Sun Java™ System

Identity Server 管理指南

2004Q2

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

文件号码：817-7011

目录

关于本指南

《*Sun Java™ System Identity Server 2004Q2 管理指南*》介绍如何通过“用户和命令行界面”管理 Sun Java™ System Identity Server 2004Q2 （以前为 Sun™ ONE Identity Server）。

本前言包含以下内容：

本指南的读者

本 《*管理指南*》适用于要使用 Sun Java System 服务器和软件来实现集成的身份管理和 Web 访问平台的 IT 管理员和软件开发者。

本指南的读者应该熟悉以下概念和技术：

- Sun Java System Directory Server
- 轻便目录存取协议 (LDAP) 概念
- Java™ 技术
- JavaServer Pages™ (JSP) 技术
- 超文本传输协议 (HTTP)

- 超文本标记语言 (HTML)
- 可扩展标记语言 (XML)

Identity Server 2004Q2 文档集

Identity Server 2004Q2 文档包括两组：

- Identity Server 2004Q2 核心文档
- Identity Server Policy Agent 文档

Identity Server 2004Q2 核心文档

Identity Server 2004Q2 文档集包含以下内容：

- *Technical Overview* (http://docs.sun.com/doc/817-5706) 提供关于如下内容的高级概述：Identity Server 各组件如何协同工作以加强身份管理并保护企业资产以及基于 Web 的应用程序。它还介绍基本的 Identity Server 概念和术语。
- *Migration Guide* (http://docs.sun.com/doc/817-5708) 详细介绍如何将现有数据和 Sun Java System 产品部署迁移至最新版本的 Identity Server。有关安装 Identity Server 和其他产品的说明，参见《*Sun Java Enterprise System 2004Q2 安装指南*》 (http://docs.sun.com/doc/817-7056)。
- *管理指南* (http://docs.sun.com/doc/817-7011) 介绍如何使用 Identity Server 控制台以及如何通过命令行管理用户和服务数据。
- *Deployment Planning Guide* (http://docs.sun.com/doc/817-5707) 介绍在现有信息技术基础结构内规划 Identity Server 部署的有关信息。
- *Developer's Guide* (http://docs.sun.com/doc/817-5710) 介绍如何定制 Identity Server 并将其功能集成到组织的当前技术基础结构中。本指南还包含关于本产品及其 API 的程序方面的详细信息。
- *Developer's Reference* (http://docs.sun.com/doc/817-5711) 提供构成公共 Identity Server C API 的数据类型、结构和功能的摘要。

- *Federation Management Guide* (http://docs.sun.com/doc/817-6362) 提供有关基于 Liberty Alliance Project 的 “联合管理”的信息。
- *发行说明* (http://docs.sun.com/doc/817-7135) 在产品发布之后可以联机方式获得。这些发行说明中收集了各种最新信息，包括当前发行版的新功能说明、已知问题和限制、安装说明，以及报告有关软件或文档的问题的方法。

可以在位于 Sun Java System 2004Q2 文档 Web 站点 (http://docs.sun.com/prod/entsys.04q2 及 http://docs.sun.com/db/prod/entsys.04q2?l=zh) 的 Identity Server 页面中找到对*发行说明*的更新和指向核心文档的修改的链接。已更新的文档将会标记上修订日期。

Identity Server Policy Agent 文档

Identity Server 策略代理文档可在以下 Web 站点中找到：

http://docs.sun.com/coll/S1_IdServPolicyAgent_21

获得 Identity Server 策略代理的时间与获取服务器产品本身的时间不同。因此，策略代理文档集可以在 Identity Server 核心文档集之外获得。本文档集包括以下内容：

- *Web Policy Agents Guide* 介绍如何在各种 Web 和代理服务器中安装和配置 Identity Server 策略代理。它还提供疑难解答，以及各代理的专用信息。
- *J2EE Policy Agents Guide* 介绍如何安装和配置可保护各种受托管的 J2EE 应用程序的 Identity Server 策略代理。它还提供疑难解答，以及各代理的专用信息。
- *发行说明*可以在代理集发布后通过联机方式获得。通常，每个代理类型发行版有一个*发行说明*文件。这些*发行说明*中收集了各种最新的信息，包括当前发行版的新功能说明、已知问题和限制、安装说明，以及报告有关软件或文档的问题的方法。

可以在 Sun Java System 文档 Web 站点的 “策略代理”页中找到对发行说明的更新和对策略代理文档的修改。已更新的文档将会标记上修订日期。

关于文档的反馈

Sun Microsystems 和 Identity Server 的技术专家有志于改进文档的质量，并欢迎您提出宝贵的意见和建议。请使用以下基于 Web 的表单向我们提供反馈：

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

请在相应字段内提供完整的文档标题和文件号码。文件号码可在本书的标题页面或文档顶部找到，它通常是一个七位或九位数。例如，《管理指南》的文件号码是 817-7011。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 817-5709，文件标题为 《Sun Java Enterprise System Identity Server 2004Q2 Administration Guide》。

本指南中使用的文档惯例

在 Identity Server 文档中，使用了一些特定的印刷惯例和术语。以下各节将介绍这些惯例。

印刷惯例

本书使用以下印刷惯例：

- *斜体*用于书籍的标题文字、新术语、需要强调的文字和以字面意义使用的文字。
- 等宽字体用于样例代码和代码列表、 API 和语言元素 （如函数名称和类名称）、文件名、路径名、目录名、 HTML 标记以及所有必须在屏幕上键入的文本。
- *斜体衬线字体*用于在代码和代码片段内表示变量占位符。例如，在下面的命令中， *filename* 用作 `gunzip` 命令的参数变量占位符：

  `gunzip -d` *filename*`.tar.gz`

术语

Identity Server 文档集中使用下列术语：

- *Identity Server* 指 Identity Server 和 Identity Server 软件的任何安装实例。

- *策略和管理服务*指在专用的部署容器 （如 Web Server）中安装并运行的 Identity Server 组件和软件的集合。
- *Directory Server* 指已安装的 Sun Java System Directory Server 实例。
- *Application Server* 指已安装的 Sun Java System Application Server （也称为 Sun ONE Application Server）实例。
- *Web Server* 指已安装的 Sun Java System Web Server （也称为 Sun ONE Web Server）实例。
- *运行 Identity Server 的 Web 容器*指安装了策略和管理服务的专用 J2EE 容器 （例如 Web Server 或 Application Server）。
- *IdentityServer_base* 表示 Identity Server 的基本安装目录。 Identity Server 2004Q2 默认基安装和产品目录根据您的特定平台而定：
  - Solaris™ 系统：`/opt/SUNWam`
  - Linux 系统：`/opt/sun/identity`

  Solaris 系统的产品目录是 `/SUNWam`，Linux 系统的产品目录是 `/identity`。安装 Identity Server 2004Q2 时，可以为 Solaris 系统上的 `/opt` 或者为 Linux 系统上的 `/opt/sun` 指定一个不同的目录；但是请勿更改 `/SUNWam` 或 `/identity` 产品目录。

  有关下列产品的基本安装目录，参见特定产品的文档。
- *DirectoryServer_base* 表示 Sun Java System Directory Server 的基本安装目录。
- *ApplicationServer_base* 是 Sun Java System Application Server 所在的安装主目录的变量占位符。
- *WebServer_base* 是 Sun Java System Web Server 所在的安装主目录的变量占位符。

相关信息

您可以从以下位置找到有用的信息：

- Directory Server 文档：
  http://docs.sun.com/coll/DirectoryServer_04q2 及
  http://docs.sun.com/coll/DirectoryServer_04q2_zh
- Web Server 文档：
  http://docs.sun.com/coll/S1_websvr61_en 及
  http://docs.sun.com/coll/S1_websvr61_zh
- Application Server 文档：
  http://docs.sun.com/coll/s1_asseu3_en 及
  http://docs.sun.com/coll/s1_asseu3_zh
- Web Proxy Server 文档：
  http://docs.sun.com/prod/s1.webproxys#hic
- 下载中心：
  http://wwws.sun.com/software/download/
- 技术支持：
  http://www.sun.com/service/sunone/software/index.html
- 专业服务：
  http://www.sun.com/service/sunps/sunone/index.html
- Sun 企业服务、 Solaris 修补程序和支持：

  http://sunsolve.sun.com/
- 开发者信息：
  http://developers.sun.com/prodtech/index.html

相关第三方站点引用

本文档中引用了第三方 URL，它们提供附加相关信息。

Sun 对本文档中提及的第三方 Web 站点的可用性概不负责。 Sun 对从此类站点或资源上获取或通过其获取的任何内容、广告、产品或其他资料既不担保也不负责。 Sun 对从此类站点或资源上获取或通过其获取的任何内容、物品或服务导致的或与之使用或依赖有关的任何实际的或所谓的损害或损失也概不负责。

第 I 部分

Identity Server 配置

本部分是《*Sun Java™ System Identity Server 2004Q2 管理指南*》的第一部分。它将介绍您在 Identity Server 安装后可执行的配置选项。本部分包含以下各章：

第 1 章

Identity Server 2004Q2 配置脚本

本章介绍如何使用 `amconfig` 脚本和无提示模式输入文件样例 (`amsamplesilent`) 来配置和部署 Sun Java™ System Identity Server （先前为 Sun™ ONE Identity Server）。主题包括：

Identity Server 2004Q2 安装概述

对于新安装，始终是通过运行 Sun Java Enterprise System 安装程序来安装 Identity Server 2004Q2 的第一个实例。运行该安装程序时，可以选择以下任一 Identity Server 配置选项：

- “立即配置”选项允许您在安装期间按照您在 Identity Server 安装面板上作出的选择 （或选择的默认值）来配置第一个实例。
- 使用 “稍后配置”选项可以先安装 Identity Server 2004Q2 组件，但在安装完以后必须对其进行配置，如重新配置 Identity Server 的实例中所述。

有关该安装程序的信息，参见 《*Sun Java Enterprise System 2004Q2 安装指南*》(http://docs.sun.com/doc/817-7056)。

Java Enterprise System 安装程序会将 Identity Server 2004Q2 `amconfig` 脚本和无提示模式输入文件样例 (`amsamplesilent`) 安装于 *IdentityServer_base*`/SUNWam/bin` 目录 （对于 Solaris 系统）或 *IdentityServer_base*`/identity/bin` 目录 （对于 Linux 系统）。

IdentityServer_base 表示 Identity Server 基本安装目录。默认基本安装目录在 Solaris 系统中为 `/opt`，在 Linux 系统中为 `/opt/sun`。不过，如果愿意，您可以在运行安装程序时指定其他目录。

`amconfig` 脚本是顶级脚本，它会根据需要调用其他脚本执行请求的操作。有关详细信息，参见 Identity Server amconfig 脚本。

无提示模式输入文件样例 (`amsamplesilent`) 给出了一个输入文件例子，您在无提示模式下运行 `amconfig` 脚本时必须指定一个输入文件。

无提示模式输入文件样例是包含 Identity Server 配置变量的 ASCII 文本文件。在运行 `amconfig` 脚本之前，先复制 （如果愿意，还可以重命名） `amsamplesilent` 文件，然后编辑文件中的变量。配置变量采用以下格式：

`variable-name=`*value*

例如：

```
DEPLOY_LEVEL=1
NEW_INSTANCE=true
SERVER_HOST=ishost.example.com
```

有关可在无提示模式输入文件中设置的变量列表，参见 Identity Server 无提示模式输入文件样例。

警告 与 Java Enterprise System 无提示安装状态文件相比，在无提示模式下运行 `amconfig` 脚本时使用的无提示模式输入文件采用了不同的格式，也不必与前者使用相同的变量名。此文件包含敏感数据，如管理员口令。确保保护好此文件或适时地将其删除。

Identity Server amconfig 脚本操作

使用 Sun Java Enterprise System 安装程序安装了 Identity Server 的第一个实例后，便可运行 `amconfig` 脚本执行以下操作，具体操作取决于无提示模式输入文件中的变量值：

- 在同一主机系统中部署和配置 Identity Server 的附加实例。例如，在配置了 web 容器的一个附加实例后，可以为该 web 容器实例部署和配置一个新的 Identity Server 实例。
- 重新配置 Identity Server 的首个实例和任何附加实例。
- 部署和配置 Identity Server SDK，该组件可对以下产品提供支持：
  - BEA WebLogic Server 6.1 SP4 和 SP5
  - BEA WebLogic Server 8.1 SP1
  - IBM WebSphere 5.1
- 部署和配置特定的 Identity Server 组件，如控制台或 “联合管理”模块。
- 使用 `amconfig` 脚本卸载所部署的 Identity Server 实例和组件。

Identity Server 无提示模式输入文件样例

运行 Java Enterprise System 安装程序后，可在 *IdentityServer_base*/SUNWam/bin 目录中 （对于 Solaris 系统）或是在 *IdentityServer_base*/identity/bin 目录中 （对于 Linux 系统）获得 Identity Server 无提示模式输入文件样例 (amsamplesilent)。

要设置配置变量，首先复制并重命名 amsamplesilent 文件。然后为要执行的操作设置副本中的变量。

此无提示模式输入文件样例包含以下配置变量：

- 部署模式变量
- Identity Server 配置变量
- Web 容器配置变量
- Directory Server 配置变量

部署模式变量

表 1-1 描述了必需变量 DEPLOY_LEVEL 的值。此变量确定了您想要 amconfig 脚本执行的操作。

表 1-1 Identity Server DEPLOY_LEVEL 变量

操作	DEPLOY_LEVEL 变量值和描述
安装	1 = 完全安装新的 Identity Server 实例 （默认值）
	2 = 仅安装 Identity Server 控制台
	3 = 仅安装 Identity Server SDK
	4 = 仅安装 SDK 并配置容器
	5 = 仅安装 “联合管理”模块
	6 = 仅安装服务器
卸载 （取消配置）	11 = 完全卸载
	12 = 仅卸载控制台
	13 = 仅卸载 SDK
	14 = 仅卸载 SDK 并取消容器配置
	15 = 卸载 “联合管理”模块
	16 = 仅卸载服务器

表 1-1 Identity Server DEPLOY_LEVEL 变量 *(续)*

操作	DEPLOY_LEVEL 变量值和描述
重新安装 （也称为重新部署或重新配置）	21 = 完全重新安装 32 = 仅重新安装控制台 31 = 仅重新安装 SDK 33 = 仅重新安装 SDK 控制台 35 = 重新安装 “联合管理”模块 26 = 仅重新安装服务器

Identity Server 配置变量

表 1-2 描述了 Identity Server 配置变量。

表 1-2 Identity Server 配置变量

变量	描述
BASEDIR	Identity Server 软件包的基本安装目录。 默认值：PLATFORM_DEFAULT 对于 Solaris 系统， PLATFORM_DEFAULT 为 `/opt` 对于 Linux 系统， PLATFORM_DEFAULT 为 `/opt/sun`
SERVER_HOST	运行 （或将要安装） Identity Server 的系统的全限定主机名。 对于远程 SDK 安装，将此变量设置为安装 （或将要安装） Identity Server 的主机（而非远程客户主机）。
SERVER_PORT	Identity Server 端口号。默认值：58080 对于远程 SDK 安装，将此变量设置为安装 （或将要安装） Identity Server 的主机（而非远程客户主机）上的端口。
SERVER_PROTOCOL	服务器协议：http 或 https。默认值：http 对于远程 SDK 安装，将此变量设置为安装 （或将要安装） Identity Server 的主机（而非远程客户主机）上的协议。
CONSOLE_HOST	安装控制台的服务器的全限定主机名。 默认值：为 Identity Server 主机 （SERVER_HOST 变量）提供的值
CONSOLE_PORT	控制台安装以及侦听连接所在 web 容器的端口。 默认值：为 Identity Server 端口 （SERVER_PORT 变量）提供的值
CONSOLE_PROTOCOL	控制台安装所在 web 容器的协议。 默认值：服务器协议 （SERVER_PROTOCOL 变量）

表 1-2 Identity Server 配置变量 *(续)*

变量	描述
CONSOLE_REMOTE	如果控制台远离 Identity Server 服务，设置为 true。否则，设置为 false。默认值：false
DS_HOST	Directory Server 的全限定主机名。
DS_PORT	Directory Server 端口。默认值：389。
DS_DIRMGRDN	目录管理器 DN：可以无限制地访问 Directory Server 的用户。 默认值："cn=Directory Manager"
DS_DIRMGRPASSWD	目录管理器 （DS_DIRMGRDN 变量）的口令。 参见 ADMINPASSWD 描述中有关特殊字符的注释。
ROOT_SUFFIX	目录的开首或根后缀。必须确保此值在所使用的 Directory Server 中存在。 参见 ADMINPASSWD 描述中有关特殊字符的注释。
ADMINPASSWD	管理员 (amadmin) 口令。必须不同于 amldapuser 的口令。 **注**：如果口令包含特殊字符，如斜线 (/) 或反斜线 (\)，则必须用单引号 (') 将特殊字符括起来。例如： ADMINPASSWD='\\\\\####///' 但是 , 口令不能将单引号作为实际的口令字符之一。
AMLDAPUSERPASSWD	amldapuser 的口令。必须不同于 amadmin 的口令。 参见 ADMINPASSWD 描述中有关特殊字符的注释。
CONSOLE_DEPLOY_URI	URI 前缀，用于访问与 “Identity Server 管理控制台” 子组件相关联的 HTML 页面、类和 JAR 文件。 默认值：/amconsole
SERVER_DEPLOY_URI	URI 前缀，用于访问与 “Identity 管理和策略服务核心” 子组件相关联的 HTML 页面、类和 JAR 文件。 默认值：/amserver
PASSWORD_DEPLOY_URI	一个 URI，用于确定运行 Identity Server 的 web 容器将在所指定的字符串和相应的部署应用程序之间使用的映射。 默认值：/ampassword
COMMON_DEPLOY_URI	URI 前缀，用于访问 web 容器上的公共域服务。 默认值：/amcommon

表 1-2 Identity Server 配置变量 *(续)*

变量	描述
COOKIE_DOMAIN	Identity Server 在将会话 ID 授予用户时返回给浏览器的信任 DNS 域名。至少应有一个值。一般而言，采用的格式是在服务器域名前加上一个英文句点。 示例：.example.com
JAVA_HOME	Java 2 起始目录的路径。默认值：/usr/jdk/entsys-j2se
AM_ENC_PWD	口令加密密钥：Identity Server 用来加密用户口令的字符串。默认值：无 **重要信息**：如果部署多个 Identity Server 实例或远程 SDK，所有实例必须使用相同的口令加密密钥。部署附加的实例时，请从第一个实例的 AMConfig.properties 文件的 am.encryption.pwd 属性中复制该值。
PLATFORM_LOCALE	平台的语言环境。默认值：en_US （美国英语）
NEW_OWNER	安装后 Identity Server 文件的新所有者。默认值：root
NEW_GROUP	安装后 Identity Server 文件的新组。默认值：other 对于 Linux 安装，将 NEW_GROUP 设置为 root。
XML_ENCODING	XML 编码。默认值：ISO-8859-1
NEW_INSTANCE	指定配置脚本是否应将 Identity Server 部署到用户创建的新 web 容器实例： • true = 将 Identity Server 部署到用户创建的新 web 容器实例，而不是 Java Enterprise System 安装程序创建的实例。 • false = 重新配置实例。 默认值：false

Web 容器配置变量

要指定 Identity Server 的 web 容器，请设置无提示模式输入文件中的 WEB_CONTAINER 变量，如表 1-3 所述。

表 1-3 Identity Server WEB_CONTAINER 变量

值	Web 容器
WS6 （默认值）	Sun Java System Web Server 6.1 SP2
AS7	Sun Java System Application Server 7.0 Update 3
WL6	BEA WebLogic Server 6.1 SP4 和 SP5 （仅限 Identity Server SDK）
WL8	BEA WebLogic Server 8.1 （仅限 Identity Server SDK）
WAS5	IBM WebSphere 5.1 （仅限 Identity Server SDK）

Sun Java System Web Server 6.1 SP2

表 1-4 描述了无提示模式输入文件中用于 Web Server 6.1 SP2 的配置变量。

表 1-4 Web Server 6.1 SP2 配置变量

变量	描述
WS61_INSTANCE	将要部署或取消部署 Identity Server 的 Web Server 实例的名称。 默认值：https-*web-server-instance-name* 其中 *web-server-instance-name* 为 Identity Server 主机 （SERVER_HOST 变量）
WS61_HOME	Web Server 基本安装目录。 默认值：`/opt/SUNWwbsvr`
WS61_PROTOCOL	将要部署 Identity Server 的 Web Server 实例 （由 WS61_INSTANCE 变量设置）使用的协议：http 或 https。 默认值：Identity Server 协议 （SERVER_PROTOCOL 变量）
WS61_HOST	Web Server 实例 （WS61_INSTANCE 变量）的全限定主机名。 默认值：Identity Server 主机实例 （SERVER_HOST 变量）
WS61_PORT	Web Server 侦听连接时所用的端口。 默认值：Identity Server 端口号 （SERVER_PORT 变量）

表 1-4 Web Server 6.1 SP2 配置变量 *(续)*

变量	描述
WS61_ADMINPORT	“Web Server 管理服务器”侦听连接时所用的端口。 默认值：58888
WS61_ADMIN	Web Server 管理员的用户 ID。 默认值："admin"
WS61_IS_SECURE	指定是否启用安全端口： • true：启用安全端口 （HTTPS 协议）。如果容器启用了 SSL，配置脚本将使用 SSL_PASSWORD 变量来启动服务器，无需用户干预。 • false：不启用安全端口 （HTTP 协议）。 默认值：false （不启用）

Sun Java System Application Server 7.0 Update 3

表 1-5 描述了无提示模式输入文件中用于 Application Server 7.0 Update 3 的配置变量。

表 1-5 Application Server 7.0 Update 3 配置变量

变量	描述
AS70_HOME	Application Server 7.0 安装目录的路径。 默认值：/opt/SUNWappserver7
AS70_PROTOCOL	Application Server 实例使用的协议：http 或 https。 默认值：Identity Server 协议 （SERVER_PROTOCOL 变量）
AS70_HOST	Application Server 实例侦听连接时所用的全限定域名 (FQDN)。 默认值：Identity Server 主机 （SERVER_HOST 变量）
AS70_PORT	Application Server 实例侦听连接时所用的端口。 默认值：Identity Server 端口号 （SERVER_PORT 变量）
AS70_ADMINPORT	Application Server 管理服务器侦听连接时所用的端口。 默认值：4848
AS70_ADMIN	Application Server 当前在其中显示的域的 Application Server 管理服务器管理员的用户名。 默认值：admin

表 1-5 Application Server 7.0 Update 3 配置变量 *(续)*

变量	描述
AS70_ADMINPASSWD	Application Server 当前在其中显示的域的 Application Server 管理员的口令。 参见 ADMINPASSWD 描述中有关特殊字符的注释。
AS70_INSTANCE	将要运行 Identity Server 的 Application Server 实例的名称。 默认值：server1
AS70_DOMAIN	要将此 Identity Server 实例部署到的域的 Application Server 目录的路径。 默认值：domain1
AS70_INSTANCE_DIR	Application Server 存储实例文件的目录的路径。 默认值：/var/opt/SUNWappserver7/domains/domain1/server1
AS70_DOCS_DIR	Application Server 存储内容文档的目录。 默认值：/var/opt/SUNWappserver7/domains/domain1/server1/docroot
AS70_IS_SECURE	指定是否启用安全端口： • true：启用安全端口 （HTTPS 协议）。如果容器启用了 SSL，配置脚本将使用 SSL_PASSWORD 变量来启动服务器，无需用户干预。 • false：不启用安全端口 （HTTP 协议）。 默认值：false （不启用） 在安装期间，如果 Application Server 管理端口启用了 SSL，配置将会失败。不要在 https 模式下使用管理服务器。

BEA WebLogic Server 6.1 SP4 和 SP5

表 1-6 描述了无提示模式输入文件中用于 BEA WebLogic Server 6.1 的配置变量。

表 1-6 BEA WebLogic Server 6.1 SP4 和 SP5 配置变量

变量	描述
WL61_HOME	WebLogic 起始目录。默认值：`/export/bea61a`
WL61_PROJECT_DIR	WebLogic 项目目录。默认值：`user_projects`
WL61_DOMAIN	WebLogic 域名。默认值：`mydomain`
WL61_SERVER	WebLogic 服务器名。默认值：`myserver`
WL61_INSTANCE	WebLogic 实例名。默认值：WS61_HOME`/wlserver6.1`
WL61_PROTOCOL	WebLogic 协议。默认值：http
WL61_HOST	WebLogic 主机名。
WL61_PORT	WebLogic 端口。默认值：7001
WL61_SSLPORT	WebLogic SSL 端口。默认值：7002
WL61_ADMIN	WebLogic 管理员。默认值：“system”
WL61_PASSWORD	WebLogic 管理员口令。 参见 ADMINPASSWD 描述中有关特殊字符的注释。
WL61_JDK_HOME	WebLogic JDK 起始目录。默认值：WS61_HOME`/jdk131`

BEA WebLogic Server 8.1

表 1-7 描述了无提示模式输入文件中用于 BEA WebLogic Server 8.1 的配置变量。

表 1-7 BEA WebLogic Server 8.1 配置变量

变量	描述
WL8_HOME	WebLogic 起始目录。默认值：`/export/bea8`
WL8_PROJECT_DIR	WebLogic 项目目录。默认值：`projects`
WL8_DOMAIN	WebLogic 域名。默认值：`mydomain`
WL8_SERVER	WebLogic 服务器名。默认值：`myserver`
WL8_INSTANCE	WebLogic 实例名。默认值：`/export/bea8/weblogic81`
WL8_PROTOCOL	WebLogic 协议。默认值：http
WL8_HOST	WebLogic 主机名。默认值：无
WL8_PORT	WebLogic 端口。默认值：7001
WL8_SSLPORT	WebLogic SSL 端口。默认值：7002
WL8_ADMIN	WebLogic 管理员。默认值：`"system"`
WL8_PASSWORD	WebLogic 管理员口令。 参见 ADMINPASSWD 描述中有关特殊字符的注释。
WL8_JDK_HOME	WebLogic JDK 起始目录。默认值：WL8_HOME`/jdk141_03`
WL8_IS_SECURE	指定是否启用安全端口： • true：启用安全端口 （HTTPS 协议）。 • false：不启用安全端口 （HTTP 协议）。 默认值：false （不启用）

IBM WebSphere 5.1

表 1-8 描述了无提示模式输入文件中用于 IBM WebSphere Server 5.1 的配置变量。

表 1-8 IBM WebSphere 5.1 配置变量

变量	描述
WAS51_HOME	WebSphere 起始目录。默认值：/opt/WebSphere/AppServer
WAS51_JDK_HOME	WebSphere JDK 起始目录。默认值：/opt/WebSphere/AppServer/java
WAS51_CELL	WebSphere 单元。默认值：sample
WAS51_DOMAIN	WebSphere 域名。默认值：mydomain
WAS51_NODE	WebSphere 节点名。默认值：WebSphere 安装服务器的主机名。默认值：sample
WAS51_INSTANCE	WebSphere 实例名。默认值：server1
WAS51_PROTOCOL	WebSphere 协议。默认值：http
WAS51_HOST	WebSphere 主机名。默认值：sample
WAS51_PORT	WebSphere 端口。默认值：9080
WAS51_SSLPORT	WebSphere SSL 端口。默认值：9081
WAS51_ADMIN	WebSphere 管理员。默认值："admin"
WAS51_ADMINPORT	WebSphere 管理员端口。默认值：9090
WAS51_IS_SECURE	指定是否启用安全端口： • true：启用安全端口 （HTTPS 协议）。 • false：不启用安全端口 （HTTP 协议）。 默认值：false （不启用）

Directory Server 配置变量

Identity Server 2004Q2 支持 Sun ONE Directory Server 5.1 和 Sun Java System Directory Server 5 2004Q2。表 1-9 描述了无提示模式输入文件中的 Directory Server 配置变量。

表 1-9 Directory Server 配置变量

变量	描述
DIRECTORY_MODE	Directory Server 模式： 1 = 用于新安装的 “目录信息树” (DIT)。 2 = 用于现有 DIT。命名属性和对象类相同，因此配置脚本会加载 `installExisting.ldif` 和 `umsExisting.ldif` 文件。 配置脚本还会用配置期间输入的实际值 （例如， BASE_DIR、 SERVER_HOST 和 ROOT_SUFFIX）来更新 LDIF 和属性文件。 此更新操作也称为 “标记交换”，因为配置脚本是以实际配置值来替换文件中的占位符标记。 3 = 在您想要进行手动加载时，用于现有的 DIT。命名属性和对象类不同，因此配置脚本不会加载 `installExisting.ldif` 和 `umsExisting.ldif` 文件。脚本会执行标记交换 （见模式 2 的描述）。 应先检查和修改 （如果需要） LDIF 文件，然后再手动加载 LDIF 文件和服务。 4 = 用于现有多服务器安装。配置脚本不会加载 LDIF 文件和服务，因为操作针对的是现有 Identity Server 安装。脚本仅执行标记交换 （见模式 2 的描述）并在平台列表中添加一个服务器条目。 5 = 用于现有升级。脚本仅执行标记交换 （见模式 2 的描述）。 默认值：1
USER_NAMING_ATTR	用户命名属性：用户或资源在其相对名称空间中的唯一标识符。默认值：`uid`
ORG_NAMING_ATTR	用户所在公司或组织的命名属性。默认值：`o`
ORG_OBJECT_CLASS	组织对象类。默认值：`sunManagedOrganization`
USER_OBJECT_CLASS	用户对象类。默认值：`inetOrgPerson`
DEFAULT_ORGANIZATION	默认组织名。默认值：无

Identity Server amconfig 脚本

运行 Java Enterprise System 安装程序后，可在 *IdentityServer_base*/SUNWam/bin 目录中 （对于 Solaris 系统）或是在 *IdentityServer_base*/identity/bin 目录中 （对于 Linux 系统）获得 amconfig 脚本。

amconfig 脚本先读取无提示安装输入文件，然后根据需要在无提示模式下调用其他脚本来执行请求的操作。

要运行 amconfig 脚本，请使用以下语法：

```
amconfig [ -s input-file ]
```

其中：

-s 表示在无提示模式下运行 amconfig。

input-file 代表无提示安装输入文件，其中包含所要执行操作的配置变量。有关详细信息，参见 Identity Server 无提示模式输入文件样例。

如果为 WebLogic Server 或 WebSphere 部署 web 容器是为了与 Identity Server SDK 配合使用， amconfig 脚本会调用其他脚本来执行配置，但这些脚本不会启动（或停止）各自的 web 容器。要启动 web 容器实例，请使用适用于您特定部署的 WebLogic Server 或 WebSphere 命令或过程。

注 在 Identity Server 2004Q2 发行版本中，不支持以下脚本：

- 带 create 参数的 amserver 脚本
- amserver.*instance*

另外，默认情况下，amserver start 仅启动 amsecuridd 和 amunixd 验证助手。 amsecuridd 助手仅在 Solaris OS SPARC 平台上才可用。

Identity Server 部署方案

使用 Java Enterprise System 安装程序安装完 Identity Server 的第一个实例后，可以另行部署和配置其他 Identity Server 实例，方法是先编辑无提示模式输入文件中的配置变量，然后运行 amconfig 脚本。

本部分介绍以下方案：

- 部署 Identity Server 的附加实例
- 重新配置 Identity Server 的实例
- 卸载 Identity Server 实例
- 卸载所有 Identity Server 实例

部署 Identity Server 的附加实例

必须先使用 web 容器的管理工具创建并启动新的 web 容器实例，然后方可部署 Identity Server 的新实例。有关信息，参见特定 web 容器文档：

- 对于 Web Server 6.1 SP2，参见：
  http://docs.sun.com/coll/S1_websvr61_en 及
  http://docs.sun.com/coll/S1_websvr61_zh
- 对于 Application Server 7.0 Update 3，参见：
  http://docs.sun.com/coll/s1_asseu3_en 及
  http://docs.sun.com/coll/s1_asseu3_zh

部署附加的 Identity Server 实例

1. 以管理员身份登录，具体取决于实例的 web 容器。例如，如果新实例的 web 容器将是 Web Server 6.1，则以超级用户 (root) 身份或以 “Web Server 管理服务器”的用户帐户登录均可。
2. 将 amsamplesilent 文件复制到某个可写目录，并使该目录成为当前目录。例如，您可能会创建一个名为 /newinstances 的目录。

   提示：可重命名 amsamplesilent 文件的副本，以描述所要部署的新实例。例如，以下步骤使用了一个名为 amnewws6instance 的输入文件来为 Web Server 6.1 安装新实例。

3. 设置新 amnewws6instance 文件中的以下变量：

```
DEPLOY_LEVEL=1
NEW_INSTANCE=true
```

根据需要为所要创建的新实例设置 amnewws6instance 文件中的其他变量。有关这些变量的描述，参见以下各部分中的表格：

- Identity Server 配置变量
- Web 容器配置变量
- Directory Server 配置变量

重要信息 所有 Identity Server 实例必须使用相同的口令加密密钥值。要为此实例设置 AM_ENC_PWD 变量，请从第一个实例的 AMConfig.properties 文件的 am.encryption.pwd 属性中复制该值。

保存 amnewws6instance 文件，以防以后可能需要卸载此实例。

4. 运行 amconfig 脚本，指定新的 amnewws6instance 文件。例如，在 Solaris 系统中：

```
cd IdentityServer_base/SUNWam/bin/
./amconfig -s /newinstances/amnewws6instance
```

-s 选项表示在无提示模式下运行 amconfig 脚本。

amconfig 脚本会根据需要调用其他配置脚本，使用 amnewws6instance 文件中的变量来部署新实例。

重新配置 Identity Server 的实例

通过运行 amconfig 脚本，您可以重新配置使用 Java Enterprise System 安装程序安装的第一个 Identity Server 实例以及所部署的任何附加 Identity Server 实例。

例如，您可能想要重新配置某个实例以更改 Identity Server 所有者和组。

重新配置 Identity Server 的实例

1. 以管理员身份登录，具体取决于实例的 web 容器。例如，如果 web 容器为 Web Server 6.1，则以超级用户 (root) 身份或以 “Web Server 管理服务器”的用户帐户登录均可。
2. 将部署实例时所使用的无提示安装输入文件复制到某个可写目录，并使该目录成为当前目录。例如，为了给 Web Server 6.1 重新配置一个实例，以下步骤使用了 /reconfig 目录中的一个名为 amnewinstanceforWS61 的输入文件。
3. 在 amnewinstanceforWS61 文件中，将 DEPLOY_LEVEL 变量设置为针对重新安装操作所述的变量值之一。例如，设置 DEPLOY_LEVEL=21 可对完全安装进行重新配置。
4. 在 amnewinstanceforWS61 文件中，将 NEW_INSTANCE 变量设置为 false：

   ```
   NEW_INSTANCE=false
   ```

5. 在 amnewinstanceforWS61 文件中设置用于重新配置该实例的其他变量。例如，要更改实例的所有者和组，请将 NEW_OWNER 和 NEW_GROUP 变量设置为各自的新值。

   有关其他变量的描述，参见以下各部分中的表格：

   - Identity Server 配置变量
   - Web 容器配置变量
   - Directory Server 配置变量

6. 运行 amconfig 脚本，指定所编辑的输入文件。例如，在 Solaris 系统中：

   ```
   cd IdentityServer_base/SUNWam/bin/
   ./amconfig -s /reconfig/amnewinstanceforWS61
   ```

   -s 选项表示在无提示模式下运行该脚本。 amconfig 脚本会根据需要调用其他配置脚本，使用 amnewinstanceforWS61 文件中的变量来重新配置实例。

卸载 Identity Server 实例

通过运行 amconfig 脚本，您可以卸载所安装的某个 Identity Server 实例。还可以暂时取消配置某个 Identity Server 实例。只要您不移除相应的 web 容器实例，它以后仍可用于重新部署另一个 Identity Server 实例。

卸载 Identity Server 的实例

1. 以管理员身份登录，具体取决于实例的 web 容器。例如，如果 web 容器为 Web Server 6.1，则以超级用户 (root) 身份或以 “Web Server 管理服务器”的用户帐户登录均可。
2. 将部署实例时所使用的无提示安装输入文件复制到某个可写目录，并使该目录成为当前目录。例如，为了给 Web Server 6.1 取消配置一个实例，以下步骤使用了 /unconfigure 目录中的一个名为 amnewinstanceforWS61 的输入文件。
3. 在 amnewinstanceforWS61 文件中，将 DEPLOY_LEVEL 变量设置为针对卸载（取消配置）操作所述的变量值之一。例如，设置 DEPLOY_LEVEL=11 可对完全安装进行卸载 （或取消配置）。
4. 运行 amconfig 脚本，指定所编辑的输入文件。例如，在 Solaris 系统中：

   ```
   cd IdentityServer_base/SUNWam/bin/
   ./amconfig -s /unconfigure/aminstanceforWS61
   ```

   -s 选项表示在无提示模式下运行该脚本。 amconfig 脚本先读取 amnewinstanceforWS61 文件，然后卸载实例。

如果以后要使用该 web 容器实例重新部署另一个 Identity Server 实例，它仍将是可用的。

卸载所有 Identity Server 实例

此方案将从系统中完全移除所有 Identity Server 2004Q2 实例和软件包。

从系统中完全移除 Identity Server 2004Q2

1. 以超级用户 (root) 身份登录或成为超级用户。
2. 在部署实例所使用的输入文件中，将 DEPLOY_LEVEL 变量设置为针对卸载（取消配置）操作所述的变量值之一。例如，设置 DEPLOY_LEVEL=11 可对完全安装进行卸载 （或取消配置）。
3. 使用步骤 2 中所编辑的文件运行 `amconfig` 脚本。例如，在 Solaris 系统中：

   ```
   cd IdentityServer_base/SUNWam/bin/
   ./amconfig -s /newinstances/amnewws6instance
   ```

   `amconfig` 脚本将在无提示模式下运行以卸载该实例。

   除了第一个实例 （即使用 Java Enterprise System 安装程序安装的实例）之外，对所要卸载的其他任何 Identity Server 实例重复以上步骤。
4. 要卸载第一个实例并从系统中移除所有 Identity Server 软件包，请运行 Java Enterprise System 卸载程序。有关卸载程序的信息，参见《*Sun Java Enterprise System 安装指南*》。

第 2 章

Identity Server 微调脚本

本章介绍 Sun Java™ System Identity Server 2004Q2 的 amtune 微调脚本，包含以下部分：

注 对于 2004Q2 发行版， amtune 脚本唯有在 Solaris 系统中才是全功能的。 Linux 和 x86 版本的 amtune 脚本也能运行，但在这些平台上尚不成熟。

amtune 脚本

amtune 脚本允许您微调 Identity Server 的性能，并优化 Identity Server 部署各组件的性能设置。

amtune 脚本是非交互式的。这意味着在运行脚本之前，必须在 amtune-env 配置文件中编辑参数以指定特定环境下要执行的微调。

要编辑微调增强功能，请在 amtune-env 文件中修改参数，然后以下列格式运行 amtune 脚本。其中 admin_password 是 “Identity Server 管理客户机实用程序”口令， dirmanager_password 是 “目录管理员” (cn=Directory Manager) 口令：

```
amtune admin_password dirmanager_password
```

如果要微调特定组件，可以使用 /amtune 目录中提供的组件脚本。组件脚本将使用 amtune-env 文件中的相关参数。可用组件脚本有：

- amntune-as7 - 此脚本微调 Sun Java System Application Server 7 Web 容器。
- amtune-identity - 此脚本微调安装的 Identity Server 实例。
- amtune-os - 此脚本微调 Solaris 操作系统 kernel 和 TCP/IP 参数。
- amtune-prepareDSTuner - 此脚本微调用于支持 Identity Server 的 Directory Server 实例。微调 Directory Server 需要执行额外级别的确认操作。 Identity Server 要求在非独占模式下使用现有 Directory Server。无论将 Directory Server 安装在何位置 （本地或远程），运行 amtune 时不会微调 Directory Server。运行脚本时，会创建名为 /tmp/amtune-directory.tar 的 tar 文件。默认情况下，将提取的文件存放在 /tmp 目录中。您需要从系统中运行 Directory Server 的机器上提取此文件，然后运行 amtune-directory 脚本。
- amtune-ws61 - 此脚本微调 Sun Java System Web Server 6.1 Web 容器。

例如，如果要微调操作系统，请使用以下格式：

```
amtune-os admin_password dirmanager_password
```

amtune 脚本及关联 amtune-env 文件可在以下目录中找到：

IdentityServer_base/SUNWam/bin/amtune （Solaris）

IdentityServer_base/identity/bin/amtune （Linux）

注 在本章中的余下部分将只给出 Solaris 目录信息。请注意 Linux 的目录结构有所不同。有关详细信息，请参见第 19 页的 “关于本指南”。

amtune

amtune 脚本有两个生成模式；一个模式用于为 Identity Server 部署生成一组微调建议，一个模式用于实现微调规范。以下是用户可指定的模式，这些模式在 amtune-env 文件的 AMTUNE_MODE 参数中定义：

- 查看模式 - 如果指定 “查看”模式， amtune 脚本将返回微调建议，但不会对部署环境做任何更改。

- 更改模式 - 如果指定 “更改”模式， amtune 脚本将根据在 amtune-env 中定义的微调进行全面修改，但 Directory Server 微调除外。

注 使用 “更改”模式时请注意，运行脚本后需要重新启动 Web 容器， amtune 可能会建议重新启动系统。

微调是一个高度迭代的过程，可以随不同的部署而变化。虽然 amtune 实用程序会尽可能应用最佳的微调参数，但每个部署都有其特定的要求，因此可能需要进一步执行自定义操作，以便满足部署的具体要求。 Identity Server 管理员应当了解并检查应用于部署的每个微调，这一点非常重要。

在任一模式下，微调建议列表和当前值都被写入 amtune 输出文件并显示在终端窗口中。此文件的位置基于 amtune-env 中的 AMTUNE_DEBUG_FILE_PREFIX 参数而定。

amtune-env 配置文件参数

amtune-env 配置文件包含用于定义 Identity Server 部署的微调选项的参数。本部分介绍 amtune-env 参数。

amtune 参数

以下参数用于特定组件微调：

AMTUNE_MODE

此参数定义以下模式：

- review - 如果指定 “查看”模式， amtune 脚本将返回微调建议，但不会对部署环境做任何更改。
- change - 如果指定 “更改”模式， amtune 脚本将根据在 amtune-env 中定义的微调进行全面修改，但 Directory Server 微调除外。

AMTUNE_MODE_OS

此参数微调 Solaris 操作系统 kernel 和 TCP/IP 设置。

AMTUNE_MODE_DS

此参数微调用于支持 Identity Server 的 Directory Server 实例。微调 Directory Server 需要执行额外级别的确认操作。 Identity Server 要求在非独占模式下使用现有 Directory Server。无论将 Directory Server 安装在何位置 （本地或远程），运行 `amtune` 时不会微调 Directory Server。运行脚本时，会创建名为 `/tmp/amtune-directory.tar` 的 tar 文件。默认情况下，将提取的文件存放在 `/tmp` 目录中。您需要从系统中运行 Directory Server 的机器上提取此文件，然后运行 `amtune-directory` 脚本。

AMTUNE_MODE_WEB_CONTAINER

此参数微调安装 Identity Server 的 Web 容器。

AMTUNE_MODE_IDENTITY

此参数微调安装的 Identity Server 实例。

以下参数用于所有 amtune 操作：

AMTUNE_DEBUG_FILE_PREFIX

此参数定义调试文件名前缀。如果将此参数设置为非空值，则会记录 `amtune` 脚本执行的所有操作。在 `AMConfig.properties` 的 `com.iplanet.services.debug.directory` 参数中设置日志文件的位置。

如果未指定值，则不记录调试信息，并将所有输出发送到 `/dev/null` 目录。

AMTUNE_PCT_MEMORY_TO_USE

此参数定义 Identity Server 所用的可用内存容量。目前， Identity Server 最少需要 512MB RAM，最多可需要 4 GB，即 32 位应用程序单进程地址空间上限。如果将此参数设置为 0 （最低值），便意味将 Identity Server 配置为使用 512MB。相反，如果将此参数设置为 100，则 Identity Server 允许使用的最大空间是 4GB 与 100% 系统可用 RAM 之间的最小值。以下是基于此设置进行微调的文件中的一些值 （完整列表请参见调试文件）：

Web 容器值

`server.xml` 文件：

- 堆栈容量设置
- `<JVMOPTIONS>-XX:PermSize` 和 `<JVMOPTIONS>-XX:MaxNewSize`
- `<JVMPTIONS>-XX:Permsize` 和 `<JVMOPTIONS>-XX:MaxPermSize`

`magnus.conf` 文件：

- `RqThrottle` 设置

Identity Server AMConfig.properties 值

通知线程池设置：

- `com.iplanet.am.notification.threadpool.size`
- `com.iplanet.am.notification.threadpool.threshold`

SDK 高速缓存最大容量设置：

- `com.iplanet.am.sdk.cache.maxsize`

会话设置：

- `com.iplanet.am.session.httpSession.enabled`
- `com.iplanet.am.session.maxSessions`
- `com.iplanet.am.session.invalidsessionmaxtime`
- `com.iplanet.am.session.purgedelay`

AMTUNE_PER_THREAD_STACK_SIZE

此参数设置每个线程的可用栈空间。每个线程的栈大小用于微调 Identity Server 和 Web 容器中与线程相关的各种参数。默认值为 128KB。此值不能更改。

