Sun Java™ System Access Manager 发行说明

第 6 版 2005Q1

2005 年 2 月 25 日

文件号码 819-1948

本发行说明包含 Sun Java System Access Manager 6 2005Q1 （以前称为 Sun Java System Identity Server）发行时可用的重要信息。这里介绍了新功能和增强功能、已知的问题和限制及其他信息。在安装与使用此发行版之前请先阅读本文档。

您可以在 Sun Java System 文档网站找到本发行说明的最新版本：

http://docs.sun.com/prod/entsys.05q1 及
http://docs.sun.com/prod/entsys.05q1?l=zh

请在安装和设置软件之前先访问此网站，并定期查看最新的发行说明和产品文档。

本发行说明包含以下内容：

本文档中引用了第三方 URL，其中提供附加的相关信息。

注 Sun 对本文档中提到的第三方 Web 站点的可用性不承担任何责任。对于此类站点或资源中的（或通过它们获得的）任何内容、广告、产品或其他材料，Sun 并不表示认可，也不承担任何责任。对于因使用或依靠此类站点或资源中的 （或通过它们获得的）任何内容、产品或服务而造成的或连带产生的实际或名义损坏或损失， Sun 概不负责，也不承担任何责任。

发行说明修订历史记录

表 1 修订历史记录

日期	更改说明
2005 年 2 月 25 日	修改表 2 “硬件和软件要求”，列出所支持的 Red Hat™ Linux 版本。
2005 年 2 月 2 日	发行 2005Q1。初次发布本发行说明。

关于 Access Manager 6 2005Q1

Sun Java System Access Manager 是一种身份管理解决方案，其设计目的是满足急速扩大的企业需求。利用 Access Manager，您可以将雇员、商业伙伴及供应商的身份统一放入一个在线目录。然后，它提供建立访问贵公司信息的策略和权限的方法。 Access Manager 对于您的全部数据、服务以及了解信息访问情况而言很关键 — 对于您所有的内部和外部业务关系很关键。

此发行版的新增功能

Access Manager 2005Q1 包括以下功能。有关这些功能的详细说明，请参阅《*Sun Java System Access Manager Technical Overview*》。

- 产品名称已从 Identity Server 改为 Access Manager
- 支持 Solaris 10
- 支持新的 Web 容器：Sun Java System Application Server Enterprise Edition 8 2005Q1 (8.1)
- 新增或修订的验证模块：
  - Java 数据库连接 (JDBC)
  - 移动站 ISDN (MSISDN)
  - 活动目录
  - 安全声明标记语言 (SAML)：SAML 验证支持已作为验证模块发行，使 SAML 验证成为验证栈的一部分。
- 会话故障转移
  - 两个或更多的 Access Manager 6 2005Q1 实例，每个实例都可在不同主机服务器上支持的 Web 容器中运行。
  - Message Queue 代理群集，用于管理 Access Manager 实例和会话存储数据库之间的会话消息。
  - Sleepycat Software, Inc. (http://www.sleepycat.com/) 的 Berkeley DB 作为会话存储数据库。 Berkeley DB 客户机守护进程是 amsessiondb。
- “策略管理”包含一个新的 “资源名称”插件：`HttpURLResourceName`。
- 控制台的增强功能：
  - 可以通过显示对象的一项或多项属性，自定义浏览窗格中每个对象类型的视图。
  - 可以在浏览窗格下拉菜单中添加新的对象类型 （例如，添加打印机或建筑物条目）。
- 客户机 SDK：

- 重新包装了 SDK （验证、服务管理、用户管理、 SAML、策略客户机和会话组件），使 Java 应用程序开发者可以更好地集成 Access Manager。
- 消除了对 serverconfig.xml 文件的依赖性，使 jar 文件占用最小的空间。

- 联合管理：
  - 支持 Liberty Alliance Project (LAP) 名称标识符映射协议
  - 支持 LAP Identity Web Services Framework (ID-WSF) 搜索服务规范 1.1 版
  - 支持 LAP ID-WSF 验证服务规范
  - 支持 LAP 元数据说明和搜索规范
  - 支持 LAP Liberty Identity Federation Framework (ID-FF) 扩展配置文件：
    - 动态身份提供者代理
    - 附属提供者联合
    - 临时联合
    - 名称标识符映射配置文件
    - 名称标识符加密配置文件
- 增加了性能调节脚本，可将 Application Server Enterprise Edition 8 2005Q1 (8.1) 调节成为 Web 容器

硬件和软件要求

本发行版的 Access Manager 要求配备以下硬件和软件。

表 2 硬件和软件要求

组件	要求
操作系统	Solaris™ 操作系统 (OS), SPARC® Platform Edition，版本 8，9，10
	Solaris™ OS, x86 Platform Edition，版本 9， 10
	Red Hat™ Linux, WS/AS/ES 2.1 Update 2
	Red Hat™ Linux, WS/AS/ES 3.0 Update 1
RAM	512 MB
磁盘空间	250 MB，用于 Access Manager 和相关的应用程序

