Sun Java™ System Access Manager Versionshinweise für Microsoft Windows

Version 7

Teilenummer 819-5798-10

Diese Versionshinweise enthalten wichtige Informationen, die zum Zeitpunkt der Veröffentlichung von Sun Java System Access Manager 7 2005Q4 (vormals Sun Java System Identity Server) für Windows. In diesem Dokument werden bekannte Probleme und Einschränkungen sowie sonstige Informationen angesprochen. Lesen Sie dieses Dokument, bevor Sie diese Version installieren und verwenden.

Die neueste Ausgabe dieser Versionshinweise finden Sie auf der Sun Java System-Dokumentationswebsite: `http://docs.sun.com/app/docs/prod/entsys.05q4`. Besuchen Sie diese Website vor der Installation und Konfiguration Ihrer Software und später regelmäßig, um stets die neuesten Versionshinweise und eine aktuelle Produktdokumentation verfügbar zu haben.

Die Versionshinweise sind in die folgenden Abschnitte gegliedert:

- Änderungsprotokoll der Versionshinweise
- Über Access Manager 7
- Behobene Fehler in dieser Version
- Wichtige Informationen
- Bekannte Probleme und Einschränkungen
- Dateien für Neuverteilung
- Problemmeldungen und Feedback
- Weitere Sun-Ressourcen

Diese Dokumentation kann URLs zu Produkten von Drittanbietern zur Bereitstellung zusätzlicher zugehöriger Informationen enthalten.

HINWEIS Sun ist nicht für die Website-Verfügbarkeit von in diesem Dokument erwähnten Drittanbietern verantwortlich. Sun prüft weder Inhalt noch Werbung, Produkte oder anderes auf diesen oder über diese Websites oder Ressourcen erhältlichen Materialien und übernimmt keine Verantwortung oder Haftung dafür. Sun übernimmt keine Verantwortung oder Haftung für Schäden oder Verluste, die tatsächlich oder angeblich auf die auf solchen oder über solche Websites verfügbaren Inhalte, Waren oder Dienstleistungen zurückzuführen sind oder im Zusammenhang damit auftreten.

Änderungsprotokoll der Versionshinweise

Tabelle 1 Änderungsprotokoll

Datum	Beschreibung der Änderungen
Februar 2006	Revenue-Release
November 2005	Beta-Release

Über Access Manager 7

Sun Java System Access Manager (Access Manager) ist Bestandteil der Sun Identity Management-Infrastruktur, die es einer Organisation erlaubt, einen sicheren Zugang zu Webanwendungen und anderen Ressourcen zu gewährleisten, sowohl innerhalb eines Unternehmens als auch über B2B-Wertschöpfungsketten (Business-to-Business) hinweg. Access Manager stellt folgende Hauptfunktionen bereit:

- Zentralisierte Authentifizierungs- und Autorisierungsdienste unter Verwendung einer rollen- und regelbasierten Zugriffssteuerung
- Single Sign-On (SSO) für den Zugriff auf die webbasierten Anwendungen einer Organisation

- Federated Identity-Unterstützung über das Liberty Alliance-Projekt und SAML (Security Assertions Markup Language)
- Protokollierung von kritischen Informationen wie beispielsweise Administrator- und Benutzeraktivitäten durch Access Manager-Komponenten für eine anschließende Analyse, Berichterstellung und Überwachung

Dieser Abschnitt enthält Informationen zu folgenden Themen:

- Neuheiten in Access Manager 7
- Hardware- und Software-Anforderungen
- Unterstützte Browser

Neuheiten in Access Manager 7

Diese Version umfasst die folgenden neuen Funktionen:

- Access Manager-Modi
- Neue Access Manager-Konsole
- Identity-Repository
- Access Manager-Informationsstruktur
- Änderungen in Bezug auf das Sitzungs-Failover
- Benachrichtigung bei Änderung von Sitzungseigenschaften
- Beschränkung von Sitzungskontingenten
- Verteilte Authentifizierung
- Unterstützung für mehrere Authentifizierungsmodulinstanzen
- "Benannte Konfiguration" oder "verketteter" Namespace für die Authentifizierung
- Verbessertes Richtlinienmodul
- Site-Konfiguration
- Bulk Federation
- Verbesserungen hinsichtlich der Protokollierung

Access Manager-Modi

Access Manager 7 2005Q4 umfasst den Realm- und den Legacy-Modus. Beide Modi bieten Unterstützung für:

- Neue Access Manager 7 2005Q4-Funktionen
- Access Manager 6 2005Q1-Funktionen, abgesehen von diesen Einschränkungen:
  - Bei der Erstellung von Bereichen (Realms) werden die entsprechenden Organisationen nicht in Sun Java System Directory Server erstellt.
  - Über die neue Access Manager 7 2005Q4-Konsole kann keine CoS-Vorlagenpriorität (Class of Service) festgelegt werden. Siehe "Festlegung der CoS-Vorlagenpriorität über die neue Access Manager-Konsole nicht möglich (6309262)" auf Seite 22.
- Identity-Repositories 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, einschließlich Messaging Server, Calendar Server, Instant Messaging oder Delegated Administrator
- Parallele Bereitstellungen, bei denen Access Manager 6 2005Q1 und Access Manager 7 2005Q4 auf denselben Directory Server zugreifen

Neue Access Manager-Konsole

Die Access Manager-Konsole wurde für diese Version umgestaltet. Wenn Access Manager jedoch mit Portal Server, Messaging Server, Calendar Server, Instant Messaging oder Delegated Administrator bereitgestellt wird, müssen Sie Access Manager im Legacy-Modus installieren und die Access Manager 6 2005Q1-Konsole verwenden:

Weitere Informationen finden Sie unter "Kompatibilitätsprobleme" auf Seite 11.

Identity-Repository

Ein Access Manager-Identity-Repository enthält Informationen zu Identitäten wie etwa Benutzern, Gruppen und Rollen. Sie können ein Identity-Repository mit Access Manager oder einem anderen Provisioning-Produkt wie beispielsweise Sun Java System Identity Manager erstellen und verwalten.

In der aktuellen Version kann ein Identity-Repository entweder in Sun Java System Directory Server oder Microsoft Active Directory gespeichert werden. Access Manager kann über Lese-/Schreibzugang oder schreibgeschützten Zugriff auf ein Identity-Repository verfügen.

Access Manager-Informationsstruktur

Die Access Manager-Informationsstruktur enthält Informationen in Bezug auf den Systemzugriff. Jede Access Manager-Instanz erstellt und verwaltet eine separate Informationsstruktur in Sun Java System Directory Server. Eine Access Manager-Informationsstruktur kann über einen beliebigen Namen (Suffix) verfügen. Die Access Manager-Informationsstruktur kann Bereiche (und Unterbereiche, falls erforderlich) umfassen, wie im nachfolgenden Abschnitt beschrieben.

Access Manager-Bereiche

Ein Bereich (Realm) und eventuelle Unterbereiche sind Bestandteil der Access Manager-Informationsstruktur und können Konfigurationsinformationen enthalten, die einen Satz aus Benutzern und/oder Gruppen, die Art der Benutzerauthentifizierung, die für einen Benutzer zugänglichen Ressourcen sowie die Informationen definieren, die für Anwendungen verfügbar sind, nachdem einem Benutzer Zugriff auf die Ressourcen erteilt wurde. Ein Bereich oder Unterbereich kann darüber hinaus weitere Konfigurationsinformationen enthalten, beispielsweise die Globalisierungskonfiguration, die Konfiguration zum Zurücksetzen des Passworts, die Sitzungs- und Konsolenkonfiguration sowie Benutzereinstellungen. Ein Bereich oder Unterbereich kann auch leer sein.

