahmen zugreifen zu können. Im oberen Rahmen wird jedoch weiterhin ein Anwendungsfehler angezeigt.

Die Versionsinformationen sind leer, wenn Access Manager auf IBM WebSphere bereitgestellt wird (6319796)

Bei jeder Ländereinstellung ist die Produktversion bei der Bereitstellung von Access Manager in der IBM WebSphere Application Server-Instanz nicht sichtbar, wenn Sie auf die Versionsschaltfläche klicken. Stattdessen wird eine leere Seite angezeigt.

Umgehung: Keine.

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

Die Client Detection-Funktion funktioniert nicht ordnungsgemäß. Änderungen der Access Manager 7 2005Q4 Console werden nicht automatisch vom Browser übernommen.

Umgehung: Es gibt zwei Lösungen:

- Starten Sie den Access Manager-Webcontainer neu, nachdem Sie im Client Detection-Abschnitt eine Änderung vorgenommen haben.

  oder

- Befolgen Sie die nachfolgenden Schritte in der Access Manager Console:

  1. Klicken Sie auf der Registerkarte `Configuration` auf `Client Detection`.
  2. Klicken Sie auf den Link `Edit` für `genericHTML`.
  3. Klicken Sie auf der Registerkarte ?HTML“ auf den Link `genericHTML`.
  4. Nehmen Sie in der Zeichensatzliste den folgenden Eintrag vor: `UTF-8;q=0.5` (Stellen Sie sicher, dass der UTF-8-Faktor `q` niedriger ist als die anderen Zeichensätze für Ihre Ländereinstellung.)
  5. Speichern Sie, melden Sie sich ab und dann erneut an.

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

Die Mehrfachbyte-Nachrichten in den Protokolldateien im Verzeichnis `/var/opt/SUNWam/logs` werden als Fragezeichen angezeigt (`?`). Protkolldateien befinden sich in der nativen Verschlüsselung und nicht immer im UTF-8-Format. Wenn eine Instanz eines Web-Containers in einem Gebietsschema gestartet wird, werden die Protokolldateien in der nativen Verschlüsselung für dieses Gebietsschema gespeichert. 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.

Umgehung: Stellen Sie sicher, die Webcontainerinstanzen immer mit derselben nativen Codierung zu starten.

Dokumentationsprobleme

Access Manager kann nicht vom Realm-Modus in den Legacy-Modus wechseln (6508473)

Wenn Sie Access Manager 7 2005Q4 im Realm-Modus installieren, können Sie nicht in den Legacy-Modus wechseln.

Wenn Sie Access Manager 7 2005Q4 jedoch im Legacy-Modus installieren, können Sie mit dem Befehl `amadmin` und der Option `-M` in den Realm-Modus wechseln. Beispiel:

```
amadmin -u cn=amAdmin,ou=People,dc=example,dc=com -w amadmin-password
-M dc=example,dc=com
```

Weitere Informationen zum Deaktivieren von persistenten Suchabfragen (6486927)

Access Manager verwendet persistente Suchabfragen, um Informationen zu geänderten Sun Java System Directory Server-Einträgen abzurufen. Access Manager erstellt beim Serverstart standardmäßig die folgenden persistenten Suchverbindungen:

`aci` - Änderungen des Attributs `aci`, wobei bei der Suche der LDAP-Filter (`aci=*`) angewendet wird.

`sm` - Änderungen des Access Manager-Informationsbaums (oder des Dienstverwaltungskontens), der Objekte mit der Markerobjektklasse `sunService` oder `sunServiceComponent` enthält. Sie können beispielsweise eine Richtlinie erstellen, um Zugriffsberechtigungen für eine geschützte Ressource festzulegen, oder die Regeln, Subjekte, Bedingungen oder Antwortanbieter für eine bestehende Richtlinie ändern.

`um` - Änderungen des Benutzerverzeichnisses (oder des Benutzerverwaltungsknotens). Sie können beispielsweise den Namen oder die Adresse eines Benutzers ändern.