支持的浏览器

本 Access Manager 发行版支持以下浏览器：

浏览器	平台
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000、 Sun Linux、 Red Hat™ Linux 8.0
Microsoft Internet Explorer 6.0	Windows 2000、 Windows™ XP、 Sun Linux、 Red Hat Linux 8.0
Mozilla 1.7.1	Windows 2000、 Sun Linux、 Red Hat Linux 8.0、 Solaris™ 9 和 10、 Solaris™ OS、 x86 Platform Edition 版本 9， 10
Netscape™ 4.79	Windows NT、 Solaris 8 和 9
Netscape™ 6.2.1	Windows NT、 Windows 98、 Sun Linux、 Red Hat™ Linux Advanced Server 2.1、 Solaris™ OS、 x86 Platform Edition 版本 9， 10
Netscape™ 7.0	Windows 2000、Sun Linux、Red Hat Linux 8.0、Solaris 9 和 10、Solaris™ OS、 x86 Platform Edition 版本 9， 10

此发行版中修复的错误

下表说明了 Access Manager 2005Q1 中修复的错误：

表 3 Access Manager 2005Q1 中修复的错误

错误编号	说明
5050332	在 Linux 系统上， amserver stop 无法停止 amunixd 进程
5049218	在禁用 “用户管理”的情况下搜索 “用户”时，控制台出错
5048378	AMConfig.properties 中的 smtp Server Port 属性不正确
5043752	在运行 am2bak 时显示失败的消息
5042100	策略管理员无法修改自己的配置文件
5041529	BasicEntitySearch 过滤器硬编码为 uid
5038600	使用 SAML 服务不能创建用户
5037978	将具有定义的 “访问权限”的角色创建为 “组织管理员”时出错
5026635	控制台范例无法编译
5016725	在子组织中未反映对参考策略规则所作的修改

表 3 Access Manager 2005Q1 中修复的错误 *（续）*

错误编号	说明
5013994	日语浏览器中，加入 “验证级别”参数时登录失败
5008960	amadmin 返回的错误消息不正确
4996479	对于用户，带 “策略模式”的服务显示为 “可添加”
4961370	“**” 搜索掩码无法工作
4959895	实体描述符搜索过滤器无法正常工作
4959071	未清除闲置会话
4931907	用户以服务类型角色登录时服务消失
4931163	命名属性应为小写
4930610	仅有英文 am2bak 和 bak2am 版本消息
4922030	冲突解决级别不随语言环境的改变而相应变化
4916683	backup_restore.po 中 msgid-msgstr 对的消息未本地化
4853809	服务注册问题
4853809	“注册所有服务”并未注册全部可用服务

安装说明

目前，在使用 Java Enterprise System 安装程序安装第一个实例之后， `amconfig` 脚本支持使用 Application Server Enterprise Edition 8 2005Q1 (8.1) 作为 Web 容器，以部署 Access Manager 的其他实例 。

有关运行配置脚本的信息，请参阅 Access Manager 6 2005Q1 管理指南。

另请参阅已知问题和限制下的安装部分。

已知问题和限制

本节包含发行 Access Manager 2005Q1 时已知的重要问题的列表。本节包括以下主题：

安装

在安全服务器的 SDK 安装上使用 amadmin 登录会抛出异常 (#5107584)

在 Access Manager 2005Q1 中，如果安装了完整的安全 Access Manager，然后安装 SDK 以使用完整安装，可能会抛出异常。这是因为 `com.iplanet.am.admin.sli.cerdb.prefix` 属性的 Web Server 值有错误。

解决方法

1. 编辑 `AMConfig.properties`。
2. 将属性 `com.iplanet.am.admin.cli.certdb.prefix` 更改为 `https-<ws-instance-name>-<ws-hostname>-`。
3. 重新启动 Web 服务器。

包含 Web 容器的 AMSDK 安装中到 Linux 上共享组件的链接无效 (#6199933)

如果在 Linux 平台上为任何 Web 容器安装 Access Manager SDK，则多个共享组件的链接会断开。

解决方法

删除不正确的链接，创建正确的链接。

要删除链接，请输入以下命令：

```
cd ${AM_INSTALL_DIR}/identity/lib
rm -rf jaxrpc-spi.jar relaxngDatatype.jar xsdlib.jar
```

要创建新链接，请输入以下命令：

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

参考完整性插件变量的排印错误影响性能 (#5029256)

当 Access Manager 为 Directory Server 启用参考完整性插件时，在插件的变量 11 中，属性名称有排印错误。属性名称指定为 `iplanet-am-modifable-by`。这在删除组织时，会在目录错误日志中产生 `search not indexed` 警告。

参考完整性插件要求将其变量中的所有属性都编入索引，已编入索引的属性是 `iplanet-am-modifiable-by`。这可能会影响 Access Manager 的性能。

Application Server xercesImpl.jar 导致 JVM 崩溃 (#6223676)

加载了 Application Server 8.1 EE 的 `xercesImpl.jar`（对于 RedHat Linux 在 `/opt/sun/appserver/lib` 中；对于 Solaris 在 `/opt/SUNWappserver/appserver/lib` 中）之后，才加载共享组件版的 `xercesImpl.jar`（对于 RedHat Linux 在 `/opt/sun/share/lib` 中；对于 Solaris 在 `/usr/share/lib` 中）。

