Sun Java™ System Identity Server 发行说明

版本 2004Q2

文件号码 817-7135

本发行说明包含 Sun Java System Identity Server 2004Q2 发行时可用的重要信息。这里介绍了新功能和增强功能、已知的问题和限制及其他信息。开始使用 Identity Server 2004Q2 之前，请先阅读此文档。

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

http://docs.sun.com/db/prod/entsys.04q2 及
http://docs.sun.com/db/prod/entsys.04q2?l=zh

请在安装和设置软件之前先访问此网站，并定期查看最新的发行说明和产品文档。

本发行说明包含以下内容：

本文档中引用了第三方 URL，并提供附加相关信息。

注 对于本文档提到的第三方 Web 站点，Sun 不负责其可访问性。此类站点或资源直接或间接提供的任何内容、广告、产品或其他材料均未经 Sun 正式认可，Sun 对此不负任何责任。对于因使用或信任此类站点提供的任何内容、商品或服务，而直接或间接造成任何实际或所谓的损害或损失，Sun 概不负责。

发行说明修订历史记录

表 1 修订历史记录

日期	更改说明
2004 年 6 月 23 日	第二次发行本发行说明以便支持 Linux。还增加了对已知问题列表的描述。
2004 年 5 月 18 日	初次发行本发行说明。

关于 Identity Server 2004Q2

Sun Java™ System Identity Server 是一种身份管理解决方案，其设计目的是满足急速扩大的企业的需求。利用 Identity Server，您可以将雇员、商业伙伴及供应商的标识统一放入一个在线目录。然后，它提供一种建立访问贵公司信息的策略和权限的方法。Identity Server 对于您的全部数据、服务以及了解信息访问情况而言很关键 — 对所有内部和外部业务关系很关键。

此发行版的新功能

Identity Server 2004Q2 的新功能包括以下几个方面 （关于这些功能的详细说明，请参阅 《*Sun Java System Identity Server Technical Overview*》）：

- 联合管理的增强功能
  - Identity Federation Framework 1.2
  - Liberty Identity Web Services Framework 1.0
  - Identity Service Instance Specification 1.0
- 支持 SAML 1.1
- 自定义 JAAS Authorization Framework
- 验证的增强功能
  - Windows 桌面 SSO 验证服务
  - JAAS 共享状态
  - Java 数据库连接验证模块示例
  - Java 卡数字身份验证模块示例
- Identity Server 控制台的增强功能
  - 嵌套组支持
  - 集中代理管理
  - 显示选项和可用操作
- Application Server 的会话故障转移
- 配置和微调脚本

硬件和软件要求

本发行版的 Identity Server 要求配备以下硬件和软件。

表 2 硬件和软件要求

组件	Solaris 要求
操作系统	Solaris™ 操作系统 (OS)、 SPARC® Platform Edition，第 8 和第 9 版
	Solaris™ 9 OS、 x86 Platform Edition
	Red Hat™ Linux, Advanced Server 2.1 Update 2
RAM	512 MB
磁盘空间	250 MB，用于 Identity Server 和相关的应用程序

此发行版中修复的错误

下表说明了 Identity Server 2004Q2 中修复的错误：

表 3 Identity Server 2004Q2 中修复的错误

错误编号	说明
4919897	匿名绑定导致验证失败。
4794971	未正确删除启动脚本。
4922287	子组织名称中的撇号导致错误。
4925958, 4948665	使用 zh_CN.GB18030 语言环境时出现问题。
4921424	韩语字符集的默认全球化设置不正确。
4918930	未注册服务被错误地作为已注册服务列出。

安装说明

此发行版的 Identity Server 将 Identity Server 软件包的安装从必须执行的配置步骤中分离出来。在此发行版中，必须使用 Java Enterprise System 安装程序来安装 Identity Server 的第一个实例。

配置脚本

安装完第一个 Identity Server 实例后，可以使用配置脚本在 Sun Java System Application Server 和 Sun Java System Web Server 上创建其他实例。