Achtung – Das Deaktivieren von persistenten Suchabfragen für eine dieser Komponenten wird nicht empfohlen, da bei deaktivierter persistenter Suche keine Benachrichtigungen vom Directory Server empfangen werden. Folglich würde der Cache der jeweiligen Komponenten nicht über die in Directory Server vorgenommenen Änderungen der Komponente benachrichtigt werden und der Cache würde veralten.

Wenn Sie beispielsweise die persistenten Suchabfragen für Änderungen des Benutzerverzeichnisses (`um`) deaktivieren, erhält der Access Manager-Server keine Benachrichtigungen vom Directory Server. Der Agent erhält folglich keine Benachrichtigungen von Access Manager für die Aktualisierung seines lokalen Benutzer-Caches mit den neuen Werten des Benutzerattributs. Wenn nun eine Anwendung die Benutzerattribute vom Agenten abfragt, erhält die Anwendung unter Umständen den alten Wert für das Attribut.

Verwenden Sie diese Eigenschaft nur in Ausnahmefällen, in denen die Eigenschaft unbedingt erforderlich ist. Wenn beispielsweise keine Dienstkonfigurationsänderungen (keine Änderung von Werten eines Dienstes, z. B. des Sitzungs- oder Authentifizierungsdienstes) in der Produktionsumgebung stattfinden, kann die persistente Suche für die Dienstverwaltungskomponente (`sm`) deaktiviert werden. Wenn jedoch eine Änderung in einem der Dienste auftritt, ist ein Neustart des Servers erforderlich. Dies gilt auch für andere persistente Suchabfragen, die von den Werten `aci` und `um` angegeben werden.

Weitere Informationen finden Sie unter "Neue Eigenschaft zum Deaktivieren persistenter Suchabfragen zur Anwendung in Ausnahmefällen (6363157)" auf Seite 65.

Von Access Manager unterstützte und nicht unterstützte Berechtigungen (2143066)

Mit Berechtigungen werden die Zugriffsrechte für Administratoren festgelegt, die Mitglieder von Rollen oder Gruppen sind, die innerhalb eines Bereichs bestehen. Access Manager ermöglicht die Konfiguration der Berechtigungen für folgende Administratortypen:

- Bereichsadministratoren können alle bereichsspezifischen Aufgaben durchführen, einschließlich der Definition von Identity-Repositories (Datenspeicher), der Konfiguration der Authentifizierung und der Definition von Richtlinien.
- Richtlinienadministratoren können Richtlinien in vorhandenen Bereichen konfigurieren.

Die folgenden Berechtigungen werden unterstützt:

- Lese- und Schreibzugriff auf alle Bereichs- und Richtlinieneigenschaften. Legt Lese- und Schreibzugriffsberechtigungen für alle Bereichsadministratoren fest.
- Lese- und Schreibzugriff nur auf Richtlinieneigenschaften. Legt Lese- und Schreibzugriffsberechtigungen für alle Richtlinienadministratoren fest.

- Unterstützte Kombinationen von Berechtigungen: Lese- und Schreibzugriff nur auf Richtlinieneigenschaften und nur Lesezugriff auf Datenspeicher. Andere Kombinationen von Berechtigungen werden nicht unterstützt.

Cookie-basiertes "Sticky Request Routing" (6476922)

Wenn Access Manager-Server hinter einem Load Balancer bereitgestellt werden, verhindert das Cookie-basierte so genannte "Sticky Request Routing" (zähe Anforderungsweiterleitung), dass Client-Anfragen an einen falschen Access Manager-Server weitergeleitet werden (d. h., auf einen Server, der nicht der Host der Sitzung ist). Diese Funktion wurde in Access Manager 7 2005Q4-Patch 3 implementiert.

