Sun Java System Access Manager 7 2005Q4 发行说明

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

文件号码 819–3475
2008 年 8 月 19 日

080908@20795

目录

Sun Java System Access Manager 7 2005Q4 发行说明

2008 年 8 月 19 日

文件号码 819-3475

Sun Java™ System Access Manager (Access Manager) 7 2005Q4 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 的新功能和已知问题及其解决方法（如果可用）。在安装与使用此发行版之前请先阅读本文档。

有关此版本发行说明的信息，参见第 6 页中的 “修订历史记录”。

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。

目录

Access Manager 7 2005Q4 发行说明包含以下内容：

修订历史记录

下表显示 Access Manager 7 2005Q4 发行说明修订历史记录。

表 1 修订历史记录

日期	更改说明
2008 年 8 月 19 日	第 9 页中的 “Access Manager 7 2005Q4 修补程序发行版” 一节中添加了关于适用于 Windows 和 HP-UX 系统的修补程序 7 的信息。
2008 年 5 月 12 日	■ 第 9 页中的 “Access Manager 7 2005Q4 修补程序发行版” 一节中添加了关于修补程序 7 的信息。 ■ 添加了第 63 页中的 “系统虚拟化支持” 一节。
2007 年 10 月 16 日	此次修订中包含以下更改： ■ 第 9 页中的 “Access Manager 7 2005Q4 修补程序发行版” 一节中添加了关于修补程序 6 的信息。 ■ 更新了第 39 页中的 “CR# 6522720：在 Windows 和 HP-UX 系统上，无法在控制台联机帮助中搜索多字节字符” 。修补程序 6 在 Windows 系统上修复了该问题。但是，HP-UX 系统上仍然存在该问题。
2007 年 7 月 10 日	此次修订中包含以下更改： ■ 第 9 页中的 “Access Manager 7 2005Q4 修补程序发行版” 一节中添加了关于适用于 HP-UX 系统的修补程序 126371-05 的信息。 ■ 添加了以下新问题：第 77 页中的 “当 Access Manager 指向 Directory Proxy 时，空属性 LDAP 搜索返回错误 (6357975)” 。
2007 年 3 月 16 日	此次修订中包含以下更改： ■ 第 9 页中的 “Access Manager 7 2005Q4 修补程序发行版” 一节中添加了关于修补程序 5 的信息。 ■ 第 85 页中的 “文档问题” 下添加了说明和新信息。 ■ 根据审查者的意见和变动请求 (Change Request, CR) 进行了各种技术性和编辑上的更改。

表 1 修订历史记录 （续）

日期	更改说明
2006 年 10 月 30 日	第 9 页中的 “Access Manager 7 2005Q4 修补程序发行版” 一节包括以下更改： ■ 添加了关于修补程序 4 的信息。 ■ 修正了 *AccessManager-base* 使用的不一致。 ■ 修订了 第 47 页中的 “CR# 6440651：Cookie 重放需要 `com.sun.identity.session.resetLBCookie` 属性” 的说明。
2006 年 8 月 25 日	第 9 页中的 “Access Manager 7 2005Q4 修补程序发行版” 一节包括以下更改： ■ 添加了关于修补程序 3 的信息。 ■ 修订并添加了有关修补程序 1 和 2 的信息。

2006 年 5 月 25 日	此次修订中包含以下更改：
	■ 新添加了第 50 页中的 “Access Manager 7 2005Q4 修补程序 2” 一节。
	■ 表 4 中添加了关于 HP-UX 和 Microsoft Windows 平台的支持的信息。
	■ 在第 85 页中的 “文档问题” 中添加了以下问题：
	  ■ 第 89 页中的 “发行说明中为某些已知问题提供的解决方法有错 (6422907)”
	  ■ 第 89 页中的 “对 `AMConfig.properties` 中的 `com.iplanet.am.session.protectedPropertiesList` 的说明 (6351192)”

2006 年 2 月 9 日	修订了第 91 页中的 “文档更新”，列出了自初始版发行以来已发布的新的和已修订的 Access Manager 7 2005Q4 文档。

2006 年 2 月 7 日	此次修订中包含以下更改：
	■ 在第 65 页中的 “已知问题和限制” 中添加了以下问题：
	  ■ 第 68 页中的 “在单独的机器上安装 Access Manager 和 Directory Server 时，没有初始化验证服务 (6229897)”
	  ■ 第 69 页中的 “Access Manager `amupgrade` 脚本不会删除本地化软件包 (6378444)”
	■ 更新了第 91 页中的 “文档更新” 一节。

表 1 修订历史记录 （续）

日期	更改说明
2006 年 1 月18 日	此次修订中包含以下更改： ■ 新添加了第 54 页中的 “Access Manager 7 2005Q4 修补程序 1” 一节。 ■ 整理了第 58 页中的 “分布式验证” 的说明，使之更为清晰。 ■ 在第 61 页中的 “硬件和软件要求” 中详细阐明了对 Solaris 10 区域的支持，以及所添加的对 AMD64 平台上 Solaris 10 OS 的支持。 ■ 在第 65 页中的 “已知问题和限制” 中添加了以下问题： ■ 第 74 页中的 “在 IBM WebSphere 中使用 RSA 密钥时，URL 签名失败 (6271087)” ■ 第 81 页中的 “在 Application Server 上运行 Access Manager 时出现 JVM 问题 (6223676)” ■ 第 82 页中的 “运行 Web 服务范例时返回 “未找到资源提供” (6359900)” ■ 第 67 页中的 “应用修补程序 1 后，`/tmp/amsilent` 文件将允许所有用户进行读取操作 (6370691)” ■ 第 71 页中的 “数据迁移后添加 `ContainerDefaultTemplateRole` 属性 (4677779)” ■ 第 89 页中的 “对支持 LDAPv3 插件的角色和过滤角色的说明 (6365196)” ■ 第 90 页中的 “对 `AMConfig.properties` 文件中未使用的属性的说明 (6344530)” ■ 第 90 页中的 “说明如何启用 XML 加密 (6275563)” ■ 新添加了第 91 页中的 “文档更新” 一节。
2005 年 11 月 8 日	修订了所支持 LDAP 版本 3 (LDAP v3) 兼容库的第 56 页中的 “身份库” 。
2005 年 10 月 3 日	初始版。
2005 年 6 月 30 日	Beta 版。

关于 Sun Java System Access Manager 7 2005Q4

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) 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。

Access Manager 7 2005Q4 修补程序发行版

可从 SunSolve Online 找到可供下载的 Access Manager 7 2005Q4 修补程序的最新版本，网址为：`http://sunsolve.sun.com`。最新的修补程序 ID 是：

- 基于 SPARC® 的系统上的 Solaris™ 操作系统 (Solaris OS)：**120954-07**
- x86 平台上的 Solaris OS：**120955-07**
- Linux 系统：**120956-07**
- Microsoft Windows 系统：**124296-07**
- HP-UX 系统：**126371-07**

注 – Access Manager 7 2005Q4 修补程序是累积的。您可在未安装修补程序 1、2、3、4、5 或 6 的情况下安装修补程序 7。不过，如果您没有安装早期的修补程序，请查阅关于早期修补程序章节中的新功能和问题，以确定是否有适用于您的部署的功能和问题。

有关 Access Manager 7 2005Q4 修补程序的信息包括：

- 第 9 页中的 “Access Manager 7 2005Q4 修补程序 7”
- 第 11 页中的 “安装前注意事项”
- 第 14 页中的 “修补程序安装说明”
- 第 18 页中的 “安装后注意事项”
- 第 21 页中的 “Access Manager 7 2005Q4 修补程序 6”
- 第 25 页中的 “Access Manager 7 2005Q4 修补程序 5”
- 第 39 页中的 “Access Manager 7 2005Q4 修补程序 4”
- 第 41 页中的 “Access Manager 7 2005Q4 修补程序 3”
- 第 50 页中的 “Access Manager 7 2005Q4 修补程序 2”
- 第 54 页中的 “Access Manager 7 2005Q4 修补程序 1”

Access Manager 7 2005Q4 修补程序 7

Access Manager 7 修补程序 7（修订版 07）可修复一系列的问题，其随附的自述文件中列出了具体内容。

修补程序 7 包含以下更改：

- 第 10 页中的 “CR# 6637806：Access Manager 在重新启动后发送无效的应用程序 SSO 令牌给代理”
- 第 10 页中的 “CR# 6612609：如果网络电缆与 Message Queue 服务器的连接断开，则会话故障转移便会发挥作用。”

CR# 6637806：Access Manager 在重新启动后发送无效的应用程序 SSO 令牌给代理

Access Manager 服务器重新启动后，Access Manager 客户机 SDK 现在会发送有意义的异常给代理，所以代理可重新验证其自身以得到新的应用程序会话。此前，在应用 Access Manager 7 2005Q4 修补程序 5 后，Access Manager 客户机 SDK 会在 Access Manager 服务器重新启动后发送无效的应用程序 SSO 令牌到代理。

该问题已通过重复的 CR 6496155 修复。修补程序 7 也提供了（`comp.iplanet.dpro.session.dnRestrictionOnly` 属性）选项以在限制性环境中发送应用程序 SSO 令牌。默认情况下，代理会发送安装代理的服务器的 IP 地址，但是如果要求严格的 DN 检查，则按以下方法在 `AMConfig.properties` 文件中设置此属性：

```
com.iplanet.dpro.session.dnRestrictionOnly=true
```

CR# 6612609：如果网络电缆与 Message Queue 服务器的连接断开，则会话故障转移便会发挥作用。

在会话故障转移部署中，如果每个 Access Manager 实例和 Message Queue 代理安装在相同服务器上，则会话故障转移会在网络电缆与服务器之一的连接断开时发挥作用。默认情况下，Message Queue `imqAddressListBehavior` 连接的出厂属性设置为 `PRIORITY`，这会使 Message Queue 按照地址在代理地址列表中出现的顺序来尝试地址（例如：`localhost:7777,server2:7777,server3:7777`）。如果将属性设置为 `RANDOM`，则 Message Queue 会以随机顺序尝试地址。

要将此属性设置为 RANDOM，请在 `amsessiondb` 脚本中设置以下参数：

```
-DimqAddressListBehavior=RANDOM
```

有关 Message Queue 的 `PRIORITY` 和 `RANDOM` 属性的信息，请参见《Sun Java System Message Queue 3.7 UR1 管理指南》中的“代理地址列表”。

CR# 6570409：负载平衡器后方的交互服务可作为身份提供者正常工作

如果部署中有两台服务器与负载平衡器相连并作为单一身份提供者运行，您必须在 `AMConfig.properties` 文件中设置以下属性：

```
com.sun.identity.liberty.interaction.lbWspRedirectHandler
com.sun.identity.liberty.interaction.trustedWspRedirectHandlers
```

com.sun.identity.liberty.interaction.interactionConfigClass 是目前唯一支持的类。因此，在默认情况下，与 Federation Liberty 捆绑的交互配置类用于访问交互配置参数。

CR# 6545176：在后期验证处理 SPI 插件中可动态设置重定向 URL

现在可在后期验证处理 SPI 插件中为登录成功、登录失败和注销动态设置重定向 URL。如果未执行后期处理插件，则不使用后期处理 SPI 中设置的重定向 URL，而像以前一样执行以其他方式设置的重定向 URL。

有关信息，请参见 com.iplanet.am.samples.authentication.spi.postprocess.ISAuthPostProcessSample.java 范例。

安装前注意事项

- 第 11 页中的 “备份文件”
- 第 13 页中的 “安装和配置 Access Manager”

备份文件

重要 如果当前安装中有自定义的文件，则在安装修补程序之前备份这些文件。安装修补程序后，将备份文件和此修补程序安装的新文件进行比较，以标识出自定义部分。将自定义部分合并到新文件中，然后进行保存。有关如何处理自定义文件的详细信息，阅读以下的信息。

安装修补程序前，也请备份以下文件。

Solaris 系统	■ *AccessManager-base*/SUNWam/bin/amsfo ■ *AccessManager-base*/SUNWam/lib/amsfo.conf ■ /etc/opt/SUNWam/config/xml/template/ 目录中的文件：idRepoService.xml、amSOAPBinding.xml、amDisco.xml、amAuthCert.xml、amAuth.xml、amSession.xml ■ *AccessManager-base*/SUNWam/locale/ 目录中的文件：amConsole.properties、amIdRepoService.properties、amAuthUI.properties、amAuth.properties、amPolicy.properties、amPolicyConfig.properties、amSessionDB.properties、amSOAPBinding.properties、amAdminCLI.properties、amSDK.properties、amAuthLDAP.properties、amSession.properties、amAuthContext.properties、amSAML.properties、amAuthCert.properties
Linux 和 HP-UX 系统	■ *AccessManager-base*/identity/bin/amsfo ■ *AccessManager-base*/identity/lib/amsfo.conf ■ /etc/opt/sun/identity/config/xml/template/ 目录中的文件：idRepoService.xml、amSOAPBinding.xml、amDisco.xml、amAuthCert.xml、amAuth.xml、amSession.xml ■ *AccessManager-base*/identity/locale/ 目录中的文件：amConsole.properties、amIdRepoService.properties、amAuthUI.properties、amAuth.properties、amPolicy.properties、amPolicyConfig.properties、amSessionDB.properties、amSOAPBinding.properties、amAdminCLI.properties、amSDK.properties、amAuthLDAP.properties、amSession.properties、amAuthContext.properties、amSAML.properties、amAuthCert.properties

Windows 系统	■ *AccessManager-base*\identity\setup\AMConfigurator.properties ■ *AccessManager-base*\identity\bin\amsfo ■ *AccessManager-base*\identity\lib\amsfo.conf ■ *AccessManager-base*\identity\config\xml\template 目录中的文件： idRepoService.xml、amSOAPBinding.xml、amDisco.xml、amAuthCert.xml、amAuth.xml、amSession.xml ■ *AccessManager-base*\identity\locale 目录中的文件： amConsole.properties、amIdRepoService.properties、amAuthUI.properties、amAuth.properties、amPolicy.properties、amPolicyConfig.properties、amSessionDB.properties、amSOAPBinding.properties、amAdminCLI.properties、amSDK.properties、amAuthLDAP.properties、amSession.properties、amAuthContext.properties、amSAML.properties、amAuthCert.properties

AccessManager-base 是基安装目录。默认的基安装目录取决于平台：

- Solaris 系统：/opt
- Linux 和 HP-UX 系统：/opt/sun
- Windows 系统：*javaes-install-directory*\AccessManager。例如：C:\Program Files\Sun\AccessManager

安装和配置 Access Manager

本文档中描述的 Access Manager 修补程序不会安装 Access Manager。安装修补程序前，服务器上必须安装有 Access Manager 7 2005Q4。有关安装的信息，参见《Sun Java Enterprise System 2005Q4 Installation Guide for UNIX》。

如果要在 Windows 系统上安装修补程序，参见《Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows》。

您还应当熟悉如何运行 amconfig 脚本来部署、重新部署和配置 Access Manager，如《Sun Java System Access Manager 7 2005Q4 管理指南》中的第 1 章 “Access Manager 7 2005Q4 配置脚本”中所述。

有关因此修补程序的推出而过时的 Access Manager 修补程序列表，以及在安装此修补程序之前必须安装的所有修补程序，参阅本修补程序随附的自述文件。

注意 – Access Manager 修补程序（如同任何其他修补程序一样）在应用于生产环境之前，应当在分阶段系统或前期部署系统中进行测试。另外，修补程序的安装程序可能无法正确升级自定义 JSP 文件，所以可能需要在这些文件中进行手动更改，以使 Access Manager 正常运行。

修补程序安装说明

Solaris 系统的修补程序安装说明

在安装 Solaris 修补程序之前，请确保已备份第 11 页中的 “安装前注意事项”中列出的文件。

要在 Solaris 系统上添加或删除修补程序，使用此 OS 提供的 `patchadd` 和 `patchrm` 命令。

patchadd 命令

使用 `patchadd` 命令可在独立计算机系统中安装修补程序。例如：

```
# patchadd /var/spool/patch/120954-07
```

注 – 如果要在 Solaris 10 全局区域上安装 Solaris 修补程序，则调用 `patchadd` 命令，参数为 `-G`。例如：

```
patchadd -G /var/spool/patch/120954-07
```

除非是在只安装了 Access Manager SDK 组件的系统中，否则 `postpatch` 脚本会显示关于重新部署 Access Manager 应用程序的消息。

`postpatch` 脚本会在以下目录中创建 `amsilent` 文件：

- Solaris 系统：*AccessManager-base*`/SUNWam`
- Linux 系统：*AccessManager-base*`/identity`

AccessManager-base 是基安装目录。Solaris 系统的默认基安装目录是 `/opt`，而 Linux 系统则是 `/opt/sun`。

`amsilent` 基于 `amsamplesilent` 文件，但根据系统中的 Access Manager 配置文件设置了某些必需的参数。但是，密码参数包含默认值。根据部署需要，取消注释并修改每个密码参数的值，仔细检查此文件中的其他参数值。

COMMON_DEPLOY_URI 参数（通用域 Web 应用程序的 URI 前缀）也包含一个默认值。如果为该 URI 选择了非默认值，则确保更新该值。否则，使用 amconfig 和修补程序生成的 amsilent 文件重新部署 Web 应用程序将会失败。

然后，运行以下命令（以安装在默认目录下的 Access Manager 为例）：

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

注意 – amsilent 文件包含纯文本格式的敏感数据（例如管理员密码），因此确保适当地保护此文件以进行部署。

运行 amconfig 脚本后，执行 updateschema.sh 脚本以加载 XML 和 LDIF 文件。安装修补程序 7 后，便可在以下目录中找到 updateschema.sh 脚本：

- Solaris SPARC 系统：*patch-home-directory* /120954-07
- Solaris x86 系统：*patch-home-directory*/120955-07

运行 updateschema 脚本后，重新启动 Access Manager 进程。例如：

```
# cd /opt/SUNWam/bin
# ./amserver stop
# ./amserver start
```

