Sun Java System Access Manager 7.1 发行说明

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

文件号码 820–0365
2007 年 7 月

070806@18135

目录

Sun Java System Access Manager 7.1 发行说明

2007 年 7 月

文件号码 820-0365

《Sun Java™ System Access Manager 7.1 发行说明》包含 Sun Java Enterprise System (Java ES) 发行时可用的重要信息，其中包括 Access Manager 的新功能以及已知问题和解决方法（如果可用）。在安装与使用此发行版之前请先阅读本文档。

要查看 Java ES 产品文档，包括 Access Manager 文档集，请访问 `http://docs.sun.com/prod/entsys.05q4` 及 `http://docs.sun.com/prod/entsys.05q4?l=zh`。

请在安装和设置软件前先访问此网站，并定期查看最新的文档。

本发行说明包含以下内容：

修订历史记录

下表显示了 Access Manager 7.1 发行说明的修订历史记录。

表 1 修订历史记录

日期	更改说明
2006 年 7 月	Beta 版。
2007 年 3 月	Java Enterprise System 5 发行版
2007 年 5 月	添加了新的已知问题 6555040、6550261、6554379、6554372、6480354
2007 年 6 月	添加了新的已知问题 6562076、6490150
2007 年 7 月	添加了新的已知问题 6485695

关于 Sun Java System Access Manager 7.1

Sun Java System 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跨企业间 (B2B) 的价值链内对 Web 应用程序和其他资源的安全访问进行管理。

Access Manager 提供以下主要功能：

- 采用基于角色和基于规则的访问控制方式提供集中验证及授权服务
- 以单点登录 (Single Sign-on, SSO) 方式访问组织中基于 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。

此发行版的新增功能

此版本包含以下新增功能：

- 第 7 页中的 “Java ES Monitoring Framework 集成”
- 第 7 页中的 “Web 服务安全性”
- 第 7 页中的 “单个 Access Manager WAR 文件部署”
- 第 7 页中的 “核心服务增强功能”
- 第 10 页中的 “过时通知和通告”

Java ES Monitoring Framework 集成

Access Manager 7.1 通过 Java Management Extensions (JMX) 集成了 Java Enterprise System Monitoring Framework。JMX 技术提供用于构建基于 Web 的分布式、模块化和动态解决方案的各种工具，以管理和监视各种设备、应用程序和服务驱动的网络。JMX 技术的典型应用包括：查询和更改应用程序配置、累计关于应用程序行为的统计信息，以及通知状态更改和错误行为。数据会传送到集中监视控制台。

Access Manager 7.1 使用 Java ES Monitoring Framework 来捕获统计信息和服务相关数据，例如下列信息：

- 尝试验证、成功验证和失败验证的次数
- 策略高速缓存统计信息
- 策略评估事务时间

Web 服务安全性

Access Manager 7.1 通过以下方法将验证功能扩展到 Web 服务：

- 在传出消息中插入令牌
- 评估传入消息的安全令牌
- 支持通过“指向并单击”(Point-and-Click) 方式选择新应用程序的验证提供者

单个 Access Manager WAR 文件部署

Access Manager 包括一个 WAR 文件，您可使用该文件将 Access Manager 服务一致地部署到所有受支持平台上的任何受支持容器中。Access Manager WAR 文件与 Java Enterprise System 安装程序共存，该安装程序可部署多个 JAR、XML、JSP、HTML、GIF 文件和各种属性文件。

核心服务增强功能

支持的 Web 容器

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

Monitoring Framework 集成

Access Manager 可使用 JES Monitoring Framework 监视以下各项：

1. 验证

- 尝试验证的次数
- 尝试远程验证的次数（可选）
- 成功验证的次数
- 失败验证的次数
- 成功注销操作的次数
- 失败注销操作的次数
- 如有可能，每个模块的事务时间（运行和等待状态）

2. 会话
   - 会话表的大小（即会话的最大数量）
   - 活动会话的数量（增量计数器）
3. 配置文件服务
   - 最大高速缓存大小
   - 操作的事务时间（运行和等待）
4. 策略
   - 策略评估内外请求
   - 主题插件的 LDAP 服务器的策略连接池统计信息

验证模块

- 无需将用于负载平衡部署的分布式验证服务固定在一台服务器上
- 无需将用于负载平衡部署的验证服务和服务器固定在一台服务器上
- 验证服务、策略代理和策略服务间支持复合建议。包括 `AuthenticateToRealm` 条件、AuthenticateToService 条件和适用于所有条件的领域限定。
- 建议组织（领域限定的验证条件）
- 验证配置/验证链接 (`AuthServiceCondition`)
- 如果执行了验证链接，则可以禁用基于模块的验证
- 分布式验证服务支持证书验证模块
- 为分布式验证 UI 添加了 `CertAuth`，使之成为功能完整的证书提取器
- 作为即装即用的新数据存储库验证模块，用于根据给定领域的已配置数据存储库进行验证
- 帐户锁定配置现在能够在多个 AM 服务器实例间持久存留
- 处理后的 SPI 类的链接

策略模块

- 添加了新的策略条件 `AuthenticateToServiceCondition`，用于强制将用户验证到特定的验证服务链接。
- 添加了新的策略条件 `AuthenticateToRealmCondition`，用于强制将用户验证到特定的领域。

- 添加了新的策略条件 `LDAPFilterCondition`，用于强制用户匹配特定的 ldap 过滤器。
- 支持一级通配符比较以帮助保护目录的内容而不保护子目录。
- 如果在全局策略配置中启用了组织别名引用，则可在子领域中创建策略而不需要父领域中的明确引用策略。
- `AuthLevelCondition` 既可指定验证级别也可指定领域名称。
- `AuthSchemeCondition` 既可指定验证模块名称也可指定领域名称。

服务管理模块

- 支持在活动目录中存储服务管理/策略配置

Access Manager SDK

- 支持用于向默认身份系统信息库框架数据库验证用户的 API

Web 服务支持

- Liberty ID-WSF SOAP 提供者： 封装由 Access Manager 实现的 Liberty ID-WSF SOAP 绑定的验证提供者。由客户机和服务提供者组成。
- HTTP 层 SSO 提供者： 封装服务器端基于 Access Manager 的 SSO 的 HttpServlet 层验证提供者

安装模块

- 将 Access Manager 重新打包为 J2EE 应用程序会生成一个 WAR 文件，然后便可进行 Web 部署
- 支持 64 位 SJS Web Server 7.0 - 从而支持 64 位 JVM