AMTUNE_SESSION_MAX_SESSION_TIME_IN_MTS

此参数设置最长会话时间 （以分钟为单位）。默认值为 60。但是，对于不同的安装，此值可能不同。如果在任何其他级别注册和自定义 “会话” 服务，则不应用微调。

将此参数值设得太高或太低会影响 Identity Server 部署可支持的活动用户会话数，因此，可选择是否使用此参数进行调节。

为使用此参数，必须确保将 AM_TUNE_DONT_TOUCH_SESSION_PARAMETERS 设置为 false。

AMTUNE_SESSION_MAX_IDLE_TIME_IN_MTS

此参数设置会话的最长空闲时间 （以分钟为单位）。默认值为 10。但是，对于不同的安装，此值可能不同。如果在任何其他级别注册和自定义 “会话”服务，则不应用微调。

将此参数值设得太高或太低会影响 Identity Server 部署可支持的活动用户会话数，因此，可选择是否使用此参数进行调节。

为使用此参数，必须确保将 AM_TUNE_DONT_TOUCH_SESSION_PARAMETERS 设置为 false。

AMTUNE_SESSION_MAX_CACHING_TIME_IN_MTS

此参数设置最长会话高速缓存时间 （以分钟为单位）。默认值为 2。但是，对于不同的安装，此值可能不同。如果在任何其他级别注册和自定义 “会话”服务，则不应用微调。

将此参数值设得太高或太低会影响 Identity Server 部署可支持的活动用户会话数，因此对于微调而言，此参数是可选的。

为使用此参数，必须确保将 AM_TUNE_DONT_TOUCH_SESSION_PARAMETERS 设置为 false。

安装环境参数

HOSTNAME

此参数定义部署 Identity Server 的系统的主机名。如果使用 hostname 命令无法获得环境的主机名，请将下行注释掉：

```
HOSTNAME='/bin/hostname'
```

然后添加一行，以设置正确的主机名。例如：

```
HOSTNAME=machine_name
```

DOMAINNAME

此参数定义部署 Identity Server 的系统的域名。如果使用 domainname 命令无法获得环境的域名，请将下行注释掉：

```
DOMAINNAME='/bin/domainname'
```

然后添加一行，以设置正确的域名。例如：

```
DOMAINNAME=example.com
```

IS_CONFIG_DIR

此参数定义 Identity Server 的配置目录。默认位置为 IdentityServer_base/SUNWam/config。不要更改此参数。

WEB_CONTAINER

此参数定义部署 Identity Server 的 Web 容器的名称。此参数接受以下值：

- WS61 - 将 Web Server 6.1 指定为 Web 容器。
- AS7 - 将 Application Server 7 指定为 Web 容器。

使用其他值会产生验证错误。

CONTAINER_BASE_DIR

此参数定义部署 Identity Server 的 Web 容器的基本目录。如果将 Web 容器安装在非默认位置，请在运行 amtune 之前更改此值。

WEB_CONTAINER_INSTANCE_NAME

此参数定义部署 Identity Server 的 Web 容器的实例名称。

对于 Java System Web Server Web 容器，实例名称通常是 Identity Server 的主机名。如果实例名称与主机名不同，则需要在此处指定正确的实例名称。例如：

```
/opt/SUNWwbsrvr/https-fully_qualified_hostname
```

在本例中，可以将 WEB_CONTAINER_INSTANCE_NAME 保留为原样，即：

```
WEB_CONTAINER_INSTANCE_NAME=$HOSTNAME
```

如果 Web Server 安装位置不是典型值，例如为 /opt/SUNWwbsrvr/https-instance1，则实例名称为 instance1。

```
WEB_CONTAINER_INSTANCE_NAME=instance1
```

注 需要从 JSWS 安装位置的目录名称中删掉 "https-"。

对于 Application Server Web 容器，实例名称通常是 server1。例如：

```
/var/opt/SUNWappserver7/domains/domain1/server1/
```

在本例中，实例名称是安装位置的最后部分，即 server1。

如果 Application Server 安装位置不是典型值，比如，如果安装位置为 /var/opt/SUNWappserver7/domains/domain1/server-identity-ssl，则实例名称为 server-identity-ssl：

```
WEB_CONTAINER_INSTANCE_NAME=server-identity-ssl
```

注 需要为 Application Server 指定完整的实例名称，通常是安装路径中的叶目录。

IS_INSTANCE_NAME

确定安装 Identity Server 的属性文件的文件名时将使用此参数。同一台机器上可以部署多个 Identity Server 实例，但通常每个 Identity Server 实例都各有一组属性文件，并且会在这些文件的文件名后附加相应的实例名称。

如果一台机器上只有一个 Identity Server 实例，则不会在文件名后附加实例名称。

例如，可能会在 Web Server 的默认实例下运行单个 Identity Sever 实例：

如果在名为 server.example.com 的机器上安装 Identity Server，则 Web Server 的第一个实例通常为 https-server.example.com。第一个 Identity Server 实例的属性文件的文件名后不会附加实例名称 （例如 AMConfig.properties）。

在有多个实例的情况下，会有不同的文件名。例如，可能会有三个 Web Server 实例。这三个 Web Server 实例分别是 server.example.com-instance1、server.example.com-instance2 和 server.example.com-instance3。如果部署三个 Identity Server 实例 （每个容器实例对应一个 Identity Server 实例），则 Identity Server 的主属性文件的文件名 （通常为 AMConfig.properties）可能与以下名称相仿：

- AMConfig-instance1.properties
- AMConfig-instance2.properties
- AMConfig-instance3.properties。

可以指定 IS_INSTANCE_NAME=instance1。 amtune 将按以下顺序确定属性文件的文件名：

1. AMConfig-*IS_INSTANCE_NAME*
2. AMConfig-*WEB_CONTAINER_INSTANCE_NAME*
3. AMConfig.properties

该工具会在列表中搜索第一个可用属性文件并使用它。

注 Web 容器和 amadmin 工具亦应指向正确的 Identity Server 实例。

对于 Web 容器，还需要在 Web 容器实例配置的 server.xml 配置文件中显式指定实例名称。例如：

```
<JVMOPTIONS>-Dserver.name=instance1</JVMOPTIONS>
```

注 amadmin 工具亦应指向正确的服务器名称 (java option -Dserver.name=instance1)。

CONTAINER_INSTANCE_DIR

此参数定义部署 Identity Server 的容器实例的基本目录。如果将 Web 容器安装在非默认位置，请在运行 amtune 之前更改此值。

Directory Server 参数

DIRMGR_UID

此参数定义 “目录管理器”的用户 ID。如果更改用户 ID 的默认值 (cn=Directory Manager)，则必须更改此参数的值。

DEFALUT_ORG_PEOPLE_CONTAINER

此参数定义顶级组织下的 Identity Server 实例的默认用户容器位置。此值用于微调 LDAP 验证服务的搜索基。搜索范围也将修改为对象级别，且默认搜索范围为子树级别。当默认组织中没有子组织时，此参数很有用。如果未指定参数值，则跳过微调。

第 3 章

在 SSL 模式中配置 Identity Server

将安全套接字层 (SSL) 和简单验证结合使用可以保证数据的保密性和完整性。要在 SSL 模式下启用 Identity Server，通常需要执行以下操作：

1. 使用安全 Web 容器配置 Identity Server
2. 配置 Identity Server 至安全 Directory Server

以下各部分将介绍这些步骤：

- 第 57 页的 “使用安全 Sun Java System Web Server 配置 Identity Server”
- 第 60 页的 “使用安全 Sun Java System Application Server 配置 Identity Server”
- 第 64 页的 “在 SSL 模式中配置 Identity Server 至 Directory Server”

使用安全 Sun Java System Web Server 配置 Identity Server

要使用 Sun Java System Web Server 在 SSL 模式下配置 Identity Server，参见以下步骤：

1. 在 Identity Server 控制台中，转到 “服务配置”模块并选择 “平台”服务。在 “服务器列表”属性中，移除 `http://` 协议，并添加 `https://` 协议。单击 “保存”。

注 请务必单击 “保存”。否则，尽管您仍能继续下面的步骤，但所作的所有配置更改都会丢失，而且您将不能以管理员身份登录来对此予以修复。

步骤 2 至步骤 25 对 Sun Java System Web Server 进行了说明。

2. 登录到 Web Server 控制台。默认端口为 58888。
3. 选择运行 Identity Server 的 Web Server 实例并单击 “管理”。

   将显示一个弹出窗口，说明配置已更改。单击 “确定”。
4. 单击屏幕右上角的 “应用”按钮。
5. 单击 “应用设置”。

   Web Server 应当会自动重新启动。单击 “确定”继续。
6. 停止选定的 Web Server 实例。
7. 单击 “安全”选项卡。
8. 单击 “创建数据库”。
9. 输入新数据库口令并单击 “确定”。

   请务必将数据库口令记下来，以备将来使用。
10. 创建证书数据库后，单击 “请求证书”。
11. 在屏幕上的字段中输入数据。

    在 “密钥对字段口令”字段中输入您在步骤 9 中输入的口令。在 “位置”字段中输入位置的完整拼写。不能输入缩写 （例如 CA）。必须定义所有字段。在 “公共名称”字段中，输入您的 Web Server 的主机名。
12. 提交表单后，您将看到如下消息：

```
--BEGIN CERTIFICATE REQUEST---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE REQUEST--
```

13. 复制并为证书请求提交该文本。

    确保您获取的是根 CA 证书。

14. 您将收到一个包含证书的证书响应，例如：

```
--BEGIN CERTIFICATE---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE---
```

15. 将这些文本复制到剪贴板或保存到文件中。
16. 转到 Web Server 控制台并单击 “安装证书”。
17. 单击该服务器的 “证书”。
18. 在 “密钥对文件口令”字段中，输入证书数据库口令。
19. 将证书粘贴到提供的文本字段中或选中单选按钮，并在文本框中输入文件名。单击 “提交”。

    浏览器将显示证书，并提供用于添加证书的按钮。

20. 单击 “安装证书”。
21. 单击 “信任的证书授权机构的证书”。

22. 按照步骤 16 至步骤 21 中所述的方法安装根 CA 证书。
23. 安装完这两种证书后，单击 Web Server 控制台中的 “首选项” 选项卡。
24. 如果要在其他端口上启用 SSL，请选择 “添加侦听套接字”。然后，选择 “编辑侦听套接字”。
25. 将安全状态从 “已禁用” 改为 “已启用”，并单击 “确定” 以提交所作的更改。

步骤 26 至步骤 28 对 Identity Server 进行了说明。

26. 打开 `AMConfig.properties` 文件。默认情况下，该文件位于 `etc/opt/SUNWam/config` 中。
27. 将出现的所有 `http://` 协议替换为 `https://` 协议 （除了 Web Server 实例目录）。还要在文件 `AMConfig.properties` 中进行指定，但是必须保持相同。
28. 保存 `AMConfig.properties` 文件。
29. 在 Web Server 控制台中，单击 Web Server 实例所属的 Identity Server 的 “开/关” 按钮。

    Web Server 将在 “启动/停止” 页面中显示一个文本框。
30. 在文本字段输入证书数据库口令并选择 “启动”。

使用安全 Sun Java System Application Server 配置 Identity Server

可以通过以下两个步骤设置 Identity Server，使其在启用了 SSL 的 Sun Java System Application Server 上运行。首先，使 Application Server 实例对于已安装的 Identity Server 来说是安全的，然后配置 Identity Server 本身。

将 Application Server 设置为具有 SSL

要保证 Application Server 实例的安全性：

1. 在浏览器中输入以下地址，以管理员身份登录到 Sun Java System Application Server 控制台：

   ```
   http://fullservername:port
   ```

   默认端口为 4848。

2. 输入在安装过程中输入的用户名和口令。
3. 选择已在 （或将在）其上安装 Identity Server 的 Application Server 实例。右侧框中显示配置已更改。
4. 单击 “应用更改”。
5. 单击 “重新启动”。 Application Server 将自动重新启动。
6. 在左侧框中，单击 “安全”。
7. 单击 “管理数据库”选项卡。
8. 如果未选择数据库，则单击 “创建数据库”。
9. 输入新数据库口令并予以确认，然后单击 “确定”按钮。请确保记下数据库口令，以备将来使用。
10. 创建证书数据库后，单击 “证书管理”选项卡。
11. 如果未选择证书，则单击 “请求”链接。
12. 为证书输入以下请求数据

    a. 如果该证书为新证书或证书更新，则选择该证书。许多证书在经过特定的一段时间之后会过期，一些证书授权机构 (CA) 会自动给您发送更新通知。

    b. 指定您要提交证书请求的方式。

       如果 CA 要求接收电子邮件形式的请求，请查看 CA 电子邮件，然后输入 CA 的电子邮件地址。要查看 CA 的列表，请单击 “可用的证书授权机构列表”。

       如果是向使用 Sun Java System Certificate Server 的内部 CA 请求证书，请单击 “CA URL”，然后输入 Certificate Server 的 URL。该 URL 应该指向 Certificate Server 的处理证书请求的程序。

    c. 输入密钥对文件的口令 （即您在步骤 9 中指定的口令）。

d. 输入以下标识信息：

公共名称。服务器的全名，包括端口号。

请求者姓名。请求者的姓名。

电话号码。请求者的电话号码。

公共名称。将要在其上安装数字证书的 Sun Java System Application Server 的全限定名称。

电子邮件地址。管理员的电子邮件地址。

组织名称。您的组织的名称。证书授权机构可能要求该属性中输入的所有主机名都属于某个已注册到该组织的域。

组织单位名称。组织的部门或其他运作单位的名称。

位置名称 （城市）。城市或城镇的名称。

州名。如果您的组织位于美国或加拿大，则分别指组织所在的州或省的名称。请不要使用缩写。

国家/地区代码。您所在国家/地区的两个字母的 ISO 代码。例如，美国的代码是 US。

13. 单击 “确定”按钮。系统将显示一条消息，例如：

```
--BEGIN NEW CERTIFICATE REQUEST---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdfla

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END NEW CERTIFICATE REQUEST--
```

14. 将该文本的所有内容复制到一个文件，然后单击 “确定”。确保您获取的是根 CA 证书。

15. 选择一个 CA，然后按照该机构的 Web 站点上的说明获取数字证书。您可以从 CMS、 Verisign 或 Entrust.net 获取证书。

16. 收到来自证书授权机构的数字证书后，您可以将文本复制到剪贴板或保存到文件中。
17. 转到 Sun Java System Application Server 控制台，然后单击 “安装”链接。
18. 为该服务器选择证书。
19. 在 “密钥对文件口令”字段中，输入证书数据库口令。（该口令与您在步骤 9 中输入的口令相同。）
20. 将证书粘贴到所提供的 “消息文本 （带标题）”文本字段中，或在该文件文本框中的 “消息”字段中输入文件名。选择相应的单选按钮。
21. 单击 “确定”按钮。浏览器将显示证书，并提供用于添加证书的按钮。
22. 单击 “添加服务器证书”。
23. 按照步骤 10 至步骤 22 中所述的方法安装根 CA 证书。但是，在步骤 18 中，请选择 “信任的证书授权机构的证书”。
24. 证书安装都完成后，请展开左框中的 “HTTP 服务器”节点。
25. 选择 “HTTP 服务器”下的 “HTTP 侦听器”。
26. 选择 “`http-listener-1`”。浏览器将显示套接字信息。
27. 将 `http-listener-1` 使用的端口值从安装 Application Server 时输入的值更改为一个更合适的值，如 443。
28. 选择 “启用 SSL/TLS”。
29. 选择 “证书昵称”。
30. 指定返回服务器。该名称应该与在步骤 12 中指定的公共名称匹配。
31. 单击 “保存”。
32. 选择将要在其上安装 Sun Java System Identity Server 软件的 Application Server 实例。右侧框中显示配置已更改。
33. 单击 “应用更改”。
34. 单击 “重新启动”。 Application Server 将自动重新启动。

在 SSL 模式中配置 Identity Server

要在 SSL 模式中配置 Identity Server：

1. 在 Identity Server 控制台中，转到 “服务配置”模块并选择 “平台”服务。在 “服务器列表”属性中，添加 HTTPS 协议格式的相同 URL 和启用 SSL 的端口号。单击 “保存”。

注 如果有一个 Identity Server 实例正在侦听两个端口 （其中一个为 Http 模式，另一个为 Https 模式），当您试图利用迟延的 cookie 访问 Identity Server 时， Identity Server 将转为无响应状态。不支持此配置。

2. 从以下默认位置打开 `AMConfig.properties` 文件：

   `/etc/opt/SUNWam/config`。

3. 将出现的所有 `http://` 协议替换为 `https://` 协议，并将端口号更改为启用 SSL 的端口号。
4. 保存 `AMConfig.properties` 文件。
5. 重新启动 Application Server。

在 SSL 模式中配置 Identity Server 至 Directory Server

为确保通过网络提供安全通信， Identity Server 中包括 LDAPS 通信协议。 LDAPS 是标准的 LDAP 协议，但它在 “安全套接字层” (SSL) 上运行。为了启用 SSL 通信，必须首先在 SSL 模式下配置 Directory Server，然后将 Identity Server 连接到 Directory Server。基本步骤如下：

1. 获得并安装 Directory Server 的证书，然后将 Directory Server 配置为信任证书授权机构 (CA) 的证书。
2. 在目录中启用 SSL。
3. 配置验证、策略和平台服务，以连接到启用 SSL 的 Directory Server。
4. 配置 Identity Server 以安全地连接到 Directory Server 后端。

在 SSL 模式中配置 Directory Server

为在 SSL 模式下配置 Directory Server，必须获得并安装服务器证书、将 Directory Server 配置为信任 CA 的证书并且启用 SSL。有关如何完成这些任务的详细说明，参见 《*Directory Server 管理指南*》的第 11 章 “管理验证和加密”。可在以下位置找到此文档：

http://docs.sun.com/doc/817-7163

还可从以下位置下载此手册的 PDF：

http://docs.sun.com/coll/DirectoryServer_04q2 及
http://docs.sun.com/coll/DirectoryServer_04q2_zh

如果 Directory Server 已经启用 SSL，请转到下一部分，以查看有关将 Identity Server 连接到 Directory Server 的详细说明。

将 Identity Server 连接到启用 SSL 的 Directory Server

在 SSL 模式下配置完 Directory Server 以后，需要将 Identity Server 安全地连接到 Directory Server 后端。为此，请执行以下步骤：

1. 在 “Identity Server 控制台”中，转到 “服务配置”模块中的 “LDAP 验证”服务。
   a. 将 Directory Server 端口更改为 SSL 端口。
   b. 选择 “对 LDAP 服务器启用 SSL 访问”属性。
2. 转到 “服务配置”模块中的 “成员资格验证”服务。
   a. 将 Directory Server 端口更改为 SSL 端口。
   b. 选择 “对 LDAP 服务器启用 SSL 访问”属性。
3. 转到 “服务配置”模块中的 “策略配置验证”服务。
   a. 将 Directory Server 端口更改为 SSL 端口。
   b. 选择 “启用 LDAP SSL”属性。

4. 在文本编辑器中打开 serverconfig.xml。该文件位于：

   etc/opt/SUNWam/config

   a. 在 <Server> 元素中，更改以下值：

      port - 输入 Identity Server 所侦听的安全端口的端口号 （默认值为 636）。

      type - 将 SIMPLE 更改为 SSL。

   b. 保存并关闭 serverconfig.xml。

5. 从以下默认位置打开 AMConfig.properties 文件：

   IdentityServer_base/SUNWam/config。

   更改以下属性：

   a. Directory Port = 636 （如果使用默认值）

   b. ssl.enabed = true

   c. 保存 AMConfig.properties。

6. 重新启动服务器

第 II 部分

通过控制台管理 Identity Server

本部分是 《*Sun Java™ System Identity Server 2004Q2 管理指南*》的第二部分。其中介绍了 Identity Server 图形用户界面以及浏览该界面的方法。本部分包含以下各章：

第 4 章

身份认证管理

本章介绍 Sun Java™ System Identity Server 2004Q2 的身份管理功能。“身份管理”模块界面提供了查看、管理和配置所有 Identity Server 对象和身份的方法。本章包含以下部分：

Identity Server 控制台

Identity Server 控制台分为三个部分：“位置”窗格、“浏览”窗格和 “数据”窗格。通过使用这三个窗格，管理员可以浏览目录、执行用户和服务配置以及创建策略。

图 4-1 Identity Server 控制台

标题窗格

“标题”窗格位于控制台的顶部。“标题”窗格中的选项卡允许管理员在各个管理模块视图之间进行切换：

- “身份管理”模块 - 允许创建和管理与身份相关的对象。
- “服务配置”模块 - 允许配置 Identity Server 的默认服务。
- “当前会话”模块 - 允许管理员查看当前会话信息以及终止任一会话。
- “联合管理”模块 - 允许使用由 Liberty Alliance Project 开发的适用于联合网络身份的开放标准。

*位置*字段用于追踪管理员在目录树中的位置。此路径用于进行浏览。

*欢迎*字段显示当前运行控制台的用户的名称，并可以链接到用户配置文件。

*搜索*链接显示用户用于搜索特定 Identity Server 对象类型的条目的界面。使用下拉菜单选择对象类型并输入搜索字符串。结果将返回到搜索表格中。允许输入通配符。

*帮助*链接可以打开一个浏览窗口，其中包含有关“身份管理”、“当前会话”、“联合管理”以及本文档中第 IV 部分 “属性参考”的信息。

*退出*链接允许用户从 Identity Server 中退出。

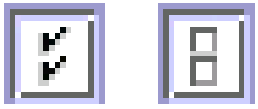
浏览窗格

“浏览”窗格位于 Identity Server 控制台的左侧。*目录对象*部分 （在灰色框中）显示当前打开的目录对象的名称及其*属性*链接。（“浏览”窗格中显示的大多数对象都将具有相应的*属性*链接。选择此链接将在右侧的 “数据”窗格中显示条目的属性。）“查看”菜单列出了选定目录对象下的目录。根据子目录的数量，界面将提供分页功能。

数据窗格

“数据”窗格位于控制台的右侧。此窗格用于显示和配置所有对象属性及其值，还可以在其中按照组、角色或组织选择其相应的条目。

提示 您可以通过单击 “全部选择”或 “全部取消”图标来选择或取消选择列表中的所有项目。



Identity Server 图形用户界面有两种基本视图。用户可能会获得 “身份管理”视图或 “用户配置文件”视图的访问权，具体取决于登录用户的角色。

“身份管理”视图

当具有管理角色的用户在 Identity Server 中进行验证时，其默认视图为 “身份管理”视图。管理员可以在该视图中执行管理任务。这些任务可以包括创建、删除和管理对象 （用户、组织、策略等）及配置服务，具体取决于管理员的角色。

图 4-2 显示了组织属性的 “身份管理”视图

用户配置文件视图

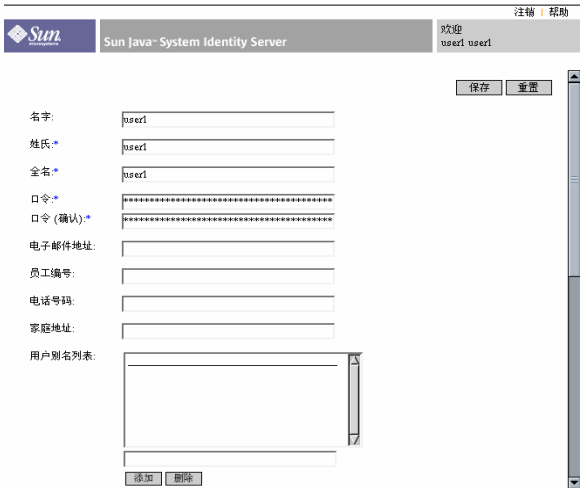
当尚未指定管理角色的用户向 Identity Server 进行验证时，默认视图为用户自己的 “用户配置文件”视图。在该视图中，用户可以修改其个人配置文件特定的属性值。包括但不限于姓名、家庭地址和口令。可以扩展 “用户配置文件”视图中显示的属性。有关为对象和身份添加自定义属性的详细信息，参见 《*Identity Server Developer's Guide*》。

属性功能

要查看或修改条目属性，请单击对象名称旁边的属性箭头。将会在 “数据”窗格中显示其属性及相应的值。不同的对象显示不同的属性。

有关如何扩展条目的属性的信息，参见 《*Identity Server Developer's Guide*》。

图 4-3 用户配置文件视图



身份管理界面

可使用 “身份管理”界面创建和管理与身份相关的对象。使用 Identity Server 控制台或命令行界面可以定义、修改或删除用户、角色、组、策略、组织、子组织和容器对象等等。控制台的默认管理员具有不同等级的权限，这些权限可用于创建和管理组织、组、容器、用户、服务和策略。（可以基于角色创建其他管理员。）管理员是在与 Identity Server 一起安装 Directory Server 时，在 Directory Server 中进行定义的。

管理 Identity Server 对象

“用户管理”界面包含查看和管理 Identity Server 对象 （组织、组、用户、服务、角色策略、容器对象和代理）必需的所有组件。本部分说明对象类型及其详细配置方法。

对于多数 Identity Server 对象类型，可选择配置 “显示选项”和 “可用操作”以显示或隐藏 Web 界面在 Identity Server 控制台中的显示方式。配置在组织和角色级完成，用户会从其所在组织以及分配给他们的角色中继承该配置。这些设置在本章的最后进行说明。

组织

在企业用来管理部门和资源的层次结构中，*组织*表示最高一级。安装时， Identity Server 会动态创建一个顶级组织 （在安装过程中定义）以管理 Identity Server 企业配置。安装后可以创建其他组织，以管理单独的企业。所有创建的组织均位于顶级组织之下。

创建组织

1. 从 “身份管理” 模块的 “查看” 菜单中选择 “组织”。
2. 在 “浏览” 窗格中单击 “新建”。
3. 输入字段的值。仅 “名称” 是必需字段。这些字段包括：

   名称。输入组织的名称。

   域名。输入组织的完整域名系统 (DNS) 名称 （如果存在）。

   组织状态。选择 “有效” 或 “无效” 状态。

   默认值为 “有效”。在组织存在期间，可以随时选择属性图标来更改该状态。如果选择 “无效”，则当登录到组织时，将禁用用户访问。

   组织别名。该字段定义组织的别名，以允许您在通过 URL 登录时使用别名进行验证。例如，如果组织的名称为 `exampleorg`，而将 `123` 和 `abc` 定义为组织的别名，则可使用以下任一 URL 登录到该组织：

   ```
   http://machine.example.com/UI/Login?org=exampleorg
   ```

   ```
   http://machine.example.com/UI/Login?org=abc
   ```

   ```
   http://machine.example.com/UI/Login?org=123
   ```

   组织别名在组织中必须唯一。可以使用 “唯一属性列表” 来强制执行唯一性。

   DNS 别名。用于添加组织的 DNS 名称的别名。该属性只接受 “真实的” 域别名 （不允许使用随机字符串）。例如，如果 DNS 的名称为 `example.com`，而名为 `exampleorg` 的组织的别名定义为 `example1.com` 和 `example2.com`，则可使用以下任一 URL 登录到该组织：

   ```
   http://machine.example.com/UI/Login?org=exampleorg
   ```

   ```
   http://machine.example1.com/UI/Login?=org=exampleorg
   ```

   ```
   http://machine.example2.com/UI/Login?org=exampleorg
   ```

   唯一属性列表。用于添加组织中用户的唯一属性名列表。例如，如果添加用于指定电子邮件地址的唯一属性名，则不能创建两个使用相同电子邮件地址的用户。也可以在该字段中输入以逗号分隔的列表。列表中的任一属性名均定义了唯一性。例如，如果该字段包含以下属性名列表：

`PreferredDomain, AssociatedDomain`

并且针对特定用户将 `PreferredDomain` 定义为 `http://www.example.com`，从而使整个以逗号分隔的列表在 URL 中唯一。

对于所有子组织都强制执行唯一性。

4. 单击 “确定”。

   将在 “浏览”窗格中显示新创建的组织。要编辑在创建组织过程中定义的任意属性，请单击所要编辑的组织旁边的属性箭头，从 “数据”窗格的 “查看”菜单中选择 “常规”，然后编辑属性并单击 “确定”。可使用 “显示选项”和 “可用操作”视图来自定义 Identity Server 控制台的外观，并为所有针对此组织进行验证的用户指定相应的行为。

删除组织

1. 从 “身份管理”模块的 “查看”菜单中选择 “组织”。

   将显示所有已创建的组织。要显示特定的组织，请输入搜索字符串并单击 “搜索”。

2. 选中要删除的组织名称旁边的复选框。

3. 单击 “删除”。

注 执行删除时不会显示警告消息。组织内的所有条目都将被删除，并且不能执行撤消操作。

将组织添加到策略

可以通过定义策略的主题将 Identity Server 对象添加到策略中。在创建或修改策略时，可以在策略的 “主题”页面中将组织、角色、组和用户定义为主题。定义了主题后，策略将被应用到对象。有关详细信息，参见第 129 页的 “管理策略”。

组

*组*代表具有共同职责、特征或利益的用户集合。通常来说，这种分组不会涉及权限。组可存在于两个级别，分别是组织和其他被管理组中。存在于其他组中的组称为*子组*。子组是 “物理上”存在于父组中的子节点。

Identity Server 还支持*嵌套组*，它们是单个组中所含现有组的 “表示形式”。与子组不同，嵌套组可以存在于 DIT 中的任何位置。使用嵌套组可以快速地为多个用户设置访问权限。

创建组时，您可以创建采用 “按订阅指定成员”的组 （*静态组*），也可以创建采用 “按过滤指定成员”的组 （*过滤组*）。这样可以控制将用户添加到组的方式。只能将用户添加到静态组。动态组则用来通过过滤器控制用户的添加。但是，嵌套组或子组却可以添加到静态组和动态组。

静态组 （按订阅指定成员）

当按订阅指定组成员时，将根据您指定的 “管理的组类型”创建静态组。如果 “管理的组类型”值为 “静态”，则使用 `groupOfNames` 或 `groupOfUniqueNames` 对象类将组成员添加到组条目中。如果 “管理的组类型”值为 “动态”，则使用特定的 LDAP 过滤器来搜索并只返回包含 `memberof` 属性的用户条目。有关详细信息，参见第 217 页的 “管理的组类型”。

注 默认情况下，管理的组类型为动态的。您可以在 “管理”服务配置中更改此默认设置。

过滤组 （按过滤指定成员）

过滤的组是指通过使用 LDAP 过滤器创建的动态组。所有条目都会被过滤器过滤并被动态指定给组。过滤器将搜索条目中的属性，并返回包含该属性的条目。例如，如果您想基于楼房编号创建组，可以使用过滤器返回一个包含楼房编号属性的所有用户的列表。

注 要使用引用完整性插件，应将 Identity Server 与 Directory Server 一起进行配置。启用引用完整性插件后，该插件会在删除或重命名操作后立即对指定属性执行完整性更新。这就确保了数据库中的所有相关条目之间总保持相应的关系。数据库索引则增强了 Directory Server 中的搜索性能。有关启用插件的详细信息，参见 《*Sun Java System Identity Server Migration Guide*》。

创建静态组

1. 转到将在其中创建组的组织、组或组容器。
2. 从 “查看” 菜单中选择 “组”。
3. 单击 “新建”。
4. 从 “数据” 窗格中选择 “按订阅指定成员” 作为组类型。
5. 在 “名称” 字段中输入组的名称。单击 “下一步”。
6. 选择 “用户可以订阅该组” 属性可以使用户自行订阅组。
7. 如果已在 DIT 中定义了多个组容器，并且未启用 （管理服务的）“显示组容器” 属性，则可以选择静态组所属的父组容器。否则，将不显示此字段。
8. 单击 “完成”。

   组创建完毕后，可以通过从 “数据” 窗格的 “查看” 菜单中选择 “常规” 来编辑 “用户可以订阅该组” 属性。

在静态组中添加或移除成员

1. 单击要向其添加成员的组旁边的属性箭头。

2. 在 “数据”窗格中，从 “查看”菜单中选择 “成员”。

   在 “选择操作”菜单中选择要执行的操作。可以执行以下操作：

   新建用户。保存用户信息时，此操作将创建新用户并自动将该用户添加到组。

   添加用户。此操作可将现有用户添加到组。选择此操作后，请创建搜索条件指定要添加的用户。用来构造该条件的字段使用 ANY 或 ALL 运算符。 ALL 将根据所有指定的字段向用户返回结果。 ANY 将根据所指定的任一字段向用户返回结果。如果某个字段保留为空，则该字段将匹配该特定属性的所有可能条目。从返回的用户列表中，选择要添加的用户并单击 “确定”。

   添加组。此操作可把嵌套组添加到当前组。选择此操作时要创建搜索条件，包括搜索范围、组的名称 （允许使用通配符 “*”），并且可指定用户是否可以自行订阅组。从返回的组列表中，选择要添加的组并单击 “确定”。

   移除成员。此操作只是从组中移除成员，不会进行永久性删除。选择要移除的成员并从操作菜单中选择 “移除成员”。

   删除成员。此操作可永久删除所选成员。

创建过滤组

1. 找到要在其中创建组的组织 （或组）。
2. 从 “查看”菜单中选择 “组”。
3. 单击 “新建”。
4. 从 “数据”窗格中为组类型选择 “按过滤指定成员”。
5. 在 “名称”字段中输入组的名称。单击 “下一步”。

6. 构造 LDAP 搜索过滤器。

   默认情况下，Identity Server 将显示 Basic 搜索过滤器界面。用于构造过滤器的 Basic 字段使用 ANY 或 ALL 运算符。 ALL 将根据所有指定的字段向用户返回结果。 ANY 将根据所指定的任一字段向用户返回结果。如果某个字段保留为空，则该字段将匹配该特定属性的所有可能条目。

   另外，您可以选择 “高级”按钮来自行定义过滤器属性。例如：

   ```
   (&(uid=user1)(|(inetuserstatus=active)(!(inetuserstatus=*))))
   ```

   单击 “完成”后，系统将自动把与搜索条件匹配的所有用户添加到组。

在过滤组中添加或移除成员

1. 单击要向其添加成员的组旁边的属性箭头。
2. 在 “数据”窗格中，从 “查看”菜单中选择 “成员”。

   在 “选择操作”菜单中选择要执行的操作。可以执行以下操作：

   添加组。此操作可把嵌套组添加到当前组。选择此操作时要创建搜索条件，包括搜索范围、组的名称 （允许使用通配符 “*”），并且可指定组是否允许用户自行订阅。从返回的组列表中，选择要添加的组并单击 “确定”。

   移除成员。此操作只是从组中移除成员，不会进行永久性删除。选择要移除的成员并单击 “确定”。

   删除成员。此操作可永久删除所选成员。

将组添加到策略

可以通过定义策略的主题将 Identity Server 对象添加到策略中。在创建或修改策略时，可以在策略的 “主题”页面中将组织、角色、组和用户定义为主题。定义了主题后，策略将被应用到对象。有关详细信息，参见第 129 页的 “管理策略”。

用户

*用户*表示个人身份。通过 “Identity Server 身份管理”模块，可以在组织、容器和组中创建和删除用户，还可以从角色和/或组中添加或移除用户。此外，还可以将服务指定给用户。

注 如果子组织中的用户使用相同的用户 ID (amadmin) 创建，以 amadmin 登录时将会失败。如果出现这种问题，管理员应该通过 Directory Server 控制台更改用户的用户 ID。这样可使管理员登录到默认组织。另外，验证服务中的 “起始用户搜索的 DN”可以设置为用户容器 DN，以确保在登录过程中返回唯一匹配项。

创建用户

1. 找到要在其中创建用户的组织、容器或用户容器。
2. 从 “查看”菜单中选择 “用户”。
3. 单击 “新建”。

   “数据”窗格中将显示 “新建用户”页面。
4. 选择要指定给用户的服务。

   仅显示那些包含用户属性并且已添加到用户所属的组织中的服务。单击 “下一步”。
5. 如果已在 DIT 中定义了多个 （两个以上）组容器，并且未启用 （管理服务器中的）“显示组容器”属性，则可以从 “用户创建”页面选择静态组所属的用户容器。否则，将不显示此字段。
6. 输入必需的属性值。

   有关用户配置文件属性的信息，参见第 341 页的 “用户属性”。
7. 单击 “确定”。

将用户添加到角色和组

1. 找到要修改的用户所属的组织。
2. 从 “查看”菜单中选择 “用户”。

3. 在 “浏览”窗格中，选择所要修改的用户并单击属性箭头。
4. 从 “数据”窗格的 “查看”菜单中选择 “角色”或 “组”。仅显示已指定给该用户的角色和组。单击 “添加”查看要从中进行选择的可用角色和组列表。
5. 选择要向其添加用户的角色或组，然后单击 “保存”。

为用户添加服务

1. 找到要修改的用户所属的组织。
2. 从 “浏览”窗格的 “查看”菜单中选择 “用户”。
3. 在 “浏览”窗格中，选择所要修改的用户并单击属性箭头。
4. 从 “数据”窗格的 “查看”菜单中选择 “服务”。
5. 单击 “添加”以选择要指定到用户的服务。
6. 单击 “保存”。

删除用户

1. 查找用户所在的位置。
2. 从 “查看”菜单中选择 “用户”。
3. 选中要删除的用户名称旁边的复选框。
4. 单击 “删除”。

注 在进行删除操作之前不会显示警告消息，且删除操作不能撤消。

将用户添加到策略

可以通过定义策略的主题将 Identity Server 对象添加到策略中。在创建或修改策略时，可以在策略的 “主题”页面中将组织、角色、组和用户定义为主题。定义了主题后，策略将被应用到对象。有关详细信息，参见第 129 页的 “管理策略”。

服务

为组织或容器激活*服务*需要两步 （容器与组织的行为相同）。首先，需要将该服务添加到组织。添加服务后，必须配置专门为该组织配置的模板。有关其他信息，参见第 5 章 “服务配置”

注 首先必须通过命令行的 `amadmin` 命令将新服务导入到 Identity Server 中。有关导入服务的 XML 模式的信息，参见 《*Identity Server Developer's Guide*》。

添加服务

1. 找到要向其中添加服务的组织。

   从 “身份管理” 模块的 “查看” 菜单中选择 “组织”，然后从 “浏览” 窗格中选择组织。“位置” 路径可以显示默认的顶级组织和选定的组织。

2. 从 “查看” 菜单中选择 “服务”。

3. 单击 “添加”。

   “数据” 窗格中将显示可添加到此组织的服务的列表。

4. 选择要每个所要添加服务旁边的复选框。

5. 单击 “确定”。将在 “浏览” 窗格中显示已添加服务。

注 只有添加到父组织的服务才会在子组织级别显示。

为服务创建模板

1. 找到添加的服务所在的组织或角色。

   从 “身份管理” 模块的 “查看” 菜单中选择 “组织”，然后从 “浏览” 窗格中选择组织。

2. 从 “查看” 菜单中选择 “服务”。

3. 单击要激活的服务名称旁边的属性图标。

   “数据”窗格中将显示消息：*当前不存在用于该服务的模板。现在是否创建一个模板？*

4. 单击 “是”。

   将为父组织或角色的该服务创建模板。“数据”窗格中将显示此服务的默认属性和值。有关默认服务属性的说明，参见第 213 页的 “属性参考”。

5. 接受或修改默认值，然后单击 “保存”。

移除服务

1. 找到要移除的服务所在的组织。

   从 “身份管理”模块的 “查看”菜单中选择 “组织”，然后从 “浏览”窗格中选择组织。

2. 从 “查看”菜单中选择 “服务”。

3. 选中要移除的服务的复选框。

4. 单击 “移除”。

注 如果服务是在子组织级别注册的，则无法在父组织级别移除这些服务。

角色

*角色*是与*组*概念类似的 Directory Server 条目机制。组有成员，角色也有成员。角色的成员是指具有该角色的 LDAP 条目。角色本身的条件被定义为具有属性的 LDAP 条目，由条目的独特的名称 (DN) 属性来标识。 Directory Server 具有很多不同类型的角色，但 Identity Server 只能管理其中的一种：被管理的角色。

注 在目录部署中还可以使用其他 Directory Server 角色类型，只是它们不能被 Identity Server 控制台管理。还可以在策略的主题定义中使用其他 Directory Server 类型。有关策略主题的详细信息，参见第 126 页的 “创建策略”。

用户可以拥有一个或多个角色。例如，可以创建一个承包商角色，其属性来自 “会话服务”和 “口令重置服务”。启动新承包商时，管理员可以将其指定为该角色，而不需在承包商条目中分别设置各个属性。如果承包商在工程部工作并且需要适用于工程员工的服务以及访问权限，则管理员可以为该承包商同时指定工程角色和承包商角色。

Identity Server 使用角色来应用访问控制指令。首次安装 Identity Server 时，会配置用于定义管理员权限的访问控制指令 (ACI)。然后会在角色 （如 “组织管理员角色”和 “组织帮助台管理员角色”）中指定这些 ACI。当将角色分配给用户时，这些角色用于定义用户的访问权限。

仅当管理服务中启用了 “显示用户的角色”属性时，用户才可以查看为其分配的角色。有关详细信息，参见第 225 页的 “在 “用户配置文件”页面中显示角色”。

注 要使用引用完整性插件，应将 Identity Server 与 Directory Server 一起进行配置。启用引用完整性插件后，该插件会在删除或重命名操作后立即对指定属性执行完整性更新。这就确保了数据库中的所有相关条目之间总保持相应的关系。数据库索引则增强了 Directory Server 中的搜索性能。有关启用插件的详细信息，参见 《*Sun Java System Identity Server Migration Guide*》。

与组类似，角色也可以通过过滤创建，或者以静态方式创建。

静态角色。与过滤的角色相比，静态角色在创建时可以不添加用户。这样，在向给定的角色添加特定用户时，您可以更好的进行控制。

过滤的角色。过滤的角色是指通过使用 LDAP 过滤器创建的动态角色。在创建角色时，会为所有通过过滤器过滤的用户指定该角色。过滤器会搜索条目中的所有属性值对 （例如， `ca=user*`），并自动将包含该属性的用户指定到角色。

创建静态角色

1. 在 “浏览”窗格中，找到要在其中创建角色的组织。

2. 从 “查看”菜单中选择 “角色”。

   配置组织时会创建一组默认角色，这些角色显示在 “浏览”窗格中。默认角色包括：

   容器帮助台管理员。“容器帮助台管理员”角色拥有对组织单元内所有条目的读取权限，但仅对自身容器单元中用户条目的 `userPassword` 属性具有写入权限。

   组织帮助台管理员。“组织帮助台管理员”拥有对组织中所有条目的读取权限以及对 `userPassword` 属性的写入权限。

注 创建一个子组织时，请注意要在该子组织中创建管理角色，而不是在父组织中创建管理角色。

容器管理员。“容器管理员”角色拥有对 LDAP 组织单元中所有条目的读写权限。在 Identity Server 中， LDAP 组织单元通常被称为容器。

组织策略管理员。“组织策略管理员”拥有对所有策略的读写权限，并可以创建、分配、修改和删除自身组织内的所有策略。

用户容器管理员。默认情况下，新创建的组织中的所有用户条目都是该组织的“用户容器”的成员。“用户容器管理员”对该组织的 “用户容器”中的所有用户条目都具有读写权限。请注意，该角色 “并不”具有对包含角色和组 DN 的属性的读写权限，因此他们不能修改角色和组的属性，也不能从角色或组中移除用户。

注 可以使用 Identity Server 配置其他容器，以包含用户条目、组条目甚至其他容器。要将 “管理员”角色应用到配置组织之后创建的容器，可使用 “容器管理员角色”或 “容器帮助台管理员”默认值。

组管理员。“组管理员”对特定组的所有成员拥有读写权限，并可以创建新用户、将用户分配给自己所管理的组以及删除自己创建的用户。

创建组时，将自动生成组管理员角色，并赋予管理组所必需的权限，但不会将角色自动指定到组成员。角色必须由组创建者或任何拥有 “组管理员角色”访问权限的人员来指定。

顶级管理员。“顶级管理员”拥有对顶级组织中所有条目的读写权限。换句话说，“顶级管理员”角色具有 Identity Server 应用程序中所有配置主用户所拥有的权限。

组织管理员。“组织管理员”拥有对组织中所有条目的读写权限。创建组织时将自动生成组织管理员角色，该角色拥有管理组织所必需的权限。

3. 在 “浏览”窗格中单击 “新建”。“数据”窗格中将显示 “新建角色”模板。
4. 选择 “静态角色”，然后输入名称。单击 “下一步”。
5. 输入角色的说明。
6. 从 “类型”菜单中选择角色类型。

   角色可以是管理角色，也可以是服务角色。角色类型由控制台使用，用来确定在哪里启动 Identity Server 控制台中的用户。管理角色会通知控制台，角色的所有人拥有管理权限；服务角色会通知控制台，角色的所有人为最终用户。

7. 从 “访问权限”菜单中选择一组默认权限以应用到角色。拥有这些权限后便可以访问组织中的条目。显示的默认权限未按照特定顺序排列。这些权限包括：

   无权限。对角色不设置权限。

   组织管理员。“组织管理员”拥有对已配置的组织中所有条目的读写权限。

   组织帮助台管理员。“组织帮助台管理员”拥有对已配置的组织中所有条目的读取权限以及对 `userPassword` 属性的写入权限。

   组织策略管理员。“组织策略管理员”拥有对组织中所有策略的读写权限。组织策略管理员不能创建对等组织的侯选策略。

   通常，“无权限 ACI”会指定给服务角色，而默认的 ACI 会指定给管理角色。

8. 单击 “完成”。

   创建的角色显示在 “浏览”窗格中，该角色的状态信息显示在 “数据”窗格中。

   通过从 “查看”菜单中选择 “显示选项”和 “可用操作”，可以有选择性地对显示选项和可用操作进行配置。有关详细信息，参见本章最后的 “显示选项”和 “可用操作”。