然后，重新启动 Access Manager Web 容器。

patchrm 命令

使用 patchrm 命令可从独立计算机系统中删除修补程序。例如：

```
# patchrm 120954-03
```

除非是在只安装了 Access Manager SDK 组件的系统中，否则 backout 脚本会显示一条与 patchadd 命令所显示的消息类似的消息。

删除修补程序后，使用 *AccessManager-base* /SUNWam 目录中的 amsilent 文件重新部署 Access Manager 应用程序，其中，*AccessManager-base* 是基安装目录。Solaris 系统的默认基安装目录是 /opt。

根据部署需要，设置 amsilent 文件中的参数。

然后运行以下命令（以将 Access Manager 安装在 Solaris 系统上的默认目录中为例）：

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

有关 patchadd 和 patchrm 命令的其他信息和示例，参见对应的 Solaris **手册**页。

有关详细信息，另请参见第 18 页中的 “安装后注意事项”。

Solaris 10 区域

Solaris 10 操作系统引进了 “区域 (Zone)” 的新概念。因而，patchadd 命令也包含了新的 -G 选项，该选项只将修补程序添加到全局区域。默认情况下，patchadd 命令在需要修补的软件包的 pkginfo 中查找 SUNW_PKG_ALLZONES 变量。但是，对所有 Access Manager 软件包来说，SUNW_PKG_ALLZONES 变量都未设置，并且如果 Access Manager 7 2005Q4 安装于全局区域，则 -G 选项是必需的。如果 Access Manager 7 2005Q4 安装于本地区域，则 patchadd -G 选项没有任何作用。

如果是在 Solaris 系统上安装 Access Manager 7 2005Q4 修补程序，建议使用 -G 选项。例如：

```
# patchadd -G AM7_patch_dir
```

与此类似，如果 Access Manager 安装于全局区域，则运行 patchrm 命令时必须使用 -G 选项。例如：

```
# patchrm -G 120954-07
```

Linux 系统的修补程序安装说明

在安装 Linux 修补程序前，确保已备份第 11 页中的 “安装前注意事项”中列出的文件。

installpatch 可在独立的 Linux 系统中安装修补程序。例如：

```
# ./installpatch
```

postpatch 脚本输出的消息类似于 Solaris 系统中的消息。但是，Linux 系统中回退修补程序的过程与 Solaris 系统不同。没有回退 Linux 修补程序的通用脚本。如果之前安装了低版本的修补程序，可重新安装该版本，然后遵循修补程序安装后说明，通过运行 amconfig 脚本重新部署 Access Manager 应用程序。

运行 amconfig 脚本后，执行 updateschema.sh 脚本（修补程序 5 及更高版本）以加载 XML 和 LDIF 文件。安装修补程序 7 后，便可在 *patch-home-directory*/120956-07/scripts 目录中找到 updateschema.sh 脚本。

运行 amconfig 和 updateschema.sh 脚本后，重新启动 Access Manager Web 容器。

如果修补程序安装在 Access Manager 7 2005Q4 RTM 发行版上，而您想要删除修补程序并将系统恢复到 RTM 状态，则必须使用 reinstallRTM 脚本重新安装 Access Manager RTM 软件包。此脚本使用 Access Manager RTM RPM 存储位置的路径，并在已修补的 RPM 基础上覆盖安装 RTM RPM。例如：

```
# ./scripts/reinstallRTM path_of_AM7_RTM_RPM_directory
```

运行 reinstallRTM 脚本后，通过运行 amconfig 脚本来重新部署 Access Manager 应用程序并重新启动 Web 容器。

有关详细信息，另请参见第 18 页中的 “安装后注意事项”。

Windows 系统的修补程序安装说明

安装 Windows 修补程序的要求包括：

- 必须在 Windows 系统上安装 Access Manager 7 2005Q4。有关安装的信息，参见《Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows》。
- 要运行修补程序脚本，Windows 系统上必需安装 ActivePerl 5.8（或更高版本）。

安装 Windows 修补程序

在安装 Windows 修补程序之前，确保已备份第 11 页中的 “安装前注意事项”中列出的文件。

输入指向修补程序脚本的基目录路径时，使用反斜线 (\)。例如：c:\sun

要安装 Windows 修补程序：

1. 以管理员组成员的身份登录到 Windows 系统。
2. 创建一个目录用于下载和解压缩 Windows 修补程序文件。例如：AM7p7
3. 将 124296-07.zip 文件下载并解压缩到上一步所创建的目录中。
4. 停止所有 Java ES 2005Q4 服务。
5. 运行 AM7p7\scripts\prepatch.pl 脚本。
6. 运行 AM7p7\124296-07.exe 以安装修补程序。
7. 运行 AM7p7\scripts\postpatch.pl 脚本。
8. 重新启动 Java ES 2005Q4 服务。
9. 重新部署 Access Manager 应用程序。有关详细信息，请参见第 18 页中的 “安装后注意事项”。
10. 运行 AM7p7\scripts\updateschema.pl 脚本以更新 Directory Server 服务模式。脚本会验证您的输入内容，然后加载文件。脚本还会写入以下日志文件：

    javaes-install-directory\AccessManager\AM70Patch-upgrade-schema- *timestamp*
11. 重新启动 Java ES 2005Q4 服务。

回退 Windows 修补程序

要回退 Windows 修补程序：

1. 以管理员组成员的身份登录到 Windows 系统。
2. 运行 Uninstall_124296-07.bat 文件。

3. 运行 `AM7p7\scripts\postbackout.pl` 脚本。
4. 重新部署 Access Manager 应用程序。
5. 重新启动 Java ES 2005Q4 服务。

注意：如果您回退修补程序，不会从 Directory Server 中删除由 `AM7p7\scripts\updateschema.pl` 脚本添加的模式更改。不过，您不需要手动删除这些模式更改，因为它们并不会在回退修补程序后影响 Access Manager 的功能性和可用性。

HP-UX 系统的修补程序安装说明

要安装或删除 HP-UX 修补程序，使用 `swinstall` 和 `swremove` 命令。例如，可使用以下命令在独立系统上安装修补程序：

```
# swinstall /var/spool/patch/126371-07
```

或者使用以下命令删除独立系统上的修补程序：

```
# swremove 126371-07
```

有关 `swinstall` 和 `swremove` 命令的信息，参阅 `swinstall` 和 `swremove` 手册页。

安装或删除修补程序后，您必须按照第 18 页中的 “安装后注意事项”一节中所述来重新部署 Access Manager 应用程序。

重新部署 Access Manager 应用程序后，执行 `updateschema.sh` 脚本（修补程序 5 及更高版本）以加载 XML 和 LDIF 文件。安装修补程序 7 后，便可在 *patch-home-directory*`/120956-07/scripts` 目录中找到 `updateschema.sh` 脚本。运行 `amconfig` 和 `updateschema.sh` 脚本后，重新启动 Access Manager Web 容器。

注意：如果删除修补程序，不会从 Directory Server 中删除由 `updateschema.sh` 脚本添加的模式更改。不过，您不需要手动删除这些模式更改，因为它们并不会在删除修补程序后影响 Access Manager 的功能性和可用性。

有关在 HP-UX 系统上部署 Access Manager 的详细信息，参见《Sun Java System Access Manager 7 2005Q4 Release Notes for HP-UX》。

安装后注意事项

安装 Access Manager 7 2005Q4 修补程序后，应注意的事项包括：

CR# 6254355 ： Access Manager 修补程序在 postpatch 脚本中不会部署 Access Manager 应用程序

修补程序的安装程序可能不会保留某些自定义 WAR 文件，而是用非自定义版本文件替换它们。为帮助标识 WAR 文件的自定义内容以及随后手动更新这些内容，请参考下列步骤 。

在以下示例中，*AccessManager-base* 是基安装目录。Solaris 系统的默认基安装目录是 `/opt`，而 Linux 系统则是 `/opt/sun`。

在 Windows 系统上，*AccessManager-base* 是 *javaes-install-directory*`\AccessManager`。例如 ： `C:\Program Files\Sun\AccessManager`

修补的 WAR 文件有 :

- `console.war`
- `password.war`
- `services.war`

这些文件位于 *AccessManager-base*`/SUNWam`（Solaris 系统）和 *AccessManager-base*`/identity`（Linux 系统）。

在 Windows 系统上 : 修补后的 WAR 文件位于 *AccessManager-base*`\`。

WAR 文件中可更改的内容包括 :

- 属性文件 :
  - Solaris 系统 : *AccessManager-base*`/SUNWam/locale/*.properties`
  - Linux 系统 : *AccessManager-base*`/identity/locale/*.properties`
  - Windows 系统 : *AccessManager-base*`\locale\*.properties`
- 标记库描述符 :
  - Solaris 系统 : *AccessManager-base*`/SUNWam/web-src/applications/WEB-INF/*.tld`
  - Linux 系统 : *AccessManager-base*`/identity/web-src/applications/WEB-INF/*.tld`
  - Windows 系统 : *AccessManager-base*`\web-src\applications\WEB-INF\*.tld`
- `web.xml` 文件以及用于构建它的文件 (`WEB-INF/web.xml` 和 `WEB-INF/*.xml`)
- 应用程序特定文件 : JSP (`*.jsp`) 文件，图像 (`*.gif`) 文件和定义背景颜色、字体大小等的样式表 (`*.css`) 文件

要确保所有自定义更改都被保留，遵循以下这些步骤。在更改文件之前，总是首先备份。

1. 安装修补程序。
2. 将 WAR 文件解压缩到临时目录。例如，将 Access Manager 安装在 Solaris 系统上的默认目录中时 :

```
# cd temporary-directory
# jar -xvf /opt/SUNWam/console.war
# jar -xvf /opt/SUNWam/services.war
# jar -xvf /opt/SUNWam/password.war
```

3. 检查解压缩后的文件，查看修补程序的安装程序是否对自定义文件进行了任何更改，然后在临时目录中向更改过的文件手动添加原来的自定义更改。对于 *AccessManager-base*/web-src/ 目录下您所修改过的文件，若修补的 WAR 文件中不包含这些文件，则无需重新进行更改。
4. 用修改后的文件更新 WAR 文件。例如，将 Access Manager 安装在 Solaris 系统上的默认目录中时：

   ```
   # cd temporary-directory
   # jar -uvf /opt/SUNWam/console.war $path/$modified file
   # jar -uvf /opt/SUNWam/services.war $path/$modified file
   # jar -uvf /opt/SUNWam/password.war $path/$modified file
   ```

   例如，对步骤 2-4：

   ```
   # mkdir /tmp/war.tmp
   # cd /tmp/war.tmp
   # jar -xvf /opt/SUNWam/services.war
   # vi index.html
   # jar -uvf /opt/SUNWam/services.war index.html
   ```

5. 重新使用修补程序生成的无提示配置文件 (amsilent) 或者根据 amsamplesilent 模板文件创建一个新的无提示配置文件，然后在文件中设置适当的配置变量，包括：
   - DEPLOY_LEVEL=21
   - DIRECTORY_MODE=5
   - DS_DIRMGRPASSWD、ADMINPASSWD 和 AMLDAPUSERPASSWD 的密码
   - Access Manager Web 容器变量

   在 Windows 系统上，重新使用 postpatch.pl 脚本生成的无提示配置文件 (amsilent)，并确保 *AccessManager-base*\setup\AMConfigurator.properties-tmp 具有有效值。然后将此文件重命名为 *AccessManager-base* \setup\AMConfigurator.properties。

   有关 Web 容器变量的详细信息，参见 amsamplesilent 文件。在 Solaris 系统中，此文件位于 /opt/SUNWam/bin 目录下，在 Linux 系统中，此文件位于 /opt/sun/identity/bin 目录下。

   在 Windows 系统上，配置文件是 *AccessManager-base*\setup\AMConfigurator.properties。
6. 按如下所示运行 amconfig 脚本。运行 amconfig 前，必须运行 Directory Server 和 Access Manager Web 容器。例如，要在 Access Manager 安装于默认基安装目录的 Solaris 系统上运行 amconfig：

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

7. 运行 amconfig 脚本后，重新启动 Access Manager 进程。例如：

```
# cd /opt/SUNWam/bin
# ./amserver stop
# ./amserver start
```

8. 确保所有的自定义 JSP 文件位于 *AccessManager-base*/SUNWam/web-src/ 目录（Solaris 系统）或 *AccessManager-base* /identity/web-src/ 目录（Linux 系统）下的适当子目录中，并且已备份所有的自定义文件。

   在 Windows 系统上，文件位于 *AccessManager-base*\web-src\。

9. 重新启动 Access Manager Web 容器。

有关运行 amconfig 脚本的详细信息，参见：《Sun Java System Access Manager 7 2005Q4 管理指南》中的第 1 章 “Access Manager 7 2005Q4 配置脚本”。

CR# 6436409：重新部署分布式验证和客户机 SDK WAR 文件

如果使用分布式验证或者客户机 SDK，则安装修补程序后，重新创建并重新部署分布式验证 WAR 文件和/或客户机 SDK WAR 文件。有关信息，参见以下文档：

- 构建分布式验证 WAR 文件：《Technical Note: Using Access Manager Distributed Authentication》
- 构建客户机 SDK WAR 文件：《Sun Java System Access Manager 7 2005Q4 Developer's Guide》中的“Installing the Client SDK”
- 部署客户机 SDK WAR 文件：《Sun Java System Access Manager 7 2005Q4 Developer's Guide》中的“To Deploy amclientwebapps.war”

Access Manager 7 2005Q4 修补程序 6

Access Manager 7 修补程序 6（修订版 06）可修复一系列问题，其随附的自述文件中列出了具体内容。修补程序 6 还包括以下新功能、问题和文档更新。

修补程序 6 的新增功能

- 第 22 页中的 “Access Manager 支持 JDK 1.5 HttpURLConnection setReadTimeout 方法”
- 第 22 页中的 “主服务器恢复后，Access Manager SDK 会回退至主 Directory Server”
- 第 23 页中的 “多个 Access Manager 实例会记录到单独的日志文件”
- 第 23 页中的 “Access Manager 7 允许多个 cookie 域”
- 第 24 页中的 “Microsoft IIS 6.0 后期验证插件支持 SharePoint Server”
- 第 24 页中的 “Access Manager 支持 Internet Explorer 7”

修补程序 6 的已知问题和限制

- 第 24 页中的 “CR# 6379325 在会话故障转移时访问控制台会抛出空指针异常”
- 第 25 页中的 “CR# 6508103：在 Windows 上，单击 “管理控制台” 中的 “帮助” 会返回应用程序错误”
- 第 25 页中的 “CR# 6564877：Access Manager 7 修补程序安装覆写 SAML v2 文件”

注 – 在安装修补程序 6 之前，建议先升级或修补以下组件：

- 如果使用的是 Sun Java System Web Server 6.1 SP5 或更早的版本，请升级到 Web Server 6.1 SP7，可从以下站点下载：

  `http://www.sun.com/download/products.xml?id=45c90ca9`

  遵循《Sun Java System Web Server 6.1 SP7 Release Notes》中的“Upgrade”。
- 从 SunSolve Online 下载并安装适用于 NSS、JSS 和 NSPR 的最新安全修补程序：`http://sunsolve.sun.com`。
  - Solaris 8 SPARC 平台：119209
  - Solaris 8 x86 平台：119210
  - Solaris 9 SPARC 平台：119211
  - Solaris 9 x86 平台：119212
  - Solaris 10 SPARC 平台：119213
  - Solaris 10 x86 和 AMD64 平台：119214
  - Windows 系统：124392
  - HP-UX 系统：124379

Access Manager 支持 JDK 1.5 `HttpURLConnection` `setReadTimeout` 方法

为支持 `setReadTimeout` 方法，`AMConfig.properties` 文件新增以下属性以便于您设置读取超时值：

```
com.sun.identity.url.readTimeout
```

如果 Web 容器使用 JDK 1.5，为避免打开过多 `HttpURLConnection` 而造成服务器挂起，请为此属性设置适当的值以使连接超时。默认值是 30000 毫秒（30 秒）。

如果 `AMConfig.properties` 文件中不存在 `com.sun.identity.url.readTimeout` 属性或该属性设置为空字符串，则 `setReadTimeout` 方法会被忽略。

主服务器恢复后，Access Manager SDK 会回退至主 Directory Server

如果 Sun Java System Directory Server 配置为多主复制 (multi-master replication, MMR)，Access Manager SDK 会在发生故障的主服务器恢复以后回退至主 Directory Server。之前，即使主服务器已恢复，Access Manager SDK 仍继续访问辅助 Directory Server。

为支持这一新行为，Access Manager 的 `AMConfig.properties` 文件中新增了以下属性：

```
com.sun.am.ldap.fallback.sleep.minutes
```

该属性设置了主服务器恢复后，辅助 Directory Server 实例在回退至主服务器之前休眠的时间（以分钟为单位）。默认值为 15 分钟。

com.sun.am.ldap.fallback.sleep.minutes 属性是隐藏的。要将此属性设置为默认值（15 分钟）以外的值，可将其显式地添加到 AMConfig.properties 文件。例如，将该值设置为 7 分钟：

```
com.sun.am.ldap.fallback.sleep.minutes=7
```

重新启动 Access Manager Web 容器才能使新值生效。

多个 Access Manager 实例会记录到单独的日志文件

通过设置 AMConfig.properties 文件中的以下新属性，运行于同一台主机服务器上的多个 Access Manager 实例可记录到不同日志记录子目录下的单独的日志文件中：

```
com.sun.identity.log.logSubdir
```

除非在“管理控制台”中更改默认日志记录目录，否则默认日志记录目录为：

- Solaris 系统：/var/opt/SUNWam/logs
- Linux 和 HP-UX 系统：/var/opt/sun/identity/logs
- Windows 系统：C:\Sun\JavaES5\identity\logs

第一个 Access Manager 实例始终会记录到默认日志记录目录中。要为其他 Access Manager 实例指定不同的日志记录子目录，可在 AMConfig.properties 文件中为其他每个 Access Manager 实例设置 com.sun.identity.log.logSubdir 属性。

例如，如果您有三个实例（am-instance-1、am-instance-2 和 am-instance-3），且全部运行于同一台 Solaris 主机服务器上，可按照以下所示设置属性：

```
com.sun.identity.log.logSubdir=am-instance-2
com.sun.identity.log.logSubdir=am-instance-3
```

com.sun.identity.log.logSubdir 属性是隐藏的。您必须根据需要将此属性显式地添加到 AMConfig.properties 文件中，并重新启动 Access Manager Web 容器使子目录值生效。

