Sun Java™ System Access Manager 适用于 Microsoft Windows 的发行说明

版本 7

文件号码 819-5803

本发行说明包含适用于 Windows 的 Sun Java System Access Manager 7 2005Q4（以前称为 Sun Java System Identity Server）发行时可用的重要信息。这里介绍了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/app/docs/prod/entsys.05q4 及
http://docs.sun.com/app/docs/prod/entsys.05q4?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：

- 发行说明修订历史记录
- 关于 Access Manager 7
- 此发行版中修复的错误
- 重要信息
- 已知问题和限制
- 可再分发的文件
- 如何报告问题和提供反馈
- 其他 Sun 资源

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
2006 年 2 月	正式版
2005 年 11 月	Beta 版

关于 Access Manager 7

Sun Java System Access Manager (Access Manager) 是 Sun 身份管理基础结构的一个组成部分，它允许组织在企业内部和企业对企业 (B2B) 价值链间对 Web 应用程序和其他资源的安全访问进行管理。 Access Manager 具有以下主要功能：

- 采用基于角色和基于规则的访问控制，提供集中验证及授权服务
- 以单点登录 (SSO) 方式访问组织基于 Web 的应用程序
- 通过 Liberty Alliance Project 和安全声明标记语言 (SAML) 支持联合身份
- 记录 Access Manager 组件中管理员和用户的活动等关键信息，用于之后的分析、报告和核查

本节包括：

- Access Manager 7 的新增功能
- 硬件和软件要求
- 支持的浏览器

Access Manager 7 的新增功能

此发行版本包含以下新增功能：

- Access Manager 模式
- 新的 Access Manager 控制台
- 身份库
- Access Manager 信息树
- 会话故障转移更改
- 会话属性更改通知
- 会话配额限制
- 分布式验证
- 支持多重验证模块实例
- 验证 “命名的配置”或 “链接”名称空间
- 策略模块增强功能
- 站点配置
- 批量联合
- 日志记录增强功能

Access Manager 模式

Access Manager 7 2005Q4 包含 “领域”模式和 “传统”模式。两种模式均支持：

- 新的 Access Manager 7 2005Q4 功能
- Access Manager 6 2005Q1 功能，但有以下限制：
  - 创建领域时，不会在 Sun Java System Directory Server 中创建相应的组织。
  - 新的 Access Manager 7 2005Q4 控制台无法设置 “服务级别”(Class of Service, CoS) 模板优先级。参见第 28 页的 “新的 Access Manager 访问控制台无法设置 CoS 模板优先级 (6309262)”。
- Sun Java System Directory Server 和其他数据存储库中的身份库

以下情形必须使用传统模式：

- Sun Java System Portal Server
- Sun Java System Communications Services 服务器，包括 Messaging Server、Calendar Server、Instant Messaging 或 Delegated Administrator

- Access Manager 6 2005Q1 和 Access Manager 7 2005Q4 访问同一 Directory Server 时部署共存的情况下

新的 Access Manager 控制台

此版本中的 Access Manager 控制台已经过重新设计。但是，如果 Access Manager 与 Portal Server、Messaging Server、Calendar Server、Instant Messaging 或 Delegated Administrator 共同部署，则必须在 “传统”模式下安装 Access Manager，并使用 Access Manager 6 2005Q1 控制台：

有关详细信息，参见第 10 页的 “兼容性问题”。

身份库

Access Manager 身份库包含与身份（如用户、组和角色）相关的信息。可以使用 Access Manager 或其他置备产品 （如 Sun Java System Identity Manager）创建和维护身份库。

在目前的发行版本中，身份库可驻留在 Sun Java System Directory Server 或 Microsoft Active Directory 中。 Access Manager 可以对身份库进行读/写操作或只读操作。

Access Manager 信息树

Access Manager 信息树包含与系统访问相关的信息。每个 Access Manager 实例均可在 Sun Java System Directory Server 中创建和维护各自的信息树。 Access Manager 信息树可拥有任意名称 （后缀）。 Access Manager 信息树包含领域 （和子领域，如果需要的话），如下节所述。

Access Manager 领域

领域及任意子领域均为 Access Manager 信息树的组成部分，它们可以包含定义用户集和/或组集的配置信息、用户验证方式、用户可访问资源的范围以及授予用户访问资源权限后应用程序可用的信息。领域或子领域也可以包含其他配置信息，其中包括全局化配置、密码重置配置、会话配置、控制台配置和用户首选项。领域或子领域也可以为空。

可以使用 Access Manager 控制台或 amadmin CLI 实用程序创建领域。有关详细信息，参阅控制台联机帮助或者 《Sun Java System Access Manager 7 2005Q4 管理指南》中的第 14 章 “amadmin 命令行工具”。

会话故障转移更改

通过将 Sun Java System Message Queue (Message Queue) 用作通信代理， Sleepycat Software, Inc. 的 Berkeley DB 用作会话存储数据库， Access Manager 可提供独立于 Web 容器的会话故障转移实现。 Access Manager 7 2005Q4 的增强功能包含用于配置会话故障转移环境的 `amsfoconfig.bat`。

有关详细信息，参见《Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide》中的 "Implementing Access Manager Session Failover"。

会话属性更改通知

会话属性更改通知功能允许 Access Manager 在特定会话属性发生改变时，向特定侦听程序发送通知。若在 Access Manager 管理控制台中启用了 “启用属性更改通知”属性，则此功能生效。例如，在单点登录 (SSO) 环境下，多个应用程序可共享一个 Access Manager 会话。当某个特定的，已在 “通知属性”列表定义的会话属性发生改变时， Access Manager 会向所有已注册的侦听程序发送通知。