将用户添加到静态角色

1. 选择要修改的角色，然后单击属性箭头。
2. 从 “数据”窗格的 “查看”菜单中选择 “用户”。
3. 单击 “添加”。

4. 输入搜索条件信息。可以选择一个或多个显示的字段，根据这些字段来搜索用户。这些字段包括：

   根据值返回用户。用于指定搜索要返回的值。

   匹配。允许您使用逻辑运算符连接所有用于过滤的字段。 ALL 将根据所有指定的字段向用户返回结果。 ANY 将根据所指定的任一字段向用户返回结果。

   用户 ID。按照用户 ID 搜索用户。

   名字。按照用户的名字搜索用户。

   姓氏。按照用户的姓氏搜索用户。

   全名。按照用户的全名搜索用户。

   用户状态。按照用户的状态 （有效或无效）搜索用户。

5. 单击 “下一步”开始搜索。将显示搜索结果。
6. 选中用户名称旁边的复选框，可以从返回的名称中选择用户。
7. 单击 “完成”。

   用户将被分配到角色。

创建过滤的角色

1. 在 “浏览”窗格中，找到要在其中创建角色的组织。
2. 从 “查看”菜单中选择 “角色”。

   配置组织时会创建一组默认角色，这些角色显示在 “浏览”窗格中。默认角色包括：

   容器帮助台管理员。“容器帮助台管理员”角色拥有对组织单元内所有条目的读取权限，但仅对自身容器单元中用户条目的 userPassword 属性具有写入权限。

   组织帮助台管理员。“组织帮助台管理员”拥有对组织中所有条目的读取权限以及对 userPassword 属性的写入权限。

注 创建一个子组织时，请注意要在该子组织中创建管理角色，而不是在父组织中创建管理角色。

容器管理员。“容器管理员”角色拥有对 LDAP 组织单元中所有条目的读写权限。在 Identity Server 中， LDAP 组织单元通常被称为容器。

组织策略管理员。“组织策略管理员”拥有对所有策略的读写权限，并可以创建、分配、修改和删除自身组织内的所有策略。

用户容器管理员。默认情况下，新创建的组织中的所有用户条目都是该组织的“用户容器”的成员。“用户容器管理员”对该组织的 “用户容器”中的所有用户条目都具有读写权限。请注意，该角色 “并不”具有对包含角色和组 DN 的属性的读写权限，因此他们不能修改角色和组的属性，也不能从角色或组中移除用户。

注 可以使用 Identity Server 配置其他容器，以包含用户条目、组条目甚至其他容器。要将 “管理员”角色应用到配置组织之后创建的容器，可使用 “容器管理员角色”或 “容器帮助台管理员”默认值。

组管理员。“组管理员”对特定组的所有成员拥有读写权限，并可以创建新用户、将用户分配给自己所管理的组以及删除自己创建的用户。

创建组时，将自动生成组管理员角色，并赋予管理组所必需的权限，但不会将角色自动指定到组成员。角色必须由组创建者或任何拥有 “组管理员角色”访问权限的人员来指定。

顶级管理员。“顶级管理员”拥有对顶级组织中所有条目的读写权限。换句话说，“顶级管理员”角色具有 Identity Server 应用程序中所有配置主用户所拥有的权限。

组织管理员。“组织管理员”拥有对组织中所有条目的读写权限。创建组织时将自动生成组织管理员角色，该角色拥有管理组织所必需的权限。

3. 在 “浏览”窗格中单击 “新建”。“数据”窗格中将显示 “新建角色”模板。
4. 选择 “过滤的角色”，然后输入名称。单击 “下一步”。
5. 输入角色的说明。
6. 从 “类型”菜单中选择角色类型。

   角色可以是管理角色，也可以是服务角色。角色类型由控制台使用，用来确定在哪里启动 Identity Server 控制台中的用户。管理角色会通知控制台，角色的所有人拥有管理权限；服务角色会通知控制台，角色的所有人为最终用户。
7. 从 “访问权限”菜单中选择默认的一组权限，以应用到角色。
8. 拥有这些权限，可以访问组织中的条目。显示的默认权限未按照特定顺序排列。这些权限包括：

   无权限。对角色不设置权限。

   组织管理员。“组织管理员”拥有对已配置的组织中所有条目的读写权限。

   组织帮助台管理员。“组织帮助台管理员”拥有对已配置的组织中所有条目的读取权限以及对 `userPassword` 属性的写入权限。

   组织策略管理员。“组织策略管理员”拥有对组织中所有策略的读写权限。组织策略管理员不能创建对等组织的侯选策略。

   通常，“无权限 ACI”会指定给服务角色，而默认的 ACI 会指定给管理角色。

9. 输入搜索条件信息。这些字段包括：

   匹配。允许您使用逻辑运算符连接所有用于过滤的字段。 ALL 将根据所有指定的字段向用户返回结果。 ANY 将根据所指定的任一字段向用户返回结果。

   用户 ID。按照用户 ID 搜索用户。

   名字。按照用户的名字搜索用户。

   姓氏。按照用户的姓氏搜索用户。

   全名。按照用户的全名搜索用户。

   用户状态。按照用户的状态 （有效或无效）搜索用户。

   另外，您可以选择 “高级”按钮来自行定义过滤器属性。例如：

   ```
   (&(uid=user1)(|(inetuserstatus=active)(!(inetuserstatus=*))))
   ```

   单击 “重置”以清除过滤器属性，或者单击 “取消”以取消创建角色进程。

10. 单击 “完成”基于过滤条件启动搜索。通过过滤条件定义的用户会自动被指定到角色。

    通过从 “查看”菜单中选择 “显示选项”和 “可用操作”，可以有选择性地对显示选项和可用操作进行配置。有关详细信息，参见本章最后的 “显示选项”和 “可用操作”。

注 可以通过 “角色配置文件”页面和 / 或 “用户配置文件”页面将用户添加到静态角色中。

从角色中移除用户

1. 找到包含要修改的角色的组织。

   从 “身份管理”模块的 “查看”菜单中选择 “组织”，然后从 “浏览”窗格中选择组织。

2. 从 “查看”菜单中选择 “角色”。

3. 选择要修改的角色。

4. 从 “查看”菜单中选择 “用户”。

5. 选择每个要移除的用户旁边的复选框。

6. 单击 “移除”。

   用户将从角色中移除。

将角色添加到策略

可以通过定义策略的主题将 Identity Server 对象添加到策略中。在创建或修改策略时，可以在策略的 “主题”页面中将组织、角色、组和用户定义为主题。定义了主题后，策略将被应用到对象。有关详细信息，参见第 129 页的 “管理策略”。

自定义角色的服务

可以基于各个角色自定义角色可用的服务，以及服务属性的访问级别。通过设置特定于角色的属性值，可以为角色自定义每个可用服务。还可以为每项服务授予访问权限并将其授予这些服务的属性。可能有些服务您仅希望由特定类型用户 （例如管理器）访问。要实现这一目的，可将该服务指定给所有用户，但仅允许属于该角色的 “管理器”类型访问特定服务。

向服务属性应用相同的逻辑。用户的帐户由多个属性组成，其中有些属性 （例如帐户到期日期）用户无权进行访问。可以授予帐户管理员访问此属性的权限，但用户（帐户拥有者）不能。通过 “浏览”窗格中角色的 “服务”视图，可以自定义服务和属性访问权限。

必须首先在组织级别添加服务，才能显示这些服务。添加到角色的用户将继承该角色的服务属性。

配置服务

1. 在角色的 “服务”视图中，转到标有 “用于该角色的服务配置”部分。
2. 可通过单击服务名称旁边的 “编辑”链接来选择允许角色访问的服务。

   如果尚未创建服务模板，系统将提示您进行创建。单击 “是”。
3. 修改服务属性。有关特定服务属性的详细信息，参见本手册的第 3 部分*属性参考指南*。
4. 单击 “保存”。

注 当对某项服务的访问被拒绝 （未选中），将不会为拥有角色的用户在 Identity Server 控制台中显示该服务。另外，不能注册用户或撤消注册用户，不能将服务指定到用户，也不能创建、删除、查看或修改 “服务”模板。

自定义属性访问

1. 在角色的 “服务”视图中，转到标有 “用于该角色的服务访问权限”部分。
2. 为要修改的服务选择启用或禁用状态。启用状态允许对访问进行修改。禁用状态不允许对访问进行修改。
3. 单击 “修改访问”链接。
4. 通过选中 “读/写”或 “只读”复选框，为属性指定访问级别。
5. 单击 “保存”。

有关特定服务属性的详细信息，参见本手册的第 3 部分*属性参考指南*。

6. 单击 “保存”。

将角色添加到策略

可以通过定义策略的主题将 Identity Server 对象添加到策略中。在创建或修改策略时，可以在策略的 “主题”页面中将组织、角色、组和用户定义为主题。定义了主题后，策略将被应用到对象。有关详细信息，参见第 129 页的 “管理策略”。

删除角色

1. 找到包含有要删除的角色的组织。
2. 从 “身份管理”模块的 “查看”菜单中选择 “组织”，然后从 “浏览”窗格中选择组织。“位置”路径可以显示默认的顶级组织和选定的组织。
3. 从 “查看”菜单中选择 “角色”。
4. 选中角色名称旁边的复选框。
5. 单击 “删除”。

策略

*策略*定义用于保护组织的 Web 资源的规则。虽然策略的创建、修改和删除是通过“身份管理”模块来执行的，但是具体过程将在第 126 页的 “创建策略”中进行说明。

代理

Identity Server 策略代理对 Web 服务器和 Web 代理服务器上的内容提供保护以防止未授权的侵入。它们基于管理员配置的策略来控制对服务和 Web 资源的访问。

*代理*对象用于定义 “策略代理”配置文件，并允许 Identity Server 存储验证及其他有关保护 Identity Server 资源的特定代理的配置文件信息。通过 Identity Server 控制台，管理员可以查看、创建、修改和删除代理配置文件。

创建代理

1. 找到包含有要创建的代理的组织。
2. 从 “查看”菜单中选择 “代理”。
3. 单击 “新建”。
4. 输入字段的值。仅 “名称”是必需字段。这些字段包括：

   名称。输入代理的名称或身份。此名称是代理用来登录 Identity Server 的名称。不接受多字节名称。

   口令。输入代理的口令。此口令必须与在 LDAP 验证过程中代理所使用的口令匹配。

   确认口令。确认口令。

   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声明的代理请求。通常仅一个属性有效，所有其他属性都将被忽略。请使用以下格式：

agentRootURL=http://*server_name:port*/

设备状态。输入代理的设备状态。如果设置为 “有效”，则代理可以通过 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。

5. 单击 “确定”。

删除代理

1. 找到包含有要删除的代理的组织。
2. 从 “查看” 菜单中选择 “代理”。
3. 选择代理名称旁边的复选框。
4. 单击 “删除”。

容器

当由于对象类和属性的不同而无法使用组织条目时，将使用 *容器*条目。须注意，Identity Server 容器条目和 Identity Server 组织条目不必等同于 LDAP 对象类 `organizationalUnit` 和 `organization`，这一点很重要。它们是抽象的身份条目。理想情况下，将使用组织条目而不使用容器条目。

注 容器的显示是可选的。要查看容器，必须在 “服务配置” 模块中选择 “在菜单中显示容器”。有关详细信息，参见第 217 页的 “在视图菜单中显示容器”。

创建容器

1. 找到要在其中创建新容器的组织或容器。

   从 “查看” 菜单中选择 “容器”。

2. 单击 “新建”。

   “数据” 窗格中将显示 “容器” 模板。

3. 输入要创建的容器的名称。

4. 单击 “确定”。

   通过从 “查看” 菜单中选择 “显示选项” 和 “可用操作”，可以有选择性地对显示选项和可用操作进行配置。有关详细信息，参见本章最后的 “显示选项” 和 “可用操作”。

删除容器

1. 找到包含要删除容器的组织或容器。
2. 从 “查看” 菜单中选择 “容器”。
3. 选中要删除的容器名称旁边的复选框。
4. 单击 “删除”。

注 删除容器会删除容器中存在的所有对象，包括所有对象和子容器。

用户容器

*用户容器*是默认的 LDAP 组织单位。在组织中创建用户时，所有的用户都将被分配给该容器。用户容器位于组织级别和用户容器级别 （作为子用户容器）。它们只能包含其他用户容器和用户。如果需要，可以将其他用户容器添加到组织中。

注 用户容器的显示是可选的。要查看 “用户容器”，必须在 “服务配置” 模块中选择 “显示用户容器”。有关详细信息，参见第 216 页的 “显示用户容器”。

创建用户容器

1. 找到要在其中创建新用户容器的组织或用户容器。

   从 “查看” 菜单中选择 “用户容器”。

2. 单击 “新建”。

   “数据” 窗格中将显示 “用户容器” 模板。

3. 输入要创建的用户容器的名称。

4. 单击 “确定”。

删除用户容器

1. 找到包含要删除的用户容器的组织或用户容器。
2. 从 “查看”菜单中选择 “用户容器”。
3. 选中要删除的用户容器名称旁边的复选框。
4. 单击 “删除”。

注 删除用户容器会同时删除容器中存在的所有对象，包括所有用户和子用户容器。

组容器

*组容器*用于管理组。它只能包含组和其他组容器。组容器组会被动态指定为所有被管理的组的父项。如果需要，可以添加其他组容器。

注 组容器的显示是可选的。要查看组容器，必须在 “服务配置”模块中选择 “显示组容器”。有关详细信息，参见第 217 页的 “显示组容器”。

创建组容器

1. 找到要在其中创建组容器的组织或组容器。
2. 从 “查看”菜单中选择 “组容器”。

   创建组织时会同时创建默认组。
3. 单击 “新建”。
4. 在 “名称”字段中输入值，然后单击 “确定”。“浏览”窗格中将显示新创建的组容器。

删除组容器

1. 找到包含要删除的组容器的组织。

2. 从 “查看” 菜单中选择 “组容器”。

   “浏览” 窗格中将显示默认组和所有已创建的组容器。

3. 选中要删除的组容器旁边的复选框。

4. 单击 “删除”。

显示选项

对于组织、角色和容器，可以使用 “显示选项” 视图自定义 Identity Server 对象在 Identity Server 控制台中的显示方式。并不是所有显示选项都可用于任意对象类型。

更改显示选项

1. 单击要为其更改显示选项的组织的属性箭头。

2. 从 “数据” 窗格的 “查看” 菜单中选择 “显示选项”。

3. 编辑 “常规” 部分的属性。这些属性包括：

   生成全名属性。选择此属性可以使 Identity Server 始终生成用户的全名，它由用户配置文件中的名字和姓氏值构成。

   始终选择第一个条目。选择此属性用于搜索，可以在 “浏览” 窗格中自动选择第一个采用给定身份对象类型的项并将其显示在 “数据” 窗格中。

   “用户配置文件” 页面的标题。从下拉菜单中选择用于 “用户配置文件页面” 标题的属性。

   禁用初始搜索。此值将禁用对一个或多个身份对象类型的初始 Identity Server 搜索。禁用初始搜索可能增强性能并降低发生超时错误的可能性。

4. 在 “Identity Server 目录对象的显示配置” 部分中更改显示选项。可以在此部分自定义显示 Identity Server 容器和对象的方式。利用 “Identity Server 目录容器” 选项可以指定在 “浏览” 窗格的 “查看” 菜单中显示的对象视图。利用 “Identity Server 目录对象” 字段可以指定在 “数据” 窗格的 “查看” 菜单中显示的对象视图。

5. 单击 “保存”。

可用操作

对于某些 Identity Server 对象类型，可以通过 “可用操作”视图来定义用户访问权限。

为用户设置可用操作

1. 单击要为其设置可用操作的身份对象的属性箭头。
2. 从 “数据”窗格的 “查看”菜单中选择 “可用操作”。
3. 选择可用于所有 Identity Server 对象的操作类型。操作类型定义用户对每个对象的访问能力。这些操作类型包括：

   无权访问。用户无权访问此对象。

   查看。用户具有对此对象的只读访问权限。

   修改。用户可以修改和查看此对象。

   删除。用户可以修改、查看和删除此对象。

   完全访问。用户可以创建、修改、查看和删除此对象。
4. 单击 “保存”。要将这些值更改为其以前保存的状态，请单击 “重置”。

第 5 章

服务配置

本章介绍 Sun Java™ System Identity Server 2004Q2 的服务管理功能。“服务配置”界面提供了查看、管理和配置所有 Identity Server 服务及其值 （默认值和自定义值）的方法，以及配置 Identity Server 控制台显示设置的方法。本章包含以下部分：

服务的定义

*服务*是一组在公共名称下定义的属性。属性定义服务向组织提供的参数。例如，在开发工资单服务过程中，开发人员可能会决定包含定义员工姓名、小时工资率和免税额的属性。当服务被注册到组织时，组织可以在其条目的配置中使用这些属性。

Identity Server 使用可扩展标记语言 (XML) 定义服务。服务管理服务文档类型定义 (`sms.dtd`) 定义服务 XML 文件的结构。此文件位于以下目录：

IdentityServer_base`/SUNWam/dtd/` (Solaris)

IdentityServer_base`/identity/dtd` (Linux)

注 在本章中的余下部分将只给出 Solaris 目录信息。请注意 Linux 的目录结构有所不同。有关详细信息，请参见第 19 页的 “关于本指南”。

有关定义 Identity Server 服务的详细信息，参见 《*Identity Server Developer's Guide*》。

Identity Server 服务

Identity Server 附带的默认服务由位于以下目录中的 XML 文件来定义：

```
etc/opt/SUNWam/config/xml
```

通过 “服务配置”界面配置其中的某些服务可以为 Identity Server 应用程序定义值。另外一些服务被注册到在 Identity Server 中配置的特定组织，用于为该组织定义默认值。

管理服务

管理服务既允许在应用程序级别 （类似于 Identity Server 应用程序的 “*首选项*”或 “*选项*”菜单）配置控制台，也允许在已配置的组织级别 （已配置组织特有的 “*首选项*”或 “*选项*”菜单）配置控制台。

验证服务

有多个验证模块，其中一个是基本模块。这就使管理员有机会选择每个已定义组织用以检验用户授权的方法。

匿名

此验证服务允许在不指定用户名和口令的情况下登录。匿名连接对服务器的访问受到限制，并由管理员进行自定义。

基于证书

此验证服务允许通过个人数字证书 (PDC) 登录。

核心

此验证服务是 Identity Server 验证服务的总体配置基础。要使用任一特定服务，必须先注册并配置该模块。允许管理员定义默认值。

HTTP Basic

此验证服务使用基本验证，它是 HTTP 协议的内置验证支持。为使用此项服务，需要注册 LDAP 验证服务。不能从 C API 进行此操作。

LDAP

此验证服务允许使用 LDAP 绑定进行验证，LDAP 绑定是一种将口令与特定 LDAP 条目关联起来的操作。

成员资格 （自注册）

此验证服务允许新用户进行自注册，以使用登录和口令进行验证。对于自注册，不需要验证。

NT

此验证服务允许使用 Windows NT™/2000™ 服务器来验证用户。为实现 NT 验证模块，必须下载并安装 Samba Client (smbclient) 2.2.2 （对于 Linux，可以使用随操作系统提供的 Samba Client）。

RADIUS

此验证服务允许使用外部 “远程验证拨入用户服务” (RADIUS) 服务器来验证用户。

为使 RADUIS 验证服务与 Sun Java System Application Server 一起正常工作，必须配置 Application Server 的 `server.policy` 文件。有关此操作的说明，参见第 143 页的 “验证选项”。

SafeWord

此验证服务允许使用 Secure Computing 的 SafeWord™ 或 SafeWord PremierAccess™ 验证服务器来验证用户。

为使 SafeWord 验证服务与 Sun Java System Application Server 一起正常工作，必须配置 Application Server 的 `server.policy` 文件。有关此操作的说明，参见第 143 页的 “验证选项”。

SecurID

此验证服务允许使用 RSA ACE/Server® 验证软件和 SecurID® 验证程序来验证用户。 Solaris x86 不支持该服务。

注 在此版本的 Identity Server 中， Linux 操作系统不支持 SecurID 验证服务。

Unix

此验证服务允许使用 Unix® 服务器、通过用户的 UNIX 标识和口令来验证用户。

Windows 桌面 SSO

此验证服务允许已通过 “Kerberos 分发中心” (KDC) 验证的用户无需重新提交登录条件即可通过验证并登录到 Identity Server （单点登录）。

验证配置服务

验证配置服务允许您为角色、用户、服务和组织配置验证，以设置用于确定验证模块优先级的规则。还可通过此服务配置基于服务的验证。

客户机检测服务

“客户机检测”服务允许 Identity Server 检测正在访问的浏览器的客户机类型，并允许管理员根据客户机类型添加和配置设备。

全局化设置服务

“全局化设置”包含若干个可以针对不同字符集对 Identity Server 进行配置的属性。

搜索服务

Identity Server 的 “联合管理”模块将使用此项服务。有关该服务的详细信息，请参见 《*Identity Server Federation Management Guide*》。

特权个人配置文件服务

Identity Server 的 “联合管理”模块将使用此项服务。有关该服务的详细信息，请参见 《*Identity Server Federation Management Guide*》。

日志服务

管理员使用日志服务来配置 Identity Server 应用程序的日志函数的值。这些值包括日志文件的大小和日志文件的位置等。

命名服务

命名服务用于为各种其他 Identity Server 服务 （例如会话、验证和日志）获取和设置 URL、插件、配置以及请求通知。

口令重置服务

口令重置服务使用户能够接收遗忘的口令，或重置其用于访问受 Identity Server 保护的给定服务或应用程序的口令。口令重置服务属性由顶层管理员定义，它们可以控制用户验证凭证 （以 “秘密问题”形式）、控制新的或现有的口令通知机制，以及设置不正确用户验证的可能的锁定间隔。

平台服务

通过平台服务可以将附加服务器添加到 Identity Server 配置以及在 Identity Server 应用程序的顶层应用的其他选项中。

策略配置服务

策略配置服务定义在策略管理和策略评估过程中策略框架将要使用的值。

SAML 服务

安全声明标记语言 (SAML) 服务定义了一个在各个安全授权机构之间交换安全声明的框架，以便在提供验证和授权服务的不同平台上实现协同工作。

会话服务

会话服务为已验证的用户会话定义值，例如最长会话时间和最长空闲时间。

SOAP 绑定服务

Identity Server 的 “联合管理”模块将使用此项服务。有关该服务的详细信息，请参见 《*Identity Server Federation Management Guide*》。

用户服务

默认的用户首选项是通过用户服务来定义的。（这些首选项包括时区、语言环境和 DN 起始视图）。

属性类型

构成 Identity Server 服务的属性可分为以下类型：*动态*、*策略*、*用户*、*组织*和*全局*。使用这些类型再细分各个服务中的属性能够更加统一地安排服务模式，还能够更加轻松地管理服务参数。

动态属性

可以将动态属性指定给 Identity Server 已配置的角色或组织。当角色被指定给用户，或在组织中创建用户时，动态属性将变为用户的一个特征。例如，为组织的员工创建一个角色。该角色可以包含组织的地址和传真号码，这两项对于所有员工来说都是固定的。将该角色指定给每个员工时，每个员工均将继承这些动态属性。

用户属性

这些属性被直接指定给各个用户。用户不从角色或组织处继承这些属性，对于每个用户来说，这些属性通常是不同的。例如，用户 ID、员工编号和口令都是用户属性。可以通过修改 `amUser.xml` 文件来添加或移除用户服务中的用户属性。有关详细信息，参见《*Identity Server Developer's Guide*》。

组织属性

组织属性只指定给组织。在这方面它们与动态属性相似，但又与动态属性不同，因为它们不由子树中的条目继承。另外，不会有任何对象类与组织属性相关联。验证服务中列出的属性被定义为组织属性，因为验证是在组织级别进行的，而不是在子树或用户级别进行的。

全局属性

全局属性被应用到整个 Identity Server 配置中。由于全局属性的目的在于自定义 Identity Server 应用程序，因此不能将它们应用到用户、角色和组织中。 Identity Server 配置中只有一个全局属性的实例。对象类与全局属性不相关。全局属性的示例包括：日志文件的大小、日志文件的位置、端口号或 Identity Server 能够用于访问数据的服务器 URL。

策略属性

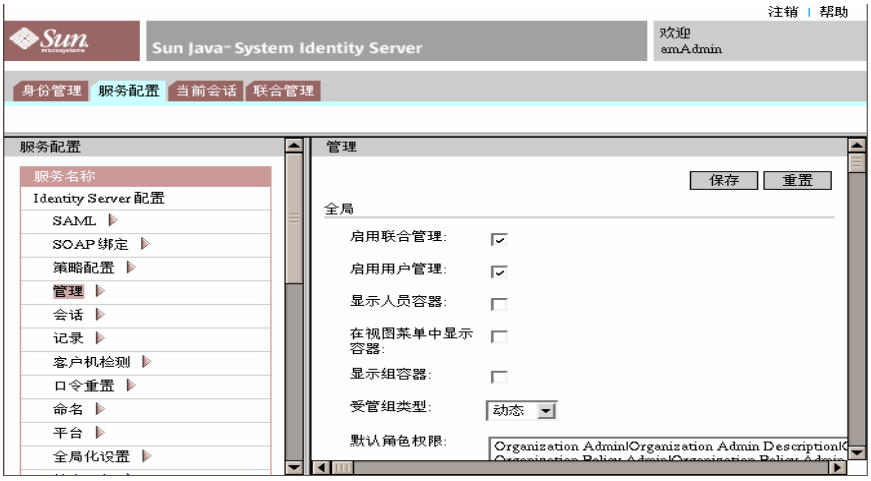
策略属性指定了与服务相关的访问控制操作 （或特权）。在将规则添加到策略时，这些属性将成为规则的一部分。如果要使用 Identity Server 策略管理此项服务的访问控制，则在服务模式中需要有 “策略” 属性。

服务配置界面

服务是通过 “服务配置” 模块进行配置和管理的。可以使用 XML （基于 Identity Server 服务文档类型定义或 DTD）编写 Identity Server 默认服务包中未包含的特定于组织的服务，然后将其添加到 “其他配置” 标题下的界面中。您可以在第 IV 部分 “属性参考”中找到有关如何进行此操作的说明，这部分内容介绍了默认服务及其相应属性的定义。

“服务配置” 模块用于显示全局级别的服务配置。换句话说，它是 Identity Server 中所有可用服务 （无论是否注册了这些服务）的默认配置的视图。当组织注册并激活了某项服务后，分配给服务的初始默认数据将显示在该服务的 “服务配置” 页面中。图 5-1 为图形用户界面的屏幕快照。

图 5-1 “服务配置”视图



通过选择 “服务配置”模块可以访问 “服务配置”视图。浏览框中将显示所有已定义的 Identity Server 服务的列表。要为服务设置全局默认值，请选择服务名称旁边的属性箭头。该服务的属性将显示在数据框中。

第 6 章

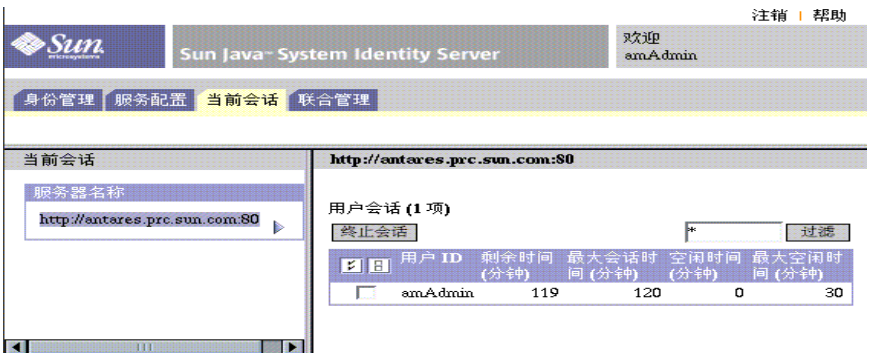
当前会话

本章介绍 Sun Java™ System Identity Server 2004Q2 的会话管理功能。会话管理模块提供了查看用户会话信息和管理用户会话的解决方案。它记录多个会话时间，并允许管理员终止会话。系统管理员应忽略 “平台服务器”列表中列出的负载平衡器服务器。

当前会话界面

拥有适当权限的管理员可以通过 “当前会话”模块界面，查看当前登录到 Identity Server 的用户的会话信息。

图 6-1 “当前会话”界面



会话管理框

“会话管理”框显示当前被管理的 Identity Server 的名称。

“会话信息”窗口

“会话信息”窗口显示当前登录到 Identity Server 的所有用户，并显示每个用户的会话时间。显示的字段包括：

用户 ID。显示当前登录用户的用户 ID。

剩余时间。显示需要重新验证之前，用户的该会话所剩余的时间 （以分钟为单位）。

最大会话时间。显示会话过期并且用户必须重新验证以重新获得访问权限之前用户可以登录的最长时间 （以分钟为单位）。

空闲时间。显示用户已处于空闲状态的时间 （以分钟为单位）。

最大空闲时间。显示在需要重新验证之前，用户可以处于空闲状态的最长时间 （以分钟为单位）。

时间限制由管理员在会话管理服务中定义。有关详细信息，参见第 335 页的 “会话服务属性”。

在 “用户 ID”字段中输入字符串，然后单击 “过滤”可以显示特定的用户会话或用户会话中特定的部分。允许输入通配符。

单击 “刷新”按钮可以更新用户会话的显示。

终止会话

拥有适当权限的管理员可以随时终止用户会话。为此，请执行以下步骤：

1. 选择要终止的用户会话。
2. 单击“终止”。

第 7 章

策略管理

本章介绍 Sun Java™ System Identity Server 2004Q2 的 “策略管理”功能。Identity Server 的 “策略管理”功能可提供进行以下操作的方法：使顶级管理员或顶级策略管理员可以查看、创建、删除和修改在所有组织上均可使用的某项特定服务的策略。它还为组织或子组织管理员或策略管理员提供了用于查看、创建、删除和修改组织专用策略的方法。

本章包含以下内容：

概述

*策略*定义了若干规则，这些规则将指定对某一组织受保护资源的访问权限。企业拥有需要进行保护、管理和监控的资源、应用程序和服务。策略定义了用户可对给定资源执行操作的时间和方式，以此来控制对上述资源的访问权限和使用情况。策略在被应用于对象后，它将定义某特定对象可访问的资源。

注 对象为主用户。*主用户*可以是单个用户、公司、角色或组等具有某种身份的任何对象。有关详细信息，参见 Java™ 2 Platform Standard Edition Javadoc。

单个策略既可定义二元决策，也可定义非二元决策。二元决策是 *yes*/*no*、*true*/*false* 或 *allow*/*deny*。非二元决策表示属性的值。例如，邮件服务可能包括 mailboxQuota 属性，其中带有为每个用户设置的最大存储值。通常，配置后的策略将定义对象可对哪一资源以及在何种条件下能够执行的具体操作。

策略管理功能

“策略管理”功能提供了用于创建和管理策略的*策略服务*。策略服务允许管理员定义、修改、授予、撤消和删除用于在 Identity Server 部署内保护资源的权限。通常，策略服务包括一个数据存储库、一个允许创建、管理和评估策略的界面库以及一个策略执行程序或*策略代理*。 Identity Server 使用 Sun Java System Directory Server 进行数据存储，并提供 Java 和用于策略评估和策略服务定制的 C API。（有关详细信息，参见 《*Identity Server Developer's Guide*》）它还允许管理员使用 Identity Server 控制台进行策略管理。 Identity Server 提供一种策略服务，即“URL 策略代理”服务，该服务使用可下载策略代理来强制实施策略。

URL 策略代理服务

Identity Server 以标准方式提供 “URL 策略代理”服务以强制执行策略。此服务允许管理员借助于策略执行程序或*策略代理*创建和管理策略。

策略代理

“策略代理”是存储企业资源的服务器的 “策略强制点” (PEP)。策略代理独立于 Identity Server 而被安装在一个 Web 服务器上，当用户向位于受保护 Web 服务器上的 Web 资源发出请求时，此代理将起到附加授权步骤的作用。此授权是对资源执行的任何用户授权请求的补充。该代理可保护 Web 服务器，而资源反过来又会受到授权插件的保护。

例如，受远程安装的 Identity Server 保护的“人力资源”Web 服务器上可能会安装某一代理。此代理可防止无适当策略的人员查看保密的工资信息或其他敏感数据。策略由 Identity Server 管理员定义，存储在 Identity Server 部署中，并由策略代理使用，以允许或拒绝用户对远程 Web 服务器内容的访问权。

最新的 “Sun Java System Identity Server 策略代理”可以从 Sun Microsystems 下载中心下载。

有关安装和管理策略代理的详细信息，可在 *Sun Java System Identity Server J2EE Policy Agents Guide* 或 *Web Policy Agents Guide* 中找到。

注 策略评估不会按特定顺序进行，尽管在对其进行评估时，如果一个操作值评估结果为 *deny*，也不再对后续策略进行评估，除非在策略配置服务中启用 “ 拒绝决策时继续评估”属性。有关详细信息，参见第 317 页的 “策略配置服务属性”。

策略代理只在 Web URL (http://...) 上强制执行决策。但是，可以使用 Java 和 C Policy Evaluation API 编写代理，以在其他资源上强制执行策略。

此外，还需要将 “策略配置服务”中的 “资源比较器”属性由其默认配置更改为：

serviceType=*Name_of_LDAPService*|class=com.sun.identity.policy.plugins.SuffixResourceName|wildcard=*|delimiter=,|caseSensitive=false

或者，提供类似于 LDAPResourceName 的实现以实现 com.sun.identity.policy.interfaces.ResourceName 并相应地配置 “资源比较器”也可达到目的。

注 “资源比较器”属性的字段将在第 317 页的 “策略配置服务属性”中说明。

策略代理过程

当 Web 浏览器向驻留于策略代理所保护的服务器中的 URL 发出请求后，即开始受保护 Web 资源的过程。服务器中已安装的策略代理会截取请求并检查现有的验证凭证 （会话标记）。

如果代理已截取请求并验证了现有的会话标记，随后将发生以下过程。

1. 如果会话标记有效，则允许或拒绝用户的访问。如果会话标记无效，则用户将被重定向到 “验证服务”，如下列各步骤所述。
2. “验证服务”会检验凭证是否同样有效，并发放一个标记。
3. 一旦用户的凭证经过正确验证，代理就会向 “命名服务”发出请求，该服务定义用于访问 Identity Server 内部服务的 URL。
4. “命名服务”返回策略服务的定位符，代理则向 “策略服务”发出请求以获取适用于该用户的决策。
5. 是允许用户访问还是拒绝用户访问，需根据当前访问资源的策略决策而定。如果对策略决策的建议指示出不同的验证级别或验证机制，代理会将请求重定向到 “验证服务”，直到所有条件都经过验证为止。

假设代理截取了某一请求，而对于该请求不存在任何现有会话标记，则代理将用户重定向到其默认登录页面，即使用不同验证方法保护资源也是如此。

注 基于策略的资源验证和用户验证属于不同类型的验证。有关此方面内容的详细信息，参见第 140 页的 “基于策略的资源管理”。

策略类型

使用 Identity Server 可以配置两种类型的策略：*标准*策略和*引用策略*。标准策略由*规则*、*主题*和*条件*组成。引用策略由*规则*和*到组织的引用*组成。

标准策略

在 Identity Server 中，用于定义访问权限的策略被称为*标准*策略。*标准*策略由*规则*、*主题*和*条件*组成。

规则

一条*规则*包含一个资源、一项或多项操作以及一个值。规则大体上对策略进行了定义。

- *资源*定义受保护的特定对象，例如 HTML 页或使用人力资源服务访问的用户工资信息。
- *操作*是可对资源执行的操作的名称， Web 服务器操作的示例是 POST 或 GET。人力资源服务允许的操作可能是 canChangeHomeTelephone。
- *值*定义操作的权限，例如，允许或拒绝。

注 允许定义不带资源的操作。

主题

*主题*定义受策略影响的用户或用户集合 （例如，组或担任特定角色的那些用户）。主题将被分配给策略。主题的一般规则是：仅当用户是策略中至少一个主题的成员时策略才适用。默认主题包括：

- 已验证用户
- Identity Server 角色
- LDAP 组
- LDAP 角色
- LDAP 用户

- 组织
- Web 服务客户机

Identity Server 角色与 LDAP 角色

Identity Server 角色是用 Identity Server 创建的。这些角色所具有的对象类由 Identity Server 进行授权。LDAP 角色是使用 Directory Server 角色功能的任意角色定义。这些角色所具有的对象类由 Directory Server 角色定义进行授权。所有 Identity Server 角色都可用作 Directory Server 角色。但是， Directory Server 角色并不一定都是 Identity Server 角色。可通过配置 “策略配置服务”从现有目录利用 LDAP 角色。Identity Server 角色只能通过托管“Identity Server 策略服务”访问。Identity Server 策略服务访问 Identity Server SDK 和缓存时，在 Identity Server 角色中评估成员资格的速度较快。可以在策略配置服务中修改 LDAP 角色搜索过滤器以缩小范围并提高性能。

嵌套角色

嵌套角色可作为策略定义主题中的 “LDAP 角色”正确评估。

条件

您可以使用 “条件”定义策略的限制条件。例如，为某个薪金应用程序定义策略时，可以为该操作定义一个条件，限定只能在特定的时间内访问该应用程序。另外，您还可以定义另一种条件，限定只有当请求是来自指定的一组 IP 地址或公司内部网时才允许执行该操作。

此外，条件还可以用于配置同一个域的不同 URI 上的不同策略。例如，`http://org.example.com/hr/*jsp` 只能由 `org.example.net` 在 9 AM 到 5 PM 之间进行访问，而 `http://org.example.com/finance/*.jsp` 可以由 `org.example2.net` 在 5 AM 到 11 PM 之间进行访问。同时使用 “IP 条件”和“时间条件”就可以实现这一目的。将规则的资源指定为 `http://org.example.com/hr/*.jsp`，策略将应用到 `http://org.example.com/hr` 下的所有 JSP，包括子目录中的 JSP。

注 候选组织、规则、资源、主题、条件、操作和值等术语分别对应 `policy.dtd` 中的 *Referral*、 *Rule*、 *ResourceName*、 *Subject*、 *Condition*、 *Attribute* 和 *Value* 元素。

引用策略

管理员可能需要将一个组织的策略定义和决策指派给另一个组织。（另外，还可以将资源的策略决策指派给其他策略产品。）*引用策略*控制着对策略创建和评估的授权。该策略由一个或多个*规则*和*候选组织*组成。

规则

规则定义策略定义和评估相关的资源。

候选组织

候选组织定义当前与策略评估相关的组织。默认情况下，有两种候选组织类型：对等组织和子组织。它们分别代表同级组织和子级组织。有关详细信息，参见第 128 页的 “为对等组织和子组织创建策略”。

注 相关组织只能为那些已相关的资源 （或子资源）定义或评估策略。但是，该限制不适用于根组织。

策略定义类型文档

一旦创建并配置了策略，它就会以 XML 形式存储在 Directory Server 中。在 Directory Server 中， XML 编码的数据存储在一个位置。尽管策略是用 amadmin.dtd （或控制台）定义和配置的，但实际上它以基于 policy.dtd 的 XML 的形式存储在 Directory Server 中。 policy.dtd 包含从 amadmin.dtd （无策略创建标记）中提取的策略元素标记。因此，“策略服务”从 Directory Server 加载策略时，它将根据 policy.dtd 分析 XML。只有在使用命令行创建策略时，才使用 amadmin.dtd。本节介绍 `policy.dtd` 的结构。 policy.dtd 位于以下位置：

IdentityServer_base`/SUNWam/dtd (Solairs)`

IdentityServer_base`/identity,dtd (Linux)`

注 在本章中的余下部分将只给出 Solaris 目录信息。请注意 Linux 的目录结构有所不同。有关详细信息，请参见第 19 页的 “关于本指南”。

Policy 元素

Policy 是根元素，它定义策略的权限或*规则*以及规则所适用的对象或*主题*。它还定义该策略是否为 *候选*（指派）策略以及是否对该策略存在限制 （或*条件*）。它可能包含一个或多个下列子元素：*Rule*、*Conditions*、*Subjects* 或 *Referrals*。必需的 XML 属性为 name，它指定策略的名称。属性 referralPolicy 指明策略是否为引用策略；如果未定义，则它默认为标准策略。可选 XML 属性包括 *name* 和 *description*。

注 将策略标记为 *referral* 时，在策略评估期间将忽略主题和条件。相反，将策略标记为 *normal* 时，在策略评估期间将忽略所有 “候选组织”。

Rule 元素

Rule 元素定义策略的具体内容，可能包含三个子元素：*ServiceName*、*ResourceName* 或 *AttributeValuePair*。它定义已经为其创建策略的服务或应用程序的类型以及资源名称和对其执行的操作。定义规则时可不带任何操作；例如，引用策略就不含任何操作。

注 已定义的策略也可以不包括定义的 *ResourceName* 元素。

ServiceName 元素

ServiceName 元素定义策略所适用的服务名称。此元素表示服务类型。它不包含任何其他元素。其值与在服务的 XML 文件 （基于 sms.dtd）中定义的完全一致。*ServiceName* 元素的 XML 服务属性是服务 （取字符串的值）的名称。

ResourceName 元素

ResourceName 元素定义将要对其执行操作的对象。策略已经过专门配置以便保护此对象。它不包含任何其他元素。 *ResourceName* 元素的 XML 服务属性是对象的名称。 *ResourceName* 的示例可能是 Web 服务器上的 http://www.sunone.com:8080/images 或目录服务器上的 ldap://sunone.com:389/dc=example,dc=com。更具体的资源可能是 salary://uid=jsmith,ou=people,dc=example,dc=com，其中被操作的对象是 John Smith 的工资信息。

AttributeValuePair 元素

AttributeValuePair 元素定义操作及其值。它被用作 *"Subject 元素"*、*"Referral 元素"* 和 *"Condition 元素"* 的子元素。它包含 *Attribute* 和 *Value* 元素，但不包含 XML 服务属性。

Attribute 元素

Attribute 元素定义操作的名称。操作是针对资源所执行的操作或事件。 POST 或 GET 是对 Web 服务器资源执行的操作， READ 或 SEARCH 是对目录服务器资源执行的操作。 *Attribute* 元素必须与 *Value* 元素组对。 *Attribute* 元素本身不包含任何其他元素。 *Attribute* 元素的 XML 服务属性是操作的名称。

Value 元素

Value 元素定义操作值。 allow/deny 或 yes/no 是操作值的示例。其他操作值可以是布尔值、数字或字符串。这些值在服务的 XML 文件 （基于 sms.dtd）中定义。 *Value* 元素不包含任何其他元素，也不包含任何 XML 服务属性。

警告 拒绝规则始终优先于允许规则。例如，如果一个策略拒绝访问而另一个策略允许访问，则结果将为拒绝 （假定两个策略的所有其他条件都满足）。建议谨慎使用拒绝策略，因为它们会导致潜在冲突。如果采用显式拒绝规则，则通过不同主题 （如角色和 / 或组成员资格）指定给某一用户的策略可能导致拒绝的访问。通常，策略定义过程应只使用允许规则。当未应用其他任何策略时，才可使用默认拒绝。

Subjects 元素

Subjects 子元素确定策略所适用的对象集合；选择此概述集合的根据是组中的成员资格、角色所有权或个别用户。它接受 *Subject* 子元素。可以定义的 XML 属性有：

name。它定义集合的名称。

description。它定义主题的说明。

includeType。当前未使用此项。

Subject 元素

Subject 子元素确定策略所适用的对象集合；此集合可从 Subjects 元素所定义的集合中准确找出更具体的对象。成员资格可基于角色、组成员资格或仅仅基于个别用户的列表。它包含子元素 “AttributeValuePair 元素”。必需 XML 属性是 `type`，它确定一个通用的对象集合，具体定义的主题从该集合中提取。其他 XML 属性包括定义集合名称的 name 和 includeType，后者规定集合是否如定义的那样，用于确定策略是否应用于 “不”属于该主题成员的用户。

注 定义了多个主题时，要使策略得以应用，至少要有一个主题应该应用于用户。当使用 includeType（被设置为 false）定义主题时，用户不应是该主题的成员。

Referrals 元素

Referrals 子元素确定策略候选组织的集合。它接受 *Referral* 子元素。定义该因素时可使用的 XML 属性有定义集合名称的 name 和包含说明的 description。

Referral 元素

Referral 子元素确定特定的策略候选组织。它接受子元素 “AttributeValuePair 元素”。必需的 XML 属性是 type，它确定一个通用的任务集合，具体定义的候选组织从该集合中提取。它也可包括用于定义集合名称的 name 属性。

Conditions 元素

Conditions 子元素确定策略限制 （时间范围、验证级别等）的集合。它必须包含一个或多个 *Condition* 子元素。定义该因素时可使用的 XML 属性有定义集合名称的 name 和包含说明的 description。

注 条件元素是策略中的可选元素。

Condition 元素

Condition 子元素确定具体的策略限制 （时间范围、验证级别等）。它接受子元素 “AttributeValuePair 元素”。它必需的 XML 属性是 type，该属性确定一个通用的限制集合，具体定义的条件从该集合中提取。它也可包括用于定义集合名称的 name 属性。

添加策略服务

默认情况下， Identity Server 将提供 “URL 策略代理”服务 (`iPlanetAMWebAgentService`)。此服务在位于以下目录的 XML 文件中定义：

```
etc/opt/SUNWam/config/xml/
```

但是，您可以向 Identity Server 添加附加的策略服务。一旦创建了策略服务，就可通过命令行实用程序 `amadmin` 将其添加到 Identity Server。

添加新策略服务

1. 在基于 sms.dtd 的 XML 文件中开发新策略服务。Identity Server 提供了两个策略服务 XML 文件，用户可能希望将其用作新策略服务文件的基础：

   amWebAgent.xml - 这是默认 “URL 策略代理”服务的 XML 文件。它位于 etc/opt/SUNWam/config/xml/。

   SampleWebService.xml - 这是示例策略服务文件，它位于 etc/opt/SUNWam/samples/policy。

2. 将该 XML 文件保存到您将从中加载新策略服务的目录。例如：

   etc/opt/SUNWam/config/xml/newPolicyService.xml

3. 使用 amadmin 命令行实用程序加载新策略服务。例如：

   IdentityServer_base/SUNWam/bin/amadmin

   --runasdn "uid=amAdmin,ou=People,*default_org*,*root_suffix*

   --password *password*

   --schema etc/opt/SUNWam/config/xml/newPolicyService.xml

4. 加载新策略服务之后，可通过 Identity Server 控制台或使用 amadmin 加载新策略来制定策略定义的规则。

创建策略

您可以通过策略 API 和 Identity Server 控制台创建、修改和删除策略，并通过 amadmin 命令行工具创建和删除策略。本节重点介绍如何通过 amadmin 命令行实用程序和 Identity Server 控制台创建策略。有关策略 API 的详细信息，参见《*Identity Server Developer's Guide*》。

