Sun Java System Access Manager 7.1 - Versionshinweise

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

Teilenr.: 820–0360–10
July 2007

070802@18135

Inhalt

Versionshinweise zu Sun Java System Access Manager 7.1

Juli 2007

Teilenr. 819-4683-13

Die Versionshinweise zu Sun Java™ System Access Manager 7.1 enthalten wichtige Informationen zur Sun Java Enterprise System (Java ES)-Version, einschließlich neuer Access Manager-Funktionen und bekannter Probleme mit Lösungen (falls verfügbar). Lesen Sie dieses Dokument vor der Installation und Verwendung dieser Version.

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

Lesen Sie die Informationen auf dieser Website, bevor Sie die Software installieren und einrichten, und besuchen Sie die Website dann regelmäßig, um die aktuellste Dokumentation einzusehen.

Diese Versionshinweise sind in folgende Abschnitte unterteilt:

Revisionsverlauf

Die folgende Tabelle erhält das Änderungsprotokoll der Versionshinweise zu Access Manager 7.1.

TABELLE 1 Revisionsverlauf

Datum	Beschreibung der Änderungen
Juli 2006	Beta-Release.
März 2007	Java Enterprise System 5-Version
Mai 2007	Aktualisiert mit neuen bekannten Problemen 6555040, 6550261, 6554379, 6554372, 6480354
Juni 2007	Aktualisiert mit neuen bekannten Problemen 6562076, 6490150
Juli 2007	Aktualisiert mit neuem bekanntem Problem 6485695

Info zu Sun Java System Access Manager 7.1

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

Access Manager bietet die folgenden Hauptfunktionen:

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

Neue Funktionen in dieser Version

Diese Version bietet die folgenden neuen Funktionen:

Java ES Monitoring Framework-Integration

Access Manager 7.1 wird über Java Management Extensions (JMX) in das Java Enterprise System Monitoring Framework integriert. Die JMX Technology bietet Werkzeuge zum Erstellen von verteilten, webbasierten, modularen und dynamischen Lösungen für die Verwaltung und Überwachung von Geräten, Anwendungen und dienstgesteuerten Netzwerken. Nachfolgend werden einige typische Einsatzbereiche der JMX Technology aufgelistet: Überprüfen und Ändern der Anwendungskonfiguration, Sammeln statistischer Daten zum Anwendungsverhalten, Benachrichtigen bei Statusänderungen und Auftreten von Fehlern. Die Daten werden an eine zentrale Überwachungskonsole gesendet.

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

- Anzahl an versuchten, erfolgreichen und fehlgeschlagenen Authentifizierungen.
- Statistiken zum Richtlinien-Caching.
- Transaktionszeiten der Richtlinienauswertung.

Webdienstsicherheit

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

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

Single Access Manager WAR-Dateibereitstellung.

Access Manager enthält eine einzelne WAR-Datei, die Sie verwenden können, um Access Manager-Dienste konsistent auf allen unterstützten Containern und Plattformen

bereitzustellen. Die Access Manager WAR-Datei koexistiert neben dem Java Enterprise System-Installer, der viele JAR-, XML-, JSP-, HTML-, GIF- und verschiedene .properties-Dateien bereitstellt.

Verbesserung der Kerndienste

Unterstützte Webcontainer

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

Monitoring Framework-Integration

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

1. Authentifizierung
   - Anzahl an versuchten Authentifizierungen
   - Anzahl an versuchten entfernten Authentifizierungen (optional)
   - Anzahl an erfolgreichen Authentifizierungen
   - Anzahl an fehlgeschlagenen Authentifizierungen
   - Anzahl an erfolgreichen Abmeldevorgängen
   - Anzahl der fehlgeschlagenen Abmeldevorgänge
   - Transaktionszeit für jedes Modul, falls möglich (im Ausführungs- und Wartestatus)
2. Sitzungen
   - Größe der Sitzungstabelle (maximale Anzahl an Sitzungen)
   - Anzahl an aktiven Sitzungen (inkrementeller Zähler)
3. Profildienst
   - Maximale Cachegröße
   - Transaktionszeit für Vorgänge (im Ausführungs- und Wartestatus)
4. Richtlinie
   - Ein- und ausgehende Anforderungen für Richtlinienbewertung
   - Statistiken zum Richtlinienverbindungspool für den LDAP-Server des Objekt-Plugins

Authentifizierungsmodul

- Dienst für verteilte Authentifizierung, der nicht auf einen einzigen Server beschränkt ist, für Bereitstellungen mit Load Balancer

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

Richtlinienmodul

- Die neue Richtlinienbedingung `AuthenticateToServiceCondition` wurde hinzugefügt, um die Authentifizierung des Benutzers bei einer bestimmten Authentifizierungsdienstkette zu erzwingen.
- Die neue Richtlinienbedingung `AuthenticateToRealmCondition` wurde hinzugefügt, um die Authentifzierung des Benutzers bei einem bestimmten Bereich zu erzwingen.
- Die neue Richtlinienbedingung `LDAPFilterCondition` wurde hinzugefügt, um die Übereinstimmung des Benutzers mit dem angegebenen LDAP-Filter zu erzwingen.
- Unterstützung von Ein-Ebenen-Platzhalter-Vergleichen; hierdurch kann der Inhalt des Verzeichnisses geschützt werden, ohne das Unterverzeichnis zu schützen.
- Richtlinien können ohne explizite Bezugsrichtlinien des übergeordneten Bereichs in Unterbereichen erstellt werden, wenn in der globalen Richtlinienkonfiguration Organisations-Aliasbezüge aktiviert wurden.
- `AuthLevelCondition` kann zusätzlich zur Authentifizierungsebene den Bereichsnamen angeben.
- `AuthSchemeCondition` kann zusätzlich zum Namen des Authentifizierungsmoduls den Bereichsnamen angeben.

Dienst-Verwaltungs-Modul

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

Access Manager-SDK

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

Unterstützung von Webdiensten

- Liberty ID-WSF SOAP-Anbieter: Authentifizierungsanbieter, der die Liberty ID-WSF SOAP-Binding als Implementierung von Access Manager enthält. Dies umfasst einen Client und einen Dienstanbieter.
- SSO-Anbieter auf HTTP-Ebene: Authentifizierungsanbieter auf HttpServlet-Ebene, der den Access Manager-basierten SSO auf der Serverseite enthält.

Installationsmodul

- Erneute Bereitstellung von Access Manager als J2EE Application, wobei eine einzelne WAR-Datei erzeugt wird, die im Web bereitgestellt werden kann.
- Unterstützt 64 Bit-SJS Web Server 7.0, um die 64 Bit-JVM zu unterstützen.

Delegationsmodul

- Unterstützt die Gruppierung von Delegationsberechtigungen

Aktualisieren

- Unterstützt die Aktualisierung auf Access Manager 7.1 von den folgenden Versionen: Access Manager 7.0 2005Q4, Access Manager 6.3 2005Q1 und Identity Server 6.2 2004Q2.

Protokollierung

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

Hinweis zu nicht mehr verfügbaren Funktionen und andere Ankündigungen

Mit den Identitätsverwaltung-APIs und XML-Vorlagen in Sun Java(TM) System Access Manager 7.1 können Systemadministratoren Identitätseinträge in Sun Java System Directory Server erstellen, löschen und verwalten. Access Manager stellt außerdem APIs für die Identitätsverwaltung bereit. Entwickler verwenden die im Paket `com.iplanet.am.sdk`

definierten öffentlichen Schnittstellen und Klassen, um Verwaltungsfunktionen in externe Anwendungen oder Dienste zu integrieren, die von Access Manager verwaltet werden sollen. Access Manager-APIs bieten eine Möglichkeit, identitätsbezogene Objekte zu erstellen oder zu löschen sowie die Objektattribute von Directory Server abzurufen, zu ändern, hinzuzufügen oder zu löschen.