有关详细信息，参见《Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide》中的 "Enabling Session Property Change Notifications"。

会话配额限制

会话配额限制功能允许 Access Manager 管理员 (`amadmin`) 设置 “活动用户会话”属性，以限制用户拥有的最大并发会话数。管理员可以在全局级别上为所有用户，或为仅应用于一个或多个特定用户的实体 （如组织、领域、角色或用户）设置会话配额限制。

默认情况下，会话配额限制为禁用（关闭），但管理员可通过在 Access Manager 管理员控制台中设置“启用配额限制”属性来启用会话配额限制。

如果用户用尽了会话限制配额，管理员也可通过设置“会话配额用尽时的操作”属性来配置系统要执行的操作：

- DENY_ACCESS。 Access Manager 将拒绝新会话的登录请求。
- DESTROY_OLD_SESSION。 Access Manager 将损坏下一个即将过期的会话。

“免除顶层管理员的限制检查”属性指定了是否将会话限制配额应用于拥有 “顶层管理员角色”的管理员。

有关详细信息，参见《Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide》中的 "Setting Session Quota Constraints"。

分布式验证

分布式验证服务允许在隔离区 (DMZ) 交互式收集用户身份与证书。向 Access Manager 验证期间，用户必须提供用户标识和证书。在此过程中，Access Manager 服务 URL 将对用户公开。使用代理服务器可防止此 URL 公开；但某些部署不支持代理服务器解决方案。

由于大多数安全的部署不允许代理 （来自 DMZ 层）直接将请求重定向至 Access Manager 服务器（位于安全区内，防火墙后），因此这是 “分布式验证”服务的基本要求。

在任何与 servlet 兼容的 Web 容器上，此功能将作为 J2EE Web 应用程序来提供和部署。“验证服务”拥有远程验证表示和提取框架 （即分布式验证 UI），可部署为 DMZ 层 （在未运行 Access Manager 的机器上）中的 J2EE Web 应用程序，然后在执行实际验证时与后端服务器通信。执行实际验证时，“分布式验证”服务可通过远程 API 与验证服务器 （远程）通信。

支持多重验证模块实例

已扩展所有验证模块 （默认配置），以支持具有控制台 UI 支持的子模式。可为每个模块类型 （已加载的模块类）创建多重验证模块实例。例如，对于 LDAP 模块类型名为 ldap1 和 ldap2 的实例而言，每个实例均可指向不同的 LDAP 目录服务器。支持名称与类型相同的模块实例向后兼容。调用方式为 *server_deploy*_uri/UI/Login?module=*module-instance-name*。

验证 “命名的配置”或 “链接”名称空间

单独的名称空间创建在组织/领域下，是验证模块实例的链接。可重复使用同一链接并将其指定给组织/领域、角色或用户。“验证服务”实例等同于 “验证链”。调用方式为 *server_deploy*_uri/UI/Login?service=*authentication-chain-name*。

策略模块增强功能

个性化属性

除规则、主题和条件外，现在策略也可拥有个性化属性 (IDResponseProvider)。现在，策略评估发送至客户机的策略决定在适用的策略中包含基于策略的响应个性化属性。支持两种类型的个性化属性：

- 静态属性。在策略中定义属性名称和值。

- 动态属性。在策略中列出属性名称，值则是在评估策略时从 “身份库”数据存储库内获取。

“策略强制点”（代理）通常将这些属性值作为 “HTTP 标头”、 "Cookie" 或 “请求属性”转发给受保护的应用程序。

Access Manager 7 2005Q4 不支持客户自定义 “响应提供者”界面的实现。

会话属性条件

会话策略条件实现 (SessionPropertyCondition) 会基于用户的 Access Manager 会话中设定的属性值，决定策略是否适用于某个请求。策略评估期间，仅当用户 Access Manager 会话的属性值均在条件中有定义时，条件才会返回 "true"。对于在条件中定义了多个值的属性，用户会话只要具有条件中列出的一个属性值便已足够。

策略主题

策略主题实现 （Access Manager 身份主题）允许将已配置身份库中的条目用作策略主题值。

策略导出

可使用 amadmin 命令，以 XML 格式导出策略。 `amAdmin.dtd` 文件中的新元素 `GetPolices` 和 `RealmGetPolicies` 支持此功能。

策略状态

策略现在拥有一个状态属性，可将其设置为活动或不活动。策略评估期间将忽略非活动的策略。

站点配置

Access Manager 7 2005Q4 引入了 “站点概念”，可为 Access Manager 部署提供集中式配置管理。当 Access Manager 配置为站点时，将始终通过负载平衡器传送客户机请求，这样可以简化部署，还可解决客户机与后端 Access Manager 服务器之间被防火墙阻隔之类的问题。

有关详细信息，参见《Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide》中的 "Configuring an Access Manager Deployment as a Site"。

批量联合

Access Manager 7 2005Q4 可以批量联合外包给业务伙伴的应用程序的用户帐户。之前，在“服务提供者”(SP) 与“身份提供者”(IDP) 之间联合帐户需要每个用户访问 SP 站点和 IDP 站点，创建帐户（如果尚未创建），然后再通过 Web 链接联合两个帐户。此过程非常耗时。并且对于使用现有帐户的部署、其自身作为身份提供者的站点或使用其合作伙伴之一作为验证提供者的站点，这种方法往往不适用。