委托模块

- 支持对委托权限进行分组

升级

- 支持从以下版本升级至 Access Manager 7.1： Access Manager 7.0 2005Q4、Access Manager 6.3 2005Q1 和 Identity Server 6.2 2004Q2。

日志记录

- 支持日志记录模块中的委托 - 控制哪些身份是经授权可以写入或读取日志文件的。
- 支持基于 JCE 的 `SecureLogHelper` - 从而能够使用 JCE（而不仅是 JSS）作为安全日志记录实现的安全提供者

过时通知和通告

Sun Java(TM) System Access Manager 7.1 身份管理 API 和 XML 模板使系统管理员可在 Sun Java System Directory Server 中创建、删除和管理身份条目。Access Manager 也提供用于身份管理的 API。开发者使用 `com.iplanet.am.sdk` 软件包中定义的公共接口和类把管理功能集成到将由 Access Manager 管理的外部应用程序或服务中。Access Manager API 不但提供创建或删除身份相关对象的方式，也提供在 Directory Server 中获取、修改、添加或删除对象属性的方法。

将来的 Access Manager 发行版不会包含 Access Manager `com.iplanet.am.sdk` 软件包（通常称作 AMSDK），包括所有相关的 API 和 XML 模板。现在没有可用的迁移选项，预计将来也不会提供。由 Sun Java System Identity Manager 提供的用户置备解决方案是兼容的替换方案，您可以从现在开始使用。有关 Sun Java System Identity Manager 的更多信息，参见 `http://www.sun.com/software/products/identity_mgr/index.xml`。

硬件和软件要求

下表显示了此发行版所需的硬件和软件。

表 2 硬件和软件要求

组件	要求
操作系统 (OS)	■ 基于 SPARC、x86 和 x64 的系统上的 Solaris™10，具有对整个根本地区域和稀疏根区域的支持。 ■ 基于 SPARC 和 x86 系统上的 Solaris 9。 ■ Red Hat™ Enterprise Linux 3 和 4，所有更新 Advanced Server（32 和 64 位版本）和 Enterprise Server（32 和 64 位版本） ■ Windows x86 上的 Windows 2000 Advanced Server、Data Center Server SP4 版 基于 x86 和 x64 的系统上的 Windows 2003 Standard（32 和 64 位版本）、Enterprise（32 和 64 位版本）、Data Center Server （32 位版本） 基于 x86 的系统上的 Windows XP Professional SP2 PA-RISC 2.0 上的 64 位 HP-UX 11i v1（uname 返回 11.11） 有关所支持操作系统的最新列表，参见《Sun Java Enterprise System 5 Release Notes for UNIX》中的“Platform Requirements and Issues”，或参见《Sun Java Enterprise System 5 Release Notes for Microsoft Windows》中的“Hardware and Software Platform Information”。
Java 2 Standard Edition (J2SE)	J2SE 平台 6.0、5.0 Update 9（HP-UX：1.5.0.03）和 1.4.2 Update 11
Directory Server	Access Manager 信息树：Sun Java System Directory Server 6.0 或 Sun Java System Directory Server 5.2 2005Q4 Access Manager 身份系统信息库：Sun Java System Directory Server 5.2 及 6.0 和 Microsoft Active Directory

表 2 硬件和软件要求 （续）

组件	要求
Web 容器	支持的平台/OS 组合（用于在 64 位 JVM 上运行 Web Server 实例）上的 Sun Java System Web Server 7.0。支持的平台： Solaris 9/SPARC、Solaris 10/SPARC、Solaris 10/AMD64、Red Hat AS 或 ES 3.0/AMD64，以及 Red Hat AS 或 ES 4.0/AMD64
	Sun Java System Application Server Enterprise Edition 8.2
	BEA WebLogic 8.1 SP4
	IBM WebSphere Application Server 5.1.1.6
RAM	基本测试： 512 MB
	实际部署： 1 GB，用于线程、Access Manager SDK、HTTP 服务器及其他内部组件
磁盘空间	512 MB，用于 Access Manager 和相关应用程序

如果您对支持这些组件的其他版本存有疑问，请联系 Sun Microsystems 技术代表。

支持的浏览器

下表显示了 Sun Java Enterprise System 5 发行版支持的浏览器。

表 3 支持的浏览器

浏览器	平台
Firefox 1.0.7	Windows XP
	Windows 2000
	Solaris OS，版本 9 和 10
	Red Hat Linux 3 和 4
	Mac OS X
Microsoft Internet Explorer™ 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows™ 2000

表 3 支持的浏览器 （续）

浏览器	平台
Mozilla™ 1.7.12	Solaris OS，版本 9 和 10
	Windows XP
	Windows 2000
	Red Hat Linux 3 和 4
	Mac OS X
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000
Netscape Communicator 7.1	Solaris OS，版本 9 和 10

常规兼容性信息

AMSDK 与 Access Manager 服务器系统间不兼容

在以下 Java Enterprise System 版本中，AMSDK 和 Access Manager 服务器的下列组合不兼容：

- Java Enterprise System 2004Q2 AMSDK 与 Java Enterprise System 5 Access Manager 服务器（本发行版）不兼容。
- Java Enterprise System 5 AMSDK（本发行版）与 Java Enterprise System Access Manger 2004Q2（以前称为 Identity Server）服务器不兼容。

Access Manager HPUX 版本不支持升级

不支持将 HPUX 版本的 Access Manager 7 2005Q4 升级到 Access Manger 7.1（本发行版）。

Access Manager 传统模式

如果将 Access Manager 与以下产品一起安装，则必须选择 Access Manager 传统 (6.x) 模式：

- Sun Java System Portal Server

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

选择 Access Manager 传统 (6.x) 模式的方式取决于 Java ES 安装程序的运行方式：

- 第 14 页中的 “使用状态文件的 Java ES 无提示安装”
- 第 14 页中的 “图形模式下的“现在配置”安装选项”
- 第 14 页中的 “基于文本的模式下的“现在配置”安装选项”
- 第 14 页中的 ““以后再配置”安装选项”

如需确定 Access Manager 7.1 安装模式的更多信息，参见第 15 页中的 “确定 Access Manager 模式” 。

使用状态文件的 Java ES 无提示安装

Java ES 安装程序的无提示安装是一种非交互式的模式，它允许在多个拥有相似配置的主机服务器上安装 Java ES 组件。首先运行安装程序以生成状态文件（实际并不安装任何组件），然后为每个计划安装 Access Manager 和其他组件的主机服务器编辑一份状态文件。