Das Access Manager `com.iplanet.am.sdk`-Paket, allgemein als AMSDK bekannt, ist in künftigen Versionen von Access Manager nicht enthalten. Dies umfasst alle verwandten APIs und XML-Vorlagen. Derzeit sind keine Migrationsoptionen verfügbar und auch für künftige Versionen nicht vorgesehen. Die in Sun Java System Identity Manager verfügbaren Benutzerbereitstellungslösungen sind kompatible Ersatzoptionen, die Sie von nun an verwenden können. Weitere Informationen über Sun Java System Identity Manager finden Sie unter `http://www.sun.com/software/products/identity_mgr/index.xml`.

Hardware- und Softwareanforderungen

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

TABELLE 2 Hardware- und Softwareanforderungen

Komponente	Anforderung
Betriebssystem (OS)	■ Solaris™10 auf SPARC-, x86- und x64-basierten Systemen, einschließlich Unterstützung ganzer Root-Local- und Sparse-Root-Zonen. ■ Solaris 9 auf SPARC- und x86-basierten Systemen. ■ Red Hat™ Enterprise Linux 3 und 4, alle Updates. Advanced Server (32- und 64-Bit-Version) und Enterprise Server (32- und 64-Bit-Version) ■ Windows Windows 2000 Advanced Server, Data Center Server-Version SP4 auf x86 Windows 2003 Standard (32- und 64-Bit-Version), Enterprise (32- und 64-Bit-Version), Data Center Server (32-Bit-Version) auf x86- und x64-basierten Systemen Windows XP Professional SP2 auf x86-basierten Systemen HP-UX 11i v1 (11.11 von uname), 64-Bit auf PA-RISC 2.0 Die aktuellste Liste der unterstützten Betriebssysteme finden Sie unter „Platform Requirements and Issues" in *Sun Java Enterprise System 5 Release Notes for UNIX* in den *Sun Java Enterprise System 5 Versionshinweisen für UNIX* bzw. unter „Hardware and Software Platform Information" in *Sun Java Enterprise System 5 Release Notes for Microsoft Windows* in den *Sun Java Enterprise System 5 Versionshinweisen für Windows.*
Java 2 Standard Edition (J2SE)	J2SE Platform 6.0, 5.0 Update 9 (HP-UX: 1.5.0.03) und 1.4.2 Update 11.
Directory-Server	Access Manager-Informationsbaum: Sun Java System Directory Server 6.0 oder Sun Java System Directory Server 5.2 2005Q4 Access Manager-Identitätsrepository: Sun Java System Directory Server 5.2 und 6.0 sowie Microsoft Active Directory

TABELLE 2 Hardware- und Softwareanforderungen *(Fortsetzung)*

Komponente	Anforderung
Webcontainer	Sun Java System Web Server 7.0 auf unterstützten Plattform-/OS-Kombinationen, die Sie zum Ausführen der Web Server-Instanz in einer 64 Bit-JVM verwenden möchten. Unterstützte Plattformen: Solaris 9/SPARC, Solaris 10/SPARC, Solaris 10/AMD64, Red Hat AS oder ES 3.0/AMD64, Red Hat AS oder ES 4.0/AMD64
	Sun Java System Application Server Enterprise Edition 8.2
	BEA WebLogic 8.1 SP4
	IBM WebSphere Application Server 5.1.1.6
RAM	Basistests: 512 MB
	Tatsächliche Bereitstellung: 1 GB für Threads, Access Manager SDK, HTTP-Server sowie andere interne Komponenten
Festplattenspeicherplatz	512 MB für Access Manager und die zugehörigen Anwendungen

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

Unterstützte Browser

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

TABELLE 3 Unterstützte Browser

Browser	Plattform
Firefox 1.0.7	Windows XP
	Windows 2000
	Solaris OS, Versionen 9 und 10
	Red Hat Linux 3 und 4
	Mac OS X
Microsoft Internet Explorer™ 6.0 SP2	Windows XP

TABELLE 3 Unterstützte Browser *(Fortsetzung)*

Browser	Plattform
Microsoft Internet Explorer 6.0 SP1	Windows™ 2000
Mozilla™ 1.7.12	Solaris OS, Versionen 9 und 10
	Windows XP
	Windows 2000
	Red Hat Linux 3 und 4
	Mac OS X
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000
Netscape Communicator 7.1	Solaris OS, Versionen 9 und 10

Allgemeine Kompatibilitätsoptionen

Inkompatibilität von AMSDK-Systemen und Access Manager-Server

Bei folgenden Kombinationen und in folgenden Java Enterprise System-Versionen bestehen Inkompatibilitäten von AMSDK und dem Access Manager-Server:

- Java Enterprise System 2004Q2 AMSDK ist mit dem Java Enterprise System 5 Access Manager-Server (vorliegende Version) nicht kompatibel.
- Java Enterprise System 5 AMSDK (vorliegende Version) ist nicht mit dem Java Enterprise System Access Manger 2004Q2-Server (ehemals: Identity Server) kompatibel.

Aufrüstung der Access Manager-HPUX-Version nicht unterstützt

Die Aufrüstung von Access Manager 7 2005Q4 auf Access Manger 7.1 (vorliegende Version) wird bei der HPUX-Version nicht unterstützt.

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:

- „Automatische Java ES-Installation mit einer Statusdatei" auf Seite 15
- „Installationsoption "Jetzt konfigurieren" im grafischen Modus" auf Seite 15
- „Installationsoption "Jetzt konfigurieren" im textbasierten Modus" auf Seite 16
- „Installationsoption "Später konfigurieren"" auf Seite 16

Weitere Informationen zum Modus einer Access Manager 7.1-Installation finden Sie unter „Ermitteln des Access Manager-Modus" auf Seite 16.

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, „Installing in Silent Mode" in *Sun Java Enterprise System 5 Installation Guide for UNIX*.

Installationsoption "Jetzt konfigurieren" im grafischen Modus

Wenn Sie das Java ES-Installationsprogramm mit der Option "Jetzt konfigurieren" 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 "Jetzt konfigurieren" im textbasierten Modus

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

Installationsoption "Später konfigurieren"