IS 安装/配置脚本执行以下操作：

- 在单一主机上为 Web 容器部署其他 Identity Server 实例。
- 重新配置 Identity Server 实例。例如：更改 Identity Server 实例的所有者和组 （例如，从超级用户更改为另一用户或组）。
- 将 Identity Server SDK 应用于网络应用程序。
- 卸载其他实例 （您应该使用 JES 卸载程序来卸载第一个实例）。

有关详细说明，请参阅 《*Identity Server 管理指南*》。请注意， amserver 命令不再受支持。

已知问题和限制

本节包含发行 Identity Server 2004Q2 时已知的重要问题的列表。本节包括以下主题：

- 国际化 (i18n)
- Cookie
- Cookie 夺取

安装

根后缀中的逗号可能会导致安装失败 (#4750396)

在安装过程中，当要求指定 Identity Server 根后缀时，请勿在根识别名 (RDN) 中使用逗号。

验证

持久 Cookie 模式属性不一致 (#5038544)

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

解决方法

非 DN 值使用 UserToken， DN 值使用 Principal。

管理员无法从父组织添加角色 (#5042217)

如果在对子组织配置验证服务时，包括了用户动态概要文件创建角色功能，则在启用动态概要文件创建的情况下登录该服务，在查看该用户属性时，并不会看到被分配的角色，因为验证服务仅对属于子组织的角色有效。

添加代理属性后无法登录 Identity Server (#4966788)

如果将代理属性添加到 server.xml，然后重新启动 Identity Server，将不能登录 Identity Server 控制台。此类情况仅在 Proxy Server 不能识别 Identity Server 时才会出现。

解决方法

在 server.xml 中，将 http.nonProxyHosts 设置为全限定主机名，然后重新启动服务器。例如：

```
<JVMOPTIONS>-Dhttp.nonProxyHosts=Identity_Server_FQDN</JVMOPTIONS>
```

为优化性能，即使 Proxy Server 能够识别 Identity Server，也应设置本解决方法中定义的属性。

重新装入“会话超时”页面将验证用户的有效用户名和密码 (#4697120)

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

必须为多个 SafeWord 服务器指定不同的目录 (#4756295)

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

命令行工具

在以 SSL 模式运行 amadmin 时， JVM 可能会终止 (#5009031)

在以安全模式运行服务器时，连续使用 amadmin 可能会终止 JVM。

如果您遇到这种情况，请与 Sun Java System 软件支持服务联系。

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

am2bak 和 bak2am 恢复脚本对在 Linux 上运行的 Identity Server 无效。

解决方法

1. 纠正以下命令的路径：

   ECHO=/usr/bin/echo

   应为 ECHO=/bin/echo

   uid=`/usr/xpg4/bin/id -un`

   应为 uid=`/usr/bin/id -un`

   /usr/bin/tar

   应为 /bin/tar

   usr/bin/rm

   应为 /bin/rm

   /usr/bin/grep

   应为 /bin/grep

   /usr/bin/ps

   应为 /bin/ps

   /usr/bin/ls

   应为 /bin/lsv

2. 修改 check_for_invalid_chars() 函数。例如：

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

```
            return 1
        else
            return 0
        fi
    }
```

在 Linux 系统上， amserver stop 无法停止 amunixd 进程 (#5050332)

在 Linux 系统上， `/etc/init.d/amserver stop` 命令无法停止 `amunixd` 验证帮助程序进程。

解决方法
首先，将 `ps` 命令与 `f` 选项配合使用来确定 `amunixd` 进程 ID：

```
ps -efl | grep /opt/sun/identity/share/bin/amunixd
```

然后，将 `kill` 命令与此进程 ID 配合使用来停止 `amunixd` 进程。

在运行 am2bak 时出现失败消息 (#5043752)

在使用 am2bak 执行备份进程时，您可能会接收到表示备份进程失败的错误消息，实际上备份并未失败。

amadmin 返回的 “错误消息”不正确 (#5008960)