Sie können einen Bereich entweder mithilfe der Access Manager-Konsole oder über das Befehlszeilenprogramm amadmin erstellen. Weitere Informationen finden Sie in der Onlinehilfe zur Konsole oder in Kapitel 14, "The amadmin Command Line Tool", im *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

Änderungen in Bezug auf das Sitzungs-Failover

Access Manager stellt eine vom Webcontainer unabhängige Sitzungs-Failover-Implementierung mit Verwendung von Sun Java System Message Queue (Message Queue) als Kommunikations-Broker und der Berkeley DB von Sleepycat Software, Inc. als Datenbank für die Sitzungsspeicherung. Zu den Erweiterungen von Access Manager 7 2005Q4 zählt die Datei `amsfoconfig.bat` für die Konfiguration der Umgebung für das Sitzungs-Failover.

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

Benachrichtigung bei Änderung von Sitzungseigenschaften

Über die Access Manager-Funktion zur Benachrichtigung bei Änderung von Sitzungseigenschaften wird eine Benachrichtigung an den konfigurierten Listener gesendet, sobald sich eine bestimmte Sitzungseigenschaft ändert. Diese Funktion tritt in Kraft, wenn das Attribut "Enable Property Change Notifications" (Benachrichtigung über Eigenschaftenänderung) in der Access Manager-Administratorkonsole aktiviert wird. In einer SSO-Umgebung (Single Sign-On)

beispielsweise kann eine Access Manager-Sitzung von mehreren Anwendungen gemeinsam genutzt werden. Sobald sich eine spezifische, in der Liste "Notification Properties" (Benachrichtigungseigenschaften) definierte Sitzungseigenschaft ändert, sendet Access Manager eine Benachrichtigung an alle registrierten Listener.

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

Beschränkung von Sitzungskontingenten

Über die Funktion zur Beschränkung von Sitzungskontingenten kann der Access Manager-Administrator (`amadmin`) unter Verwendung des Attributs "Active User Sessions" (Aktive Benutzersitzungen) die maximale Anzahl an parallelen Sitzungen festlegen, die für einen Benutzer zulässig sind. Der Administrator kann eine Sitzungskontingentbeschränkung auf globaler Ebene für alle Benutzer oder auf Elementebene, z. B. für Organisationen, Bereiche, Rollen oder Benutzer festlegen.

Per Voreinstellung ist die Beschränkung der Sitzungskontingente deaktiviert (OFF), der Administrator kann diese Funktion jedoch über das Attribut "Enable Quota Constraints" (Kontingentbeschränkung aktivieren) in der Access Manager-Administratorkonsole aktivieren.

Der Administrator kann darüber hinaus über das Attribut "Resulting Behavior If Session Quota Exhausted" (Verhalten bei Überschreitung des Sitzungskontingents) das Verhalten bei Überschreitung des festgelegten Sitzungskontingents für einen Benutzer konfigurieren.

- DENY_ACCESS. Access Manager lehnt Anmeldeanforderungen für eine neue Sitzung ab.
- DESTROY_OLD_SESSION. Access Manager beendet eine demnächst ablaufende Sitzung.

Das Attribut "Exempt Top-Level Admins From Constraint Checking" (Top-Level-Administratoren von der Kontingentprüfung ausnehmen) legt fest, ob Sitzungskontingente auch für Administratoren mit der Rolle "Top-Level-Administrator" gelten oder nicht.

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

Verteilte Authentifizierung

Der Dienst für die verteilte Authentifizierung ermöglicht einen Austausch von Benutzeridentitäts- und Anmeldeinformationen für die demilitarisierte Zone (DMZ, demilitarized zone). Zur Authentifizierung bei Access Manager muss der Benutzer Identifikations- und Anmeldeinformationen bereitstellen. Während dieses Vorgangs werden die Access Manager-Dienst-URLs gegenüber dem Benutzer offengelegt. Sie können diese Offenlegung durch Einsatz eines Proxy-Servers vermeiden; ein Proxy-Server ist in einigen Bereitstellungen jedoch keine akzeptable Lösung.

Die Mehrzahl der sicheren Bereitstellungen lässt eine direkte Agenten-Umleitung von Anforderungen (aus der demilitarisierten Zone) an den Access Manager-Server (in der sicheren Zone hinter der Firewall) nicht zu, deshalb ist dies die primäre Anforderung den Distributed Authentication-Dienst.

Diese Funktion wird auf jedem Servlet-fähigen Webcontainer als J2EE-Webanwendung bereitgestellt. Der Authentifizierungsdienst kann eine Remote-Authentifizierung und ein Extrahierungs-Framework (d. h. eine Benutzerschnittstelle für die verteilte Authentifizierung) bieten, die als J2EE-Webanwendung in der DMZ-Schicht (auf einem Computer mit Access Manager) bereitgestellt wird, die wiederum mit den Backend-Servern zur Durchführung der eigentlichen Authentifizierung kommuniziert. Der Dienst für die verteilte Authentifizierung kommuniziert (remote) mit dem Authentifizierungsserver und führt die eigentliche Authentifizierung über eine Remote-API aus.

Unterstützung für mehrere Authentifizierungsmodulinstanzen

Alle Authentifizierungsmodule (Standard) wurden zur Unterstützung des Unterschemas mit Konsolen-UI-Unterstützung erweitert. Es können für jeden Modultyp (geladene Modulklasse) mehrere Authentifizierungsmodulinstanzen erstellt werden. Beispielsweise kann bei Instanzen mit Namen `ldap1` und `ldap2` für einen LDAP-Modultyp jede Instanz auf einen anderen LDAP-Directory Server verweisen. Modulinstanzen, deren Namen mit denen der zugehörigen Typen übereinstimmen, werden aus Gründen der Abwärtskompatibilität unterstützt. Der Aufruf erfolgt über *server_deploy*`_uri/UI/Login?module=`*module-instance-name*.

"Benannte Konfiguration" oder "verketteter" Namespace für die Authentifizierung

Unterhalb einer Organisation / eines Bereichs wird ein separater Namespace erstellt, der eine Kette von Authentifizierungsmodulinstanzen darstellt. Die Kette kann wiederverwendet und einer Organisation / einem Bereich, einer Rolle oder einem Benutzer zugewiesen werden. Die Authentifizierungsdienstinstanz entspricht der Authentifzierungskette. Der Aufruf erfolgt über *server_deploy*`_uri/UI/Login?service=`*authentication-chain-name*.

Verbessertes Richtlinienmodul

Personalisierungsattribute

Zusätzlich zu Regeln, Objekten und Bedingungen können Richtlinien ab sofort personalisierte Attribute (IDResponseProvider) umfassen. Die von der Richtlinienauswertung an den Client gesendete Richtlinienentscheidung umfasst nun richtlinienbasierte Antwortpersonalisierungsattribute in den anwendbaren Richtlinien. Es werden zwei Arten von Personalisierungsattributen unterstützt:

- Statische Attribute. Sie definieren Attributname und -wert in der Richtlinie.
- Dynamische Attribute. Sie geben die Attributnamen in der Richtlinie an, die zugehörigen Werte werden bei Auswertung der Richtlinie aus dem Identity-Repository abgerufen.

PEP-Agenten (Policy Enforcement Points) leiten diese Attribute typischerweise als HTTP-Header oder Cookies oder Anforderungsattribute an die geschützte Anwendung weiter.

Access Manager 7 2005Q4 bietet keine Unterstützung für durch den Benutzer angepasste Implementierungen der Response Provider-Schnittstelle.

Bedingungen für Sitzungseigenschaften

Die Implementierung von Bedingungen für Sitzungseigenschaften (SessionPropertyCondition) legt basierend auf den in einer Access Manager-Benutzersitzung eingestellten Eigenschaftenwerten fest, ob eine Richtlinie auf die Anforderung anwendbar ist. Bei Auswertung der Richtlinie wird für die Bedingung nur dann der Wert "true" zurückgegeben, wenn die Access Manager-Benutzersitzung alle in der Bedingung definierten Eigenschaftenwerte umfasst. Für Eigenschaften, für die in der Bedingung mehrere Werte definiert wurden, reicht es aus, dass die Benutzersitzung mindestens einen der in der Bedingung aufgeführten Eigenschaftenwerte enthält.