Wenn Sie das Java ES-Installationsprogramm mit der Option "Später konfigurieren" 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
...
```

Weitere Informationen zur Konfiguration von Access Manager durch Ausführen des `amconfig`-Skripts finden Sie hier: *Sun Java System Access Manager 7.1 Administration Guide* .

Ermitteln des Access Manager-Modus

Um zu ermitteln, ob eine ausgeführte Access Manager 7.1-Installation im Realm- oder Legacy-Modus konfiguriert wurde, führen Sie folgenden Aufruf durch:

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

Die Ergebnisse lauten:

- true: Realm-Modus
- false: Legacy-Modus

Access Manager-Richtlinienagenten

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

TABELLE 4 Kompatibilität von Richtlinienagenten mit den Access Manager 7.1-Modi

Agent und Version	Kompatibler Modus
Web- und J2EE-Agenten, Version 2.2	Legacy- und Realm-Modus
Web- und J2EE-Agenten (Version 2.1) werden in Access Manager 7.1 nicht unterstützt	

Bekannte Probleme und Einschränkungen

In diesem Abschnitt werden die folgenden bekannten Probleme und ggf. Lösungen beschrieben, die zum Zeitpunkt der Veröffentlichung von Access Manager 7.1 verfügbar waren.

Installationsprobleme

Informationen zu Installationsproblemen bei Java Enterprise System finden Sie in den Versionshinweisen zu JES5. Lesen Sie den Abschnitt „Access Manager Installation Issues” in *Sun Java Enterprise System 5 Release Notes for UNIX* .

Dieser Abschnitt enthält folgende bekannte Probleme:

Bereitstellung von einzelner WAR-Datei durch Access Manager auf WebLogic erfordert die Kommunikation der JAR-Dateien von JAX-RPC 1.0 mit Client-SDK (6555040)

Es besteht ein bekanntes Problem für die auf Weblogic 8.1 bereitgestellte einzelne WAR-Datei bei der JAX-RPC-Initialisierung. Damit Access Manager mit dem Client-SDK kommunizieren kann, müssen Sie die JAX-RCP 1.1-JAR-Dateien durch JAX-RPC 1.0-JAR-Dateien ersetzen.

Problemumgehung:

Es gibt zwei Möglichkeiten, um an die WAR-Datei zu gelangen. Sie erhalten sie entweder über das Installationsprogramm für Java Enterprise System 5, indem Sie für Access Manager die Option "Später konfigurieren" einstellen, oder über die Download-Site von Sun.

Wenn Sie die WAR-Datei mit dem JES 5-Installationsprogramm über die Option "Später konfigurieren" generiert haben:

1. Entfernen Sie folgende `.jar`-Dateien von JAXRPC 1.1 aus *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib` :
   - `jaxrpc-api.jar`
   - `jaxrpc-spi.jar`
   - `jaxrpc-impl.jar`
2. Kopieren Sie folgende `.jar`-Dateien von ihrem jeweiligen Speicherort nach *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib` :
   - `jaxrpc-api.jar` aus `/opt/SUNWam/lib/jaxrpc 1.0`
   - `jaxrpc_ri.jar` aus `/opt/SUNWam/lib/jaxrpc 1.0`
   - `commons-logging.jar` aus `/opt/SUNWmfwk/lib`
3. Wechseln Sie zu *AccessManager-base*`/SUNWam/bin/` , und führen Sie nachfolgenden Befehl aus:

   `amconfig –s` *samplesilent*

   Weitere Informationen zur Konfiguration von Access Manager mithilfe des amconfig-Skripts finden Sie unter Running the Access Manager amconfig Script im *Access Manager Post Installation Guide*.

Wenn Sie die WAR-Datei von der Download-Site von Sun (`http://www.sun.com/download/index.jsp`) heruntergeladen haben:

1. Sobald Sie über die Datei *ZIP_ROOT*`/applications/jdk14/amserver.war` verfügen, entpacken Sie sie in einen Staging-Bereich, z. B. `/tmp/am-staging` .
2. Entfernen Sie folgende `.jar`-Dateien von JAXRPC 1.1 aus `/tmp/am-staging/WEB-INF/lib`:
   - `jaxrpc-api.jar`
   - `jaxrpc-spi.jar`
   - `jaxrpc-impl.jar`

3. Kopieren Sie nachfolgende `.jar`-Dateien von JAXRPC 1.0 und die `.jar`-Datei für Commons-Logging aus dem Verzeichnis *ZIP_ROOT*`/applications/jdk14/jarFix` nach `/tmp/am-staging/WEB-INF/lib`:
   - `jaxrpc-api.jar`
   - `jaxrpc-ri.jar`
   - `commons-logging.jar`
4. Erstellen Sie die WAR-Datei von Access Manager neu, und stellen Sie sie bereit. Weitere Informationen finden Sie unter Deploying Access Manager as a Single WAR File im *Access Manager Post Installation Guide*.

Für die vom JES5-Installationsprogramm für Websphere 5.1 generierte WAR-Datei wird eine zusätzliche .jar-Datei benötigt. (6550261)

Wenn die einzelne WAR-Datei von Access Manager mithilfe des JES 5-Installationsprogramms über die Option "Später konfigurieren" generiert wird, sind zusätzliche `.jar`-Dateien erforderlich, damit Sie Websphere 5.1 bereitstellen können.

Problemumgehung:

1. Kopieren Sie `jsr173_api.jar` aus dem Verzeichnis `/usr/share/lib` nach *AcessManager-base*`/opt/SUNWam/web-src/WEB-INF/lib .`
2. Wechseln Sie zu *AccessManager-base*`/SUNWam/bin/` , und führen Sie nachfolgenden Befehl aus:

   `amconfig –s` *samplesilent*

   Weitere Informationen zur Konfiguration von Access Manager mithilfe des amconfig-Skripts finden Sie unter Running the Access Manager amconfig Script im *Access Manager Post Installation Guide*.

Bereitstellung von einzelner WAR-Datei für Websphere erfordert Änderungen an server.xml, um Kommunikation mit Client-SDK zu ermöglichen (6554379)

Damit die Bereitstellung der einzelnen WAR-Datei von Access Manager mit Websphere 5.1 mit der Client-SDK kommunizieren kann, müssen Sie Änderungen an der Datei `server.xml` vornehmen.

Problemumgehung:

Gehen Sie folgendermaßen vor, um die Datei `server.xml` ordnungsgemäß zu ändern:

1. Beschaffen Sie die Datei `amserver.war`. Es gibt zwei Möglichkeiten, die einzelne WAR-Datei zu erhalten: über das JES 5-Installationsprogramm mithilfe der Option "Später konfigurieren" oder über die Download-Site von Sun.

Hinweis – Wenn Sie die WAR-Datei über das JES 5-Installationsprogramm generiert haben, gehen Sie gemäß den im bekannten Problem Nr. 6550261 angegebenen Schritten vor.

2. Entpacken Sie die Access Manager-WAR in einen Staging-Bereich, z. B. `/tmp/am-staging`.
3. Kopieren Sie folgende gemeinsam genutzte `.jar`-Dateien von `/tmp/am-staging/WEB-INF/lib` an einen Speicherort mit gemeinsamem Zugriff, beispielsweise `/export/jars`:

jaxrpc-api.jar	jaxrpc-spi.jar	jaxrpc-impl.jar	saaj-api.jar
saaj-impl.jar	xercesImpl.jar	namespace.jar	xalan.jar
dom.jar	jax-qname.jar	jaxb-api.jar	jaxb-impl.jar
jaxb-libs.jar	jaxb-xjc.jar	jaxr-api.jar	jaxr-impl.jar
xmlsec.jar	swec.jar	acmecrypt.jar	iaik_ssl.jar
iaik_jce_full.jar	mail.jar	activation.jar	relaxngDatatype.jar
xsdlib.jar	mfwk_instrum_tk.jar	FastInfoset.jar	jsr173_api.jar

4. Entfernen Sie dieselben `.jar`-Dateien aus dem Verzeichnis `/tmp/am-staging/WEB-INF/lib` im Staging-Bereich.
5. Aktualisieren Sie die Datei `server.xml` der Websphere-Instanz. Nehmen Sie nachfolgend beschriebene Änderungen an *jvmEntries* in der Datei `server.xml` vor, wenn der Standardspeicherort der Instanz `/opt/WebSphere/AppServer/config/cells/`*node-name*`/nodes/`*node-name*`/servers/server1` lautet:

   ```
   <classpath>/export/jars/jaxrpc-api.jar:/export/jars/jaxrpc-spi.jar:
       /export/jars/jaxrpc-impl.jar:/export/jars/saaj-api.jar:
       /export/jars/saaj-impl.jar:/export/jars/xercesImpl.jar:
       /export/jars/namespace.jar:/export/jars/xalan.jar:/export/jars/dom.jar:
       /export/jars/jax-qname.jar:/export/jars/jaxb-api.jar:/export/jars/jaxb-impl.jar:
       /export/jars/jaxb-libs.jar:/export/jars/jaxb-xjc.jar:/export/jars/jaxr-api.jar:
       /export/jars/jaxr-impl.jar:/export/jars/xmlsec.jar:/export/jars/swec.jar:
       /export/jars/acmecrypt.jar:/export/jars/iaik_ssl.jar:
       /export/jars/iaik_jce_full.jar:/export/jars/mail.jar:
       /export/jars/activation.jar::/export/jars/relaxngDatatype.jar:
       /export/jars/xsdlib.jar:/export/jars/mfwk_instrum_tk.jar:
       /export/jars/FastInfoset.jar:/export/jars/jsr173_api.jar</classpath>
   ```

6. Starten Sie den Container neu.
7. Erstellen Sie die WAR-Datei von Access Manager neu, und stellen Sie sie über /tmp/am-staging bereit. Weitere Informationen finden Sie unter Deploying Access Manager as a Single WAR File im *Access Manager Deployment Planning Guide*.

Änderungen erforderlich, damit verteilte Authentifizierung bei einzelner WAR-Datei von Access Manager für Weblogic und Websphere funktioniert (6554372)

Für die WAR-Datei zur verteilten Authentifizierung werden zusätzliche .jar-Dateien für das Parsing sowohl für Weblogic 8.1 und Websphere 5.1 benötigt, da die Containerversion JDK14 ist. Die `.jar` -Dateien von JDK14 befinden sich in der `.zip`-Datei in folgendem Verzeichnis:

ZIP-ROOT`/applications/jdk14/jarFix`

Problemumgehung:

Für Weblogic 8.1:

1. Konfigurieren Sie die verteilte Authentifizierung mithilfe der Setup-Skripts. Informationen hierzu finden Sie unter Deploying a Distributed Authentication UI Server im *Access Manager Post Installation Guide*.
2. Entpacken Sie die aktualisierte WAR-Datei für die verteilte Authentifizierung in ein temporäres Verzeichnis, beispielsweise `/tmp/dist-auth`.
3. Kopieren Sie `xercesImpl.jar, dom.jar` und `xalan.jar` von *ZIP-ROOT*`/applications/jdk14/jarFix` in das Verzeichnis `/tmp/dist_auth/WEB-INF/lib`.
4. Erzeugen Sie die WAR-Datei für die verteilte Authentifizierung über das temporäre Verzeichnis erneut, und stellen Sie sie bereit. Weitere Informationen finden Sie unter Deploying a Distributed Authentication UI Server WAR File im *Access Manager Post Installation Guide*.

Für Websphere 5.1:

1. Konfigurieren Sie die verteilte Authentifizierung mithilfe der Setup-Skripts. Informationen hierzu finden Sie unter Deploying a Distributed Authentication UI Server im *Access Manager Post Installation Guide*.
2. Entpacken Sie die aktualisierte WAR-Datei für die verteilte Authentifizierung in ein temporäres Verzeichnis, beispielsweise `/tmp/dist_auth`.
3. Kopieren Sie `xercesImpl.jar, dom.jar` und `xalan.jar` von *ZIP-ROOT*`/applications/jdk14/jarFix` in das Verzeichnis `/tmp/dist_auth/WEB-INF/lib`.
4. Bearbeiten Sie die Datei `WEB-INF/web.xml` und ersetzen Sie `jar://web-app_2_3.dtd` durch `http://java.sun.com/dtd/web-app_2_3.dtd` .
5. Erzeugen Sie die WAR-Datei für die verteilte Authentifizierung über das temporäre Verzeichnis erneut, und stellen Sie sie bereit. Weitere Informationen finden Sie unter Deploying a Distributed Authentication UI Server WAR File im *Access Manager Post Installation Guide*.

Konfigurator für einzelne WAR-Datei schlägt bei DS fehl (6562076)

Wenn Access Manager als einzelne WAR-Datei bereitgestellt wird, schlägt die Konfiguration auf Directory Server 6 mit einem Einzelkomponenten-Root-Suffix fehl. Beispiel: `dc=example`. Mit einem Mehrfachkomponenten-Root-Suffix wie beispielsweise `dc=example,dc=com` ist der Vorgang jedoch erfolgreich.

Problemumgehung: Verwenden Sie das Mehrfachkomponenten-Root-Suffix, z. B. `dc=example,dc=com`.

Konfiguration für mehrere Server der einzelnen WAR-Datei für Access Manager auf demselben Host gibt einen Ausnahmefehler zurück (6490150)

Bei der Konfiguration der zweiten Instanz der einzelnen WAR-Datei von Access Manager auf demselben Host gegen Directory Server wird beim Aktualisieren des Organisations-Alias ein Ausnahmefehler zurückgegeben. Dieses Problem tritt nicht auf, wenn die zweite Instanz auf einem anderen Host konfiguriert wird.

Upgrade-Probleme

Informationen zu Upgrade-Problemen finden Sie im Abschnitt „Upgrade Issues" in *Sun Java Enterprise System 5 Release Notes for UNIX* in den *Sun Java Enterprise System 5 Release Notes for UNIX*.

Kompatibilitätsprobleme

Access Manager Single Sign-On schlägt unter Universal Web Client (6367058, 6429573) fehl

Dieses Problem tritt auf, nachdem Sie Access Manager, Messaging Server und Calendar Server installiert, für den gemeinsamen Betrieb konfiguriert und anschließend den JES5 120955-01

Patch installiert haben. Der Benutzer erhält einen Anmeldefehler. Dieser Fehler tritt aufgrund einer Inkompatibilität zwischen den Eigenschaften von Policy Agent 2.1 und AMSDK auf. Derzeit ist keine Abhilfemöglichkeit bekannt.

StackOverflowError tritt unter Web Server 7.0 im 64–Bit-Modus auf (6449977)

Wird Access Manager auf einer Web Server 7.0-Instanz unter Verwendung einer 64-Bit-JVM konfiguriert, wird beim Zugriff auf die Anmeldeseite der Konsole ein Serverfehler ausgegeben. Im Web Server-Fehlerprotokoll ist die Ausnahme `StackOverflowError` enthalten.

Problemumgehung: Ändern Sie die Web Server-Konfiguration, indem Sie die folgenden Schritte durchführen:

1. Melden Sie sich bei der Web Server-Administration Console als Web Server-Administrator an.
2. Klicken Sie auf "Edit Configuration„.

   Wählen Sie im Feld "Edit Configuration„ die Option "64„ und klicken Sie auf "Speichern„.
3. Klicken Sie auf die Registerkarte "Java„ und anschließend auf "JVM Settings„.
   - Suchen Sie unter "Optionen„ nach dem Mindestwert für die Heap-Größe (z. B.: -Xms). Der Mindestwert für die Heap-Größe sollte mindestens 512m betragen. Wenn der Wert für die Heap-Größe nicht -Xms512m oder höher beträgt, ändern Sie diesen Wert in mindestens -Xms512m.
   - Der Höchstwert für die Heap-Größe sollte mindestens 768m betragen. Wenn der Höchstwert für die Heap-Größe nicht -Xmx768m oder höher ist, ändern Sie diesen Wert in mindestens -Xmx768m.
   - Legen Sie die Java Stack-Größe auf 512k oder 768k fest, indem Sie `-Xss512k` oder `-Xss768k` verwenden. Sie können den Standardwert für 64 Bit-JVM unter Solaris Sparc (1024k) verwenden, indem Sie den Wert leer lassen.
4. Klicken Sie auf die Registerkarte "Performance„ und klicken Sie auf den Link "Thread Pool Settings—

   Ändern Sie den Wert der Stack-Größe in mindestens 261144 und klicken Sie auf "Speichern„.
5. Klicken Sie oben rechts im Bildschirm auf "Deployment Pending„.

   Klicken Sie auf der Seite "Configuration Deployment„ auf "Deploy„.
6. Klicken Sie im Fenster "Ergebnisse„ auf "OK„, um die Web Server-Instanz neu zu starten.

   Klicken Sie im Fenster "Ergebnisse„ auf "Schließen„, nachdem Web Server neu gestartet wurde.

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

Der Access Manager 7.1-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 7.1 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.

Problemumgehung: Keine.

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.

Problemumgehung: Dieses Problem tritt auf, wenn Sie Access Manager auf Version 7.1 aufrüsten, Delegated Administrator jedoch nicht aufrüsten.

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.

Problemumgehung: Die Lösung entspricht der des oben beschriebenen Problems.

Konfigurationsprobleme

Falsche Konsolenumleitung hinter Load Balancer (6480354)

Wenn Sie Instanzen von Access Manager hinter einem Load Balancer bereitgestellt haben, wird die Anmeldung bei der Access Manager Console möglicherweise an eine der Access Manager-Instanzen umgeleitet anstatt an den Load Balancer. Die URL im Browser ändert sich ebenfalls in die der Access Manager-Instanz. Dieses Problem kann beispielsweise auftreten, wenn Sie sich über folgende URL bei der Konsole anmelden:

```
http://loadbalancer.example.com/amserver/realm
```

Diese Umleitung kann sowohl bei der Bereitstellung für den Bereichsmodus als auch für den Legacy-Modus auftreten.

Das Problem kann auf zwei verschiedene Arten umgangen werden. Sie können eine der folgenden Möglichkeiten nutzen:

1. Melden Sie sich über eine der folgenden URLs an:

   `http://` *loadbalancer*`/amserver/UI/Login`

   `http://` *loadbalancer*`/amserver`

2. Stellen Sie in `AMConfig.properties` für die Eigenschaft `com.sun.identity.loginurl` den Namen des Load Balancers ein. Dieser Vorgang muss für jede Access Manager-Instanz wiederholt werden, die sich hinter dem Load Balancer befindet.

Benachrichtigungs-URL muss für Access Manager-SDK-Installation ohne Webcontainer aktualisiert werden (6491977)

Wenn Sie das Access Manager-SDK ohne Webcontainer installieren, indem Sie das Java ES 5-Installationsprogramm mit der Option "Jetzt konfigurieren" ausführen, ist die Eigenschaft `com.iplanet.am.notification.url` in der Datei AMConfig.properties auf

NOTIFICATION_URL eingestellt. Wenn Sie keine zusätzliche Webcontainerkonfiguration vornehmen, erhalten die Benutzer vom Access Manager-Remote-Server keine Benachrichtigungen.

Problemumgehung: Ändern Sie diese Eigenschaft wie folgt:
com.iplanet.am.notification.url=""

Der Dienst für die Passwortzurücksetzung gibt Benachrichtigungsfehler an, wenn ein Passwort geändert wird (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
```