要在传统 (6.x) 模式下选择 Access Manager，请在无提示模式下运行安装程序前，设置状态文件中的以下参数（连同其他参数）：

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

有关在无提示模式下使用状态文件运行 Java ES 安装程序的更多信息，参见《Sun Java Enterprise System 5 Installation Guide for UNIX》中的第 5 章 “Installing in Silent Mode”。

图形模式下的“现在配置”安装选项

如果在图形模式下使用“现在配置”选项运行 Java ES 安装程序，则在“Access Manager：管理 (1/6)”面板上，选择默认值“传统模式（6.x 版样式）”。

基于文本的模式下的“现在配置”安装选项

如果是在基于文本的模式下使用 “现在配置” 选项运行 Java ES 安装程序， 则对于**安装类型（ 领域** - Realm/**传统** - Legacy **）模式**：[Legacy]，选择默认值 Legacy（ **传统** ）。

“以后再配置”安装选项

如果使用“以后再配置“选项运行 Java ES 安装程序，则在安装完成后必须运行 amconfig 脚本来配置 Access Manager。要选择传统 (6.x) 模式，设置配置脚本输入文件 (amsamplesilent) 中的以下参数：

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

有关运行 amconfig 脚本以配置 Access Manager 的更多信息，参阅《Sun Java System Access Manager 7.1 管理指南》。

确定 Access Manager 模式

要确定正在运行的 Access Manager 7.1 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

下表显示了策略代理与 Access Manager 7.1 模式的兼容性。

表 4 策略代理与 Access Manager 7.1 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
Access Manager 7.1 中不支持 Web 和 J2EE 代理版本 2.1	

已知问题和限制

此节描述了 Access Manager 7.1 发行时的已知问题及解决方法（如果可用）。

安装问题

有关 Java System Enterprise 安装问题的信息包含在 JES5 发行说明中。参见《Sun Java Enterprise System 5 Release Notes for UNIX》中的“Access Manager Installation Issues”一节。

本节包含以下已知问题：

WebLogic 上的 Access Manager 单个 WAR 部署需要 JAX-RPC 1.0 JAR 文件才能与客户机 SDK 通信 (6555040)

Weblogic 8.1 上部署的单个 WAR 在 JAX-RPC 初始化时存在一个已知问题。为了让 Access Manager 与客户机 SDK 通信，需要用 JAX-RPC 1.0 jar 文件替换 JAX-RPC 1.1 jar 文件。

解决方法：

有两种方法可以获得 WAR 文件。一种是通过将 Access Manager 设置为“以后再配置”选项运行 Java Enterprise System 5 安装程序，另一种是从 Sun 下载站点下载。

如果已经通过选择“以后再配置”选项运行 JES 5 安装程序生成了 WAR 文件：

1. 从 *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib` 中删除下列 JAXRPC 1.1 `.jar` 文件：
   - `jaxrpc-api.jar`
   - `jaxrpc-spi.jar`
   - `jaxrpc-impl.jar`
2. 将下列 `.jar` 文件从其各自的位置复制到 *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib` 中：

- /opt/SUNWam/lib/jaxrpc 1.0 中的 jaxrpc-api.jar
- /opt/SUNWam/lib/jaxrpc 1.0 中的 jaxrpc_ri.jar
- /opt/SUNWmfwk/lib 中的 commons-logging.jar

3. 转至 *AccessManager-base*/SUNWam/bin/ 并运行下列命令：

   amconfig –s *samplesilent*

   有关使用 amconfig 脚本配置 Access Manager 的更多信息，参见 Access Manager Post Installation Guide 中的“Running the Access Manager amconfig Script”。

如果已经从 Sun 下载站点 (http://www.sun.com/download/index.jsp) 下载了 WAR 文件：

1. 获取 *ZIP_ROOT*/applications/jdk14/amserver.war 文件并将它解压缩到临时位置，如 /tmp/am-staging。
2. 从 /tmp/am-staging/WEB-INF/lib 中删除下列 JAXRPC 1.1 .jar 文件：
   - jaxrpc-api.jar
   - jaxrpc-spi.jar
   - jaxrpc-impl.jar
3. 将 *ZIP_ROOT*/applications/jdk14/jarFix 目录中的下列 JAXRPC 1.0 .jar 文件及通用日志 .jar 文件复制到 /tmp/am-staging/WEB-INF/lib 中：
   - jaxrpc-api.jar
   - jaxrpc-ri.jar
   - commons-logging.jar
4. 重新创建和部署 Access Manager WAR。有关更多信息，参见 Access Manager Post Installation Guide 中的“Deploying Access Manager as a Single WAR File”。

由 JES 5 安装程序为 Websphere 5.1 生成的单个 WAR 需要附加的 .jar 文件 (6550261)

如果 Access Manager 单个 WAR 是通过选择“以后再配置”选项运行 JES 5 安装程序生成的，则需要附加 .jar 文件才能部署 Websphere 5.1。

解决方法：

1. 从 /usr/share/lib 将 jsr173_api.jar 复制到 *AcessManager-base*/opt/SUNWam/web-src/WEB-INF/lib 目录中。
2. 转至 *AccessManager-base*/SUNWam/bin/ 并运行下列命令：

   amconfig –s *samplesilent*

   有关使用 amconfig 脚本配置 Access Manager 的更多信息，参见 Access Manager Post Installation Guide 中的“Running the Access Manager amconfig Script”。

Webshpere 的单个 WAR 部署需要修改 server.xml 才能与客户机 SDK 通信 (6554379)

为使 Websphere 5.1 的 Access Manager 单个 WAR 部署能成功地与客户机 SDK 通信，必须对 `server.xml` 文件做一些更改。

解决方法：

要正确更改 `server.xml` 文件，请参见以下步骤：

1. 获取 `amserver.war` 文件。有两种方法可以获取单个 WAR 文件：通过选择“以后再配置”选项运行 JES 5 安装程序，或从 Sun 下载站点下载。

   注 – 如果通过 JES 5 安装程序生成 WAR 文件，确保完成已知问题 #6550261 中列出的步骤。

   ---

2. 将 Access Manager WAR 解压缩到临时位置，如 `/tmp/am-staging`。
3. 从 `/tmp/am-staging/WEB-INF/lib` 中将下列共享 `.jar` 文件复制到共享位置（如 `/export/jars`）：

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

4. 从临时位置的 `/tmp/am-staging/WEB-INF/lib` 中删除相同的 `.jar` 文件。
5. 更新 Webshpere 实例的 `server.xml`。如果默认实例位置是 `/opt/WebSphere/AppServer/config/cells/`*node-name*`/nodes/`*node-name*`/servers/server1`，请更改 `server.xml` 里的*jvmEntries*，如下所示：