Richtlinienobjekt

Die Richtlinienobjektimplementierung (Access Manager IdentitySubject) ermöglicht Ihnen die Verwendung von Einträgen aus dem konfigurierten Identity-Repository als Richtlinienobjektwerte.

Richtlinienexport

Sie können über den Befehl `amadmin` Richtlinien im XML-Format exportieren. Die neuen Elemente `GetPolices` und `RealmGetPolicies` in der Datei `amAdmin.dtd` bieten Unterstützung für diese Funktion.

Richtlinienstatus

Eine Richtlinie weist nun ein Statusattribut auf, das als aktiv oder inaktiv gesetzt werden kann. Inaktive Richtlinien werden bei der Richtlinienauswertung ignoriert.

Site-Konfiguration

In Access Manager 7 2005Q4 wird das "Site-Konzept" eingeführt, das eine zentralisierte Konfigurationsverwaltung für eine Access Manager-Bereitstellung bietet. Wenn Access Manager als Site konfiguriert wird, werden Clientanforderungen immer an den Load Balancer gesendet, der die Bereitstellung vereinfacht und Probleme wie z. B. eine Firewall zwischen Client und Backend-Access Manager-Server löst.

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

Bulk Federation

Access Manager 7 2005Q4 bietet eine Bulk Federation-Funktion zur Verbindung von Benutzerkonten mit Anwendungen, die an Geschäftspartner ausgelagert sind. Bisher erfolgte der Verbund von Konten zwischen einem Service Provider (SP) und einem Identity Provider (IDP) folgendermaßen: Der Benutzer musste sowohl auf die SP- als auch auf die IDP-Site zugreifen, es mussten Konten erstellt werden, und anschließend wurden die zwei Konten über einen Weblink miteinander verbunden. Dieser Prozess war sehr zeitaufwändig. Darüber hinaus war diese Vorgehensweise nicht für Bereitstellungen mit vorhandenen Konten sowie für Sites geeignet, die selbst als Identity Provider fungierten oder einen ihrer Partner als Authentifizierungs-Provider einsetzten.

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

Verbesserungen hinsichtlich der Protokollierung

Access Manager 7 2005Q4 umfasst verschiedene Verbesserungen im Hinblick auf die Protokollierung:

- Neue Felder (oder Spalten): Das Feld `MessageID` enthält die Meldungskennung für das protokollierte Ereignis. Das Feld `ContextID` umfasst die Kontextkennung, die einer Sitzungskennung entspricht und für alle Ereignisse einer bestimmten Benutzeranmeldesitzung gilt. Bei einer spezifischen Anmeldesitzung eines Benutzers ist `ContextID` in allen Protokolldateien für protokollierte Ereignisse identisch.
- Protokollierungs-API. Die API umfasst Erweiterungen für das Lesen von Protokolleinträgen. Dies schließt Datenbanken ein, wenn die Protokollierung in einer Datenbank konfiguriert wurde. Informationen zum Abruf von Protokolleinträgen aus einer flachen Datei oder einem Datenbanktabellen-Repository finden Sie in der Datei `LogReaderSample.java` im Verzeichnis `<install-dir>\samples\logging`.

ACHTUNG Datenbanktabellen sind in der Regel größer als flache Dateiprotokolle. Daher sollten Sie bei einer Anforderung nicht alle Einträge einer Datenbanktabelle abrufen, denn die Datenmenge kann schnell sämtliche Access Manager-Serverressourcen verbrauchen.

Hardware- und Software-Anforderungen

Folgende Hardware und Software ist für den Einsatz dieser Version von Access Manager erforderlich:

Tabelle 2 Hardware- und Software-Anforderungen

Komponente	Anforderung
Betriebssystem	Microsoft Windows 2000 Advanced Server, Service Pack 4
	Microsoft Windows 2000 Professional
	Microsoft Windows 2003 Enterprise Server
RAM	512 MB
Festplattenspeicher	250 MB

Unterstützte Browser

Diese Version von Access Manager unterstützt die folgenden Browser:

Tabelle 3 Unterstützte Browser

Browser	Plattformen
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

Behobene Fehler in dieser Version

Keine.

Wichtige Informationen

Nachfolgend werden aktuelle Informationen bereitgestellt, die in der Produktdokumentation nicht enthalten sind. Dieser Abschnitt enthält Informationen zu den folgenden Themen:

- Kompatibilitätsprobleme
- Installationshinweise
- Eingabehilfen für Benutzer mit Behinderungen

Kompatibilitätsprobleme

- Access Manager-Legacy-Modus
- Ermitteln des Access Manager-Modus
- Access Manager-Richtlinienagenten

Access Manager-Legacy-Modus

Access Manager 7 2005Q4 kann in zwei Modi konfiguriert werden:

- Erweiterte (7.x) Installation oder Realm-Modus
- Kompatible (6.x) Installation oder Legacy-Modus

Wenn Sie Access Manager mit Portal Server, Messaging Server, Calendar Server, Instant Messaging oder Delegated Administrator installieren, müssen Sie den Access Manager-kompatiblen (6.x) Modus wählen.

Weitere Informationen finden Sie im Abschnitt "Access Manager-Installationsarten"

Configure Automatically During Installation (Automatisch während der Installation konfigurieren)

Bei Auswahl dieser Option konfiguriert das Installationsprogramm Access Manager im Legacy-Modus.

Configure Manually After Installation (Nach der Installation manuell konfigurieren)

Wenn Sie das Java ES-Installationsprogramm mit der Option "Configure Manually After Installation" (Nach der Installation manuell konfigurieren) ausführen, müssen Sie nach der Installation die Datei `amconfig bat` ausführen, um Access Manager zu konfigurieren.

Zur Auswahl des kompatiblen Installationstyps (6.x) setzen Sie in der Konfigurationsskript-Eingabedatei die folgenden Parameter (`AMConfigurator.Properties`):

```
AM_REALM=disabled
```

```
CONSOLE_DEPLOY_URI=/amconsole
```

So wählen Sie den erweiterten Modus aus:

```
AM_REALM=enabled
```

```
CONSOLE_Deploy_URI=/amserver/console
```

Weitere Informationen zur Konfiguration von Access Manager durch Ausführung der Datei `amconfig.bat` finden Sie im *Sun Java System Access Manager Administration Guide* http://docs.sun.com/doc/817-7647.

Ermitteln des Access Manager-Modus

Über den folgenden Befehl können Sie ermitteln, ob eine ausgeführte Access Manager 7 2005Q4-Installation im Realm- oder Legacy-Modus konfiguriert wurde:

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

Ergebnis:

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

Access Manager-Richtlinienagenten

Die folgende Tabelle zeigt die Kompatibilität der Richtlinienagenten mit den Access Manager 7 2005Q4-Modi.

Tabelle 4 Kompatibilität von Richtlinienagenten mit Access Manager 7 2005Q4-Modi

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

Installationshinweise

Die Installationshinweise zu Access Manager umfassen die folgenden Informationen.

Access Manager-Installationsarten

Wenn Sie das Java ES-Installationsprogramm ausführen, kann Access Manager 7 2005Q4 entweder im Modus "Configure Automatically During Installation" (Automatisch während der Installation konfigurieren) oder im Modus "Configure Manually After Installation" (Nach der Installation manuell konfigurieren) installiert werden.