该 Application Server 版本在共享组件版本之前由类加载程序加载。此时，过期的 Application Server 版本无法应付数千个等待处理的 JSP。 JVM 将会挂起或崩溃。

解决方法

重命名 SPARC 和 x86 的 `xercesImpl.jar`（对于 Red Hat AS 2.1 或 3.0 在 `/opt/sun/appserver/lib` 中；对于 Solaris 9 或 10 在 `/opt/SUNWappserver/appserver/lib` 中）。JVM 类加载程序然后会被迫使用共享组件的 `xerceImpl.jar`（对于 Red Hat AS 2.1 或 3.0 在 `/opt/sun/share/lib` 中；对于 Solaris 9 和 10 在 `/usr/share/lib` 中）。

安装程序不允许用户在 AM SDK 安装期间输入协议 (#6180090)

如果安装 Access Manager SDK，“Access Manager: Web Container for running Sun Java System Access Manager Services”面板不会要求输入运行 Access Manager 服务的 Web 容器的协议。安装程序会假定 Web 容器使用 `http` 协议；但您可能需要指定 `https` 协议才能访问使用 Access Manager（已启用 SSL）安装的 SDK。

解决方法

在 `AMConfig.properties` 文件中，将与安装的 Access Manager 服务器关联的协议设置为 `https`。例如：

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

Access Manager 将 servlet.jar 加入服务器 CLASSPATH (#5016348)

Access Manager 将在服务器 CLASSPATH 中为其支持的 Web 容器放置 `servlet.jar`。此文件可能导致意外结果，因为每个 Web 容器都会在其实现中捆绑 `servlet.jar` 文件。

解决方法

从 CLASSPATH 中删除 `servlet.jar`。

Access Manager 范例

范例在使用 JDK 1.5 编译时会返回警告 (#5102149)

Access Manager 包括的范例如果使用 JDK 1.5 进行编译，将返回警告。

解决方法

避免这些警告的方法有：

- 在使用 JDK 1.5 时，在编译命令行中添加 `encoding="ISO-8859-1"`。

  或

- 使用 JDK 1.4 编译范例。

SAML xmlsig 范例中的删减导致编译失败 (#5090925)

SAML `xmlsig` 范例中有所删减，如果使用 JDK 1.5 编译，将导致编译失败。但如果使用 JDK 1.4.2 编译，则不会发生此问题。

解决方法

如果使用 JDK 1.5 进行编译，请按照以下步骤设置 LD_LIBRARY_PATH：

1. 在 `xmlsig` 目录中找到 SAML 范例的 Readme.html 或 Readme.txt 文件。
2. 在第 3 节 “在 Solaris 上设置 XMLSIG 范例的说明”的步骤 4 中，将 LD_LIBRARY_PATH 设置为 *web-server-install-directory*`/bin/https/lib`。
3. 添加 `/usr/lib/mps/secv1` 到 LD_LIBRARY_PATH 以获取 JSS 库及其依赖性。

验证

通过电子邮件的用户修改通知无法工作 (#6212964)

“管理服务”中通过电子邮件的用户修改通知机制当前无法工作。

SafeWord 连接没有关闭 (#5073718)

如果您登录 Access Manager，进入 SafeWord 挑战响应页面，但不输入密码，连接也不会超时。如果关闭浏览器，连接不会随 SafeWord 服务器的关闭而关闭。

LDAP 验证对 LDAP Directory Server 连接进行匿名绑定 (#5090018)

Access Manager 不传送 LDAP 连接绑定 DN 和密码到 Directory Server，在 LDAP Directory Server 中的匿名绑定被禁用时会影响到验证。

解决方法

为 Directory Server 启用匿名绑定。

持久 Cookie 模式属性不一致 (#5038544)

在“持久 Cookie 模式”下，标记中设置的用户 ID 属性不一致。因此，由用户 ID 属性决定的策略代理可能会失败。

解决方法

非 DN 值使用 `UserToken`， DN 值使用 `Principal`。

重新装入 “会话超时” 页面将验证用户的有效用户名和密码 (#4697120)

在登录页面中，如果用户等待页面超时，然后输入了有效的用户名和密码，则用户将看到 “会话超时” 页面。如果用户重新装入此页面而未重新输入用户名和密码，则将通过 Access Manager 验证用户。

必须为多个 SafeWord 服务器指定不同的目录 (#4756295)

配置多个使用各自 SafeWord 服务器的组织时，必须在其 SafeWord 验证服务模板中指定各自的 `.../serverVerification` 目录。如果您保留默认值，并且所有服务器均使用同一目录，则第一个要通过其 SafeWord 服务器进行验证的组织将成为唯一有效的组织。

命令行工具

/opt/SUNWam/bin 目录中的 ldapsearch 和 ldapmodify 实用程序无法正确工作 (#4954779)

/opt/SUNWam/bin 目录中的 ldapsearch 和 ldapmodify 实用程序返回致命错误。

解决方法

添加 *DirectoryServer-base*`/lib/` 路径到 LD_LIBRARY_PATH 环境变量中。

am2bak 和 bak2am 脚本对于 Linux 无效 (#5053866)