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

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

如果执行 Identity Server 控制台安装， amverifyarchive 实用程序在脚本中将不会替换以下标签：

- JSSHOME
- JDK_HOME
- BASEDIR
- PRODUCT_DIR

配置

amconfig 脚本选择 “稍后配置”选项后，无法配置本地化的 Identity Server (#5062437)

如果您使用 Java Enterprise System 安装程序安装了 Identity Server 2004Q2 的本地化版本，并且选择 “稍后配置”选项，则 amconfig 脚本随后将无法配置 Identity Server。

解决方法
在运行 amconfig 脚本之前，根据用于运行 Identity Server 的 Web 容器编辑 Web 容器脚本。

1. 找到 Web 容器脚本：
   - Web 服务器：amws61config
   - Application Server：amas70config

   两个脚本同时位于 Solaris 系统上的 *IdentityServer_base*/SUNWam/bin 目录，或 Linux 系统上的 *IdentityServer_base*/identity/bin 目录。
2. 在 Web 容器脚本中，将 /WEB-INF 目录添加至以下 if 语句中的 $DEPLOY_SRC 变量：

```
if [ ! -d $DEPLOY_SRC/WEB-INF ]; then
  mkdir -p $DEPLOY_SRC
  cd $DEPLOY_SRC
  jar xf $PKGDIR/$warfile
```

3. 运行 amconfig 脚本以配置 Identity Server。有关 amconfig 脚本的信息，请参阅 《*Identity Server 2004Q2 管理指南*》：

   http://docs.sun.com/doc/817-7011

请勿使用带 “无提示文件选项”的 amconfig (#5003430, 5003386, 5000964)

请勿使用 amconfig 的交互模式。示例：amconfig -s　结果无法预料。

解决方法
在无提示模式下调用 amconfig。示例：amconfig -s *path-to-silent-file*

无论后端名为何，始终为 userRoot 创建索引 (#5002886)

index.ldif 对 userRoot 进行硬编码以便为属性创建索引。可以在位于任意名称后端数据库的根后缀上安装 Identity Server。可以将 nsslapd-suffix=SUFFIX_NAME 用作过滤器，通过具有基础 cn=config 的 ldapsearch 命令获得后端名。

联合

如果属性值为空，会抛出 PP Modify 的异常 (#5047103)

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

策略生效要求重启服务器 (#5045036)

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

Identity Server 控制台

将具有 “定义的访问权限”的角色创建为 “组织管理员”时出错 (#5037978)

如果以 “组织管理员”的身份登录，然后创建一个角色，并为该角色分配 “访问权限”（如，创建 “组织管理员”和 “帮助台管理员”角色 ），将收到错误信息。

组织管理员权限的设置是为了防止他们修改组织的值。当创建具有权限的角色时，将尝试修改组织项中的 ACI。

解决方法

1. 安装完成后，转到 XML 文件所在的目录。缺省情况下，目录为：

   /etc/opt/SUNWam/config/xml (Solaris)

   /etc/opt/sun/identity/config/xml (Linux)

2. 备份 amAdminConsole.xml 文件。例如：

   cp amAdminConsole.xml amAdminConsole.bak

3. 编辑 amAdminConsole.xml。

a. 搜索所有以 “S1IS Organization Admin Role access allow read” 开始的行，删除该 ACI。例如，删除所有出现的用于组织管理员角色的 ACI：

aci:(target="ldap:///ORGANIZATION")(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com))))(targetattr != "nsroledn")(version 3.0; acl "S1IS Organization Admin Role access allow read"; allow (read,search) roledn = "ldap:///ROLENAME";)

b. 搜索所有以 “S1IS Organization Admin Role access allow all” 开始的行，编辑该 ACI，删除 ACI 开头的 '*,'：

aci:(target="ldap:///*,

编辑所有出现的用于组织管理员角色的 ACI：例如：

修改该 ACI：

aci:(target="ldap:///*,ORGANIZATION")(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help D esk Admin Role,dc=iplanet,dc=com))))(targetattr != "nsroledn")(version 3.0; acl "S1IS Organization Admin Role access allow all"; allow (all) roledn = "ldap:///ROLENAME″;)