- Im Modus "Configure Automatically During Installation" (Automatisch während der Installation konfigurieren) konfiguriert das Java ES-Installationsprogramm Access Manager im Legacy-Modus. Die kompatible (6.x) Installation (Legacy-Modus) bietet Unterstützung für Access Manager 6-Funktionen, einschließlich der Access Manager 6-kompatiblen Konsole und Verzeichnisinformationsstruktur (Directory Information Tree, DIT).

  Der standardmäßige Konsolenbereitstellungs-URI für die kompatible Installation (6.x) lautet `amconsole`.

- Im Modus "Configure Manually After Installation" (Nach der Installation manuell konfigurieren) kann Access Manager entweder im Legacy- oder im erweiterten Modus konfiguriert werden. Die erweiterte (7.x) Installation (Realm-Modus) bietet Unterstützung für Access Manager 7-Funktionen, einschließlich der neuen Access Manager 7-Konsole.

  Informationen zur Konfiguration von Access Manager im erweiterten Modus finden Sie unter "Configure Manually After Installation (Nach der Installation manuell konfigurieren)" auf Seite 11.

  Der standardmäßige Konsolenbereitstellungs-URI für die erweiterte Installation (7.x) sowohl für die Server- als auch für die Remote-Konsoleninstallation lautet `amserver/console`.

Wenn Sie das Java ES-Installationsprogramm im unbeaufsichtigten Modus ausführen oder die Access Manager-Datei `amconfig.bat` verwenden, setzen Sie in der Statusdatei oder der Konfigurationsskript-Eingabedatei die folgenden Variablen: `AMConfig.Properties`:

Für den erweiterten (7.x) Modus:

```
AM_REALM=enabled

CONSOLE_DEPLOY_URI=/amserver/console
```

Für den kompatiblen (6.x) Modus:

```
AM_REALM=disabled

CONSOLE_DEPLOY_URI=/amconsole
```

Aktualisierungsanweisungen für Access Manager

Wenn Sie eine Aktualisierung auf Access Manager 7 2005Q4 durchführen, folgen Sie den Anweisungen im *Sun Java Enterprise System 2005Q4 Upgrade Guide for Microsoft Windows* unter http://docs.sun.com/app/docs/doc/819-4461.

Eingabehilfen für Benutzer mit Behinderungen

Informationen zu Eingabehilfen, die seit der Veröffentlichung dieses Dokuments herausgegeben wurden, finden Sie in der Produktbewertung nach Section 508. Dieses Dokument, das Sie bei Sun anfordern können, stellt Informationen dazu bereit, welche Produktversionen am besten für die Bereitstellung von barrierefreien Lösungen geeignet sind. Aktualisierte Anwendungsversionen finden Sie unter: http://sun.com/software/javaenterprisesystem/get.html.

Informationen über die Sun-Projekte zur Barrierefreiheit finden Sie unter http://sun.com/access.

Bekannte Probleme und Einschränkungen

In diesem Abschnitt werden bekannte Probleme und Einschränkungen sowie Umgehungen für diese (sofern verfügbar) zum Zeitpunkt der Veröffentlichung dieser Version beschrieben.

- "Kompatibilitätsprobleme" auf Seite 15
- "Installationsprobleme" auf Seite 17
- "Konfigurationsprobleme" auf Seite 18
- "Access Manager-Konsolenprobleme" auf Seite 21
- "SDK- und Client-Probleme" auf Seite 24
- "Probleme mit Befehlszeilen-Dienstprogrammen" auf Seite 25
- "Authentifizierungsprobleme" auf Seite 26

- "Sitzungs- und SSO-Probleme" auf Seite 27
- "Richtlinienprobleme" auf Seite 28
- "Probleme beim Serverstart" auf Seite 29
- "Federation- und SAML-Probleme" auf Seite 29
- "Globalisierungsprobleme (G11N)" auf Seite 31
- "Dokumentationsprobleme" auf Seite 33

Kompatibilitätsprobleme

- "Inkompatibilität zwischen Java ES 2004Q2-Servern und IM unter Java ES 2005Q4 (6309082)" auf Seite 15
- "Es bestehen Inkompatibilitäten im Kernauthentifizierungsmodul für den Legacy-Modus (6305840)" auf Seite 16
- "Anmeldung als Agent nicht möglich, da kein Profil in der Organisation vorhanden ist (6295074)" auf Seite 16
- "Das Dienstprogramm `commadmin` von Delegated Administrator erstellt keine Benutzer (6294603)" auf Seite 16
- "Das Dienstprogramm `commadmin` von Delegated Administrator erstellt keine Organisation (6292104)" auf Seite 17

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

Dieses Problem wurde durch das folgende Bereitstellungsszenario verursacht:

- 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

Bei Ausführung des Dienstprogramms `imconfig` zur Konfiguration von Instant Messaging auf Server-4 war die Konfiguration nicht erfolgreich. Das von Instant Messaging (IM) auf Server-4 verwendete Access Manager 7 2005Q4 SDK ist nicht mit der Java ES 2004Q2-Version 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 Upgrade Guide.

Es bestehen Inkompatibilitäten im Kernauthentifizierungsmodul für den Legacy-Modus (6305840)

Der Access Manager 7 2005Q4-Legacy-Modus weist folgende Inkompatibilitäten mit dem Kernauthentifizierungsmodul von Access Manager 6 2005Q1 auf:

- Organisations-Authentifizierungsmodule werden im Legacy-Modus entfernt.
- Die Darstellung von "Administrator Authentication Configuration" (Administrator-Authentifizierungskonfiguration) und "Organization Authentication Configuration" (Organisations-Authentifizierungskonfiguration) wurde geändert. In der Access Manager 7 2005Q4-Konsole ist per Voreinstellung der Eintrag `ldapService` ausgewählt. In der Access Manager 6 2005Q1-Konsole wurde eine Bearbeitungsschaltfläche bereitgestellt, und das LDAP-Modul war nicht standardmäßig ausgewählt.

Umgehung

Keine.

Anmeldung als Agent nicht möglich, da kein Profil in der Organisation vorhanden ist (6295074)

Erstellen Sie im Realm-Modus über die Access Manager-Konsole einen Agenten. Wenn Sie sich abmelden und anschließend unter Verwendung des Agentennamens neu anmelden, gibt Access Manager einen Fehler aus, da der Agent keine Berechtigungen zum Zugriff auf den Bereich besitzt.

Umgehung

Ändern Sie die Berechtigungen ab, um dem Agenten Lese- und Schreibzugriff zu erteilen.

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

Das Dienstprogramm `commadmin` von Delegated Administrator erstellt über die Optionen `-S mail, cal` keinen Benutzer in der Standarddomäne.

Umgehung

Dieses Problem tritt auf, wenn Sie Access Manager auf Version 7 2005Q4 aktualisieren, jedoch keine Aktualisierung von Delegated Administrator vornehmen. Informationen zur Aktualisierung von Delegated Administrator finden Sie im *Sun Java Enterprise System 2005Q4 Upgrade Guide for Microsoft Windows.*

Wenn Sie keine Aktualisierung von Delegated Administrator planen, führen Sie die folgenden Schritte aus:

1. Markieren Sie in der Datei `UserCalendarService.xml` die Attribute `mail`, `icssubcribed` und `icsfirstday` anstelle von erforderlich als optional. Diese Datei befindet sich per Voreinstellung im Verzeichnis `<install-dir>\DelegatedAdmin\lib\services`.
2. Entfernen Sie in Access Manager die vorhandene XML-Datei durch Ausführung des Befehls `amadmin`:

   ```
   amadmin.bat -u amadmin -w password -r UserCalendarService
   ```

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

   ```
   amadmin.bat -u amadmin -w password

   <install-dir>\DelegatedAdmin\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 erstellt über die Optionen `-S mail, cal` keine Organisation.

Umgehung

Siehe Umgehung für das vorherige Problem.

Installationsprobleme

- "Bei SDK-Installation mit Containerkonfiguration ist der Benachrichtigungs-URL nicht korrekt (6327845)" auf Seite 18
- "Access Manager-Klassenpfad verweist auf abgelaufenes JCE 1.2.1-Paket (6297949)" auf Seite 18
- "Access Manager-Klassenpfad verweist auf abgelaufenes JCE 1.2.1-Paket (6297949)" auf Seite 18
- "Falsche Protokollierungs- und Debug-Verzeichnisberechtigungen für Nicht-Root-Benutzer (6257161)" auf Seite 18
- "Falsche Protokollierungs- und Debug-Verzeichnisberechtigungen für Nicht-Root-Benutzer (6257161)" auf Seite 18
- "Konfigurationsprobleme" auf Seite 18

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

Wenn Sie eine SDK-Installation mit Containerkonfiguration (DEPLOY_LEVEL=4) vornehmen, ist der Benachrichtigungs-URL nicht richtig angegeben.

Umgehung

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

   ```
   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-Klassenpfad verweist auf abgelaufenes JCE 1.2.1-Paket (6297949)

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

Umgehung

Keine. Wenngleich sich der Paketverweis in `classpath` befindet, wird dieses Paket nicht von Access Manager verwendet.