如果 Access Manager 在 Linux 系统上运行， `am2bak` 和 `bak2am` 恢复脚本无法工作。

解决方法

1. 纠正以下命令的路径：
   - `ECHO=/usr/bin/echo` 应为 `ECHO=/bin/echo`
   - `uid='/usr/xpg4/bin/id -un'` 应为 `uid='/usr/bin/id -un'`
   - `/usr/bin/tar` 应为 `/bin/tar`
   - `/usr/bin/rm` 应为 `/bin/rm`
   - `/usr/bin/grep` 应为 `/bin/grep`
   - `/usr/bin/ps` 应为 `/bin/ps`
   - `/usr/bin/ls` 应为 `/bin/ls`

2. 修改 check_for_invalid_chars() 函数。例如：

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

amadmin 返回的 “错误消息”不正确 (#5008960)

amadmin 的 import 选项对于所有相关错误错误地抛出相同的错误消息。

仅控制台安装的 amverifyarchive 具有 “未替换”标签 (#4993375)

如果执行 Access Manager 仅控制台安装， amverifyarchive 实用程序在脚本中将不会替换以下标签：JSSHOME、 JDK_HOME、 BASEDIR 和 PRODUCT_DIR。

配置

在 Linux 上成功配置后，无法启动 WebSphere Application Server 5.1 (#6204646)

如果在 Linux 上安装用于 WebSphere 的 Access Manager SDK 组件，然后用正确的 amsamplesilent 文件运行 amwas51config， WebSphere 将无法启动。

解决方法

在 LD_LIBRARY_PATH 中添加 /opt/sun/private/lib，如下所示：

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

在 server.xml 中，删除 -Djava.util.logging.config.class 选项前的 **“/:”**。

没有为 Web Server 正确设置 certdb 别名 (#6212532)

如果通过 Access Manager 为 Web Server 启用 SSL，然后运行 amadmin，将抛出“namingservice 不可用”的错误。而浏览器工作正常。

无论后端名为何，始终为 userRoot 创建索引 (#5002886)

index.ldif 对 userRoot 进行硬编码以便为属性创建索引。可以在任意后端数据库名上驻留的根后缀上安装 Access Manager。可以将 nsslapd-suffix=SUFFIX_NAME 用作过滤器，通过具有基础 cn=config 的 ldapsearch 命令获得后端名。

联合

联合管理联系人抛出异常 (#6213102)

如果创建新的提供者，然后为该提供者添加新的联系人，可能会收到以下错误：

```
The server encountered an internal error () that prevented it from fulfilling this request
```

无法远程记录 amFederation.access 日志 (#6197608)

配置远程记录日志后，所有日志都会正常写入远程 Access Manager 实例， amFederation.access 除外。没有写入该日志记录。

解决方法

使用 LogUtils 中的 AccessController.doPrivileged(AdminTokenAction.getInstance());。

fedCookie 状态未改变 (#6202574)

如果对 SP 和 IDP 的联合用户终止联合关系， fedCookie 状态仍显示 YES。它应该显示 NO。

个人配置文件容器无法进行查询/修改 (#6189808)

以下个人配置文件容器无法进行查询或修改操作：

```
LegalIdentity/Gender
EmploymentIdentity/AltO
```

如果属性值为空，会抛出 PP Modify 的异常 (#5047103)

如果在属性值为空时执行 PP Modify， Access Manager 抛出异常。例如，如果创建设置以测试 sis-ep 范例，然后发送 EP Modify 页面并在未输入任何属性值的情况下单击该按钮，则会错误地抛出异常。

策略生效要求重启服务器 (#5045036)

联合策略实现只有在重启服务器后才能生效。这对 Application Server 和 Web Server 都有效。只有在完成全新安装和第一次执行策略时才必须重启服务器。

Access Manager 控制台

无法在 DIT 中使用大量人员容器时创建用户 (#5079609)

如果创建大量人员容器 （一千以上），然后登录 Access Manager 控制台并创建新用户，则会因为找不到人员容器而无法创建用户。

这是因为 `UMCreateUserModelImpl.getPeopleContainers()` 因搜索时间限制错误而失败，即使 Directory Server 在到达限制时间之前找到大量人员容器也同样如此。

解决方法

在 Access Manager 控制台中启用 “显示人员容器”，进入特定的人员容器并在其中创建用户。

具有只读访问权限的顶层帮助台管理员角色可以创建新用户 (#5109348)

帮助台管理员角色当前默认设置为 “完全访问”。将其改为 “修改”会禁用浏览框中的 “新建”和 “删除”按钮，但仍然允许管理员修改用户条目属性。

解决方法

调出帮助台管理员属性页面，将视图改为可用操作。找到 “用户”行，将设置从 “完全访问”改为 “修改”。

选择附属提供者实体的附属提供者选项时抛出异常 (#6203563)

在联合管理模块中，于 “附属提供者实体”页面中选择 “查看” > “附属提供者”时会抛出异常。

解决方法

修改 JSP，使高度属性在 JATO 结束标记之外。在 `FSAffiliateProfile.jsp` 中，行 104 变为：

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

请注意， `/>` 在高度属性之前。

附属提供者显示选项出错 (#6194139)