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

6. 重新启动容器。
7. 从 /tmp/am-staging 重新创建和部署 Access Manager WAR。有关更多信息，参见 Access Manager Deployment Planning Guide 中的 Deploying Access Manager as a Single WAR File。

分布式验证需要更改才能与 Weblogic 和 Webshpere 上的 Access Manager 单个 War 共同工作 (6554372)

因为容器是 JDK14 版本，分布式验证 WAR 需要附加 jar 文件才能为 Weblogic 8.1 及 Websphere 5.1 解析。JDK14 `.jar` 文件位于 `.zip` 文件的以下目录中：

ZIP-ROOT`/applications/jdk14/jarFix`

解决方法：

对于 Weblogic 8.1：

1. 用设置脚本配置分布式验证。参见 Access Manager Post Installation Guide 中的“Deploying a Distributed Authentication UI Server”。
2. 将更新过的分布式验证 WAR 解压缩到临时位置，如 `/tmp/dist-auth`。
3. 从 *ZIP-ROOT*`/applications/jdk14/jarFix` 中将 `xercesImpl.jar`、`dom.jar` 及 `xalan.jar` 复制到 `/tmp/dist_auth/WEB-INF/lib` 目录中。
4. 从临时位置重新生成分布式验证 WAR 并对其进行部署。有关更多信息，参见 Access Manager Post Installation Guide 中的“Deploying a Distributed Authentication UI Server WAR File”。

对于 Websphere 5.1：

1. 用设置脚本配置分布式验证。参见 Access Manager Post Installation Guide 中的“Deploying a Distributed Authentication UI Server”。
2. 将更新过的分布式验证 WAR 解压缩到临时位置，如 `/tmp/dist-auth`。
3. 从 *ZIP-ROOT*`/applications/jdk14/jarFix` 中将 `xercesImpl.jar`、`dom.jar` 及 `xalan.jar` 复制到 `/tmp/dist_auth/WEB-INF/lib` 目录中。
4. 编辑 `WEB-INF/web.xml` 文件并用 `http://java.sun.com/dtd/web-app_2_3.dtd` 替换 `jar://web-app_2_3.dtd`。
5. 从临时位置重新生成分布式验证 WAR 并对其进行部署。有关更多信息，参见 Access Manager Post Installation Guide 中的“Deploying a Distributed Authentication UI Server WAR File”。

单个 WAR 配置程序在 DS 上失败 (6562076)

部署为单个 WAR 的 Access Manager 使用单个组件根后缀（例如 `dc=example`）在 Directory Server 6 上配置会失败。但是，使用多个组件根后缀（例如 `dc=example,dc=com`）可以成功配置。

解决方法：使用多个组件根后缀，如 `dc=example,dc=com`。

在同一主机上进行 AM 单个 WAR 的多服务器配置会抛出异常 (6490150)

如果在同一主机上对 Directory Server 配置第二个 Access Manager 单个 WAR 实例，则更新组织别名时会抛出异常。在不同主机上配置第二个实例就不会发生该问题。

升级问题

关于升级问题的信息，参见《Sun Java Enterprise System 5 Release Notes for UNIX》中的“Upgrade Issues”一节。

兼容性问题

- 第 20 页中的 “通用 Web 客户机上 Access Manager 单点登录失败 (6367058, 6429573)”
- 第 20 页中的 “64 位模式下运行的 Web Server 7.0 中发生 StackOverflowError 错误 (6449977)”
- 第 21 页中的 “传统模式的核心验证模块存在不兼容性 (6305840)”
- 第 21 页中的 “Delegated Administrator `commadmin` 实用程序不创建用户 (6294603)”
- 第 22 页中的 “Delegated Administrator `commadmin` 实用程序不创建组织 (6292104)”

通用 Web 客户机上 Access Manager 单点登录失败 (6367058, 6429573)

如果安装了 Access Manager、Messaging Server 和 Calendar Server 并把它们配置为共同工作，而后又安装 JES5 120955-01 修补程序，则会出现此问题。用户遇到登录错误。该错误是由于 Policy Agent 2.1 属性与 AMSDK 不兼容所造成的。现在还没有解决方法。

64 位模式下运行的 Web Server 7.0 中发生 StackOverflowError 错误 (6449977)

如果在使用 64 位 JVM 的 Web Server 7.0 上配置 Access Manager，则用户会在访问控制台登录页面时遇到“服务器错误”消息。Web Server 错误日志包含 `StackOverflowError` 异常。

解决方法：按以下步骤修改 Web Server 配置：

1. 以 Web Server 管理员身份登录 Web Server 管理控制台。
2. 单击“编辑配置”。

   在“平台”字段中选择 64，然后单击“保存”。

3. 单击“Java”选项卡，然后单击“JVM 设置”选项卡。
   - 在“选项”下查找最小堆大小条目（例如：-Xms）。最小堆大小的值至少应为 512m。例如，如果堆大小的值不是 -Xms512m 或小于此值，则应将值更改为至少 -Xms512m。
   - 最大堆大小的值至少应为 768m。如果最大堆大小的值不是 -Xmx768m 或小于此值，则应将值更改为至少 -Xmx768m。
   - 以 `-Xss512k` 或 `-Xss768k` 将 Java 堆栈大小设置为 512k 或 768k。在 Solaris Sparc 的 64 位 JVM 上也可将此值留空，以采用默认大小 (1024k)。
4. 单击“性能”选项卡，然后单击链接“线程池设置”。

   把堆栈大小的值更改为至少 261144，然后单击“保存”。
5. 单击屏幕右上角的链接“部署暂挂”。

   在“配置部署”页面上，单击“部署”按钮。
6. 在“结果”窗口中，单击“确定”以重新启动 Web Server 实例。

   重新启动 Web Server 后单击“结果”窗口中的“关闭”。

传统模式的核心验证模块存在不兼容性 (6305840)

Access Manager 7.1 传统模式与 Access Manager 6 2005Q1 发行版在核心验证模块方面存在以下不兼容性：

- 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 7.1 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。

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

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

解决方法：如果只将 Access Manager 升级至版本 7.1，而未升级 Delegated Administrator，则会出现此问题。

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` 属性标记为可选而非必需。默认情况下，该文件位于 Solaris 系统的 `/opt/SUNWcomm/lib/services/` 目录下。
2. 在 Access Manager 中，通过运行 `amadmin` 命令删除现有 XML 文件，如下所示：