策略通常通过 XML 文件创建，再通过命令行实用程序 amadmin 添加到 Identity Server，然后使用 Identity Server 控制台进行管理 （尽管策略可通过控制台创建）。这是因为不能直接使用 amadmin 修改策略。要修改策略，必须先从 Identity Server 中删除该策略，然后使用 amadmin 添加已修改的策略。

通常在组织 （或子组织）级创建策略，并应用于该组织的整个树结构。

使用 amadmin 创建策略

1. 创建基于 policy.dtd 的策略 XML 文件。该文件位于以下目录：

   IdentityServer_base/SUNWam/dtd

2. 策略的 XML 文件生成之后，便可使用以下命令加载它：

IdentityServer_base/SUNWam/bin/amadmin

   --runasdn "uid=amAdmin,ou=People,*default_org*,*root_suffix*"

   --password *password*

   --data *policy.xml*

要同时添加多个策略，请将这些策略放在一个 XML 文件中，而不是在每个 XML 文件中放一个策略。如果一连串使用多个 XML 文件装入策略，则可能会损坏内部策略索引，并且某些策略可能不会参与策略评估。

通过 amadmin 创建策略时，确保在创建验证模式条件时向组织注册验证模块；确保在创建组织主题、 LDAP 组主题、 LDAP 角色主题和 LDAP 用户主题时，存在相应的 LDAP 对象 （组织、组、角色和用户）；确保在创建 IdentityServerRoles 主题时，存在 Identity Server 角色；确保在创建子组织或对等组织推荐时，存在相关的组织。

请注意， SubOrgReferral、 PeerOrgReferral、 Organization 主题、 IdentityServerRoles 主题、 LDAPGroups 主题、 LDAPRoles 主题和 LDAPUsers 主题中的值元素的文本中需要使用完整 DN。

使用 Identity Server 控制台创建策略

1. 找到 “身份管理”界面。

2. 选择要为其创建策略的组织。

   确保 “策略管理”窗口正确地显示了您的组织。

3. 从 “查看”菜单中选择 “策略”。

   默认情况下，“组织”视图会显示在 “查看”菜单中。如果存在子组织，则在组织下面还可以看到配置的所有子组织。如果为子组织创建策略，请选择子组织，然后从 “查看”菜单中选择 “策略”。

4. 单击浏览框中的 “新建”。屏幕上将显示 “新建策略”窗口。

5. 选择您要创建的策略类型：标准或候选组织。

   如果子组织没有相应的引用策略，则不能为该子组织创建任何策略。

   此时，您不必为标准或引用策略定义所有字段。您可以在创建策略之后再添加规则、主题、候选组织等字段。

6. 键入策略的名称，然后单击 “确定”。

7. 默认情况下，屏幕上将显示 “常规”视图。

   “常规”视图显示了策略的名称，且允许您输入所创建策略的说明。

8. 单击 “保存”完成策略的配置。

为对等组织和子组织创建策略

要为对等组织和子组织创建策略，首先必须在父组织 （或其他对等组织）中创建引用策略。另外，还应该注册策略配置服务并在子组织中创建模板。引用策略的规则定义中必须包含子组织所管理的资源前缀。一旦在父组织 （或其他对等组织）中创建了引用策略，就可以在子组织 （或对等组织）中创建标准策略。

在本示例中， `o=isp` 为父组织， `o=example.com` 为子组织并且管理 `http://www.example.com` 的资源和子资源。

为子组织创建策略

1. 在 o=isp 中创建引用策略。有关引用策略的信息，参见第 136 页的 “修改引用策略”过程。

   此引用策略必须将 http://www.example.com 定义为规则中的资源，并且必须包含一个以 example.com 作为候选组织中的值的 SubOrgReferral。

2. 转到 “组织”视图并找到子组织 example.com。

3. 确保在子组织级别 （即 example.com）上注册策略配置服务。有关信息，参见第 139 页的 “添加策略配置服务”。

4. 现在，已通过 isp 将资源指向了 sun.com，因此可为资源 http://www.example.com 或所有以 http://www.example.com 开头的资源创建标准策略。

   有关创建标准策略的信息，参见第 129 页的 “修改标准策略”过程。

   要为 example.com 所管理的其他资源定义策略，必须在 o=isp 上创建其他引用策略。

管理策略

一旦创建了标准或引用策略并将其添加到 Identity Server，您就可以使用 Identity Server 控制台通过修改规则、主题、条件和候选组织来管理策略。

修改标准策略

通过 “身份管理”界面，您可以创建用于定义访问权限的策略。此类策略称为*标准*策略。标准策略可由多个规则、主题和条件组成。本节列出并定义了您在创建标准策略时可以指定的默认字段。

修改规则

1. 从 “身份管理”界面的 “查看”菜单中选择 “策略”。

   屏幕上将显示为该组织创建的策略。

2. 选择您要修改的策略，然后单击属性箭头。数据框中将显示 “编辑策略”窗口。

   默认情况下，屏幕上将显示 “常规”视图。“常规”视图中所包含的属性在第 126 页的 “创建策略”中进行介绍。

3. 从 “查看”菜单中选择 “规则”，然后单击 “新建”。

   如果存在多个服务，这些服务会在 “数据”窗格中列出。选择要为其创建策略的服务，然后单击 “下一步”。随即将显示 “新建规则”窗口。

4. 在 “规则”的各个字段中定义资源、操作和操作值。这些字段包括：

   类型 。显示要创建策略的服务。默认值为 URL 策略代理。

   规则名称。输入规则的名称。

   资源名称。输入资源的名称。例如：

   `http://www.example.com`

   目前，策略代理只支持 `http://` 和 `https://` 资源，不支持代替主机名的 IP 地址。

   资源名称、端口号和协议都支持通配符。例如：

   `http*://*:*/*.html`

   对于 “URL 策略代理”服务，如果未输入端口号，则 `http://` 的默认端口号为 80， `https://` 的默认端口号为 443。

   要能够管理安装在某特定机器上的所有服务器的资源，可将资源定义为 http://host*:*。此外，还可以定义以下资源，以授予管理员对该组织中所有服务的组织权限：

   `http://*.subdomain.domain.topleveldomain`

   选择操作。对于 “URL 策略代理”服务，您可以选择以下两项默认操作或其中任何一项：

   - `GET`
   - `POST`

   选择操作值。对于 “URL 策略代理”服务，您可以选择下列任一操作值：

- Allow 允许您访问与规则中定义的资源相匹配的资源。
- Deny 拒绝您访问与规则中定义的资源相匹配的资源。

在策略中，拒绝规则始终比允许规则具有优先权。例如，如果某种给定的资源存在两个策略，一个拒绝访问而另一个允许访问，结果为拒绝访问（假定两个策略的条件都满足）。建议谨慎使用拒绝策略，因为它们会导致策略间的潜在冲突。通常来说，在定义策略的过程中，应只使用允许规则，在没有策略适用于实现拒绝条件时使用默认的拒绝规则。

当采用了显示拒绝规则时，即使一个或多个策略允许访问，通过多个不同主题（如角色和 / 或组成员资格）指定给给定用户的策略可能仍然会导致对资源的拒绝访问。例如，如果应用于员工角色的资源的策略为拒绝策略，而应用于经理角色的同一资源的策略为允许策略，则被指派了员工和经理两个角色的用户的策略决策将为拒绝。

解决此问题的一个方法是使用条件插件来设计策略。在上述情况下，将拒绝策略应用于通过员工角色验证的用户并将允许策略应用于通过经理角色验证的用户的“角色条件”可以帮助区分两种策略。另一个方法是使用验证级别条件，其中经理角色在更高验证级别进行验证。有关详细信息，参见第 134 页的“添加或修改条件”。

注 如果定义了服务，则操作不需要定义资源，因此不会显示资源字段。如果服务包括两种操作类型（某些操作需要资源，另一些操作则不需要资源），则系统会显示一个选项，让您选择操作需要资源的规则或操作不需要资源的规则。

5. 单击“完成”保存规则。此操作仅将配置保存在内存中。执行步骤 7 以完成该进程。
6. 重复执行步骤 1 至 5 以创建其他规则。

7. 为该策略创建的所有规则均显示在 “规则” 视图的表中。单击 “保存” 将规则添加到策略。

   要从策略中移除规则，请选择该规则，然后单击 “移除”。

   您可以通过单击规则名称旁边的 “编辑” 链接来编辑任何规则定义。

修改主题

1. 要定义策略的主题，请从 “查看” 菜单中选择 “主题”，然后单击 “新建”。
2. 选择以下任一默认主题类型：

   已验证用户。此主题类型表明任何具有有效 SSO 令牌的用户都是此主题的成员。

   Identity Server 角色。此主题类型表明任何使用 Identity Server 角色的成员都是此主题的成员。 Identity Server 角色是通过 Identity Server 创建的。这些角色具有通过 Identity Server 授权的对象类。 Identity Server 角色只能通过所属的 Identity Server 策略服务进行访问。

   LDAP 组。此主题类型表明 LDAP 组的任何成员都是此主题的成员。

   LDAP 角色。此主题类型表明任何使用 LDAP 角色的成员都是此主题的成员。 LDAP 角色是使用 Directory Server 角色功能的任意角色定义。这些角色具有通过 Directory Server 角色定义授权的对象类。可以在策略配置服务中修改 LDAP 角色搜索过滤器以缩小范围并提高性能。

   LDAP 用户。此主题类型表明任何 LDAP 用户都是此主题的成员。

   组织。此主题类型表明任何组织的成员都是此主题的成员。

   Web 服务客户机。此主题类型表明，如果 SSOToken 中包含的主体的 DN 与此主题的任意选定值匹配，则该 SSOToken 所标识的 Web 服务客户机 (WSC) 是此主题的成员。有效值为本地 JKS 密钥库中的可信赖证书（对应于可信赖 WSC 证书）的 DN。此主题取决于特权 Web 服务框架，并且只能由特权服务提供商用来对 WSC 进行授权。

   确保您已在将此主题添加到策略之前创建了密钥库。有关设置密钥库的信息可在以下位置找到：

   IdentityServer_base/SUNWam/samples/saml/xmlsig/keytool.html

   单击 “下一步” 继续。
3. 输入主题的名称。

4. 选择或取消选择 “专用”字段。

   如果未选择该字段 （默认），策略将应用到属于该主题的成员的身份。如果选择该字段，策略将应用到不属于该主题的成员的身份。

   如果该策略中存在多个主题，至少要有一个主题表明该策略适用于给定的身份，策略才能应用到该身份。

5. 执行搜索以显示要添加到主题的身份。此步骤不适用于已验证用户主题。

   默认 (*) 搜索模式将显示所有符合条件的条目。

6. 选择要为主题添加的各个身份，或单击 “全部添加”一次添加所有身份。单击 “添加”将这些身份移至 “选择”列表框中。

7. 单击 “完成”。

8. 主题的名称、类型和专有状态显示在 “主题”视图的表中。单击 “保存”。

   要从策略中移除主题，请选择相应主题并单击 “删除”，然后单击 “保存”。

   您可以通过单击主题名称旁边的 “编辑”链接来编辑任何主题定义。

添加或修改条件

1. 从 “查看”菜单中选择 “条件”。单击 “新建”添加新的条件，或单击 “编辑”链接编辑现有的条件。

2. 选择以下默认条件之一：

   - 验证级别
   - 验证方案
   - IP 地址
   - LE 验证级别
   - 会话

- 时间

对于验证级别，如果用户的验证级别大于或等于条件中设置的验证级别，则应用该策略。对于 LE 验证级别，如果用户的验证级别小于或等于条件中设置的验证级别，则应用该策略。

3. 单击“下一步”。
4. 定义给定条件的值。这些字段包括：

名称。输入条件的名称。

验证级别

验证级别。指明验证的信任级别。验证级别和验证模块表格中显示了可用的验证级别。

验证方案

验证方案。在下拉菜单中选择条件的验证方案。这些验证方案取自组织验证模块中的核心服务模板。

IP 地址

起始 / 结束 IP 地址。指定 IP 地址的范围。

DNS 名称。指定 DNS 的名称。此字段可以是全限定主机名，也可以是采用下列格式之一的字符串：

域名

**.domainname*

时间

起始 / 结束日期。指定日期的范围。

时间。指定一天中的时间范围。

天。指定表示天数的范围。

时区。指定一个标准的或自定义的时区。自定义的时区只能是可由 Java 识别的时区 ID（例如， PST）。如果未指定值，默认值为 Identity Server JVM 中设置的时区。

会话

最长会话时间。指定应用策略的最长用户会话时间。

终止会话。如果选择该字段，当会话时间超过 “最长会话时间”字段中定义的最大允许时间时，系统将终止该用户会话。

5. 条件定义完毕后，请单击 “完成”。

   为该策略创建的所有条件均显示在 “条件”视图的表中。

6. 单击 “保存”。

   要从策略中移除条件，请选择该条件，然后单击 “删除”。

   您可以通过单击条件名称旁边的 “编辑”链接来编辑任何条件定义。

修改引用策略

通过 “身份管理”界面，您可以将一个组织的策略定义和决策指派给另一个组织。（您还可以将资源的策略决策授权给其他策略产品。）*引用策略*控制着对策略创建和评估的授权。它由*规则*和*候选组织*本身组成。

修改规则

1. 从 “查看”菜单中选择 “规则”。单击 “新建”添加新的规则，或单击 “编辑”链接编辑现有的规则。
2. 选择 “服务类型”。如果要创建新规则，请单击 “下一步”。
3. 在 “规则”字段中定义资源。这些字段包括：

   类型。显示可用于所创建策略的策略服务。

   规则名称。输入规则的名称。

   资源名称。输入资源的名称。例如：

`http://www.sunone.com`

目前，策略代理只支持 `http://` 和 `https://` 资源，不支持代替主机名的 IP 地址。

资源名称、端口号和协议都支持通配符。

对于 “URL 策略代理”服务，如果未输入端口号，则 `http://` 的默认端口号为 80， `https://` 的默认端口号为 443。

如果将资源定义为 `http://host*:*`，即可允许对安装在特定计算机上的所有服务器的资源进行管理。此外，还可以定义以下资源，以授予管理员对该组织中所有服务的组织权限：

`http://*.`*`subdomain.domain.topleveldomain*

4. 单击 “完成”。
5. 重复执行步骤 1 至 4 以创建其他规则。

   为该策略创建的所有规则均显示在 “规则”视图的表中。
6. 单击 “保存”。

   要从策略中移除规则，请选择该规则，然后单击 “删除”。

   您可以通过单击规则名称旁边的 “编辑”链接来编辑任何规则定义。

添加候选组织

1. 从 “查看”菜单中选择 “候选组织”。单击 “新建”添加新候选组织，或单击 “编辑”链接编辑现有候选组织。
2. 在 “规则”字段中定义资源。这些字段包括：

   候选组织。显示当前候选组织类型。

   名称。输入候选组织的名称。

   包含。指定将显示在 “值”字段中的组织名称的过滤器。默认情况下，该字段将显示所有组织名称。

   值。选择该候选组织的组织名称。

3. 依次单击 “确定”和 “保存”。

   要从策略中移除候选组织，请选择该候选组织，然后单击 “删除”。

   您可以通过单击候选组织名称旁边的 “编辑”链接来编辑任何候选组织定义。

策略配置服务

策略配置服务用于通过 Identity Server 控制台为每个组织配置与策略相关的属性。也可定义用于 Identity Server 验证服务的资源名称实现和 Directory Server 数据库。

缓存主题评估

为了提高策略评估的性能，主题评估将被缓存若干分钟的一段时间，具体时间长短如策略配置服务中的 “主题结果的生存时间”属性定义。在达到 “主题结果的生存时间”属性中所定义的时间之前，将持续引用这些缓存的策略决策。一旦达到该时间，下次评估策略时，其决策将反映用户的已更改状态 （如果适用），例如，已从组中移除该用户。

amldapuser 定义

amldapuser 是在安装过程中创建的用户，用于在 LDAP 和成员资格验证期间绑定和搜索 Directory Server。它也用于策略配置服务。一旦将 LDAP、成员资格或策略配置服务注册到组织，就必须输入此用户 （在安装过程中配置）的口令。有关详细信息，参见 《*Sun Java System Identity Server Migration Guide*》。

添加策略配置服务

添加策略配置服务与添加其他任何类型的服务一样，只不过它是在 “身份管理” 界面中完成的。默认情况下，系统会自动将策略配置服务添加至顶级组织。必须将所创建的任何策略服务添加至所有组织。无论何时添加策略配置服务，均必须在模板中输入 LDAP 绑定口令。

添加策略配置服务

1. 找到 “身份管理” 界面。

   在打开控制台时，默认界面是 “身份管理”。

2. 选择要为其创建策略的组织。

   如果以顶层管理员身份登录，请确保 “身份管理” 模块位于顶层组织，在此可以看到所有配置的组织。默认顶层组织是在安装过程中定义的。

3. 从 “查看” 菜单中选择 “服务”。

   如果组织已具有注册的服务，浏览框中将显示这些注册的服务。

4. 单击浏览框中的 “添加”。

   数据框中将显示尚未向该组织注册的服务列表。

5. 在数据框中打开的 “添加服务” 窗口中，选择 “策略配置”，然后单击 “确定”。

   “策略配置服务” 会添加到浏览框的服务列表中。

6. 单击属性箭头可配置策略服务。

   a. 如果尚未配置策略模板，则需为新注册的策略服务创建服务模板。

   b. 要配置策略服务，请单击 “创建”。

   c. 修改策略配置属性。有关这些属性的说明，参见第 317 页的 “策略配置服务属性”。

7. 单击“保存”。

   现在已向所选组织添加了策略配置服务。

注 子组织必须注册自己的策略服务，这与父组织无关。换言之，子组织 o=suborg,dc=sun,dc=com 不能从父组织 dc=sun,dc=com 处继承策略配置服务。

基于策略的资源管理

某些组织需要高级验证方案，其中用户将根据他们尝试要访问的资源用特定模块进行验证。基于策略的资源管理是 Identity Server 的一种功能，其中用户在访问 Web 资源时不需要传递其默认验证模块。

限制

基于策略的资源管理具有以下限制：

1. 适用于资源的所有策略都需要相同的验证模式或验证级别。例如，如果在针对 LDAP 验证模块的策略中定义了 abc.html，就不能在针对基于证书的验证模块的策略中再对其进行定义。
2. 级别和模式是可为此策略定义的仅有的两个条件。
3. 此功能在不同的 DNS 域中不起作用。

配置基于策略的资源管理

一旦安装了 Identity Server 与策略代理，即可配置基于策略的资源管理。为此，必须将 Identity Server 指向网关 servlet。

1. 打开 AMAgent.properties。

   AMAgent.properties 可在 /etc/opt//SUNWam/agents/config/ 中找到 （在 Solaris 环境中）。

2. 注释掉以下行：

   #com.sun.am.policy.am.loginURL = http://identity_server_host.domain_name:port/amserver/UI/Login。

3. 在文件中添加以下行：

   com.sun.am.policy.am.loginURL = http://identity_server_host.domain_name:port/amserver/gateway

4. 重新启动代理。

第 8 章

验证选项

Sun Java™ System Identity Server 2004Q2 提供了一个验证 （验证在企业内部访问应用程序的用户的身份的进程）的框架。在访问 Identity Server 控制台或任何其他受 Identity Server 保护的资源之前，用户必须通过验证进程。验证是通过验证用户身份的插件来实现的。（在 《*Identity Server Developer's Guide*》中对此插件体系结构进行了更为全面的介绍。）

Identity Server 控制台用于设置默认值、添加验证服务、创建验证模板以及启用服务。本章概括介绍了验证服务并提供了添加这些验证服务的操作说明。本章包含以下内容：

核心验证

默认情况下，除了核心验证服务以外， Identity Server 还提供了十一项不同的验证服务。核心验证服务为验证服务提供总体配置。在添加和启用匿名、基于证书、HTTP Basic、LDAP、成员资格、NT、RADIUS、SafeWord、SecurID、Windows 桌面 SSO 及 Unix 验证之前，必须先添加和启用核心验证。系统会自动为默认组织启用核心及 LDAP 验证服务。第 20 章 “核心验证属性”中包含核心属性的详细列表。

添加和启用核心服务

1. 转到要为其添加核心服务的组织。
2. 从 “查看”菜单中选择 “服务”。
3. 在 “浏览”窗格中单击 “添加”。

   此时 “数据”窗格中会显示可用服务列表。
4. 选中核心验证的复选框并单击 “添加”。

   核心验证服务将显示在 “浏览”窗格中，向管理员证实已添加了该服务。
5. 单击核心验证的属性箭头。

   数据窗格中将显示消息 “*当前不存在用于该服务的模板。要现在创建一个模板吗？*”。

6. 单击 “创建”。

   “数据”窗格中将显示核心属性。根据需要修改这些属性。您可以在第 20 章 “核心验证属性”中，或通过单击控制台右上角的 “帮助”链接找到有关核心属性的说明。

匿名验证

默认情况下，如果启用了此模块，用户可以以匿名用户身份登录到 Identity Server 中。还可以通过配置有效匿名用户列表属性为此模块定义匿名用户的列表 （参见第 233）。允许匿名访问意味着无需提供口令即可访问该服务器。可以将匿名访问限于特定的访问类型 （例如，读取访问或搜索访问）或者限于目录中的特定子树或单个条目。

添加和启用匿名验证

您必须以组织管理员或顶层管理员身份登录到 Identity Server 中。

1. 转到要为其添加匿名验证的组织。
2. 从 “查看”菜单中选择 “服务”。

   如果已添加，“核心”服务会显示在 “浏览”窗格中。如果该服务尚未添加，可以与匿名验证服务一同添加。

3. 在 “浏览”窗格中单击 “添加”。

   此时 “数据”窗格中会显示可用服务列表。

4. 选中匿名验证的复选框并单击 “添加”。

   匿名验证服务将显示在 “浏览”窗格中，向管理员证实已添加了该服务。

5. 单击匿名验证的属性箭头。

   数据窗格中将显示消息：*当前不存在用于该服务的模板。要现在创建一个模板吗？*

6. 单击 “创建”。

   “数据”窗格中将显示匿名验证属性。根据需要修改这些属性。您可以在第 18 章 “匿名验证属性”中，或通过单击控制台右上角的 “帮助”链接找到这些属性的说明。

7. 单击 “保存”。

   匿名验证服务已经启用。

使用匿名验证登录

为了使用匿名验证登录，必须修改核心验证服务属性 （第 246 页的 “组织验证模块”）以启用和选择匿名验证。这可以确保用户登录时使用 `http(s)://hostname:port/SERVER_DEPLOY_URI//UI/Login?module=Anonymous&org=org_name`。要在不使用 “匿名验证”登录窗口的情况下登录，请使用以下语法：

```
http(s)://hostname:port/SERVER_DEPLOY_URI//UI/Login?module=Anonymous
&org=org_name&Login.Token1=user_id
```

根据正在使用的验证类型 （例如服务、角色、用户和组织），如果将验证模块配置为默认模块，则无需在 URL 中指定模块名称。

注 匿名验证服务中的 “默认匿名用户名”属性值为 anonymous。这是用户登录时使用的名称。必须在组织中创建默认的匿名用户。用户 ID 应当与在匿名验证属性中指定的用户名相同。此项也可要求区分大小写。

基于证书的验证

基于证书的验证中使用个人数字证书 (PDC) 来识别和验证用户。可以将 PDC 配置为必须与 Directory Server 中存储的某个 PDC 相匹配，并且必须对照证书撤回列表进行检验。

在将基于证书的验证服务添加到组织之前，需要完成若干事项。首先，需要保护与 Identity Server 一起安装的 Web 容器，并将其配置为使用基于证书的验证。在启用基于证书的服务之前，请先参见 *Sun ONE Web Server 6.1 Administrator's Guide* 中的第 6 章 “Using Certificates and Keys”，以了解相应的初始 Web Server 配置步骤。可以在以下位置找到此文档：

```
http://docs.sun.com/db/prod/s1websrv#hic
```

或者，请参见 *Sun ONE Application Sever Administrator's Guide to Security*，其所在位置如下：

```
http://docs.sun.com/db/prod/s1appsrv#hic
```

注 每位将使用基于证书的服务进行验证的用户均必须为用户的浏览器请求一个 PDC。使用的浏览器不同，具体的说明也不同。有关详细信息，请参见您浏览器的文档。

添加和启用基于证书的验证

您必须以组织管理员身份登录到 Identity Server 中。

1. 转到要为其添加基于证书的验证的组织。
2. 从 “查看”菜单中选择 “服务”。

   如果已添加，“核心”服务会显示在 “浏览”窗格中。如果该服务尚未添加，可以与基于证书的验证服务一同添加。
3. 在 “浏览”窗格中单击 “添加”。

   此时 “数据”窗格中会显示可用服务列表。
4. 选中基于证书的验证的复选框并单击 “添加”。

   基于证书的验证服务将显示在 “浏览”窗格中，向管理员证实已添加了该服务。
5. 单击基于证书的验证的属性箭头。

   数据窗格中将显示消息：*当前不存在用于该服务的模板。要现在创建一个模板吗？*

6. 单击 “创建”。

   “数据”窗格中将显示基于证书的验证属性。根据需要修改这些属性。您可以在第 19 章 “证书验证属性”中，或通过单击控制台右上角的 “帮助”链接找到这些属性的说明。

7. 单击 “保存”。

在平台服务器列表中为基于证书的验证添加服务器 URL

为了添加此服务，您必须以组织管理员身份登录到 Identity Server，为 SSL 配置 Identity Server 和 Web 容器并且启用客户机验证。有关详细信息，参见第 57 页的 “在 SSL 模式中配置 Identity Server”。

使用基于证书的验证登录

为了使基于证书的验证成为默认验证方法，必须修改核心验证服务属性 “组织验证模块”（参见第 246）。这可以确保当用户使用

`http://hostname:port/deploy_URI/UI/Login?module=Cert` 登录时，将看到 “基于证书的验证”登录窗口。根据正在使用的验证类型 （例如角色、用户和组织），如果将验证模块配置为默认模块，则无需在 URL 中指定模块名称。

HTTP Basic 验证

该模块使用基本验证，它是 HTTP 协议内置的验证支持。 Web server 发出对用户名和口令的客户机请求，并将这些信息作为已验证的请求的一部分发送回服务器。Identity Server 将检索用户名和口令，然后在 LDAP 验证模块中内部验证该用户。为使 HTTP Basic 正常工作，还必须添加 LDAP 验证模块 （只添加 HTTP Basic 模块将无法正常工作）。有关详细信息，请参见第 150 页的 “添加和启用 LDAP 验证”。用户成功进行验证后，他 / 她将可以在不提供用户名和口令的情况下重新进行验证。

添加和启用 HTTP Basic 验证

您必须以组织管理员或顶层管理员身份登录到 Identity Server，而且必须已经注册 LDAP 验证服务。

1. 转到要为其添加 HTTP Basic 验证的组织。
2. 从 “查看” 菜单中选择 “服务”。

   如果已添加，“核心” 服务会显示在 “浏览” 窗格中。如果该服务尚未添加，可以与 HTTP Basic 验证服务一同添加。
3. 在 “浏览” 窗格中单击 “添加”。

   此时 “数据” 窗格中会显示可用服务列表。
4. 选中 HTTP Basic 验证的复选框并单击 “添加”。

   HTTP Basic 验证服务将显示在 “浏览” 窗格中，向管理员证实已添加了该服务。
5. 单击 HTTP Basic 验证的属性箭头。

   数据窗格中将显示消息：*当前不存在用于该服务的模板。要现在创建一个模板吗？*
6. 单击 “创建”。

   “数据” 窗格中将显示 HTTP Basic 验证属性。根据需要修改这些属性。您可以在第 21 章 “HTTP Basic 验证属性”中，或通过单击控制台右上角的 “帮助” 链接找到这些属性的说明。
7. 单击 “保存”。

   HTTP Basic 验证服务已经启用。

使用 HTTP Basic 验证登录

为了使用 LDAP 验证登录，必须修改核心验证服务属性 （第 246 页的 “组织验证模块”）以启用和选择 HTTP Basic 验证。这可以确保当用户使用 `http://hostname:port/server_deploy_URI/UI/Login?module=HTTPBasic` 登录时，将看到验证登录窗口。根据正在使用的验证类型 （例如服务、角色、用户和组织），如果将验证模块配置为默认模块，则无需在 URL 中指定模块名称。如果验证失败，将打开新的实例，用户将再次登录。要在使用 HTTP Basic 验证后彻底注销，必须关闭所有现有的浏览器实例，并启动新的浏览器实例。

LDAP 目录验证

在 LDAP 验证服务中，用户登录时需要使用特定的用户 DN 和口令绑定到 LDAP Directory Server 上。这是所有基于组织的验证的默认验证模块。如果用户提供的用户 ID 和口令在 Directory Server 中存在，则允许用户访问并为其创建一个有效的 Identity Server 会话。系统会自动为默认组织启用核心及 LDAP 验证服务。万一该服务被禁用，请参考下面所提供的操作说明。

添加和启用 LDAP 验证

您必须以组织管理员或顶层管理员身份登录到 Identity Server 中。

1. 转到要为其添加 LDAP 验证的组织。
2. 从 “查看” 菜单中选择 “服务”。

   如果已添加，“核心” 服务会显示在 “浏览” 窗格中。如果该服务尚未添加，可以与 LDAP 验证服务一同添加。
3. 在 “浏览” 窗格中单击 “添加”。

   此时 “数据” 窗格中会显示可用服务列表。

4. 选中 LDAP 验证的复选框并单击 “添加”。

   LDAP 验证服务将显示在 “浏览”窗格中，向管理员证实已添加了该服务。

5. 单击 LDAP 验证的属性箭头。

   数据窗格中将显示消息：*当前不存在用于该服务的模板。要现在创建一个模板吗？*

6. 单击 “创建”。

   “数据”窗格中将显示 LDAP 验证属性。根据需要修改这些属性。您可以在第 22 章 “LDAP 验证属性”中，或通过单击控制台右上角的 “帮助”链接找到这些属性的说明。

7. 在 “用户绑定的口令”属性中输入口令。默认情况下，安装过程中输入的 `amldapuser` 口令将用作绑定用户。如果您的 Directory Server 允许通过匿名访问来读取用户条目，则可跳过此步骤。

   要使用其他绑定用户，请在 “超级用户绑定的 DN”属性中更改用户的 DN，并在 “超级用户绑定的口令”属性中输入该用户的口令。

8. 单击 “保存”。

   LDAP 验证服务已经启用。

使用 LDAP 验证登录

为了使用 LDAP 验证登录，必须修改核心验证服务属性 （第 246 页的 “组织验证模块”）以启用和选择 LDAP 验证。这可以确保当用户使用 `http://`*`hostname:port`*`/server_`*`deploy_URI`*`/UI/Login?module=LDAP` 登录时，将看到 “LDAP 验证”登录窗口。根据正在使用的验证类型 （例如服务、角色、用户和组织），如果将验证模块配置为默认模块，则无需在 URL 中指定模块名称。

启用 LDAP 验证故障转移

LDAP 验证属性包括主 Directory Server 和辅助 Directory Server 的值字段。如果主服务器不可用，则 Identity Server 将转向辅助服务器进行验证。有关详细信息，参见 LDAP 属性第 258 页的 “主 LDAP 服务器”和第 258 页的 “辅助 LDAP 服务器”。

多个 LDAP 配置

管理员可以在一个组织下定义多个 LDAP 配置，作为故障转移的形式或者在 Identity Server 控制台只提供一个值字段时为一个属性配置多个值。尽管这些附加配置无法通过控制台查看，但如果未找到对于请求用户的授权的初始搜索，这些配置将与主配置一起发挥作用。有关多 LDAP 配置的信息，参见 《*Identity Server Developer's Guide*》中的 “Multi LDAP Configuration”。

成员资格验证

成员资格验证的实现类似与个性化站点，例如 `my.site.com` 或 `mysun.sun.com`。启用了此服务后，用户可以创建帐户并对其进行个性化，而无需管理员的帮助。利用这个新帐户，用户可以作为已添加的用户来访问该服务。用户还可以访问作为授权数据和用户首选项保存在用户配置文件数据库中的查看器界面。

添加和启用成员资格验证

您必须以组织管理员或顶层管理员身份登录到 Identity Server 中。

1. 转到要为其添加成员资格验证的组织。
2. 从 “查看”菜单中选择 “服务”。

   如果已添加，“核心”服务会显示在 “浏览”窗格中。如果该服务尚未添加，可以与成员资格验证服务一同添加。

3. 在 “浏览”窗格中单击 “添加”。

   此时 “数据”窗格中会显示可用服务列表。

4. 选中成员资格验证的复选框并单击 “添加”。

   成员资格验证服务将显示在 “浏览”窗格中，向管理员证实已添加了该服务。

5. 单击成员资格验证的属性箭头。

   数据窗格中将显示消息：*当前不存在用于该服务的模板。要现在创建一个模板吗？*

6. 单击 “创建”。

   “数据”窗格中将显示成员资格验证属性。根据需要修改这些属性。您可以在第 23 章 “成员资格验证属性”中，或通过选择控制台右上角的 “帮助”链接找到这些属性的说明。

7. 在 “超级用户绑定的口令”属性中输入口令。默认情况下，安装过程中输入的 `amldapuser` 口令将用作绑定用户。

   要使用其他绑定用户，请在 “超级用户绑定的 DN”属性中更改用户的 DN，并在 “超级用户绑定的口令”属性中输入该用户的口令。

8. 单击 “保存”。

   成员资格验证服务已经启用。

使用成员资格验证登录

为了使用成员资格验证登录，必须修改核心验证服务属性 （第 246 页的 “组织验证模块”）以启用和选择成员资格验证。这可以确保当用户使用 `http://`*`hostname:port/deploy_URI`*`/UI/Login?module=Membership` （注意区分大小写）登录时，将看到 “成员资格验证”登录 （自注册）窗口。根据正在使用的验证类型 （例如服务、角色、用户和组织），如果将验证模块配置为默认模块，则无需在 URL 中指定模块名称。

NT 验证

可以将 Identity Server 配置为与已安装的 NT/Windows 2000 服务器一起工作。Identity Server 提供了 NT 验证的客户机部分。只有 Solaris 平台上支持 NT 验证服务。

1. 配置 NT 服务器。有关详细说明，请参见 NT 服务器文档。
2. 必须先获得并在您的 Solaris 系统中安装与 Identity Server 进行通信的 Samba 客户机，才能添加和启用 NT 验证服务。有关详细信息，参见第 269 页的 “NT 验证属性”。
3. 添加和启用 NT 验证服务。

安装 Samba 客户机

要激活 NT 验证模块，必须下载 Samba Client 2.2.2 并将其安装到下面的目录：

```
IdentityServer_base/SUNWam/bin
```

Samba Client 是文件服务器和打印服务器，它将 Windows 计算机和 UNIX 计算机融合在一起而无需使用单独的 Windows NT/2000 服务器。有关该软件的详细信息及下载该软件，请访问 http://wwws.sun.com/software/download/products/3e3af224.html。

Red Hat Linux 随 Samba 客户机一起提供，它位于以下目录中：

```
/usr/bin
```

为了使用 Linux 的 NT 验证服务进行验证，请将客户机二进制文件复制到以下 Identity Server 目录：

```
IdentityServer_base/sun/identity/bin
```

注 如果有多个界面，则需要额外配置。可通过在 `smb.conf` 文件中进行配置设置多个界面，这样它就会传递到 `mbclient`。

添加和启用 NT 验证

您必须以组织管理员或顶层管理员身份登录到 Identity Server 中。

1. 转到要为其添加 NT 验证的组织。
2. 从 “查看” 菜单中选择 “服务”。

   如果已添加，“核心” 服务会显示在 “浏览” 窗格中。如果该服务尚未添加，可以与 NT 验证服务一同添加。
3. 在 “浏览” 窗格中单击 “添加”。

   此时 “数据” 窗格中会显示可用服务列表。
4. 选中 NT 验证的复选框并单击 “添加”。

   NT 验证服务将显示在 “浏览” 窗格中，向管理员证实已添加了该服务。
5. 单击 NT 验证的属性箭头。

   数据窗格中将显示消息：*当前不存在用于该服务的模板。要现在创建一个模板吗？*
6. 单击 “创建”。

   “数据” 窗格中将显示 NT 验证属性。根据需要修改这些属性。您可以在第 24 章 “NT 验证属性”中，或通过选择控制台右上角的 “帮助” 链接找到这些属性的说明。
7. 单击 “保存”。

   NT 验证服务已经启用。

使用 NT 验证登录

为了使用 NT 验证登录，必须修改核心验证服务属性 （第 246 页的 “组织验证模块”）以启用和选择 NT 验证。这可以确保当用户使用 `http://hostname:port/deploy_URI/UI/Login?module=NT` 登录时，将看到 “NT 验证” 登录窗口。根据正在使用的验证类型 （例如服务、角色、用户和组织），如果将验证模块配置为默认模块，则无需在 URL 中指定模块名称。

RADIUS 服务器验证

可以将 Identity Server 配置为与已安装的 RADIUS 服务器一起工作。如果您的企业中使用传统 RADIUS 服务器进行验证，此功能将很有用。启用 RADIUS 验证服务的过程分为两步：

1. 配置 RADIUS 服务器。

   有关详细说明，请参见 RADIUS 服务器文档。

2. 注册和启用 RADIUS 验证服务。

添加和启用 RADIUS 验证

您必须以组织管理员身份登录到 Identity Server 中。

1. 转到要为其添加 RADIUS 验证的组织。
2. 从 “查看” 菜单中选择 “服务”。

   如果已添加，“核心” 服务会显示在 “浏览” 窗格中。如果该服务尚未添加，可以与 RADIUS 验证服务一同添加。

3. 在 “浏览” 窗格中单击 “添加”。

   此时 “数据” 窗格中会显示可用服务列表。

4. 选中 RADIUS 验证的复选框并单击 “添加”。

   RADIUS 验证服务将显示在 “浏览” 窗格中，向管理员证实已添加了该服务。

5. 单击 RADIUS 验证的属性箭头。

   数据窗格中将显示消息：*当前不存在用于该服务的模板。要现在创建一个模板吗？*

6. 单击 “创建”。

   “数据” 窗格中将显示 RADIUS 验证属性。根据需要修改这些属性。您可以在第 25 章 “RADIUS 验证属性”中，或通过选择控制台右上角的 “帮助” 链接找到这些属性的说明。

7. 单击“保存”。

   RADIUS 验证服务已经启用。

使用 RADIUS 验证登录

为了使用 RADIUS 验证登录，必须修改核心验证服务属性（第 246 页的“组织验证模块”）以启用和选择 RADIUS 验证。这可以确保当用户使用 `http://hostname:port/deploy_URI/UI/Login?module=RADIUS` 登录时，将看到“RADIUS 验证”登录窗口。根据正在使用的验证类型（例如服务、角色、用户和组织），如果将验证模块配置为默认模块，则无需在 URL 中指定模块名称。

使用 Sun ONE Application Server 配置 RADIUS

默认情况下，当 RADUIS 客户机建立到其服务器的套接字连接时，在 Application Server 的 `server.policy` 文件中只允许 SocketPermissions 连接权限。为使 RADUIS 验证正常工作，对于以下操作应授予权限：

- 接受
- 连接
- 侦听
- 解析

要授予套接字连接权限，必须在 Application Server 的 `server.policy` 文件中添加一个条目。 SocketPermission 由主机规范和指定连接到该主机的方式的一组操作组成。请按以下格式指定主机：

```
host = hostname | IPaddress:portrange:portrange = portnumber |
-portnumberportnumber-portnumber
```

主机可以表示为 DNS 名称、数字 IP 地址或 localhost（对于本地计算机）。可以在指定的 DNS 主机名中包含一处通配符“*”。如果包含该通配符，它必须在最左侧的位置，如 `*.example.com`。

端口 （或 portrange）是可选的。形式为 N- 的端口规范 （其中 N 为端口号）表示编号为 N 及以上的所有端口。形式为 -N 的规范表示编号为 N 及以下的所有端口。

listen 操作仅在与本地主机一起使用时才有意义。任意其他操作存在时， resolve （解析主机 /IP 名称服务查找）操作才能执行。

例如，当创建 SocketPermissions 时，请注意如果将以下权限授予某些代码，将允许该代码连接到 machine1.example.com 上的 port 1645，并接受该端口上的连接：

```
permission java.net.SocketPermission machine1.example.com:1645,
"connect,accept";
```

类似地，如果将以下权限授予某些代码，将允许该代码接受本地主机上 1024 和 65535 之间的所有端口上的连接、连接到这些端口或侦听它们：

```
permission java.net.SocketPermission machine1.example.com:1645,
"connect,accept";

permission java.net.SocketPermission "localhost:1024-",
"accept,connect,listen";
```

注 授予代码权限以接受或建立到远程主机的连接可能会引起问题，因为恶意代码可以更容易地在各方之间传送和共享机密数据，使可能不具有数据访问权限的人访问到数据。请确保通过指定确切的端口号（而不是指定一个端口号的范围）仅授予适当的权限。

SafeWord 验证

可以对 Identity Server 进行配置，以处理到 Secure Computing 的 SafeWord™ 或 SafeWord PremierAccess™ 验证服务器的 SafeWord 验证请求。 Identity Server 提供 SafeWord 验证的客户机部分。SafeWord 服务器可以在安装了 Identity Server 的系统中存在，或者在单独的系统中存在。

添加和启用 SafeWord 验证

您必须以组织管理员或顶层管理员身份登录到 Identity Server 中。

1. 转到要为其添加 SafeWord 验证的组织。
2. 从 “查看” 菜单中选择 “服务”。

   如果已添加，“核心” 服务会显示在 “浏览” 窗格中。如果该服务尚未添加，可以与 SafeWord 验证服务一同添加。
3. 在 “浏览” 窗格中单击 “添加”。

   此时 “数据” 窗格中会显示可用服务列表。
4. 选中 SafeWord 验证的复选框并单击 “添加”。

   SafeWord 验证服务将显示在 “浏览” 窗格中，向管理员证实已添加了该服务。
5. 单击 SafeWord 验证的属性箭头。

   数据窗格中将显示消息：*当前不存在用于该服务的模板。要现在创建一个模板吗？*
6. 单击 “创建”。

   “数据” 窗格中将显示 SafeWord 验证属性。根据需要修改这些属性。您可以在第 26 章 “SafeWord 验证属性”中，或通过单击控制台右上角的 “帮助” 链接找到有关这些属性的说明。
7. 单击 “保存”。

   SafeWord 验证服务已经启用。

使用 SafeWord 验证登录

为了使用 SafeWord 验证登录，必须修改核心验证服务属性 （第 246 页的 “组织验证模块”）以启用和选择 SafeWord 验证。这可以确保当用户使用 `http://hostname:port/deploy_URI/UI/Login?module=SAFEWORD` 登录时，将看到 “SafeWord 验证” 登录窗口。根据正在使用的验证类型 （例如角色、用户和组织），如果将验证模块配置为默认模块，则无需在 URL 中指定模块名称。

使用 Sun ONE Application Server 配置 SafeWord

默认情况下，当 SafeWord 客户机建立到其服务器的套接字连接时，在 Application Server 的 `server.policy` 文件中只允许 SocketPermissions 连接权限。为使 SafeWord 验证正常工作，对于以下操作应授予权限：

- 接受
- 连接
- 侦听
- 解析

要授予套接字连接权限，必须在 Application Server 的 `server.policy` 文件中添加一个条目。 SocketPermission 由主机规范和指定连接到该主机的方式的一组操作组成。请按以下格式指定主机：

```
host = (hostname | IPaddress)[:portrange] portrange = portnumber |
-portnumberportnumber-[portnumber]
```

主机可以表示为 DNS 名称、数字 IP 地址或 localhost （对于本地计算机）。可以在指定的 DNS 主机名中包含一处通配符 “*”。如果包含该通配符，它必须在最左侧的位置，如 `*.example.com`。

端口 （或 portrange）是可选的。形式为 `N-` 的端口规范 （其中 `N` 为端口号）表示编号为 `N` 及以上的所有端口。形式为 `-N` 的规范表示编号为 `N` 及以下的所有端口。

`listen` 操作仅在与本地主机一起使用时才有意义。任意其他操作存在时， `resolve` （解析主机 /IP 名称服务查找）操作才能执行。

例如，当创建 SocketPermissions 时，请注意如果将以下权限授予某些代码，将允许该代码连接到 `machine1.example.com` 上的 `port 1645`，并接受该端口上的连接：

```
permission java.net.SocketPermission machine1.example.com:5030,
"connect,accept";
```

类似地，如果将以下权限授予某些代码，将允许该代码接受本地主机上 1024 和 65535 之间的所有端口上的连接、连接到这些端口或侦听它们：

```
permission java.net.SocketPermission machine1.example.com:5030,
"connect,accept";

permission java.net.SocketPermission "localhost:1024-",
"accept,connect,listen";
```

注 授予代码权限以接受或建立到远程主机的连接可能会引起问题，因为恶意代码可以更容易地在各方之间传送和共享机密数据，使可能不具有数据访问权限的人访问到数据。请确保通过指定确切的端口号（而不是指定一个端口号的范围）仅授予适当的权限。

SecurID 验证

可以对 Identity Server 进行配置，以处理到 RSA 的 ACE/Server 验证服务器的 SecureID 验证请求。Identity Server 提供 SecurID 验证的客户机部分。ACE/Server 可能位于安装 Identity Server 的系统或单独的系统中。为了验证本地管理的用户 ID（请参见 `admintool` [1M]），必须具备 root 访问权限。