为：

aci:(target="ldap:///ORGANIZATION")(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com))))(targetattr !="nsroledn")(version 3.0; acl "S1IS Organization Admin Role access allow all"; allow (all) roledn = "ldap:///ROLENAME";)

c. 保存文件。

4. 使用 amadmin 命令行工具删除 iPlanetAMAdminConsoleService：

/opt/SUNWam/bin/amadmin -u "uid=amAdmin,ou=People,dc=iplanet,dc=com" -w "iplanet1" -r "iPlanetAMAdminConsoleService"

5. 如果文件已成功删除，将显示以下信息：

Deleting Service Schema iPlanetAMAdminConsoleService

Success 0:Successfully completed.

6. 使用 amadmin 命令行工具通过新改的 amAdminConsole.xml 重新导入同一服务：

/opt/SUNWam/bin/amadmin -u "uid=amAdmin,ou=People,dc=iplanet,dc=com" -w "iplanet1" -s /etc/opt/SUNWam/config/xml/amAdminConsole.xml

7. 如果文件已成功加载，将显示以下信息：

   Loading Service Schema XML /etc/opt/SUNWam/config/xml/amAdminConsole.xml

   Success 0:Successfully completed.

8. 重新启动 Identity Server。

控制台示例无法编译 (#5026635)

某些 Identity Server 控制台示例不能编译，原因是此发行版更改了文件位置。

解决方法

在 rules.mk 文件中将现有 jato.jar 路径改为以下路径：

$*USER_DIR*/share/lib/identity/console-war/WEB-INF/lib/jato.jar

使用 SAML 服务不能创建用户 (#5038600)

只有顶层管理员才能在分配 SAML 服务的同时创建用户。

解决方法

组织管理员需要在不使用 SAML 服务的情况下创建用户。用户创建完成后，可以通过 “用户配置文件”页面添加该项服务。

单击 “上一步”按钮时值未保留 (#4992972)

每当出现多页面处理情况，如创建组、角色或为策略添加条件时，选中 “上一步”按钮，前一页上的值将不能恢复。

策略管理员无法修改自己的配置文件 (#5042100)

策略管理员不能通过 Identity Server 控制台修改自己的配置文件。

解决方法

将 “浏览视图”的 “显示选项”设置为 “用户”，将用户的 “可用操作”设置为 “完全访问”。

在禁用 “用户管理”的情况下搜索 “用户”时，控制台出错 (#5049218)

如果禁用了 “用户管理”之后执行用户搜索，可能会收到 “服务器错误”。

解决方法

使用新的 JSP 替换 PMAdminRoldSelect.jsp。新的 JSP 位于以下位置：

IdentityServer_base/applications/console/policy

实体说明搜索过滤器无法正常工作 (#4959895)

在 “联合模块”中的 “实体说明符”视图下，使用 “搜索”字段寻找实体说明符时，搜索结果有时不准确。

“**”搜索掩码无法工作 (#4961370)

如果在 Identity Server 控制台中将不带有附加字符的 “**”用作搜索过滤器掩码，搜索将失败。搜索字段接受带有附加字符的 “**”，如：**a 或 a**。

联合管理模块中的托管提供商存在刷新问题 (#4915894)

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

解决方法

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

控制台不能刷新用户属性更改 (#4931455)

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

Internet Explorer 出现端口问题 (#4864133)

由于与 Internet Explorer 不兼容，在运行一个 http 时，不得将 80 用作 Identity Server 端口号，在运行 https 时，不得将 443 用作 Identity Server 端口号。

日志服务

启用 Java 安全性时出现日志问题 (#4926520)

启用 Java 安全性时， jdk_logging.jar 可能无法运行。

解决方法

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

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

策略

参考策略规则中的修改未反映在子组织中 (#5016725)

删除根组织的参考策略后，子组织中的标准策略规则未被删除 （也不能删除）。

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

匹配条目未返回 Identity Server 控制台，尽管已达到 nslookthrough 中定义的管理限制。

解决方法

调整 nslookthroughlimit 参数以补足条目数。

未对别名令牌强制执行策略 (#4985823)