Falsche Protokollierungs- und Debug-Verzeichnisberechtigungen für Nicht-Root-Benutzer (6257161)

Wenn ein Nicht-Root-Benutzer in der Konfigurationsdatei für die unbeaufsichtigte Installation angegeben ist, werden die Berechtigungen für Debug-, Protokollierungs- und Startverzeichnisse nicht richtig festgelegt.

Umgehung

Ändern Sie die Berechtigungen für diese Verzeichnisse, um dem Nicht-Root-Benutzer Zugriff zu erteilen.

Konfigurationsprobleme

- "Application Server 8.1-Datei `server.policy` muss bearbeitet werden, wenn keine Standard-URIs verwendet werden (6309759)" auf Seite 19
- "Plattformserverliste und FQDN-Aliasattribut werden nicht aktualisiert (6309259, 6308649)" auf Seite 20
- "Datenvalidierung für erforderliche Attribute in den Diensten (6308653)" auf Seite 20
- "Die Datei `amconfig.bat` führt keine Aktualisierung der Bereichs-/DNS-Aliase und Plattformserver-Listeneinträge durch (6284161)" auf Seite 20

- "Die Datei amconfig.bat führt keine Aktualisierung der Bereichs-/DNS-Aliase und Plattformserver-Listeneinträge durch (6284161)" auf Seite 20
- "Access Manager-Realm-Modus ist Standardwert in der Statusdateivorlage für die Konfiguration (6280844)" auf Seite 21

Application Server 8.1-Datei `server.policy` muss bearbeitet werden, wenn keine Standard-URIs verwendet werden (6309759)

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

Umgehung

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

1. Beenden Sie die Application Server-Instanz, auf der Access Manager bereitgestellt wurde.
2. Wechseln Sie zum Verzeichnis `/config`. Beispiel:

   ```
   <install-dir>ApplicationServer\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 den 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` in der folgenden Zeile durch den Nicht-Standard-URI, der für die Dienste-Webanwendung verwendet wird:

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

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

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

7. Ersetzen Sie `ampassword` in der folgenden Zeile durch den Nicht-Standard-URI, der für die Passwort-Webanwendung verwendet wird:

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

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

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

In einer Multi-Server-Bereitstellung werden die Plattformserverliste und das FQDN-Aliasattribut nicht aktualisiert, wenn Sie Access Manager auf dem zweiten Server (und nachfolgenden Servern) installieren.

Umgehung

Fügen Sie Bereichs- / DNS-Aliase und Plattformserver-Listeneinträge manuell hinzu. Die erforderlichen Schritte werden unter "Adding Additional Instances to the Platform Server List and Realm / DNS Aliases" im *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide* beschrieben.

Datenvalidierung für erforderliche Attribute in den Diensten (6308653)

Access Manager 7 2005Q4 erzwingt für erforderliche Attribute in Dienste-XML-Dateien das Vorhandensein von Standardwerten.

Umgehung

Wenn Sie Dienste mit erforderlichen Attributen verwenden, die keine Werte aufweisen, fügen Sie Werte für die Attribute hinzu, und laden Sie den Dienst neu.

Die Datei `amconfig.bat` führt keine Aktualisierung der Bereichs-/DNS-Aliase und Plattformserver-Listeneinträge durch (6284161)

In einer Multi-Server-Bereitstellung führt das Skript `amconfig` keine Aktualisierung der Bereichs- / DNS-Aliase und Plattformserver-Listeneinträge für zusätzliche Access Manager-Instanzen durch.

Umgehung

Fügen Sie Bereichs-/DNS-Aliase und Plattformserver-Listeneinträge manuell hinzu. Die erforderlichen Schritte werden unter "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" im *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide* beschrieben.

Access Manager-Realm-Modus ist Standardwert in der Statusdateivorlage für die Konfiguration (6280844)

Per Voreinstellung ist der Access Manager-Realm-Modus (Variable `AM_REALM`) in der Statusdateivorlage für die Konfiguration aktiviert.

Umgehung

Zur Installation oder Konfiguration von Access Manager im Legacy-Modus setzen Sie die Variable in der Statusdatei zurück:

```
AM_REALM = disabled
```

Access Manager-Konsolenprobleme

- "Für SAML werden beim Duplizieren von Trusted Partner-Einträgen in der Konsole Fehler generiert (6326634)" auf Seite 22
- "Remote-Protokollierung funktioniert nicht für `amConsole.access` und `amPasswordReset.access` (6311786)" auf Seite 22
- "Das Hinzufügen weiterer `amadmin`-Eigenschaften in der Konsole führt zur Änderung des `amadmin`-Benutzerpassworts (6309830)" auf Seite 22
- "Festlegung der CoS-Vorlagenpriorität über die neue Access Manager-Konsole nicht möglich (6309262)" auf Seite 22
- "Ausnahmefehler beim Hinzufügen einer Gruppe zu einem Benutzer als Richtlinien-Administratorbenutzer (6299543)" auf Seite 23
- "Im Legacy-Modus können nicht alle Benutzer aus einer Rolle entfernt werden (6293758)" auf Seite 23
- "Hinzufügen, Löschen oder Bearbeiten von Discovery Service-Ressourcenangeboten nicht möglich (6273148)" auf Seite 23
- "Falsches LDAP-Bindungspasswort sollte Fehler für die Antragstellersuche ausgeben (6241241)" auf Seite 23
- "Access Manager kann unterhalb eines Containers im Legacy-Modus keine Organisation erstellen (6290720)" auf Seite 23

- "Beim Hinzufügen von Portal Server-bezogenen Diensten wird die alte Konsole geöffnet (6293299)" auf Seite 24
- "Konsole gibt nach Erreichen des Ressourcenlimits keine Ergebnissätze aus Directory Server zurück (6239724)" auf Seite 24

Für SAML werden beim Duplizieren von Trusted Partner-Einträgen in der Konsole Fehler generiert (6326634)

Erstellen Sie in der Access Manager-Konsole unterhalb der Registerkarte "Federation > SAML" einen "SAML Trusted Partner". Wenn Sie versuchen, den Trusted Partner zu duplizieren, werden Fehler ausgegeben.

Umgehung

Keine.

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

Wenn die Remote-Protokollierung konfiguriert wurde, werden alle Protokolle in die Remote-Instanz von Access Manager geschrieben, nicht jedoch für `amConsole.access` und `amPasswordReset.access` zur Aufzeichnung von Informationen zum Zurücksetzen von Passwörtern. Protokolleinträge werden an keiner Stelle aufgezeichnet.

Umgehung

Keine.

Das Hinzufügen weiterer `amadmin`-Eigenschaften in der Konsole führt zur Änderung des `amadmin`-Benutzerpassworts (6309830)

Das Hinzufügen oder Bearbeiten einiger Eigenschaften für den Benutzer `amadmin` in der Administrationskonsole führt dazu, dass das amadmin-Benutzerpasswort geändert wird.

Umgehung

Keine.

Festlegung der CoS-Vorlagenpriorität über die neue Access Manager-Konsole nicht möglich (6309262)

Über die neue Access Manager 7 2005Q4-Konsole kann keine CoS-Vorlagenpriorität (Class of Service) festgelegt oder geändert werden.

Umgehung

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

Ausnahmefehler beim Hinzufügen einer Gruppe zu einem Benutzer als Richtlinien-Administratorbenutzer (6299543)

Die Access Manager-Konsole gibt einen Ausnahmefehler aus, wenn Sie als Richtlinien-Administratorbenutzer eine Gruppe einem Benutzer hinzufügen.

Umgehung

Keine.

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

Wenn Sie im Legacy-Modus versuchen, alle Benutzer aus einer Rolle zu entfernen, bleibt ein Benutzer erhalten.

Umgehung

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

Hinzufügen, Löschen oder Bearbeiten von Discovery Service-Ressourcenangeboten nicht möglich (6273148)

In der Access Manager-Administrationskonsole ist es nicht möglich, die Ressourcenangebote für einen Benutzer, eine Rolle oder einen Bereich zu löschen oder zu bearbeiten oder solche hinzuzufügen.

Umgehung

Keine.

Falsches LDAP-Bindungspasswort sollte Fehler für die Antragstellersuche ausgeben (6241241)

Die Access Manager-Administrationskonsole gibt keinen Fehler aus, wenn das falsche LDAP-Bindungspasswort verwendet wird.

Umgehung

Keine.

Access Manager kann unterhalb eines Containers im Legacy-Modus keine Organisation erstellen (6290720)

Wenn Sie einen Container erstellen und anschließend versuchen, unterhalb des Containers eine Organisation zu erstellen, gibt Access Manager einen Fehler zur Verletzung der Eindeutigkeit aus.

Umgehung

Keine.

Beim Hinzufügen von Portal Server-bezogenen Diensten wird die alte Konsole geöffnet (6293299)

Portal Server und Access Manager sind auf demselben Server installiert. Access Manager befindet sich im Legacy-Modus. Melden Sie sich unter Verwendung von `/amserver` an der neuen Access Manager-Konsole an. Wenn Sie einen vorhandenen Benutzer auswählen und versuchen, Dienste hinzuzufügen (z. B. NetFile oder Netlet), wird plötzlich die alte Access Manager-Konsole (`/amconsle`) angezeigt.

Umgehung

Keine. Die aktuelle Version von Portal Server erfordert die Access Manager 6 2005Q1-Konsole.

Konsole gibt nach Erreichen des Ressourcenlimits keine Ergebnissätze aus Directory Server zurück (6239724)

Installieren Sie Directory Server und Access Manager mit der vorhandenen DIT-Option. Melden Sie sich an der Access Manager-Konsole an, und erstellen Sie eine Gruppe. Bearbeiten Sie die Benutzer in der Gruppe. Fügen Sie beispielsweise Benutzer mit dem Filter `uid=*999*` hinzu. Die Ergebnisliste ist leer, und die Konsole zeigt weder eine Fehler-, Informations- noch eine Warnmeldung an.

Umgehung

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

SDK- und Client-Probleme

- "Sitzungsdienstkonfiguration für einen Unterbereich kann nicht entfernt werden (6318296)" auf Seite 24
- "CDC-Servlet-Umleitung auf ungültige Anmeldeseite wenn Richtlinienbedigung angegeben (6311985)" auf Seite 25
- "Clients erhalten nach Serverneustart keine Benachrichtigung (6309161)" auf Seite 25
- "Identity-Repository ldapv3-Plug-In und openldap erfordern Patch (6305268)" auf Seite 25
- "SDK-Clients müssen nach Änderung des Dienstschemas neu gestartet werden (6292616)" auf Seite 25

Sitzungsdienstkonfiguration für einen Unterbereich kann nicht entfernt werden (6318296)

Nach der Erstellung eines Unterbereichs des Top-Level-Bereichs und dem Hinzufügen des Sitzungsdienstes zu diesem Unterbereich führen anschließende Versuche zum Entfernen der Sitzungsdienstkonfiguration zu einer Fehlermeldung.

Umgehung

Entfernen Sie das standardmäßige ID-Repository erster Ebene, AMSDK1, und fügen Sie dieses Repository anschließend erneut in die Konfiguration ein.

CDC-Servlet-Umleitung auf ungültige Anmeldeseite wenn Richtlinienbedigung angegeben (6311985)

Wenn sich der Apache-Agent 2.2 im CDSSO-Modus befindet und auf die agentengeschützte Ressource zugegriffen wird, leitet das CDC-Servlet den Benutzer nicht auf die standardmäßige Anmeldeseite, sondern auf die Seite zur anonymen Authentifizierung um.

Umgehung

Keine.

Clients erhalten nach Serverneustart keine Benachrichtigung (6309161)

Mit dem Client-SDK (amclientsdk.jar) geschriebene Anwendungen erhalten keine Benachrichtigung, wenn der Server neu gestartet wird.

Umgehung

Keine.

Identity-Repository ldapv3-Plug-In und openldap erfordern Patch (6305268)

`openldap` unterstützt keine fortlaufende Suche, und ohne eine Verbindung für die fortlaufende Suche kann das Plug-In nicht gestartet werden.

Umgehung

Fordern Sie zur Verwendung des ldapv3-Plug-Ins ein Access Manager-Patch beim technischen Support von Sun Microsystems an.

SDK-Clients müssen nach Änderung des Dienstschemas neu gestartet werden (6292616)

Wenn Sie ein Dienstschema ändern, gibt `ServiceSchema.getGlobalSchema` nicht das neue, sondern weiterhin das alte Schema zurück.

Umgehung

Starten Sie den Client nach einer Änderung des Dienstschemas neu.

Probleme mit Befehlszeilen-Dienstprogrammen

- "XML-Dokumente mit Escape-Zeichen können in Internet Explorer 6.0 nicht gespeichert werden (4995100)" auf Seite 26

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 einem "&") in eine XML-Datei einfügen, wird die Datei zunächst ordnungsgemäß gespeichert. Wenn Sie das XML-Profil später jedoch unter Verwendung von Internet Explorer 6.0 abrufen, wird die Datei nicht ordnungsgemäß angezeigt. Wenn Sie anschließend versuchen, das Profil erneut zu speichern, wird ein Fehler ausgegeben.

Umgehung

Keine.

Authentifizierungsprobleme

- "UrlAccessAgent-SSO-Token läuft ab (6327691)" auf Seite 26
- "Anmeldung an Unterbereich mit LDAPV3-Plug-In / dynamischem Profil nach Passwortkorrektur nicht möglich (6309097)" auf Seite 26
- "Inkompatibilität für Access Manager-Standardkonfiguration des Statistikdienstes im (kompatiblen) Legacy-Modus (6286628)" auf Seite 27
- "Attributeindeutigkeit in Top-Level-Organisation für Namensattribute nicht gegeben (6204537)" auf Seite 27

UrlAccessAgent-SSO-Token läuft ab (6327691)

Das UrlAccessAgent-SSO-Token läuft ab, da das Anwendungsmodul nicht den spezifischen Benutzer-DN zurückgibt, wodurch der Abgleich des Benutzer-DNs und damit ein Token ohne Ablaufdatum fehlschlägt.

Umgehung

Keine.

Anmeldung an Unterbereich mit LDAPV3-Plug-In/dynamischem Profil nach Passwortkorrektur nicht möglich (6309097)

Wenn Sie im Realm-Modus einen ldapv3-Datenspeicher in einem Bereich mit einem "falschen" Passwort erstellen und das Passwort später als Benutzer `amadmin` ändern, wird bei der erneuten Anmeldung als der Benutzer, dessen Passwort geändert wurde, ein Anmeldefehler zurückgegeben, nach dem kein Profil vorhanden ist.

Umgehung

Keine.

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

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

- Der Dienst ist per Voreinstellung aktiviert (`com.iplanet.services.stats.state=file`). Vor der Installation war der Dienst deaktiviert.
- Das Standardintervall (`com.iplanet.am.stats.interval`) wurde von 3600 in 60 geändert.
- Das standardmäßige stats-Verzeichnis (`com.iplanet.services.stats.directory`) wurde von `<install-dir>\AccessManager\debug` in `<install-dir>\AccessManager\stats`.

Umgehung

Keine.

Attributeindeutigkeit in Top-Level-Organisation für Namensattribute nicht gegeben (6204537)

Melden Sie sich nach der Installation von Access Manager als `amadmin` an, und fügen Sie die Attribute `o`, `sunPreferredDomain`, `associatedDomain`, `sunOrganizationAlias`, `uid` und `mail` zur Liste der eindeutigen Attribute hinzu. Wenn Sie zwei neue Organisationen mit identischen Namen erstellen, schlägt die Operation fehl. Access Manager zeigt jedoch anstelle der erwarteten Fehlermeldung zur Verletzung der Eindeutigkeit eine Meldung an, nach der die Organisation bereits vorhanden ist.

Umgehung

Keine. Ignorieren Sie die falsche Meldung. Access Manager funktioniert ordnungsgemäß.

Sitzungs- und SSO-Probleme

- "Access Manager-Instanzen für unterschiedliche Zeitzonen führen zu Timeouts anderer Benutzersitzungen (6323639)" auf Seite 27
- "Das System erzeugt ungültige Diensthostnamen, wenn ein Load Balancer mit SSL-Terminierung verwendet wird (6245660)" auf Seite 28

Access Manager-Instanzen für unterschiedliche Zeitzonen führen zu Timeouts anderer Benutzersitzungen (6323639)

Access Manager-Instanzen, die über unterschiedliche Zeitzonen hinweg installiert wurden und sich im selben Vertrauensbereich befinden, können zu Timeouts bei Benutzersitzungen führen.

Das System erzeugt ungültige Diensthostnamen, wenn ein Load Balancer mit SSL-Terminierung verwendet wird (6245660)

Wenn Access Manager mit Web Server als Webcontainer und einem Load Balancer mit SSL-Terminierung bereitgestellt wird, werden Clients nicht an die richtige Web Server-Seite weitergeleitet. Beim Klicken auf die Registerkarte "Sessions" (Sitzungen) in der Access Manager-Konsole wird ein Fehler zurückgegeben, da der Host ungültig ist.

Umgehung

In den folgenden Beispielen überwacht Web Server Port 3030. Der Load Balancer überwacht Port 80 und leitet Anforderungen an Web Server um.

Bearbeiten Sie in der Datei *web-server-instance-name*\config\server.xml das Attribut servername gemäß der verwendeten Web Server-Version, damit dieses auf den Load Balancer verweist.

Bearbeiten Sie das Attribut servername für Web Server 6.1 Service Pack (SP) folgendermaßen:

```
<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 einen Protokollwechsel von http auf https oder von https auf http vornehmen. Daher muss servername wie folgt bearbeitet werden:

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

Richtlinienprobleme

Das Löschen von dynamischen Attributen im Richtlinienkonfigurationsdienst führt zu Problemen bei der Richtlinienbearbeitung (6299074)

Das Löschen von dynamischen Attributen im Richtlinienkonfigurationsdienst führt im folgenden Szenario zu Problemen bei der Richtlinienbearbeitung:

1. Erstellen Sie zwei dynamische Attribute im Richtlinienkonfigurationsdienst.
2. Erstellen Sie eine Richtlinie, und wählen Sie die dynamischen Attribute (aus Schritt 1) im Response Provider aus.
3. Entfernen Sie die dynamischen Attribute im Richtlinienkonfigurationsdienst, und erstellen Sie zwei weitere Attribute.
4. Versuchen Sie, die in Schritt 2 erstellte Richtlinie zu bearbeiten.

Ergebnis: Es wird eine Fehlermeldung ausgegeben, nach der eine ungültige dynamische Eigenschaft gesetzt wurde. Es wurden per Voreinstellung keine Richtlinien in der Liste angezeigt. Nach einem Suchlauf werden die Richtlinien angezeigt, Sie können die vorhandenen Richtlinien jedoch weder bearbeiten noch löschen, und es ist nicht möglich, eine neue Richtlinie zu erstellen.

Umgehung

Bevor Sie die dynamischen Attribute aus dem Richtlinienkonfigurationsdienst entfernen, entfernen Sie die Verweise auf diese Attribute aus den Richtlinien.

Probleme beim Serverstart

- "Debug-Fehler beim Access Manager-Start (6309274, 6308646)" auf Seite 29

Debug-Fehler beim Access Manager-Start (6309274, 6308646)

Beim Start von Access Manager 7 2005Q4 wird ein Debug-Fehler in den Debug-Dateien `amDelegation` und `amProfile` zurückgegeben:

- `amDelegation`: Plug-In-Instanz für Delegierung kann nicht abgerufen werden
- `amProfile`: Ausnahme bei Delegierung empfangen

Umgehung

Keine. Sie können diese Meldungen ignorieren.

Federation- und SAML-Probleme

- "Federation schlägt fehl, wenn das Artifact-Profil verwendet wird (6324056)" auf Seite 30
- "Sonderzeichen (&) in SAML-Anweisungen müssen codiert werden (6321128)" auf Seite 30
- "Ausnahmefehler bei dem Versuch, einer Rolle den Disco Service hinzuzufügen (6313437)" auf Seite 30
- "Auth Context-Attribute erst konfigurierbar, wenn andere Attribute konfiguriert und gespeichert wurden (6301338)" auf Seite 30
- "EP-Beispiel funktioniert nicht, wenn Root-Suffix das Zeichen "&" enthält (6300163)" auf Seite 30
- "Abmeldefehler bei Federation (6291744)" auf Seite 31

Federation schlägt fehl, wenn das Artifact-Profil verwendet wird (6324056)

Wenn Sie einen Identity Provider (IDP) und einen Service Provider (SP) einrichten, das Kommunikationsprotokoll zur Verwendung des Browser-Artifact-Profils ändern und anschließend versuchen, Benutzer zwischen IDP und SP zu verbinden, schlägt der Federation-Vorgang fehl.

Umgehung

Keine.

Sonderzeichen (&) in SAML-Anweisungen müssen codiert werden (6321128)

Bei Verwendung von Access Manager als Quell- und Ziel-Site und Einsatz von SSO tritt ein Fehler in der Ziel-Site auf, da die Sonderzeichen (&) in den SAML-Anweisungen nicht codiert sind und die Assertionsprüfung fehlschlägt.

Umgehung

Keine.

Ausnahmefehler bei dem Versuch, einer Rolle den Disco Service hinzuzufügen (6313437)

Wenn Sie im Access Manager versuchen, dem Disco Service ein Ressourcenangebot hinzuzufügen, wird eine unbekannte Ausnahme ausgegeben.

Umgehung

Keine.

Auth Context-Attribute erst konfigurierbar, wenn andere Attribute konfiguriert und gespeichert wurden (6301338)

Auth Context-Attribute sind erst konfigurierbar, wenn Sie andere Attribute konfiguriert und gespeichert haben.

Umgehung

Konfigurieren und speichern Sie ein Provider-Profil, bevor Sie die Auth Context-Attribute konfigurieren.