Das frühere Verhalten, ohne Cookie-basiertes Sticky Request Routing, führte häufig dazu, dass Anforderungen von nicht browserbasierten Clients (z. B. Richtlinienagenten und Clients, die das Remote-Access Manager Client SDK verwenden) fälschlicherweise an einen Access Manager, der nicht Host der Sitzung ist, weitergeleitet wurden. Um die Anforderung an den richtigen Server zu senden, musste der Access Manager-Server die Sitzung durch Kommunikation über einen Rückkanal überprüfen, was in den meisten Fällen zu Leistungseinbußen führte. Durch den Einsatz von Cookie-basiertem Sticky Request Routing wird diese Rückkanal-Kommunikation nicht benötigt und dadurch die Leistung von Access Manager verbessert.

Um Cookie-basiertes Request Routing zu implementieren, muss die Access Manager-Bereitstellung als Site konfiguriert sein. Weitere Informationen finden Sie unter "Configuring an Access Manager Deployment as a Site" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

So konfigurieren Sie Cookie-basiertes Sticky Request Routing

1. Um einen Cookie-Namen anzugeben, legen Sie die Eigenschaft `com.iplanet.am.lbcookie.name` in der Datei `AMConfig.properties` fest. Access Manager erzeugt anschließend unter Verwendung der 2-Byte-Server-ID (z. B. 01, 02 oder 03) den Cookie-Wert für den Load Balancer. Wenn Sie keinen Cookie-Namen angeben, erzeugt Access Manager das Cookie für den Load Balancer mit dem Standardnamen `amlbcookie` und der 2-Byte-Server-ID.

   Wenn Sie den Cookie-Namen auf dem Access Manager-Server festlegen, müssen Sie denselben Namen in der Datei `AMAgent.properties` für einen Richtlinienagenten verwenden. Ebenso müssen Sie denselben Cookie-Namen wie den vom Access Manager-Server verwendeten Namen verwenden, wenn Sie das Access Manager Client-SDK verwenden.

   Hinweis: Legen Sie nicht die Eigenschaft `com.iplanet.am.lbcookie.value` fest, da Access Manager den Cookie-Wert unter Verwendung der 2-Byte-Server-ID festlegt.

2. Konfigurieren Sie Ihren Load Balancer mit dem Cookie-Namen aus Schritt 1. Mit der Access Manager-Bereitstellung kann ein Hardware- oder Software-Lastenausgleichssystem verwendet werden.

3. Wenn Sitzungs-Failover implementiert ist, aktivieren Sie die Eigenschaft `com.sun.identity.session.resetLBCookie` für beide Richtlinienagenten und für den Access Manager-Server.
   - Fügen Sie für den Richtlinienagenten die Eigenschaft der Datei `AMAgents.properties` hinzu und aktivieren Sie sie.
   - Fügen Sie für Access Manager-Server die Eigenschaft der Datei `AMConfig.properties` hinzu und aktivieren Sie sie.

   Beispiel:

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

   Tritt eine Failover-Situation auf, wird die Sitzung an einen sekundären Access Manager-Server weitergeleitet und der Cookie-Wert des Load Balancer unter Verwendung der Server-ID des sekundären Access Manager-Servers festgelegt. Alle nachfolgenden Anforderungen für die Sitzung werden an den sekundären Access Manager-Server weitergeleitet.

Windows Desktop SSO-Konfiguration für Windows 2003 (6487361)

Um Windows Desktop SSO auf Windows 2003 zu konfigurieren (wie unter "Configuring Windows Desktop SSO" in *Sun Java System Access Manager 7 2005Q4 Administration Guide* beschrieben), verwenden Sie folgenden `ktpass`-Befehl:

```
ktpass /out filename /mapuser username
/princ HTTP/hostname.domainname /crypto encryptiontype /rndpass
/ptype principaltype /target domainname
```

Beispiel:

```
ktpass /out demo.HTTP.keytab
/mapuser http /princ HTTP/demo.identity.sun.com@IDENTITY.SUN.COM
/crypto RC4-HMAC-NT /rndpass /ptype KRB5_NT_PRINCIPAL /target IDENTITY.SUN.COM
```

Syntaxdefinitionen finden Sie auf folgender Website:

`http://technet2.microsoft.com/WindowsServer/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true`

Schrittanleitung für das Einrichten von Passwörtern für einen Server mit Verteilter Authentifizierungsbenutzeroberfläche (6510859)

Das folgende Verfahren beschreibt, wie Sie die verschlüsselten Passwörter für einen Server mit Verteilter Authentifizierungsbenutzeroberfläche einrichten, der mit einem Access Manager-Server kommuniziert.