Problemumgehung: Ändern Sie die Konfiguration in
/opt/SUNWam/locale/amPasswordResetModuleMsgs.properties.

- Ändern Sie die from-Adresse. Ändern Sie fromAddress.label=<Identity-Server> in fromAddress.label=<IdentityServer@myhost.company.com>.
- Ändern Sie die Eigenschaft lockOutEmailFrom, um sicherzustellen, dass Sperrbenachrichtigungen die richtige from-Adresse verwenden.

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.

Problemumgehung: Fügen Sie die Realm/DNS-Aliasnamen und Plattform-Serverlisteneinträge manuell hinzu. Schrittweise Anleitungen finden Sie im Abschnitt „Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" in *Sun Java System Access Manager 7.1 Postinstallation Guide*.

Datenvalidierung für erforderliche Attribute in Diensten (6308653)

Access Manager 7.1 erzwingt für die erforderlichen Attribute in XML-Dateien von Diensten Standardwerte.

Problemumgehung: 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 7.1 in einer sicheren (SSL-fähigen) BEA WebLogic 8.1 SP4-Instanz bereitstellen, tritt während der Bereitstellung der einzelnen Access Manager-Webanwendungen eine Ausnahme auf.

Problemumgehung: Gehen Sie wie folgt vor:

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.

Problemumgehung: Fügen Sie die Realm/DNS-Aliasnamen und Plattform-Serverlisteneinträge manuell hinzu. Schrittweise Anleitungen finden Sie im Abschnitt „Adding Additional Instances to the Platform Server List and Realm/DNS Aliases” in *Sun Java System Access Manager 7.1 Postinstallation 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.

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

```
AM_REALM = disabled
```

Probleme mit der Systemleistung

Im Bereichsmodus wird bei der Erstellung neuer Gruppen ein Gruppenadministrator mit ACIs erstellt, die nie verwendet werden (6485695)

Wenn Access Manager im Bereichsmodus installiert ist, erstellt Access Manager, immer wenn eine neue Gruppe erstellt wird, dynamisch einen neuen Gruppenadministrator mit den ACIs, die zur Verwaltung der Gruppe erforderlich sind. Im Bereichsmodus werden diese Gruppenadministrator-ACIs nicht verwendet. Directory Server wertet diese jedoch beim Verarbeiten von Einträgen unter dem Suffix trotzdem aus, wodurch die Leistung von Access Manager beeinträchtigt werden kann, insbesondere wenn bei der Bereitstellung eine große Anzahl von Gruppen erstellt wird.

Problemumgehung: Um das Problem zu umgehen, sind zwei Maßnahmen erforderlich:

- Verhindern, dass Access Manager einen Gruppenadministrator und entsprechende ACIs erstellt, wenn eine neue Gruppe erstellt wird
- Entfernen vorhandener Gruppenadministrator-ACIs von Directory Server

Verhindern, dass Gruppenadministrator-ACIs erstellt werden

Mit dem folgenden Verfahren wird verhindert, dass Acccess Manager einen Gruppenadministrator und entsprechende ACIs erstellt, wenn ein neue Gruppe erstellt wird.

Hinweis – Durch dieses Verfahren wird dauerhaft verhindert, dass beim Erstellen neuer Gruppen Gruppenadministratoren und entsprechende ACIs erstellt werden. Wenden Sie dieses Verfahren nur an, wenn dieses Verhalten für Ihre Bereitstellung geeignet ist.