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

策略范例有问题 (#4923898)

位于策略范例中的 Readme.html 不包括导致范例无法运行的信息。为了运行范例， LD_LIBRARY_PATH 需要包含到 NSPR、 NSS 和 JSS 共享库的路径。

将环境变量 LD_LIBRARY_PATH 设置为 /usr/lib/mps/secv1 （对于 Solaris）或 /opt/sun/pirvate/lib （对于 Linux)。如果未正确设置此环境变量，您将遇到错误。

会话服务

未清除闲置会话 (#4959071)

当前未正确清除闲置会话。请与支持人员联系，以获得修补程序以解决此问题。有关详细信息，请参见如何报告问题和提供反馈。

SDK

使用 SSL 服务器的 Identity Server SDK 安装的 certutil 的文档使用 (#5027614)

用户在尝试从仅 SDK 机器与具备 SSL 功能的 Identity Server 2004Q2 服务器通信时，遇到与安全相关的错误和异常。在此方案中， Identity Server SDK 未部署在 Web 容器上或部署在第三方 Web 容器上，例如， BEA WebLogic Server 或 IBM WebSphere Application Server。

解决方法
在仅 SDK 机器上安装证书数据库，并将 Identity Server 服务器的根 CA 证书安装至此数据库：

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

   在 Solaris 系统上：

   cd *JavaEnterpriseSystem_base*/Solaris_*arch*/Product/shared_components/Packages
   pkgadd -d . SUNWtlsu

   在 Linux 系统上：

   cd *JavaEnterpriseSystem_base*/Linux_x86/Product/shared_components/Packages
   rpm -Uvh sun-nss-3.3.10-1.i386.rpm
4. 为该证书数据库的令牌密码创建密码文件。例如：

   在 Solaris 系统上：

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

   在 Linux 系统上：

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

   其中， *cert-database-password* 是令牌密码。

5. 检查 LD_LIBRARY_PATH 变量：

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

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

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

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

   例如：

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

   其中：

   certutil-home 是 certutil 的位置：

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

   cert-database-dir 是证书和密钥数据库的数据库目录。

   config-home 是 Identity Server 配置文件的位置：

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

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

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

8. 使用编辑器查看 AMConfig.properties 文件并确认以下值

   - 证书数据库目录：com.iplanet.am.admin.cli.certdb.dir
   - 前缀：com.iplanet.am.admin.cli.certdb.prefix
   - 密码文件：com.iplanet.am.admin.cli.certdb.passfile

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

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

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

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

BasicEntitySearch 硬编码为 uid (#5041529)

如果安装 Identity Server 时将用户命名属性设置为 cn，然后登录 Identity Server 控制台并创建一个代理实体，则 “导航窗格”中将不显示该代理实体。这是因为该实体的搜索模板硬编码为 uid。

解决方法

在 Directory Server 管理控制台中将过滤器从 uid 改为 cn 并重新启动服务器。

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

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

Identity Server 将 JSS 用作安全提供者，而 Weblogic 在缺省情况下使用 JCE。当调用 init 方法时，Weblogic 尝试使用 JCE 来验证其许可证，而 JSS 正在初始化。

解决方法

将 AMConfig.properties 文件中的缺省安全加密从 JSSEncryption 改为 JCEEncryption。

任何以 “{SSHA}”符号开始的密码均不可用 (#4966191)

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

AMConfig.properties 中的 smtp Server Port 属性不正确 (#5048378)

AMConfig.properties 中的 smtp server port 属性不正确。已发送邮件查找 com.iplanet.am.smtpport 的方式不正确。

命名属性应为小写 (#4931163)

由于 SDK 的限制，命名属性必须为小写。例如，如果您在 Directory Server 之上安装了 Identity Server 实例，并在用户命名属性定义为 CN 的情况下装入 Identity Server 模式，则用户创建将失败。

解决方法

在 Directory Sever 控制台中更改命名属性。例如，将创建模板的 basicuser 用户命名属性由 CN 更改为 cn。

“组创建”选项仅添加一个 memberURL 属性 (#4931958)