然后 Access Manager 实例会记录到以下目录：

```
/var/opt/SUNWam/logs/log-files-for-am-instance-1
/var/opt/SUNWam/logs/am-instance-2/log-files-for-am-instance-2
/var/opt/SUNWam/logs/am-instance-3/log-files-for-am-instance-3
```

Access Manager 7 允许多个 cookie 域

为支持多个 cookie 域，Access Manager 新增了以下属性：

```
com.sun.identity.authentication.setCookieToAllDomains
```

默认值为 true。此新属性是隐藏的。要将此值设置为 false，可将该属性显式地添加到 AMConfig.properties 文件，并重新启动 Access Manager Web 容器。

Microsoft IIS 6.0 后期验证插件支持 SharePoint Server

Microsoft Internet 信息服务 (Internet Information Services, IIS) 6.0 验证插件现在支持 Microsoft Office SharePoint Server。用户可使用用户 ID 或登录名称登录 Access Manager。但是 SharePoint Server 只接受登录名称，导致用户在指定用户 ID 时会出错。

为了允许登录 SharePoint Server，后期验证插件 (ReplayPasswd.java) 现使用以下新属性：

```
com.sun.am.sharepoint_login_attr_name
```

该新属性指示 SharePoint Server 用于验证的用户属性。例如，以下属性指定用于验证的通用名称 (common name, cn)：

```
com.sun.am.sharepoint_login_attr_name=cn
```

后期验证插件读取 com.sun.am.sharepoint_login_attr_name 属性，并从 Directory Server 获取相应的用户属性值。然后该插件设置授权标头以允许用户访问 SharePoint Server。

此属性是隐藏的。要设置该属性，将其显式地添加到 AMConfig.properties 文件，然后重新启动 Access Manager Web 容器使该值生效。

Access Manager 支持 Internet Explorer 7

Access Manager 7 2005Q4 修补程序 6 现在可支持 Microsoft Windows Internet Explorer 7。

CR# 6379325 在会话故障转移时访问控制台会抛出空指针异常

在此情况下，多个 Access Manager 服务器部署为会话故障转移模式且位于负载平衡器后方，而负载平衡器配置为基于 cookie 的粘性请求路由选择。Access Manager 管理员通过负载平衡器访问 Access Manager 控制台。管理员登录到控制台时，会在其中一个 Access Manager 服务器上创建会话。如果该服务器关闭，控制台会话会按照预期故障转移到另一个 Access Manager 服务器。但是，有时管理员会在浏览器或 Web 容器错误日志中遇到间歇性空指针异常。

此问题只在故障转移时影响活动的 Access Manager 控制台会话，而不会影响 Access Manager 服务器的功能。

解决方法：阻止出现这些间歇性空指针异常的方法是：

- 要临时解决此问题，可刷新浏览器，或者先注销，然后重新登录控制台。
- 要永久解决此问题，可在不参与会话故障转移的单独 Access Manager 实例上部署 Access Manager 控制台。

CR# 6508103：在 Windows 上，单击“管理控制台”中的“帮助”会返回应用程序错误

在 Windows 2003 Enterprise Edition 上，如果在非英文语言环境中将 Access Manager 部署在 Sun Java System Application Server 上，单击“领域模式的管理控制台窗口”中的“帮助”会返回应用程序错误。

解决方法：

1. 将 *javaes-install-dir*`\share\lib\jhall.jar` 文件复制到 `%JAVA_HOME%\jre\lib\ext` 目录。

   其中，*javaes-install-dir* 为 Windows 安装目录

2. 重新启动 Application Server 实例。

CR# 6564877：Access Manager 7 修补程序安装覆写 SAML v2 文件

如果安装了 SAML v2 插件，修补程序安装会覆写与 SAML v2 相关的文件，`postpatch` 脚本会显示此消息：

```
The postpatch script detected that the SAML v2 plug-in is installed in your
environment. When you run the amconfig script to redeploy the Access Manager
applications, the script will recreate the amserver.war file and the SAML v2
related files will be lost. Therefore, after you run amconfig, recreate and
redeploy the amserver.war file, as described in the Sun Java System SAML v2
Plug-in for Federation Services User's Guide.
```

解决方法：安装修补程序并运行 `amconfig` 脚本后，为使用 SAML v2 插件的 Federation Manager 或 Access Manager 部署重新创建并重新部署 `amserver.war` 文件。

有关具体步骤，参见《Sun Java System SAML v2 Plug-in for Federation Services User's Guide》中的第 2 章 “Installing the SAML v2 Plug-in for Federation Services”。

Access Manager 7 2005Q4 修补程序 5

Access Manager 7 修补程序 5（修订版 05）可修复一系列的问题，其随附的自述文件中列出了具体内容。修补程序 5 还包括以下新功能、问题和文档更新。

修补程序 5 的新增功能

- 第 27 页中的 “支持 HP-UX 系统”
- 第 27 页中的 “支持 Microsoft Windows 系统”
- 第 27 页中的 “提供新的 `updateschema.sh` 脚本来加载 LDIF 和 XML 文件”
- 第 28 页中的 “支持特定的应用程序闲置会话超时值”
- 第 29 页中的 “可在分布式验证 UI 服务器上部署 CDC Servlet”
- 第 29 页中的 “可在 CDC servlet 重定向至 Access Manager 登录 URL 时指定领域”

修补程序 5 的已知问题和限制

全球化 (Globalization, g11n) 问题

文档更新

支持 HP-UX 系统

修补程序 **126371** 提供对 HP-UX 系统的支持。有关更多信息，请参见：

有关 HP-UX 系统上的安装的信息，参见《Sun Java Enterprise System 2005Q4 Installation Guide for UNIX》。

支持 Microsoft Windows 系统

修补程序 **124296** 提供对 Windows 系统的支持。有关更多信息，请参见：

有关 Windows 系统上的安装的信息，参见《Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows》。

提供新的 `updateschema.sh` 脚本来加载 LDIF 和 XML 文件

修补程序 5（及更高版本）包含 `updateschema.sh` 脚本，从而可加载下列文件以更新 Directory Server 服务模式：

- `AddLDAPFilterCondition.xml`
- `amPolicyConfig_mod_ldfc.xml`
- `accountLockoutData.xml`
- `accountLockout.ldif`
- `idRepoServiceAddAttrSchemaRequest_Cache.xml`
- `wsf1.1_upgrade.xml`
- `amAuth_mod.xml`
- `amAuthCert_mod.xml`

在以前的 Access Manager 修补程序版本中，您需要手动加载这些文件。

要运行 `updateschema.sh` 脚本：

1. 以超级用户 (root) 身份登录或成为超级用户。
2. 转至修补程序目录。
3. 运行该脚本。例如，在 Solaris 系统上：

```
# cd /120954-07
# ./updateschema.sh
```

   在 Windows 系统上，脚本为 updateschema.pl。
4. 在脚本提示时，输入以下各项：
   - Directory Server 主机名和端口号
   - Directory Server 管理员用户 DN 和密码
   - amadmin DN 和密码
5. 脚本会验证您的输入内容，然后加载文件。脚本还会写入以下日志文件：
   - Solaris 系统：/var/opt/SUNWam/logs/AM70Patch.upgrade.schema.*timestamp*
   - Linux 系统：/var/opt/sun/identity/logs/AM70Patch.upgrade.schema.*timestamp*
6. 脚本结束后，重新启动 Access Manager Web 容器。

注意：如果您回退修补程序 5，那么不会从 Directory Server 中删除由 updateschema.sh 脚本添加的模式更改。不过，您不需要手动删除这些模式更改，因为它们并不会在回退修补程序后影响 Access Manager 的功能性和可用性。

支持特定的应用程序闲置会话超时值

修补程序 5 允许不同的应用程序拥有不同的会话闲置超时值。在企业中，某些应用程序可能需要比会话服务中指定的会话闲置超时更短的会话闲置超时值。例如，您在会话服务中将会话的闲置超时值指定为 30 分钟，但 HR 应用程序应在用户闲置超过 10 分钟后即超时。

使用此功能的要求如下：

- 必须将保护应用程序的代理配置为从 Access Manager 强制执行 URL 策略决定。
- 代理必须配置为在自我策略决定高速缓存模式下运行。参见以下属性：
  - 对于 Web 代理：com.sun.am.policy.am.fetch_from_root_resource
  - 对于 J2EE 代理：com.sun.identity.policy.client.cacheMode
- Access Manager AMConfig.properties 文件必须指定策略组件评估顺序以便最后评估“条件”。参见以下属性：

  com.sun.identity.policy.Policy.policy_evaluation_weights
- Access Manager 上的“条件”无法得知代理根据本地高速缓存的决策所允许的应用程序访问。因此，实际的应用程序闲置超时将介于应用程序闲置超时与应用程序闲置超时减去代理高速缓存持续时间之间。

要使用此功能：

- 将“验证模式条件”添加到保护应用程序（这些应用程序需要特定于应用程序的会话闲置超时）的策略中。
- 在“验证模式条件”中指定“应用程序名称”和“超时值”。
- 在所有适用于应用程序资源的策略中使用相同的“应用程序名称”和“超时值”。
- 指定“超时值”（单位为分钟）。如果该值为 0 或大于在会话服务中指定的会话闲置超时值，则忽略该值并应用来自会话服务的超时。

例如，考虑具有如下“验证模式条件”的策略 `http://host.sample.com/hr/*`：

- 验证模式：LDAP
- 应用程序名称：HR
- 超时值：10

如果定义了多个策略来保护 HR 应用程序的资源，则您必须将该“条件”添加到所有策略。

当不同会话中的用户尝试访问 Access Manager 代理所保护的 HR 应用程序时，系统会提示该用户进行 LDAP 模式验证（如果用户尚未通过验证）。

如果用户已通过 LDAP 模式验证，则仅当距上次验证的时间小于 10 分钟或距用户上次访问 HR 应用程序的时间小于 10 分钟时，才允许用户执行访问。否则，系统会再次提示用户进行 LDAP 模式验证以访问应用程序。

可在分布式验证 UI 服务器上部署 CDC Servlet

CDC Servlet 可与分布式验证 UI 服务器在 DMZ 中共存以启用跨域单点登录 (Cross-Domain Single Sign-On, CDSSO)。可将 Access Manager 服务器部署在防火墙之后，所有访问 Access Manager 以实现 CDSSO 的操作均由分布式验证 UI 服务器中的 CDC Servlet 处理。要启用 CDSSO，参阅特定的策略代理文档并执行以下附加步骤：

- 修改代理的 `AMAgent.properties` 文件以指向分布式验证端（客户机）上的 CDC Servlet。例如，对于 Web 代理，更改以下属性：

  ```
  com.sun.am.policy.agents.config.cdcservlet.url=
      http://DAhost.DAdomain:DAport/DISTAUTH_DEPLOY_URI/cdcservlet
  ```

- 在 Access Manager 中，根据需要为需要代理保护的资源定义策略。如果代理位于 `host.example.com:80`，则将资源的策略定义为 `http://host.example.com:80/*`。

可在 CDC servlet 重定向至 Access Manager 登录 URL 时指定领域

现在，您可将领域名称指定给 CDC servlet，这样在重定向至 Access Manager 登录 URL 时，领域名称便会包括在其中，而且用户可登录到特定领域。例如：

```
com.sun.am.policy.agents.config.cdcservlet.url=
    http://lb.example.com/amserver/cdcservlet?org=realm1
```

证书验证可使用 UPN 值来映射用户配置文件

以前，证书验证只使用 subjectDN 中的 dn 组件来映射用户配置文件。现在， Access Manager 允许使用 SubjectAltNameExt 中的用户主体名称 (user principal name, UPN) 值来执行配置文件映射。

在多服务器环境中对注销操作进行后期验证处理

现在，当用户在多服务器环境中从一个与最初登录的服务器不同的服务器注销时，会进行后期验证处理（无论是否配置了会话故障转移）。

SAML 支持新的名称标识符 SPI

SAML 现在支持新的名称标识符服务提供者接口 (service provider interface, SPI)，以便站点可自定义 SAML 声明中的名称标识符。站点可实现新的 NameIdentifierMapper 接口以将用户帐户映射到 SAML 声明主题中的名称标识符。

站点监视的新配置属性

Access Manager 站点监视功能包括以下新属性以允许您指定站点状态检查的行为。

属性	描述
com.sun.identity.urlchecker.invalidate.interval	用于识别停止或非响应站点的时间间隔（单位为毫秒）。 默认值：70000 毫秒（70 秒）。
com.sun.identity.urlchecker.sleep.interval	站点状态检查应休止的时间间隔（单位为毫秒）。 默认值：30000 毫秒（30 秒）。
com.sun.identity.urlchecker.targeturl	用于检查 Access Manager 进程状态的不同目标 URL。 默认值：“/amserver/namingservice”。

修补程序没有将这些属性添加到 AMConfig.properties 文件中。若要以默认值以外的其他值使用这些新属性，请执行下列操作：

1. 将属性及其值添加到 AMConfig.properties 文件。对于策略代理，将这些属性添加到 AMAgents.properties 文件。
2. 重新启动 Access Manager Web 容器以使这些值生效。

用户不必再在验证链中验证两次

考虑以下情况。站点配置一个具有三个 LDAP 模块的验证链。所有模块均设为 SUFFICIENT，并且 iplanet-am-auth-shared-state-enabled 和 iplanet-am-auth-store-shared-state-enabled 选项设为 true。例如：

```
<AttributeValuePair>
   <Value>A-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>B-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>C-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
</AttributeValuePair>
```

修补程序 5 向模块选项添加了新的 iplanet-am-auth-shared-state-behavior-pattern 选项，可能值为以下两者：tryFirstPass（默认值）和 useFirstPass。

为避免用户必须输入两次用户 ID 和密码才能通过验证（如之前的情况所述），对于此链中的所有模块，将此新选项设为 useFirstPass。以前，仅存在于第三个 LDAP 实例中的用户需输入两次用户 ID 和密码才能通过验证。

对性能调节脚本的更改

修补程序 5 包括以下对性能调节脚本的更改：

- 第 31 页中的 “调节脚本支持密码文件”
- 第 32 页中的 “调节脚本从 Directory Server 中删除不必要的 ACI”
- 第 32 页中的 “调节脚本可调节分布式验证 UI 服务器的 Web 容器”
- 第 33 页中的 “单个 amtune-os 脚本可调节 Solaris OS 和 Linux OS”
- 第 33 页中的 “在 Solaris 10 本地区域中调节脚本可以完整执行”
- 第 33 页中的 “Windows 系统可使用调节脚本”
- 第 33 页中的 “Sun Fire T1000 和 T2000 服务器的调节注意事项”

另请参见 第 35 页中的 “CR# 6527663：com.sun.identity.log.resolveHostName 属性的默认值应为 false 而不是 true”。

调节脚本支持密码文件

修补程序 5 允许您在文本文件中为调节脚本指定密码。以前，您只能将密码作为命令行参数输入，这样可能导致安全问题。要使用密码文件，在文件中根据需要设置以下变量：

```
DS_ADMIN_PASSWORD=DirectoryServer-admin-password
AS_ADMIN_PASSWORD=ApplicationServer8-admin-password
```

例如，要调节 Application Server 8：

```
# ./amtune-as8 password-file
```

其中，*password-file* 包含设为 Application Server 8 管理员密码的 `AS_ADMIN_PASSWORD` 。

调节脚本在调用 `ldapmodify`、`ldapsearch`、`db2index` 和 `dsconf` Directory Server 实用程序时使用 `-j` *password-file* 选项。

调节脚本从 Directory Server 中删除不必要的 ACI

如果在“领域模式”下安装 Access Manager 7 2005Q4，则使用委托权限来确定访问权限，因此某些 Directory Server ACI 为不必要。Access Manager 7 2005Q4 修补程序 5 允许您通过 `amtune-prepareDSTuner` 脚本来删除不必要的 ACI。此脚本从 `remacis.ldif` 文件读取 ACI 列表，然后调用 `ldapmodify` 实用程序来删除它们。

可运行 `amtune-prepareDSTuner` 脚本来删除 Solaris、Linux、HP-UX 和 Windows 系统上不必要的 ACI。有关详细信息（包含如何运行该脚本），参见《Technical Note: Sun Java System Access Manager ACI Guide》 。

调节脚本可调节分布式验证 UI 服务器的 Web 容器

在 Web 容器上部署分布式验证 UI 服务器后，可通过运行 Access Manager 调节脚本来调节 Web 容器。以下调节脚本会为各 Web 容器设置 JVM 及其他调节选项 :

表 2 Access Manager Web 容器调节脚本

Web 容器	调节脚本
`amtune-ws61`	Web Server 6.1
`amtune-as7`	Application Server 7
`amtune-as8`	Application Server Enterprise Edition 8.1

要调节分布式验证 UI 服务器的 Web 容器 :

1. 由于 Access Manager 服务器未安装在部署了分布式验证 UI 服务器的系统上，因此从 Access Manager 服务器安装中复制相应的 Web 容器调节脚本（如上表中所示）、`amtune-env` 配置文件和 `amtune-utils` 脚本。如果您想要调节 Solaris 或 Linux 操作系统，则还需复制 `amtune-os` 脚本。
2. 编辑 `amtune-env` 配置文件中的参数以指定 Web 容器和调节选项。要在 REVIEW 模式下运行脚本，请在 `amtune-env` 文件中设置 `AMTUNE_MODE=REVIEW`。
3. 在 REVIEW 模式下运行 Web 容器调节脚本。在 REVIEW 模式下，脚本会根据 `amtune-env` 文件建议调节更改，但不会对部署做任何实际更改。
4. 查看调试日志文件中的调节建议。如有需要，根据本次运行情况对 `amtune-env` 文件执行更改。
5. 要执行调节更改，在 `amtune-env` 文件中设置 `AMTUNE_MODE=CHANGE`。

6. 在 CHANGE 模式下运行调节脚本以对部署执行调节更改。

有关运行调节脚本以调节 Access Manager Web 容器的详细信息，参见《Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide》中的第 2 章 “Access Manager Tuning Scripts”。