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

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

```
# ./amadmin -u amadmin -w password
-s /opt/SUNWcomm/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。

配置问题

- 第 23 页中的 “不使用 web 容器的 Access Manager SDK 安装需要更新通知 URL (6491977)”
- 第 23 页中的 “密码重置服务在更改密码时报告通知错误 (6455079)”
- 第 23 页中的 “平台服务器列表和 FQDN 别名属性未更新 (6309259, 6308649)”
- 第 23 页中的 “服务中的必需属性要求验证数据 (6308653)”
- 第 23 页中的 “在安全的 WebLogic 8.1 实例上的部署解决方法 (6295863)”
- 第 24 页中的 “`amconfig` 脚本不更新领域/DNS 别名和平台服务器列表条目 (6284161)”
- 第 24 页中的 “在配置状态文件模板中，默认的 Access Manager 模式为领域 (6280844)”

部署在负载平衡器后面出现控制台重定向错误 (6480354)

如果 Access Manager 实例部署在负载平衡器后面，登录 Access Manager 控制台可能会重定向到 Access Manager 实例之一，而不是负载平衡器。浏览器中的 URL 也会变为 Access Manager 实例。例如，如果用以下 URL 登录到控制台就可能发生该问题：

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

“领域”模式和“传统”模式部署中都可能发生此重定向。

该问题有两种解决方法。可任选一种使用：

1. 用下列 URL 之一登录：

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

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

2. 在 `AMConfig.properties` 中，将 `com.sun.identity.loginurl` 属性设置为负载平衡器的名称。负载平衡器后面的每个 Access Manager 实例都需要这样设置。

不使用 web 容器的 Access Manager SDK 安装需要更新通知 URL (6491977)

如果使用“现在配置”选项通过 Java ES 5 安装程序来安装不包含 web 容器的 Access Manager SDK，那么 AMConfig.properties 文件中的 `com.iplanet.am.notification.url` 属性会被设置为 `NOTIFICATION_URL`。如果不执行任何其他 web 容器配置，则用户不会接收到来自远程 Access Manager 服务器的通知。

解决方法：将该属性重置为以下内容：`com.iplanet.am.notification.url=""`

密码重置服务在更改密码时报告通知错误 (6455079)

更改密码后，Access Manager 使用不合格的发件人名称 `Identity-Server` 提交电子邮件通知，这会导致 `amPasswordReset` 日志中出现错误条目。示例：

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

解决方法：更改 `/opt/SUNWam/locale/amPasswordResetModuleMsgs.properties` 中的配置。

- 更改发件人地址。将 `fromAddress.label=<Identity-Server>` 更改为 `fromAddress.label=<IdentityServer@myhost.company.com>`
- 更改 `lockOutEmailFrom` 属性以确保锁定通知使用正确的**发件人**地址。

平台服务器列表和 FQDN 别名属性未更新 (6309259, 6308649)

在多服务器部署中，如果将 Access Manager 安装在第二台服务器（及随后的服务器）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。有关操作步骤，参见《Sun Java System Access Manager 7.1 Postinstallation Guide》中的“Adding Additional Instances to the Platform Server List and Realm/DNS Aliases”一节。

服务中的必需属性要求验证数据 (6308653)

Access Manager 7.1 强制要求服务 XML 文件中的必需属性具备默认值。

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。

在安全的 WebLogic 8.1 实例上的部署解决方法 (6295863)

如果将 Access Manager 7.1 部署至安全的（启用了 SSL）BEA WebLogic 8.1 SP4 实例内，则在部署每个 Access Manager Web 应用程序期间将出现异常。

解决方法：请按照以下步骤进行操作：

1. 应用 WebLogic 8.1 SP4 修补程序 JAR `CR210310_81sp4.jar`，此文件可从 BEA 中得到。
2. 在 `/opt/SUNWam/bin/amwl81config` 脚本（Solaris 系统）或 `/opt/sun/identity/bin/amwl81config` 脚本（Linux 系统）中，通过更新 `doDeploy` 函数和 `undeploy_it` 函数，将修补程序 JAR 的路径置于 `wl8_classpath` 变量前，此变量包含用于部署和取消部署 Access Manager Web 应用程序的 `classpath`。

   找到以下包含 `wl8_classpath` 的行：

   ```
   wl8_classpath= ...
   ```
3. 找到步骤 2 中所述的行后，直接在其后添加以下行：

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

`amconfig` 脚本不更新领域/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。有关操作步骤，参见《Sun Java System Access Manager 7.1 Postinstallation Guide》中的“Adding Additional Instances to the Platform Server List and Realm/DNS Aliases”一节。

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，在配置状态文件模板中 Access Manager 模式（`AM_REALM` 变量）为启用。

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
```

性能问题

在领域模式下，创建新组时会生成带有 ACI 的组管理员，而这些 ACI 永远不会得到使用 (6485695)

如果 Access Manager 安装在领域模式下，每当创建新组时，Access Manager 都会动态创建一个组管理员，且该管理员带有管理该组所需的 ACI。在领域模式下，这些组管理员 ACI 不会被使用。然而，当 Directory Server 处理后缀下的条目时，仍然要评估它们，这就降低了 Access Manager 的性能，尤其是在部署创建了大量组的情况下。

解决方法：此问题的解决方法包括两部分：

- 阻止 Access Manager 在创建新组时创建组管理员和相应的 ACI。

- 从 Directory Server 中删除现有的全部组管理员 ACI。

阻止创建组管理员 ACI

下列过程可阻止 Access Manager 在创建新组时创建组管理员和相应的 ACI。

注 – 该过程会永久性阻止在创建新组时创建组管理员和相应的 ACI。仅当此行为适合您的特定部署时才使用该过程。

---

1. 备份 `amAdminConsole.xml` 文件。根据您的平台，此文件位于下列目录：
   - Solaris 系统：`/etc/opt/SUNWam/config/xml`
   - Linux 及 HP-UX 系统：`/etc/opt/sun/identity/config/xml`
   - Windows 系统：*javaes-install-dir*`\identity\config\xml`

     javaes-install-dir 表示 Java ES 5 安装目录。其默认值为 `C:\Program Files\Sun\JavaES5`。
2. 在 `amAdminConsole.xml` 文件中删除下列注释行之间的组管理员条目：

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

3. 用 amadmin 从 Access Manager 中删除 Admin Console 服务。例如，在 Solaris 系统上：

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

4. 使用 amadmin 将 Admin Console 服务从步骤 2 中已编辑的 amAdminConsole.xml 文件中重新装入到 Access Manager。例如：