EP-Beispiel funktioniert nicht, wenn Root-Suffix das Zeichen "&" enthält (6300163)

Wenn Directory Server über ein Root-Suffix mit dem Zeichen "&" verfügt und Sie versuchen, ein Employee Profile Service-Ressourcenangebot hinzuzufügen, wird eine Ausnahme ausgegeben.

Umgehung

Keine.

Abmeldefehler bei Federation (6291744)

Wenn Sie im Realm-Modus Benutzerkonten auf einem Identity Provider (IDP) und Service Provider (SP) verbinden, den Federation-Vorgang beenden und sich anschließend abmelden, wird ein Fehler erzeugt: Fehler: Keine Unterorganisation gefunden.

Umgehung

Keine.

Globalisierungsprobleme (G11N)

- "Ländereinstellungen des Benutzers werden nicht auf die gesamte Administrationskonsole angewendet (6326734)" auf Seite 31
- "Entfernung von UTF-8-Zeichensatz funktioniert nicht in Clienterkennung (5028779)" auf Seite 31
- "Multibyte-Zeichen werden in Protokolldateien als Fragezeichen angezeigt (5014120)" auf Seite 32
- "Teilweise nicht lokalisierte Access Manager-Anmeldeseite unter Windows 2000 (Spanisch) (6358371)" auf Seite 32

Ländereinstellungen des Benutzers werden nicht auf die gesamte Administrationskonsole angewendet (6326734)

Teile der Access Manager-Administrationskonsole entsprechen nicht der Ländereinstellung des Benutzers, sondern verwenden die Ländereinstellung des Browsers. Dieses Problem betrifft die Schaltflächen für Version, Abmeldung und den Aufruf der Onlinehilfe sowie die Inhalte von Versionsanzeige und Onlinehilfe.

Umgehung

Ändern Sie die Browsereinstellungen so ab, dass sie mit den Benutzereinstellungen übereinstimmen.

Entfernung von UTF-8-Zeichensatz funktioniert nicht in Clienterkennung (5028779)

Die Client-Erkennungsfunktion arbeitet nicht ordnungsgemäß. Änderungen an der Access Manager 7 2005Q4-Konsole werden nicht automatisch an den Browser übertragen.

Umgehung

Es gibt zwei Möglichkeiten zur Umgehung:

- Starten Sie den Access Manager-Webcontainer neu, nachdem Sie eine Änderung im Client-Erkennungsabschnitt vorgenommen haben.

  oder

- Führen Sie in der Access Manager-Konsole die folgenden Schritte aus:
- Klicken Sie unterhalb der Registerkarte `Configuration` (Konfiguration) auf `Client Detection` (Client-Erkennung).
- Klicken Sie auf den Link `Edit` (Bearbeiten) für `genericHTML`.
- Klicken Sie unterhalb der Registerkarte `HTML` auf den Link `genericHTML`.
- Fügen Sie in die Liste mit den Zeichensätzen den folgenden Eintrag ein: `UTF-8;q=0.5` (Stellen Sie sicher, dass der Faktor `UTF-8 q` niedriger ist als für die anderen Zeichensätze Ihrer Ländereinstellung.)
- Speichern Sie, melden Sie sich ab, und melden Sie sich erneut an.

Multibyte-Zeichen werden in Protokolldateien als Fragezeichen angezeigt (5014120)

Multibyte-Meldungen in Protokolldateien im Verzeichnis `<install-dir>\AccessManager\logs` werden als Fragezeichen (?) angezeigt. Protokolldateien werden nicht immer in UTF-8, sondern in der systemeigenen Codierung gespeichert. Wenn eine Webcontainerinstanz in einer bestimmten Ländereinstellung gestartet wird, werden die Protokolldateien in der systemeigenen Codierung für diese Ländereinstellung gespeichert. Wenn Sie auf eine andere Ländereinstellung wechseln und die Webcontainerinstanz neu starten, werden neue Meldungen in der systemeigenen Codierung für die aktuelle Ländereinstellung, Meldungen mit der vorherigen Codierung werden jedoch als Fragezeichen angezeigt.

Umgehung

Stellen Sie sicher, dass Webcontainerinstanzen immer mit derselben systemeigenen Codierung gestartet werden.

Teilweise nicht lokalisierte Access Manager-Anmeldeseite unter Windows 2000 (Spanisch) (6358371)

Die spanische Version der Access Manager-Anmeldeseite zeigt unter Windows 2000 teilweise nicht lokalisierten Inhalt.

Umgehung

Verwenden Sie den Mozilla Firefox-Browser.

Dokumentationsprobleme

- "Serverseitige Eigenschaft com.iplanet.am.session.client.polling.enable darf nicht auf "true" gesetzt werden (6320475)" auf Seite 33
- "Standardmäßiger URL bei erfolgreicher Authentifizierung in der Konsolen-Onlinehilfe falsch dokumentiert (6296751)" auf Seite 33

Serverseitige Eigenschaft com.iplanet.am.session.client.polling.enable darf nicht auf "true" gesetzt werden (6320475)

Die Eigenschaft com.iplanet.am.session.client.polling.enable in der Datei AMConfig.properties darf auf Serverseite nicht auf true gesetzt werden.

Umgehung

Diese Eigenschaft ist per Voreinstellung auf false gesetzt und darf nicht in true geändert werden.

Standardmäßiger URL bei erfolgreicher Authentifizierung in der Konsolen-Onlinehilfe falsch dokumentiert (6296751)

Der Standard-URL bei erfolgreicher Authentifizierung ist in der Onlinehilfedatei service.scserviceprofile.iplanetamauthservice.html falsch dokumentiert. Das Feld "Default Success URL" (Standardmäßiger Erfolgs-URL) akzeptiert eine aus mehrereren Werten bestehende Liste, die den URL angibt, auf den Benutzer nach einer erfolgreichen Authentifizierung umgeleitet werden. Das Format für dieses Attribut lautet clientType|URL, wenngleich Sie auch nur den URL-Wert angeben können, was den Standardtyp HTML voraussetzt.

Der Standardwert "/amconsole" ist falsch.

Umgehung

Der richtige Standardwert lautet "/amserver/console".

Dateien für Neuverteilung

Der Sun Java System Access Manager 7 enthält keine Dateien für die Neuverteilung an nicht lizenzierte Produktbenutzer.

Problemmeldungen und Feedback

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

- Sun-Softwaresupport unter
  http://www.sun.com/service/sunone/software

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

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

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

Kommentare sind willkommen

Sun ist daran interessiert, seine Dokumentation zu verbessern und freut sich auf Ihre Kommentare und Vorschläge. Verwenden Sie das webbasierte Formular, um uns Ihr Feedback mitzuteilen:

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

Tragen Sie den vollständigen Titel der Dokumentation und die vollständige Teilenummer in die entsprechenden Felder ein. Die Teilenummer ist eine 7-stellige oder 9-stellige Zahl, die Sie auf der Titelseite des Handbuchs oder am Anfang des Dokuments finden. Die Teilenummer dieses Dokuments mit Versionshinweisen lautet beispielsweise 819-5798-10.

Weitere Sun-Ressourcen

Nützliche Ressourcen zu Sun Java System finden Sie unter den folgenden Internetadressen:

- Sun Java System-Dokumentation
  http://docs.sun.com/app/docs/prod/entsys.05q4#hic
- Sun Java System-Services
  http://www.sun.com/service/products/software/javaenterprisesystem/
- Sun Java System-Softwareprodukte und -Services
  http://wwws.sun.com/software/
- Sun Java System-Softwaresupport
  http://www.sun.com/service/sunone/software
- Sun Java System-Support und Knowledge Base
  http://sunsolve.sun.com
- Sun Java System-Consulting und -Services
  http://www.sun.com/service/products/software/javaenterprisesystem
- Sun Java System-Informationen für Entwickler
  http://developers.sun.com/
- Sun-Entwicklersupport
  http://www.sun.com/developers/support