单个 amtune-os 脚本可调节 Solaris OS 和 Linux OS

修补程序 5 包括可调节 Solaris OS 和 Linux OS 的单个 amtune-os 脚本。此脚本使用 uname -s 命令来确定 OS 类型。以前，Access Manager 提供单独的 amtune-os 脚本来调节各种 OS。

在 Solaris 10 本地区域中调节脚本可以完整执行

如果 Access Manager 安装在 Solaris 10 本地区域中，则除 amtune-os 以外的所有调节脚本均可在本地区域中运行。在本地区域中，amtune-os 脚本显示一条警告消息，但不调节 OS。接下来，脚本会继续运行您已请求的任何其他调节脚本。以前，在本地区域中，amtune-os 会异常中止，并且不会运行任何您已请求的后续调节脚本。

在 Solaris 10 全局区域中，amtune 脚本会调用 amtune-os 来调节 OS 以及您已请求运行的任何其他脚本。

Windows 系统可使用调节脚本

修补程序 5 包括以下用于 Windows 系统的调节脚本。在 Windows 系统上运行调节脚本与在 Solaris 系统或 Linux 系统上运行脚本类似，但有以下区别：

- Windows 脚本以 Perl 编写并且需要运行 Active Perl 5.8。
- 如果您要调节 Directory Server，在运行 amtune-prepareDSTuner.pl 脚本后，您必须将 amtune-utils.pl、amtune-directory.pl、remacis.ldif 和 amtune-samplepassordfile 文件复制到 Directory Server 系统，因为脚本无法压缩这些文件。
- 没有可调节 Windows 操作系统的脚本。
- 未提供对区域的支持。
- 在运行脚本之前，必须将 amtune-env.pl 文件中的 $BASEDIR 参数设为 Access Manager 安装目录。

Sun Fire T1000 和 T2000 服务器的调节注意事项

如果 Access Manager 安装在 Sun Fire T1000 或 T2000 服务器上，则适用于 Web Server 6.1 和 Application Server 8 的修补程序 5 调节脚本将 JVM GC ParallelGCThreads 参数设为 8：

```
-XX:ParallelGCThreads=8
```

此参数减少垃圾回收线程数，在具备 32 线程处理能力的系统中该线程数量可能会显得不必要的高。不过，如果 32 位虚拟 CPU 计算机（如 Sun Fire T1000 或 T2000 服务器）将所有垃圾回收活动数量最小化，您仍可将该值增加到 16 甚至 20。

同时，对于带有采用 CoolThreads 技术的 CMT 处理器的 Solaris SPARC 系统，建议在 `/etc/opt/SUNWam/config/AMConfig.properties` 文件的结尾处添加以下属性：

```
com.sun.am.concurrencyRate=value
```

默认的 *value* 为 16，但可将此属性设为更低的值，具体取决于 Sun Fire T1000 或 T2000 服务器中的核心数。

IIS 6.0 策略代理中的基本验证

要在 Microsoft Internet 信息服务 (Internet Information Services, IIS) 6.0 中启用基本验证，策略代理必须获得用户名和密码。修补程序 5 包括以下新类，它们可使用用户密码的 DES 加密来启用此功能：

- `DESGenKey.java` 生成用于加密和解密用户密码的唯一密钥。
- `ReplayPasswd.java` 从 `AMConfig.properties` 文件中的 `com.sun.am.replaypasswd.key` 属性中读取加密密钥值，加密密码，然后将其指定给 `sunIdentityUserPassword` 会话属性。

要在 IIS 6.0 中使用基本验证，您必须在 Access Manager 服务器端和 IIS 6.0 策略代理端上执行以下步骤。

在 Access Manager 服务器端：

1. 执行 `DESGenKey.java` 生成唯一的加密密钥来对密码进行加密和解密。在 Solaris 系统上，`DESGenKey.java` 文件位于 `com/sun/identity/common` 目录下，包括在 `/opt/SUNWam/lib` 目录的 `am_sdk.jar` 中。例如，以下命令可生成加密密钥：

   ```
   # cd /opt/SUNWam/lib
   # java -cp am_sdk.jar com.sun.identity.common.DESGenKey
   ```
2. 将从步骤 1 得到的加密密钥值指定给 `AMConfig.properties` 文件中的 `com.sun.am.replaypasswd.key` 属性。
3. 将 `ReplayPasswd.java` 部署为后期验证插件。配置插件时，请使用完整的类名：`com.sun.identity.authentication.spi.ReplayPasswd`。

在 IIS 6.0 策略代理端：

1. 将从服务器端得到的加密密钥值指定给 `AMAgent.properties` 文件中的 `com.sun.am.replaypasswd.key` 属性。Access Manager 服务器和 IIS 6.0 策略代理必须使用相同的加密密钥。
2. 在 IIS 6.0 Manager 中启用基本验证。

IIS 6.0 策略代理从会话响应中读取加密密码，从 com.sun.am.replaypasswd.key 属性解密密码，并设置验证标头使基本验证生效。

有关 IIS 6.0 策略代理的信息，参见《Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0》 。

CR# 6567746：在 HP-UX 系统上，如果超过密码重试次数，Access Manager 修补程序 5 会报告错误的 errorCode 值

当用户帐户被锁定时，如果超过密码重试次数，HP-UX 系统上的 Access Manager 7 2005Q4 修补程序 5 会报告 errorCode = null 而非 errorCode = 107。

解决方法。无。

CR# 6527663：com.sun.identity.log.resolveHostName 属性的默认值应为 false 而不是 true

在运行 amtune-identity 调节脚本之前，建议将以下设为 false 的属性添加到 AMConfig.properties 文件中：

```
com.sun.identity.log.resolveHostName=false
```

值为 false 可最小化解析主机名的影响，从而提升性能。不过，如果要在 amAuthentication.access 日志中显示客户机的主机名，则将该值设为 true。

CR# 6527528：删除修补程序会留下带明文格式 amldapuser 密码的 XML 文件

如果从 Access Manager 完整服务器安装中删除修补程序 5，则 amAuthLDAP.xml 和 amPolicyConfig.xml 文件会包含明文格式的 amldapuser 密码。根据平台的不同，这些文件会位于以下目录：

- Solaris 系统：/etc/opt/SUNWam/config/xml
- Linux 和 HP-UX 系统：/etc/opt/sun/identity/config/xml

解决方法：编辑 amAuthLDAP.xml 和 amPolicyConfig.xml 文件并删除明文密码。

CR# 6527516：WebLogic 上的完整服务器要求 JAX-RPC 1.0 JAR 文件与客户机 SDK 进行通信

在 Access Manager 7 2005Q4 修补程序中，Access Manager 用于 BEA WebLogic Server 的配置脚本 (amwl81config) 将 JAX-RPC 1.1 JAR 文件添加到 WebLogic 实例的 classpath 中。尽管此修改对 Sun Java System Portal Server 之类的产品有益，但是部署在 WebLogic Server 上的完整服务器安装 (DEPLOY_LEVEL=1) 将无法与客户机 SDK 安装进行通信，并且随后会发生异常。

如果 Access Manager 7 2005Q4 服务器安装在 BEA WebLogic Server 上，则 `startWebLogic.sh` 脚本中的 `CLASSPATH` 必须设为 JAX-RPC 1.0 JAR 文件所在的位置后，它才能与 Access Manager 客户机 SDK 进行通信。

解决方法：应用 Access Manager 修补程序之前，在 `startWebLogic.sh` 脚本中设置 `CLASSPATH` 使 WebLogic Server 实例使用 JAX-RPC 1.0 JAR 文件而非 JAX-RPC 1.1 JAR 文件：

1. 在 Access Manager 服务器上，以超级用户身份登录或成为超级用户 (`root`)。
2. 编辑 `startWebLogic.sh` 脚本并将 `CLASSPATH` 替换为使用 JAX-RPC 1.0 JAR 文件。例如：

当前值：

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-spi.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-impl.jar:
```

新值：

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc_1.0/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-ri.jar:
```

其中，*AccessManager-base* 为基安装目录。默认值为 `/opt`（Solaris 系统上）或 `/opt/sun`（Linux 和 HP-UX 系统上）。*AccessManager-package-dir* 是 Access Manager 软件包目录。

5. 重新启动 WebLogic Server 实例。

CR # 6523499：修补程序 5 `amsilent` 文件对于 Linux 系统上的所有用户均为可读

在 Linux 系统上，`postpatch` 脚本会创建具有 644 权限的 `/opt/sun/identity/amsilent` 文件，它允许所有用户的读取访问。

解决方法：在执行 `installpatch` 脚本后，更改 `amsilent` 文件的权限，只允许所有者拥有读取和写入访问权限。例如：

```
# chmod 600 /opt/sun/identity/amsilent
```

CR# 6520326：将修补程序 5 应用到服务器上的第二个 Access Manager 实例会覆写第一个实例的 serverconfig.xml

在这种部署情况中，两个 Access Manager 实例部署在同一主机服务器上，且每个实例位于不同的 Web 容器实例上。然后执行以下步骤：

1. 应用修补程序 5。
2. 修改 amsilent 文件并重新部署第一个 Access Manager 实例。
3. 再次修改第二个 Access Manager 实例的 amsilent，然后重新部署该实例。

如果在 amsilent 文件中 NEW_INSTANCE=false，则第一个 Access Manager 实例的 serverconfig.xml 文件将被来自第二个 Access Manager 实例的信息所覆盖。随后重新启动第一个 Access Manager 实例将失败。根据平台的不同，serverconfig.xml 文件将位于以下目录：

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

解决方法：在部署第二个 Access Manager 时，在 amsilent 文件中设置 NEW_INSTANCE=true。这样第二个 Access Manager 实例的 serverconfig.xml 文件就能更新为正确的信息，而第一个 Access Manager 实例的 serverconfig.xml 文件也不会被覆写。

CR# 6520016：修补程序 5 的仅 SDK 安装会覆写范例 makefile

将修补程序 5 应用到仅安装 SDK 的计算机会覆写范例 makefile。

解决方法：将修补程序 5 应用到仅安装 SDK 的计算机不需要重新配置；不过，如果要使用范例 makefile，请遵循以下步骤来更新范例 makefile 的 LDIF 和属性文件（即执行标记交换）：

1. 运行 amconfig 脚本（DEPLOY_LEVEL=14）来卸载 SDK 和取消配置 Web 容器。
2. 运行 amconfig 脚本（DEPLOY_LEVEL=4）来重新安装 SDK 并重新配置 Web 容器。

CR#6515502：LDAPv3 系统信息库插件不能始终正确处理别名搜索属性

对于大多数搜索，此问题已得到修复。不过，在设置“别名搜索属性”时需谨慎。别名搜索属性的值必须在整个组织内唯一。如果设置了多个别名搜索属性，则有可能出现数据存储库中的一个条目匹配一个属性，而另一个条目匹配另一个属性。在这种情况下，Access Manager 服务器会抛出以下错误：

出现内部验证错误。请与您的系统管理员联系。

解决方法：无

CR# 6515383：分布式验证和 J2EE 代理在同一 Web 容器上不起作用

分布式验证 UI 服务器和 J2EE 策略代理如果安装在同一 Web 容器中则不起作用。

解决方法：创建另一个 Web 容器实例，并在容器的不同实例上部署分布式验证 UI 服务器和 J2EE 策略代理。

CR# 6508103：Application Server 在 Windows 系统上时，联机帮助会返回应用程序错误

如果在 Windows 系统中的 Sun Java System Application Server 上部署 Access Manager，则单击“领域模式”控制台的帮助屏幕左面板中的“帮助”会返回一个应用程序错误。

解决方法：将 *javaes-install-dir*`\share\lib\jhall.jar` 文件复制到 `JAVA_HOME\jre\lib\ext` 目录，然后重新启动 Application Server。

CR# 6507383 和 CR# 6507377：分布式验证要求显式 `goto` URL 参数

如果未指定显式 `goto` URL 参数，则分布式验证 UI 服务器会尝试重定向至 Access Manager 中指定的成功 URL 上的 `goto`。此重定向可能会由于以下原因而失败：

- URL 是相对位置，并且在分布式验证 UI 服务器中没有可用的对应页面
- URL 是绝对位置，并且浏览器无法访问该 URL。

解决方法：始终为分布式验证 UI 服务器指定一个显式 `goto` URL 参数。

CR# 6402167：LDAP JDK 4.18 导致 LDAP客户机/Directory Server 问题

在 Java ES 2005Q4 发行版中，Access Manager 7 2005Q4 是随 LDAP JDK 4.18 一起发行的，从而导致了多个 Access Manager 与 Directory Server 连接问题。

解决方法：应用以下 Sun Java System LDAP Java Development Kit 修补程序之一：

- Solaris OS、SPARC 和 x86 平台：119725-04
- Linux OS：120834-02

这些修补程序可从 SunSolve Online 获取：`http://sunsolve.sun.com`。

CR# 6352135：分布式验证 UI 服务器文件的安装位置不正确

在 Solaris 系统上，Java ES 安装程序将分布式验证 UI 服务器 `Makefile.distAuthUI`、`README.distAuthUI` 和 `amauthdistui.war` 文件安装在错误的位置：`/opt/SUNComm/SUNWam`。

解决方法：将这些文件复制到正确的位置：`/opt/SUNWam`。

注意：任何在修补程序中修复的分布式验证 UI 服务器问题均会进入 `/opt/SUNComm/SUNWam/amauthdistui.war` 文件，因此，无论何时将修补程序应用到 Access Manager 服务器然后重建并部署 WAR 文件时，您还必须将这些文件复制到 `/opt/SUNWam` 目录。

CR# 6522720：在 Windows 和 HP-UX 系统上，无法在控制台联机帮助中搜索多字节字符

在 Windows 或 HP-UX 系统上，如果在使用多字节字符（如日文）的语言环境下安装 Access Manager，则无法在控制台联机帮助中使用通过多字节字符输入的关键字进行搜索。

解决方法：无

修补程序 6 更新：Access Manager 7 2005Q4 修补程序 6 在 Windows 系统上修复了该问题。但是，HP-UX 系统上仍然存在该问题。

CR# 6524251：在 Windows 系统上配置 Access Manager 的过程中，输出消息中的多字节字符为乱码

如果在 Windows 系统上安装使用多字节字符的语言环境（例如日文或中文）的 Access Manager，则在 Access Manager 配置过程中，终端窗口中的输出消息为乱码。

解决方法：无，但此问题不影响配置本身。

CR# 6526940：在 Windows 系统的非英文语言环境中安装修补程序 5 时会出现属性键，而不是消息文本

如果在 Windows 系统的非英文语言环境中安装修补程序 5 (124296-05)，则安装面板中的某些字符串将显示为属性键而非实际的消息文本。属性键的示例为 `PRODUCT_NAME`、`JES_Patch_FinishPanel_Text1` 和 `JES_Patch_FinishPanel_Text2`。

解决方法：无

CR# 6513653：与 com.iplanet.am.session.purgedelay 属性设置相关的问题

Access Manager `amtune` 脚本将 `com.iplanet.am.session.purgedelay` 属性设为 1，以便允许尽可能多的 Access Manager 会话。此属性指定清除会话操作延迟的分钟数。不过，对于诸如 Sun Java System Portal Server 之类的客户机，值为 1 可能还不够。

解决方法：运行 `amtune` 脚本后重置 `com.iplanet.am.session.purgedelay` 属性：

1. 在 `AMConfig.properties` 文件中，将该属性设为新值。例如：

   ```
   com.iplanet.am.session.purgedelay=5
   ```

2. 重新启动 Access Manager Web 容器以使新值生效。

Access Manager 7 2005Q4 修补程序 4

Access Manager 7 2005Q4 修补程序 4（修订版 04）修补了以下问题：

- CR# 6463796：禁用 genericHTML 的 iPlanetAMClientDetection 服务阻止访问任何 Access Manager HTML 页面
- CR# 6463779：分布式验证的 amProfile_Client 和 Access Manager 服务器的 amProfile_Server 中充满了无害的异常
- CR# 6463730：goto 和 gx-charset 参数存在跨站脚本 (Cross-site scripting, XSS) 漏洞
- CR# 6435889：由于未设置 RestrictedTokenContext，方法 Session.getSession 失败

修补程序 4 的已知问题和限制

- 第 40 页中的 “CR# 6470055：分布式验证 UI 服务器性能改进”
- 第 40 页中的 “CR# 6455079：密码重置服务在密码更改时报告通知错误”

CR# 6470055：分布式验证 UI 服务器性能改进

要提高分布式验证 UI 服务器用户在读取、搜索和比较用户属性方面的性能，请执行以下步骤：

1. 在 Makefile.distAuthUI 文件中，将应用程序用户名从 anonymous 更改为其他用户。例如：

```
APPLICATION_USERNAME=user1
```

2. 在 Directory Server 中，添加新用户（本例中为 user1）和 ACI 以允许读取、搜索和比较用户属性。以下示例添加新的 ACI：

```
dn:ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com
changetype:modify add:aci
aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com")
(targetattr = *")(version 3.0;
acl "SunAM client data access to a Distributed Auth App User";
allow (read, search, compare)
userdn =  "ldap:///uid=user1,ou=people,dc=example,dc=com";)
```

CR# 6455079：密码重置服务在密码更改时报告通知错误

更改密码后，Access Manager 使用无限定的发件人名称 Identity-Server 来提交电子邮件通知，这会导致 amPasswordReset 日志中出现错误条目。例如：

```
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“从”地址以包括 amPasswordResetModuleMsgs.properties 文件中主机服务器的全限定域名：

1. 更改“从”地址标签。例如：

```
fromAddress.label=<Identity-Server@amhost.example.com>
```

2. 更改 `lockOutEmailFrom` 属性以确保锁定通知使用正确的“从”地址。例如：