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

5. 重新启动 Access Manager Web 容器。（如果计划按下一过程所述内容从 Directory Server 中删除 ACI，请在完成该过程后等待并重新启动 Web 容器。）

删除现有的组管理员 ACI

注 – 下列过程用 ldapsearch 和 ldapmodify 实用程序找到并删除组管理员 ACI。如果您的部署使用 Directory Server 6.0，则也可以用 Directory Server Control Center (DSCC) 或 dsconf 命令来完成这些功能。有关更多信息，参见 Directory Server 6.0 文档：

http://docs.sun.com/app/docs/coll/1224.1 及
http://docs.sun.com/app/docs/coll/1606.1

下列过程删除已经存在于 Directory Server 上的组管理员 ACI。

1. 创建一个 LDIF 文件以搭配 ldapmodify 使用来删除组管理员 ACI。使用 ldapsearch（或其他您喜欢的目录搜索工具）可找到这些 ACI。

   例如，命名为 Remove_Group_ACIs.ldif 的范例 LDIF 文件中的以下条目将删除命名为 New Group 的组的 ACI：

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

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

```
dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///o=isp")
(targetfilter=(&(|(memberof=*cn=New Group,ou=Groups,o=isp)
(iplanet-am-static-group-dn=*cn=New Group,ou=Groups,o=isp))
(!(|(nsroledn=cn=Top-level Admin Role,o=isp)
(nsroledn=cn=Top-level Help Desk Admin Role,o=isp)
(nsroledn=cn=Top-level Policy Admin Role,o=isp)
(nsroledn=cn=Organization Admin Role,o=isp)(
nsroledn=cn=Container Admin Role,o=isp)
(nsroledn=cn=Organization Policy Admin Role,o=isp)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list ||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members";
allow (read,write,search)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)
aci: (target="ldap:///o=isp")(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the root suffix";
allow (all) userdn = "ldap: ///cn=dsameuser,ou=DSAME Users,o=isp"; )
```

2. 使用 `ldapmodify` 搭配上一步的 LDIF 文件将组 ACI 从 Directory Server 上删除。例如：

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

3. 重新启动 Access Manager Web 容器。

Access Manager 控制台问题

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

新的 Access Manager 7.1 控制台无法设置或修改服务类 (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。

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 结果集 (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：组成员资格不得大于 Directory Server 搜索大小限制。如果组成员资格较大，则相应更改搜索大小限制。

数据迁移后添加 `ContainerDefaultTemplateRole` 属性 (4677779)

在传统模式中，不是在 Access Manager 中创建的组织下面不会显示用户的角色。在调试模式下将显示以下消息：

错误：`DesktopServlet.handleException()`
`com.iplanet.portalserver.desktop.DesktopException:`
`DesktopServlet.doGetPost()`：**没有权限运行桌面**

此错误在运行 Java ES 安装程序迁移脚本后变得更加明显。`ContainerDefaultTemplateRole` 属性未被自动添加到从现有目录信息树 (DIT) 或其他来源迁移而来的组织中。

解决方法：使用 Directory Server 控制台从另一 Access Manager 组织中复制 `ContainerDefaultTemplateRole` 属性，然后将其添加到受影响的组织中。

命令行问题

组织管理员角色无法使用 amadmin 命令行实用程序创建新用户 (6480776)

由于日志记录权限不正确，指定了组织管理员角色的管理员无法使用 amadmin 命令行实用程序创建新用户。

解决方法：组织管理员和顶级管理员都可设置权限。通过管理控制台按照下列步骤来进行设置：

1. 转到组织管理员所属的组织。

2. 单击“权限”选项卡。
3. 单击“组织管理员角色”链接。
4. 选择“**对所有日志文件的读写权限**”或“**对所有日志文件的写入权限**”。
5. 单击“保存”。

SDK 和客户机问题

- 第 29 页中的 “重新启动服务器后，客户机没有收到通知 (6309161)”
- 第 29 页中的 “需要在服务器模式更改后重新启动 SDK 客户机 (6292616)”

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。

需要在服务器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。

修补程序 1 会修复此问题。

验证问题

- 第 29 页中的 “如果应用程序用户没有足够的权限，则分布式验证 UI 服务器的性能会下降 (6470055)”
- 第 30 页中的 “传统（兼容）模式下，Access Manager 默认配置的统计信息服务不兼容 (6286628)”
- 第 30 页中的 “顶级组织在命名属性时违反了属性唯一性 (6204537)”

如果应用程序用户没有足够的权限，则分布式验证 UI 服务器的性能会下降 (6470055)

使用默认应用程序用户部署分布式验证 UI 服务器时，由于默认应用程序用户权限受限，服务器的性能会显著下降。

解决方法：使用适当的权限创建新用户。

按照以下方法使用适当的 ACI 创建新用户：

1. 在 Access Manager 控制台中创建新用户。例如，创建名为 `AuthUIuser` 的用户。

2. 在 Directory Server 控制台中添加以下 ACI。

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

注意，`userdn` 是设置为 `"ldap:///<AuthUIuser's DN>"`。

3. 有关编辑 `amsilent` 文件和运行 `amadmin` 命令的说明，参见《Sun Java System Access Manager 7.1 Postinstallation Guide》中的"To Install and Configure a Distributed Authentication UI Server"一节的说明。
4. 在 `amsilent` 文件中设置以下属性：

   APPLICATION_USER　　输入 `AuthUIuser`。

   APPLICATION_PASSWD　　输入 `AuthUIuser` 的密码。
5. 保存文件。
6. 使用新的配置文件运行 `amconfig` 脚本。例如，在 Access Manager 安装于默认目录下的 Solaris 系统上：

   ```
   # cd /opt/SUNWam/bin

   # ./amconfig -s ./DistAuth_config
   ```
7. 重新启动分布式验证 UI 服务器上的 Web 容器。

传统（兼容）模式下，Access Manager 默认配置的统计信息服务不兼容 (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 `/var/opt/SUNWam/debug` 更改为 `/var/opt/SUNWam/stats`。

解决方法：无。

顶级组织在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`、`sunOrganizationAlias`、`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。

会话和 SSO 问题

负载平衡器终止 SSL 时，系统创建的服务主机名无效 (6245660)