SecurID 验证使用验证*帮助器* `amsecuridd`，后者是独立于主 Identity Server 进程以外的进程。在启动时，此帮助器将在端口上侦听配置信息。如果将 Identity Server 安装为以 `nobody` 运行，或以 root 以外的用户 ID 运行，*`IdentityServer_base`*`/SUNWam/share/bin/amsecuridd` 进程必须仍以 root 身份执行操作。有关 `amsecuridd` 帮助器的详细信息，请参见第 209 页的 “amsecuridd 帮助器”。

注 对于本 Identity Server 发行版，SecurID 验证服务不可用于 Linux 或 Solaris x86 平台。

添加和启用 SecurID 验证

您必须以组织管理员或顶层管理员身份登录到 Identity Server 中。

1. 转到要为其添加 SecurID 验证的组织。
2. 从 “查看” 菜单中选择 “服务”。

   如果已添加，“核心” 服务会显示在 “浏览” 窗格中。如果该服务尚未添加，可以与 SecurID 验证服务一同添加。
3. 在 “浏览” 窗格中单击 “添加”。

   此时 “数据” 窗格中会显示可用服务列表。
4. 选中 SecurID 验证的复选框并单击 “添加”。

   SecurID 验证服务将显示在 “浏览” 窗格中，向管理员证实已添加了该服务。
5. 单击 SecurID 验证的属性箭头。

   数据窗格中将显示消息：*当前不存在用于该服务的模板。要现在创建一个模板吗？*
6. 单击 “创建”。

   “数据” 窗格中将显示 SecurID 验证属性。根据需要修改这些属性。您可以在第 27 章 “SecurID 验证属性”中，或通过单击控制台右上角的 “帮助” 链接找到有关这些属性的说明。
7. 单击 “保存”。

   SecurID 验证服务已经启用。

使用 SecurID 验证登录

为了使用 SecurID 验证登录，必须修改核心验证服务属性 （第 246 页的 “组织验证模块”）以启用和选择 SecurID 验证。这可以确保当用户使用 `http://hostname:port/deploy_URI/UI/Login?module=SecurID` 登录时，将看到 “SecurID 验证” 登录窗口。根据正在使用的验证类型 （例如角色、用户和组织），如果将验证模块配置为默认模块，则无需在 URL 中指定模块名称。

Unix 验证

可以配置 Identity Server 使其按照 Solaris 或 Linux 系统 （其中安装了 Identity Server）已知的 Unix 用户 ID 和口令来处理验证请求。尽管 Unix 验证只有一个组织属性和几个全局属性，仍有一些面向系统的注意事项。为了验证本地管理的用户 ID （请参见 `admintool` [1M]），必须具备 root 访问权限。

Unix 验证使用验证 *帮助器* `amunixd`，后者是独立于主 Identity Server 进程以外的进程。在启动时，此帮助器将在端口上侦听配置信息。每个 Identity Server 仅有一个 Unix 帮助器为该服务器的所有组织服务。

如果将 Identity Server 安装为以 `nobody` 运行，或以 root 以外的用户 ID 运行，*`IdentityServer_base`*`/SUNWam/share/bin/amunixd` 进程必须仍以 root 身份执行操作。 Unix 验证模块通过打开到 `localhost:58946` 的套接字调用 `amunixd` 守护程序以侦听 Unix 验证请求。要在默认端口上运行 `amunixd` 帮助器进程，请输入以下命令：

```
./amunixd
```

要在非默认端口上运行 `amunixd`，请输入以下命令：

```
./amunixd [-c portnm] [ipaddress]
```

IP 地址和端口号位于 `AMConfig.properties` 中的 `UnixHelper.ipadrs` （以 IPV4 格式）和 `UnixHelper.port` 属性中。您可以通过 `amserver` 命令行实用程序运行 `amunixd` （`amserver` 自动运行进程，从 `AMConfig.properties` 中检索端口号和 IP 地址）。

`/etc/nsswitch.conf` 文件中的 `passwd` 条目确定是否查询 `/etc/passwd` 和 `/etc/shadow` 文件或 NIS 以进行验证。

添加和启用 Unix 验证

在以下步骤中，您必须以顶层管理员身份登录到 Identity Server 中。

1. 选择 “服务配置”模块。
2. 在 “服务名称”列表中的 Unix 验证的属性箭头上单击。

   将显示几个全局属性和一个组织属性。因为一个 Unix 帮助器为 Identity Server 服务器的所有组织服务，所以大多数 Unix 属性是全局属性。您可以在第 28 章 “Unix 验证属性”中，或通过单击控制台右上角的 “帮助”链接找到有关这些属性的说明。
3. 单击 “保存”保存属性的新值。

   您可以以组织管理员身份登录到 Identity Server，为组织启用 Unix 验证。
4. 转到要为其添加 Unix 验证的组织。
5. 从 “查看”菜单中选择 “服务”。

   如果已添加，“核心”服务会显示在 “浏览”窗格中。如果该服务尚未添加，可以与 Unix 验证服务一同添加。
6. 在 “浏览”窗格中单击 “添加”。

   此时 “数据”窗格中会显示可用服务列表。
7. 选中 Unix 验证的复选框并单击 “添加”。

   Unix 验证服务将显示在 “浏览”窗格中，向管理员证实已添加了该服务。
8. 单击 Unix 验证的属性箭头。

   数据窗格中将显示消息：*当前不存在用于该服务的模板。要现在创建一个模板吗？*
9. 单击 “创建”。

   “数据”窗格中将显示 Unix 验证组织属性。根据需要修改验证级别属性。您可以在第 28 章 “Unix 验证属性”中，或通过单击控制台右上角的 “帮助”链接找到有关此属性的说明。
10. 单击 “保存”。 Unix 验证服务即被启用。

使用 Unix 验证登录

为了使用 Unix 验证登录，必须修改核心验证服务属性 （第 246 页的 “组织验证模块”）以启用和选择 Unix 验证。这可以确保当用户使用 `http://hostname:port/deploy_URI/UI/Login?module=Unix` 登录时，将看到 “Unix 验证”登录窗口。根据正在使用的验证类型 （例如服务、角色、用户和组织），如果将验证模块配置为默认模块，则无需在 URL 中指定模块名称。

Windows 桌面 SSO 验证

Windows 桌面 SSO 验证服务是一个基于 Kerberos 的验证插件模块，用于 Windows 2000™。它允许已通过 Kerberos 分发中心 (KDC) 验证的用户无需重新提交登录条件即可验证到 Identity Server （单一登录）。

添加和启用 Windows 桌面 SSO 验证

启用 Windows 桌面 SSO 验证的过程分为三步：

1. 在 Windows 2000 域控制器中创建用户。
2. 设置 Internet Explorer。
3. 添加和配置 Windows 桌面 SSO 验证服务。

在 Windows 2000 域控制器中创建用户

1. 在域控制器中，为 Identity Server 验证服务创建用户帐户。
   a. 在 “开始”菜单中，转到 “程序” > “管理工具”。
   b. 选择 “活动目录和计算机”。
   c. 以 Identity Server 主机名作为用户 ID （登录名）创建新用户。 Identity Server 主机名中不能包括域名。

2. 在用户帐户与服务提供商名称间建立关联，并将键表文件导出至装有 Identity Server 的系统。为此，请运行以下命令：

   ```
   ktpass -princ host/hostname.domainname@DCDOMAIN -pass password
   -mapuser userName-out hostname.host.keytab
   ```

   ```
   ktpass -princ HTTP/hostname.domainname@DCDOMAIN -pass password
   -mapuser userName-out hostname.host.keytab
   ```

   ktpass 命令接受下列参数：

   hostname。运行 Identity Server 的主机名 （不含域名）。

   domainname。 Identity Server 域名。

   DCDOMAIN。域控制器的域名。它可能与 Identity Server 域名不同。

   password。用户帐户的口令。请确保口令正确，因为 ktpass 不校验口令。

   userName。用户帐户 ID。它应与主机名相同。

注 确保两个键表文件都已安全保管。

3. 重新启动服务器。

设置 Internet Explorer

1. 在 “工具” 菜单中，转到 “Internet 选项” > “高级/安全” > “安全”。
2. 选择 “集成的 Windows 验证” 选项。
3. 转到 “安全” > “本地 Internet”。
   a. 选择 “自定义级别”。在 “用户验证/登录” 面板中，选择 “只在内联网区域自动登录” 选项。
   b. 转到 “站点” 并选择所有选项。
   c. 单击 “高级”，将 Identity Server 添加到本地区域 （如果尚未添加）。

注 以上步骤适用于 Microsoft Internet Explorer™ 6 及更高版本。如果您使用的是较早版本，请确保 Identity Server 位于浏览器的 internet 区域并启用 “本地 Windows 验证”。

添加和配置 Windows 桌面 SSO 验证

您必须以组织管理员或顶层管理员身份登录到 Identity Server 中。

1. 转到要为其添加 Windows 桌面 SSO 验证的组织。
2. 从 “查看”菜单中选择 “服务”。

   如果已添加，“核心”服务会显示在 “浏览”窗格中。如果该服务尚未添加，可以与 Windows 桌面 SSO 验证服务一同添加。
3. 在 “浏览”窗格中单击 “添加”。

   此时 “数据”窗格中会显示可用服务列表。
4. 选中与 Windows 桌面 SSO 验证相应的复选框，然后单击 “添加”。

   Windows 桌面 SSO 验证服务将显示在 “浏览”窗格中，向管理员证实已添加了该服务。
5. 单击 Windows 桌面 SSO 验证的属性箭头。

   数据窗格中将显示消息：*当前不存在用于该服务的模板。要现在创建一个模板吗？*
6. 单击 “创建”。

   “数据”窗格中将显示 Windows 桌面 SSO 验证属性。根据需要修改这些属性。您可以在第 29 章 “Windows 桌面 SSO 验证属性”中，或通过选择控制台右上角的 “帮助”链接找到这些属性的说明。
7. 单击 “保存”。 Windows 桌面 SSO 验证服务即被启用。

使用 Windows 桌面 SSO 验证登录

为了使用 Windows 桌面 SSO 验证登录，必须修改核心验证服务属性 （第 246 页的“组织验证模块”）以启用和选择 Windows 桌面 SSO 验证。这可确保当用户从一主机登录 （该主机属于 Windows 2000 域控制器的一部分，并已使用 `http://hostname:port/deploy_URI/UI/Login?module=WindowsDesktopSSO` 以域用户身份登录），将会对用户进行验证。根据正在使用的验证类型 （例如服务、角色、用户和组织），如果将验证模块配置为默认模块，则无需在 URL 中指定模块名称。

验证配置

验证配置服务用于定义以下任一验证类型的验证模块：

- 组织
- 角色
- 服务
- 用户

为其中一种验证类型定义了验证模块后，可以基于成功的或失败的验证进程配置该模块以提供重定向 URL 以及后处理 Java 类规范。

在能够配置验证模块之前，必须先修改核心验证服务属性 “组织验证模块”以包含特定的验证模块名称。

验证配置用户界面

验证配置服务允许您定义一个或多个验证服务 （或*模块*），用户必须先通过这些验证服务才能访问控制台或 Identity Server 中的任何受保护的资源。基于组织、角色、服务和用户的验证使用通用用户界面定义验证模块。（随后的各节中介绍了访问特定对象类型的 “验证配置”界面的说明）。

1. 单击对象的 “验证配置”属性旁边的 “编辑”链接，以显示 “模块列表”窗口。
2. 此窗口列出了已指定给对象的验证模块。如果不存在任何模块，请单击 “添加”以显示 “添加模块”窗口。

   “添加模块”窗口包含三个要定义的文件：

“模块名称”。此下拉列表允许您选择可用于 Identity Server 的验证模块 （包括可以添加的自定义模块）。默认情况下，这些模块包括：

- LDAP
- 证书
- 匿名
- SafeWord
- SecurID
- HTTP Basic
- 成员资格
- NT
- RADIUS
- Unix
- Windows 桌面 SSO

标志。该下拉菜单允许您指定验证模块要求，可以指定以下值之一：

- **必需** - 要求验证模块必须成功。无论验证成功或失败，都将继续验证列表中的下一个验证模块。

- **必要** - 要求验证模块必须成功。如果验证成功，将继续验证列表中的下一个验证模块。如果验证失败，则返回到应用程序 （不继续验证列表中的下一个验证模块）。
- **充足** - 不要求验证模块必须成功。如果验证成功，则立即返回到应用程序（不继续验证列表中的下一个验证模块）。如果验证失败，将继续验证列表中的下一个验证模块。
- **可选** - 不要求验证模块必须成功。无论验证成功或失败，都将继续验证列表中的下一个验证模块。

这些标志建立了其定义的验证模块的执行标准。执行是有等级的：**必需**等级最高，**可选**等级最低。

例如，如果管理员定义了一个具有必需标志的 LDAP 模块，则用户的凭证必须通过 LADP 验证要求才能访问给定的资源。

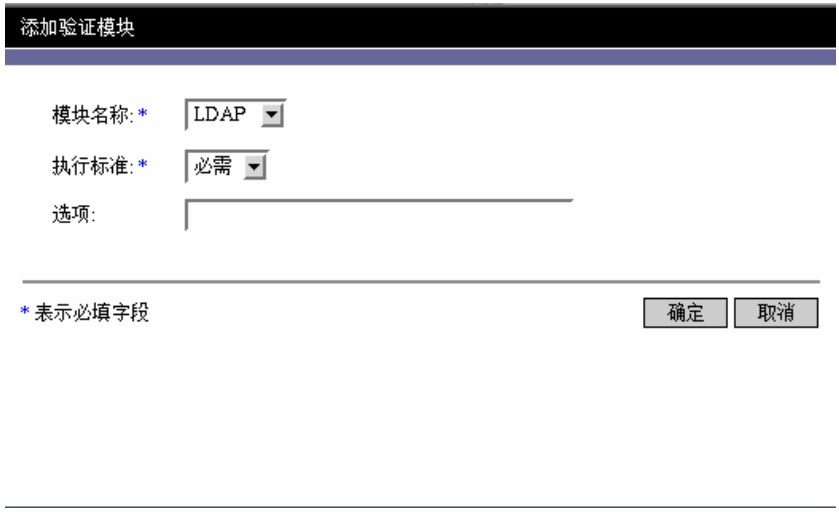
如果添加多个验证模块，并将每个模块的 “标志”都设置成必需，则用户必须通过所有验证要求才能被授予权限。

有关标志定义的详细信息，请参考 JAAS （Java 验证和授权服务），网址为：

```
http://java.sun.com/security/jaas/doc/module.html
```

选项。模块的其他选项，格式为 “关键字 = 值”对。多个选项之间用空格分隔。

图 8-1 用于用户的 “添加模块列表” 窗口



3. 选择了字段后，请单击 “确定” 返回 “模块列表” 窗口。此窗口中将列出已定义的验证模块。单击 “保存”。

   您可以根据需要将任意数目的验证模块添加到此列表。添加多个验证模块称为 *链式添加*。如果要链式添加验证模块，请注意模块列出的顺序将决定执行的层次结构的顺序。

   要更改验证模块的顺序，请执行以下步骤：

   a. 单击 “重新排序” 按钮。

   b. 选择要重新排序的模块。

   c. 使用 “上移” 和 “下移” 按钮将其放置到必需的位置。

4. 要从列表中移除任一验证模块，请选中验证模块旁边的复选框并单击 “删除”。

注 如果在链中的任一模块中输入 `amadmin` 凭证，您将会收到 amadmin 配置文件。在这种情况下，验证不检查别名映射，也不检查链中的模块。

用于组织的验证配置

组织的验证模块是在首次将核心验证服务添加到该组织时设置的。

要配置组织的验证属性，请执行以下操作：

1. 找到您将为其配置验证属性的组织。
2. 从 “查看” 菜单中选择 “服务”。
3. 在服务列表中单击核心属性箭头。

   “数据” 窗格中将显示核心验证属性。
4. 单击 “管理员验证” 属性旁边的 “编辑” 链接。此操作只允许您为管理员定义验证服务。管理员是需要访问 Identity Server 控制台的用户。如果需要将管理员的验证模块与最终用户的验证模块区别开来，则可以使用该属性。默认验证模块为 LDAP。

   定义了验证服务之后，请单击 “保存” 以保存所作的更改，然后单击 “关闭” 返回组织的核心验证属性。
5. 单击 “组织验证配置” 属性旁边的 “编辑” 链接。此操作允许您为组织中的所有用户定义验证模块。默认验证模块为 LDAP。
6. 定义了验证服务之后，请单击 “保存” 以保存所作的更改，然后单击 “关闭” 返回组织的核心验证属性。

用于角色的验证配置

角色的验证模块是在角色级别添加了验证配置服务之后设置的。

1. 找到您将为其配置验证属性的组织。
2. 从 “查看” 菜单中选择 “角色”。
3. 选择要为其设置验证配置的角色并单击属性箭头。

   “数据” 窗格中将显示角色的属性。
4. 从 “数据” 窗格的 “查看” 菜单中选择 “服务”。

5. 根据需要修改验证配置属性。您可以在第 30 章 “验证配置服务属性”中，或通过单击控制台右上角的 “帮助”链接找到有关这些属性的说明。

6. 单击 “保存”。

.

注 如果要创建新角色，验证配置服务将不会自动指定给该角色。请确保在创建新角色之前先选择 “角色配置文件”页面顶部的 “验证配置服务”选项。

如果启用了基于角色的验证，可以将 LDAP 验证模块保留为默认设置，因为不需要配置成员资格。

用于服务的验证配置

服务的验证模块是在添加了验证配置服务之后设置的。为此，请执行以下步骤：

1. 从 “身份管理”模块的 “查看”菜单中选择 “服务”。

   将显示已添加服务的列表。如果未添加验证配置服务，请继续执行以下步骤。如果已添加了该服务，请跳到步骤 4。

2. 在 “浏览”窗格中单击 “添加”。

   “数据”窗格中将显示可用服务的列表。

3. 选中验证配置的复选框并单击 “添加”。

   验证配置服务将显示在 “浏览”窗格中，向管理员证实已添加了该服务。

4. 单击验证配置属性箭头。

   “数据”窗格中将显示 “服务实例列表”。

5. 单击要为其配置验证模块的服务实例。

6. 修改验证配置属性并单击 “保存”。可以在第 30 章 “验证配置服务属性” 中，或通过单击控制台右上角的 “帮助” 链接，找到这些属性的说明。

用于用户的验证配置

1. 从 “身份管理” 模块的 “查看” 菜单中选择 “用户”。

   “浏览” 窗格中将显示用户列表。

2. 选择要修改的用户，然后单击属性箭头。

   数据窗格中将显示用户配置文件。

注 如果要创建新用户，验证配置服务将不会自动指定给该用户。请确保在创建用户之前先选择 “用户配置文件” 页面顶部的 “验证配置服务” 选项。如果未选择此选项，用户将不会继承为角色定义的验证配置。

3. 要确保将验证配置服务指定给该用户，请从 “查看” 菜单中选择 “服务”。指定之后，验证配置服务将被列为已指定的服务。
4. 从 “数据” 窗格的 “查看” 菜单中选择 “用户”。
5. 单击 “用户验证配置” 属性旁边的 “编辑” 链接，以定义用于用户的验证模块。
6. 单击 “保存”。

验证级别验证

每个验证模块均可以与其*验证级别*的整数值相关联。单击 “服务配置” 中验证模块的属性箭头，然后更改模块的 “验证级别” 属性相应的值，可以指定验证级别。用户通过一个或多个验证模块的验证后，较高的验证级别将决定较高的用户信任级别。

用户成功地通过模块的验证之后，系统将在用户的 SSO 令牌中设置验证级别。如果用户需要通过多个验证模块的验证并且成功地通过了这些验证，系统将在用户的 SSO 令牌中设置最高的验证级别值。

如果用户试图访问某个服务，该服务可以通过查看用户的 SSO 令牌中的验证级别来确定是否允许该用户进行访问。随后服务将用户重定向到具有相应验证级别的验证模块进行验证。

用户还可以访问具有特定验证级别的验证模块。例如，用户使用以下语法进行登录：

```
http://hostname:port/deploy_URI/UI/Login?authlevel=auth_level_value
```

所有验证级别高于或等于 *auth_level_value* 的模块将显示为验证菜单以供用户选择。如果只找到一个匹配的模块，则将直接显示该验证模块的登录页面。

基于模块验证

用户可以使用以下语法访问特定的验证模块：

```
http://hostname:port/deploy_URI/UI/Login?module=module_name
```

在能够访问验证模块之前，必须先修改核心验证服务属性 “组织验证模块”以包含该验证模块名称。如果此属性中不包含该验证模块名称，则当用户尝试进行验证时，将会显示 “验证模块被拒绝”页面。有关详细信息，参见第 246 页的 “组织验证模块”。

URL 重定向

在验证配置服务中，您可以指定 URL 重定向以进行成功的或不成功的验证。而 URL 本身是在该服务的 “登录成功 URL”和 “登录失败 URL”属性中进行定义的。为了启用 URL 重定向，必须将验证配置服务添加到您的组织中，以便可以为角

色、组织或用户进行配置。添加验证配置服务时，请确保添加一个验证模块，例如 LDAP - 必需。有关为身份对象添加验证配置服务的信息，请参见第 168 页的 “验证配置”。

验证服务故障转移

如果主服务器因硬件或软件故障失败或者服务器被临时关闭，则验证服务故障转移会自动将验证请求重定向到辅助服务器。

必须首先在提供验证服务的 Identity Server 实例上创建验证环境。如果此 Identity Server 实例不可用，则可通过验证故障转移机制在其他的 Identity Server 实例上创建验证环境。验证环境将按以下顺序检查服务器可用性。

1. 验证服务 URL 将被传递给 AuthContext API。例如：

   ```
   AuthContext(orgName, url)
   ```

   如果使用此 API，则它将仅使用由 URL 所引用的服务器。即使在该服务器中提供了验证服务，也不会进行故障转移。

2. 验证环境将检查在 `AMConfig.properties` 文件的 `com.iplanet.am.server*` 属性中定义的服务器。

3. 如果步骤 2 失败，则验证环境将从提供有命名服务的服务器查询平台列表。此平台列表是在安装共享同一个 Directory Server 实例的多个 Identity Server 实例（通常是为故障转移目的）时自动创建的。

   例如，如果该平台列表包含 `Server1`、 `Server2` 和 `Server3` 的 URL，则验证环境会在 `Server1`、 `Server2` 和 `Server3` 之间循环，直到验证在其中一个服务器上成功为止。

平台列表不可能始终从同一个服务器获得，因为它取决于命名服务的可用性。而且，命名服务故障转移可能会首先进行。在 `com.iplanet.am.naming.url` 属性（在 `AMConfing.properties` 中）中将指定多个命名服务 URL。第一个可用的命名服务 URL 将用于确定服务器，该服务器中包含将会进行验证故障转移的服务器 （限于其平台服务器列表范围内）的列表。

第 9 章

口令重置服务

Sun Java™ System Identity Server 2004Q2 提供口令重置服务，使用户可以重置其用于访问受 Identity Server 保护的给定服务或应用程序的口令。口令重置服务属性由顶层管理员定义，它们可以控制用户验证凭证 （以*秘密问题*形式）、控制新的或现有的口令通知机制，以及设置不正确用户验证的可能的锁定间隔。

本章包含以下部分：

注册口令重置服务

不需要为用户所在的组织注册口令重置服务。如果用户所在的组织中不存在口令重置服务，该服务将继承在 “服务配置”模块中为服务定义的值。

为另一组织中的用户注册口令重置

1. 在 “身份管理”模块中，选择 “组织”并选择您要为其注册服务的组织。

2. 单击浏览框中的 “注册”。

   数据框中将显示可用服务的列表。

3. 选中口令重置的复选框并单击 “注册”。

   口令重置服务将显示在浏览框中，向管理员表明已注册该服务。

配置口令重置服务

注册口令重置服务后，必须由具有管理员特权的用户来配置该服务。

配置服务

1. 选择要为其注册口令重置服务的组织。
2. 单击口令重置属性箭头。

   数据框中将显示消息 “没有适用于此服务的模板”。单击 “创建”。

3. 数据框中将显示口令重置属性，使您可以定义口令重置服务的要求。确保启用口令重置服务 （此为默认情况）。至少必须定义以下属性：

   - 用户验证
   - 秘密问题
   - 绑定 DN
   - 绑定口令

   绑定 DN 属性必须包含具有重置口令特权的用户 （例如，帮助台管理员）。受 Directory Server 限制，当绑定 DN 为 `cn=directory manager` 时口令重置不起作用。

   其他属性是可选的。有关 “口令重置”属性的说明，参见第 307 页的 “口令重置服务属性”，也可以单击控制台右上角的 “帮助”链接。

注 Identity Server 会自动为随机口令生成安装口令重置 Web 应用程序。但是，您可以写自己的口令生成和口令通知插件类。有关这些插件类的样例，参见以下位置中的 Readme.html 文件。

PasswordGenerator：

```
IdentityServer_base/SUNWam/samples/console/PasswordGenerator
```

NotifyPassword：

```
IdentityServer_base/SUNWam/samples/console/NotifyPassword
```

4. 如果用户要定义其独特的私人问题，则选择 “启用私人问题”属性。定义这些属性后，单击 “保存”。

口令重置锁定

口令重置服务包含锁定功能，该功能将限制用户对于正确回答其秘密问题所能尝试的特定次数。锁定功能通过口令重置服务属性配置。有关这些属性的说明，参见第 307 页的 “口令重置服务属性”。口令重置支持两种锁定类型，内存锁定和物理锁定。

内存锁定

这是一种临时锁定，仅当 “口令重置失败锁定持续时间”属性中的值大于零并启用了 “启用口令重置失败锁定”属性时才有效。该锁定功能可以防止用户通过口令重置 Web 应用程序重置其口令。锁定将持续 “口令重置失败锁定持续时间”中指定的时间，或持续到重新启动服务器。

物理锁定

这是一种更持久的锁定。如果将 “口令重置失败锁定计数”属性中的值设置为 0 并启用了 “启用口令重置失败锁定”属性，则当用户不能正确回答秘密问题时，会将其帐户状态改为无效。

最终用户口令重置

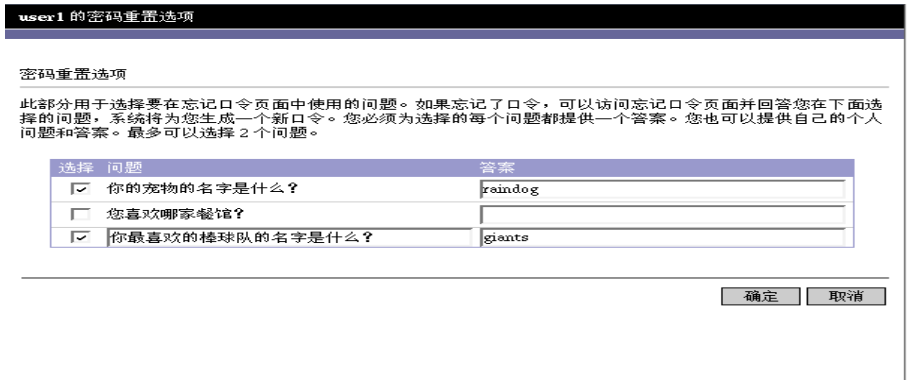
以下各部分介绍了使用 “口令重置”服务的用户体验。

自定义口令重置

启用口令重置服务并且管理员定义属性之后，用户就可以登录到 Identity Server 控制台自定义其秘密问题。例如：

1. 用户登录到 Identity Server 控制台，提供用户名和口令并成功通过验证。
2. 在 “用户配置文件”页面中，用户选择口令重置选项。将显示 “可用问题答案”屏幕。
3. 为用户提供管理员为该服务定义的可用问题，例如：
   - 您的宠物叫什么名字？
   - 您最喜欢的电视节目是什么？
   - 您母亲婚前姓什么？
   - 您喜欢哪家餐馆？
4. 用户可以选择多个秘密问题，但数目不能超过管理员为该组织定义的问题的最大数目 （最大数目在口令重置服务中定义）。然后用户需要为选定问题提供答案。这些问题和答案将成为重置用户口令 （参见下一部分）的基础。如果管理员已选择 “启用私人问题”属性，将显示文本字段，用户可以在其中输入独特的秘密问题并提供答案。

图 9-1 已启用私人问题的 “可用问题答案” 屏幕



5. 用户单击 “保存”。

重置遗忘口令

在用户忘记其口令的情况下， Identity Server 将使用口令重置 Web 应用程序随机生成新口令并将其通知用户。一般的遗忘口令解决方案如下：

1. 用户从管理员为其提供的 URL 登录到口令重置 Web 应用程序。例如：

   `http://`*`hostname:port`*`/ampassword` （对于默认组织）

   或

   `http://`*`/hostname: port /deploy_uri`*`/UI/PWResetUserValidation?org=`*`orgname`*，其中 *orgname* 是组织的名称。

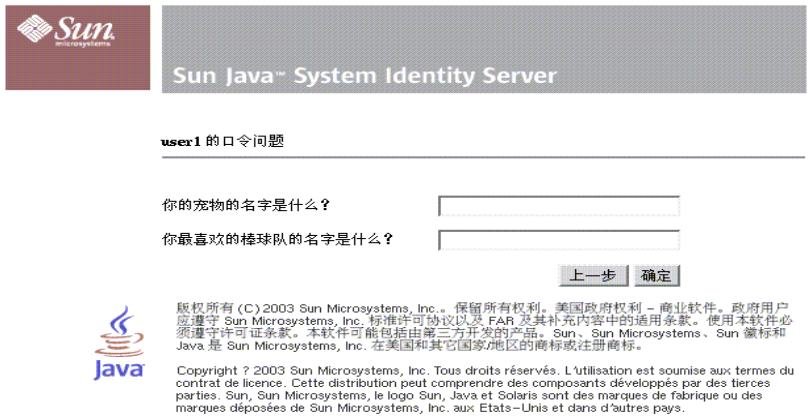
注 如果没有为父组织但为子组织启用了口令重置服务，则用户必须使用以下语法访问服务：

`http://`*`hostname:`*
`port``/`*`deploy_uri`*`/UI/PWResetUserValidation?org=`*`orgname`*

2. 用户输入用户 ID。

3. 系统将显示在口令重置服务中定义并且用户在自定义过程中选择的私人问题。如果用户以前没有登录到“用户配置文件”页面并自定义私人问题，将不会生成口令。

图 9-2 “用户的口令问题”屏幕



用户正确回答问题后，将生成新口令并用电子邮件将其发送给用户。不管问题回答得是否正确，都会给用户发送尝试通知。用户必须在“用户配置文件”页面中输入其电子邮件地址，才能接收新口令和尝试通知。

口令策略

安全口令策略通过强制实施以下措施将与易猜测的口令相关的风险降到最低程度：

- 用户必须定期更改其口令。
- 用户必须提供不常见的口令。

- 输入一定次数的错误口令之后，可以锁定帐户。

Directory Server 提供了几种在树中的任一节点设置口令策略的方法，并且有几种方法设置策略。有关详细信息，参见以下 Directory Server 文档：

http://docs.sun.com/source/816-6700-10/aci.html#14773

http://docs.sun.com/source/816-6852-10/useracct.html#410626

第 III 部分

命令行参考指南

本部分是 《Sun Java™ System Identity Server 2004Q2 管理指南》的第三部分 “命令行参考指南”。本部分包含以下各章：

本部分中所述的所有命令行工具均可在以下默认位置找到：

```
IdentityServer_base/SUNWam/bin (Solairs)
IdentityServer_base/identity/bin (Linux)
```

第 10 章

amadmin 命令行工具

本章介绍有关 amadmin 命令行工具的信息，并包含以下几节：

amadmin 命令行可执行文件

命令行可执行文件 amadmin 的主要用途是将 XML 服务文件装入 Directory Server 并在 DIT 上执行批管理任务。可以在 IdentityServer_base/SUNWam/bin 中找到 amadmin，其用途包括：

- 装入 XML 服务文件 - 管理员将服务装入使用 XML 服务文件格式（在 sms.dtd 中定义）的 Identity Server。所有服务必须使用 amadmin 装入，而不能通过 Identity Server 控制台导入。

注 XML 服务文件作为由 Identity Server 引用的 XML 数据的静态 *blobs* 存储在 Directory Server 中。此信息不适用于只了解 LDAP 的 Directory Server。

- 对 DIT 执行身份对象的批更新 - 管理员可以使用在 amadmin.dtd 中定义的批处理 XML 文件格式执行对 Directory Server DIT 的批更新。例如，如果管理员要创建 10 个组织、1000 个用户和 100 个组，可以通过将请求放在一个或多个批处理 XML 文件中并使用 amadmin 装入这些文件即可一次完成任务。有关详细信息，参见 《*Identity Server Developer's Guide*》中的 “Service Management”一章。

注 amadmin 仅支持 Identity Server 控制台支持的功能的一部分，并且不能作为后者的替代命令。建议将控制台用于小的管理任务，而将 amadmin 用于较大的管理任务。

amadmin 语法

必须遵守若干结构性规则才能使用 amadmin。使用该工具的通用语法为：

- amadmin -u | --runasdn *dnname* -w | --password *password* [-l | --locale *localename*] [[-v | --verbose] | [-d |--debug]] -t | --data *xmlfile1* [*xmlfile2* ...]
- amadmin -u | --runasdn *dnname* -w | --password *password* [-l | --locale *localename*] [[-v | --verbose] | [-d | --debug]] -s | --schema *xmlfile1* [*xmlfile2* ...]
- amadmin -u | --runasdn *dnname* -w | --password *password* [-l | --locale *localename*] [[-v | --verbose] | [-d | --debug]] -r | --deleteService *serviceName1* [*serviceName2* ...]
- amadmin -u | --runasdn *dnname* -w | --password *password* or -f | --password file *passwordfile* [-c | --continue] [-l | --locale *localename*] [[-v | --verbose] | [-d | --debug]] -m | --session *servername pattern*
- amadmin -h | --help
- amadmin -n | --version
- amadmin -u | --runasdn *dnname* -w | --password *password* or - f |--passwordfile *passwordfile* [-l | --locale *localename*] [[-v | --verbose] | [-d] |--debug]] -a |--addAttributes *serviceName schemaType xmlfile*[*xmlfile2*] ...

注 必须完全按照语法中所示，输入两个连字符。

amadmin 选项

以下为 amadmin 命令行参数选项的定义：

--runasdn (-u)

`--runasdn` 用于在 LDAP 服务器中验证用户。该变量的值为被授权运行 `amadmin` 的用户的独特名称 (DN)，例如

`--runasdn uid=amAdmin,ou=People,o=iplanet.com,o=isp`。

还可以在 DN 中的域组件之间插入空格，并将整个 DN 用双引号引起，如下所示：`--runasdn "uid=amAdmin, ou=People, o=iplanet.com, o=isp"`。

--password (-w)

`--password` 是强制性选项，其值为使用 `--runasdn` 选项指定的 DN 的口令。

--locale (-l)

`--locale` 选项的值为语言环境的名称。此选项可用于自定义消息语言。如果未提供该选项的值，将使用默认的语言环境 `en_US`。

--continue (-c)

如果使用 --continue 选项，则即使出现了错误， amadmin 命令仍然会继续处理 XML 文件。例如，如果要同时装入三个 XML 文件，而第一个 XML 文件失败，则 `amadmin` 将继续装入剩余的文件。

--session (-m)

`--session` (`-m`) 选项用于管理会话或显示当前会话。指定 `--runasdn` 时，其值必须与 `AMConfig.properties` 中的超级用户的 DN 相同，或为顶层管理员用户的 ID。

以下示例将显示特定服务主机名的所有会话：

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com -v  -w 12345678 -m
http://sun.com:58080
```

以下示例将显示特定用户的会话：

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com -v  -w 12345678 -m
http://sun.com:58080 username
```

可以通过输入相应的索引编号来终止会话，或输入多个索引编号 （以空格分开）来终止多个会话。

而使用以下选项：

amadmin -m | --session *servername pattern*

pattern 可以是通配符 (*)。如果此模式 (pattern) 使用通配符 (*)，则必须在 Shell（命令解释器）中用元字符 (\) 对其进行换码。

--debug (-d)

`--debug` 选项可用于将消息写入在 *identity_server_root*`/var/opt/SUNWam/debug` 目录下创建的 `amadmin` 文件。这些消息在技术上很详细，但与 i18n 不兼容。要生成 `amadmin` 操作日志，则在记录到数据库时，需要手动添加数据库驱动程序的类路径。例如，如果在 `amadmin` 中要将日志记录到 `mysql`，请添加以下各行：

```
CLASSPATH=$CLASSPATH:/opt/IS61/SUNWam/lib/mysql-connector-java-3.0.6-stable-bin.jar

export CLASSPATH
```

--verbose (-v)

`--verbose` 选项用于将 `amadmin` 命令的总体进度显示到屏幕上。它不会将详细信息打印到文件中。输出到命令行的消息与 i18n 兼容。

--data (-t)

`--data` 选项的值将采用要导入的批处理 XML 文件的名称。可以指定一个或多个 XML 文件。此 XML 文件可以创建、删除和读取各种目录对象，还可以注册和取消注册服务。有关可将哪些类型的 XML 文件传递给该选项的详细信息，参见《*Identity Server Developer's Guide*》中的 “Servic Management”一章。

--schema (-s)

`--schema` 选项用于将 Identity Server 服务的属性装入 Directory Server。它的变量值为在其中定义服务属性的 XML 服务文件。此 XML 服务文件基于 `sms.dtd`。可以指定一个或多个 XML 文件。

注 必须指定 `--data` 或 `--schema` 选项，具体取决于是为 DIT 配置批更新还是装入服务模式和配置数据。

--deleteservice (-r)

`--deleteservice` 选项用于只删除服务及其模式。

--serviceName

`--serviceName` 选项的值为在 XML 服务文件的 `Service name=...` 标记下定义的服务名称。此部分在第 191 页的 代码示例 10-1 中显示。

代码示例 10-1 `sampleMailService.xml` 部分

```
...
<ServicesConfiguration>
    <Service name="sampleMailService" version="1.0">
        <Schema
 serviceHierarchy="/other.configuration/sampleMailService"
            i18nFileName="sampleMailService"
            i18nKey="iplanet-am-sample-mail-service-description">
...
```

--help (-h)

`--help` 参数用于显示 `amadmin` 命令的语法。

--version (-n)

`--version` 参数用于显示实用程序名称、产品名称、产品版本和法律声明。

使用 amadmin 进行联合管理

本节列出供 “联合管理” 使用的 amadmin 参数。有关 “联合管理” 的详细信息，参见 《*Identity Server Federation Management Guide*》。

将特权元数据符合性 XML 装入 Directory Server

```
amadmin -u|--runasdn <user's DN>

    -w|--password <password> or -f|--passwordfile <passwordfile>

    -e|--entityname <entity name>

    -g|--import <xmlfile>
```

--runasdn (-u)

用户的 DN

--password (-w)
用户的口令。

--passwordfile (-f)
包含用户口令的文件的名称。

--entityname (-e)
实体名称。例如 `http://www.example.com`。某一实体应只属于一个组织。

--import (-g)
包含元数据信息的 XML 文件的名称。此文件应该符合特权元数据规范和 XSD。

将实体导出到 XML 文件 （无 XML 数字签名）

amadmin -u|--runasdn <user's DN>

```
-w|--password <password> or -f|--passwordfile <passwordfile>
    -e|--entityname <entity name>
    -o|--export <filename>
```

--runasdn (-u)
用户的 DN

--password (-w)
用户的口令。

--passwordfile (-f)
包含用户口令的文件的名称。

--entityname (--e)

驻留在 Directory Server 中的实体的名称

--export (-o)

要包含实体的 XML 的文件名称。 XML 应符合特权元数据 XSD。

将实体导出到 XML 文件 （有 XML 数字签名）

```
amadmin -u|--runasdn <user's DN>
```

```
-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-q|--exportwithsig <filename>
```

--runasdn (-u)
用户的 DN

--password (-w)
用户的口令。

--passwordfile (-f)
包含用户口令的文件的名称。

--entityname (--e)

驻留在 Directory Server 中的实体的名称

--exportwithsig (-o)

要包含实体的 XML 的文件名称。此文件已经过数字签名。 XML 必须符合特权元数据 XSD。

将 amadmin 用于资源包

下面的一节介绍用于添加、查找和删除资源包的 amadmin 语法。

添加资源包

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>
       -b|--addresourcebundle <name-of-resource-bundle>
       -i|--resourcebundlefilename <resource-bundle-file-name>
       [-R|--resourcelocale] <locale>
```

获取资源字符串

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>
       -z|--getresourcestrings <name-of-resource-bundle>
```

```
        [-R|--resourcelocale] <locale>
```

移除资源包

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>
        -j|--deleteresourcebundle <name-of-resource-bundle>
        [-R|--resourcelocale] <locale>
```

第 11 章

amserver 命令行工具

本章介绍有关 amserver 命令行工具的信息。本章包含以下内容：

amserver 命令行可执行文件

amserver 命令行可执行文件可以在 Solaris 平台上创建、启动、停止和删除附加的 Identity Server 实例。 Windows 2000 平台上的 amserver 只允许启动和停止 Identity Server。

amserver 语法

使用该工具的通用语法为：

```
./amserver { start | stop }
```

start

start 命令用于启动 Identity Server。

stop

stop 命令用于停止 Identity Server。

第 12 章

am2bak 命令行工具

本章介绍有关 am2bak 命令行工具的信息，包含以下内容：

am2bak 命令行可执行文件

Identity Server 包含一个 am2bak 实用程序，该实用程序位于 IdentityServer_base/SUNWam/bin 下。该实用程序用于备份 Identity Server 的所有组件或可选组件。在备份日志时必须运行 Directory Server。

am2bak 语法

在 Solaris 操作系统中使用 am2bak 工具的通用语法为：

```
./am2bak [ -v | --verbose ] [ -k | --backup backup-name ] [ -l |
--location location ] [[-c | --config] | [-b | --debug] | [-g | --log]
| [-t | --cert] | [-d | --ds] | [-a | --all]]*
```

```
./am2bak -h | --help
```

```
./am2bak -n | --version
```

在 Windows 2000 操作系统中使用 am2bak 工具的通用语法为：

```
am2bak [ -v | --verbose ] [ -k | --backup backup-name ] [ -l |
--location location ] [[-c | --config] | [-b | --debug] | [-g | --log]
| [-t | --cert] | [-d | --ds] | [-a | --all]]*
```

```
am2bak -h | --help
```

```
am2bak -n | --version
```

注 必须完全按照语法中所示，输入两个连字符。

am2bak 选项

--verbose (-v)

--verbose 用于在详细模式下运行备份实用程序。

--backup backup-name (-k)

--backup *backup-name* 定义备份文件的名称。默认值为 ambak。

--location (-l)

--location 指定备份的目录位置。默认位置为 IdentityServer_base/backup。

--config (-c)

--config 指定仅备份配置文件。

--debug (-b)

--debug 指定仅备份调试文件。

--log (-g)

--log 指定仅备份日志文件。

--cert (-t)

--cert 指定仅备份证书数据库文件。

--ds (-d)

--ds 指定仅备份 Directory Server。

--all (-a)

--all 指定备份整个 Identity Server。

--help (-h)

--help 参数用于显示 am2bak 命令的语法。

--version (-n)

`--version` 参数用于显示实用程序名称、产品名称、产品版本和法律声明。

备份过程

1. 以 root 身份登录。

   运行此脚本的用户必须具有 root 访问权限。

2. 如果需要，运行确保使用正确路径的脚本。

   该脚本将会备份以下 Solaris™ 操作环境文件：

   - 配置文件和自定义文件：
     - *IdentityServer_base*/SUNWam/config/
     - *IdentityServer_base*/SUNWam/locale/
     - *IdentityServer_base*/SUNWam/servers/httpacl
     - *IdentityServer_base*/SUNWam/lib/*.properties （Java 属性文件）
     - *IdentityServer_base*/SUNWam/bin/amserver.*instance-name*
     - *IdentityServer_base*/SUNWam/servers/https-*all_instances*
     - *IdentityServer_base*/SUNWam/servers/web-apps-*all_instances*
     - *IdentityServer_base*/SUNWam/web-apps/services/WEB-INF/config
     - *IdentityServer_base*/SUNWam/web-apps/services/config
     - *IdentityServer_base*/SUNWam/web-apps/applications/WEB-INF/classes
     - *IdentityServer_base*/SUNWam/web-apps/applications/console
     - /etc/rc3.d/K55amserver.*all_instances*
     - /etc/rc3.d/S55amserver.*all_instances*
     - *DirectoryServer_base*/slapd-*host*/config/schema/
     - *DirectoryServer_base*/slapd-*host*/config/slapd-collations.conf
     - *DirectoryServer_base*/slapd-*host*/config/dse.ldif
   - 日志文件和调试文件：
     - var/opt/SUNWam/logs （Identity Server 日志文件）
     - var/opt/SUNWam/install （Identity Server 安装日志文件）

- var/opt/SUNWam/debug （Identity Server 调试文件）

- 证书：
  - *IdentityServer_base*/SUNWam/servers/alias
  - *DirectoryServer_base*/alias

该脚本还会备份以下 Microsoft® Windows 2000 操作系统文件：

- 配置文件和自定义文件：
  - *IdentityServer_base*/web-apps/services/WEB-INF/config/*
  - *IdentityServer_base*/locale/*
  - *IdentityServer_base*/web-apps/applications/WEB-INF/classes/*.properties（java 属性文件）
  - *IdentityServer_base*/servers/https-*host*/config/jvm12.conf
  - *IdentityServer_base*/servers/https-*host*/config/magnus.conf
  - *IdentityServer_base*/servers/https-*host*/config/obj.conf
  - *DirectoryServer_base*/slapd-host/config/schema/*.ldif
  - *DirectoryServer_base*/slapd-host/config/slapd-collations.conf
  - *DirectoryServer_base*/slapd-host/config/dse.ldif
- 日志文件和调试文件：
  - var/opt/logs （Identity Server 日志文件）
  - var/opt/debug （Identity Server 调试文件）
- 证书：
  - *IdentityServer_base*/servers/alias
  - *IdentityServer_base*/alias

第 13 章

bak2am 命令行工具

本章介绍有关 bak2am 命令行工具的信息，包含以下内容：

bak2am 命令行可执行文件

Identity Server 包含一个 bak2am 实用程序，该实用程序位于 IdentityServer_base/SUNWam/bin 下。该实用程序用于恢复由 am2back 实用程序备份的 Identity Server 的组件。

bak2am 语法

在 Solaris 操作系统中使用 bak2am 工具的通用语法为：