```
lockOutEmailFrom=<Identity-Server@amhost.example.com>
```

`amPasswordResetModuleMsgs.properties` 文件位于 *AccessManager-base*`/SUNWam/locale` 目录（Solaris 系统）和 *AccessManager-base*`/identity/locale` 目录（Linux 系统）。

AccessManager-base 是基安装目录。Solaris 系统的默认基安装目录是 `/opt`，而 Linux 系统的默认基安装目录是 `/opt/sun`。

Access Manager 7 2005Q4 修补程序 3

Access Manager 7 修补程序 3（修订版 03）可修复一系列的问题，其随附的自述文件中列出了具体内容。修补程序 3 还具有以下新增功能和已知问题：

修补程序 3 的新增功能

- 第 42 页中的 “站点监视的新配置属性”
- 第 43 页中的 “Liberty Identity Web Services Framework (ID-WSF) 1.1 支持”

修补程序 3 的已知问题和限制

- 第 43 页中的 “CR# 6463779 分布式验证的 `amProfile_Client` 日志和 Access Manager 服务器的 `amProfile_Server` 日志中充满了无害的异常”
- 第 44 页中的 “CR# 6460974 默认分布式验证应用程序用户不应该是 `amadmin`”
- 第 44 页中的 “CR# 6460576 控制台联机帮助的“过滤的角色”下，没有“用户服务”的链接”
- 第 44 页中的 “CR# 6460085 运行 `reinstallRTM` 并重新部署 Web 应用程序之后，无法访问 WebSphere 上的服务器”
- 第 45 页中的 “CR# 6455757：升级前必须将 `sunISManagerOrganization` 标记类添加到组织中”
- 第 45 页中的 “CR# 6454489：Access Manager 7 2005Q4 修补程序 2 升级导致控制台“当前会话”选项卡中出错”
- 第 46 页中的 “CR# 6452320：在客户机 SDK 中使用轮询时抛出异常”
- 第 46 页中的 “CR# 6442905 已验证用户的 `SSOToken` 可能会在无意中透露给流氓站点”
- 第 47 页中的 “CR# 6441918：站点监视时间间隔和超时属性”
- 第 47 页中的 “CR# 6440697：分布式验证应以非 amadmin 用户身份运行”
- 第 47 页中的 “CR# 6440695：包含负载平衡器的分布式验证 UI 服务器”
- 第 47 页中的 “CR# 6440651：Cookie 重放需要 `com.sun.identity.session.resetLBCookie` 属性”
- 第 48 页中的 “CR# 6440648：`com.iplanet.am.lbcookie.name` 属性假定默认值为 `amlbcookie`”

- 第 48 页中的 “CR# 6440641：com.iplanet.am.lbcookie.value 属性已过时”
- 第 48 页中的 “CR# 6429610：在 ID-FF SSO 使用案例中无法创建 SSO 令牌”
- 第 48 页中的 “CR# 6389564：在 Access Manager 登录期间，会在 LDAP v3 数据存储库中对用户的角色成员资格进行重复不断的查询”
- 第 48 页中的 “CR# 6385185：验证模块必须能够覆盖 "goto" URL，并指定另一不同的 URL”
- 第 49 页中的 “CR# 6385184：当 SSO 令牌仍处于无效状态时，从自定义验证模块重定向”
- 第 50 页中的 “CR# 6324056：使用辅件配置文件时联合失败”

站点监视的新配置属性

Access Manager 站点监视功能包括以下新属性：

属性	描述
com.sun.identity.sitemonitor.interval	站点监视的间隔时间（单位为毫秒）。站点监视功能会在指定的时间间隔内检查每个站点的可用性。默认值：60000 毫秒（1 分钟）。
com.sun.identity.sitemonitor.timeout	站点可用性检查的超时时间（单位为毫秒）。站点监视功能会在指定的超时时间内等待站点的响应。默认值：5000 毫秒（5 秒）。

修补程序没有将这些属性添加到 AMConfig.properties 文件中。若要以默认值以外的其他值使用这些新属性，请执行下列操作：

1. 将属性及其值添加到位于以下目录的 AMConfig.properties 文件中，具体目录取决于您所使用的平台：
   - Solaris 系统：/etc/opt/SUNWam/config
   - Linux 系统：/etc/opt/sun/identity/config

   对于策略代理，将这些属性添加到 AMAgents.properties 文件。
2. 重新启动 Access Manager Web 容器以使这些值生效。

自定义实现。另外，com.sun.identity.sitemonitor.SiteStatusCheck 类允许您使用以下接口自定义用于检查站点可用性的实现：

```
package com.iplanet.services.naming.WebtopNaming$SiteStatusCheck
```

每个实现类均必须使用 doCheckSiteStatus 方法。

```
public interface SiteStatusCheck {
public boolean doCheckSiteStatus(URL siteurl);
}
```

Liberty Identity Web Services Framework (ID-WSF) 1.1 支持

Access Manager 7 修补程序 3 中的 ID-WSF 默认版本为 WSF1.1。除示例需使用新的安全机制外，触发 ID-WSF 不需要单独的配置。用于 ID-WSF1.1 的新安全机制为：

```
urn:liberty:security:2005-02:null:X509
urn:liberty:security:2005-02:TLS:X509
urn:liberty:security:2005-02:ClientTLS:X509
urn:liberty:security:2005-02:null:SAML
urn:liberty:security:2005-02:TLS:SAML
urn:liberty:security:2005-02:ClientTLS:SAML
urn:liberty:security:2005-02:null:Bearer
urn:liberty:security:2005-02:TLS:Bearer
urn:liberty:security:2005-02:ClientTLS:Bearer
```

Liberty ID-WSF 支持的新属性

在 Access Manager 充当 WSC 的情况下，当无法通过入站消息或资源提供来确定 Liberty ID-WSF 框架时，`com.sun.identity.liberty.wsf.version` 属性可确定 Liberty ID-WSF 框架。其值可以是 1.0 或者 1.1，默认为 1.1。

注 安装修补程序时不会在 `AMConfig.properties` 文件中添加 `com.sun.identity.liberty.wsf.version` 属性 (CR# 6458184)。要使用此新属性，在安装修补程序后，将它和适当的值添加到 `AMConfig.properties` 文件中，然后重新启动 Access Manager Web 容器。

安装 Access Manager 7 修补程序 3 后，运行以下命令来加载模式更改（以将 Access Manager 安装在 Solaris 系统上的默认目录中为例）：

```
# /opt/SUNWam/bin/amadmin -u amadmin -w amadmin_password
-t /etc/opt/SUNWam/wsf1.1_upgrade.xml
```

注册时，ID-WSF 搜索注册可使用这些新的安全机制。此外，WSC 在与 WSP 通信时会自动检测应使用哪个版本。要为 ID-WSF1.1 进行配置，请遵循产品随附的 Liberty ID-FF 范例 1 和 ID-WSF 范例的自述文件进行操作。

CR# 6463779 分布式验证的 amProfile_Client 日志和 Access Manager 服务器的 amProfile_Server 日志中充满了无害的异常

通过分布式验证 UI 向 Access Manager 服务器发送请求时，会触发异常并记录到 `distAuth/amProfile_Client` 日志和 Access Manager 服务器的 `debug/amProfile_Server` 日志中。经过大量会话后，`amProfile_Client` 日志的大小可增长到数千兆字节，而 Access Manager 服务器的 `amProfile_Server` 日志的大小可达数兆字节。日志中的这些异常不会对功能造成影响，但它们能导致用户接收到虚假报警，并且这些日志可能会填满整个硬盘空间。

解决方法。运行 `cron` 作业以清空日志文件内容。例如：

- 在分布式验证 UI 客户机上，每隔几个小时就运行一次 "cat /dev/null > distAuth/amProfile_Client"，具体间隔时间视流量大小而定。
- 在 Access Manager 服务器上，每隔几天（而不是几小时）就运行一次 "cat /dev/null > /var/opt/SUNWam/debug/amProfile_Server"。

CR# 6460974 默认分布式验证应用程序用户不应该是 amadmin

如果部署的是分布式验证 UI 服务器，则分布式验证管理员不应该是 amadmin。Makefile.distAuthUI 文件中的默认分布式验证应用程序用户是 amadmin，在客户机端部署 distAuth.war 文件后，此设置也随后出现在 AMConfig.properties 文件中。amadmin 用户具有的 AppSSOToken 会在 amadmin 会话结束时过期，这将在 amSecurity 日志文件（默认情况下位于 /tmp/distAuth 目录下）中产生 FATAL ERROR。

解决方法。将 UrlAccessAgent 指定为分布式验证应用程序用户。例如：

在客户机 Web 容器中部署 distAuth.war 文件之前，更改 Makefile.distAuthUI 文件中的以下参数：

```
APPLICATION_USERNAME=UrlAccessAgent
APPLICATION_PASSWORD=shared-secret-password 或 amldapuser-password
```

或

在客户机 Web 容器中部署 distAuth.war 文件之后，在 AMConfig.properties 文件中更改每个 Access Manager 服务器的以下属性：

```
com.sun.identity.agents.app.username=UrlAccessAgent
com.iplanet.am.service.password=shared-secret-password 或 amldapuser-password
```

另请参见第 47 页中的 “CR# 6440697：分布式验证应以非 amadmin 用户身份运行”。

CR# 6460576 控制台联机帮助的“过滤的角色”下，没有“用户服务”的链接

Access Manager 控制台联机帮助的“过滤的角色”下没有“用户服务”链接。在联机帮助中，转至“内容”、“过滤的角色”、“创建过滤的角色”。向下翻页，根据您所选的身份类型，会显示服务列表，但其中没有“用户服务”链接。

解决方法。无

CR# 6460085 运行 reinstallRTM 并重新部署 Web 应用程序之后，无法访问 WebSphere 上的服务器

在 Red Hat Linux AS 3.0 Update 4 的 IBM WebSphere Application Server 5.1.1.6 上对 DEPLOY_LEVEL=1 的部署应用 Access Manager 7 修补程序 3 之后，运行 reinstallRTM 脚本恢复 RTM RPM。在编辑了由 reinstallRTM 脚本生成的 amsilent 文件后，重新部署

Web 应用程序。用 stopServer.sh 和 startServer.sh 脚本重新启动 WebSphere。然后，访问登录页面时，WebSphere 却显示与 amlcontroller 过滤器相关的 500 错误。

发生此问题的原因是 reinstallRTM 脚本生成的新 server.xml 文件已损坏。

解决方法。amconfig 脚本备份的 server.xml 文件仍然有效。可以按照以下步骤来使用先前的副本：

1. 停止服务器。
2. 用 amconfig 脚本备份的副本替换损坏的 server.xml。

   amconfig 脚本备份的 server.xml 文件的名称为 server.xml-orig- *pid*，其中 *pid* 是 amwas51config 脚本的进程 ID。此文件位于下面的目录中：

   WebSphere-home-directory/config/cells/*WebSphere-cell*
   /nodes/*WebSphere-node*/servers/*server-name*
3. 重新启动服务器。

CR# 6455757：升级前必须将 sunISManagerOrganization 标记类添加到组织中

在 Access Manager 7 发行之前创建的 Access Manager DIT 中的组织可能不具有 sunISManagerOrganization 对象类。而且，由 Access Manager 以外的其他产品所创建组织的定义中也不会有 sunISManagerOrganization 对象类。

解决方法。在升级到 Access Manager 7 2005Q4 前，确保 DIT 中所有组织的定义中都具有 sunISManagerOrganization 对象类。如有必要，在升级前手动添加此对象类。

CR# 6454489：Access Manager 7 2005Q4 修补程序 2 升级导致控制台“当前会话”选项卡中出错

升级导致在 Access Manager 控制台的“当前会话”选项卡中出现以下错误：

无法从指定服务器获取有效的会话

对于从根后缀格式为 o=orgname 的 Access Manager 6 版本升级的部署，均会出现此问题。

解决方法。安装 Manager 7 2005Q4 后，应用 Manager 7 修补程序 3，然后运行 amupgrade 脚本以进行数据迁移，方法如下：

1. 备份 Access Manager 6 DIT。
2. 运行 ampre70upgrade 脚本。
3. 安装 Access Manager 7 2005Q4，选择“以后再配置”选项。
4. 取消部署 Access Manager Web 应用程序。
5. 部署 Access Manager Web 应用程序。

6. 应用 Access Manager 7 修补程序 3，但不要应用 XML/LDIF 更改。XML/LDIF 更改必须在下一步运行 amupgrade 脚本之后再应用。
7. 运行 amupgrade 脚本。
8. 因为 Access Manager 7 修补程序 3 进行了更改，重新部署 Access Manager Web 应用程序。
9. 访问 Access Manager 控制台。

CR# 6452320：在客户机 SDK 中使用轮询时抛出异常

若在部署 Access Manager 客户机 SDK (amclientsdk.jar) 后启用轮询，可能发生如下错误：

```
错误：发送轮询错误：
com.iplanet.am.util.ThreadPoolException：
amSessionPoller 线程池的作业队列已满。
```

部署分布式验证 UI 服务器、J2EE 代理后，或者在客户机上部署了 Access Manager 客户机 SDK 的情况下，均可能发生此类错误。

解决方法。如果只有数百个并发会话，则在 AMConfig.properties 文件或者 AMAgents.properties 文件中添加以下属性和值：

```
com.sun.identity.session.polling.threadpool.size=10
com.sun.identity.session.polling.threadpool.threshold=10000
```

如果有数千或数万个会话，则应将值设置为与运行 amtune-identity 脚本后 Access Manager AMConfig.properties 文件中通知的值相同。例如，对于一台有 4 GB RAM 的计算机，Access Manager amtune-identity 脚本会设置以下值：

```
com.sun.identity.session.notification.threadpool.size=28
com.sun.identity.session.notification.threadpool.threshold=76288
```

在拥有 4 GB RAM 的客户机上部署了分布式验证 UI 服务器或 Access Manager 客户机 SDK 后，应在客户机端的 AMAgent.properties 或 AMConfig.properties 文件中设置类似的值。

CR# 6442905 已验证用户的 SSOToken 可能会在无意中透露给流氓站点

已验证的 Access Manager 用户单击流氓站点的 URL 时，可能会在无意中将 SSOToken 透露给流氓站点。

解决方法。在 Access Manger 中总是为所有参与的策略代理创建唯一的代理用户配置文件，以确保站点不是流氓站点。同时确保这些唯一代理用户使用的密码均不与共享的秘密密码或者 amldapuser 密码相同。默认情况下，Access Manager 应用程序验证模块将策略代理验证为 UrlAccessAgent 用户。

有关使用 Access Manager 管理控制台创建代理的详细信息，参见《Sun Java System Access Manager 7 2005Q4 管理指南》中的“代理”。

CR# 6441918：站点监视时间间隔和超时属性

Access Manager 站点故障转移包括以下新属性：

```
com.sun.identity.sitemonitor.interval
com.sun.identity.sitemonitor.timeout
```

有关详细信息，参见第 42 页中的 “站点监视的新配置属性”。

CR# 6440697：分布式验证应以非 amadmin 用户身份运行

要为分布式验证应用程序验证创建默认管理用户 (amadmin) 以外的分布式验证管理员，遵循以下步骤：

1. 为分布式验证管理员创建 LDAP 用户。例如：

   ```
   uid=DistAuthAdmin,ou=people,o=am
   ```

2. 将分布式验证管理员添加到特殊用户列表。例如：

   ```
   com.sun.identity.authentication.special.users=cn=dsameuser,
   ou=DSAME Users,o=am|cn=amService-UrlAccessAgent,ou=DSAME Users,
   o=am|uid=DistAuthAdmin,ou=People,o=am
   ```

   将此属性添加到所有 Access Manager 服务器的 `AMConfig.properties` 文件中，这样分布式验证管理员的 `AppSSOToken` 在会话到期后也不会过期。

CR# 6440695：包含负载平衡器的分布式验证 UI 服务器

如果您的部署中在多个分布式验证 UI 服务器之前包含负载平衡器，则在部署 WAR 文件之后设置 `AMConfig.properties` 文件中的以下属性。

```
com.iplanet.am.lbcookie.name=DistAuthLBCookieName
com.iplanet.am.lbcookie.value=DistAuthLBCookieValue
```

CR# 6440651：Cookie 重放需要 com.sun.identity.session.resetLBCookie 属性

为使 Access Manager 会话故障转移的 cookie 重放功能正常工作，为策略代理和 Access Manager 服务器添加值为 `true` 的 `com.sun.identity.session.resetLBCookie` 属性。例如：

```
com.sun.identity.session.resetLBCookie='true'
```

- 对于策略代理，将此属性添加到 `AMAgent.properties` 文件。

- 对于 Access Manager 服务器，将此属性添加到 `AMConfig.properties` 文件。

注意：仅当已实施 Access Manager 会话故障转移后需要此属性。

CR# 6440648：`com.iplanet.am.lbcookie.name` 属性假定默认值为 `amlbcookie`

默认情况下，策略代理和 Access Manager 服务器假定负载平衡器 cookie 名称为 `amlbcookie`。如果在后端服务器更改了此 cookie 的名称，则必须为策略代理在 `AMAgent.properties` 文件中使用相同的名称。同样，如果使用 Access Manager 客户机 SDK，也必须使用后端服务器所使用的同一 cookie 名称。

CR# 6440641：`com.iplanet.am.lbcookie.value` 属性已过时

Access Manager 不再支持服务器上的 `com.iplanet.am.lbcookie.value` 属性自定义负载平衡器 cookie。现在，对于由代理重放的 cookie 值及名称，Access Manager 使用配置为会话配置一部分的服务器 ID 。

CR# 6429610：在 ID-FF SSO 使用案例中无法创建 SSO 令牌

设置 Liberty Identity Federation Framework (ID-FF) 范例 1 后，联合成功，但 SSO 失败。

解决方法。在 `AMConfig.properties` 文件中，将 `dsameuser` 的 `uuid` 添加到 `com.sun.identity.authentication.special.users` 属性。对于应用程序验证，`dsameuser` 需要 Access Manager 服务器不会过期的 SSO 令牌。

CR# 6389564：在 Access Manager 登录期间，会在 LDAP v3 数据存储库中对用户的角色成员资格进行重复不断的查询

用户登录到 Access Manager 时，会发生对用户的 `nsRoleDN` 属性进行重复 LDAP 搜索的情况。

解决方法。安装 Access Manager 7 修补程序 3 后，运行以下命令（以将 Access Manager 安装在 Solaris 系统上的默认目录中为例）：

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/idRepoServiceAddAttrSchemaRequest_Cache.xml
```