---

1. Sichern Sie die Datei `amAdminConsole.xml`. Diese Datei befindet sich je nach Plattform im folgenden Verzeichnis:
   - Solaris: `/etc/opt/SUNWam/config/xml`
   - Linux- und HP-UX-Systeme: `/etc/opt/sun/identity/config/xml`
   - Windows-Systeme: *javaes-install-dir*`\identity\config\xml`

     javaes-install-dir steht für das Java ES 5-Installationsverzeichnis. Der Standardwert ist `C:\Program Files\Sun\JavaES5`.
2. Entfernen Sie in der Datei `amAdminConsole.xml` den folgenden Gruppenadministrator-Eintrag, der zwischen den Kommentarzeilen angezeigt wird:

```
<AttributeSchema name="iplanet-am-admin-console-dynamic-aci-list"
    type="list"
    syntax="string"
    i18nKey="g111">
    <DefaultValues>
...
# Beginning of entry to delete
                <Value>Group Admin|Group Admin Description|ORGANIZATION:aci:
(target="ldap:///GROUPNAME")(targetattr = "*")
(version 3.0; acl "Group and people container admin role";
allow (all) roledn = "ldap:///ROLENAME";)##ORGANIZATION:aci:
(target="ldap:///ORGANIZATION")
(targetfilter=(&amp;FILTER(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Policy Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Organization Admin Role,ORGANIZATION)
(nsroledn=cn=Container Admin Role,ORGANIZATION)
(nsroledn=cn=Organization Policy Admin Role,ORGANIZATION)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members"; allow (read,write,search)
roledn = "ldap:///ROLENAME";)</Value>
# End of entry to delete
...
    </DefaultValues>
</AttributeSchema>
```

3. Verwenden Sie `amadmin`, um den Admin- Konsolen-Dienst von Access Manager zu löschen. Beispielsweise auf Solaris-Systemen:

   ```
   # cd /opt/SUNWam/bin
   # ./amadmin -u amadmin -w amadmin_password
   --deleteService iPlanetAMAdminConsoleService
   ```

4. Laden Sie den Admin-Konsolen-Dienst mit `amadmin` in Access Manager aus der in Schritt 2 bearbeiteten Datei `amAdminConsole.xml`. Beispiel:

   ```
   # ./amadmin -u amadmin -w amadmin_password
   -t /etc/opt/SUNWam/config/xml/amAdminConsole.xml
   ```

5. Starten Sie den Access Manager-Webcontainer neu. (Wenn Sie ACIs von Directory Server wie im nächsten Verfahren beschrieben entfernen möchten, warten Sie, und starten Sie den Webcontainer neu, nachdem Sie dieses Verfahren abgeschlossen haben.)

Entfernen vorhandener Gruppenadministrator-ACIs

Hinweis – Im folgenden Verfahren werden die Dienstprogramme `ldapsearch` und `ldapmodify` verwendet, um die Gruppenadministrator-ACIs zu suchen und zu entfernen. Wenn in Ihrer Bereitstellung Directory Server 6.0 verwendet wird, können Sie auch Directory Server Control Center (DSCC) oder den Befehl `dsconf` für diese Funktionen verwenden. Weitere Informationen finden Sie in der Dokumentation zu Directory Server 6.0:

`http://docs.sun.com/app/docs/coll/1224.1`

Durch das folgende Verfahren werden Gruppenadministrator-ACIs entfernt, die bereits in Directory Server vorhanden sind.

1. Erstellen Sie eine LDIF-Datei für die Verwendung mit `ldapmodify`, um die Gruppenadministrator-ACIs zu entfernen. Suchen Sie nach diesen ACIs mit `ldapsearch` (oder einem anderen Tool zur Verzeichnissuche, das Sie bevorzugen).

   Beispielsweise entfernen die folgenden Einträge in der LDIF-Beispieldatei `Remove_Group_ACIs.ldif` ACIs für eine Gruppe namens New Group:

```
dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///cn=New Group,ou=Groups,o=isp")(targetattr = "*")
(version 3.0; acl "Group and people container admin role"; allow (all)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///ou=People,o=isp")(targetattr="nsroledn")
(targattrfilters="add=nsroledn:(!(nsroledn=*)),
del=nsroledn:(!(nsroledn=*))") (version 3.0;
acl "Group admin's right to add user to people container"; allow (add)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///o=isp")
(targetfilter=(&(|(memberof=*cn=New Group,ou=Groups,o=isp)
(iplanet-am-static-group-dn=*cn=New Group,ou=Groups,o=isp))
(!(|(nsroledn=cn=Top-level Admin Role,o=isp)
(nsroledn=cn=Top-level Help Desk Admin Role,o=isp)
(nsroledn=cn=Top-level Policy Admin Role,o=isp)
(nsroledn=cn=Organization Admin Role,o=isp)(
nsroledn=cn=Container Admin Role,o=isp)
(nsroledn=cn=Organization Policy Admin Role,o=isp)))))
```

```
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list ||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members";
allow (read,write,search)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)
aci: (target="ldap:///o=isp")(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the root suffix";
allow (all) userdn = "ldap: ///cn=dsameuser,ou=DSAME Users,o=isp"; )
```

2. Verwenden Sie `ldapmodify` mit der LDIF-Datei aus dem vorherigen Schritt, um die Gruppen-ACIs von Directory Server zu entfernen. Beispiel:

   ```
   # ldapmodify -h ds-host -p 389 -D "cn=Directory Manager"
   -w ds-bind-password -f Remove_Group_ACIs.ldif
   ```

3. Starten Sie den Access Manager-Webcontainer neu.

Probleme mit Access Manager Console

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

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

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

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

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

Problemumgehung: 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.

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

Attribut `ContainerDefaultTemplateRole` nach Datenmigration hinzufügen (4677779)

Im Legacy-Modus wird die Rolle des Benutzers nicht unterhalb 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.

Problemumgehung: 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.

Problem mit der Befehlszeile

Organisations-Admin-Rolle kann mit dem amadmin-Befehlszeilendienstprogramm keinen neuen Benutzer erstellen (6480776)

Ein Administrator, dem die Organisations-Admin-Rolle zugewiesen wurde, kann aufgrund falscher Protokollierberechtigungen mit dem amadmin-Befehlszeilendienstprogramm keinen neuen Benutzer erstellen.

Umgehung: Sowohl der Organisations-Admin als auch der Top-Level-Admin dürfen die Berechtigungen festlegen. Zur Durchführung dieses Schritts über Administration Console:

1. Begeben Sie sich zu der Organisation, der der Organisations-Admin zugehörig ist.
2. Klicken Sie auf die Registerkarte “Berechtigungen„.
3. Klicken Sie auf den Link der Organisations-Admin-Rolle.
4. Wählen Sie `Read and write access to all log files` oder `Write access to all log files`.
5. Klicken Sie auf “Speichern„.

SDK- und Client-Probleme

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.

Problemumgehung: 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.

Problemumgehung: Starten Sie den Client nach einer Dienstschemaänderung neu.

Dieses Problem wird mit Patch 1 behoben.

Authentifizierungsprobleme

Die Distributed Authentication UI-Serverleistung verringert sich, wenn der Anwendungsbenutzer unzureichende Berechtigungen hat (6470055)

Wenn Sie den Distributed Authentication UI-Server mit dem standardmäßigen Anwendungsbenutzer bereitstellen, kommt es aufgrund der eingeschränkten Berechtigungen dieses Benutzers zu einem beträchtlichen Leistungsabfall.

Problemumgehung: Erstellen Sie einen neuen Benutzer mit den erforderlichen Berechtigungen.

So erstellen Sie einen Benutzer mit den erforderlichen ACIs:

1. Erstellen Sie in der Access Manager-Konsole einen neuen Benutzer. Erstellen Sie beispielsweise einen Benutzer mit dem Namen `AuthUIuser`.
2. Fügen Sie in der Directory Server-Konsole die folgende ACI hinzu.