有关详细信息，参见《Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide》。

日志记录增强功能

Access Manager 7 2005Q4 包含以下新的日志记录增强功能：

- 新的字段（或列）：`MessageID` 字段包含已记录事件的消息标识符。ContextID 字段包含上下文标识符，这与会话标识符类似，并且适用于特定用户登录会话的所有事件。对于用户的特定登录会话， ContextID 在所有已记录事件的日志文件中均相同。
- 日志记录 API。 API 包括读取日志记录的附加功能；如果配置了数据库日志记录，还会读取来自数据库 (DB) 的日志记录。参阅 `<install-dir>\samples\logging` 目录下的 `LogReaderSample.java` 文件，该文件显示了从平面文件或 DB 表格库检索日志记录的相关信息。

注意 数据库表格往往比平面文件日志大。因此，请勿在给定请求中检索数据库表格中的所有记录，因为过大的数据量会耗尽 Access Manager 服务器的全部资源。

硬件和软件要求

此发行版的 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	Microsoft Windows 2000 Advanced Server, Service Pack 4
	Microsoft Windows 2000 Professional
	Microsoft Windows 2003 Enterprise Server
RAM	512 MB

表 2 硬件和软件要求 （续）

组件	要求
磁盘空间	250 MB

支持的浏览器

此 Access Manager 发行版支持以下浏览器：

表 3 支持的浏览器

浏览器	平台
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000
Microsoft Internet Explorer 6.0	Windows 2000、 Windows XP
Mozilla 1.7.1	Solaris OS，版本 9 和 10 Java Desktop System Windows 2000 Red Hat™ Linux 8.0
Netscape™ 7.0	Solaris OS，版本 9 和 10 Java Desktop System Windows 2000 Red Hat Linux 8.0

此发行版中修复的错误

无。

重要信息

本节包括一些在核心产品文档中未提供的最新信息。本节包括以下主题：

- 兼容性问题
- 安装说明
- 为残疾人士提供的辅助功能

兼容性问题

- Access Manager 传统模式
- 确定 Access Manager 模式
- Access Manager 策略代理

Access Manager 传统模式

可以在两种模式下配置 Access Manager 7 2005Q4：

- 增强 (7.x) 类型或领域模式
- 兼容 (6.x) 类型或传统模式

如果与 Portal Server、Messaging Server、Calendar Server、Instant Messaging 或 Delegated Administrator 一起安装 Access Manager，则必须按以下说明选择 Access Manager 兼容 (6.x) 类型：

有关详细信息，参见 Access Manager 安装类型。

安装期间自动进行配置

选中此选项后，安装程序将在传统模式下配置 Access Manager。

安装后手动进行配置

如果使用 “安装后手动进行配置”选项运行 Java ES 安装程序，您必须在安装后运行 `amconfig bat` 配置 Access Manager。

若要选择兼容 (6.x) 安装类型，在配置脚本输入文件 (`AMConfigurator.Properties`) 中设置以下参数：

```
AM_REALM=disabled
```

CONSOLE_DEPLOY_URI=/amconsole

要选择增强模式：

AM_REALM=enabled

CONSOLE_Deploy_URI=/amserver/console

有关运行 amconfig.bat 配置 Access Manager 的详细信息，参阅 Sun Java System Access Manager 管理指南 (http://docs.sun.com/doc/819-1940)。

确定 Access Manager 模式

要确定正在运行的 Access Manager 7 2005Q4 安装是在领域模式下配置的还是在传统模式下配置的，可调用：

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

结果为：

- true：“领域”模式
- false：“传统”模式

Access Manager 策略代理

下表显示 “策略代理”与 Access Manager 7 2005Q4 模式的兼容性。

表 4 策略代理与 Access Manager 7 2005Q4 模式的兼容性

代理与版本	兼容模式
Web 和 J2EE 代理，版本 2.2	传统模式和领域模式
Web 代理，版本 2.1	传统模式和领域模式
J2EE 代理，版本 2.1	仅传统模式

安装说明

Access Manager 安装说明包含以下信息。

Access Manager 安装类型

运行 Java ES 安装程序时，可以使用 “安装期间自动进行配置”或 “安装后手动进行配置”安装 Access Manager 7 2005Q4。

- 在“安装期间自动进行配置”模式中，Java ES 安装程序会在传统模式下配置 Access Manager。兼容 (6.x) 类型 （或传统模式）支持 Access Manager 6 功能，其中包括 Access Manager 6 兼容的控制台和目录信息树 (DIT)。

  兼容 (6.x) 类型的默认 “控制台部署 URI”是 `amconsole`。

- 在“安装后手动进行配置”模式下，可以在传统模式或增强模式下配置 Access Manager。增强 (7.x) 类型 （或领域模式）支持 Access Manager 7 功能，其中包括新的 Access Manager 7 控制台。

  要在增强模式下配置 Access Manager，参见第 10 页的 “安装后手动进行配置”。

  服务器和远程控制台安装的增强 (7.x) 类型的默认“控制台部署 URI”是 `amserver/console`。

如果以无提示模式或 Access Manager amconfig.bat 运行 Java ES 安装程序，在状态文件或配置脚本输入文件 `AMConfig.Properties` 中设置以下变量：

对于增强 (7.x) 模式：

```
AM_REALM=enabled
CONSOLE_DEPLOY_URI=/amserver/console
```

对于兼容 (6.x) 模式：

```
AM_REALM=disabled
CONSOLE_DEPLOY_URI=/amconsole
```

Access Manager 升级说明

如果您要从较早发行版升级到 Access Manager 7 2005Q4，请遵照 《Sun Java Enterprise System 2005Q4 Upgrade Guide for Microsoft Windows》（http://docs.sun.com/app/docs/doc/819-4461）中的升级说明进行操作。