CR# 6385185：验证模块必须能够覆盖 "goto" URL，并指定另一不同的 URL

验证模块可覆盖 "goto" URL 并请求重定向到其他外部 Web 站点的 URL 以验证用户状态

要在验证完成后覆盖 "goto" URL，在 `SSOToken` 中设置以下示例中所示的属性。可使用实现 `AMPostAuthProcessInterface` 的 `PostProcess` 类的 `onLoginSuccess` 方法来设置此属性。 例如，在下例中 *OverridingURL* 即是覆盖 "goto" URL 的 URL：

```
public class <..> implements AMPostAuthProcessInterface {
...
    public void onLoginSuccess(...) {
        try {
            ssoToken.setProperty("PostProcessSuccessURL", OverridingURL);
         } catch (Exception ...) {
         ...         }
...
}
```

CR# 6385184：当 SSO 令牌仍处于无效状态时，从自定义验证模块重定向

自定义验证模块中的新 `RedirectCallback` 方法允许通过验证 UI 重定向至外部 Web 站点来进行用户验证。如果验证成功，则会在之后将用户重定向回原来的 Access Manager 服务器 URL。范例文件包括：

- `LoginModuleSample.java`
- `LoginModuleSample.xml`
- `testExtWebSite.jsp`

要实现此功能：

1. 使用范例 `LoginModuleSample.java` 创建自定义验证模块。
2. 将此模块加载到 Access Manager 服务器中。
3. 使用范例 `LoginModuleSample.xml` 在 XML 文件中构造 `RedirectCallback`。
4. 为外部 Web 站点使用范例 `testExtWebSite.jsp` 文件以测试此模块。
5. 使用以下 URL 登录：

```
http://example.com/amserver/UI/Login?module=LoginModuleSample
```

用户名和密码均重定向至外部 Web 站点进行验证。如果用户名和密码都有效，则验证成功，然后将用户重定向回原来的 Access Manager 服务器 URL。

例如，设想一下这样的方案 - 在此方案中部署使用自定义验证模块来访问某个置备/信用卡站点：

1. 用户调用自定义验证模块的验证进程/登录页面。
2. 此用户输入证书（用户名和密码），然后向自定义验证模块提交请求。
3. 自定义验证模块将用户重定向至外部置备/信用卡站点，并同时传递请求和所需的用户信息。
4. 外部置备/信用卡站点检查用户的状态，然后返回请求以及成功或失败信息（已设为返回请求的一部分）。
5. 自定义验证模块根据第 4 步返回的状态验证用户，并向验证服务返回相应的状态。
6. 用户验证完成（成功或失败）。

CR# 6324056：使用辅件配置文件时联合失败

解决方法：要修复此问题，根据您所使用的平台，应用最新版本的 "Core Mobile Access" 修补程序：

- 基于 SPARC 系统的 Solaris OS：119527
- x86 平台上的 Solaris OS：119528
- Linux 系统：119529

应用修补程序后，重新启动 Web 容器。

Access Manager 7 2005Q4 修补程序 2

Access Manager 7 2005Q4 修补程序 2（修订版 02）可修复一系列的问题，其随附的自述文件中列出了具体内容。修补程序 2 还具有以下新增功能和已知问题：

修补程序 2 的新增功能

- 第 50 页中的 “用户管理、身份库和服务管理高速缓存的新属性”
- 第 52 页中的 “联合服务提供者的新属性”
- 第 52 页中的 “LDAP 过滤条件支持”

修补程序 2 的已知问题和限制

- 第 52 页中的 “CR# 6283582：Access Manager 实例之间没有共享登录失败次数”
- 第 53 页中的 “CR# 6293673：发出会话超时通知时，需要保留原来的会话信息”
- 第 53 页中的 “CR# 6244578：Access Manager 应当警告用户：浏览器 cookie 支持已禁用/不可用”
- 第 53 页中的 “CR# 6236892：登录后，CDCServlet 处理 AuthNResponse 时显示图像/文本占位符”
- 第 53 页中的 “CR# 6363157：如果确实需要，新属性可禁用持久性搜索”
- 第 54 页中的 “CR# 6385696：现有的及新的 IDP 和 SP 不可见”

用户管理、身份库和服务管理高速缓存的新属性

修补程序 2 包含以下用于用户管理 (Access Manager SDK)、身份库 (Identity Repository, IdRepo) 和服务管理高速缓存的新属性。这些属性允许您基于部署要求独立地启用和禁用不同的高速缓存，以及为高速缓存条目设置生存时间 (Time To Live, TTL)。

表 3 用户管理、身份库和服务管理高速缓存的新属性

属性	描述
用于启用和禁用高速缓存的新属性	

表 3 用户管理、身份库和服务管理高速缓存的新属性 （续）

`com.iplanet.am.sdk.caching.enabled`	用于启用 (True) 或禁用 (False) 身份库 (IdRepo)、用户管理和服务管理高速缓存的全局属性。如果为 True，或者属性没有出现在 `AMConfig.properties` 文件中，则这三个高速缓存都会启用。
注意：仅在上述全局属性设置为 False 时，才能应用以下三个用来启用或禁用特定高速缓存的属性。	
`com.sun.identity.amsdk.cache.enabled`	仅启用 (True) 或禁用 (False) 用户管理 (Access Manager SDK) 高速缓存。
`com.sun.identity.idm.cache.enabled`	仅启用 (True) 或禁用 (False) 身份库 (IdRepo) 高速缓存。
`com.sun.identity.sm.cache.enabled`	仅启用 (True) 或禁用 (False) 服务管理高速缓存。
TTL 的新用户管理高速缓存属性.	
`com.iplanet.am.sdk.cache.entry.expire.enabled`	启用 (True) 或禁用 (False) 用户管理高速缓存的到期时间（由以下两个属性所定义）。
`com.iplanet.am.sdk.cache.entry.user.expire.time`	指定用户管理高速缓存中的用户条目在上次修改之后保持有效的时间，以分钟为单位。即，在指定的时间过去之后（上次修改或从目录读取之后），被高速缓存的条目的数据将会过期。此后，如果对这些条目的数据有新请求，则必须从目录读取数据。
`com.iplanet.am.sdk.cache.entry.default.expire.time`	指定用户管理高速缓存中的非用户条目在上次修改之后保持有效的时间，以分钟为单位。即，在指定的时间过去之后（上次修改或从目录读取之后），被高速缓存的条目的数据将会过期。此后，如果对这些条目的数据有新请求，则必须从目录读取数据。TTL 的新身份库高速缓存属性
`com.sun.identity.idm.cache.entry.expire.enabled`	启用 (True) 或禁用 (False) IdRepo 高速缓存的到期时间（由以下属性所定义）。
`com.sun.identity.idm.cache.entry.default.expire.time`	指定 IdRepo 高速缓存中的非用户条目在上次修改之后保持有效的时间，以分钟为单位。即，在指定的时间过去之后（上次修改或从系统信息库读取之后），被高速缓存的条目的数据将会过期。此后，如果对这些条目的数据有新请求，则必须从系统信息库读取数据。

使用新的高速缓存属性

Access Manager 7 2005Q4 修补程序不会自动将新的高速缓存属性添加到 `AMConfig.properties` 文件中。

使用新的高速缓存属性：

1. 使用文本编辑器，将属性和它们的值添加到以下目录（由具体平台而定）的 `AMConfig.properties` 文件中：
   - Solaris 系统：`/etc/opt/SUNWam/config`
   - Linux 系统：`/etc/opt/sun/identity/config`
2. 重新启动 Access Manager Web 容器以使这些值生效。

联合服务提供者的新属性

新的 `com.sun.identity.federation.spadapter` 属性定义了 `com.sun.identity.federation.plugins.FederationSPAdapter` 的实现类，该类用于在服务提供者端的联合处理期间添加特定于应用程序的处理。

另请参见第 54 页中的 “CR# 6385696：现有的及新的 IDP 和 SP 不可见”。

LDAP 过滤条件支持

修补程序 2 中添加了“LDAP 过滤条件”支持。策略管理员现在可以在定义策略时，在条件中指定 LDAP 过滤器。仅当用户的 LDAP 条目满足条件中指定的 LDAP 过滤器时，才会对该用户应用策略。用户的 LDAP 条目是在策略配置服务中指定的目录内进行查找。

要注册和使用“LDAP 过滤器条件”，请在安装 Access Manager 7 修补程序 2 后运行以下命令（以将 Access Manager 安装在 Solaris 系统上的默认目录中为例）：

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-s /etc/opt/SUNWam/AddLDAPFilterCondition.xml
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/amPolicyConfig_mod_ldfc.xml
```

修补程序 5 说明如果您已添加 Access Manager 7 2005Q4 修补程序 5 并运行 `updateschema.sh` 脚本，则您不需要使用 `amadmin` 来加载这些文件。有关更多信息，请参见第 27 页中的 “提供新的 `updateschema.sh` 脚本来加载 LDIF 和 XML 文件”。

CR# 6283582：Access Manager 实例之间没有共享登录失败次数

安装 Access Manager 7 修补程序 2 后，运行以下命令（以安装在 Solaris 系统的默认目录下的 Access Manager 为例）：

```
# cd DirectoryServer-base/shared/bin
# ./ldapmodify -h DirectoryServerHost -p DirectoryServerPort
-D "cn=Directory Manager" -w DirectoryMangerPassword
-a -f /etc/opt/SUNWam/accountLockout.ldif
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/accountLockoutData.xml
```

DirectoryServer-base 的默认值在 Solaris 系统中是 `/var/opt/mps/serverroot`，而在 Linux 系统中是 `/var/opt/sun/directory-server`。

修补程序 5 说明如果您已添加 Access Manager 7 2005Q4 修补程序 5 并运行 `updateschema.sh` 脚本，则您不需要使用 `amadmin` 来加载这些文件。有关更多信息，请参见第 27 页中的 “提供新的 `updateschema.sh` 脚本来加载 LDIF 和 XML 文件”。

CR# 6293673：发出会话超时通知时，需要保留原来的会话信息

`AMConfig.properties` 文件中的新 `com.sun.identity.session.property.doNotTrimList` 属性可包含会话属性名称的列表（以逗号分隔）。一旦会话超时，此列表中定义的属性也不会被移除，因此在清除会话前均可以访问这些属性。例如：

`com.sun.identity.session.property.doNotTrimList=`*UserId*`,`*HostName*

CR# 6244578：Access Manager 应当警告用户：浏览器 cookie 支持已禁用/不可用

`AMConfig.properties` 文件中的新 `com.sun.identity.am.cookie.check` 属性指示服务器是否应当检查浏览器中的 cookie 支持/cookie 启用。其值为 `true` 时，服务器将检查浏览器中的 cookie 支持/cookie 启用。如果浏览器不支持或没有启用 cookie，则服务器会抛出错误页面。如果希望服务器对验证功能提供无 cookie 模式支持，则应将此值设置为 false（即默认值）。

CR# 6236892：登录后，CDCServlet 处理 AuthNResponse 时显示图像/文本占位符

以下新属性被添加到 `AMConfig.properties` 文件中，并由 CDCServlet 读取：

- `com.iplanet.services.cdc.WaitImage.display` 如果设置为 true，则当用户在 CDSSO 方案中等待受保护的页面时，浏览器中将显示一个图像。默认值是 false。
- `com.iplanet.services.cdc.WaitImage.name` 用于指定图像名称。默认值是 `waitImage.gif`。此图像是从 `login_images` 目录中复制的。
- `com.iplanet.services.cdc.WaitImage.width` 用于指定图像宽度。默认值是 420。
- `com.iplanet.services.cdc.WaitImage.height` 用于指定图像高度。默认值是 120。

CR# 6363157：如果确实需要，新属性可禁用持久性搜索

`AMConfig.properties` 文件中的新 `com.sun.am.event.connection.disable.list` 属性用于指定可禁用的事件连接。其值（不区分大小写）可为：

`aci` - 对 `aci` 属性所做的更改，且使用 LDAP 过滤器 (`aci=*`) 进行搜索

`sm` - Access Manager 信息树（或服务管理节点）中的更改，包括具有 `sunService` 或 `sunServiceComponent` 标记对象类的对象。例如，您可以创建一个策略来定义受保护资源的访问权限，或者您可以修改现有策略的规则、对象、条件或响应提供者。

um - 用户目录（或用户管理节点）中的更改。例如，您可以更改用户的名称或地址。

例如，要禁用对 Access Manager 信息树（或服务管理节点）更改的持久性搜索：

```
com.sun.am.event.connection.disable.list=sm
```

要指定多个值，请将每个值以逗号分隔。

注意 – 持久性搜索会导致 Directory Server 上性能系统开销增加。如果您确定删除某些此类性能系统开销在生产环境中确实非常必要，可使用 `com.sun.am.event.connection.disable.list` 属性禁用一个或多个持久性搜索。

不过，在禁用持久性搜索前，您应该了解上述限制。强烈建议不要更改此属性，除非确实有必要。引入此属性的主要目的是避免在 Directory Server 上使用多个 2.1 J2EE 代理时产生的系统开销，因为这些代理中的每一个都会建立此类持久性搜索。2.2 J2EE 代理不再建立此类持久性搜索，因此您可能不需要使用此属性。

有关更多信息，请参见第 85 页中的 “记录关于禁用持久性搜索的更多信息 (6486927)” 。

CR# 6385696：现有的及新的 IDP 和 SP 不可见

`AMConfig.properties` 文件中的新 `com.sun.identity.federation.spadapter` 属性可指定联合服务提供者适配器的默认实现，应用程序可从中获得声明和响应信息。例如：