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

服务注册问题 (#4853809)

如果您创建了服务模板，并在父组织中进行了注册，然后尝试为子组织注册这些模板，则已在父组织中注册的某些服务将无法在子组织中注册，尽管 amConsole.access 显示这些服务已注册。

解决方法

刷新 Identity Server 控制台并重新注册服务。

用户以服务类型角色登录时服务消失 (#4931907)

如果以服务类型角色登录的用户在管理起始视图设置为 orgDN 的情况下登录到 Identity Server，然后用户尝试撤消注册某项服务，则列出的所有服务将消失。

解决方法

重新启动服务器，服务将重新显示。

单点登录

无法用不同的部署 URI 执行 SSO (#4770271)

如果两个不同 Identity Server 实例间的部署 URI 不同，则单点登录将无法正常运行。

国际化 (i18n)

“注册所有服务”并未注册全部可用服务 (#4853809)

如果通过 Identity Server 控制台注册所有服务，有些服务可能并未列在 “可用服务”中。

解决方法

请勿多次单击 “添加”按钮。

对于用户，带 “策略模式” 的服务显示为 “可添加” (#4996479)

给用户添加服务时， wsrp 用户服务显示为可用。但是，如果已经被选中，它却不能被添加，因此会失败。而且，如果连同用户服务选中多项服务，则所有的添加都失败。

解决方法

请勿从 “身份认证管理” 模块添加 WSRP 服务。

日语浏览器的 “验证级别” 登录失败 (#5013994)

第一次以 “验证级别” 登录 Identity Server 时，如果浏览器语言设置为 ja，则 Identity Server 对以下日语浏览器无效：

- IE6.0ja
- IE7.0ja
- Mozilla1.2.1

解决方法

显示 “验证模块被拒绝” 错误时，请单击 “回到登录页” 链接。或者，输入以下 URL：

http://*server*:*port*/amserver/UI/Login?*authlevel=number*

日语在线帮助显示不正确 (#5024138)

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

解决方法

创建符号链接，从 docs_en 到 docs_en_US°£

用户 ID 生成模式从名字 / 姓氏生成用户 ID (#5028750)

Identity Server 不支持多字节用户 ID。在缺省情况下，用户 ID 生成模式从名字和姓氏生成用户 id。

客户机检测功能工作不正常 (#5028779)

在 “客户机检测” 服务中，删除 UTF-8 无法正常工作。

解决方法

如果删除 UTF-8 字符集，请在更改完成后重新启动 Web 容器。

G11NSetting 无法处理 Q 因数中的空格 (#5008860)

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

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

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

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

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

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

日志文件在 Ja 语言环境下成为乱码 (#4882286)

以下日志文件含有日语字符，打开时成为乱码：

IdentityServer_base/SUNWam/debug 目录下的所有文件 （deploy.log 和 undeploy.log 除外）。

URL 中的语言环境参数显示混合语言的登录页面 (#4915137)

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

解决方法

将以下符号链接

I*dentityServer_base*/SUNWam/web-apps/services/config/auth/default

更改为

IdentityServer_base/SUNWam/web-apps/services/config/auth/default_en

HTTP Basic 的错误消息未本地化 (#4921418)

如果您使用 HTTP Basic 验证模块登录，并单击 “取消”按钮，将会显示 “未本地化”错误消息。这是 Application Server 的已知问题；它仅会在 Identity Server 与 Application Server 共同部署时发生。

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

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

解决方法

运行语言环境设置为 en 的 Application Server。

锁定通知发送不可读的电子邮件 (#4938511)

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

解决方法

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

user1@example.com|zh|GB2312

冲突解决级别不随语言环境的改变而相应变化。 (#4922030)

如果用户以某种特定的语言环境 （例如 zh）登录到 Identity Server 控制台、注册 “验证配置”服务，为服务创建了模板，然后注销并在另一种语言环境中重新登录后，“冲突解决级别”项目将以原始语言环境的格式不正确地列出。

仅有英文 am2bak 和 bak2am 版本消息 (#4930610)