   ```
   dn:ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>
   changetype:modifyadd:aci
   aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>")
   (targetattr = "*"(version 3.0; acl "SunAM client data anonymous access";
   allow (read, search, compare) userdn = "ldap:///<AuthUIuser's DN>";)
   ```

   Beachten Sie, dass `userdn` auf "`ldap:///<AuthUIuser's DN>`„ eingestellt ist.
3. Lesen Sie die Anweisungen in „To Install and Configure a Distributed Authentication UI Server" in *Sun Java System Access Manager 7.1 Postinstallation Guide* hinsichtlich der Bearbeitung der Datei `amsilent` und der Ausführung des Befehls `amadmin`.
4. Legen Sie in der Datei `amsilent` die folgenden Eigenschaften fest:

APPLICATION_USER	Geben Sie `AuthUIuser` ein.
APPLICATION_PASSWD	Geben Sie ein Passwort für `AuthUIuser` ein.

5. Speichern Sie die Datei.

6. Führen Sie das Skript `amconfig` mit der neuen Konfigurationsdatei aus. Beispielsweise auf einem Solaris-System, auf dem Access Manager im Standardverzeichnis installiert ist:

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

7. Starten Sie den Webcontainer auf dem Distributed Authentication UI-Server neu.

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.

Problemumgehung: 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.

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

Sitzungs- und SSO-Probleme

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.

Problemumgehung: In den folgenden Beispielen hört der Web Server Port 3030 ab. Der Load Balancer hört Port 80 ab und leitet die Anforderungen an den 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"/>
```

Verwendung von `HttpSession` mit Webcontainern anderer Hersteller

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

Richtlinienprobleme

- „Das Löschen der dynamischen Attribute im Policy Configuration Service führt zu Problemen beim Bearbeiten der Richtlinien (6299074)" auf Seite 37

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

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

1. Erstellen Sie zwei dynamische Attribute im Policy Configuration Service.
2. Erstellen Sie eine Richtlinie und wählen Sie die 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: Fehlermeldung, dass eine ungültige dynamische Eigenschaft festgelegt wurde.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.

Problemumgehung: 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)" auf Seite 37

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

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

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

Problemumgehung: Keine. Sie können diese Meldungen ignorieren.

AMSDK-Probleme

- „Bei Ausführung von AMIdentity.modifyService wird ein Fehler ausgegeben (6506448)" auf Seite 38
- „Gruppenmitglieder werden nicht in der ausgewählten Liste angezeigt (6459598)" auf Seite 38

- „Der Anmelde-URL von Access Manager gibt die Meldung “Organisation dieser Art nicht gefunden„ aus. (6430874)” auf Seite 39
- „Das Erstellen einer untergeordneten Organisation von Access Manager aus ist mit `amadmin` nicht möglich (5001850)” auf Seite 39

Bei Ausführung von AMIdentity.modifyService wird ein Fehler ausgegeben (6506448)

Wenn `AMIdentity.modifyService` zur Festlegung des dynamischen Attributs eines Desktopdienstes für einen Bereich (Realm) verwendet wird, gibt Access Manager eine Null-Zeiger-Ausnahme zurück.

Problemumgehung:Fügen Sie `AMConfig.properties` die nachfolgend angegebene Eigenschaft hinzu und starten Sie dann den Server neu.:

```
com.sun.am.ldap.connnection.idle.seconds=7200
```

Gruppenmitglieder werden nicht in der ausgewählten Liste angezeigt (6459598)

Das Problem tritt unter den folgenden Bedingungen auf:

1. Definieren Sie einen Bereich mit der folgenden Bereichsdefinition:
   - Die oberste Bereichsebene lautet `amroot`. Ein untergeordneter Bereich lautet `example.com`.
   - Der untergeordnete Bereich `example.com` enthält zwei Data Stores: `exampleDB` und `exampledminDB`.
   - Der Data Store `exampleDB` enthält alle Benutzer ab `dc=example,dc=com`. Die unterstützten LDAPv3-Operationen sind auf `user=read,write,create,delete,service` eingestellt.
   - Der Data Store `exampleadminDB` enthält eine Admin-Gruppe für den Bereich. Die Admin-Gruppe lautet `DN: cn=example.com Realm Administrators,ou=Groups,dc=example,dc=com`. Diese Gruppe enthält ein einziges Mitglied mit dem Namen `scarter`. Die unterstützten LDAPv3-Operationen sind auf `group=read,write,create,delete` eingestellt.
2. Klicken Sie auf die Registerkarte "Betreffe", dann "Gruppen" und anschließend auf den Eintrag für `example.com Realm Administrators`.
3. Klicken Sie auf die Registerkarte “Benutzer„.

Alle Benutzer im Data Store `exampleDB` werden als verfügbar angezeigt, der Benutzer `scarter` wird jedoch nicht im Feld “Ausgewählt„ angezeigt.

Problemumgehung: Fügen Sie die Operation `user=read` den unterstützten LDAPv3-Operationen im Data Store `exampleadminDB` hinzu.

Der Anmelde-URL von Access Manager gibt die Meldung "Organisation dieser Art nicht gefunden„ aus. (6430874)

Dieses Problem kann aufgrund von Groß- und Kleinschreibung im vollständig qualifizierten Domänennamen (FQDN) auftreten.

Beispiel: `HostName.PRC.Example.COM`

Lösung: Verwenden Sie nach der Installation nicht den standardmäßigen Anmelde-URL von Access Manager. Fügen Sie der Anmelde-URL stattdessen den LDAP-Speicherort der Standardorganisation hinzu. Beispiel:

```
http://HostName.PRC.Example.COM/amserver/UI/Login?org=dc=PRC,dc=Example,dc=COM
```

Nachdem Sie sich erfolgreich bei Access Manager angemeldet haben, können Sie die Einstellung so ändern, dass es nicht mehr erforderlich ist, beim Anmelden bei Access Manager den gesamten Pfad zur Organisation des Benutzers einzugeben. Gehen Sie wie folgt vor:

1. Öffnen Sie im Realm-Modus die Registerkarte "Bereich„ oder im Legacy-Modus die Registerkarte "Organisation„.
2. Klicken Sie auf den standardmäßigen Bereichs- oder Organisationsnamen.

   Klicken Sie in diesem Beispiel auf `prc`.
3. Ändern Sie alle Großbuchstaben des Werts `Bereich-/DNS-Alias` in Kleinbuchstaben.

   Fügen Sie in diesem Beispiel den in Kleinbuchstaben geschriebenen Wert `hostname.prc.example.com` zur Liste hinzu, und entfernen Sie den in Groß- und Kleinbuchstaben geschriebenen Wert `HostName.PRC.Example.COM` aus der Liste.
4. Klicken Sie auf "Speichern„ und melden Sie sich von der Access Manager-Konsole ab.

Sie können sich nun mit jedem der folgenden URLs anmelden:

- `http://hostname.PRC.Example.COM/amserver/UI/Login`
- `http://hostname.PRC.Example.COM/amserver`
- `http://hostname.PRC.Example.COM/amserver/console`

Das Erstellen einer untergeordneten Organisation von Access Manager aus ist mit `amadmin` nicht möglich (5001850)

Dieses Problem tritt auf, wenn die Multi-Master-Replikation zwischen zwei Directory-Servern aktiviert ist und Sie versuchen, mit dem Dienstprogramm `amadmin` eine untergeordnete Organisation zu erstellen.

Problemumgehung: Stellen Sie auf beiden Directory Servern die Eigenschaft `nsslapd-lookthroughlimit` auf -1 ein.

SSL-Problem

Das amconfig-Skript schlägt fehl, wenn das SSL-Zertifikat abgelaufen ist. (6488777)

Wenn der Access Manager-Container im SSL-Modus ausgeführt wird und das SSL-Zertifikat des Containers abgelaufen ist, schlägt `amconfig` fehl und kann zu einer Klassenpfadbeschädigung führen.

Problemumgehung: Wenn Sie `amconfig` bereits mit einem abgelaufenen Zertifikat ausgeführt haben und der Klassenpfad beschädigt ist, benötigen Sie zunächst ein gültiges SSL-Zertifikat. Verwenden Sie die ursprüngliche Datei `domain.xml` oder eine Kopie der Datei `domain.xml`, in der der Klassenpfad nicht beschädigt ist. Führen Sie dann den Befehl `amconfig` erneut aus:

```
/opt/SUNWam/bin/amconfig -s $PWD/amsamplesilent
```

Problem mit Beispielen

Clientsdk-Beispielverzeichnis enthält unerwünschtes Makefile (6490071)

Beispieldateien sind im Client-SDK enthalten. Aus ihnen geht hervor, wie eigenständige Programme und Webanwendungen geschrieben werden. Die Beispiele befinden sich unterhalb des Verzeichnisses, in dem Sie `Makefile.clientsdk` erstellt haben, sowie in folgenden Unterverzeichnissen:

```
.../clientsdk-samples/
```

```
.../clientsdk-webapps/
```

Clientsdk-samples enthält Beispiele für eigenständige Authentifizierungs-, Protokollierungs und Richtlinienprogramme sowie eigenständige SAML-Programme. Clientsdk-webapps

enthält Beispiele für Benutzerverwaltungs-, Dienstverwaltungs- und Richtlinienprogramme. Zu jedem Beispiel gehört eine Readme.html-Datei mit Anweisungen zum Kompilieren und Ausführen des Beispielprogramms.

Zur Kompilierung der Beispiele sollte das Makefile im entsprechenden Unterverzeichnis ausgeführt werden. Das Top-Level-Makefile kompiliert die Beispiele in den Unterverzeichnissen nicht.

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.

Problemumgehung: 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;
```

Probleme mit Windows und HP-UX

Automatische Access Manager-Konfiguration schlägt bei der Installation unter den zh_TW- und es-Gebietsschemata fehl (6515043)

Problemumgehung: Unter den Gebietsschemata `zh_TW` und `es` auf der HP-UX-Plattform darf Access Manager nur im Modus “Später konfigurieren„ konfiguriert werden. Starten Sie das JavaES-Installationsprogramm, installieren Sie das Access Manager-Produkt und beenden Sie

das JavaES-Installationsprogramm. Rufen Sie dann das Access Manager-Konfigurationsprogramm wie nachfolgend dargestellt auf:

1. `LANG=C`
2. `export LANG`
3. Bearbeiten Sie die Datei *accessmanager-base*`/bin/amsamplesilent`.
4. Führen Sie *accessmanager-base*`/bin/amconfig -s amsamplesilent` aus.

HP-UX benötigt bei der Installation des vollständigen JES-Stacks die gettext-Binärdatei mit AM (6497926)

Für dieses Problem gibt es derzeit keine Lösung.

Verbund- und SAML-Probleme

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.

Problemumgehung: Keine.

Globalisierungsprobleme (g11n)

Administration Console-Komponenten werden unter zh-Gebietsschema in englischer Sprache angezeigt (6470543)

Wenn das Gebietsschema des Browsers auf `zh` eingestellt wird, werden die Administration Console-Komponenten, etwa die Schaltfläche für Version, Hilfe und Abmeldung, in englischer Sprache angezeigt.

Problemumgehung: Stellen Sie das Gebietsschema des Browsers anstelle von `zh` auf `zh-cn` ein.

Aktueller Wert und neuer Wert werden in der Console nicht richtig angezeigt (6476672)

In der lokalisierten Version von Administration Console werden die Bezeichnungen für den aktuellen Wert und den neuen Wert nicht richtig angezeigt, nämlich als label.current.value bzw. label.new.value.

Das Datum der Richtlinienbedingung muss gemäß der englischen Ländereinstellung angegeben werden (6390856)

Die Datumformatbeschriftungen der Richtlinienbedingung in der chinesischen Ländereinstellung werden nicht richtig angezeigt. Die Beschriftungen schlagen das englische Datumformat vor. Verwandte Felder akzeptieren ebenfalls englische Datumformate.

Problemumgehung: Verwenden Sie für jedes Feld das in der Feldbeschriftung vorgeschlagene Datumformat.

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

Die Client Detection-Funktion funktioniert nicht ordnungsgemäß. Änderungen der Access Manager 7 .1 Console werden nicht automatisch vom Browser übernommen.

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

Problemumgehung: Stellen Sie sicher, die Webcontainerinstanzen immer mit derselben nativen Codierung zu starten.

Dokumentationsprobleme

Beschreibung der Unterstützung für Rollen und gefilterte Rollen 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 in Access Manager 7.1 Administration Console für die LDAPv3-Konfiguration in das Feld "LDAPv3-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
```

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 herunter (`http://www.bouncycastle.org/`). 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

Sie können auf diese Dokumente in der Access Manager 7.1-Sammlung unter folgender Adresse zugreifen:

http://docs.sun.com/coll/1292.1

Die Access Manager 7 2005Q4-Sammlung wurde um ein neues Dokument mit dem Titel Kapitel 1, „Technical Note: Deploying Access Manager Instances to an Application Server Cluster" in *Technical Note: Deploying Access Manager to an Application Server Cluster* ergänzt.

Die Sun Java System Access Manager Richtlinien-Agenten 2.2-Sammlung beinhaltet nun auch eine Dokumentation zu den neuen Agenten:

http://docs.sun.com/coll/1322.1

Dateien für Neuverteilung

Sun Java System Access Manager 7.1 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) 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 Sie bestmöglich bei der Problembeseitigung unterstützen können, sollten Sie folgende Informationen zur Hand haben, wenn Sie unser Support-Team kontaktieren:

- Beschreibung des Problems, einschließlich der Situation, in der das Problem auftrat, sowie seine Auswirkungen auf Ihre Arbeit.
- 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 Kernspeicherauszüge.

Sun freut sich über Ihre Kommentare

Sun möchte seine Dokumentation laufend verbessern. Ihre Kommentare und Vorschläge sind daher immer willkommen. Klicken Sie unter `http://docs.sun.com/` auf "Send Comments„.

Geben Sie in den entsprechenden Feldern den vollständigen Dokumenttitel sowie die Teilenummer ein. Die Teilenummer ist eine 7-stellige oder 9-stellige Zahl, die Sie auf der Titelseite des Handbuchs oder am Anfang des Dokuments finden. Die Teilenummer von *Access Manager Versionshinweise* lautet z. B. 819-4683-13.

Weitere Quellen von Sun

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

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

Zugriffsfunktionen für Personen mit Behinderungen

Um Eingabehilfen zu erhalten, die nach 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 Anwendungsversionen finden Sie unter:
`http://sun.com/software/javaenterprisesystem/get.html`.

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

Verwandte Websites von Drittanbietern

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

Hinweis – Sun ist nicht für die Verfügbarkeit von Websites Dritter verantwortlich, die in diesem Dokument genannt werden. Sun ist nicht verantwortlich oder haftbar für die Inhalte, Werbung, Produkte oder andere Materialien, die auf solchen Websites/Ressourcen oder über diese verfügbar sind, und unterstützt diese nicht. Sun lehnt jede Verantwortung oder Haftung für direkte oder indirekte Schäden oder Verluste ab, die durch die bzw. in Verbindung mit der Verwendung von oder der Stützung auf derartige Inhalte, Waren oder Dienstleistungen, die auf oder über diese Sites oder Ressourcen verfügbar sind, entstehen können.