当“附属提供者显示”选项在联合管理模块中是菜单中的唯一选项并且设置为默认值时， Access Manager 将返回一个错误页面。

无法为管理员角色的用户修改服务 (#6174652)

如果您是作为顶层管理员角色登录的，可以为用户添加新服务，但不能修改任何服务。

解决方法

编辑管理员角色的显示配置文件，为其提供必要的视图菜单和可用操作。

单击“返回”按钮时值未保留 (#4992972)

在多页面操作过程中，如创建组、角色或为策略添加条件时，在单击“返回”按钮后，上一页中的值无法恢复。

联合管理模块中的托管提供者存在刷新问题 (#4915894)

在联合管理模块中，如果您在托管提供者的“身份提供者”视图中修改并保存了任何属性，则您的更改将被保存，但不会在显示中自动刷新。

解决方法

通过选择另一个模块 （例如，服务配置）退出联合管理模块，然后再返回联合管理模块。这将刷新显示。

控制台不能刷新用户属性更改 (#4931455)

Access Manager 控制台的浏览框不能刷新，无法指明在数据框中所作的用户属性值的更改。手动刷新页面，以查看已更改的值。

Internet Explorer 出现端口问题 (#4864133)

由于与 Internet Explorer 不兼容，在运行 http 时不得将 80 用作 Access Manager 端口号，在运行 https 时不得将 443 用作 Access Manager 端口号。

日志服务

启用 Java 安全性时出现日志问题 (#4926520)

启用 Java 安全性时， `jdk_logging.jar` 可能无法运行。

解决方法

启用了 Java 安全性后，如果您使用的是 JDK 1.4 以前的版本，则请在 Java 安全性文件中包含以下权限：

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

策略

达到 nslookthrough 限制时匹配条目未返回 (#5013538)

未返回匹配条目至 Access Manager 控制台，尽管已达到 nslookthrough 中定义的管理限制。

解决方法

调节 nslookthroughlimit 参数以补足条目数。

未对别名令牌强制执行策略 (#4985823)

如果使用用户别名借助于 LDAP 或“成员资格”之外的授权模块来登录 Access Manager，然后尝试访问受保护的资源时，访问将被拒绝。

策略范例有问题 (#4923898)

位于策略范例中的 Readme.html 不包括导致范例无法运行的信息。

解决方法

要运行范例， LD_LIBRARY_PATH 环境变量必须包括到 NSPR、 NSS 和 JSS 共享库的属性。在 Solaris 系统上，设置 LD_LIBRARY_PATH 以包括 /usr/lib/mps/secv1，在 Linux 系统上则设置为包括 /opt/sun/private/lib。

Access Manager SDK

命名属性的顶层组织违反了属性唯一性 (#6204537)

命名属性的属性唯一性在顶层组织中不起作用。但是会正确的强制实施用户和组织的属性唯一性。

EventService 在无法获取持续搜索连接时陷入了紧密循环 (#6205443)

即使连接了一定数目的持续搜索， EventService (ES) 线程也会成功地添加侦听程序 （LDAP JDK 成功地添加侦听程序）。但是，当 ES 线程尝试取得响应时， LDAPResponse 会报告 （错误代码为 51）持续搜索连接不可用。接着 ES 会再次尝试重新创建侦听程序，这样就变成一个死循环。

关于在安装 Access Manager SDK 的服务器上利用 certutil 来使用 SSL 服务器的说明文档 (#5027614)

用户在尝试从仅 SDK 机器与具备 SSL 功能的 Access Manager 服务器通信时，遇到与安全相关的错误和异常。在此方案中， Access Manager SDK 未部署在 Web 容器上或部署在第三方 Web 容器上，例如， BEA WebLogic Server 或 IBM WebSphere Application Server。

解决方法

在仅 SDK 机器上安装证书数据库，并将 Access Manager 服务器的根 CA 证书安装至此数据库：

1. 以超级用户身份 (`root`) 登录到仅 SDK 机器。
2. 确认安装了所需的 Netscape Security Services (NSS) 软件包：
   - 在 Solaris 系统上：SUNWtlsu
   - 在 Linux 系统上：sun-nss RPM
3. 如果未安装该软件包，则安装。例如：

   在 Solaris 系统上：

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

   在 Linux 系统上：

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

4. 为该证书数据库的令牌密码创建密码文件。例如：

   在 Solaris 系统上：

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

   在 Linux 系统上：

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

   其中，*cert-database-password* 是令牌密码。

5. 检查 LD_LIBRARY_PATH 变量：

   在 Solaris 系统上，检查 LD_LIBRARY_PATH 以查看是否存在 /usr/lib、/usr/lib/mps/secv1 和 /usr/lib/mps 目录。如果不存在，则添加任何缺少的目录。

   在 Linux 系统上，检查 LD_LIBRARY_PATH 以查看是否存在 /opt/sun/private/lib 目录。如果不存在，则添加该目录。

6. 使用证书数据库工具 (certutil) 以创建证书和密钥数据库。有关 certutil 的信息，请参阅以下网站：

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

   例如：

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

   其中：

   certutil-home 是 certutil 的位置：

   - 在 Solaris 系统上：/usr/sfw/bin
   - 在 Linux 系统上：/opt/sun/private/bin

   cert-database-dir 是证书和密钥数据库的数据库目录。

   config-home 是 Access Manager 配置文件的位置：

   - 在 Solaris 系统上：/etc/opt/SUNWam/config
   - 在 Linux 系统上：/etc/opt/sun/identity/config