为残疾人士提供的辅助功能

欲获得自本介质发行以来所发布的辅助功能，请联系 Sun 索取有关 "Section 508" 法规符合性的产品评估文档，以便确定哪些版本最适合部署辅助功能解决方案。可通过以下网址获取应用程序的更新版本：http://sun.com/software/javaenterprisesystem/get.html。

有关 Sun 在辅助功能方面所做出的努力，请访问 http://sun.com/access。

已知问题和限制

本节描述了发行时的已知问题及其解决方法 （如果可用）。

- 第 13 页的 “兼容性问题”
- 第 15 页的 “安装问题”
- 第 16 页的 “配置问题”
- 第 19 页的 “Access Manager 控制台问题”
- 第 21 页的 “SDK 和客户机问题”
- 第 23 页的 “命令行实用程序问题”
- 第 23 页的 “验证问题”
- 第 24 页的 “会话与 SSO 问题”
- 第 25 页的 “策略问题”
- 第 26 页的 “服务器启动问题”
- 第 26 页的 “联合与 SAML 问题”
- 第 27 页的 “全球化 (g11n) 问题”
- 第 29 页的 “文档问题”

兼容性问题

- 第 14 页的 “Java ES 2004Q2 服务器与 Java ES 2005Q4 上的 IM 不兼容 (6309082)”
- 第 14 页的 “传统模式与核心验证模块存在不兼容性 (6305840)”
- 第 14 页的 “代理无法登录，因为 “组织中没有配置文件”(6295074)”
- 第 14 页的 “Delegated Administrator `commadmin` 实用程序不创建用户 (6294603)”
- 第 15 页的 “Delegated Administrator commadmin 实用程序不创建组织 (6292104)”

Java ES 2004Q2 服务器与 Java ES 2005Q4 上的 IM 不兼容 (6309082)

以下部署方案导致了这一问题：

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

在服务器 4 上运行 imconfig 实用程序配置 Instant Messaging 时，配置不成功。服务器 4 上的 Instant Messaging (IM) 所使用的 Access Manager 7 2005Q4 SDK 与 Java ES 2004Q2 发行版不兼容。

解决方法

理想情况下， Access Manager 服务器和 Access Manager SDK 应为同一版本。有关详细信息，参见《Sun Java Enterprise System 2005Q4 升级指南》。

传统模式与核心验证模块存在不兼容性 (6305840)

Access Manager 7 2005Q4 传统模式与 Access Manager 6 2005Q1 的核心验证模块存在以下不兼容性：

- 传统模式中已删除 “组织验证模块”。
- 已更改“管理员验证配置”和“组织验证配置”的表示。在 Access Manager 7 2005Q4 控制台中，下拉列表中默认选定了 ldapService。在 Access Manager 6 2005Q1 控制台中提供了“编辑”按钮，并且默认情况下不会选定 LDAP 模块。

解决方法

无。

代理无法登录，因为 “组织中没有配置文件”(6295074)

在 Access Manager 控制台中，在领域模式下创建一个代理。如果注销后再使用该代理名称登录，则 Access Manager 将返回一个错误，因为该代理不具有访问领域的权限。

解决方法

修改权限以允许代理的读/写访问。

Delegated Administrator `commadmin` 实用程序不创建用户 (6294603)

带有 `-S mail,cal` 选项的 Delegated Administrator `commadmin` 实用程序在默认域内不会创建用户。

解决方法

如果只将 Access Manager 升级至版本 7 2005Q4，而未升级 Delegated Administrator，则会出现此问题。有关升级 Delegated Administrator 的详细信息，参见 《Sun Java Enterprise System 2005Q4 升级指南》。

如果不准备升级 Delegated Administrator，则按以下步骤操作：

1. 在 `UserCalendarService.xml` 文件中，将 `mail`、`icssubcribed` 和 `icsfirstday` 属性标记为可选的而非必需的。默认情况下，该文件位于 `<install-dir>\DelegatedAdmin\lib\services` 目录下。
2. 在 Access Manager 中，运行 amadmin 命令以删除现有 XML 文件，如下所示：