```
com.sun.identity.federation.spadapter=com.sun.identity.federation.plugins.FSDefaultSPAdapter
```

Access Manager 7 2005Q4 修补程序 1

Access Manager 7 2005Q4 修补程序 1（修订版 01）可修复一系列的问题，其随附的自述文件中列出了具体内容。修补程序 1 还具有以下新增功能和已知问题：

- 第 54 页中的 “创建调试文件”
- 第 55 页中的 “支持 LDAPv3 插件中的角色和过滤的角色”
- 第 55 页中的 “CR# 6320475：服务器端的 `com.iplanet.am.session.client.polling.enable` 不能为 true”
- 第 55 页中的 “CR# 6358751：如果加密密钥包含空格，则无法应用 Access Manager 7 修补程序 1”

创建调试文件

默认情况下，Access Manager 调试文件创建于调试目录中，即使 `AMConfig.properties` 文件中的 `com.iplanet.services.debug.level` 属性设置为 error 时也是如此。Access Manager 7 修补程序 1 发布前，仅在第一条调试消息记录到文件中时才创建调试文件。

支持 LDAPv3 插件中的角色和过滤的角色

如果数据存储在 Sun Java System Directory Server 中，则 Access Manager 7 修补程序 1 支持 LDAPv3 插件中的角色和过滤的角色。有关详细信息，参见第 89 页中的 “对支持 LDAPv3 插件的角色和过滤角色的说明 (6365196)”。

CR# 6320475：服务器端的 `com.iplanet.am.session.client.polling.enable` 不能为 true

服务器端的 `AMConfig.properties` 文件中的 `com.iplanet.am.session.client.polling.enable` 属性默认设置为 false，并且任何时候都不能将其重置为 true。

CR# 6358751：如果加密密钥包含空格，则无法应用 Access Manager 7 修补程序 1

如果密码加密密钥包含空格，则无法应用此修补程序。

解决方法。使用不包含空格的新加密密钥。有关更改加密密钥的详细步骤，参见：《Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide》中的附录 B “Changing the Password Encryption Key”。

此发行版的新增功能

有关 Access Manager 修补程序发行版中的新功能的信息，请参见第 9 页中的 “Access Manager 7 2005Q4 修补程序发行版”。Access Manager 7 2005Q4 的初始版包括以下新功能：

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：

- Access Manager 7 2005Q4 的新功能
- Access Manager 6 2005Q1 功能，但是有以下限制：
  - 创建领域时，不在 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 75 页中的 “新的 Access Manager 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

以下情形必须要用传统模式：

- 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
- Access Manager 6 2005Q1 和 Access Manager 7 2005Q4 访问同一 Directory Server 时不同部署共存的情形

新的 Access Manager 控制台

已为此版本重新设计了 Access Manager 控制台。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 63 页中的 “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。使用 Access Manager 或另一置备产品（如 Sun Java System Identity Manager），可创建和维护身份库。

在当前版本中，身份库既可以驻留在 Sun Java System Directory Server 上也可以驻留在 Microsoft Active Directory 上。Access Manager 对身份库可以拥有读/写或只读权限。

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，如有必要），如下节所述。

Access Manager 领域

领域和任意子领域均为 Access Manager 信息树的组成部分，其中可包含：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资源访问权限后应用程序可用的信息。领域或子领域也可包含其他配置信息，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。领域或子领域也可为空。

使用 Access Manager 控制台或 `amadmin` CLI 实用程序可创建领域。有关详细信息，参阅控制台联机帮助或《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

Access Manager 可提供一个与 Web 容器相独立的会话故障转移实现，其中 Sun Java System Message Queue (Message Queue) 为通信代理，Sleepycat Software, Inc. 的 Berkeley DB 为会话存储数据库。Access Manager 7 2005Q4 的增强功能包括用于配置会话故障转移环境的 `amsfoconfig` 脚本，以及用于启动和停止 Message Queue 代理及 Berkeley DB 客户机的 `amsfo` 脚本。

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更改时，向特定监听程序发送通知。此功能将在 Access Manager 管理员控制台中启用了“启用属性更改通知”属性后生效。例如，在单点登录 (Single Sign-On, SSO) 环境下，多个应用程序可共享一个 Access Manager 会话。当“通知属性”列表中定义的特定会话属性发生更改时，Access Manager 会向所有已注册的监听程序发送通知。

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，以限制允许某个用户拥有的最大并发会话数。管理员可在全局级别上为所有用户设置会话配额限制，或为某个实体（如组织、领域、角色或用户）设置仅应用于一个或多个特定用户的会话配额限制。

默认情况下，会话配额限制为已禁用（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”属性来启用它们。

如果用户用尽会话限制配额，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 会拒绝新会话的登录请求。
- DESTROY_OLD_SESSION。Access Manager 会中断同一用户下一个即将过期的现有会话，然后允许处理新的登录请求。

“免除顶层管理员的限制检查”属性可指定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

Access Manager 7 2005Q4 包括了“分布式验证 UI”，它是一种可在同一部署的两个防火墙间提供安全的分布式验证的远程验证 UI 组件。如果没有“分布式验证 UI”组件，Access Manager 服务 URL 将会向最终用户开放。使用代理服务器虽可避免此现象发生，但对许多部署而言，代理服务器却未必是可接受的解决方案。

“分布式验证 UI”组件安装在 Access Manager 部署的非安全保护 (DMZ) 层中的一台或多台服务器上。分布式验证 UI 服务器并不运行 Access Manager；它存在的目的仅是通过 Web 浏览器向最终用户提供验证界面。

最终用户将发送 HTTP 请求到“分布式验证 UI”，然后“分布式验证 UI”向用户显示登录页面。“分布式验证”组件随即将用户的请求通过第二道防火墙发送到 Access Manager 服务器，这样就可以不用打开最终用户与 Access Manager 服务器之间的防火墙通道。

有关详细信息，参见《Technical Note: Using Access Manager Distributed Authentication》。

支持多重验证模块实例

已扩展所有验证模块（默认配置），以支持带有控制台 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。支持名称与其类型名称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

在“组织/领域”下创建单独的名称空间，即验证模块实例链。同一链可被重新使用并指定给组织/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`)。在适用的策略中，策略评估且发送至客户机的策略决策，现在还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。可定义策略中的属性名称和值。
- 动态属性。可在策略中列出属性名称，而值是在评估策略时从“身份库”数据存储库内获取的。

“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”发送到受保护的应用程序。

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。评估策略时，仅当用户 Access Manager 会话的属性值均在条件中有所定义时，条件才会返回 “true”。对于在条件中定义了多个值的属性，用户会话拥有条件中列出的其中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

策略现在拥有一个可设置为活动或不活动的状态属性。策略评估期间将忽略处于非活动状态的策略。

站点配置

Access Manager 7 2005Q4 引入了“站点概念”，可提供对 Access Manager 部署的集中式配置管理。将 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，如此可简化部署，还可解决诸如客户机与后端 Access Manager 服务器之间的防火墙阻断等问题。

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同时访问 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。这一过程非常耗时。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，将应用至特定用户登录会话的所有事件。对于用户的特定登录会话，在所有已记录事件的日志文件中 ContextID 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 /opt/SUNWam/samples/logging 目录下的 LogReaderSample.java 文件，该文件显示了如何从平面文件或 DB 表格系统信息库检索日志记录。

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

下表显示此版本所需的硬件和软件。

表 4 硬件和软件要求

组件	要求
操作系统 (OS)	基于 SPARC™ 的系统上的 Solaris OS，版本 8、9 和 10；包含对 Solaris 10 上的整个根本地区域的支持 x86 平台上的 Solaris OS，版本 9 和 10；包含对 Solaris 10 上的整个根本地区域的支持 AMD64 平台上的 Solaris OS，版本 10；包含对整个根本地区域的支持 Red Hat™ Linux WS/AS/ES 2.1 Update 6 或更高版本 Red Hat Linux WS/AS/ES 3.0 Red Hat Linux WS/AS/ES 3.0 Update 1、2、3 和 4 HP-UX OS。参见适用于 HP-UX 的 Sun Java Enterprise System 2005Q4 文档集：`http://docs.sun.com/coll/1258.2` 及 `http://docs.sun.com/coll/1529.1` Windows OS。参见适用于 Microsoft Windows 的 Sun Java Enterprise System 2005Q4 文档集：`http://docs.sun.com/coll/1259.2` 及 `http://docs.sun.com/coll/1512.1`
Java 2 Standard Edition (J2SE)	J2SE 平台 1.5.0_04、1.5_01、1.5 和 1.4.2
Directory Server	Access Manager 信息树：Sun Java System Directory Server 5 2005Q4 Access Manager 身份库：Sun Java System Directory Server 5 2005Q4 或 Microsoft Active Directory

表 4 硬件和软件要求 （续）

组件	要求
Web 容器	Sun Java System Web Server 6.1 2005Q4 SP5
	Sun Java System Application Server Enterprise Edition 8.1 2005Q2
	BEA WebLogic Server 8.1 SP4
	IBM WebSphere Application Server 5.1 和 5.1.1（以及相关的不断补充的补丁）
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 Sun Java Enterprise System 2005Q4 版本支持的浏览器。

表 5 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

系统虚拟化支持

系统虚拟化是一项允许多个操作系统 (OS) 实例在共享硬件上独立执行的技术。从功能讲，在虚拟环境中托管的 OS 上部署的软件通常不会意识到基础平台已被虚拟化。Sun 在所选择的系统虚拟化和 OS 组合上执行其 Sun Java System 产品的测试，以帮助验证 Sun Java System 产品是否能够在适当大小及正确配置的虚拟环境中继续运行，就像在非虚拟系统上一样。有关 Sun 对虚拟化环境中 Sun Java System 产品的支持，请参见 http://docs.sun.com/doc/820-4651。

兼容性问题

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：

如需确定 Access Manager 7 2005Q4 安装方式的更多信息，参见第 64 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 安装程序的详细信息，参见《Sun Java Enterprise System 2005Q4 Installation Guide for UNIX》中的第 5 章 “Installing in Silent Mode”。

图形模式下的“立即配置”安装选项

如果在图形模式下使用“立即配置”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“立即配置”安装选项

如果是在基于文本的模式下使用“立即配置”选项运行 Java ES 安装程序， 则为 `Install type (Realm/Legacy) [Legacy]` 选择默认值 `Legacy`。

“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
...
```

在 Windows 系统上，配置文件是 *AccessManager-base* `\setup\AMConfigurator.properties`。

有关运行 `amconfig` 脚本以配置 Access Manager 的详细信息，参阅《Sun Java System Access Manager 7 2005Q4 管理指南》 。

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 6 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 安装说明包括以下信息：

- 第 63 页中的 “Access Manager 传统模式”
- 第 67 页中的 “安装问题”

已知问题和限制

此部分描述了此版本发布时的已知问题及其解决方法（如果可用）。

- 第 65 页中的 “兼容性问题”
- 第 67 页中的 “安装问题”
- 第 69 页中的 “升级问题”
- 第 71 页中的 “配置问题”
- 第 74 页中的 “Access Manager 控制台问题”
- 第 76 页中的 “SDK 和客户机问题”
- 第 77 页中的 “命令行实用程序问题”
- 第 78 页中的 “验证问题”
- 第 79 页中的 “会话与 SSO 问题”
- 第 80 页中的 “策略问题”
- 第 81 页中的 “服务器启动问题”
- 第 81 页中的 “Linux OS 问题”
- 第 82 页中的 “联合与 SAML 问题”
- 第 83 页中的 “全球化 (Globalization, g11n) 问题”
- 第 85 页中的 “文档问题”

兼容性问题

- 第 66 页中的 “Java ES 2004Q2 服务器与 Java ES 2005Q4 上的 IM 不兼容 (6309082)”
- 第 66 页中的 “传统模式与核心验证模块存在不兼容性 (6305840)”

- 第 66 页中的 “代理无法登录，因为“组织中没有配置文件” (6295074)”
- 第 66 页中的 “Delegated Administrator commadmin 实用程序不创建用户 (6294603)”
- 第 67 页中的 “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)

以下部署方案导致产生了这个问题：

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

运行 `imconfig` 实用程序以配置 server-4 上的 Instant Messaging 时，配置不成功。Instant Messaging (IM) 在 server-4 上使用的 Access Manager 7 2005Q4 SDK 与 Java ES 2004Q2 版本不兼容。

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 传统模式在 Access Manager 6 2005Q1 版本核心验证模块中存在以下不兼容性：

- 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 2005Q4，而未升级 Delegated Administrator，则会出现此问题。有关升级 Delegated Administrator 的信息，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。

安装问题

- 第 67 页中的 “应用修补程序 1 后，`/tmp/amsilent` 文件将允许所有用户进行读取操作 (6370691)”
- 第 68 页中的 “在使用容器配置安装的 SDK 上，通知 URL 不正确 (6327845)”
- 第 68 页中的 “Access Manager `classpath` 引用了过期的 JCE 1.2.1 软件包 (6297949)”
- 第 68 页中的 “在现有 DIT 上安装 Access Manager 需重建 Directory Server 索引 (6268096)”
- 第 68 页中的 “非超级用户的日志和调试目录权限不正确 (6257161)”
- 第 68 页中的 “在单独的机器上安装 Access Manager 和 Directory Server 时，没有初始化验证服务 (6229897)”
- 第 69 页中的 “安装程序不为现在安装的目录添加平台条目 (6202902)”

应用修补程序 1 后，`/tmp/amsilent` 文件将允许所有用户进行读取操作 (6370691)

应用修补程序 1 后，`/tmp/amsilent` 文件允许所有用户进行读取操作。

解决方法：应用修补程序后，重置文件权限，仅允许 Access Manager 管理员拥有读取权限。

在使用容器配置安装的 SDK 上，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。

在现有 DIT 上安装 Access Manager 需重建 Directory Server 索引 (6268096)

要提高搜索性能，Directory Server 需拥有多个新的索引。

解决方法：使用现有目录信息树 (DIT) 完成对 Access Manager 的安装后，运行 `db2index.pl` 脚本以重建 Directory Server 索引。例如：

```
# ./db2index.pl -D "cn=Directory Manager" -w password -n userRoot
```

`db2index.pl` 脚本位于 *DS-install-directory/slapd-hostname/* 目录下。

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。

在单独的机器上安装 Access Manager 和 Directory Server 时，没有初始化验证服务 (6229897)

虽然 `classpath` 和其他 Access Manager web 容器环境变量已在安装期间进行了更新，但安装过程仍未重新启动 Web 容器。如果尝试在已安装 Access Manager 但尚未重新启动 Web 容器的情况下进行登录，则将返回以下错误：

未初始化验证服务。请与您的系统管理员联系。

解决方法：登录 Access Manager 前重新启动 Web 容器。登录前还必须运行 Directory Server。

安装程序不为现在安装的目录添加平台条目 (6202902)

Java ES 安装程序不为现在安装的目录服务器 (DIRECTORY_MODE=2) 添加平台条目。

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"。

升级问题

- 第 69 页中的 "Access Manager `ampre70upgrade` 脚本不会删除本地化软件包 (6378444)"
- 第 69 页中的 "`AMConfig.properties` 文件中的 Web 容器为旧版本 (6316833)"
- 第 70 页中的 "节点代理 `server.policy` 文件未随 Access Manager 升级而更新 (6313416)"
- 第 70 页中的 "升级完成后，"条件"列表中缺少"会话属性条件"(6309785)"
- 第 70 页中的 "升级完成后，策略主题列表中缺少 "身份主题" 类型 (6304617)"
- 第 70 页中的 "Access Manager 升级因 `classpath` 未迁移而失败 (6284595)"
- 第 70 页中的 "升级完成后，`amadmin` 命令返回了错误的版本 (6283758)"
- 第 71 页中的 "数据迁移后添加 `ContainerDefaultTemplateRole` 属性 (4677779)"

Access Manager `ampre70upgrade` 脚本不会删除本地化软件包 (6378444)

将 Access Manager 升级到 Access Manager 7 2005Q4 时，`ampre70upgrade` 脚本并不会删除系统上的任何 Access Manager 本地化软件包。

解决方法：在升级到 Access Manager 7 2005Q4 之前，使用 `pkgrm` 命令手动删除系统上已安装的所有 Access Manager 本地化软件包。

`AMConfig.properties` 文件中的 Web 容器为旧版本 (6316833)

将 Access Manager 和 Application Server 升级至 Java ES 2005Q4 版本后，Access Manager 的 `AMConfig.properties` 文件中的 Application Server 为旧版本。

解决方法：运行 Delegated Administrator 配置程序 (`config-commda`) 前，更改 `AMConfig.properties` 文件中的以下属性：

```
com.sun.identity.Webcontainer=IAS8.1
```

节点代理 server.policy 文件未随 Access Manager 升级而更新 (6313416)

Access Manager 升级完成后， 节点代理的 server.policy 文件未更新。

解决方法：将节点代理的 server.policy 文件替换为以下文件：

```
/var/opt/SUNWappserver/domains/domain1/config/server.policy
```

升级完成后，“条件”列表中缺少“会话属性条件”(6309785)

将 Access Manager 由版本 2005Q1 升级至版本 2005Q4 后，如果尝试将“条件”添加至策略，则“策略条件”列表未将“会话属性条件”显示为一个选项。

解决方法：在相应领域中选择策略配置服务模板中的“会话属性条件”类型。

升级完成后，策略主题列表中缺少“ 身份主题 ”类型 (6304617)

将 Access Manager 由版本 2005Q1 升级至版本 2005Q4 后，在策略主题列表中未将最新添加的“身份主题”策略主题类型显示为一个选项。

解决方法：在策略配置服务模板中将“身份主题”类型选择为默认主题类型。

Access Manager 升级因 classpath 未迁移而失败 (6284595)

Access Manager 在从 Java ES 2004Q2 升级至 Java ES 2005Q4 期间， 从 Java ES 2004Q2 升级至 Java ES 2005Q1 失败。 Access Manager 部署于 Application Server 上， 也从 Java ES 2004Q2 升级到了 Java ES 2005Q4。 domain.xml 文件中的 classpath 没有 Access Manager JAR 文件路径。

解决方法：请按照以下步骤进行操作：

1. 运行 amupgrade 脚本之前， 重新建立 Directory Server 的索引， 因为 comm_dssetup.pl 脚本存在问题。
2. 将 Access Manager 的条目添加至节点代理的 server.policy 文件。默认服务器策略 (/var/opt/SUNWappserver/domains/domain1/config/server.policy) 的 server.policy 文件副本就已足够。
3. 按如下方式更新节点代理 domain.xml 文件中的 classpath。将 classpath-suffix 和相关的 classpath 从 server.xml 文件 java-config 元素的 server-classpath 属性复制到 domain.xml 文件 java-config 元素的相应属性中。 java-config 元素可在 domain.xml 的 config 元素下找到。

升级完成后，amadmin 命令返回了错误的版本 (6283758)

在将 Access Manager 由版本 6 2005Q1 升级至版本 7 2005Q4 后， amadmin --version 命令返回了错误的版本： Sun Java System Access Manager 版本 2005Q1。

解决方法：升级 Access Manager 后，运行 amconfig 脚本以配置 Access Manager。运行 amconfig 时，指定配置 (amsamplesilent) 文件的完整路径。例如，在 Solaris 系统上：

```
# ./amconfig -s ./config-file
```

或

```
# ./amconfig -s /opt/SUNWam/bin/config-file
```

数据迁移后添加 ContainerDefaultTemplateRole 属性 (4677779)

不是在 Access Manager 中创建的组织下面未显示用户的角色。在调试模式下将显示以下消息：

```
错误：DesktopServlet.handleException()
com.iplanet.portalserver.desktop.DesktopException:
DesktopServlet.doGetPost(): no privilige to execute desktop
```

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。

配置问题

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：按如下操作编辑 `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：

```
cd /var/opt/SUNWappserver/domains/domain1/config
```

3. 生成 `server.policy` 文件的副本。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 强制要求 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。

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

如果将 Access Manager 7 2005Q4 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解除部署 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，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
```

在 IBM WebSphere 中使用 RSA 密钥时，URL 签名失败 (6271087)

在 IBM WebSphere 中使用 RSA 密钥时，URL 字符串签名失败并抛出以下异常：

错误：`FSSignatureUtil.signAndReturnQueryString`：**签署查询字符串时发生** `FSSignatureException`：**无此提供者：**`SunRsaSign`

解决方法：WebSphere 绑定的 JDK 中缺少“SunRsaSign”提供者。要修复此问题，请编辑 *websphere_jdk_root*`/jre/lib/security/java.security` 文件，并添加以下行以启用 "SunRsaSign" 作为提供者之一：

```
security.provider.6=com.sun.rsajca.Provider
```

Access Manager 控制台问题

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。此问题已在修补程序 1 中修复。有关对特定平台应用该修补程序的信息，参见第 54 页中的 “Access Manager 7 2005Q4 修补程序 1”。

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

配置远程记录后，除密码重置信息的 `amConsole.access` 和 `amPasswordReset.access` 之外，所有日志都可写入远程 Access Manager 实例。未在任何地方写入其日志记录。

解决方法：无。

在控制台中添加更多 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。此问题已在修补程序 1 中修复。有关对特定平台应用该修补程序的信息，参见第 54 页中的 “Access Manager 7 2005Q4 修补程序 1”。

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，无法删除角色中的所有用户 (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。此问题已在修补程序 1 中修复。有关对特定平台应用该修补程序的信息，参见第 54 页中的 “Access Manager 7 2005Q4 修补程序 1”。

在主题搜索中，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。

SDK 和客户机问题

无法删除子领域的会话服务配置 (6318296)

在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” 配置将导致显示错误消息。

解决方法：移除默认的顶层 ID 库 AMSDK1，然后将此库添加回配置中。

此问题已在修补程序 1 中修复。有关对特定平台应用该修补程序的信息，参见第 54 页中的 “Access Manager 7 2005Q4 修补程序 1”。

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

在 CDSSO 模式下使用 Apache 代理 2.2 时，CDC servlet 将在访问代理受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。此问题已在修补程序 1 中修复。有关对特定平台应用该修补程序的信息，参见第 54 页中的 “Access Manager 7 2005Q4 修补程序 1”。

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。

此问题已在修补程序 1 中修复。有关对特定平台应用该修补程序的信息，参见第 54 页中的 “Access Manager 7 2005Q4 修补程序 1”。

命令行实用程序问题

当 Access Manager 指向 Directory Proxy 时，空属性 LDAP 搜索返回错误 (6357975)

如果使用 Sun Java System Directory Proxy Server，空属性 LDAP 搜索会返回错误。例如：