7. 在新建的证书数据库中，为在 Access Manager 服务器上安装的 SSL 证书添加根 CA 证书。例如：

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

8. 使用编辑器查看 AMConfig.properties 文件并确认以下值
   - 证书数据库目录：com.iplanet.am.admin.cli.certdb.dir
   - 前缀：com.iplanet.am.admin.cli.certdb.prefix
   - 密码文件：com.iplanet.am.admin.cli.certdb.passfile

     如果不存在，则按照需要编辑设置。例如，前缀设置应为空 （即，等于 “”）。

9. 如果对 AMConfig.properties 进行了更改，并且将 Access Manager SDK 部署至 Web 容器，则重新启动 Web 容器。

使用 DNSAlias 与 JCE 提供者进行 SSL 信号交换失败 (#5038876)

当使用 subjectaltname 中有效 DNSAlias 名称的证书时， SSL 与 JCE 提供者进行信号交换失败。

在过滤器的 Init() 中的 Identity 方法导致 Weblogic 崩溃 (#5016283)

当过滤器的 init() 方法中含有 Access Manager 相关代码时， WebLogic 服务器将无法启动。在 ServletFilter servlet 的 init 方法中调用 Access Manager API。

Access Manager 将 JSS 用作安全提供者，而 WebLogic 在缺省情况下使用 JCE。当调用 init 方法时，WebLogic 尝试使用 JCE 来验证其许可证，但是将初始化 JSS。

解决方法

将 AMConfig.properties 文件中的默认安全加密从 JSSEncryption 改为 JCEEncryption。

任何以 “{SSHA}” 符号开始的密码均不可用 (#4966191)

Access Manager 不支持在密码中使用散列的 {SSHA} 符号。

“组创建” 选项仅添加一个 memberURL 属性 (#4931958)

如果您使用多个 LDAP 过滤器选项 (-f) 创建了一个组，则不能正确创建只有一个 memberURL 属性的组。

调节

没有为 Solaris-x86 提供 amtune 和相关的文件 (#6213019)

在本发行版中，在 Solaris-x86 的相应目录中没有安装 amtune 脚本及其相关的文件。

解决方法

使用为 Sparc-Solaris 提供的 amtune 文件。

amtune-as8 脚本包含密码文件错误 (#6212380)

使用 amtune 脚本无法自动调节 Application Server 8 (amtune-as8)，因为使用 asadmin 密码创建了临时密码文件。目前在文件中只有密码。

解决方法

在 amtune-as8 中，使用以下语法输入字符串：

```
"TOKEN=Value"
```

例如：

```
"AS_ADMIN_PASSWORD=11111111"
```

输入此更改 amtune-env:

```
#ASADMIN=$CONTAINER_BASE_DIR/bin/asadmin
ASADMIN=/opt/SUNWappserver/appserver/bin/asadmin
```

单点登录

无法用不同的部署 URI 执行 SSO (#4770271)

如果两个不同 Access Manager 实例间的部署 URI 不同，则无法正常运行单点登录。

国际化 (i18n)

当组名为多字节时，不会列出组成员 (#6197041)

在 Access Manager 6 2005Q1 的国际化版本中，当组名为多字节时，不会在 Access Manager 控制台中列出组成员。

在 Linux 上的开始和停止消息不可读 (#6207421)

Access Manager 上 zh/zh_TW 字符集的开始和停止消息不可读。这种情况发生在 Linux 平台上。

在非英语语言环境上无法使用 HTTPBasic 和 WindowsDesktopSSO 登录 (#6209324)

在非英语语言环境中无法登录到 HTTPBasic 和 WindowsDesktopSSO 验证模块。

解决方法

在 XML 文件中将这些参数还原为英语：

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

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

当 Access manager 部署到 Application Server 中时，这些文件通常安装到以下目录：

```
/var/opt/sun/appserver/domains/domain1/applications/j2ee-modules/amserver/con
fig/auth/default_<lang>
```

当 Access manager 部署到 Web Server 中时，这些文件通常安装到以下目录：

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

日语在线帮助显示不正确 (#5024138)

如果您使用的是日语版的 Access Manager 并将语言更改为 en_US，则仍然会显示日语帮助上下文环境。

解决方法

创建符号链接，从 `docs_en` 到 `docs_en_US`。

客户机检测功能工作不正常 (#5028779)

在 “客户机检测”服务中，删除 UTF-8 无法正常工作。

解决方法

如果删除 UTF-8 字符集，请在更改完成后重新启动 Web 容器。

G11NSetting 无法处理 Q 因数中的空格 (#5008860)

当客户机数据在 `q` 因数内或周围含有空格时，G11NSettings 代码无法正确进行分析并返回以下错误：

```
ERROR:G11NSettings::Fetchcharset() Unable toparse  charset entry invalid Q  q
```