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

3. 在 Access Manager 中，添加更新的 XML 文件，如下所示：

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

   <install-dir>\DelegatedAdmin\lib\services\UserCalendarService.xml
   ```

4. 重新启动 Access Manager Web 容器。

Delegated Administrator commadmin 实用程序不创建组织 (6292104)

带有 `-S mail,cal` 选项的 Delegated Administrator `commadmin` 实用程序不创建组织。

解决方法

参见上一问题的解决方法。

安装问题

- 第 16 页的 “使用容器配置安装 SDK 时，通知 URL 不正确 (6327845)”
- 第 16 页的 “Access Manager classpath 引用了过期的 JCE 1.2.1 软件包 (6297949)”
- 第 16 页的 “非超级用户的日志和调试目录权限不正确 (6257161)”

使用容器配置安装 SDK 时，通知 URL 不正确 (6327845)

如果使用容器配置 (DEPLOY_LEVEL=4) 来执行 SDK 安装，则通知 URL 不正确。

解决方法

1. 在 AMConfig.properties 文件中设置以下属性：

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

2. 重新启动 Access Manager 以使新值生效。

Access Manager classpath 引用了过期的 JCE 1.2.1 软件包 (6297949)

Access Manager classpath 引用了已在 2005 年 7 月 27 日过期的 Java 加密扩展 (Java Cryptography Extension, JCE) 1.2.1 软件包 （签发证书）。

解决方法

无。虽然在 `classpath` 中存在该软件包引用条目，但 Access Manager 并不使用该软件包。

非超级用户的日志和调试目录权限不正确 (6257161)

在无提示安装配置文件中指定非超级用户时，对调试、日志以及启动目录的权限设置不正确。

解决方法

更改这些目录的权限以允许非超级用户进行访问。

配置问题

- 第 17 页的“使用非默认的 URI 时，必须编辑 Application Server 8.1 的 `server.policy` 文件 (6309759)”
- 第 18 页的 “平台服务器列表和 FQDN 别名属性没有更新 (6309259, 6308649)”
- 第 18 页的 “服务中的必需属性要求验证数据 (6308653)”
- 第 18 页的 “`amconfig.bat` 不更新领域/DNS 别名和平台服务器列表条目 (6284161)”

- 第 18 页的 “在配置状态文件模板中，默认的 Access Manager 模式为领域 (6280844)”

使用非默认的 URI 时，必须编辑 Application Server 8.1 的 server.policy 文件 (6309759)

如果在 Application Server 8.1 上部署 Access Manager 7 2005Q4，并且使用了服务、控制台和密码 Web 应用程序的非默认 URI（其默认 URI 值分别为 amserver、amconsole 和 ampassword），则在尝试通过 Web 浏览器访问 Access Manager 前，必须编辑应用服务器域的 server.policy 文件。

解决方法

按如下操作编译 server.policy 文件：

1. 停止部署 Access Manager 的 Application Server 实例。
2. 更改为 /config 目录。例如：

   ```
   <install-dir>ApplicationServer\domains\domain1\config
   ```

3. 制作 server.policy 文件的备份。例如：

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

4. 在 server.policy 文件中，查找以下策略：

   ```
   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. 在以下行中，将 amserver 替换为服务 Web 应用程序所使用的非默认 URI：

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

6. 对于传统模式安装，则将以下行中的 amconsole 替换为控制台 Web 应用程序所使用的非默认 URI：

   ```
   grant codeBase "file:\${com.sun.aas.instanceRoot}/
   ```

```
applications/j2ee-modules/amconsole/-" {
```

7. 将以下行中的 ampassword 替换为密码 Web 应用程序所使用的非默认 URI：

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

8. 启动部署 Access Manager 的 Application Server 实例。

平台服务器列表和 FQDN 别名属性没有更新 (6309259, 6308649)

在多服务器部署中，如果将 Access Manager 安装在第二台服务器 （及其后的服务器）上，则不会更新平台服务器列表和 FQDN 别名属性。

解决方法

手动添加领域/DNS 别名和平台服务器列表条目。有关详细步骤，参见 《Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide》中的 "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases"。

服务中的必需属性要求验证数据 (6308653)

Access Manager 7 2005Q4 强制服务 XML 文件中的必需属性使用默认值。

解决方法

如果服务的必需属性没有值，则为该属性添加值，然后重新装入服务。

`amconfig.bat` 不更新领域/DNS 别名和平台服务器列表条目 (6284161)

在多服务器部署中， amconfig 脚本不更新附加 Access Manager 实例的领域/DNS 别名和平台服务器列表条目。

解决方法

手动添加领域/DNS 别名和平台服务器列表条目。有关详细步骤，参见 《Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide》中的 "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases"。

在配置状态文件模板中，默认的 Access Manager 模式为领域 (6280844)

默认情况下，配置状态文件模板中的 Access Manager 模式 （AM_REALM 变量）处于启用状态。

解决方法

要在传统模式下安装或配置 Access Manager，重置状态文件中的以下变量：

```
AM_REALM = disabled
```

Access Manager 控制台问题

- 第 19 页的 “对于 SAML，在控制台中复制 “可信赖的伙伴”时出现错误 (6326634)”
- 第 19 页的 “amConsole.access 和 amPasswordReset.access 无法使用远程日志记录 (6311786)”
- 第 20 页的 “在控制台中添加多个 amadmin 属性将更改 amadmin 用户密码 (6309830)”
- 第 20 页的 “新的 Access Manager 控制台无法设置 CoS 模板优先级 (6309262)”
- 第 20 页的 “将组作为策略管理用户添加到用户时出现异常 (6299543)”
- 第 20 页的 “传统模式下，无法从角色中删除所有用户 (6293758)”
- 第 20 页的 “无法添加、删除或修改搜索服务资源提供 (6273148)”
- 第 20 页的 “搜索主题时，如果使用了错误的 LDAP 绑定密码，应返回错误消息 (6241241)”
- 第 21 页的 “传统模式下， Access Manager 无法在容器下创建组织 (6290720)”
- 第 21 页的 “添加 Portal Server 相关服务时出现旧版本的控制台 (6293299)”
- 第 21 页的 “达到资源限额后，控制台不返回 Directory Server 设定的结果 (6239724)”

对于 SAML，在控制台中复制 “可信赖的伙伴”时出现错误 (6326634)

在 Access Manager 控制台中，在 “联合” > "SAML" 选项卡下创建 SAML 可信赖的伙伴。如果尝试复制 “可信赖的伙伴”，则出现错误。

解决方法

无。

amConsole.access 和 amPasswordReset.access 无法使用远程日志记录 (6311786)

配置远程日志记录后，除重置密码信息的 amConsole.access 和 amPasswordReset.access 之外，所有的日志都可以写入远程 Access Manager 实例。未在任何地方写入其日志记录。