So richten Sie die Passwörter für einen Server mit Verteilter Authentifizierungsbenutzeroberfläche ein

1. Führen Sie folgende Schritte auf dem Access Manager-Server durch:
   a. Verwenden Sie das Dienstprogramm `ampassword -e`, um das `amadmin`-Passwort zu verschlüsseln. Beispielsweise auf Solaris-Systemen:

      ```
      # cd /opt/SUNWam/bin
      # ./ampassword -e amadmin-password
      AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      ```

      Speichern Sie den verschlüsselten Wert.
   b. Kopieren und speichern Sie die Eigenschaft `am.encryption.pwd` aus der Access Manager-Serverdatei `AMConfig.properties`. Beispiel:

      ```
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```

2. Nehmen Sie auf dem Server mit Verteilter Authentifizierungsbenutzeroberfläche folgende Änderungen der Datei `AMConfig.properties` vor:
   a. Kommentieren Sie die Eigenschaft `com.iplanet.am.service.password` aus.
   b. Legen Sie die Eigenschaft `com.iplanet.am.service.secret` auf das in Schritt 1a verschlüsselte `amadmin`-Passwort fest.
   c. Fügen Sie `am.encryption.pwd` und den in Schritt 1b verschlüsselten Wert hinzu. Beispiel:

      ```
      com.sun.identity.agents.app.username=username
      #com.iplanet.am.service.password=password
      com.iplanet.am.service.secret=AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```

3. Starten Sie den Server mit Verteilter Authentifizierungsbenutzeroberfläche neu.

Fehlender Schritt in Onlinehilfe unter ?So erstellen Sie einen neuen Site-Namen“ (2144543)

In der Onlinehilfe der Access Manager-Konsole fehlt unter ?So erstellen Sie einen neuen Site-Namen“ in ?Konfiguration>Systemeingenschaften>Plattform“ der Schritt mit der Anweisung zum Speichern. Wenn Sie nach dem Hinzufügen einer neuen Site nicht auf ?Speichern“ und anschließend einen Instanznamen hinzufügen möchten, schlägt der Vorgang fehl. Klicken Sie daher nach dem Hinzufügen eines Site-Namens immer auf ?Speichern“ und fügen Sie anschließend den Instanznamen hinzu.

Konfigurationsparameter für Administrator-Passwort lautet auf Windows-Systemen `ADMIN_PASSWD` (6470793)

Auf Solaris- und Linux-Systemen lautet der in der Datei `amsamplesilent` enthaltene Konfigurationsparameter für das Passwort des Access Manager-Administrators (`amadmin`) `ADMINPASSWD`. Auf Windows-Systemen lautet der Parameter in der Datei `AMConfigurator.properties` jedoch `ADMIN_PASSWD`.

Wenn Sie `amconfig.bat` auf einem Windows-System ausführen, legen Sie das `amadmin`-Passwort in der Datei `AMConfigurator.properties` mit dem Parameter `ADMIN_PASSWORD` und nicht mit `ADMINPASSWD` fest.

Versionshinweise enthalten falsche Lösung für ein bekanntes Problem (6422907)

Schritt 3 der Lösung für "Ausführen des Webdienstes gibt Fehler "Ressourcenangebot nicht gefunden" zurück (6359900)" auf Seite 100 wurde korrigiert.