本发行版仅能提供英文版的 am2bak 和 bak2am 恢复实用程序的版本消息。

多字节名称在自注册中不起作用 (#4732470)

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

解决方法

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

或

用户可以在 “自注册”登录页面上选择 “创建个人”选项。

日文版 Identity Server 不能与 Netscape 6.22 和 6.23 一起运行 (#4902421)

在日文版 Identity Server 6.1 中，您不能用 Netscape 6.22 或 6.23 登录控制台。

时间条件格式未更改 (#4888416)

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

Hour:Minute AM/PM

backup_restore.po 中 msgid-msgstr 对的消息未本地化 (#4916683)

收到说明 backup_restore.po 脚本中缺少 msgid-mgstr 对并且 Directory Server 证书未备份的消息时，Directory Server 证书仍会被进行备份。此消息尚未本地化。

客户机检测屏幕未本地化 (#4922013)

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

已更新的 genericHTML 客户机属性未被应用 (#4922348)

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

解决方法

用 amserver 重新手动启动服务器。

日志文件标题未本地化 (#4923536)

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

amSSO.access 中的数据字段值未本地化 (#4923549)

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

Exception.jsp 有固定编码的消息 (#4772313)

Exception.jsp 未本地化，它包含固定编码的标题、错误消息和版权信息。仅在极端的情况下调用该异常错误 jsp 页。例如，在 Directory Server 关闭时，或在不能调用 Identity Server 服务并且该 jsp 页不可本地化时。

Cookie

Cookieless 模式无效 (#4967866)

如果浏览器接入 Identity Service 然后关闭 cookie 支持，而且该浏览器支持 cookie，则该浏览器将继续发送旧的 Identity Service cookie。这会导致对 Identity Server 资源的访问被拒绝。

解决方法
选择以下一个解决方法：

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

Cookie 夺取

当应用程序使用不可信的会话 cookie 时，安全性可能会降低。

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

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

- 所有应用程序共享同一个 `http` 会话 cookie。这可能导致一个 rouge 应用程序夺取会话 cookie，然后在另一应用程序中冒充用户。
- 如果应用程序不使用 `https` 协议，则会话 cookie 可能遭受网络窃听。
- 只要有一个应用程序可被夺取，整个基础结构的安全性就会大大折扣。
- rouge 应用程序可使用会话 cookie 来获取用户的配置文件属性并可能进行修改。如果该用户拥有管理权限，则应用程序将能够造成更多损害。

解决方法
请按照以下步骤进行操作：

1. 使用 Identity Server 管理控制台为每个代理设置一个条目。

   a. 在包含要创建的代理的组织内，从 “视图” 菜单中选择 “代理”，然后单击 “新建”。

   b. 提供以下信息：

      名称。输入代理的名称或身份。示例：agent123

      密码。输入代理的密码。示例：agent123

      确认密码。确认该密码。

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

      代理关键字值。使用关键字/值对设置代理属性。Identity Server 使用此属性接收有关用户的证书断言的代理请求。

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

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

      设备状态。输入代理的设备状态。如果设置为 “有效”，则代理可以向 Identity Server 进行验证并与其进行通信。如果设置为 “无效”，则代理不能通过 Identity Server 进行验证。