```
# ldapsearch -b base-dn uid=user ""
```

如果 Access Manager 直接指向 LDAP 目录服务器，同样的搜索就会成功。

解决方法：如果使用 Directory Proxy Server，则启用空属性搜索或提供搜索的属性名称。

`amserveradmin` 脚本缺少新的模式文件 (6255110)

安装完成后，在需要运行 `amserveradmin` 脚本以加载服务至 Directory Server 时，该脚本缺少 `defaultDelegationPolicies.xml` 和 `idRepoDefaults.xml` 模式文件。

解决方法：使用带有 `-t` 选项的 `amadmin` CLI 工具手动加载 `defaultDelegationPolicies.xml` 和 `idRepoDefaults.xml` 文件。

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

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，从而导致特定用户 DN 匹配，进而使得没有过期的令牌失效。

解决方法：无。此问题已在修补程序 1 中修复。有关对特定平台应用该修补程序的信息，参见第 54 页中的 “Access Manager 7 2005Q4 修补程序 1”。

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 /var/opt/SUNWam/debug 更改为 /var/opt/SUNWam/stats。

解决方法：无。

顶层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。

会话与 SSO 问题

- 第 79 页中的 “跨时区的 Access Manager 实例使得其他用户会话超时 (6323639)”
- 第 79 页中的 “会话故障转移 (`amsfoconfig`) 脚本在 Linux 2.1 系统上的权限不正确 (6298433)”
- 第 79 页中的 “会话故障转移 (`amsfoconfig`) 脚本在 Linux 2.1 系统上失败 (6298462)”
- 第 80 页中的 “负载平衡器终止 SSL 时，系统创建的服务主机名无效 (6245660)”
- 第 80 页中的 “通过第三方 Web 容器使用 `HttpSession`（无 CR 编号）”

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、并在同一信任圈中的 Access Manager 实例会导致会话超时。

会话故障转移 (`amsfoconfig`) 脚本在 Linux 2.1 系统上的权限不正确 (6298433)

会话故障转移配置脚本 (`/opt/sun/identity/bin/amsfoconfig`) 在 Linux 2.1 系统上拥有不正确的权限且无法执行。

解决方法：更改权限以使 `amsfoconfig` 脚本可执行（例如，755）。

此问题已在修补程序 1 中修复。有关对特定平台应用该修补程序的信息，参见第 54 页中的 “Access Manager 7 2005Q4 修补程序 1”。

会话故障转移 (`amsfoconfig`) 脚本在 Linux 2.1 系统上失败 (6298462)

会话故障转移配置脚本 (`amsfoconfig`) 在 Linux 2.1 服务器上失败是由于对制表符 (`\t`) 的解释不正确。

解决方法：手动配置会话故障转移。有关详细步骤，参见《Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide》中的“Configuring Session Failover Manually”。

此问题已在修补程序 1 中修复。有关对特定平台应用该修补程序的信息，参见第 54 页中的 “Access Manager 7 2005Q4 修补程序 1”。

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"/>
```

通过第三方 Web 容器使用 `HttpSession`（无 CR 编号）

维持验证会话的默认方法是“内部会话”而非 `HttpSession`。默认无效会话最大时间为三分钟便已足够。`amtune` 脚本将 Web Server 或 Application Server 的默认无效会话最大时间设置为一分钟。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 容器的最大 `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

- 第 81 页中的 “Access Manager 启动时出现调试错误 (6309274, 6308646)”
- 第 81 页中的 “将 BEA WebLogic Server 用作 Web 容器”

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。

将 BEA WebLogic Server 用作 Web 容器

如果通过将 BEA WebLogic Server 用作 Web 容器来部署 Access Manager，则可能会无法访问 Access Manager。

解决方法：重新启动 WebLogic Server 以使 Access Manager 可以访问。

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：要解决此问题，在启动 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 或 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;
```

联合与 SAML 问题

运行 Web 服务范例时返回 “ 未找到资源提供 ” (6359900)

将 Access Manager 配置为访问 *AccessManager-base*`/SUNWam/samples/phase2/wsc` 目录（Solaris 系统）或 *AccessManager-base* `/identity/samples/phase2/wsc` 目录（Linux 系统）下的 Web 服务范例后，查询 “搜索服务” 或修改 “资源提供” 会返回错误消息：“未找到资源提供” 。

AccessManager-base 是基安装目录。Solaris 系统的默认基安装目录是 `/opt`，而 Linux 系统则是 `/opt/sun`。

解决方法：

1. 转到以下范例目录：*AccessManager-base* `/SUNWam/samples/phase2/wsc` 目录（Solaris 系统）或 *AccessManager-base*`/identity/samples/phase2/wsc` 目录（Linux 系统）
2. 在 `index.jsp` 文件中，搜索以下字符串：

   ```
   com.sun.org.apache.xml.security.utils.XMLUtils.outputDOM
   ```

3. 如果某行包含在上一步骤中找到的字符串，则在该行前插入以下新行：

   ```
   com.sun.org.apache.xml.security.Init.init();
   ```

4. 重新运行范例。（无需重新启动 Access Manager。）

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，则联合失败。

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。此问题已在修补程序 1 中修复。有关对特定平台应用该修补程序的信息，参见第 54 页中的 “Access Manager 7 2005Q4 修补程序 1” 。

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，并尝试添加“员工配置文件服务资源提供”，则抛出异常。

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 (Globalization, g11n) 问题

未将用户语言环境首选项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，而使用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。

如果在 IBM WebSphere 上部署 Access Manager，则欧洲语言的联机帮助不完全可用 (6325024)

在所有欧洲语言环境（西班牙语、德语和法语）中，如果在 IBM WebSphere Application Server 实例上部署了 Access Manager，则不能完全访问所有的联机帮助。对于以下框架，联机帮助将显示“应用程序错误”：

- 上方框架，其中应包括“帮助”按钮和“关闭”按钮。
- 左框架，其中应包括“内容”、“索引”和“搜索”按钮。

解决方法：将浏览器语言设置为“英语”，然后刷新页面以访问左框架。然而上方框架仍会显示 “应用程序错误”

如果在 IBM WebSphere 上部署 Access Manager，则版本信息为空 (6319796)

在所有语言环境中，如果在 IBM WebSphere Application Server 实例上部署了 Access Manager，则单击“版本”按钮时，都看不到产品版本信息。只显示空白页面。

解决方法：无。

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。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：
  1. 单击 “**配置**” 选项卡下方的 “**客户机检测**” 。
  2. 单击 "`genericHTML`" 的 “**编辑**” 链接。
  3. 在 HTML 选项卡下方，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。

文档问题

记录 Access Manager 无法从领域模式返回传统模式 (6508473)

如果在领域模式下安装 Access Manager 7 2005Q4，则无法返回到传统模式。

但是，如果在传统模式下安装 Access Manager 7 2005Q4，可通过使用带 `-M` 选项的 `amadmin` 命令来更改为领域模式。例如：

```
amadmin -u cn=amAdmin,ou=People,dc=example,dc=com -w amadmin-password -M
dc=example,dc=com
```

记录关于禁用持久性搜索的更多信息 (6486927)

Access Manager 使用持久性搜索来接收有关更改过的 Sun Java System Directory Server 条目的信息。默认情况下，Access Manager 在服务器启动过程中创建以下持久性搜索连接：

`aci` - 对 `aci` 属性所做的更改，且使用 LDAP 过滤器 (`aci=*`) 进行搜索

`sm` - Access Manager 信息树（或服务管理节点）中的更改，包括具有 `sunService` 或 `sunServiceComponent` 标记对象类的对象。例如，您可以创建一个策略来定义受保护资源的访问权限，或者您可以修改现有策略的规则、对象、条件或响应提供者。

`um` - 用户目录（或用户管理节点）中的更改。例如，您可以更改用户的名称或地址。

注意 – 不建议禁用所有此类组件的持久性搜索，因为禁用了持久性搜索的组件不能收到来自 Directory Server 的通知。因此，在 Directory Server 中对该特定组件所做的更改将无法通知组件高速缓存，且组件高速缓存将失去时效。

例如，如果您禁用对用户目录 (um) 中更改的持久性搜索，则 Access Manager 服务器将不会收到来自 Directory Server 的信息。因此，代理将不会从 Access Manager 收到使用用户属性的新值来更新其本地用户高速缓存的通知。然后，如果应用程序向代理查询用户属性，它会收到该属性的旧值。

仅在特定环境中确实必要时使用此属性。例如，如果您知道生产环境中不会发生服务配置更改（与任何服务（例如“会话服务”和“验证服务”）值的更改相关），则可以禁用对“服务管理”(sm) 组件的持久性搜索。不过，如果任何服务发生了任何更改，则需要重新启动服务器。同样的情形也适用于 `aci` 和 `um` 值所指定的其他持久性搜索。

有关更多信息，请参见第 53 页中的 “CR# 6363157：如果确实需要，新属性可禁用持久性搜索”。

记录 Access Manager 支持和不支持的权限 (2143066)

权限定义管理员的访问权限，此类管理员为领域内存在的角色或组的成员。Access Manager 允许您为以下管理员类型配置权限：

- 领域管理员，可执行所有与领域相关的任务，包括定义身份认证系统信息库（数据存储库）、配置验证和定义策略。
- 策略管理员，可在现有领域中配置策略。

支持以下权限：

- 所有领域和策略属性的读写访问权限。为领域管理员定义读写访问权限。
- 仅针对策略属性的读写访问权限。为策略管理员定义读写访问权限。
- 支持的权限组合：仅针对策略属性的读写访问权限和对数据存储库的只读权限。不支持其他权限组合。

记录基于 cookie 的粘性请求路由 (6476922)

将 Access Manager 服务器部署到负载平衡器后面后，基于 cookie 的粘性请求路由可避免客户机请求被错误地路由到不正确的 Access Manager 服务器（即路由到没有托管该会话的服务器）。已在 Access Manager 7 2005Q4 修补程序 3 中实现此功能。

在以前的操作中，由于没有基于 cookie 的粘性请求路由，来自不基于任何浏览器的客户机（如使用远程 Access Manager 客户机 SDK 的策略代理和客户机）的请求经常被错误地路由到没有托管会话的 Access Manager 服务器。然后，为了将请求发送到正确的服

务器，Access Manager 服务器必须使用后台频道通信来验证会话，这通常会导致某种程度的性能降级。基于 cookie 的粘性请求路由不必进行此类后台频道通信，因而提高了 Access Manager 的性能。

要实施基于 cookie 的粘性请求路由，必须将 Access Manager 部署配置为一个站点。有关信息，参见《Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide》中的“Configuring an Access Manager Deployment as a Site”。

要配置基于 cookie 的粘性请求路由：

1. 要指定 cookie 名称，在 `AMConfig.properties` 文件中设置 `com.iplanet.am.lbcookie.name` 属性。然后，Access Manager 会使用两个字节的服务器 ID（例如 01、02 和 03）生成负载平衡器 cookie 值。如果未指定 cookie 名称，则 Access Manager 会使用默认名称 `amlbcookie` 加上两个字节的服务器 ID 来生成负载平衡器 cookie 值。

   如果在 Access Manager 服务器上设置 cookie 名称，则必须在策略代理的 `AMAgent.properties` 文件中使用相同的名称。同样，如果使用 Access Manager 客户机 SDK，也必须使用与 Access Manager 服务器使用的同一 cookie 名称。

   注意：请勿设置 `com.iplanet.am.lbcookie.value` 属性，因为 Access Manager 会使用两个字节的服务器 ID 来设置 cookie 值。
2. 使用步骤 1 中得到的 cookie 名称来配置负载平衡器。可将硬件或软件负载平衡器与 Access Manager 部署一起使用。
3. 如果实施了会话故障转移，则同时对策略代理和 Access Manager 服务器启用 `com.sun.identity.session.resetLBCookie` 属性。
   - 对于策略代理，在 `AMAgent.properties` 文件中添加并启用此属性。
   - 对于 Access Manager 服务器，在 `AMConfig.properties` 文件中添加并启用此属性。

   例如：

   ```
   com.sun.identity.session.resetLBCookie='true'
   ```

   如果发生故障转移，则将会话路由至备用 Access Manager 服务器，并使用备用 Access Manager 服务器的服务器 ID 来设置负载平衡器 cookie 值。然后该会话的任何后续请求都将路由至备用 Access Manager 服务器。

记录 Windows 2003 的 Windows 桌面 SSO 配置 (6487361)

要在 Windows 2003 上配置 Windows 桌面 SSO（如《Sun Java System Access Manager 7 2005Q4 管理指南》中的“配置 Windows 桌面 SSO”中所述），可使用以下 `ktpass` 命令：

```
ktpass /out filename /mapuser username
/princ HTTP/hostname.domainname /crypto encryptiontype /rndpass
/ptype principaltype /target domainname
```

例如：

```
ktpass /out demo.HTTP.keytab
/mapuser http /princ HTTP/demo.identity.sun.com@IDENTITY.SUN.COM
/crypto RC4-HMAC-NT /rndpass /ptype KRB5_NT_PRINCIPAL /target IDENTITY.SUN.COM
```

有关语法定义，参见以下站点：

http://technet2.microsoft.com/WindowsServer/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true

记录设置分布式验证 UI 服务器密码的步骤 (6510859)

以下步骤说明如何为与 Access Manager 服务器通信的分布式验证 UI 服务器设置加密的密码。

要为分布式验证 UI 服务器设置密码：

1. 在 Access Manager 服务器上：
   a. 使用 `ampassword -e` 实用程序加密 `amadmin` 密码。例如，在 Solaris 系统上：

      ```
      # cd /opt/SUNWam/bin
      # ./ampassword -e amadmin-password
      AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      ```

      保存该加密值。
   b. 从 Access Manager 服务器的 `AMConfig.properties` 文件中复制并保存 `am.encryption.pwd` 属性值。例如：

      ```
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```
2. 在分布式验证 UI 服务器上，对 `AMConfig.properties` 文件执行以下更改：
   a. 注释掉 `com.iplanet.am.service.password` 属性。
   b. 将 `com.iplanet.am.service.secret` 属性设为步骤 1a 中得到的加密 `amadmin` 密码。
   c. 添加从步骤 1b 中复制的 `am.encryption.pwd` 和加密的值。例如：

      ```
      com.sun.identity.agents.app.username=username
      #com.iplanet.am.service.password=password
      com.iplanet.am.service.secret=AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```
3. 重新启动分布式验证 UI 服务器。

“创建新站点名称”的在线帮助需要更多信息 (2144543)

Access Manager 控制台在线帮助的“配置”>“系统属性”>“平台”下缺少“创建新站点名称”的“保存”步骤。如果在添加新站点名称后没有单击“保存”然后又接着尝试添加一个实例名，进程将失败。因此，在添加站点名称后务必单击“保存”，然后再添加实例名。

记录 Windows 系统上的管理员密码配置参数为 ADMIN_PASSWD (6470793)

在 Solaris 和 Linux 系统上，`amsamplesilent` 文件中的 Access Manager 管理员 (`amadmin`) 密码配置参数为 `ADMINPASSWD`。但是，在 Windows 系统上，`AMConfigurator.properties` 文件中的此参数为 `ADMIN_PASSWD`。

如果要在 Windows 系统上运行 `amconfig.bat`，则使用 `ADMIN_PASSWORD` 参数而非 `ADMINPASSWD` 在 `AMConfigurator.properties` 文件中设置 `amadmin` 密码。

发行说明中为某些已知问题提供的解决方法有错 (6422907)

已更正了第 82 页中的 “运行 Web 服务范例时返回“未找到资源提供”(6359900)”的解决方法的步骤 3。

对 AMConfig.properties 中的 com.iplanet.am.session.protectedPropertiesList 的说明 (6351192)

`com.iplanet.am.session.protectedPropertiesList` 参数允许您保护特定核心和内部会话属性，防止它们被会话服务的 `SetProperty` 方法远程更新。通过设置此“隐藏”的关键安全性参数，可以自定义会话属性以参与授权以及其他 Access Manager 特性。若要使用此参数：

1. 使用文本编辑器将参数添加到 `AMConfig.properties` 文件中。
2. 将参数设置为需要保护的会话属性。例如：

   ```
   com.iplanet.am.session.protectedPropertiesList =
   PropertyName1,PropertyName2,PropertyName3
   ```

3. 重新启动 Access Manager Web 容器以使这些值生效。

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的角色（修复了 CR 6349959）。在 Access Manager 7 2005Q4 管理控制台“LDAPv3 插件支持的类型和操作”字段的 LDAPv3 配置中，按以下格式输入值：

```
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
```

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

服务器端 AMConfig.properties 文件中的 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。该属性的格式为 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"。

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。

有关详细信息，参阅问题 ID 5110285（XML 加密需要 Bouncy Castle JAR 文件）。

文档更新

Sun Java System Access Manager 7 2005Q4 文档集

下表列出了自发行最初版本以来已发布的新的和已修订的 Access Manager 7 2005Q4 文档。要访问这些文档，请参见 Access Manager 7 2005Q4 文档集：

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

表 7 Access Manager 7 2005Q4 文档更新历史记录

标题	出版日期
Sun Java System Access Manager 7 2005Q4 发行说明	参见 “表 1”。
Sun Java System Access Manager 7 2005Q4 管理指南	2006 年 2 月
Sun Java System Access Manager 7 2005Q4 Developers Guide	2006 年 2 月
Sun Java System Access Manager Policy Agent 2.2 User's Guide	2006 年 2 月
Sun Java System Access Manager 7 2005Q4 C API Reference	2006 年 2 月
Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide	2006 年 2 月
Technical Note: Using Access Manager Distributed Authentication	2006 年 2 月
Technical Note: Installing Access Manager to Run as a Non-Root User	2006 年 2 月

表 7 Access Manager 7 2005Q4 文档更新历史记录 （续）

标题	出版日期
Sun Java System SAML v2 Plug-in for Federation Services User's Guide	2006 年 2 月
Sun Java System SAML v2 Plug-in for Federation Services Release Notes	2006 年 2 月
Sun Java System SAMLv2 Plug-in for Federation Services Java API Reference	2006 年 2 月
Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide	2006 年 1 月
Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide	2005 年 12 月
Sun Java System Access Manager 7 2005Q4 Technical Overview	2005 年 12 月

Sun Java System Federation Manager 7.0 2005Q4 文档集

要访问 Federation Manager 7.0 2005Q4 文档集中的文档，请参见：

http://docs.sun.com/coll/1321.1

Sun Java System Access Manager Policy Agent 2.2 文档集

当前正在修订 Access Manager Policy Agent 2.2 文档集以记录新的代理。要访问此文档集中的文档，请参见：

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

可再分发的文件

Sun Java System Access Manager 7 2005Q4 不含任何可以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。如果您要提出意见，请转到 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 819-3475，文档标题为《Sun Java System Access Manager 7 2005Q4 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 819–2134–20，文件标题为《Sun Java System Access Manager 7 2005Q4 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。