解决方法

无。

在控制台中添加多个 amadmin 属性将更改 amadmin 用户密码 (6309830)

在管理控制台中添加或编辑 amadmin 用户的某些属性将导致 amadmin 用户密码更改。

解决方法

无。

新的 Access Manager 控制台无法设置 CoS 模板优先级 (6309262)

新的 Access Manager 7 2005Q4 控制台无法设置或修改 “服务级别” (Class of Service, CoS) 模板优先级。

解决方法

登录到 Access Manager 6 2005Q1 控制台以设置或修改 CoS 模板优先级。

将组作为策略管理用户添加到用户时出现异常 (6299543)

将组作为策略管理用户添加到用户时， Access Manager 控制台将返回异常错误。

解决方法

无。

传统模式下，无法从角色中删除所有用户 (6293758)

在传统模式下，如果尝试从角色中删除所有用户，则会保留一个用户。

解决方法

再次从角色中删除该用户。

无法添加、删除或修改搜索服务资源提供 (6273148)

Access Manager 管理控制台不允许添加、删除或修改用户、角色或领域的资源提供。

解决方法

无。

搜索主题时，如果使用了错误的 LDAP 绑定密码，应返回错误消息 (6241241)

Access Manager 管理控制台在使用了错误的 LDAP 绑定密码时没有返回错误消息。

解决方法

无。

传统模式下， Access Manager 无法在容器下创建组织 (6290720)

如果创建了容器，然后尝试在容器下创建组织，则 Access Manager 将返回一个“唯一性违规错误”。

解决方法

无。

添加 Portal Server 相关服务时出现旧版本的控制台 (6293299)

Portal Server 和 Access Manager 安装于同一台服务器上。在传统模式下安装 Access Manager 后，使用 `/amserver` 登录到新的 Access Manager 控制台。如果选择了现有用户，然后尝试添加服务（如 NetFile 或 Netlet），旧的 Access Manager 控制台 (`/amconsle`) 会突然出现。

解决方法

无。当前版本的 Portal Server 需要使用 Access Manager 6 2005Q1 控制台。

达到资源限额后，控制台不返回 Directory Server 设定的结果 (6239724)

首先安装 Directory Server，然后使用现有 DIT 选项安装 Access Manager。登录到 Access Manager 控制台，然后创建组。编辑组中的用户。例如，使用过滤器 uid=*999* 添加用户。最终的列表框为空，并且控制台不显示任何错误、信息或警告消息。

解决方法

组成员人数不能超过 Directory Server 搜索大小限制。如果组成员人数较多，则相应地更改搜索大小限制。

SDK 和客户机问题

- 第 22 页的 “无法删除子领域的会话服务配置 (6318296)”
- 第 22 页的 “指定策略条件时， CDC servlet 重定向到无效的登录页面 (6311985)”
- 第 22 页的 “重新启动服务器后，客户机没有收到通知 (6309161)”
- 第 22 页的 “身份库 ldapv3 插件和 Openldap 需要修补程序 (6305268)”

- 第 22 页的 “需要在服务模式更改后重新启动 SDK 客户机 (6292616)”

无法删除子领域的会话服务配置 (6318296)

创建顶层领域的子领域并为其添加会话服务后，随后尝试删除 “会话服务”配置将显示错误消息。

解决方法

删除默认的顶层 ID 系统信息库 AMSDK1，然后将此系统信息库添加回配置中。

指定策略条件时， CDC servlet 重定向到无效的登录页面 (6311985)

在 CDSSO 模式下使用 Apache 代理 2.2 时，CDC servlet 将在访问受代理保护的资源时将用户重定向至匿名验证页面，而非默认的登录页面。

解决方法

无。

重新启动服务器后，客户机没有收到通知 (6309161)

如果重新启动服务器，则使用客户机 SDK (amclientsdk.jar) 编写的应用程序不会收到通知。

解决方法

无。

身份库 ldapv3 插件和 Openldap 需要修补程序 (6305268)

Openldap 不支持持久性搜索，缺少持久性搜索连接插件将无法启动。

解决方法

要使用 ldapv3 插件，请从 Sun Microsystems 技术代表那里获取 Access Manager 修补程序。

需要在服务模式更改后重新启动 SDK 客户机 (6292616)

修改任意服务模式后， ServiceSchema.getGlobalSchema 将返回旧模式而非新模式。

解决方法

更改服务模式后，重新启动客户机。

命令行实用程序问题

- 第 23 页的 “无法在 Internet Explorer 6.0 中保存包含转义符的 XML 文档 (4995100)”

无法在 Internet Explorer 6.0 中保存包含转义符的 XML 文档 (4995100)

如果在 XML 文件中添加特殊字符 （如在 “&” 旁添加字符串 “amp;” 可正常保存文件；但在稍后使用 Internet Explorer 6.0 检索 XML 配置文件时，该文件无法正常显示。如果再次尝试保存配置文件，则返回错误。

解决方法

无。

验证问题

- 第 23 页的 “UrlAccessAgent SSO 令牌即将过期 (6327691)”
- 第 23 页的 “更正密码后无法登录到带有 LDAPV3 插件/动态配置文件的子领域 (6309097)”
- 第 24 页的“传统（兼容）模式下，Access Manager 统计信息服务的默认配置不兼容 (6286628)”
- 第 24 页的 “在顶层组织命名属性时违反了属性唯一性 (6204537)”

UrlAccessAgent SSO 令牌即将过期 (6327691)