   c. 单击 “确定”。

2. 对在步骤 1b 输入的密码执行以下命令。

   /opt/SUNWam/agents/bin/crypt_util agent123

   此时输出以下信息：

   WnmKUCg/y3l404ivWY6HPQ==

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

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


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


# Cross-Domain Single Sign On URL

# Is CDSSO enabled.

com.sun.am.policy.agents.cdsso-enabled=true


# This is the URL the user will be redirected to after successful login

# in a CDSSO Scenario.

com.sun.am.policy.agents.cdcservletURL =
http://server.example.com:port/amserver/cdcservlet
```

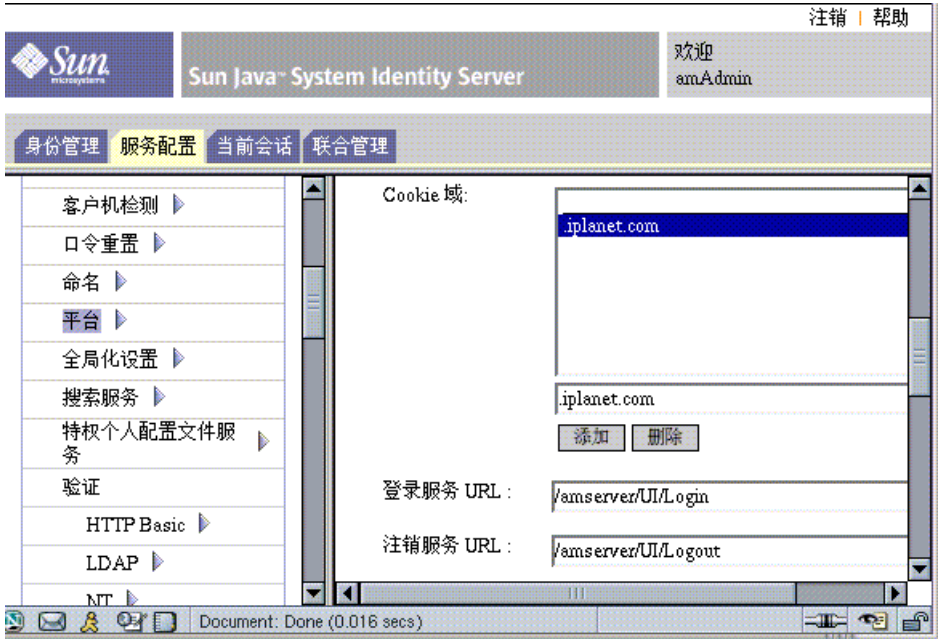
4. 更改 AMConfig.properties 以反映新值，然后重新启动 Identity Server。示例：

```
com.sun.identity.enableUniqueSSOTokenCookie=true

com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer


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

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



6. 在 Cookie 域列表中更改 cookie 域名：

   a. 选择缺省 `iplanet.com` 域，然后单击 “删除”。

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

   示例：server.example.com

   应该会在浏览器上看见两个 cookie 集：

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

可重新分配的文件

Sun Java System Identity Server 2004Q2 不包含可重新分配的任何文件。

如何报告问题和提供反馈

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

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

  此站点包含到知识库、联机支持中心、产品跟踪器以及维护程序和联系支持人员的电话号码的链接。
- 与维护合同相关的本地服务电话号码

为使我们能够更好地帮助您解决问题，请在联系支持人员时准备好以下信息：

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

Sun 欢迎您提出意见

Sun 非常愿意改进其文档，并欢迎您提出意见和建议。请使用网上表格将反馈意见提供给 Sun：

http://docs.sun.com/db/coll/IdentityServer_04q2 及
http://docs.sun.com/db/coll/IdentityServer_04q2_zh

请在相应的字段内填写完整的文档标题和文件号码。您可以在本书的标题页面和文档顶部找到文件号码，文件号码通常包含七个或九个数字。例如，本发行说明文档的文件号码是 817-7135。提出意见时您还需要在表格中输入文件的英文文件号码和标题。本文件的英文文件号码是 817-5712-10，文件标题为 Sun Java Enterprise System Identity Server 2004Q2 Release Notes。

其他 Sun 资源

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

- Sun Java System 文档
  http://docs.sun.com/db/prod/entsys.04q2 及
  http://docs.sun.com/db/prod/entsys.04q2?l=zh
- Sun Java System 专业服务
  http://www.sun.com/service/products/software/javaenterprisesystem/
- Sun Java System 软件产品和服务
  http://wwws.sun.com/software/
- Sun Java System 软件支持服务
  http://www.sun.com/supportraining
- Sun Java System 支持和知识库
  http://sunsolve.sun.com
- Sun Java System 咨询和专业服务
  http://www.sun.com/service/products/software/javaenterprisesystem
- Sun 开发者支持服务
  http://www.sun.com/developers/support