```
./bak2am [ -v | --verbose ] -z | --gzip tar.gz-file
./bak2am [ -v | --verbose ] -t | --tar tar-file
./bak2am -h | --help
./bak2am -n | --version
```

在 Windows 2000 操作系统中使用 bak2am 工具的通用语法为：

```
bak2am [ -v | --verbose ] -d | --directory directory-name
bak2am -h | --help
bak2am -n | --version
```

注 必须完全按照语法中所示，输入两个连字符。

bak2am 选项

--gzip backup-name

`--gzip` 以 `tar.gz` 格式指定备份文件的完整路径和文件名。默认情况下，路径为 `IdentityServer_base/backup`。此选项仅适用于 Solaris。

--tar backup-name

`--tar` 以 `tar` 格式指定备份文件的完整路径和文件名。默认情况下，路径为 `IdentityServer_base/backup`。此选项仅适用于 Solaris。

--verbose

`--verbose` 用于在详细模式下运行备份实用程序。

--directory

`--directory` 指定备份目录。默认情况下，路径为 `IdentityServer_base/backup`。此选项仅适用于 Windows 2000。

--help

`--help` 参数用于显示 `bak2am` 命令的语法。

--version

`--version` 参数用于显示实用程序名称、产品名称、产品版本和法律声明。

1. 以 root 身份登录。

   运行此脚本的用户必须具有 root 访问权限。

2. 将输入的 tar 文件脱档。

   该文件是在运行备份脚本时生成的。

第 14 章

ampassword 命令行工具

本章介绍有关 amPassword 命令行工具的信息，包含以下内容：

ampassword 命令行可执行文件

Identity Server 包含一个 ampassword 实用程序，该实用程序位于 etc/opt/SUNWam/bin 下。该实用程序允许您更改管理员或用户的 Identity Server 口令。

ampassword 语法

使用 ampassword 工具的通用语法为：

```
ampassword -a | --admin [ -o | --old oldPassword -n | --new newPassword
]

ampassword -p | --proxy [ -o | --old oldPassword -n | --new newPassword
]

ampassword -e | --encrypt [ password ]
```

注 必须完全按照语法中所示，输入两个连字符。

ampassword 选项

--admin (-a)

--admin 用于更改管理口令。

--proxy (-p)

`--proxy` 用于更改代理服务器口令。该选项与代理服务器用户（`serverconfig.xml` 中用户类型为 `proxy`）相对应。

--encrypt (-e)

`--encrypt` 用于加密口令。该选项被打印到命令行。例如，要加密新的 `dsamuser` 口令，可使用以下命令：

```
ampassord -e newPassword
```

然后，将新的 `dsamuser` 口令放入 `serverconfig.xml` 并重新启动 Web 容器 （Web Server 或 Application Server）。

在 SSL 上运行 ampassword

要使用在安全套接字层 (SSL) 模式中运行的 Identity Server 运行 ampassword，请执行以下步骤：

1. 修改位于以下目录的 `serverconfig.xml` 文件：

   `IdentityServer_base/SUNWam/config/`

2. 将服务器属性 `port` 更改为运行 Identity Server 的 SSL 端口。

3. 将 `type` 属性更改为 SSL。

   例如：

```
<iPlanetDataAccessLayer>
<ServerGroup name="default" minConnPool="1" maxConnPool="10">
    <Server name="Server1" host="sun.com" port="636" type="SSL" />
    <User name="User1" type="proxy">
```

```
        <DirDN>

                 cn=puser,ou=DSAME Users,dc=iplanet,dc=com

        </DirDN>

        <DirPassword>

                  AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf

         </DirPassword>

</User> ...
```

ampassword 只更改 Directory Server 中的口令。您必须手动更改 `ServerConfig.xml` 和 Identity Server 的所有验证模板中的口令。

第 15 章

VerifyArchive 命令行工具

本章介绍有关 VerifyArchive 命令行工具的信息，包含以下部分：

VerifyArchive 命令行可执行程序

VerifyArchive 用于验证日志归档文件。日志归档文件为一组带有时间戳的日志及其相应的密钥库 （密钥库包含用于生成 MAC 和数字签名的密钥， MAC 和数字签名用于检测日志文件是否被篡改）。检验归档文件可以检测归档文件中是否可能有文件被篡改和/或删除。

VerifyArchive 针对给定的 logName 提取所有的归档文件集以及属于各个归档文件集的所有文件。执行 VerifyArchive 时，它将搜索每项日志记录以检测其是否被篡改。如果检测到了篡改，则将打印一条消息，指出被篡改的文件和记录号。

VerifyArchive 还会检查是否有文件已从归档文件集中被删除。如果检测到文件被删除，则将打印一条消息，说明验证已失败。如果未检测到文件被篡改或被删除，将返回一条消息，说明归档文件的验证已成功完成。

注 如果以无管理员权限的用户身份运行 amverifyarchive，可能会出错。

VerifyArchive 语法

所有的参数选项都是必需的。其语法如下所示：

```
VerifyArchive -l logName -p path -u uname -w password
```

VerifyArchive 选项

logName

logName 指要验证的日志的名称 （例如， amConsole、 amAuthentication 等等）。 VerifyArchive 将验证给定 logName 的访问日志和错误日志。例如，如果指定了 amConsole，验证器将验证 amConsole.access 和 amConsole.error 文件。也可以将 logName 指定为 amConsole.access 或 amConsole.error，从而仅对相应的日志进行验证。

path

path 为存储日志文件的完整目录路径。

uname

uname 为 Identity Server 管理员的用户 ID。

password

password 为 Identity Server 管理员的口令。

第 16 章

amsecuridd 帮助器

本章介绍有关 amsecuiridd 帮助器的信息，包含以下内容：

amsecuridd 帮助器命令行可执行文件

使用 Security Dynamic ACE/Client C API 和 amsecruidd 帮助器 （用于在 Identity Server SecurID 验证模块和 SecurID 服务器之间进行通信）来实现 Identity Server SecurID 验证模块。 SecurID 验证模块通过打开到 localhost:57943 的套接字调用 amsecuridd 守护程序以侦听 SecurID 验证请求。

注 57943 为默认端口号。如果此端口号已经使用，您可以在 SecurID 验证模块中的 SecurID 帮助器验证端口属性中指定其他端口号。此端口号在所有组织中必须唯一。

由于到 amsecuridd 的接口经 stdin 后为明文形式，所以只允许本地主机连接。amsecuridd 使用后端的 SecurID 远程 API （版本 5.x）进行数据加密。

amsecuridd 帮助器在编号为 58943 的端口上侦听 （默认情况下）以接收其配置信息。如果该端口已经使用，您可以在 AMConfig.properties 文件 （默认情况下，位于 *IdentityServer_base*/SUNWam/config/）中的 securidHelper.ports 属性中更改端口。 securidHelp.ports 属性包含针对每个 amsecuridd 帮助器实例的以空格分隔的端口的列表。保存对 AMConfig.properties 的更改后，请立即重新启动 Identity Sever。

注 对于每个与单独的 ACE/Server （包含不同的 sdconf.rec 文件）进行通信的组织，都应当有一个单独的 amsecuridd 的实例运行。

amsecuridd 语法

其语法如下所示：

```
amsecuridd [-v] [-c portnum]
```

amsecuridd 选项

verbose (-v)

打开详细模式并登录到 /var/opt/SUNWam/debug/securidd_client.debug。

configure portnumber (-c portnm)

配置侦听端口号。默认端口为 58943。

运行 amsecuridd 帮助器

默认情况下， amsecuridd 位于 *IdentityServer_base*/SUNWam/share/bin。要在默认端口上运行帮助器，请输入以下命令 （不需要选项）：

```
./amsecuridd
```

要在非默认端口上运行帮助器，请输入以下命令：

```
./amsecuridd [-v] [-c portnm]
```

也可以通过 amserver 命令行实用程序运行 amsecuridd （但它只在默认端口上运行）。

必需的库

要运行帮助器，需要以下库 （大部分可以在 /usr/lib/ 中的操作系统中找到）：

- libnsl.so.1
- libthread.so.1
- libc.so.1
- libdl.so.1
- libmp.so.2
- librt.so.1
- libaio.so.1
- libmd5.so.1

注 将 LD_LIBRARY_PATH 设置为 *IdentityServer_base*/Sunwam/lib/ 以找到 libaceclnt.so。

第 IV 部分

属性参考

本部分是 《Sun Java System Identity Server 管理指南》的第四部分 “属性参考”。其中介绍了在 Identity Server 的默认服务中配置的属性。本部分包含以下各章：

- 第 313 页的 “平台服务属性”
- 第 317 页的 “策略配置服务属性”
- 第 327 页的 “SAML 服务属性”
- 第 335 页的 “会话服务属性”
- 第 341 页的 “用户属性”

第 17 章

管理服务属性

管理服务由全局属性和组织属性组成。全局属性所采用的值将被应用到整个 Sun Java System Identity Server 配置中，并被所有已配置的组织所继承。由于全局属性的目的在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。组织属性所采用的值是各个已配置的组织的默认值，当服务注册到组织时，这些值可以更改。组织属性不会被组织项继承。管理属性可分为：

全局属性

管理服务中的全局属性包括：

- 第 220 页的 “启用管理组”
- 第 220 页的 “启用符合用户删除”
- 第 220 页的 “动态管理角色 ACI”
- 第 222 页的 “用户配置文件服务类”
- 第 222 页的 “DC 节点属性列表”
- 第 223 页的 “用于删除的对象的搜索过滤器”
- 第 223 页的 “默认用户容器”
- 第 223 页的 “默认组容器”
- 第 223 页的 “默认代理容器”

启用联合管理

选中该字段将启用联合管理。默认情况下将选中该字段。要禁用此功能，请取消选择该字段。控制台中将不再显示 “联合管理服务”选项卡。

启用用户管理

选中该字段将启用用户管理。默认情况下将启用该字段。

显示用户容器

该属性用于指定是否在 Identity Server 控制台中显示 “用户容器”。如果选中该选项，组织、容器和组容器的 “查看”菜单中将显示 “用户容器”菜单选项。仅在平面结构的 DIT 的顶层才会显示 “用户容器”。

用户容器是包含用户配置文件的组织单元。建议在 DIT 中只使用一个用户容器，并利用角色的灵活性来管理帐户和服务。 Identity Server 控制台在默认情况下会隐藏用户容器。但是，如果 DIT 中有多个用户容器，请选择 “显示用户容器”以将用户容器显示为 Identity Server 控制台中的管理对象。

在视图菜单中显示容器

该属性用于指定是否在 Identity Server 控制台的 “查看”菜单中显示所有容器。默认值是 `false`。管理员可以选择以下两个值之一：

- `false`（未选中复选框）- 不在组织和其他容器顶层的 “查看”菜单的选择项中列出容器。
- `true`（选中复选框）- 在组织和其他容器顶层的 “查看”菜单的选择项中列出容器。

显示组容器

该属性用于指定是否在 Identity Server 控制台中显示 “组容器”。如果选中该选项，组织、容器和组容器的 “查看”菜单中将显示 “组容器”菜单选项。组容器是组的组织单元。

管理的组类型

该选项用于指定通过控制台创建的是静态订阅组还是动态订阅组。控制台将创建并显示静态订阅组和/或动态订阅组。（不管为这个属性指定了何值，始终都支持过滤组。）默认值是 Dynamic。

- 通过使用 `groupOfNames` 或 `groupOfUniqueNames` 对象类，静态组明确列出每个组成员。组条目包含组中每个成员的 `uniqueMember` 属性。可以手动添加静态组成员；用户条目本身将保持不变。静态组适用于成员较少的组。
- 动态组使用的是每个组成员条目中的 `memberOf` 属性。通过使用 LDAP 过滤器来搜索并返回所有包含 `memberOf` 属性的条目，可以生成动态组成员。动态组适用于成员较多的组。

- 过滤组使用 LDAP 过滤器来搜索并返回符合过滤器要求的成员。例如，过滤器可以生成具有特定 uid (`uid=g*`) 或电子邮件地址 (`email=*@sun.com`) 的成员。在示例中， LDAP 过滤器将分别返回 uid 以 `g` 开头和电子邮件地址以 `sun.com` 结尾的所有用户。只能在 “用户管理”视图中通过选择 “过滤成员”来创建过滤组。

管理员可以选择以下选项之一：

- `Dynamic` - 通过 “按订阅指定成员”选项创建的将是动态组。
- `Static` - 通过 “按订阅指定成员”选项创建的将是静态组。

默认角色权限 (ACI)

该属性定义用于在创建新角色时授予管理员特权的默认访问控制指令 (ACI) 或*权限*列表。可以根据必需的特权级别来选择某个 ACI。 Identity Server 在出厂时设置了四种默认角色权限：

无权限

对角色不设置权限。

组织管理员

组织管理员拥有对已配置的组织中所有条目的读写权限。

组织帮助台管理员

组织帮助台管理员拥有对已配置的组织中所有条目的读取权限以及对 `userPassword` 属性的写入权限。

组织策略管理员

组织策略管理员拥有对组织中所有策略的读写权限。组织策略管理员不能创建对等组织的侯选策略。

注 使用 `aci_name | aci_desc | dn:aci ## dn:aci ## dn:aci` 格式定义角色，其中：

- *aci_name* 是 ACI 的名称，
- *aci_desc* 是对这些 ACI 允许的权限的说明。为了使说明更加浅显易懂，假定该说明的阅读者并不了解 ACI 或其他目录概念。

aci_name 和 *aci_desc* 是 `amAdminUserMsgs.properties` 文件中包含的 i18n key。控制台中显示的值来自 `.properties` 文件，可以使用这两个关键字来检索这些值。

- *dn:aci* 代表用 ## 分隔的 DN 和 ACI 对。 Identity Server 将在关联的 DN 条目中设置各个 ACI。该格式还支持可以代替值的标记 （否则需要在 ACI 中实际指定值）：ROLENAME、 ORGANIZATION、 GROUPNAME 和 PCNAME。使用这些标记您可以非常灵活地定义角色，以将其用作默认角色。当基于某个默认角色创建角色时， ACI 中的标记将解析为从新角色的 DN 中提取的值。

启用域组件树

域组件树 （DC 树）是许多 Sun Java System 组件使用的特定 DIT 结构，用于在 DNS 名称与组织的条目之间建立映射。

如果在创建组织时输入了组织的 DNS 名称，则启用该选项将创建组织的 DC 树条目。“创建组织”页面中将显示 “DNS 名称”字段。该选项仅适用于顶层组织，对于子组织将不显示该选项。

通过 Identity Server SDK 对组织树中的 `inetdomainstatus` 属性所作的任何状态更改将会更新相应的 DC 树条目状态。（不是通过 Identity Server SDK 进行的状态更新将不会同步进行。）例如，如果创建一个 DNS 名称属性为 sun.com 的新组织：`sun`，则将在 DC 树中创建以下条目：

`dc=sun,dc=com,o=internet,`*root suffix*

通过在 `AMConfig.properties` 中设置 `com.iplanet.am.domaincomponent`，可以选择性地配置 DC 树的根后缀。默认情况下，它将被设置成 Identity Server 的根。如果需要其他后缀，则需要使用 LDAP 命令创建后缀。需要修改创建组织的管理员的 ACI，以使他们能够无限制地访问新的 DC 树根。

启用管理组

该选项用于指定是否创建 DomainAdministrators 和 DomainHelpDeskAdministrators 组。如果选中该选项 (`true`)，将创建这些组，并将其分别与组织管理员角色和组织帮助台管理员角色关联。创建成功后，当在某个关联的角色中添加或删除用户时，对应的组中也将自动添加或移除该用户。但是该操作不能反向进行。当在其中的某个组中添加或移除用户时，不会在该用户的关联角色中添加或移除该用户。

只有在启用该选项后创建的组织中才能创建 DomainAdministrators 和 DomainHelpDeskAdministrators 组。

注 该选项不适用于子组织，但 `root org` 除外。对于 `root org`，将创建 ServiceAdministrators 和 ServiceHelpDeskAdministrators 组，并将其分别与顶层管理员和顶层帮助台管理员角色关联。上面的操作同样适用于该组织。

启用符合用户删除

该选项指定是从目录中删除用户条目还是只将其标记为已删除。如果是在选中该选项 (`true`) 的情况下删除用户条目，该用户条目仍将存在于目录中，只是将被标记为已删除。Directory Server 搜索时不会返回标记为已删除的用户条目。如果未选定该选项，将会从目录中删除用户条目。

动态管理角色 ACI

该属性用于定义管理员角色的访问控制指令，其中的管理员角色是在使用 Identity Server 配置组或组织时动态创建的。这些角色用于为创建的特定条目分组授予管理特权。仅在该属性列表中才能修改默认 ACI。

警告 组织级别的管理员拥有比组管理员更大的权限。但是，如果在默认情况下将某用户添加到组管理员角色中，则该用户可以修改组中任何人员的口令。其中包括同时是该组中成员的任何组织管理员。

容器帮助台管理员

容器帮助台管理员角色拥有对组织单元内所有条目的读取权限，但仅对自身容器单元中用户条目的 `userPassword` 属性拥有写入权限。

组织帮助台管理员

组织帮助台管理员拥有对组织中所有条目的读取权限以及对 `userPassword` 属性的写入权限。

注 创建一个子组织时，请注意要在该子组织中创建管理角色，而不是在父组织中创建管理角色。

容器管理员

容器管理员角色拥有对 LDAP 组织单元中所有条目的读写权限。在 Identity Server 中， LDAP 组织单元通常被称为容器。

组织策略管理员

组织策略管理员具有对所有策略的读写权限，可以创建、指定、修改和删除自身组织内的所有策略。

用户容器管理员

默认情况下，新创建的组织中的所有用户条目都是该组织的 “用户容器”的成员。“用户容器管理员”对该组织的 “用户容器”中的所有用户条目都具有读写权限。请注意，该角色 “并不”具有对包含角色和组 DN 的属性的读写权限，因此他们不能修改角色和组的属性，也不能从角色或组中移除用户。

注 可以使用 Identity Server 配置其他容器，以包含用户条目、组条目甚至其他容器。要将管理员角色应用到配置组织之后创建的容器，请使用默认的容器管理员角色或容器帮助台管理员角色。

组管理员

组管理员对特定组的所有成员具有读写权限，可以创建新用户、将用户指定到自己所管理的组以及删除自己创建的用户。

创建组时，将自动生成组管理员角色，并赋予管理组所必需的权限，但不会将角色自动指定到组成员。角色必须由组创建者或任何拥有 “组管理员角色”访问权限的人员来指定。

顶层管理员

顶层管理员拥有对顶层组织中所有条目的读写权限。换句话说，顶层管理员角色具有 Identity Server 应用程序内所有配置主体所拥有的特权。

组织管理员

组织管理员拥有对组织中所有条目的读写权限。创建组织时将自动生成组织管理员角色，该角色拥有管理组织所必需的权限。

用户配置文件服务类

该属性列出了 “用户配置文件”页面中具有自定义显示的服务。对于某些服务来说，由控制台生成的默认显示不能完全满足需要。该属性为任意服务创建自定义显示，并完全控制显示信息的内容和方式。其语法如下所示：

service name | *relative url*

注 “创建用户”页面中将不会显示该属性中列出的服务。必须在 “用户配置文件”页面中执行自定义服务显示的所有数据配置。

DC 节点属性列表

该字段用于定义当创建对象时将在 DC 树条目中设置的属性集。默认参数包括：

- maildomainwelcomemessage
- preferredmailhost
- mailclientattachmentquota
- mailroutingsmarthost

- mailroutingsmarthost
- mailroutingsmarthost
- mailaccessproxyreplay
- preferredlanguage
- domainuidseparator
- maildomainmsgquota
- maildomainallowedserviceaccess
- preferredmailmessagestore
- maildomaindiskquota
- maildomaindiskquota
- objectclass=maildomain
- mailroutinghosts

用于删除的对象的搜索过滤器

该字段定义当启用用户符合移除模式时，用于要删除的对象的搜索过滤器。

默认用户容器

此属性用于指定将在其中创建用户的默认用户容器。

默认组容器

此属性用于指定将在其中创建组的默认组容器。

默认代理容器

此属性用于指定将在其中创建代理的默认代理容器。

组织属性

管理服务中的组织属性包括：

组默认用户容器

该字段用于指定在创建用户时放置他们的默认用户容器。该字段没有默认值。其有效值是用户容器的 DN。有关用户容器属性为空时的替代顺序，参见组用户容器列表属性下的说明。

组用户容器列表

该字段用于指定用户容器列表，组管理员在创建新用户时会从中选择用户容器。如果目录树中存在多个用户容器，则可以使用该列表。（如果没有在这个列表和 “组默认用户容器” 字段中指定 “用户容器”，则将在默认的 Identity Server 用户容器 `ou=people` 中创建用户。）该字段不存在默认值。该属性的语法如下所示：

dn of group | *dn of people container*

注 创建用户时，将查看要在其中放置用户条目的容器的该属性。如果该属性为空，则检查容器的 “组默认用户容器” 属性。如果后一个属性也为空，将在 `ou=people` 中创建用户。

用户配置文件显示类

该属性指定显示 “用户配置文件” 页面时， Identity Server 控制台使用的 Java 类。

最终用户配置文件显示类

该属性用于指定显示 “最终用户配置文件” 页面时， Identity Server 控制台使用的 Java 类。

在 “用户配置文件” 页面中显示角色

该选项指定是否在用户的 “用户配置文件” 页面中显示指定给用户的角色列表。如果值为 `false` （即未选中该选项），则 “用户配置文件” 页面将只对管理员显示用户的角色。默认值是 `false`。

在 “用户配置文件”页面中显示组

该选项指定是否在用户的 “用户配置文件”页面中显示指定给用户的组列表。如果值为 `false`（即未选中该选项），则 “用户配置文件”页面将只对管理员显示用户的组。默认值是 `false`。

对组启用用户自订阅

该选项用于指定用户是否能够将自身添加到可以自由订阅的组。如果值为 false，则 “用户配置文件”页面将只允许管理员修改用户的组成员资格。默认值是 `false`。

注 仅当选定在 “用户配置文件”页面中显示组选项时，此选项才可用。

用户配置文件显示选项

该菜单用于指定 “用户配置文件”页面中显示的服务属性。管理员可以选择以下选项之一：

- `UserOnly` - 显示指定给用户的服务的可查看 “用户”模式属性。

  属性包含关键字 “Display”时，用户可以查看用户服务属性。有关详细信息，参见 《*Identity Server Developer's Guide*》。

- `Combined` - 显示指定给用户的服务的可查看 “用户”和 “动态”模式属性。

用户创建默认角色

该列表用于定义将被自动指定给新创建的用户的角色。该字段没有默认值。管理员可以输入一个或多个角色的 DN。

注 该字段只接受完整的独特名称地址，不接受角色名称。角色只能是 Identity Server 角色，而不能是 LDAP (Directory Server) 角色。

“管理控制台”选项卡

此字段列出要显示在控制台顶部的模块的 Java 类。语法是 `i18N key | java class name`。（i18N key 是 “查看”菜单中条目的本地化名称。）

搜索返回的结果的最大数目

该字段定义搜索返回的结果的最大数目。默认值为 100。

警告 将该属性设置为较大值时，请参考本注意。有关属性值大小限制的信息，参见位于以下位置的 *Sun Java System Directory Server Installation and Tuning Guide*：

`http://docs.sun.com/db/doc/816-6697-10`

搜索超时

该字段用于定义在执行多长时间 （以秒为单位）后搜索将超时。它可用于终止可能耗时过长的搜索。达到最大搜索时间后，将返回错误信息。默认值是 5 秒。

JSP 目录名称

该字段用于指定包含 `.jsp` 文件的目录名称，该 `.jsp` 文件用于构造控制台，以使组织具有一个不同的外观 （自定义）。 `.jsp` 文件需要复制到该字段指定的目录中。

联机帮助文档

该字段列出将在 Identity Server 主帮助页上创建的联机帮助链接。这样，其他应用程序也可以在 Identity Server 页面中添加自己的联机帮助链接。该属性的格式如下：

linki18nkey | *html page to load when clicked* | *i18n properties file* | *remote server*

注 其中*远程服务器*是可选变量，可用于指定联机帮助文档所在的远程服务器。

例如：

```
IdentityServer Help | /AMAdminHelp.html | amAdminModuleMsgs
```

必需的服务

该字段列出创建用户条目时向其动态添加的服务。管理员可以选择创建时要添加的服务。

该属性不适用于控制台，但适用于 Identity Server SDK。动态创建和通过 amadmin 命令行实用程序创建的用户，将被指定此属性中列出的服务。

用户搜索关键字

该字段用于定义在显示从简单搜索返回的用户时使用的属性名称。该属性的默认值是 cn。例如，如果该属性使用默认值，则：

如果在浏览框的 “名称” 字段中输入 j*，将显示名称以 “j” 或 “J” 开头的用户。

用户搜索返回属性

该字段定义当显示简单搜索返回的用户时，使用的属性名，默认值为 uid cn。此时将显示用户 ID 和用户的全名。

列出的第一个属性名称还将作为对要返回的用户集进行排序时使用的关键字。要防止性能下降，请使用其值在用户条目中进行设置的属性。

用户创建通知列表

该字段用于定义在创建新用户时，要向其发送通知的电子邮件地址列表。可以指定多个电子邮件地址，语法如下：

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

通过使用 |locale 选项，通知列表还可以接受不同的语言环境。例如，将通知发送到在法国的管理员：

someuser@example.com|fr|fr

有关语言环境的列表，参见第 249 页的表 20-1。

注 通过修改 amProfile.properties（默认情况下位于 IdentityServer_base/SUNWam/locale 中）中的属性 497，可以更改发送者的电子邮件 ID。

用户删除通知列表

该字段用于定义在删除用户时，要向其发送通知的电子邮件地址列表。可以指定多个电子邮件地址，语法如下：

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

通过使用 |locale 选项，通知列表还可以接受不同的语言环境。例如，将通知发送到在法国的管理员：

someuser@example.com|fr|fr

有关语言环境的列表，参见第 249 页的表 20-1。

注 通过修改 amProfile.properties（默认情况下位于 IdentityServer_base/SUNWam/locale 中）中的属性 497，可以更改发送者的电子邮件 ID。默认的发送者 ID 是 DSAME。

用户修改通知列表

该字段用于定义属性及其关联的电子邮件地址列表。如果修改了列表中定义的用户属性，将向该属性关联的电子邮件地址发送通知。每个属性都可以有不同的关联地址集。可以指定多个电子邮件地址，语法如下：

```
attrName e-mail|locale|charset e-mail|locale|charset .....
attrName e-mail|locale|charset e-mail|locale|charset .....
```

`self` 关键字可以用于代替某个地址。这时将向其配置文件被修改的用户发送电子邮件。

例如：

```
manager someuser@sun.com|self|admin@sun.com
```

邮件将被发送到 `manager` 属性中指定的地址：`someuser@sun.com`、 `admin@sun` 以及修改用户的人员 (`self`)。

通过使用 `|locale` 选项，通知列表还可以接受不同的语言环境。例如，将通知发送到在法国的管理员：

```
manager someuser@sun.com|self|admin@sun.com|fr
```

有关语言环境的列表，参见第 249 页的表 20-1。

注 该属性名称与 Directory Server 方案中显示的名称相同，但与控制台中显示的名称不同。

每页可以显示的最大条目数

该属性允许您定义每页可以显示的最大行数。默认值是 25。例如，如果某个用户搜索返回 100 行，将用 4 页来显示该结果，每页上显示 25 行。

事件侦听程序类

该属性包含用于接收 Identity Server 控制台中创建、修改和删除事件的侦听程序的列表。

处理前和处理后的类

该字段通过插件定义实现类列表，这些插件会扩展 `com.iplanet.am.sdk.AMCallBack` 类，以接收在处理对用户、组织、角色和组的操作前和处理后之间的回叫。这些操作包括：

- 创建
- 删除
- 修改
- 将用户添加到角色/组
- 从角色/组中删除用户

必须输入插件的完整类名。例如：

```
com.iplanet.am.sdk.AMCallbacSample
```

然后，必须更改 Web 容器的类路径 （从 Identity Server 安装库），以包含插件类位置的完整路径。

启用外部属性获取

该选项启用插件的回叫以检索外部属性 （所有专用于外部应用程序的属性）。外部属性不会缓存在 Identity Server SDK 中，因此该属性允许您在各个组织级别启用属性检索。默认情况下，不启用该选项。

用户 ID 和口令验证插件类

此类提供了一种用户 ID 和口令验证插件机制。

需要由为用户验证用户 ID 和/或口令的实现插件模块来覆盖此类的方法。每当使用 Identity Server 控制台、 `amadmin` 命令行界面或使用 SDK 来添加或修改用户 ID 或口令值时，将调用该实现插件模块。

可以为每个组织配置扩展此类的插件。如果未为组织配置插件，将使用在全局级别上配置的插件。

如果插件的验证失败，则插件模块可能抛出异常，通知应用程序指示用户所提供的用户 ID 或口令中的错误。

第 18 章

匿名验证属性

匿名验证属性是组织属性。在 “服务配置”下匿名验证属性所采用的值将成为匿名验证模板的默认值。为组织注册服务之后，需要创建服务模板。组织的管理员可以在注册后更改默认值。组织属性不会被组织子树中的条目继承。匿名验证属性包括：

有效匿名用户列表

该字段包含登录时不需要提供证书的用户 ID 列表。如果用户的登录名称与此列表中的用户 ID 匹配，则允许访问并将会话分配给指定的用户 ID。

如果此列表为空，访问以下默认模块登录 URL 将作为默认匿名用户名被验证：

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name
```

如果此列表不为空，访问默认模块登录 URL （同上）将提示用户输入任意有效匿名用户名。

如果此列表不为空，则用户可以通过访问以下 URL 登录而无需进入登录页面：

protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name&IDToken1=< 有效匿名用户名 >

默认匿名用户名

如果有效匿名用户列表为空并且访问以下默认模块登录 URL，则该字段用于定义被指定会话的用户 ID：

protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name

默认值是 anonymous。还必须在组织中创建匿名用户。

注 如果有效匿名用户列表不为空，则可以使用默认匿名用户名中定义的用户登录而无需访问登录页面。可以通过访问以下 URL 来完成此操作：

protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name&IDToken1=<DefaultAnonymous User Name>

启用区分大小写的用户 ID

如果启用，该选项允许对用户 ID 区分大小写。默认情况下，不启用该属性。

验证级别

各种验证方法都单独设置了验证级别。验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。当 SSO 令牌传递到用户要访问的应用程序时，应用程序将根据存储的值来确定级别是否足以授予用户访问权限。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。默认值为 0。

注 如果未指定任何验证级别，核心验证属性 “默认验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，参见第 254 页的 “默认验证级别”。对于 2004Q2 发行版，此功能无法正常执行。但在先前的版本中，此功能可正常执行。

第 19 章

证书验证属性

证书验证属性是组织属性。在 “服务配置”下证书验证属性所采用的值将成为证书验证模板的默认值。为组织注册服务之后，需要创建服务模板。组织的管理员可以在注册后更改默认值。组织属性不会被组织子树中的条目继承。证书验证属性包括：

- 第 242 页的 “验证级别”

在 LDAP 中匹配证书

该选项用于指定是否检查用户登录时提交的证书是否存储在 LDAP Server 中。如果没有找到匹配的证书，用户将被拒绝访问。如果找到匹配的证书，且不需要其他验证，则允许用户访问。在默认情况下，证书验证服务不会检查用户证书。

注 Directory Server 中存储的证书不一定是有效的，证书撤回列表中也可能存在该证书。请参见第 238 页的 “将证书与 CRL 匹配”。但是， Web 容器可以在登录时检查用户提交的证书的有效性。

用于在 LDAP 中搜索证书的主题 DN 属性

该字段指定证书的 `SubjectDN` 值的属性，该属性将用于在 LDAP 中搜索证书。该属性必须唯一标识用户条目。搜索将使用实际值。默认值是 `CN`。

将证书与 CRL 匹配

该选项用于指定是否将用户证书与 LDAP Server 中的证书撤回列表 (CRL) 进行对照。 CRL 由发布者的 `SubjectDN` 中的其中一个属性名称来定位。如果 CRL 中存在该证书，用户将被拒绝访问；如果不存在，则允许用户继续进行操作。在默认情况下，该属性被禁用。

注 发生以下情况时，应该撤消证书：证书所有者的状态发生变化，不再拥有使用证书的权限；或证书所有者的专用密钥已经损坏。

用于在 LDAP 中搜索 CRL 的发送者 DN 属性

该字段指定接收到的证书的发布者 SubjectDN 值的属性，该属性将用于在 LDAP 中搜索 CRL。仅在启用 “将证书与 CRL 匹配”属性时，才能使用该字段。搜索将使用实际值。默认值是 CN。

用于 CRL 更新的 HTTP 参数

该字段用于指定进行 CRL 更新时从某个 servlet 获得 CRL 的 HTTP 参数。要获得这些参数，请与您的 CA 管理员联系。

启用 OCSP 验证

此参数通过与相应的 OCSP 响应器联系来启用要执行的 OCSP 验证。运行时，将按照以下步骤确定 OCSP 响应器：

- 如果 com.sun.identity.authentication.ocspCheck 为 true，并且在 com.sun.identity.authentication.ocsp.repsonder.url 属性中设置了 OCSP 响应器，则该属性的值将用作 OCSP 响应器。
- 如果将 com.sun.identity.authentication.ocspCheck 设置为 true，但没有在 AMConfig.properties 文件中设置属性值，则客户证书中提交的 OCSP 响应器将用作 OCSP 响应器。

如果将 com.sun.identity.authentication.ocspCheck 设置为 false，或者将 com.sum.identity.authentication.ocspCheck 设置为 true，但无法找到 OCSP 响应器，则不能执行 OCSP 验证。

注 在启用 OCSP 验证之前，请确保 Identity Server 计算机和 OCSP 响应器计算机的时间尽可能同步。而且， Identity Server 计算机的时间不能晚于 OCSP 响应器的时间。例如：

OCSP 响应器计算机 - 12:00:00 pm

Identity Server 计算机 - 12:00:30 pm

存储证书的 LDAP 服务器

该字段用于指定存储证书的 LDAP 服务器的名称和端口号。默认值是安装 Identity Server 时指定的主机名和端口号。可以使用存储证书的任意 LDAP 服务器的主机名和端口号。格式为：*hostname:port*。

LDAP 起始搜索 DN

该字段指定节点的 DN，应从该节点开始搜索用户证书。该字段没有默认值。它接受任何有效的 DN。如果指定多个条目，条目前面必须带有本地服务器名称。格式如下所示：

```
servername|search dn
```

对于多个条目

```
servername1|search dn servername2|search dn servername3|search dn...
```

如果同一搜索找到多个用户，则验证失败。

LDAP Server 主要用户

该字段用于指定存储证书的 LDAP Server 的主要用户 （通常是目录管理员）的 DN。该字段没有默认值，它接受任何有效的 DN。需要向主要用户授予读取和搜索 Directory Server 中存储的信息的权限。

LDAP Server 主要口令

该字段用于指定与 “LDAP Server 主要用户”字段中指定的用户相关联的 LDAP 口令。该字段没有默认值，它接受指定主要用户的有效 LDAP 口令。

注	目录中该值将存储为可读文本。

配置文件 ID 的 LDAP 属性

该字段用于指定 Directory Server 条目中与证书匹配的属性，其值将用于标识正确的用户配置文件。该字段不存在默认值，它接受用户条目中能够用作用户 ID 的任何有效属性 （例如 `cn`、 `sn` 等）。

使用 SSL 进行 LDAP 访问

该选项用于指定是否使用 SSL 来访问 LDAP 服务器。在默认情况下，证书验证服务不使用 SSL 来访问 LDAP 服务器。

用于访问用户配置文件的证书字段

该菜单指定应使用证书的 “主题 DN”中的哪个字段来搜索匹配的用户配置文件。例如，如果选择 `email address`，证书验证服务将搜索与用户证书中 `emailAddr` 属性匹配的用户配置文件。用户将使用匹配的配置文件进行登录。默认字段是 `subject CN`。该列表包含以下内容：

- email address
- subject CN
- subject DN
- subject UID
- other

用于访问用户配置文件的其他证书字段

如果将 “用于访问用户配置文件的证书字段”属性的值设置为 `other`，则该字段指定将从接收到的证书的 `subjectDN` 值中选择的属性。验证服务将搜索与该属性值匹配的用户配置文件。

可信赖的远程主机

该属性定义可信赖的主机列表，这些主机是可信赖的，可以向 Identity Server 发送证书。 Identity Server 必须检验证书是否是由这些主机中的某一台发送的。此配置仅与 Sun Java System Portal Server 一起使用。

此属性接受以下值：

- **none**。此属性被禁用。这是默认设置。
- **any**。从任意客户机 IP 地址接受 Portal Server 网关式样证书验证。
- ***IP ADDR***。列出要从该处接受 Portal Server 网关式样证书验证请求的 IP 地址（网关的 IP 地址）。可以基于组织对该属性进行配置。

SSL 端口号

该属性指定安全套接字层的端口号。目前，该属性只由网关 servlet 使用。在添加或更改 SSL 端口号之前，请参见《*Identity Server Developer's Guide*》第 7 章中的“Policy-Based Resource Management”一节。

验证级别

各种验证方法都单独设置了验证级别。验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。当 SSO 令牌传递到用户要访问的应用程序时，应用程序将根据存储的值来确定级别是否足以授予用户访问权限。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。默认值为 0。

注 如果未指定任何验证级别，核心验证属性“默认验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，参见第 254 页的“默认验证级别”。对于 2004Q2 发行版，此功能无法正常执行。但在先前的版本中，此功能可正常执行。

第 20 章

核心验证属性

核心验证服务是所有默认验证服务的基本服务，也是所有自定义验证模块属性的基本服务。需要为每个希望使用任意形式验证的组织配置核心验证服务。核心验证属性由全局属性和组织属性组成。全局属性所采用的值被应用到整个 Sun Java System Identity Server 配置，并被每个已配置的组织所继承。（由于全局属性的目的在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。）在“服务配置”下组织属性所采用的值将成为核心验证模板的默认值。为组织添加服务之后，需要创建服务模板。组织的管理员可以在添加后更改默认值。组织属性不会被组织中的条目所继承。核心验证属性分为：

全局属性

核心验证服务中的全局属性包括：

可插接的验证模块类

该字段用于指定 Identity Server 平台中所有已配置的组织都可以使用的验证模块的 Java 类。默认情况下，包括 LDAP、 SafeWord、 SecurID、应用程序、匿名、 HTTP Basic、成员资格、 Unix、证书、 NT、 RADIUS 和 Windows 桌面 SSO。您可以通过实现 AMLoginModule SPI 或 JAAS LoginModule SPI 来写入自定义验证模块。有关详细信息，请参见 《*Identity Server Developer's Guide*》。要定义新的服务，该字段必须使用文本字符串以指定每个新验证服务的完整类名 （包括软件包名称）。

客户机支持的验证模块

该属性用于指定特定客户机所支持的验证模块列表。格式如下所示：

```
clientType | module1,module2,module3
```

当启用了客户机检测时，该属性有效。

LDAP 连接池大小

该属性用于指定特定 LDAP 服务器与端口所使用的最小和最大连接池。该属性仅适用于 LDAP 和成员资格验证服务。格式如下所示：

```
host:port:min:max
```

注 该连接池与 `serverconfig.xml` 中配置的 SDK 连接池不同。

LDAP 连接池的默认大小

该属性用于设置与所有 LDAP 验证模块配置一起使用的连接池的默认最大值和最小值。如果 “LDAP 连接池大小”属性中存在主机和端口条目，最小值和最大值设置将不使用 “LDAP 连接池的默认大小”中的相应值。

组织属性

核心验证服务中的组织属性包括：

组织验证模块

该列表用于指定组织可以使用的验证模块。每个管理员均可以为其特定组织选择验证类型。虽然多个验证模块使用起来比较灵活，但是用户必须确保其登录设置适用于选定的验证模块。默认验证模块为 LDAP。 Identity Server 包括的验证服务有：

- LDAP
- 证书
- 匿名
- HTTP Basic
- 成员资格
- NT
- SafeWord
- RADIUS
- SecurID
- Unix
- Windows 桌面 SSO

注 管理员必须在已创建的组织中创建并通知核心验证模块模板，以使该组织正常工作。

用户配置文件

该选项允许您为用户配置文件指定选项。

- 必需 - 指定对于成功验证，与 Identity Server 一起安装的本地 Directory Server 中需要存在用户配置文件，验证服务才会发布 SSOToken。
- 动态创建 - 指定对于成功验证，如果尚无用户配置文件，验证服务将创建用户配置文件，然后发布 SSOToken。用户配置文件创建于与 Identity Server 一起安装的本地 Directory Server 中。

- 忽略 - 指定对于成功验证，验证服务不需要用户配置文件就可以发布 SSOToken。

管理员验证配置

单击 “编辑”链接允许您仅为管理员定义验证服务。管理员是需要访问 Identity Server 控制台的用户。如果需要将管理员的验证模块与最终用户的验证模块区别开来，则可以使用该属性。在 Identity Server 控制台被访问时，将使用该属性中配置的模块。例如：

```
http://servername.port/console_deploy_uri
```

用户配置文件动态创建默认角色

如果在第 246 页的 “用户配置文件”特征中选中了 “动态创建”，则该字段将指定为新用户所指派的角色，这些用户的配置文件已创建完毕。该字段没有默认值。管理员必须指定要分配给新用户的角色的 DN。

注 所指定的角色必须位于正在为其配置验证的组织下。该角色可以是 Identity Server 角色，也可以是 LDAP 角色，但不能是过滤后的角色。

启用持久 Cookie 模式

该选项用于确定用户能否重新启动浏览器并仍返回其经过验证的会话。通过启用 “启用持久 Cookie 模式”可以保留用户会话。启用 “启用持久 Cookie 模式”之后，直到用户会话的持久 Cookie 过期或用户明确注销后，该用户会话才会过期。过期时间是在 “持久 Cookie 最长时间”中指定的。默认值是 “持久 Cookie 模式”未启用，且验证服务仅使用内存 Cookie。

注 客户机必须明确申请持久 Cookie，方法是使用登录 URL 中的 `iPSPCookie=yes` 参数。

持久 Cookie 最长时间

该字段用于指定经过多长时间后持久 Cookie 过期。(必须通过选中相应复选框启用“启用持久 Cookie 模式”。）该时间间隔从成功验证用户的会话时起开始计算。默认值为 2147483 （以秒为单位）。该字段可以是 0 与 2147483 之间的任意整数值。

所有用户的用户容器

用户验证成功后，将检索用户的配置文件。该字段中的值用于指定搜索配置文件的位置。通常情况下，该值将是默认用户容器的 DN。会自动将添加到组织的所有用户条目添加到组织的默认 “用户容器”中。默认值是 ou=People，通常情况下包括组织名称和根后缀。该字段可以接受任何组织单元的有效 DN。

注

验证通过以下途径搜索用户配置文件：

- 在默认的用户容器中搜索，然后
- 在默认的组织中搜索，然后
- 使用 “别名搜索属性名称”属性在默认组织中搜索用户。

最后一种搜索方式适用于 SSO 情形，在这种情形中，用于验证的用户名可能不是配置文件中的命名属性。例如，用户可能使用 jn10191 的 Safeword ID 进行验证，但配置文件却是 uid=jamie。

别名搜索属性名称

用户验证成功后，将检索用户的配置文件。该字段用于指定次 LDAP 属性，当根据第 249 页的 “用户命名属性”中指定的首选 LDAP 属性进行搜索时，如果没有找到匹配的用户配置文件，将使用该字段指定的属性进行搜索。该属性主要用于当验证模块返回的用户标识与 “用户命名属性”中指定的用户标识不相同时。例如，RADIUS 服务器可能返回 abc1234，但用户名却是 abc。该属性不存在默认值，它可以接受任何有效的 LDAP 属性 （例如 cn）。

用户命名属性

用户验证成功后，将检索用户的配置文件。该属性的值指定用于进行搜索的 LDAP 属性。默认情况下， Identity Server 假定用户条目是由 `uid` 属性标识的。如果您的 Directory Server 使用的是其他属性 （例如 `givenname`），请在该字段中指明属性名称。

默认验证语言环境

该字段用于指定验证服务要使用的默认语言子类型。默认值为 `en_US`。可以在表 20-1 中找到有效语言子类型的列表。

为了使用其他语言环境，首先必须创建该语言环境的所有验证模板。然后需要为这些模板创建新的目录。有关详细信息，请参见 《*Identity Server Developer's Guide*》中的第三章 “Authentication Service”。

表 20-1 支持的语言环境

语言标记	语言
af	南非荷兰语
be	白俄罗斯语
bg	保加利亚语
ca	加泰罗尼亚语
cs	捷克斯洛伐克语
da	丹麦语
de	德语
el	希腊语
en	英语
es	西班牙语
eu	巴斯克语
fi	芬兰语
fo	法罗语
fr	法语

表 20-1 支持的语言环境 *(续)*

语言标记	语言
ga	爱尔兰语
gl	加利西亚语
hr	克罗地亚语
hu	匈牙利语
id	印度尼西亚语
is	冰岛语
it	意大利语
ja	日语
ko	朝鲜语
nl	荷兰语
no	挪威语
pl	波兰语
pt	葡萄牙语
ro	罗马尼亚语
ru	俄语
sk	斯洛伐克语
sl	斯洛文尼亚语
sq	阿尔巴尼亚语
sr	塞尔维亚语
sv	瑞典语
tr	土耳其语
uk	乌克兰语
zh	汉语