Dokument `com.iplanet.am.session.protectedPropertiesList` in `AMConfig.properties` (6351192)

Der `com.iplanet.am.session.protectedPropertiesList`-Parameter ermöglicht es Ihnen, bestimmte Eigenschaften von Kernsitzungen bzw. internen Sitzungen vor Remote-Aktualisierungen per `SetProperty`-Methode des Sitzungs-Dienstes zu schützen. Durch Festlegen dieses "versteckten" Schlüsselsicherheitsparameters können Sie Sitzungsattribute anpassen, um bei der Autorisierung sowie bei anderen Access Manager-Funktionen teilzunehmen. So verwenden Sie diesen Parameter:

1. Fügen Sie den parameter mit einem Texteditor zur `AMConfig.properties` -Datei hinzu.
2. Stellen Sie den Parameter für die Sitzungseigenschaften ein, die Sie schützen möchten. Beispiel:

   ```
   com.iplanet.am.session.protectedPropertiesList =
   PropertyName1 , PropertyName2 , PropertyName3
   ```

3. Starten Sie den Access Manager-Webcontainer neu, damit die Werte in Kraft treten.

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 (behebt Problem 6349959). Geben Sie auf der Access Manager 7 2005Q4 Administrator Console für die LDAPv3-Konfiguration in das Feld "LDAPc3-Plugin: Unterstützte Typen und Vorgänge" die Werte wie folgt ein:

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

Sie können einen oder beide der oben genannten Einträge eingeben, je nachdem, welche Rollen und gefilterte Rollen Sie in Ihrer LDAPv3-Konfiguration verwenden möchten.