如果 Access Manager 与 Web Server（作为 Web 容器）共同部署，并且负载平衡器终止了 SSL，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) 版本，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"/>
```

配合第三方 Web 容器使用 HttpSession

维持验证会话的默认方法是“内部会话”而非 `HttpSession`。默认无效会话最长时间为三分钟便已足够。`amtune` 脚本将 Web Server 或 Application Server 的默认无效会话最长时间设置为一分钟。但是，如果您正在使用第三方的 Web 容器（IBM WebSphere 或 BEA WebLogic Server）和可选的 `HttpSession`，则可能需要限制 Web 容器的最长 `HttpSession` 时间限制以避免出现性能问题。

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动态属性（来自步骤 1）。
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，列表中不会显示任何策略。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：在从“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

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

Access Manager 7.1 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。

AMSDK 问题

执行 AMIdentity.modifyService 时显示错误 (6506448)

使用 AMIdentity.modifyService 设置领域上的桌面服务动态属性时， Access Manager 返回 null 指针异常。

解决方法：将以下属性添加到 AMConfig.properties，然后重新启动服务器：

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

选定列表中不显示组成员 (6459598)

在以下情况中会出现此问题：

1. 使用以下领域配置定义领域：
   - 顶级领域是 amroot。子领域是 example.com。
   - 子领域 example.com 具有两个数据存储库： exampleDB 和 exampleadminDB。
   - 数据存储库 exampleDB 包含所有以 dc=example,dc=com 开头的用户。支持的 LDAPv3 操作设置为 user=read,write,create,delete,service。
   - 数据存储库 exampleadminDB 包含领域的管理员组。管理员组为 DN: cn=example.com Realm Administrators,ou=Groups,dc=example,dc=com。该组拥有单个成员 scarter。支持的 LDAPv3 操作设置为 group=read,write,create,delete。
2. 单击“主题”选项卡，再单击“组”，然后单击 example.com Realm Administrators 的条目。
3. 单击“用户”选项卡。

exampleDB 数据存储库中的所有用户都显示为可用，但是“选定”字段中不显示 scarter。

解决方法：将操作 user=read 添加至 exampleadminDB 数据存储库内支持的 LDAPv3 操作中。

Access Manager 登录 URL 返回消息“ 未找到此类组织 ”(6430874)

出现此问题的原因可能是在全限定域名 (fully qualified domain name, FQDN) 中混合使用了大小写（同时包含大写和小写）字符。

示例： HostName.PRC.Example.COM

解决方法：完成安装后不要使用默认的 Access Manager 登录 URL。而是在登录 URL 中包括默认组织的 LDAP 位置。例如：

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

一旦成功登录 Access Manager，便无需每次登录 Access Manager 时都输入用户组织的完整路径。请按照以下步骤进行操作：

1. 转至“领域”模式下的“领域”选项卡，或转至“传统”模式下的“组织”选项卡。
2. 单击默认领域或组织名称。

   在本示例中，单击 `prc`。
3. 将**领域/DNS 别名**值中的所有大写字符更改为小写字符。

   在本示例中，将所有小写值 `hostname.prc.example.com` 添加至列表，然后从列表中删除混合大小写的 `HostName.PRC.Example.COM` 值。
4. 单击“保存”，然后注销 Access Manager 控制台。

现在便可使用以下任一 URL 进行登录：

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

使用 amadmin 时无法从 Access Manager 创建子组织 (5001850)

如果在两个 Directory Server 之间启用了多主复制而您尝试使用 `amadmin` 实用程序创建子组织，则会出现此问题。

解决方法：将两个 Directory Server 的 `nsslapd-lookthroughlimit` 属性都设置为 -1。

SSL 问题

- 第 34 页中的 “SSL 证书到期后 amconfig 脚本失败。(6488777)”

SSL 证书到期后 amconfig 脚本失败。(6488777)

如果在 SSL 模式下运行 Access Manager 容器，而且容器 SSL 证书已到期，则 `amconfig` 会失败且可能导致类路径被破坏。

解决方法：如果使用过期的证书运行了 `amconfig`，而且类路径已被破坏，则首先需要获取有效的 SSL 证书。恢复为类路径未被破坏的原先的 `domain.xml` 文件，或该文件的副本。然后重新运行 `amconfig` 命令：

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

范例问题

Clientsdk 范例目录包含多余的 makefile (6490071)

范例文件包含在客户机 SDK 中。这些文件说明如何编写独立程序和 Web 应用程序。范例位于生成 `Makefile.clientsdk` 的目录和下列子目录中：