组织验证配置

该属性用于设置组织的验证模块。默认验证模块为 LDAP。通过单击 “编辑” 链接可以选择一个或多个验证模块。如果选择了多个模块，则用户需要成功通过所有选定模块的验证。

该属性中配置的模块用于对以 /server_deploy_uri/UL/Login 形式访问验证模块的用户进行验证。有关详细信息，请参见 《Identity Server Developer's Guide》。

启用登录失败锁定模式

该功能用于指定用户在第一次登录失败后是否可以尝试第二次验证。选择该属性将启用锁定功能，用户将只有一次验证的机会。默认情况下，不启用锁定功能。该属性与同锁定相关的属性和通知属性一起发挥作用。

登录失败锁定计数

该属性用于定义在 "登录失败锁定间隔" 中指定的时间间隔内，用户在被锁定之前试图进行验证的次数。

登录失败锁定间隔

该属性用于定义两次失败的登录尝试之间的时间 （以分钟为单位）。如果一次登录失败并且在锁定间隔内随后的一次登录仍失败，则锁定计数将加 1。否则，将重置锁定计数。

用于发送锁定通知的电子邮件地址

该属性用于指定发生用户锁定时将会接到通知的电子邮件地址。要向多个地址发送电子邮件通知，请用空格将每个电子邮件地址分隔开。

N 次失败后警告用户

该属性用于指定在 Identity Server 发送警告消息警告用户将被锁定之前，允许发生的验证失败次数。

登录失败锁定时间

该属性用于启用内存锁定。默认情况下，锁定机制将使 “锁定属性名称”中定义的用户配置文件失效 （一次登录失败后）。如果登录失败锁定时间的值大于 0，则将在指定的时间 （分钟数）内锁定其内存锁定和用户帐户。

锁定属性名称

该属性用于指定所有要设置为锁定的 LDAP 属性。还必须更改 “锁定属性值”中的值以启用该属性名称的锁定。默认情况下，在 Identity Server 控制台中 “锁定属性名称”为空。当用户被锁定并且登录失败锁定时间设置为 0 时，默认执行值为 `inetuserstatus` （LDAP 属性）和 `inactive`。

锁定属性值

该属性用于指定对于 “锁定属性名称”中定义的属性启用或禁用锁定。默认情况下，将 `inetuserstatus` 的值设置为无效。

默认成功登录 URL

该字段接受一系列的值，这些值用于指定验证成功后用户被重定向到的 URL。此属性的格式为 `clientType|URL`，尽管您可以只指定 URL 的值 （默认类型为 HTML）。成功登录 URL 设置于 `remote-auth.dtd` 中的 `LoginStatus` 元素中。有关详细信息，请参见 《*Identity Server Developer's Guide*》。

默认失败登录 URL

该字段接受一系列的值，这些值用于指定验证成功后用户被重定向到的 URL。此属性的格式是 `clientType|URL`，尽管您可仅指定 URL 的值 （默认类型为 HTML）。失败登录 URL 在 `remote-auth.dtd` 的 `LoginStatus` 元素中设置。有关详细信息，请参见 《*Identity Server Developer's Guide*》。

验证后处理类

该字段用于指定为成功或不成功登录自定义验证后处理所使用的 Java 类的名称。示例：

```
com.abc.authentication.PostProcessClass
```

Java 类必须实现以下 Java 接口：

```
com.sun.identity.authentication.spi.AMPostAuthProcessInterface
```

另外，必须将类所在的路径添加到 Web Server 的 “Java Classpath”属性中。

启用生成用户 ID 模式

该属性适用于成员资格验证模块。如果启用了该属性字段，则成员资格模块可以在自注册过程中生成特定用户的用户 ID （如果用户 ID 已经存在）。用户 ID 是从在 “可插接用户名生成器类”中指定的 Java 类生成的。

可插接用户名生成器类

该字段用于指定当启用了 “启用生成用户 ID 模式”时，用来生成用户 ID 的 Java 类的名称。

默认验证级别

验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。 SSO 令牌被提交到用户要访问的应用程序时，该应用程序使用存储的值来判断验证级别是否足够高，以确定是否允许用户访问。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。

验证级别应在组织的特定验证模板中进行设置。此处所述的 “默认验证级别”值仅当未在特定组织的验证模板的 “验证级别”字段中指定任何验证级别时才适用。 “默认验证级别”的默认值为 0。（该属性中的值不是由 Identity Server 使用，而是由可能选择使用它的外部应用程序所使用。）对于 2004Q2 发行版，此功能无法正常执行。但在先前的版本中，此功能可正常执行。

第 21 章

HTTP Basic 验证属性

HTTP Basic 验证属性是组织属性。在 “服务配置”下 HTTP Basic 验证属性采用的值将成为 HTTP Basic 验证模板的默认值。为组织注册服务之后，需要创建服务模板。组织的管理员可以在注册后更改默认值。组织属性不会被组织中的条目所继承。

HTTP Basic 验证属性包括：

验证级别

各种验证方法都单独设置了验证级别。验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。当 SSO 令牌传递到用户要访问的应用程序时，应用程序将根据存储的值来确定级别是否足以授予用户访问权限。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。默认值为 0。

注 如果未指定任何验证级别，核心验证属性 “默认验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 254 页的 “默认验证级别”。对于 2004Q2 发行版，此功能无法正常执行。但在先前的版本中，此功能可正常执行。

第 22 章

LDAP 验证属性

LDAP 验证属性是组织属性。在 “服务配置”下 LDAP 验证属性采用的值将成为 LDAP 验证模板的默认值。为组织注册服务之后，需要创建服务模板。组织的管理员可以在注册后更改默认值。组织属性不会被组织中的条目所继承。 LDAP 验证属性包括：

主 LDAP 服务器

该字段指定 Identity Server 安装过程中指定的主 LDAP 服务器的主机名和端口号。这是 LDAP 验证时搜索的首选服务器。格式为：`hostname:port`。（如果没有端口号，将采用 `389`）。

如果在多个域部署 Identity Server，可以按以下格式 （如果指定多个条目，条目前面必须带有本地服务器名称）指定 Identity Server 和 Directory Server 的特定实例之间的通信链接：

```
local_servername|server:port local_servername2|server:port ...
```

例如，如果您在不同位置 （`L1-machine1-IS` 和 `L2- machine2-IS`）部署两个 Identity Server，它们分别与 Identity Server 的不同实例 （`L1-machine1-DS` 和 `L2-machine2-DS`）进行通信，格式如下：

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

辅助 LDAP 服务器

该字段指定 Identity Server 平台上可用的辅助 LDAP 服务器的主机名和端口号。如果主 LDAP 服务器对验证请求不响应，则将会搜索辅助服务器。如果主服务器恢复正常， Identity Server 将切换回主服务器。格式仍为 `hostname:port`。如果指定多个条目，条目前面必须带有本地服务器名称。

警告 当验证来自远离 Identity Server 企业的 Directory Server 的用户时，主 LDAP 服务器和辅助 LDAP 服务器的端口都具有值十分重要。两个字段可以使用一个 Directory Server 位置的值。

起始用户搜索的 DN

该字段指定节点的 DN，将从该 DN 开始搜索用户。（为了获取较好性能， DN 应当尽可能明确。）默认值是目录树的根。可以接受任何有效的 DN。如果在 “搜索范围”属性中选择 OBJECT，则 DN 应指定配置文件所在级别的上一级。

如果指定多个条目，条目前面必须带有本地服务器名称。格式如下所示：

`servername|search dn`

对于多个条目

`servername1|search dn servername2|search dn servername3|search dn...`

如果同一搜索找到多个用户，则验证失败。

超级用户绑定的 DN

该字段用于指定用户的 DN，该用户将作为管理员被绑定到 “主 LDAP 服务器和端口”字段中指定的 Directory Server。验证服务需要进行该 DN 绑定，以便基于用户的登录 ID 搜索匹配的用户 DN。默认值为 `amldapuser`。可以接受任何有效的 DN。

在注销之前，请确保口令正确。因为如果口令不正确，您将被锁定。如果出现这种情况，您可以使用 `AMConfig.Properties` 文件中的 `com.iplanet.authentication.super.user` 属性中的超级用户 DN 登录。默认情况下，虽然要使用完整 DN，但使用 amAdmin 帐户可以正常登录。例如：

`uid_amAdmin,ou=People,`*`IdentityServer_base`*

超级用户绑定的口令

该字段指定在 “超级用户绑定的 DN”字段中指定的管理员配置文件的口令。该字段没有默认值。只有管理员的有效 LDAP 口令才会被认可。

超级用户绑定的口令 （确认）

对口令进行确认。

用于检索用户配置文件的 LDAP 属性

用户验证成功后，将检索用户的配置文件。该属性的值用于执行搜索。该字段指定要使用的 LDAP 属性。默认情况下， Identity Server 假定用户条目是由 `uid` 属性标识的。如果您的 Directory Server 使用的是其他属性 （例如 `givenname`），请在该字段中指明属性名称。

注 用户搜索过滤器将是 “搜索过滤器”属性与 “用于检索用户配置文件的 LDAP 属性”的组合。

用于搜索要进行验证的用户的 LDAP 属性

该字段会列出为即将验证的用户形成搜索过滤器时所要使用的属性，并允许用户使用用户条目中的多个属性进行验证。例如，如果该字段被设置成 `uid`、`employeenumber` 和 `mail`，则用户可以使用这些名称中的任意一个来进行验证。

用户搜索过滤器

该字段指定一个属性，用于在 “起始用户搜索的 DN”字段中搜索用户。它与 “用户条目命名属性”一起起作用。该字段没有默认值。可以接受任何有效的用户条目属性。

搜索范围

该菜单指明 Directory Server 中搜索匹配的用户配置文件时所用的级别号。从第 259 页的 “起始用户搜索的 DN”属性中指定的节点开始搜索。默认值为 `SUBTREE`。可以从列表中选择以下选项之一：

- OBJECT - 仅搜索指定的节点

- ONELEVEL - 搜索指定节点一级及其下面一级
- SUBTREE - 搜索指定节点及以下的所有条目

警告 即使子组织处于无效状态，子组织中的用户可能也能够登录。要避免这种情况，请确保将 “搜索范围”和 “基本 DN”设置成用户所属的特定组织。

对 LDAP 服务器启用 SSL 访问

该选项用于启用 SSL 来访问 “主/辅助 LDAP 服务器和端口”字段中指定的 Directory Server。默认情况下，不启用该属性，并且不使用 SSL 协议访问 Directory Server。但是，如果启用该属性，您可以绑定到非 SSL 服务器。

返回用户 DN 以进行验证

当 Identity Server 目录与为 LDAP 配置的目录相同时，则可能启用了该选项。如果启用了该选项， LDAP 验证模块将返回 DN，而不是 `userId`，并且不需要进行搜索。通常情况下，验证模块仅返回 `userId`，且验证服务搜索本地 Identity Server LDAP 中的用户。如果使用了外部 LDAP 目录，则通常不启用该选项。

LDAP 服务器检查间隔

该属性用于 LDAP 服务器故障回复。它定义了在检验 LDAP 主服务器是否正在运行之前，线程将 “休眠”的分钟数。

用户创建属性列表

当 LDAP 服务器被配置为外部 LDAP 服务器时，该属性用于 LDAP 验证模块。它包含本地和外部 Directory Server 之间的属性映射。该属性具有以下格式：

```
attr1|externalattr1
```

```
attr2|externalattr2
```

填充该属性后，将从外部 Directory Server 读取外部属性的值，并将这些值应用到内部 Directory Server 属性。仅当 “用户配置文件” 属性 （位于核心验证模块中）设置为 “动态创建”，并且本地 Directory Server 实例中不存在该用户时，才会在内部属性中设置外部属性的值。新创建的用户将包含内部属性的值 （在 “用户创建属性列表” 中指定），内部属性采用其映射的外部属性的值。

验证级别

各种验证方法都单独设置了验证级别。验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。当 SSO 令牌传递到用户要访问的应用程序时，应用程序将根据存储的值来确定级别是否足以授予用户访问权限。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。默认值为 0。

注 如果未指定任何验证级别，核心验证属性 “默认验证级别” 中指定的值将会存储到 SSO 令牌中。有关详细信息，参见第 254 页的 “默认验证级别”。对于 2004Q2 发行版，此功能无法正常执行。但在先前的版本中，此功能可正常执行。

第 23 章

成员资格验证属性

成员资格验证属性是组织属性。在 “服务配置”下成员资格验证属性采用的值将成为成员资格验证模板的默认值。为组织注册服务之后，需要创建服务模板。组织的管理员可以在注册后更改默认值。组织属性不会被组织子树中的条目继承。成员资格验证属性包括：

- 第 268 页的 “验证级别”

最小口令长度

该字段用于指定自注册过程中设置口令时要求的最小字符数。默认值为 8。

如果更改了该值，还应在以下文件的注册和错误文本中更改此值：

IdentityServer_base/locale/amAuthMembership.properties (PasswdMinChars *entry)*

默认用户角色

该字段用于指定分配给其配置文件是在自注册过程中创建的新用户的角色。该字段没有默认值。管理员必须指定要分配给新用户的角色的 DN。

注 所指定的角色必须位于正在为其配置验证的组织下。在自注册过程中，只能添加可以指派给用户的角色。所有其他 DN 将被忽略。该角色可以是 Identity Server 角色，也可以是 LDAP 角色，但不接受过滤的角色。

注册后的用户状态

该菜单用于指定服务是否立即可以供已自注册的用户使用。默认值为 Active，服务可供新用户使用。通过选中 Inactive，管理员不对新用户提供服务。

主 LDAP 服务器

该字段指定 Identity Server 安装过程中指定的主 LDAP 服务器的主机名和端口号。这是 LDAP 验证时搜索的首选服务器。格式为：hostname:port。（如果没有端口号，将采用 389）。

如果在多个域部署 Identity Server，可以按以下格式 （如果指定多个条目，条目前面必须带有本地服务器名称）指定 Identity Server 和 Directory Server 的特定实例之间的通信链接：

```
local_servername|server:port local_servername2|server:port ...
```

例如，如果您在不同位置 （L1-machine1-IS 和 L2-machine2-IS）部署两个 Identity Server，它们分别与 Identity Server 的不同实例 （L1-machine1-DS 和 L2-machine2-DS）进行通信，格式如下：

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

辅助 LDAP 服务器

该字段指定 Identity Server 平台上可用的辅助 LDAP 服务器的主机名和端口号。如果主 LDAP 服务器对验证请求不响应，则将会搜索辅助服务器。如果主服务器恢复正常， Identity Server 将切换回主服务器。格式仍为 `hostname:port`。如果指定多个条目，条目前面必须带有本地服务器名称。

警告 当验证来自远离 Identity Server 企业的 Directory Server 的用户时，主 LDAP 服务器和辅助 LDAP 服务器的端口都具有值十分重要。两个字段可以使用一个 Directory Server 位置的值。

起始用户搜索的 DN

该字段指定节点的 DN，将从该 DN 开始搜索用户。（为了获取较好性能， DN 应当尽可能明确。）默认值是目录树的根。可以接受任何有效的 DN。如果在 “搜索范围”属性中选择 OBJECT，则 DN 应指定配置文件所在级别的上一级。

如果使用了多个条目，条目必须以本地服务器名称为前缀。格式如下：

```
servername|search dn
```

对于多个条目

servername1|search dn servername2|search dn servername3|search dn...

如果同一搜索找到多个用户，则验证失败。

超级用户绑定的 DN

该字段用于指定用户的 DN，该用户将作为管理员被绑定到 “主 LDAP 服务器和端口”字段中指定的 Directory Server。验证服务需要进行该 DN 绑定，以便基于用户的登录 ID 搜索匹配的用户 DN。默认值为 amldapuser。可以接受任何有效的 DN。

超级用户绑定的口令

该字段指定在 “超级用户绑定的 DN”字段中指定的管理员配置文件的口令。该字段没有默认值。只有管理员的有效 LDAP 口令才会被认可。

超级用户绑定的口令 （确认）

对口令进行确认。

用于检索用户配置文件的 LDAP 属性

该字段用于指定用户条目命名惯例的属性。默认情况下， Identity Server 假定用户条目是由 uid 属性标识的。如果您的 Directory Server 使用的是其他属性 （例如 givenname），请在该字段中指明属性名称。

用于搜索要进行验证的用户的 LDAP 属性

该字段会列出为即将验证的用户形成搜索过滤器时所要使用的属性，并允许用户使用用户条目中的多个属性进行验证。例如，如果该字段被设置成 uid、employeenumber 和 mail，则用户可以使用这些名称中的任意一个来进行验证。

用户搜索过滤器

该字段指定一个属性，用于在 “起始用户搜索的 DN”字段中搜索用户。它与 “用户命名”属性共同发挥作用。该字段没有默认值。可以接受任何有效的用户条目属性。

搜索范围

该菜单指明 Directory Server 中搜索匹配的用户配置文件时所用的级别号。从第 265 页的 “起始用户搜索的 DN”属性中指定的节点开始搜索。默认值为 `SUBTREE`。可以从列表中选择以下选项之一：

- OBJECT - 仅搜索指定的节点
- ONELEVEL - 在指定节点级别及其下一级上搜索
- SUBTREE - 搜索指定节点及其下的所有条目

对 LDAP 服务器启用 SSL 访问

该选项用于启用 SSL 来访问 “主/辅助 LDAP 服务器和端口”字段中指定的 Directory Server。默认情况下未选中该复选框， SSL 协议不用于访问 Directory Server。

返回用户 DN 以进行验证

当 Identity Server 目录与为 LDAP 配置的目录相同时，则可能启用了该选项。如果启用了该选项， LDAP 验证模块将返回 DN，而不是 `userId`，并且不需要进行搜索。通常情况下，验证模块仅返回 `userId`，且验证服务搜索本地 Identity Server LDAP 中的用户。如果使用了外部 LDAP 目录，则通常不启用该选项。

验证级别

各种验证方法都单独设置了验证级别。验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。当 SSO 令牌传递到用户要访问的应用程序时，应用程序将根据存储的值来确定级别是否足以授予用户访问权限。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。默认值为 0。

注 如果未指定任何验证级别，核心验证属性 “默认验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 254 页的 “默认验证级别”。对于 2004Q2 发行版，此功能无法正常执行。但在先前的版本中，此功能可正常执行。

第 24 章

NT 验证属性

NT 验证属性是组织属性。在 “服务配置” 下 NT 验证属性采用的值将成为 NT 验证模板的默认值。为组织注册服务之后，需要创建服务模板。组织的管理员可以在注册后更改默认值。组织属性不会被组织子树中的条目继承。

要激活 NT 验证模块，必须下载 Samba Client 2.2.2 并将其安装到下面的目录：

IdentityServer_base/SUNWam/bin

Samba Client 是文件服务器和打印服务器，它将 Windows 计算机和 UNIX 计算机融合在一起而无需使用单独的 Windows NT/2000 服务器。有关该软件的详细信息及下载该软件，请访问 http://wwws.sun.com/software/download/products/3e3af224.html。

Red Hat Linux 随 Samba 客户机一起提供，它位于以下目录中：

/usr/bin

为了使用 Linux 的 NT 验证服务进行验证，请将客户机二进制文件复制到以下 Identity Server 目录：

IdentityServer_base/identity/bin

NT 验证属性包括：

- 第 270 页的 “NT 验证域”
- 第 270 页的 “NT 验证主机”
- 第 270 页的 “验证级别”

NT 验证域

该属性用于定义用户所属的域名。

NT 验证主机

该属性用于定义 NT 验证的主机名。主机名应是 netBIOS 名称，而不是全限定域名 (FQDN)。默认情况下， FQDN 的第一部分是 netBIOS 名称。

如果使用了 DHCP （动态主机配置协议），则可以在 Windows 2000 计算机上的 HOSTS 文件中加入合适的条目。

将基于 netBIOS 名称进行名称解析。如果您的子网上没有任何提供 netBIOS 名称解析的服务器，则应该对映射进行硬编码。

例如，主机名应是 `example1`，而不是 `example1.company1.com`。

验证级别

各种验证方法都单独设置了验证级别。验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。当 SSO 令牌传递到用户要访问的应用程序时，应用程序将根据存储的值来确定级别是否足以授予用户访问权限。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。默认值为 `0`。

注 如果未指定任何验证级别，核心验证属性 “默认验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，参见第 254 页的 “默认验证级别”。对于 2004Q2 发行版，此功能无法正常执行。但在先前的版本中，此功能可正常执行。

第 25 章

RADIUS 验证属性

RADIUS 验证属性是组织属性。在 “服务配置” 下 RADIUS 验证属性采用的值将成为 RADIUS 验证模板的默认值。为组织注册服务之后，需要创建服务模板。组织的管理员可以在注册后更改默认值。组织属性不会被组织中的条目所继承。
RADIUS 验证属性包括：

RADIUS 服务器 1

该字段用于显示主 RADIUS 服务器的 IP 地址或全限定主机名。默认的 IP 地址为 `127.0.0.1`。该字段接受任何有效的 IP 地址和主机名。如果指定多个条目，条目前面必须带有本地服务器名称，语法如下：

```
local_servername|ip_address local_servername2|ip_adress ...
```

RADIUS 服务器 2

该字段用于显示辅助 RADIUS 服务器的 IP 地址或全限定域名 (FQDN)。该服务器用于故障解决，当联系不上主服务器时将联系该服务器。默认的 IP 地址为 `127.0.0.1`。如果指定多个条目，条目前面必须带有本地服务器名称，语法如下：

```
local_servername|ip_address local_servername2|ip_adress ...
```

RADIUS 共享秘密

该字段用于指定 RADIUS 验证的共享秘密。共享秘密应与精选口令具有相同的地位。该字段不存在默认值。

RADIUS 共享秘密 （确认）

确认 RADIUS 验证的共享秘密。

RADIUS 服务器的端口

该字段用于指定 RADIUS 服务器监听的端口。默认值为 `1645`。

超时

该字段指定超时前等待 RADIUS 服务器响应所经过的时间间隔，以秒为单位。默认值为 3 秒。该字段接受使用任何以秒为单位的数值来指定超时。

验证级别

各种验证方法都单独设置了验证级别。验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。当 SSO 令牌传递到用户要访问的应用

程序时，应用程序将根据存储的值来确定级别是否足以授予用户访问权限。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。默认值为 0。对于 2004Q2 发行版，此功能无法正常工作。但在先前的版本中，此功能可正常工作。

第 26 章

SafeWord 验证属性

SafeWord 验证属性是组织属性。在 “服务配置”下 SafeWord 验证属性采用的值将成为 SafeWord 验证模板的默认值。为组织注册服务之后，需要创建服务模板。组织的管理员可以在注册后更改默认值。组织属性不会被组织子树中的条目继承。

该服务允许使用 Secure Computing 的 SafeWord 或 SafeWord PremierAccess 验证服务器来验证用户。 SafeWord 验证属性包括：

SafeWord 服务器

该字段指定 SafeWord 或 SafeWord PremiereAccess 服务器的名称和端口。端口 7482 为 SafeWord 服务器的默认端口。SafeWord PremierAccess 服务器的默认端口号为 5030。

SafeWord 服务器验证文件目录

该字段用于指定 SafeWord 客户机库放置其验证文件的目录。默认路径如下所示：

```
/var/opt/SUNWam/auth/safeword/serverVerification
```

如果该字段中指定的是其他目录，进行 SafeWord 验证前该目录必须存在。

SafeWord 日志级别

该属性已停用。

SafeWord 日志文件

该属性用于指定 SafeWord 客户机日志的目录路径和日志文件名。默认路径如下所示：

```
/var/opt/SUNWam/auth/safeword/safe.log
```

如果指定的是其他路径或文件名，进行 SafeWord 验证前这些路径或文件名必须存在。

如果多个组织同时配置了 SafeWord 验证，并且它们使用不同的 SafeWord 服务器，则必须指定不同的路径，否则， SafeWord 验证只在第一个进行验证的组织中生效。与此类似，如果某个组织更改了 SafeWord 服务器，则验证前必须删除指定目录中的 `swec.dat` 文件，以使新配置的 SafeWord 服务器生效。

验证级别

各种验证方法都单独设置了验证级别。验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。当 SSO 令牌传递到用户要访问的应用程序时，应用程序将根据存储的值来确定级别是否足以授予用户访问权限。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。默认值为 `0`。

注 如果未指定任何验证级别，核心验证属性 “默认验证级别” 中指定的值将会存储到 SSO 令牌中。有关详细信息，参见第 254 页的 “默认验证级别”。对于 2004Q2 发行版，此功能无法正常工作。但在先前的版本中，此功能可正常工作。

第 27 章

SecurID 验证属性

SecurID 验证属性是组织属性。在 “服务配置”下 SecurID 验证属性采用的值将成为 SecurID 验证模板的默认值。为组织注册服务之后，需要创建服务模板。组织的管理员可以在注册后更改默认值。组织属性不会被组织子树中的条目继承。

该服务允许使用 RSA 的 ACE/Server 验证服务器对用户进行验证。 SecurID 验证属性包括：

注 在此版本的 Identity Server 中， Linux 和 x86 操作系统不支持 SecurID 验证服务。

SecurID ACE/Server 配置路径

该字段用于指定 SecurID ACE/Server `sdconf.rec` 文件所在的目录。默认路径如下所示：

```
/opt/ace/data
```

如果该字段中指定的是其他目录，进行 SecurID 验证前该目录必须存在。

SecurID 帮助器配置端口

该属性用于指定当启动 “SecurID 帮助器验证端口”属性中包含的配置信息时，SecurID 帮助器 “侦听”的端口。默认端口为 58943。

如果更改了该属性，需要同时更改 `AMConfig.properties` 文件中的 `securidHelper.ports` 条目，并重新启动 Identity Server。`AMConfig.properties` 文件中的该条目是由空格分隔的 SecurID 帮助器实例端口列表。对于每一个与不同的 ACE/Server （具有不同的 `sdconf.rec` 文件）进行通信的组织，都必须有一个单独的 SecurID 帮助器。

SecurID 帮助器验证端口

该属性用于指定一个端口，组织的 SecurID 验证模块将配置其 SecurID 帮助器实例以 “侦听”该端口的验证请求。在所有使用 SecurID 或 Unix 验证的组织中，该端口号必须是唯一的。默认端口为 57943。

验证级别

各种验证方法都单独设置了验证级别。验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。当 SSO 令牌传递到用户要访问的应用程序时，应用程序将根据存储的值来确定级别是否足以授予用户访问权限。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。默认值为 `0`。

注 如果未指定任何验证级别，核心验证属性 “默认验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，参见第 254 页的 “默认验证级别”。对于 2004Q2 发行版，此功能无法正常工作。但在先前的版本中，此功能可正常工作。

第 28 章

Unix 验证属性

Unix 验证服务由全局属性和组织属性组成。全局属性所采用的值会应用到整个 Sun Java System Identity Server 配置，并且会被每个已配置的组织继承。由于全局属性的目的在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。组织属性所采用的值是各个已配置的组织的默认值，当服务注册到组织时，这些值可以更改。组织属性不会被组织项继承。 Unix 验证属性分为：

注 如果修改了 Unix 验证属性，则必须重新启动 Identity Server 和 `amunixd` 帮助器。

全局属性

Unix 验证服务中的全局属性包括：

Unix 帮助器配置端口

该属性指定启动时 Unix 帮助器为获得 “Unix 帮助器验证端口”、“Unix 帮助器超时”和 “Unix 帮助器线程”属性中包含的配置信息所 “侦听”的端口。默认端口为 58946。

如果更改该属性，还必须更改 `AMConfig.properties` 文件中的 `unixHelper.port` 项，并重新启动 Identity Server。

Unix 帮助器验证端口

该属性指定配置之后 Unix 帮助器为获取验证请求所 “侦听”的端口。默认端口为 57946。

Unix 帮助器超时

该属性指定用户为完成验证而花费的时间 （分钟）。如果用户超过分配的时间，验证将自动失败。默认时间为 3 分钟。

Unix 帮助器线程

该属性指定允许同时进行的 Unix 验证会话的最大数目。如果在给定时间内达到了最大数目，将不再允许随后的验证尝试，直到有会话被释放。默认值为 5。

组织属性

Unix 验证服务的组织属性包括：

验证级别

各种验证方法都单独设置了验证级别。各种验证方法都单独设置了验证级别的值。验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。当 SSO 令牌传递到用户要访问的应用程序时，应用程序将根据存储的值来确定级别是否足以授予用户访问权限。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。默认值为 0。

注 如果未指定任何验证级别，核心验证属性 “默认验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，参见第 254 页的 “默认验证级别”。对于 2004Q2 发行版，此功能无法正常执行。但在先前的版本中，此功能可正常执行。

第 29 章

Windows 桌面 SSO 验证属性

Windows 桌面 SSO 验证属性是组织属性。在 “服务配置”下 Windows 桌面 SSO 验证属性采用的值将成为 Windows 桌面 SSO 验证模板的默认值。为组织注册服务之后，需要创建服务模板。组织的管理员可以在注册后更改默认值。组织属性不会被组织子树中的条目继承。

此验证模块需要 Kerberos 验证服务，后者由作为域控制器运行的 Windows 2000 服务器提供。

Windows 桌面 SSO 验证属性包括：

服务主用户

此属性指定用来验证的 Kerberos 主用户。请使用以下格式：

```
HTTP/hostname.domainname@dc_domain_name
```

hostname 和 *domainame* 表示 Identity Server 实例的主机名和域名。*dc_domain_name* 是 Windows 2000 Kerberos 服务器 （域控制器）所在的 Kerberos 域。它可能与 Identity Server 的域名不同。

密钥文件名

此属性指定用来验证的 Kerberos 密钥文件。使用以下格式 （尽管该格式不是必需的）：

hostname.HTTP.keytab

hostname 指 Identity Server 实例的主机名。

Kerberos 领域

此属性指定 Kerberos 分发中心 （域控制器）域名。域控制器的域名可能与 Identity Server 域名不同，具体取决于配置。

Kerberos 服务器名

此属性指定 Kerberos 分发中心 （域控制器）主机名。必须输入该域控制器的全限定域名 (FQDN)。

返回主用户的域名

此属性启用后允许 Identity Server 在验证期间自动一同返回 Kerberos 主用户与域控制器的域名。

验证级别

各种验证方法都单独设置了验证级别。验证级别值表示信任验证的程度。用户进行验证之后，该值将存储在会话的 SSO 令牌中。当 SSO 令牌传递到用户要访问的应用程序时，应用程序将根据存储的值来确定级别是否足以授予用户访问权限。如果 SSO 令牌中存储的验证级别没有达到必需的最小级别，应用程序将提示用户使用具有较高验证级别的服务再次进行验证。默认值为 0。

注 如果未指定任何验证级别，核心验证属性 “默认验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，参见第 254 页的 “默认验证级别”。对于 2004Q2 发行版，此功能无法正常工作。但在先前的版本中，此功能可正常工作。

第 30 章

验证配置服务属性

验证配置服务属性是动态属性，也是组织属性。可以为组织、服务或角色定义这些属性。组织属性在核心验证模块中定义。

如果将角色指定给用户或将用户指定给组织，则在默认情况下这些属性将被用户继承。验证配置属性包括：

验证配置

单击 “编辑”链接将显示 “验证配置”界面。该界面使您能够为基于角色或基于组织的验证配置验证模块。

下表列出了验证模块的配置选项：

模块名称	允许您从 Identity Server 可以使用的默认验证模块列表中选择。

标志

该下拉菜单允许您指定验证模块要求，可以指定以下值之一：

- **必需** - 要求验证模块必须成功。无论验证成功或失败，都将继续验证列表中的下一个验证模块。
- **必要** - 要求验证模块必须成功。如果验证成功，将继续验证列表中的下一个验证模块。如果验证失败，则返回到应用程序（不继续验证列表中的下一个验证模块）。
- **充足** - 不要求验证模块必须成功。如果验证成功，则立即返回到应用程序（不继续验证列表中的下一个验证模块）。如果验证失败，将继续验证列表中的下一个验证模块。
- **可选** - 不要求验证模块必须成功。无论验证成功或失败，都将继续验证列表中的下一个验证模块。

这些标志建立了其定义的验证模块的执行标准。执行的层次结构是：**必需**位于最高层，**可选**位于最底层。

例如，如果管理员定义了一个具有**必需**标志的 LDAP 模块，则用户的凭证必须通过 LADP 验证要求才能访问给定的资源。

如果添加多个验证模块，并将每个模块的“标志”都设置成**必需**，则用户必须通过所有验证要求才能被授予权限。

有关标志定义的详细信息，请参考 JAAS（Java 验证和授权服务），网址为：

`http://java.sun.com/security/jaas/doc/module.html`

选项

模块的其他选项，格式为“关键字 = 值”对。多个选项之间用空格分隔。

登录成功 URL

该属性指定用户在验证成功后，重新指向的 URL。

登录失败 URL

该属性指定用户在验证失败后，重新指向的 URL。

验证后期处理类

该属性定义用于在登录成功或失败后自定义后期验证处理的 Java 类的名称。

冲突解决级别

该属性仅适用于角色。冲突解决级别为可能包含相同用户的多个角色设置验证配置属性的优先级级别。例如，如果 User1 被同时指派给 Role1 和 Role2，您可以为 Role1 定义较高的优先级级别，这样，当用户试图验证时， Role1 将对成功或失败重定向以及后期验证处理拥有较高的优先级。

第 31 章

客户机检测服务属性

客户机检测服务属性是全局属性。它们所采用的值将被应用到整个 Identity Server 配置，并被每个已配置的组织所继承。（由于全局属性的用途在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。）客户机检测属性包括：

客户机类型

要检测客户机类型， Identity Server 需要识别其标识特征。这些特征以客户机数据的形式标识所有支持的类型的属性。该属性允许您通过 “客户机管理器”界面修改客户机数据。要访问客户机管理器，请单击 “编辑”链接。

此外， Identity Server 包含以下客户机类型：

- HDML
- HTML
- JHTML
- VoiceX
- WML

- XHTML
- cHTML
- iHTML
- 有关这些客户机类型的说明，请参见 Sun Java System Portal Server 下的 Mobile Access 2004Q2 Administration Guide，该指南位于以下位置：

  http://docs.sun.com/prod/entsys#hic

客户机管理器

“客户机管理器”界面列出了基本客户机、式样和相关属性，并允许您添加和配置设备。

基本客户机类型

“客户机管理器”顶部列出了各种基本客户机类型。这些客户机类型包含可以由属于客户机类型的所有设备继承的默认属性。

式样配置文件

“客户机管理器”在 “式样”下拉菜单中对所有可用的客户机 （包括基本客户机类型本身）进行了分组。选定的式样 （或父配置文件）定义了对其已配置的子设备通用的属性。这些设备动态继承父配置文件的属性。

“当前式样属性”链接将启动只读的 “客户机编辑器”窗口，查看式样属性。

设备配置文件

选定一个式样后，“客户机管理器”会显示该式样所配置的设备配置文件。设备按用户代理 （设备名称）排序，并可在 “过滤器”字段 （可输入通配符）中输入用户代理字符串进行过滤。

对于每个设备，您均可以单击位于每个设备名称旁边的 “编辑”链接修改客户机属性。然后这些属性会显示在 “客户机编辑器”窗口中。要编辑属性，请从下拉列表中选择以下分类：

硬件平台。包含设备的硬件属性，例如显示大小、支持的字符集等。

软件平台。包含设备的应用程序环境、操作系统和已安装软件的属性。

网络特征。包含描述网络环境 （包括支持的载体）的属性。

BrowserUA。包含设备上运行的浏览器用户代理的相关属性。

WapCharacteristics。包含设备所支持的无线应用协议 (WAP) 环境的属性。

PushCharacteristicsNames。包含设备所支持的 WAP 环境的属性。

其他属性。允许您添加设备的其他属性。

有关具体属性定义，请参见以下位置的 Open Mobile Alliance Ltd. (OMA) *Wireless Application Protocol, Version 20-Oct-2001*：

http://www1.wapforum.org/tech/terms.asp?doc=WAP-248-UAProf-20011020-a.pdf

属性修改完成后，单击 “保存”。设备将显示 “**” 字符以表示该设备已经自定义。使用 “默认” 链接可以移除自定义的属性并将设备重置为默认设置。

要为式样添加新设备，请单击 “新设备” 按钮。将显示 “创建新设备” 窗口，包括以下字段：

式样。显示设备的基本式样，例如 `HTML`。

设备用户代理。接受设备的名称。

单击 “下一步” 以显示以下字段：

客户机类型名称。显示客户机类型，例如 HTML。客户机类型名称必须在所有设备中唯一。

立即接受此设备的父类型。接受设备的父 （基本）客户机类型。例如， HTML。

HTTP 用户代理字符串。定义 HTTP 请求标题中的用户代理。例如， Mozilla/4.0。

单击 “确定” 并自定义设备属性。有关具体属性定义，请参见以下位置的 Open Mobile Alliance Ltd. (OMA) *Wireless Application Protocol, Version 20-Oct-2001*：

http://www1.wapforum.org/tech/

要复制设备及其属性，请单击 “复制”链接。设备名称必须唯一。默认情况下，Identity Server 将把设备重命名为 `copy_of_`*devicename*。

要删除设备，请单击设备旁边的 “删除”链接。

默认客户机类型

该属性定义 “客户机类型”属性中客户机类型列表的默认客户机类型。默认值为 `genericHTML`。

客户机检测类

该属性定义路由所有客户机检测请求的客户机检测类。该属性返回的字符串应该与 “客户机类型”属性中列出的某种客户机类型相匹配。默认客户机检测类为 `com.sun.mobile.cdm.FEDIClientDetector`。 Identity Server 还包含 `com.iplanet.services.cdm.ClientDetectionDefaultImpl`。

启用客户机检测

该属性允许您启用客户机检测。如果启用 （选中）了客户机检测，则通过 “客户机检测类”属性中指定的类来路由各个请求。

默认情况下，客户机检测功能处于启用状态。如果未选择该属性， Identity Server 将假定客户机类型为 genericHTML 并且通过 HTML 浏览器访问。

第 32 章

全球化设置服务属性

全球化设置服务属性是全局属性。它们所采用的值将被应用到整个 Identity Server 配置，并被每个已配置的组织所继承。（由于全局属性的用途在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。）全局属性包括：

各个语言环境支持的字符集

该属性列出各个语言环境支持的字符集，指明语言环境与字符集之间的映射。格式如下所示：

`locale=`*localename*`|charset=charset1;charset2;charset3;...;charsetn`

可以使用位于属性底部的按钮来添加、编辑、复制和移除字符集。

字符集别名

该属性列出将用于发送响应的代码集名称 （映射到 IANA 名称）。这些代码集名称无需与 java 代码集名称匹配。当前提供了一个散列表，可用来在 java 字符集与 IANA 字符集之间建立相互的映射。别名格式如下所示：

mimeName=*charset*|javaName=*charset*

例如：

```
mimeName=Shift_JIS|javaName=SJIS
```

这意味着二者表示同一个字符集。

可以使用位于属性底部的按钮来添加、编辑、复制和移除字符集别名。

自动生成的通用名称格式

该显示选项用于定义自动生成名称的方式，从而针对不同语言环境和字符集提供名称格式。默认语法如下 （请注意，定义中包含的逗号和 / 或空格将显示在名称格式中）：

```
en_us = {givenname} {initials} {sn}
```

例如，如果要使用中文字符集显示带有 uid （为 11111）的用户 （用户 One）的新名称格式，请使用以下形式：

```
zh = {sn}{givenname}({uid})
```

这将显示为：

```
OneUser 11111
```

第 33 章

日志服务属性

日志服务属性是全局属性。它们所采用的值将被应用到整个 Sun Java System Identity Server 配置，并被每个已配置的组织所继承。（由于全局属性的目的在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。）日志属性包括：

- 第 301 页的 “启用时间缓冲”

最大日志大小

该属性指定 Identity Server 日志文件的最大值 （以字节为单位）。默认值为 1000000。

历史文件数目

该属性的值与为进行历史分析而保留的备份日志文件的数目相等。在本地系统的分区大小和可用磁盘空间允许的情况下，可以输入任何整数。默认值为 3。

注 对输入值 0 与输入值 1 的解释相同，即如果指定 0，则会创建备份日志文件。

日志文件位置

基于文件的日志函数需要一个可以存储日志文件的位置。该字段接受该位置的完整目录路径。默认位置为：

/var/opt/SUNWam/logs

如果使用了非默认目录，正在运行 Identity Server 的用户必须具有该目录的写入权限。

配置 DB （数据库）日志 （如 Oracle 或 MySQL）的日志位置时，日志位置的有些部分区分大小写。

例如，如果记录到 Oracle 数据库，日志位置应为：

jdbc:oracle:thin:@machine.domain:port:DBName

jdbc:oracle:thin 必须为小写。

注 需要重新启动 Identity Server 后，对日志属性值所作的更改才会生效。

日志类型

该属性允许您为平面文件日志指定文件或为数据库日志指定 DB。

数据库用户名

当 “日志类型” 属性设置为 “DB” 时，该属性采用要连接到数据库的用户的名称。

数据库用户口令

当 “日志类型” 属性设置为 “DB” 时，该属性采用数据库用户口令。

数据库用户口令 （确认）

确认数据库口令。

数据库驱动程序名

该属性允许用户指定日志实现类的驱动程序。

可配置日志字段

该参数指定将被记录的字段列表。默认情况下，将记录以下字段：

- Domain
- Hostname
- IPAddress
- LoggedBy
- Loglevel

- LoginID
- ModuleName

日志验证频率

该属性用于设置服务器为检测篡改而检验日志的频率 （以秒为单位）。默认时间为 3600 秒。该参数仅适用于安全日志。

日志签名时间

该参数用于设置对日志进行签名的频率 （以秒为单位）。默认时间为 900 秒。该参数仅适用于安全日志。

启用安全日志

该属性用于指定是否启用安全日志。默认情况下，安全日志为关闭状态。启用安全日志后，可以检测对安全日志进行的未授权更改或篡改。

最大记录数目

该属性用于设置 Java LogReader 接口返回的最大记录数目，而不管有多少记录与读取查询相匹配。默认情况下，该属性被设置成 500。日志 API 的呼叫者可以通过 LogQuery 参数覆盖该属性。

每个归档文件中的文件数目

该属性仅适用于安全日志。该属性用于指定对于后续安全日志，何时需要归档日志文件和密钥库以及何时重新生成安全密钥库。默认情况下每个记录器中含有五个文件。

缓冲区大小

该属性用于指定日志记录在被发送到日志服务进行记录之前，内存缓冲区中存储的最大日志记录数目。默认情况下是一条记录。

缓冲时间

该属性定义日志记录在被发送到日志服务进行记录之前，日志记录将在内存缓冲区中存储的时间。默认值是 3600 秒。

启用时间缓冲

当选择 ON 时， Identity Server 将为要在内存缓冲区中存储的日志记录设置时间限制。时间值在 “缓冲时间”属性中设置。

第 34 章

命名服务属性

命名服务属性是全局属性。它们所采用的值将被应用到整个 Sun Java System Identity Server 配置，并被每个已配置的组织所继承。（由于全局属性的目的在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。）

如果平台运行了多个 Identity Server，命名服务可以使客户机找到正确的服务 URL。找到命名 URL 时，命名服务将对用户会话进行解码，并使用会话中的参数动态替换协议、主机和端口。这将确保服务返回的 URL 是其上创建有用户会话的主机。命名属性包括：

配置服务 URL

该字段采用的值为

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/profileservice`

该语法允许动态替换基于特定会话参数的配置 URL。

会话服务 URL

该字段采用的值为

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/sessionservice`

该语法允许动态替换基于特定会话参数的会话 URL。

日志服务 URL

该字段采用的值为

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/loggingservice`

该语法允许动态替换基于特定会话参数的日志 URL。

策略服务 URL

该字段采用的值为

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/policyservice`

该语法允许动态替换基于特定会话参数的策略 URL。

验证服务 URL

该字段采用的值为

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/authservice`

该语法允许动态替换基于特定会话参数的验证 URL。

SAML Web 配置 / 辅件服务 URL

该字段采用的值为

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/SAMLAwareServlet`

该语法允许动态替换基于特定会话参数的 SAML Web 配置/辅件 URL。

SAML SOAP 服务 URL

该字段采用的值为

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/SAMLSOAPReceiver`

该语法允许动态替换基于特定会话参数的 SAML SOAP URL。

SAML Web 配置 /POST 服务 URL

该字段采用的值为

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/SAMLPOSTProfileServlet`

该语法允许动态替换基于特定会话参数的 SAML Web 配置 /POST URL。

SAML 断言管理器服务 URL

该字段采用的值为

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/AssertionManagerServlet/AssertionManagerIF`

该语法允许动态替换基于特定会话参数的 SAML 断言管理器服务 URL。

联合断言管理器服务 URL

该字段采用的值为

```
%protocol://%host:%port/amserver/FSAssertionManagerServlet/FSAssertionMana
gerIF
```

该语法允许动态替换基于特定会话参数的联合断言管理器服务 URL。

身份 SDK 服务 URL

该字段采用的值为

```
%protocol://%host:%port/amserver/UserManagementServlet/
```

该语法允许动态替换基于特定会话参数的身份 SDK 服务 URL。

第 35 章

口令重置服务属性

口令重置服务属性是组织属性。在 “服务配置”下口令重置属性所采用的值将成为给定组织中口令重置服务的默认值。组织属性不会被组织子树中的条目继承。

口令重置属性包括：

- 第 311 页的 “N 次失败后警告用户”
- 第 311 页的 “口令重置失败锁定持续时间”
- 第 311 页的 “口令重置锁定属性名称”
- 第 311 页的 “口令重置锁定属性值”

用户验证

该属性指定搜索要重置其口令的用户时使用的值。

秘密问题

可以在该字段中添加多个问题，用户可以使用这些问题来重置其口令。要添加问题，在 “秘密问题”字段中键入问题并单击 “添加”。选定的问题将会显示在用户的 “用户配置文件”页面中。用户可以选择一个问题来重置口令。