对于 ja 字符集，使用多字节角色参数登录 URL 时，登录页面失败 (#4905708)

如果您创建了多字节角色，然后尝试以已经注册为多字节角色的用户登录 URL，则登录页面将产生失败错误。

解决方法

为使验证框架对 URL 中指定的多字节角色值进行解码，您需要同时指定 gx_charset 和参数。例如：

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

日志文件在 Ja 语言环境下成为乱码 (#4882286)

以下日志文件含有日语字符，打开时成为乱码：

/var/opt/SUNWam/debug 目录中除 deploy.log 和 undeploy.log 之外的所有文件。

URL 中的语言环境参数显示混合语言的登录页面 (#4915137)

如果您现在将基于非英语的浏览器与用 Web Server 安装的 Access Manager 实例一起使用，并且登录到 http://*host*:*port*/amserver/UI/Login?locale=en，则登录页面将显示英语和非英语的混合字符。

解决方法

将以下符号链接

AccessManager-base/SUNWam/web-apps/services/config/auth/default

更改为

AccessManager-base/SUNWam/web-apps/services/config/auth/default_en

Application Server 为 ja 时，登录窗口中为混合语言环境 (#4932089)

当浏览器的语言设置为 en，而 Application Server 的语言环境设置为 ja 时，Access Manager 登录窗口在默认情况下将不会改回英文。

解决方法

运行语言环境设置为 en 的 Application Server。

锁定通知发送的电子邮件不可读 (#4938511)

如果运行 Access Manager 时 Web 容器的首选语言环境已设置为 C 之外的任一值，并且某个用户被服务器锁定，则会发送锁定通知电子邮件，但是它不可读。

解决方法

在 “发送锁定通知的电子邮件地址”属性中，设置 email|local|charset （而不仅仅是 email 参数）。例如：

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

多字节名称在自注册中不起作用 (#4732470)

如果用重复的用户 ID 和多字节名字和姓氏在自注册 （成员资格验证服务）模块下创建用户，将会出错。多字节用户 ID 不受支持。

解决方法

如果用户在多字节环境下使用 “自注册”登录，管理员必须确保 “核心验证”中的 “用户生成器模式”属性未被选中。

或

用户可以在 “自注册”登录页面上选择 “创建个人”选项。

日文版 Access Manager 不能与 Netscape 6.22 和 6.23 一起运行 (#4902421)

在日文版 Access Manager 中，您不能用 Netscape 6.22 或 6.23 登录控制台。

时间条件格式未更改 (#4888416)

在为策略定义的时间条件中，不管采用何种语言环境，以下时间显示格式都不会更改：

```
Hour:Minute AM/PM
```

客户机检测屏幕未本地化 (#4922013)

在本发行版中，“客户机检测”界面的 “当前式样属性”屏幕的某些部分未本地化。

已更新的 genericHTML 客户机属性未被应用 (#4922348)

如果您从客户机检测服务的 genericHTML 客户机属性中的字符集列表中删除了 UTF-8，然后保存此更改，启动 “客户机检测”，注销再重新登录，则登录页面仍然使用 UTF-8 字符集。

解决方法

用 amserver 重新手动启动服务器。

日志文件标题未本地化 (#4923536)

所有日志文件的前两行均未本地化，特别是 `Version` 和 `Field` 部分及其字段列表。

amSSO.access 中的数据字段值未本地化 (#4923549)

在 `amSSO.access` 日志文件中， `Data` 字段下的所有值均未本地化。

Exception.jsp 有硬编码的消息 (#4772313)

`Exception.jsp` 未本地化，它包含硬编码的标题、错误消息和版权信息。仅在极端的情况下调用该异常错误 jsp 页。例如，在 Directory Server 关闭时，或在不能调用 Access Manager 服务并且该 jsp 页无可用本地化版本时。

Cookie

Cookieless 模式无效 (#4967866)

如果支持 cookie 的浏览器访问 Access Manager 并且关闭了 cookie 支持，则浏览器将继续发送更旧的 Access Manager cookie。此问题会导致对 Access Manager 资源的访问被拒绝。

解决方法

选择以下一个解决方法：

- 清除浏览器 cookie 高速缓存以删除所有的 Access Manager cookie。
- 禁用浏览器中的 cookie。

Cookie 夺取

当应用程序使用不可信的会话 cookie 时，安全性可能会降低。

Access Manager 部署启用单点登录 (SSO) 或跨域单点登录 (CDSSO) 时，在用户浏览器上将设置 `http(s)` 会话 cookie。会跨多个应用程序来验证这些 cookie。当 Access Manager 跨多个 DNS 域部署时， Liberty 协议将 `http(s)` 会话 cookie 从已验证的 DNS 域传送到 Web 应用程序目标域。

虽然用户可以自动登录网络资源，但是当应用程序使用不可信的会话 cookie 时存在固有安全隐患。当身份提供者将用户的验证、授权及配置文件信息提供给由第三方或公司未授权组织所开发的应用程序（或服务提供者）时，安全隐患就可能呈现出来。可能的安全问题包括：