UrlAccessAgent SSO 令牌即将过期，因为应用程序模块未返回特定用户 DN，导致特定用户 DN 匹配，从而使得没有过期的令牌失效。

解决方法

无。

更正密码后无法登录到带有 LDAPV3 插件/动态配置文件的子领域 (6309097)

在领域模式下，如果在领域中使用 “不正确的”密码来创建 ldapv3 数据存储库，并在稍后将密码更改为 amadmin，则在使用已更改的密码再次尝试登录时，登录将失败，并且系统提示配置文件不存在。

解决方法

无。

传统 （兼容）模式下， Access Manager 统计信息服务的默认配置不兼容 (6286628)

在传统模式下安装 Access Manager 后，已更改统计信息服务的默认配置：

- 默认情况下，已开启服务 (com.iplanet.services.stats.state=file)。在此之前，它则是关闭的。
- 默认的时间间隔 (com.iplanet.am.stats.interval) 已从 3600 更改为 60。
- 默认的统计信息目录 (com.iplanet.services.stats.directory) 已从 <install-dir>\AccessManager\debug 更改为 <install-dir>\AccessManager\stats。

解决方法

无。

在顶层组织命名属性时违反了属性唯一性 (6204537)

Access Manager 安装完成后，以 amadmin 身份登录并将 o、sunPreferredDomain、associatedDomain、sunOrganizatio]nAlias、 uid 和 mail 属性添加到 “唯一属性列表”中。使用同一名称创建两个新组织会导致操作失败，但 Access Manager 将显示 “组织已存在”消息而非预期的 “违反了属性唯一性”消息。

解决方法

无。忽略不正确的消息。 Access Manager 工作正常。

会话与 SSO 问题

- 第 24 页的 “跨时区的 Access Manager 实例使得其他用户会话超时 (6323639)”
- 第 24 页的 “负载平衡器终止 SSL 时，系统创建的服务主机名无效 (6245660)”

跨时区的 Access Manager 实例使得其他用户会话超时 (6323639)

跨不同时区安装的且在同一信任圈中的 Access Manager 实例会导致会话超时。

负载平衡器终止 SSL 时，系统创建的服务主机名无效 (6245660)

如果使用终止了 SSL 的负载平衡器将 Access Manager 作为 Web 容器与 Web Server 共同部署，则客户机将被导向至错误的 Web Server 页面。单击 Access Manager 控制台中的 “会话”选项卡将返回一个错误，因为主机是无效的。

解决方法

在下例中，Web Server 将侦听 3030 端口。负载平衡器则侦听 80 端口并将请求重定向至 Web Server。

在 *web-server-instance-name*\config\server.xml 文件中，编辑 servername 属性以指向负载平衡器，具体操作取决于正在使用的 Web Server 版本。