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
```

`com.iplanet.am.session.client.polling.enable` auf Serverseite darf nicht true sein (6320475)

Die `com.iplanet.am.session.client.polling.enable`-Eigenschaft in der `AMConfig.properties`-Datei darf auf Serverseite niemals auf true festgelegt werden.

Umgehung: Diese Eigenschaft wird standardmäßig auf false festgelegt und sollte niemals erneut auf true festgelegt werden.

Der Standarderfolgs-URL ist in der Konsolenonlinehilfe fehlerhaft (6296751)

Der Standarderfolgs-URL ist in der Onlinehilfedatei `service.scserviceprofile.iplanetamauthservice.html` fehlerhaft. Das Feld "Default Success URL" akzeptiert eine Liste mit mehreren Werten, die den URL angeben, an den die Benutzer nach einer erfolgreichen Authentifizierung geleitet werden. Das Format dieses Attributs lautet `clientType|URL`, obwohl Sie nur den Wert des URL angeben können, der einen HTML-Standardtyp annimmt.

Der Standardwert "`/amconsole`" ist fehlerhaft.

Umgehung: Der richtige Standardwert lautet "`/amserver/console`".

Beschreibung der Aktivierung der XML-Verschlüsselung (6275563)

Um die XML-Verschlüsselung für Access Manager oder Federation Manager unter Verwendung der Bouncy Castle-JAR-Datei für das Generieren eines Transportschlüssels zu aktivieren, gehen Sie wie folgt vor:

1. Wenn Sie eine ältere JDK-Version als JDK 1.5 verwenden, laden Sie den Bouncy Castle-JCE-Anbieter von der Bouncy Castle-Website (`http://www.bouncycastle.org/`) herunter. Wenn Sie beispielsweise JDK 1.4 verwenden, laden Sie die Datei `bcprov-jdk14-131.jar` herunter.

2. Wenn Sie im vorherigen Schritt eine JAR-Datei heruntergeladen haben, kopieren Sie die Datei in das Verzeichnis *jdk_root*`/jre/lib/ext`.
3. Laden Sie für die verwendete Version des JDK die JCE Unlimited Strength Jurisdiction Policy Files 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.
4. Kopieren Sie die heruntergeladenen Dateien `US_export_policy.jar` und `local_policy.jar` in das Verzeichnis *jdk_root*`/jre/lib/security` .
5. 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. Beispiel:

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

6. Legen Sie in der Datei `AMConfig.properties` die folgende Eigenschaft als true fest:

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

7. Starten Sie den Access Manager-Webcontainer neu.

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

Dokumentationsaktualisierungen

Sun Java System Access Manager 7 2005Q4-Sammlung

In der folgenden Tabelle werden die neuen und überarbeiteten Access Manager 7 2005Q4-Dokumente aufgelistet, die seit der Erstausgabe veröffentlicht wurden. Sie können auf diese Dokumente in der Access Manager 7 2005Q4-Sammlung unter folgender Adresse zugreifen:

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

TABELLE 7 Aktualisierungsprotokoll der Access Manager 7 2005Q4-Dokumentation

Titel	Veröffentlichungsdatum
Sun Java System Access Manager 7 2005Q4 Versionshinweise	Siehe Tabelle 1.
Sun Java System Access Manager 7 2005Q4 Administration Guide	Februar 2006
Sun Java System Access Manager 7 2005Q4 Developers Guide	Februar 2006
Sun Java System Access Manager Policy Agent 2.2 User's Guide	Februar 2006
Sun Java System Access Manager 7 2005Q4 C API Reference	Februar 2006
Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide	Februar 2006
Technical Note: Using Access Manager Distributed Authentication	Februar 2006
Technical Note: Installing Access Manager to Run as a Non-Root User	Februar 2006
Sun Java System SAML v2 Plug-in for Federation Services User's Guide	Februar 2006
Sun Java System SAML v2 Plug-in for Federation Services Release Notes	Februar 2006
Sun Java System SAMLv2 Plug-in for Federation Services Java API Reference	Februar 2006
Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide	Januar 2006
Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide	Dezember 2005
Sun Java System Access Manager 7 2005Q4 Technical Overview	Dezember 2005

Sun Java System Federation Manager 7.0 2005Q4-Sammlung

Sie können unter folgender Adresse auf die Dokumente in der Federation Manager 7.0 2005Q4-Sammlung zugreifen:

`http://docs.sun.com/coll/1321.1`

Sun Java System Access Manager Policy Agent 2.2-Sammlung

Die Access Manager Policy Agent 2.2-Sammlung wird regelmäßig mit Informationen zu neuen Agenten überarbeitet. Sie können unter folgender Adresse auf die Dokumente in dieser Sammlung zugreifen:

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

Weiter vertreibbare Dateien

Sun Java System Access Manager 7 2005Q4 enthält keine Dateien, die Sie an nicht lizenzierte Benutzer des Produkts weitervertreiben können.

Problemmeldungen und 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)-Dienste unter/.`http://sunsolve.sun.com/`.

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

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 Softwareanwendungen, die das Problem verursacht haben könnten.
- 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. Wechseln Sie zu `http://docs.sun.com/`, und klicken Sie 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 für dieses Dokument mit Access Manager-Versionshinweisen lautet beispielsweise 819-3479.

Weitere Quellen von Sun

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

- Sun Java Enterprise System-Dokumentation: `http://docs.sun.com/prod/entsys.05q4`
- Sun-Dienste: `http://www.sun.com/service/consulting/`
- Software-Produkte und Dienste: `http://wwws.sun.com/software/`
- Support-Ressourcen `http://sunsolve.sun.com/`
- Informationen zu Entwicklern: `http://developers.sun.com/`
- Support-Dienste für Sun-Developer: `http://www.sun.com/developers/support/`

Zugriffsfunktionen für Personen mit Behinderungen

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. Aktualisierte Versionen der Anwendungen finden Sie unter `http://sun.com/software/javaenterprisesystem/get.html`.

Informationen zur Verfügbarkeitsverpflichtung von Sun erhalten Sie unter `http://sun.com/access`.

Verwandte Websites von Drittanbietern

In der vorliegenden Dokumentation wird auf URLs von Drittanbietern verwiesen, über die zusätzliche relevante Informationen zur Verfügung gestellt werden.

Hinweis – Sun ist für die Verfügbarkeit von Drittanbieterwebsites, die in diesem Dokument erwähnt werden, nicht verantwortlich. 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 verwantwortlich 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.