- 所有应用程序共享同一个 `http` 会话 cookie。这可能导致某欺骗应用程序夺取会话 cookie，然后在另一应用程序中冒充用户。
- 如果应用程序不使用 `https` 协议，则会话 cookie 可能遭受网络窃听。
- 只要有一个应用程序可被夺取，整个基础结构的安全性就会大打折扣。
- 欺骗应用程序可使用会话 cookie 来获取用户的配置文件属性并可能进行修改。如果该用户拥有管理权限，则应用程序将能够造成更多损害。

解决方法

请按照以下步骤进行操作：

1. 使用 Access Manager 管理控制台为每个代理设置一个条目。
   a. 在包含要创建的代理的组织内，从“视图”菜单中选择“代理”，然后单击“新建”。
   b. 提供以下信息：

      名称。输入代理的名称或身份。示例：`agent123`

      密码。输入代理的密码。示例：`agent123`

      确认密码。确认该密码。

      说明。输入代理的简短说明。例如，可以输入代理实例名称或其保护的应用程序的名称。

      代理关键字值。使用关键字/值对设置代理属性。 Access Manager 使用此属性接收有关用户的证书声明的代理请求。

      为 `agentRootURL` 输入属性值，该值要与带端口号的代理 URL 的值相同。注意：`agentRootURL` 的值区分大小写。

      示例：`agentRootURL=http://`*`server_name:99`*`/`

      设备状态。输入代理的设备状态。如果设置为“活动”，则代理可以通过 Access Manager 进行验证并与其进行通信。如果设置为“不活动”，则代理不能通过 Access Manager 进行验证。

c. 单击“确定”。

2. 对在步骤 1b 输入的密码执行以下命令。

AccessManager-base/SUNWam/agents/bin/crypt_util agent123

此时输出以下信息：

```
WnmKUCg/y3l404ivWY6HPQ==
```

3. 更改 AMAgent.properties 以反映新值，然后重新启动该代理。示例：

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


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


# Cross-Domain Single Sign On URL
# Is CDSSO enabled.
com.sun.am.policy.agents.cdsso-enabled=true


# This is the URL the user will be redirected to after successful login
# in a CDSSO Scenario.
com.sun.am.policy.agents.cdcservletURL =
http://server.example.com:port/amserver/cdcservlet
```

4. 更改 AMConfig.properties 以反映新值，然后重新启动 Access Manager。示例：

```
com.sun.identity.enableUniqueSSOTokenCookie=true
com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer


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

5. 在 Access Manager 管理控制台中选择 “服务配置” > “平台”。

6. 在 Cookie 域列表中更改 cookie 域名：

   a. 选择缺省 iplanet.com 域，然后单击 “删除”。

   b. 输入 Access Manager 安装的主机名，然后单击 “添加”。

   示例：server.example.com

   应该会在浏览器上看见两个 cookie 集：

Cookie	主机名
iPlanetDirectoryPro	server.example.com
sunIdentityServerAuthNServer	example.com

可再分发的文件

Sun Java System Access Manager 2005Q1 不含任何可以再分发到产品非许可用户的文件。

如何报告问题和提供反馈

如果您的 Sun Java System Access Manager 有问题，请使用以下机制之一与 Sun 客户支持人员联系：

- 要获得 Sun 软件支持联机服务，请访问以下站点：
  http://www.sun.com/supportraining

  此站点上有一些链接，通过这些链接可以访问知识库、在线支持中心、 ProductTracker，还可了解维护方案以及用于联系支持部门的电话号码。

- 随维护合同一起分发的电话号码

为使我们能够更好地帮助您解决问题，请在联系支持人员时准备好以下信息：

- 问题描述，包括问题出现时的情况及其对您的操作的影响
- 计算机类型、操作系统版本和产品版本，包括可能影响问题的所有修补程序和其他软件
- 您用于重现问题的方法的详细步骤
- 所有错误日志或核心转储

Sun 欢迎您提出意见

Sun 致力于提高其文档的质量，并十分乐意收到您的意见和建议。请使用网上表格将反馈意见提供给 Sun：

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

请在相应的字段内填写完整的文档标题和文件号码。您可以在本书的标题页面和文档顶部找到文件号码，文件号码通常包含七个或九个数字。例如，本发行说明的文件号码是 819-1948。提出意见时您还需要在表格中输入文件的英文文件号码和标题。本文件的英文文件号码是 817-7642，文件标题为《Sun Java Enterprise System Access Manager 6 2005Q1 Release Notes》。

其他 Sun 资源

您可以从以下 Internet 位置找到有用的 Sun Java System 信息：

- Sun Java System 文档
  http://docs.sun.com/prod/entsys.05q1 及
  http://docs.sun.com/prod/entsys.05q1?l=zh
- Sun Java System 专业服务
  http://www.sun.com/service/products/software/javaenterprisesystem/
- Sun Java System 软件产品和服务
  http://wwws.sun.com/software/
- Sun Java System 软件支持服务
  http://www.sun.com/supportraining
- Sun Java System 支持和知识库
  http://sunsolve.sun.com
- Sun Java System 咨询和专业服务
  http://www.sun.com/service/products/software/javaenterprisesystem

- Sun Java System 开发者信息
  http://developers.sun.com/
- Sun 开发者支持服务
  http://www.sun.com/developers/support