对于 Web Server 6.1 Service Pack (SP) 发行版，按如下所示编辑 servername 属性：

```
<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（或更高版本）可将 http 协议转换为 https 协议，或是将 https 转换为 http 协议。因此，按如下所示编辑 servername：

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

策略问题

删除 “策略配置服务”中的动态属性将导致策略编辑出现问题 (6299074)

在下述方案中，删除 “策略配置服务”中的动态属性将导致策略编辑出现问题：

1. 在 “策略配置服务”中创建两个动态属性。
2. 创建一个策略，然后在响应提供者中选择在步骤 1 中创建的动态属性。
3. 删除 “策略配置服务”中的动态属性，然后再创建两个属性。
4. 尝试编辑在步骤 2 中创建的策略。

结果为：“错误：设置的动态属性无效。”默认情况下，不在列表中显示任何策略。搜索完成后将显示策略，但无法编辑或删除现有的策略，也不能创建新的策略。

解决方法

从 “策略配置服务”中删除动态属性前，先从策略中删除这些属性的引用条目。

服务器启动问题

- 第 26 页的 “Access Manager 启动时出现调试错误 (6309274, 6308646)”

Access Manager 启动时出现调试错误 (6309274, 6308646)

Access Manager 7 2005Q4 启动时将返回 `amDelegation` 和 `amProfile` 调试文件中的调试错误：

- `amDelegation`：无法获取委托的插件实例
- `amProfile`：收到委托异常

解决方法

无。可忽略这些消息。

联合与 SAML 问题

- 第 26 页的 “使用 “辅件” 配置文件时联合失败 (6324056)”
- 第 26 页的 “应编码 SAML 声明中的特殊字符 (&) (6321128)”
- 第 27 页的 “尝试将 Disco 服务添加到角色时出现异常 (6313437)”
- 第 27 页的 “配置并保存其他属性之前无法配置 “验证环境” 属性 (6301338)”
- 第 27 页的 “如果根后缀包含 "&" 字符，则 EP 范例不起作用 (6300163)”
- 第 27 页的 “联合中出现注销错误 (6291744)”

使用 “辅件” 配置文件时联合失败 (6324056)

如果设置了 “身份提供者” (IDP) 和 “服务提供者” (SP)，更改通信协议以使用浏览器 “辅件” 配置文件，然后尝试在 IDP 与 SP 之间联合用户时，联合失败。

解决方法

无。

应编码 SAML 声明中的特殊字符 (&) (6321128)

将 Access Manager 作为源站点和目标站点，并配置了 SSO，目标站点中会出现错误。原因是未编码 SAML 声明中的特殊字符 (&)，从而导致声明解析失败。

解决方法

无。

尝试将 Disco 服务添加到角色时出现异常 (6313437)

在 Access Manager 控制台中，如果尝试将资源提供添加到 Disco 服务中，会出现未知异常。

解决方法

无。

配置并保存其他属性之前无法配置 “验证环境”属性 (6301338)

配置并保存其他属性之前无法配置 “验证环境”属性。

解决方法

配置 “验证环境”属性之前，先配置并保存提供者配置文件。

如果根后缀包含 "&" 字符，则 EP 范例不起作用 (6300163)

如果 Directory Server 拥有包含 "&" 字符的根后缀，则尝试添加 “员工配置文件服务资源提供”时，会抛出异常。

解决方法

无。

联合中出现注销错误 (6291744)

在领域模式下，如果联合“身份提供者”(IDP) 和“服务提供者”(SP) 上的用户帐户，之后终止联合并注销，则出现错误：“错误：未找到任何子组织”。

解决方法

无。

全球化 (g11n) 问题

- 第 28 页的 “用户语言环境首选项没有应用于整个管理控制台 (6326734)”
- 第 28 页的 “客户机检测中无法删除 UTF-8 (5028779)”
- 第 28 页的 “日志文件中的多字节字符显示为问号 (5014120)”
- 第 29 页的 “在 Windows 2000 中，部分未本地化的 Access Manager 登录页面显示为西班牙文 (6358371)”

用户语言环境首选项没有应用于整个管理控制台 (6326734)

Access Manager 管理控制台的某些部分未遵照用户语言环境首选项，使用的是浏览器语言环境设置。这一问题将影响 “版本”、“注销”和联机帮助按钮，以及 “版本”和联机帮助的内容。

解决方法

将浏览器设置更改为与用户首选项相同的语言环境。

客户机检测中无法删除 UTF-8 (5028779)

“客户机检测”功能没有正常工作。不能将 Access Manager 7 2005Q4 控制台中的更改自动传送至浏览器。

解决方法

有两个解决方法：

- 在 “客户机检测”部分中进行更改后，重新启动 Access Manager Web 容器。

  或

- 在 Access Manager 控制台中，按以下步骤进行操作：
- 单击 “配置”选项卡下的 “客户机检测”。
- 单击 genericHTML 的 “编辑”链接。
- 在 HTML 选项卡下方，单击 genericHTML 链接。
- 在字符集列表中输入以下条目：UTF-8;q=0.5（确保 UTF-8 q 因数低于语言环境的其他字符集）。
- 保存、注销、然后再次登录。

日志文件中的多字节字符显示为问号 (5014120)

<install-dir>\AccessManager\logs 目录下的日志文件中的多字节消息显示为问号 (?)。日志文件为本地编码，并非总是 UTF-8。在某一语言环境中启动 Web 容器后，日志文件为该语言环境的本地编码。如果切换至另一个语言环境，然后重新启动 Web 容器实例，则正在传送的消息将使用当前语言环境的本地编码，而使用先前编码的消息将显示为问号。

解决方法

确保始终使用相同的本地编码来启动任何 Web 容器实例。

在 Windows 2000 中，部分未本地化的 Access Manager 登录页面显示为西班牙文 (6358371)

在 Windows 2000 中， Access Manager 登录页面以西班牙文显示部分未本地化的内容。

解决方法

使用 Mozilla Firefox 浏览器。

文档问题

- 第 29 页的 “服务器端的 com.iplanet.am.session.client.polling.enable 不能为 true (6320475)”
- 第 29 页的 “控制台联机帮助中的 “默认成功 URL” 不正确 (6296751)”

服务器端的 com.iplanet.am.session.client.polling.enable 不能为 true (6320475)

服务器端 AMConfig.properties 文件的 com.iplanet.am.session.client.polling.enable 属性不能设置为 true。

解决方法

该属性默认设置为 false，请勿设置为 true。

控制台联机帮助中的 “默认成功 URL” 不正确 (6296751)

service.scserviceprofile.iplanetamauthservice.html 联机帮助文件中的 “默认成功 URL” 不正确。“默认成功 URL” 字段接受一系列的值，这些值用于指定验证成功后用户被重定向到的 URL。此属性的格式为 clientType|URL，尽管您可以只指定 URL 的值 （默认类型为 HTML）。

"/amconsole" 默认值不正确。

解决方法

正确的默认值是 "/amserver/console"。

可再分发的文件

Sun Java System Access Manager 7 不包含任何可再分发给产品非许可用户的文件。

如何报告问题和提供反馈

如果在使用 Sun Java System Access Manager 时遇到问题，请通过下列任一方式与 Sun 客户支持联系：

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

  此站点有到“知识库”、“在线支持中心”、ProductTracker 的链接，除此以外，还提供维护计划和联系支持人员的电话号码。
- 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，并十分乐意接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。文件号码通常包含七位或九位数字，您可以在本书的标题页或文档最上部找到文件号码。例如，本发行说明文档的文件号码是 819-5803，文档标题为《Sun Java™ System Access Manager 7 2005Q4 适用于 Microsoft Windows 的发行说明》。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 819-4262-10，文件标题为 《Sun Java™ System Access Manager 7 2005Q4 Release Notes for Microsoft Windows》。

其他 Sun 资源

可在以下 Internet 位置找到有用的 Sun Java System 信息：

- Sun Java System 文档
  http://docs.sun.com/app/docs/prod/entsys.05q4#hic 及
  http://docs.sun.com/app/docs/prod/entsys.05q4?l=zh#hic
- 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://www.sun.com/software/
- Sun Java System 软件支持服务
  http://www.sun.com/service/sunone/software
- 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