```
.../clientsdk-samples/

.../clientsdk-webapps/
```

Clientsdk-samples 包括验证、日志记录、策略和 SAML 独立程序的范例。Clientsdk-webapps 包括用户管理、服务管理和策略程序的范例。每个范例都含有 Readme.html 文件，该文件说明如何编译和运行范例程序。

要编译范例，应该在相应的子目录中运行 makefile。顶层 makefile 不会编译子目录中的范例。

Linux OS 问题

在 Application Server 上运行 Access Manager 时出现 JVM 问题 (6223676)

如果您正在 Red Hat Linux 上运行 Application Server 8.1，由于 Red Hat OS 为 Application Server 所创建的线程堆栈大小为 10 MB，因此，当 Access Manager 用户会话数达到 200 时会出现 JVM 资源问题。

解决方法：启动 Application Server 前，通过执行 `ulimit` 命令将 Red Hat OS 的工作堆栈大小设置为较小的值，如 2048 甚至 256 KB。在用于启动 Application Server 的同一控制台上执行 `ulimit` 命令。例如：

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

Windows 和 HP-UX 问题

在 zh_TW 和 es 语言环境中安装时，Access Manager 自动配置失败 (6515043)

解决方法：在 HP-UX 平台的 zh_TW 和 es 语言环境中，Access Manager 仅能在“以后再配置”模式下配置。启动 JavaES 安装程序，安装 Access Manager 产品并退出 JavaES 安装程序。然后按照以下方法调用 Access Manager 配置程序：

1. LANG=C
2. export LANG
3. 编辑 *accessmanager-base*/bin/amsamplesilent 文件
4. 运行 *accessmanager-base*/bin/amconfig -s amsamplesilent

完整安装 JES 时，HP-UX 需要 AM 的 gettext 二进制文件 (6497926)

该问题现在还没有解决方法。

联合与 SAML 问题

- 第 36 页中的 “联合中出现注销错误 (6291744)”

联合中出现注销错误 (6291744)

在领域模式下，如果在“身份提供者”(IDP) 和“服务提供者”(SP) 上联合用户帐户，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 36 页中的 “zh 语言环境中的管理控制台组件以英文显示 (6470543)”
- 第 37 页中的 “控制台中的“当前值”和“新值”显示不正确 (6476672)”
- 第 37 页中的 “必须根据英文习惯指定策略条件日期 (6390856)”
- 第 37 页中的 “客户机检测无法删除 UTF-8 (5028779)”
- 第 37 页中的 “日志文件中的多字节字符显示为问号 (5014120)”

zh 语言环境中的管理控制台组件以英文显示 (6470543)

当浏览器语言环境设置为 zh 时，管理控制台组件会以英文显示，例如 "Version"（版本）、"Help"（帮助）和 "Logout"（注销）等按钮。

解决方法：将浏览器语言环境设置为 zh-cn 而不是 zh。

控制台中的“ 当前值 ”和“ 新值 ”显示不正确 (6476672)

在管理控制台的本地化版本中，“当前值”和“新值”属性的标签分别错误地显示为 label.current.value 和 label.new.value。

必须根据英文习惯指定策略条件日期 (6390856)

中文语言环境下，策略条件日期格式标签的显示不符合中文习惯。标签显示的日期格式类似英文日期格式。相关字段也接受英文日期格式值。

解决方法：对于每个字段，都遵循字段标签中给定的日期格式示例。

客户机检测无法删除 UTF-8 (5028779)

“客户机检测”功能不能正常工作。Access Manager 7.1 控制台中的更改没有自动传播至浏览器。

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：
  1. 单击“**配置**”选项卡下的“**客户机检测**”。
  2. 单击 "genericHTML" 的“**编辑**”链接。
  3. 在 HTML 选项卡下，单击 "genericHTML" 链接。
  4. 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）。
  5. 保存、注销，然后重新登录。

日志文件中的多字节字符显示为问号 (5014120)

`/var/opt/SUNWam/logs` 目录下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。

文档问题

- 第 38 页中的 “对支持 LDAPv3 插件的角色和过滤角色的说明 (6365196)”
- 第 38 页中的 “对 `AMConfig.properties` 文件中未使用的属性的说明 (6344530)”

- 第 38 页中的 “说明如何启用 XML 加密 (6275563)”

对支持 LDAPv3 插件的角色和过滤角色的说明 (6365196)

应用相应的修补程序后，如果数据存储在 Sun Java System Directory Server 中，则可为 LDAPv3 插件配置角色和过滤角色（修复了问题 ID 6349959）。在 Access Manager 7.1 管理控制台 “LDAPv3 插件支持的类型和操作” 字段的 LDAPv3 配置中，输入以下值：

```
role: read,edit,create,delete
filteredrole: read,edit,create,delete
```

您可以输入上述两个条目中的一条，或两条都输入，这取决于计划在 LDAPv3 中使用的角色和过滤角色。

对 AMConfig.properties 文件中未使用的属性的说明 (6344530)

未使用 AMConfig.properties 文件中的以下属性：

```
com.iplanet.am.directory.host
com.iplanet.am.directory.port
```

说明如何启用 XML 加密 (6275563)

要使用 Bouncy Castle JAR 文件生成传输密钥以启用 Access Manager 或 Federation Manager 的 XML 加密功能，请按以下步骤进行操作：

1. 如果当前使用的 JDK 版本早于 JDK 1.5，从 Bouncy Castle 网站 (http://www.bouncycastle.org/) 下载 Bouncy Castle JCE 提供者。例如，对于 JDK 1.4，应下载 bcprov-jdk14-131.jar 文件。
2. 如果在上一步骤中已下载了 JAR 文件，则将此文件复制到 *jdk_root*/jre/lib/ext 目录下。
3. 对于国内版本的 JDK，则应从 Sun 的网站 (http://java.sun.com) 下载与所用 JDK 版本相对应的 JCE Unlimited Strength Jurisdiction Policy Files。对于 IBM WebSphere，请转到相应的 IBM 网站以下载所需文件。
4. 将已下载的 US_export_policy.jar 文件和 local_policy.jar 文件复制到 *jdk_root*/jre/lib/security 目录下。
5. 如果当前使用的 JDK 版本早于 JDK 1.5，则应编辑 *jdk_root*/jre/lib/security/java.security 文件，将 Bouncy Castle 添加为提供者之一。例如：

   ```
   security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider
   ```

6. 将 AMConfig.properties 文件中的以下属性设置为 true：

   ```
   com.sun.identity.jss.donotInstallAtHighestPriority=true
   ```

7. 重新启动 Access Manager Web 容器。

有关更多信息，参阅问题 ID 5110285（XML 加密需要 Bouncy Castle JAR 文件）。

文档更新

要访问这些文档，参见 Access Manager 7.1 文档集：

http://docs.sun.com/coll/1292.1 及 http://docs.sun.com/coll/1384.1

已将《Technical Note: Deploying Access Manager to an Application Server Cluster》中的第 1 章 “Technical Note: Deploying Access Manager Instances to an Application Server Cluster”的新文档添加到 Access Manager 7 2005Q4 文档集。

Sun Java System Access Manager Policy Agent 2.2 文档集已修订过，以记录新的代理：

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

可再分发的文件

Sun Java System Access Manager 7.1 不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

如果您在使用 Access Manager 或 Sun Java Enterprise System 期间遇到问题，请通过以下方式与 Sun 客户支持部门联系：

- Sun 支持资源 (SunSolve) 服务，网址：http://sunsolve.sun.com/。

  此站点上有一些链接，通过这些链接可以访问知识库、联机支持中心和 Product Tracker，还可了解维护程序以及用于联系支持部门的电话。
- 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
- 用于再现问题的详细步骤
- 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。要分享您的意见，请转至 http://docs.sun.com/，然后单击 "Send Comments"（发送意见）。

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 Access Manager 发行说明的文件号码是 820-0365。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 819-4683-13，文件标题为《Sun Java System Access Manager 7.1 Release Notes》。

其他 Sun 资源

可在以下位置找到关于 Access Manager 的有用信息和资源：

- Sun Java Enterprise System 文档：http://docs.sun.com/prod/entsys.05q4 及 http://docs.sun.com/prod/entsys.05q4?l=zh
- Sun 服务：http://www.sun.com/service/consulting/
- 软件产品和服务：http://wwws.sun.com/software/
- 支持资源：http://sunsolve.sun.com/
- 开发者信息：http://developers.sun.com/
- Sun 开发者支持服务：http://www.sun.com/developers/support/

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。

相关的第三方 Web 站点

本文档引用第三方 URL，并提供其他相关信息。

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、产品或其他资料，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。