如果选择了 “启用私人问题”属性，用户可以创建自己的问题。

搜索过滤器

该属性指定用于查找用户条目的搜索过滤器。

基本 DN

该属性指定用户搜索的起始 DN。如果未指定任何 DN，搜索将从组织 DN 开始。为防止代理服务器验证冲突，不应将 `cn=directorymanager` 用作基本 DN。

绑定 DN

可以同时使用该属性值与 “绑定口令”来重置用户口令。

绑定口令

可以同时使用该属性值与“绑定 DN”来重置用户口令。

口令重置选项

该属性用于确定重置口令时使用的类名。默认的类名为：

```
com.sun.identity.password.RandomPasswordGenerator
```

可以通过插件自定义口令重置类，这个类需要由 `PasswordGenerator` 接口实现。有关详细信息，参见 《*Identity Server Developer's Guide*》。

口令更改通知选项

该属性用于确定重置口令时通知用户的方法。默认的类名为：

```
com.sun.identity.password.EmailPassword
```

可以通过插件自定义口令通知类，这个类需要由 `NotifyPassword` 接口实现。有关详细信息，参见 《*Identity Server Developer's Guide*》。

启用口令重置

选择该属性将启用口令重置功能。

启用个人问题

选择该属性将允许用户创建独特的口令重置问题。

问题的最大数目

该值用于指定最多可以在口令重置页面上提多少个问题。

在下一次登录时强制更改口令

如果启用此选项，下次登录时，将强制用户更改其口令。如果希望管理员 （而不是顶层管理员）来设置强制口令重置选项，必须修改默认权限 ACI 才能允许访问该属性。

启用口令重置失败锁定

该属性指定如果用户最初重置口令 （使用口令重置应用程序）失败，是否禁止用户重置其口令。默认情况下，不启用该功能。

口令重置失败锁定计数

该属性用于定义在 “口令重置失败锁定间隔”中指定的时间间隔内，用户在被锁定之前可以重置口令的次数。

例如，如果将 “口令重置失败锁定计数”设置成 5，将 “登录失败锁定间隔”设置成 5 分钟，则在被锁定之前，用户可以在 5 分钟之内重置 5 次口令。

口令重置失败锁定间隔

该属性用于定义用户在被锁定之前，可以尝试重置口令 （重置次数在 “口令重置失败锁定计数”中定义）的时间 （以分钟为单位）。

用于发送锁定通知的电子邮件地址

该属性用于指定用户被口令重置服务锁定时接收通知的电子邮件地址。可以在以空格分隔的列表中指定多个电子邮件地址。

N 次失败后警告用户

该属性指定在 Identity Server 发送警告消息，警告用户将被锁定之前，允许的口令重置失败的次数。

口令重置失败锁定持续时间

该属性定义在发生锁定之后，用户不能重置口令的持续时间 （以分钟为单位）。

口令重置锁定属性名称

该属性包含 “口令重置锁定属性值”中设置的 inetuserstatus 值。如果用户在口令重置中被锁定，且 “口令重置失败锁定持续时间 （分钟）”变量设置为 0，则 inetuserstatus 将被设置为无效，以禁止用户重置其口令。

口令重置锁定属性值

该属性用于将用户状态的 inetuserstatus 值 （包含在 “口令重置锁定属性名称”中）指定为有效或无效。如果用户在口令重置中被锁定，且 “口令重置失败锁定持续时间 （分钟）”变量设置为 0，则 inetuserstatus 将被设置为无效，以禁止用户重置其口令。

第 36 章

平台服务属性

平台服务属性是全局属性。它们所采用的值将被应用到整个 Sun Java System Identity Server 配置，并被每个已配置的组织所继承。（由于全局属性的目的在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。）平台属性包括：

服务器列表

命名服务在初始化时读取该属性。该列表包含单个 Identity Server 配置中的 Identity Server 会话服务器。例如，如果安装了两个 Identity Server，且它们应该作为一个 Identity Server 运行，则它们必须都包含在该列表中。如果列表中不存在服务 URL 请求中指定的主机，则命名服务将拒绝请求。列表中的第一个值指出安装期间指定的服务器的主机名及端口。列表末尾有一个两字节的值，该值唯一标识服务器。参与平衡负荷或故障转移的每个服务器都必须具有唯一的标识符。标识符还用于通过将服务器 URL 映射到服务器 ID 来缩短 Cookie 的长度。例如：

protocol://*server_domain*:*port*|01

可以使用 protocol://*server_domain*:*port* |01|*instance_name* 格式来添加附加服务器。

此属性中应只使用命名服务协议。

平台语言环境

平台语言环境的值是安装 Identity Server 时使用的默认语言子类型。验证、记录和管理服务是用该默认值的语言进行管理的。默认值为 en_US。有关所有支持的语言子类型的列表，参见第 249 页的表 20-1。

Cookie 域

这是一个域列表，当在验证过程中向用户的浏览器设置了 Cookie 时， Cookie 标题中将返回该列表。如果列表为空，则不设置 Cookie 域。换句话说， Identity Server 会话 Cookie 只会发送到 Identity Server 自身，而不会发送到域中的其他服务器。如果域中的其他服务器需要 SSO，该属性必须和 Cookie 域一同设置。如果在一个 Identity Server 上的不同域中有两个接口，则需要在该属性中对两个 Cookie 域进行设置。如果使用了负载平衡器，则 Cookie 域必须是负载平衡器的域，而不是负载平衡器背后的服务器。该字段的默认值是安装的 Identity Server 的域。

注 确保输入正确的 Cookie 域。如果 Cookie 域不正确，您将无法登录到 Identity Server。

登录服务 URL

该字段用于指定登录页面的 URL。该属性的默认值为 */Service_DEPLOY_URI*/UI/Login。

注销服务 URL

该字段用于指定注销页面的 URL。该属性的默认值为 */Service_DEPLOY_URI*/UI/Logout。

可用的语言环境

该属性用于存储为平台配置的所有可用的语言环境。以一个允许用户选择自身语言环境的应用程序为例。该应用程序将从平台配置文件中获取该属性，并向用户提供语言环境列表。用户将选择一个语言环境，应用程序会在用户条目 preferredLocale 中设置该环境。

客户机字符集

该属性用于为位于平台级别上的不同客户机指定字符集。它包含一个客户机类型及其相应字符集的列表。格式如下所示：

```
clientType|charset
clientType2|charset
```

例如：

```
genericHTML|UTF-8
```

第 37 章

策略配置服务属性

策略配置服务属性由全局属性和组织属性组成。全局属性所采用的值被应用到整个 Sun Java System Identity Server 配置，并被每个已配置的组织所继承。（由于全局属性的目的在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。）在 “服务管理”中组织属性所采用的值将成为策略配置的默认值。为组织注册服务之后，需要创建服务模板。组织的管理员可以在注册后更改默认值。组织属性不会被组织中的条目所继承。策略配置属性分为：

全局属性

“策略配置”服务中的全局属性包括：

资源比较器

该属性用于指定资源比较器的信息，这些信息用于比较策略规则定义中指定的资源。在策略创建和评估的过程中，都要用到资源比较。该属性包含以下值：

serviceType	指定要使用比较器的服务。
class	定义实现资源比较算法的 java 类。
wildcard	指定可在资源名称中定义的通配符。
delimiter	指定资源名称中使用的分界符。
caseSensitivity	指定对两种资源进行比较时应考虑条件还是忽略条件。 False 表示忽略条件， True 表示考虑条件。

拒绝决策时继续评估

此属性指定策略框架是否应继续评估后续策略 （甚至是在策略决策为 “拒绝” 时）。如果取消选择 （默认设置），确认 “拒绝” 决策后，策略评估将跳过后续策略。

组织属性

策略配置服务中的组织属性包括：

- 第 320 页的 “LDAP 服务器和端口”
- 第 321 页的 “LDAP 基本 DN”
- 第 321 页的 “LDAP 用户基本 DN”
- 第 321 页的 “Identity Server 角色基本 DN”
- 第 321 页的 “LDAP 绑定 DN”
- 第 321 页的 “LDAP 绑定口令”
- 第 321 页的 “LDAP 绑定口令 （确认）”

LDAP 服务器和端口

该字段用于指定安装 Identity Server 过程中指定的主 LDAP 服务器的主机名和端口号，这些数据将用于搜索策略主题，如 LDAP 用户、 LDAP 角色、 LDAP 组等。格式为 *hostname:port*，例如：

```
machine1.example.com:389
```

对于多个 LDAP 服务器主机的故障转移配置，该值可为以空格分隔的主机列表。格式为 hostname1:port1 hostname2:port2...

例如：

```
machine1.example1.com:389 machine2.example1.com:389
```

如果指定多个条目，条目前面必须带有本地服务器名称。这使 Identity Server 可以配置为与特定 Directory Server 进行通信。

格式为 `servername|hostname:port`

例如：

```
machine1.example1.com|machine1.example1.com:389
```

```
machine1.example2.com|machine1.example2.com:389
```

对于故障转移配置：

```
IS_Server1.example1.com|machine1.example1.com:389 machine2.example.com1:389
```

```
IS_Server2.example2.com|machine1.example2.com:389 machine2.example2.com:389
```

注 该属性已更改为接受一系列值，以支持多个服务器。在 6.0 SP1 发行版中，该属性仅接受单个值。

如果您试图将 6.0SP1 和 6.1 放在一个部署环境中，可能会出现问题，尤其在 Identity Server 6.0 SP1 实例指向 6.1 DIT 的情况下。

要成功地将它们放在一个部署环境中，请确保此属性只包含一个 LDAP 服务器。

LDAP 基本 DN

该字段指定 LDAP 服务器中的基本 DN，搜索将从该 DN 开始。默认情况下，基本 DN 是 Identity Server 安装的顶级组织。

LDAP 用户基本 DN

该属性指定由 LDAP 服务器中的 LDAP 用户主题使用的基本 DN，搜索将从此 DN 开始进行。默认情况下，它是 Identity Server 安装库的顶级组织。

Identity Server 角色基本 DN

该属性指定由 LDAP 服务器中的 Identity Server 角色主题使用的基本 DN，搜索将从此 DN 开始进行。默认情况下，它是 Identity Server 安装库的顶级组织。

LDAP 绑定 DN

该字段指定 LDAP 服务器中的绑定 DN。

LDAP 绑定口令

该属性定义用于绑定 LDAP 服务器的口令。默认情况下，安装过程中输入的 `amldapuser` 口令将用作绑定用户。

LDAP 绑定口令 （确认）

确认 LDAP 绑定口令。

LDAP 组织搜索过滤器

指定用于查找组织条目的搜索过滤器。默认值为 `(objectclass=sunMangagedOrganization)`。

LDAP 组织搜索范围

该属性定义用于查找组织条目的范围。该范围必须为以下值之一：

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB （默认值）

LDAP 组搜索过滤器

该属性指定用于查找组条目的搜索过滤器。默认值为 (objectclass=groupOfUniqueNames)。

LDAP 组搜索范围

该属性定义用于查找组条目的范围。该范围必须为以下值之一：

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB （默认值）

LDAP 用户搜索过滤器

指定用于查找用户条目的搜索过滤器。默认值为 (objectclass=inetorgperson)。

LDAP 用户搜索范围

该属性定义用于查找用户条目的范围。该范围必须为以下值之一：

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB （默认值）

LDAP 角色搜索过滤器

该属性指定用于查找角色条目的搜索过滤器。默认值为 (&(objectclass=ldapsubentry)(objectclass=nsroledefinitions))。

LDAP 角色搜索范围

该属性定义用于查找角色条目的范围。该范围必须为以下值之一：

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB （默认值）

Identity Server 角色搜索范围

该属性定义用于查找 Identity Server 角色主题的条目的范围。该范围必须为以下值之一：

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB （默认值）

LDAP 组织搜索属性

该字段用于定义搜索组织时使用的属性类型。默认值为 o。

LDAP 组搜索属性

该字段用于定义搜索组时使用的属性类型。默认值为 cn。

LDAP 用户搜索属性

该字段用于定义搜索用户时使用的属性类型。默认值为 `uid`。

LDAP 角色搜索属性

该字段用于定义搜索角色时使用的属性类型。默认值为 `cn`。

搜索返回的结果的最大数目

该字段定义搜索返回的结果的最大数目。默认值为 100。如果搜索限制超过了指定的数量，将返回达到该数量前搜索到的条目。

搜索超时

该属性用于指定经过多长时间后搜索将超时。如果搜索超过了指定的时间，将返回在该时间前搜索到的条目。

启用 LDAP SSL

该属性用于指定 LDAP 服务器是否运行 SSL。选择该属性将启用 SSL，取消选择（默认）则将禁用 SSL。

LDAP 连接池的最小尺寸

该属性指定用于连接 Directory Server 的连接池的最小尺寸，它与 LDAP 服务器属性中指定的一致。默认端口为 1。

LDAP 连接池的最大尺寸

该属性指定用于连接 Directory Server 的连接池的最大尺寸，它与 LDAP 服务器属性中指定的一致。默认端口为 10。

选定的策略主题

该属性允许您选择一组主题类型以用于在组织中定义策略。

选定的策略条件

该属性允许您选择一组条件类型以用于在组织中定义策略。

选定的策略候选组织

该属性允许您选择一组候选组织类型以用于在组织中定义策略。

主题结果的生存时间

该属性指定一段时间 （以分钟为单位），在这段时间内，可以使用缓存的主题结果基于单点登录令牌对同一策略请求进行评估。

当基于 SSO 令牌对策略开始进行评估时，将评估该策略中的主题实例以确定该策略是否适用于给定的用户。通过 SSO 令牌 ID 添加了密钥的主题结果缓存在策略中。如果在 “主题结果的生存时间”属性中指定的时间内对同一个策略中的同一个 SSO 令牌 ID 进行了另一次评估，策略框架将检索缓存的主题结果，而不是评估主题实例。这会明显减少策略评估的时间。

启用用户别名

如果创建策略来保护其主题的成员在远程 Directory Server 中化名为本地用户的资源，则必须启用该属性。

例如，如果在远程 Directory Server 中创建 `uid=rmuser`，然后将 `rmuser` 作为别名添加到 Identity Server 中的本地用户 （例如 `uid=luserf©`，则必须启用该属性。当您以 `rmuser` 进行登录时，将使用本地用户 (`luser`) 创建会话，并且将成功实现策略强制。

第 38 章

SAML 服务属性

安全声明标记语言 (SAML) 服务属性是全局属性。它们所采用的值将被应用到整个 Sun Java System Identity Server 配置，并被每个已配置的组织所继承。（由于全局属性的目的在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。）

有关 SAML 服务体系结构的详细信息，参见 《*Identity Server Developer's Guide*》。

SAML 属性包括：

站点 ID 和站点发布者姓名

该属性包含一个条目列表，其中每个条目都包含一个实例 ID、站点 ID 和站点发布者姓名。默认值将在安装过程中指定。格式如下所示：

instanceid=serverprotocol://servername:portnumber|siteid=*site_id*|issuerName=*site_issuer_name*

为 SSL 配置完该属性后 （在源站点和目标站点中），请确保 instanceid 协议为 HTTPS//。

签署 SAML 请求

该属性指定在传送 SAML 请求前是否要对所有这些请求进行数字签名 (XML DSIG)。单击该选项将启用该功能。

签署 SAML 响应

该属性指定在传送 SAML 响应前是否要对所有这些响应进行数字签名 (XML DSIG)。单击该选项将启用该功能。

不管该选项是否启用，都将对 “SAML Web 公告”配置文件使用的所有 SAML 响应进行数字签名。

签名断言

该属性指定在传送 SAML 断言前是否要对所有这些断言进行数字签名 (XML DSIG)。单击该选项将启用该功能。

SAML 辅件名称

该属性指定 “SAML 服务”配置中定义的 SAML 辅件的变量名。 SAML 辅件是一种用来标识断言和源站点的限定了大小的数据。它作为 URL 查询字符串的一部分并通过重定向被传送到目标站点。默认值为 SAMLart。例如，使用默认 SAMLart 服务配置，重定向查询字符串可以为：

http://*host:port*/*deploy_URI*/SamlAwareServlet?TARGET=http://*URL*/&SAMLart=artifact123

目标说明符

该属性指定重定向中使用的目标站点 URL 的变量名。默认值为 `Target`。

辅件超时

该属性指定为辅件创建的断言超时。默认端口为 400。

断言不早于偏差因数

该属性用于计算断言的 “不早于” 时间。例如，如果 IssueInstant 的值为 `2002-09024T21:39:49Z`，并且 “断言不早于偏差因数” 的值设为 300 秒 （默认值为 180），则断言的条件元素的 “不早于” 属性将是 `2002-09-24T21:34:49Z`。

断言超时

该属性指定经过多少秒后发生声明超时。默认值为 420。

注 断言的总有效时间由 “断言不早于偏差因素” 和 “断言超时” 属性中设置的值定义。

可信赖的伙伴站点

该属性用于存储伙伴的信息，这样，一个站点可以与其伙伴站点之间建立一种可信赖的通信关系。

该属性包含一个条目列表，其中每个条目都包含 “关键字 / 值” 对 （对与对之间由 “|” 分隔）。每个条目都要求具有源 ID。例如：

`SourceID=siteid|SOAPURL=https://servername:portnumber/amserver/SAMLSOAPReceiver|AuthType=SSL|hostlist=ipaddress`（或 *server DNS name* 或 *cert alias*）

所用参数包括：

表 38-1 可信赖的伙伴站点参数

SourceID	该参数是在 SiteID 和发布者姓名中定义的一个 20 字节长的序列。
target	该参数在一个特定的域中定义，可带端口号，也可不带。如果您希望联系该特定域中提供的某个 Web 页， target 用于指定在下一步的操作中重定向到由 SAMLUrl 或 POSTUrl 参数定义的 URL。 如果同时存在两个条目（一个含有端口号，另一个不含有端口号），这两个条目都具有 “可信赖的伙伴站点”属性中指定的同一个域属性，则包含端口号的条目具有更高的优先级。 例如，如果您具有以下两个可信赖的伙伴站点定义： target=sun.com|SAMLUrl=http://machine1.sun.com:8080/amserver/SAMLAwareServlet 和 target=sun.com:8080|SAMLUrl=httyp://machine2.sun.com:80/amserver/SAMLAwareServlet 并且要查找以下页面： http://somemachine.sun.com:8080/index.html 第二个定义将被选中来提供 SAML 服务，因为其 target 参数中同时存在匹配的域和端口。
SAMLUrl	定义提供 SAML 服务的 URL。 URL 中指定的 servlet 实现在 OASIS-SAML 绑定和配置文件规范中定义的 Web-browser SSO with Artifact 配置文件。
POSTUrl	定义提供 SAML 服务的 URL。该 URL 中指定的 servlet 实现在 OASIS-SAML 绑定和配置文件规范中定义的 Web-browser SSO with POST 配置文件。
issuer	定义在 Identity Server 中生成的断言创建者。语法为： hostname:port。
SOAPUrl	指定 SOAP 接收方服务 URL。

AuthType	定义 SAML 中使用的验证类型。它应为以下类型之一： • NOAUTH • BASICAUTH • SSL • SSLWITHBASICAUTH 该参数可选，如果未指定，默认值为 NOAUTH。 如果指定为 BASICAUTH 或 SSLWITHBASICAUTH，“User”参数将为必需参数，并且 SOAPUrl 应为 HTTPS。
User	定义伙伴的 uid，用来保护伙伴的 SOAP 接收方。
version	定义用于发送 SAML 请求的 SAML 版本。指定 SAML 版本为 1.0 版或 1.1 版。如果未定义此参数，将从 AMConfig.properties 使用以下默认值： com.example.identity.saml.asertion.version-1.1 com.example.identity.saml.protocol.version=1.1
hostlist	该属性列出所有主机的 IP 地址和 / 或 certAlias，在指定的伙伴站点中，这些主机都可以向该站点发送请求。这样就确保了请求者确实是 SAML 辅件的预定接收方。 如果请求者的主机或客户机证书在接收方站点的这个列表中，服务将继续进行。如果主机或客户机证书与 hostlist 中的任何主机或证书都不匹配， SAML 服务将拒绝请求。
AccountMapper	指定一个可插接的类，用来定义断言主题与目标站点中的标识之间的相关方式。它的默认值为： com.sun.identity.saml.plugins.DefaultAccountMapper
attributeMapper	指定一个类，该类包含 attributeMapper 所在的路径。利用应用程序可以开发一个 attributeMapper 来获得 SSOToken ID，或者获得包含来自查询的 AuthenticationStatement 的断言。接着将使用该映射程序来检索主题的属性。如果未指定 attributeMapper，将使用 DefaultAttributeMapper。

actionMapper	指定一个类，该类包含 actionMapper 所在的路径。利用应用程序可以开发一个 actionMapper 来获得 SSOToken ID，或者获得包含来自查询的 AuthenticationStatement 的断言。接着将使用该映射程序来检索查询中定义的操作的授权决策。如果未指定 actionMapper，将使用 DefaultActionMapper。
siteAttributeMapper	指定一个类，该类包含 siteAttributeMapper 所在的路径。利用应用程序可以开发一个 siteAttributeMapper 来获得要在 SSO 期间包含在断言中的属性。如果未找到任何 siteAttributeMapper，则在 SSO 期间将不会有任何属性被包含到断言中。
certAlias=*aliasName*	指定出现以下情况时用来验证断言中签名的 certAlias 名称：当断言已由伙伴签名，而在已签名断言的 KeyInfo 部分中又找不到该伙伴的证书。

下表用于列出可信赖的伙伴站点的配置示例。由于并不是所有的实例都需要用到所有的参数，因此可选参数被放在括号中。

	发送方	**接收方**
辅件	sourceid	sourceid
	target	SOAPUrl
	SAMLUrl	[accountMapper]
	hostlist	[AuthType]
	[siteAttributeMapper]	[User]
		[certAlias]
POST 配置文件	sourceid	sourceid
	target	issuer
	POSTUrl	[accountMapper]
	[siteAttributeMapper]	[certAlias]

	发送方	接收方

SOAP 请求		`sourceid`
		`hostlist`
		[`attributeMapper`]
		[`actionMapper`]
		[`certAlias`]
		[`issuer`]

发送给目标 URL 的 POST

如果该属性中列出了站点中通过 SSO （可为辅件配置文件或 POST 配置文件）接收到的目标 URL，则从 SSO 接收到的一个或多个断言将通过 http:FORM POST 发送到目标 URL。避免使用 POST 中的测试 URL 或任何其他的 URL。

第 39 章

会话服务属性

会话服务属性是全局属性，也是动态属性。全局属性所采用的值将被应用到整个 Identity Server 配置中，并被所有已配置的组织所继承。（由于全局属性的用途在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。）

动态属性所采用的值将被应用到角色或组织中。如果将角色指定给用户或将用户指定给组织，则在默认情况下这些属性将被用户继承。在 “服务配置”中，所有在 Identity Server 上注册过的组织都设置有相应的默认会话值。通过为特定的组织注册会话服务、创建模板和输入一个不同于默认值的值，可以为不同的组织设置不同的会话值。

全局属性

全局属性包括：

搜索结果的最大数目

该属性指定会话搜索返回的结果的最大数目。默认值为 120。

搜索的超时时间 （秒）

该属性定义在会话搜索终止前，允许的最长搜索时间。默认值为 5 秒。

动态属性

动态属性包括：

最长会话时间 （分钟）

该属性的值以分钟为单位，这个值表示经过多长时间后会话将过期，过期后用户就必须重新验证才能重新获得访问权。它接受 1 以上 （含 0）的值。默认值为 120。（为了同时实现安全和方便两方面的要求，可以考虑将 “最长会话时间”的时间间隔设置为一个较大的值，而将 “最长空闲时间”的时间间隔设置为一个相对小的值。）“最长会话时间”限制了会话的有效性。会话不能超过设定的 “最长会话时间”。

最长空闲时间 （分钟）

该属性的值以分钟为单位，这个值表示会话在过期以前能够处于非活动状态的最长时间，过期后用户就必须重新验证才能重新获得访问权。它接受 1 以上 （含 0）的值。默认值为 30。（为了同时实现安全和方便两方面的要求，可以考虑将 “最长会话时间”的时间间隔设置为一个较大的值，而将 “最长空闲时间”的时间间隔设置为一个相对小的值。）

最长缓存时间 （分钟）

该属性的值以分钟为单位，这个值表示客户机联系 Identity Server 来刷新缓存的会话信息的最长时间间隔。它接受 0 以上 （含 0）的值。默认值为 3。建议最长缓存时间应始终小于最长空闲时间。

第 40 章

SOAP 绑定服务属性

SOAP 绑定属性是全局属性。它们所采用的值将被应用到整个 Sun Java System Identity Server 配置，并被每个已配置的组织所继承。（由于全局属性的目的在于自定义 Identity Server 应用程序，因此此类属性不能直接应用到角色和组织。）

SOAP 绑定属性包括：

请求处理程序列表

此属性存储有关 Identity Server 中所部署的 Web 服务提供商 (WSP) 的信息。其中所列条目包含关键字/值对 （用 “|” 分隔）。例如：

```
key=disco|class=com.example.identity.liberty.ws.disco.DiscoveryService|soa
pActions=sa1 sa2 sa2
```

要添加新的请求处理程序，请单击 “添加” 按钮。关键字和类参数都是必需的。所用参数包括：

关键字。此参数定义 WSP 的 SOAP 终点的 URI 路径的第二部分。 SOAP 服务将第一部分定义为 “特权”。例如，如果将 disco 定义为关键字，则搜索服务的 SOAP 终点为：

protocol://*hostname*:*port*/*deloy_uri*/Liberty/disco

类。此参数为 WSP 指定实现类的名称。特权 SOAP 层提供由每个 WSP 实现的处理程序界面，以处理请求的信息并返回响应信息。

SOAP 操作。这是一个用于指定受支持的 SOAP 操作的可选参数。如果未指定此参数，将支持所有 SOAP 操作。如果 Web 服务用户 (WSC) 所发送的请求含有不支持的 SOAP 操作， SOAP 层将拒绝该请求，而不会将其传送给相应的 WSP。

Web 服务验证器

此属性定义 `WebServiceAuthenicator` 界面的实现类，它将根据请求为 Web 服务用户 (WSC) 验证和生成一个证书。

支持的验证机制

此属性用于指定 SOAP 终点所支持的验证机制。默认情况下，所有机制都处于选定状态。如果 WSC 在某种验证机制未选定的情况下使用该验证机制发送了一个请求，则 SOAP 层将拒绝该请求，并且不会将其传送到相应的 WSP。

第 41 章

用户属性

用户属性包含在以下两个位置：“服务配置”窗口和 “用户管理”窗口。“服务配置”窗口中包含已注册组织的默认属性。“用户管理”窗口中包含用户项属性。

用户服务属性

用户服务属性是动态属性。动态属性所采用的值会被分配到 Identity Server 中配置的角色或组织。当角色被分配给用户，或用户被分配到组织时，动态属性将变为用户的一个特征。用户属性分为：

- 用户首选语言
- 用户首选时区
- 继承的语言环境
- 管理员 DN 起始视图
- 默认用户状态

默认的用户值是为所有 Identity Server 已注册的组织设置的。而通过以下操作可以为各个组织设置不同的用户值：先将用户服务注册到特定组织，然后创建模板并输入值 （非默认值）。

用户首选语言

该字段指定用户选择在 Identity Server 控制台中显示的文本语言。默认值为 en。该值会将一组本地化关键字映射到用户会话，这样，屏幕上的文本将以适合用户的语言显示。

用户首选时区

该字段指定用户访问 Identity Server 控制台时所在的时区。该字段没有默认值。

继承的语言环境

该字段指定用户的语言环境。默认值为 en_US。可以使用第 249 页的表 20-1 中的任何值。

管理员 DN 起始视图

如果用户是 Identity Server 管理员，该字段指定当该用户登录时，在 Identity Server 控制台中显示为起点的节点。该字段没有默认值。可以使用用户至少拥有读取权限的有效 DN。

默认用户状态

该选项用于指示新创建的用户的默认状态。该状态会由 “用户项”的状态取代。只有有效的用户才能通过 Identity Server 进行验证。默认值为 “有效”。可以从下拉菜单中选择以下任意一个选项：

- 有效 – 用户可以通过 Identity Server 进行验证。
- 无效 – 用户不能通过 Identity Server 进行验证，但用户配置文件仍会存储在目录中。

单个用户的状态可以通过以下操作设置：注册 “用户”服务，选择相应的值并将其应用到某个角色，然后将该角色添加到用户的配置文件中。

用户配置文件属性

用户配置文件属性是用户配置文件的默认属性。这些值由管理员或用户在登录时，在 “用户配置文件”视图中设置。管理员可以将自己的用户属性添加到用户配置文件中，也可以创建新服务。有关详细信息，参见 《Identity Server Developer's Guide》。

注 Identity Server 不强制用户项中的属性必须保持唯一。例如， `userA` 和 `userB` 可以在相同的组织中创建，他们的电子邮件地址属性都可以设置为 `jimb@madisonparc.com`。管理员可以配置 Sun Java System Directory Server 的属性唯一性插件，来强制使属性值唯一。有关详细信息，参见本章结尾处的 “唯一用户 ID”或参见 《*Sun Java System Directory Server 管理员指南*》。

名字

该字段中是用户的名字。（“名字”值和 “姓氏”值可以标识 Identity Server 控制台右上角 “当前已登录”字段中的用户。）

姓氏

该字段中是用户的姓氏。（“名字”值和 “姓氏”值可以标识 Identity Server 控制台右上角 “当前已登录”字段中的用户。）

全名

该字段中是用户的全名。

口令

该字段中是在 “用户 ID”字段中指定的名称的口令。

口令 （确认）

对口令进行确认。

电子邮件地址

该字段中是用户的电子邮件地址。

员工编号

该字段中是用户的员工编号。

电话号码

该字段中是用户的电话号码。

主页地址

该字段中是用户的主页地址。

用户状态

该选项指示是否允许用户通过 Identity Server 进行验证。只有有效的用户才能通过 Identity Server 进行验证。默认值为 “有效”。可以从下拉菜单中选择以下任意一个选项：

- 有效 – 用户可以通过 Identity Server 进行验证。
- 无效 – 用户不能通过 Identity Server 进行验证，但用户配置文件仍会存储在目录中。

注 将用户状态更改为“无效”将只影响通过 Identity Server 进行的验证。 Directory Server 将使用 nsAccountLock 属性来确定用户帐户的状态。对于 Identity Server 验证无效的用户帐户，仍可以执行不需要使用 Identity Server 的任务。要使目录中的用户帐户无效，而且不仅针对 Identity Server 验证，请将 nsAccountLock 设置为 true。如果委托管理员要定期将用户设置为无效，则可以将 nsAccountLock 属性添加到 Identity Server“用户配置文件”页面中。有关详细信息，参见《Identity Server Developer's Guide》。

帐户到期日期

如果存在该属性，则当前日期和时间超过指定的“帐户到期日期”时，验证服务将不允许登录。该属性的格式如下：

(mm/dd/yyyy hh:mm)

用户验证配置

该属性设置用户的验证方法。默认的验证方法是 LDAP。通过单击“编辑”链接可以选择一个或多个验证方法。如果选择多个验证方法，用户可能需要通过所有选定的方法来进行验证。

用户别名列表

该字段定义用户可能使用的别名列表。要使用该属性中配置的别名，必须修改 LDAP 服务，即向 LDAP 服务中的“用户条目搜索属性”字段添加 iplanet-am-user-alias-list 属性。

首选语言环境

该字段指定用户的语言环境。默认值为 en_US。可以使用第 249 页的表 20-1 中的任何值。

可以使用下拉菜单中的以下属性之一：

- 忽略
- 自定义
- 继承

成功 URL

该字段接受一系列的值，这些值用于指定验证成功后用户被重定向到的 URL。此属性的格式为 `clientType|URL`，尽管您可以只指定 URL 的值（默认类型为 HTML）

失败 URL

该字段接受一系列的值，这些值用于指定验证成功后用户被重定向到的 URL。此属性的格式为 `clientType|URL`，尽管您可以只指定 URL 的值（默认类型为 HTML）

唯一用户 ID

为了在 Identity Server 应用程序中强制使用户 ID 唯一， Directory Server 提供的插件必须进行如下配置：

```
dn:cn=uid uniqueness,cn=plugins,cn=config

objectClass:top

objectClass:nsSlapdPlugin

objectClass:extensibleObject

cn:uid uniqueness

nsslapd-pluginPath:/ids908/lib/uid-plugin.so

nsslapd-pluginInitfunc:NSUniqueAttr_Init

nsslapd-pluginType:preoperation

nsslapd-pluginEnabled:on

nsslapd-pluginarg0:attribute=uid

nsslapd-pluginarg1:markerObjectClass=nsManagedDomain
```

```
nsslapd-plugin-depends-on-type:database
nsslapd-pluginId:NSUniqueAttr
nsslapd-pluginVersion: 6.1
nsslapd-pluginVendor:Sun | SunONE
nsslapd-pluginDescription:Enforce unique attribute values
```

建议使用 nsManagedDomain 对象类来标记要使其中的用户 ID 唯一的组织。默认状态下，不会启用该插件。

要按组织进行配置，以使用户 ID 保持唯一，可以在插件项中添加每个组织的 DN，或者使用标记对象类选项并将 nsManagedDomain 添加到各个顶级组织项中。

```
nsslapd-pluginEnabled:on
nsslapd-pluginarg0:attribute=uid
nsslapd-pluginarg1:markerObjectClass=nsManagedDomain
```

错误代码

本附录提供了由 Sun Java System Identity Server 生成的错误消息列表。此列表并不全面，但本章提供的信息可作为解决一般问题的良好开端。本附录中列出的表格提供了错误代码、错误说明和/或可能的原因，并介绍了为解决所遇到的问题可以采取的操作。

本附录列出了以下功能方面的错误代码：

- Identity Server 控制台错误
- 验证错误代码
- 策略错误代码
- amadmin 错误代码

如果在诊断错误时需要更多帮助，请与 Sun 技术支持联系：

http://www.sun.com/service/sunone/software/index.html

Identity Server 控制台错误

下表介绍了由 Identity Server 控制台生成和显示的错误代码。

表 A-1 Identity Server 控制台错误

错误消息	说明 / 可能的原因	操作
删除以下内容时出现错误：	当前用户移除该对象之前，该对象可能已被其他用户移除。	重新显示正试图删除的对象，然后再次尝试删除操作。

表 A-1 Identity Server 控制台错误

错误消息	说明 / 可能的原因	操作
您输入的 URL 无效	如果输入的 Identity Server 控制台窗口的 URL 不正确，将会出现此错误。	
没有匹配搜索条件的条目。	在搜索窗口或过滤字段中输入的参数与目录中任何对象都不匹配。	输入另一组参数，然后再次运行搜索。
没有属性可以显示。	选中的对象不包含任何在其模式中定义的可编辑属性。	
该服务没有信息可以显示。	从 “服务配置” 模块查看到的服务不具有全局或基于组织的属性。	
已超出搜索大小限制。请改进搜索。	搜索中指定的参数所返回的条目数超过了允许返回的条目数。	将 “管理” 服务中的 “搜索返回的结果的最大数目” 属性修改为一个更大的值。您也可以修改搜索参数以加强限制。
已超出搜索时间限制。请改进搜索。	指定参数的搜索所耗费的时间已超出允许的范围。	将 “管理” 服务中的 “搜索的超时时间” 属性修改为一个更大的值。您也可以修改搜索参数，使其放宽限制，以返回更多的值。
用户的起始位置无效。请联系您的管理员。	用户条目中的起始位置 DN 已无效。	在 “用户配置文件” 页面中，将起始 DN 的值更改为有效 DN。
无法创建*身份对象*。用户不具有足够的访问权限。	操作由不具有足够权限的用户执行。用户拥有的权限决定了他们可以执行何种操作。	

验证错误代码

下表介绍了由验证服务生成的错误代码。这些错误在验证模块中显示给用户 / 管理员。

表 A-2 验证错误代码

错误消息	说明 / 可能的原因	操作
authentication.already.login.	用户已经登录并具有有效会话，但没有定义成功 URL 重定向。	注销或通过 Identity Server 控制台设置一些登录成功重定向 URL。使用以 “管理控制台 URL” 作为参数值的 “goto” 查询参数。
logout.failure.	用户无法退出 Identity Server。	重新启动服务器。
uncaught_exception	由于不正确的处理程序而抛出验证异常	检查登录 URL 是否包含无效或特殊字符。
redirect.error	Identity Server 无法重定向到成功重定向 URL 或失败重定向 URL。	检查 Web 容器的错误日志，查看是否有错误。
gotoLoginAfterFail	多数错误出现时均生成该链接。该链接将使用户返回原始登录 URL 页面。	
invalid.password	输入的口令无效。	口令必须包含至少 8 个字符。检查口令是否包含相应数量的字符并确保其未过期。
auth.failed	验证失败。这是显示在默认登录失败模板中的一般错误消息。最常见的原因是凭证无效 / 不正确。	输入有效和正确的用户名 / 口令（被调用的验证模块需要的凭证）。
nouser.profile	在给定组织中未找到匹配输入的用户名的用户配置文件。登录到成员资格 / 自注册验证模块时，可能显示此错误。	再次输入您的登录信息。如果是第一次登录，请在登录屏幕中选择 “新用户”。
notenough.characters	输入口令的字符数不足。登录到成员资格 / 自注册验证模块时，可能显示此错误。	默认情况下，登录口令必须包含至少 8 个字符 （此数目可通过成员资格验证模块配置）。

表 A-2 验证错误代码

错误消息	说明 / 可能的原因	操作
useralready.exists	在给定组织中已存在此用户名。登录到成员资格 / 自注册验证模块时，可能显示此错误。	用户 ID 在组织内必须唯一。
uidpasswd.same	“用户名”字段和 “口令”字段的值不能相同。登录到成员资格 / 自注册验证模块时，可能显示此错误。	确保用户名和口令不相同。
nouser.name	未输入用户名。登录到成员资格 / 自注册验证模块时，可能显示此错误。	确保输入用户名。
no.password	未输入口令。登录到成员资格 / 自注册验证模块时，可能显示此错误。	确保输入口令。
missing.confirm.passwd	缺少确认口令字段。登录到成员资格 / 自注册验证模块时，可能显示此错误。	确保在 “确认口令”字段中输入口令。
password.mismatch	口令与确认口令不匹配。登录到成员资格 / 自注册验证模块时，可能显示此错误。	确保口令与确认口令匹配。
存储用户配置文件时出现错误。	存储用户配置文件时出现错误。登录到成员资格 / 自注册验证模块时，可能显示此错误。	确保 `Membership.xml` 文件中包含的针对自注册的属性和元素有效、正确。
orginactive	该组织处于非活动状态。	通过 Identity Server 控制台，将组织状态从 “无效”更改为 “有效”来激活组织。
internal.auth.error	内部验证错误。这是一个通用验证错误，可能是由不同和多个环境和 / 或配置问题所导致。	

表 A-2 验证错误代码

错误消息	说明 / 可能的原因	操作
usernot.active	用户已不处于有效状态。	通过管理控制台将用户状态从“无效”更改为“有效”来激活用户。 如果用户已通过“内存锁定”被锁定，请重新启动服务器。
user.not.inrole	用户不属于指定的角色。进行基于角色的验证时显示此错误。	确保登录用户属于为基于角色的验证指定的角色。
session.timeout	用户会话已超时。	请重新登录。
authmodule.denied	指定的验证模块被拒绝。	确保必需的验证模块在必需的组织下注册，并为该模块创建和保存模板，还要在核心验证模块的“组织验证模块”列表中选择该模块。
noconfig.found	未找到配置。	检查验证配置服务以查找必需的验证方法。
cookie.notpersistent	永久性 Cookie 域中不存在永久性 Cookie 用户名。	
nosuch.domain	已找到组织。	确保请求的组织有效并且正确。
userhasnoprofile.org	用户在指定的组织中没有配置文件。	确保用户在本地 Directory Server 中的指定的组织中存在并且有效。
reqfield.missing	未完成某一必需字段。请确保在所有必需字段中均输入值。	确保在所有必需字段中均输入值。
session.max.limit	已达到最大会话限制。	注销，然后再次登录。

策略错误代码

下表介绍了由策略框架生成并显示在 Identity Server 控制台中的错误代码。

表 A-3 策略错误代码

错误消息	说明 / 可能的原因	操作
illegal_character_/_in_name	策略名称中含有非法字符 “/”。	确保策略名称中不包含 “/” 字符。
policy_already_exists_in_org	具有相同名称的规则已存在。	使用其他名称创建策略。
rule_name_already_present	另一个具有给定名称的规则已存在。	使用其他规则名称创建策略。
rule_already_present	具有相同规则值的规则已存在。	使用其他规则值。
no_referral_can_not_create_policy	组织中不存在参照策略。	为了在子组织下创建策略，必须在其父组织创建参照策略，以表明该子组织可以引用何种资源。
ldap_search_exceed_size_limit	已超出 LDAP 搜索大小限制。由于搜索找到的结果数目超出结果的最大数目而出现错误。	更改组织的搜索模式或策略配置，从而修改搜索控制参数。搜索大小限制位于策略配置服务中。
ldap_search_exceed_time_limit	已超出 LDAP 搜索时间限制。由于搜索找到的结果数目超出结果的最大数目而出现错误。	更改组织的搜索模式或策略配置，从而修改搜索控制参数。搜索时间限制位于策略配置服务中。
ldap_invalid_password	LDAP 绑定口令无效。	策略配置中定义的 LDAP 绑定用户的口令不正确。这会导致无法获得通过验证的 LDAP 连接从而执行策略操作。
app_sso_token_invalid	应用程序 SSO 令牌无效。	服务器无法验证应用程序 SSO 令牌。很可能 SSO 令牌已过期。

表 A-3 策略错误代码

错误消息	说明 / 可能的原因	操作
user_sso_token_invalid	用户 SSO 令牌无效。	服务器无法验证用户 SSO 令牌。很可能 SSO 令牌已过期。
property_is_not_an_Integer	属性值不是整数。	该插件的属性的值应为整数。
property_value_not_defined	应定义属性值。	为给定属性提供一个值。
start_ip_can_not_be_greater_than_end_ip	起始 IP 大于结束 IP。	尝试在 IP 地址条件中将结束 IP 地址设置为大于起始 IP 地址。起始 IP 不能大于结束 IP。
start_date_can_not_be_larger_than_end_date	起始日期大于结束日期。	尝试在策略的 “时间条件”中将结束日期设置为大于起始日期。起始日期不能大于结束日期。
policy_not_found_in_organization	在组织中未找到策略。试图在组织中定位不存在的策略时出现错误。	确保策略在指定的组织下存在。
insufficient_access_rights	用户不具有足够的访问权限。用户不具有执行策略操作的足够权限。	具有相应访问权限的用户才能执行策略操作。
invalid_ldap_server_host	LDAP 服务器主机无效。	更改在策略配置服务中输入的无效 LDAP 服务器主机。

amadmin 错误代码

下表介绍了由 amadmin 命令行工具生成并显示在 Identity Server 的调试文件中的错误代码。

表 A-4 amadmin 错误代码

错误消息	代码	说明 / 可能的原因	操作
nocomptype	1	变量过少。	确保在命令行中提供强制性变量（--runasdn、 --password、 --passwordfile、 --schema、 --data 和 --addAttributes）及其值。
file	2	未找到输入 XML 文件。	检查语法并确保输入 XML 有效。
nodnforadmin	3	--runasdn 值中缺少用户 DN。	在 --runasdn 值中提供用户 DN。
noservicename	4	--deletservice 值中缺少服务名称。	在 --deleteservice 值中提供服务名称。
nopwdforadmin	5	--password 值中缺少口令。	在 --password 值中提供口令。
nolocalename	6	未提供语言环境名称。默认语言环境为 en_US。	有关语言环境的列表，参见默认验证语言环境。
nofile	7	缺少 XML 输入文件。	至少提供一个输入 XML 文件名以供处理。
invopt	8	一个或多个变量不正确。	检查是否所有变量均有效。对于一组有效变量，键入 amadmin --help。
oprfailed	9	操作已失败。	amadmin 失败时，会产生更精确的错误代码以表明特定错误。请参考这些错误代码来评估问题。
execfailed	10	无法处理请求。	amadmin 失败时，会产生更精确的错误代码以表明特定错误。请参考这些错误代码来评估问题。
policycreatexception	12	无法创建策略。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。

表 A-4 amadmin 错误代码

错误消息	代码	说明 / 可能的原因	操作
policydelexception	13	无法删除策略。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
smsdelexception	14	无法删除服务。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
ldapauthfail	15	无法验证用户。	确保用户 DN 和口令正确。
parserror	16	无法分析输入 XML 文件。	确保 XML 被正确格式化并符合 amAdmin.dtd。
parseiniterror	17	由于应用程序错误或分析器初始化错误导致无法分析。	确保 XML 被正确格式化并符合 amAdmin.dtd。
parsebuilterror	18	由于无法生成具有指定选项的分析器导致无法分析。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
ioexception	19	无法读取输入 XML 文件。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
fatalvalidationerror	20	由于 XML 文件不是有效文件导致无法分析。	检查语法并确保输入 XML 有效。
nonfatalvalidationerror	21	由于 XML 文件不是有效文件导致无法分析。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
validwarn	22	XML 文件验证时出现的警告。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
failedToProcessXML	23	无法处理 XML 文件。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
nodataschemawarning	24	命令中既没有 --data 选项也没有 --schema 选项。	检查是否所有变量均有效。对于一组有效变量，键入 amadmin --help。

表 A-4 amadmin 错误代码

错误消息	代码	说明 / 可能的原因	操作
doctyperror	25	XML 文件不符合正确的 DTD。	检查 XML 文件中的 DOCTYPE 元素。
statusmsg9	26	由于 DN、口令、主机名或端口号无效导致 LDAP 验证失败。	确保用户 DN 和口令正确。
statusmsg13	28	服务管理器异常 （SSO 异常）。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
statusmsg14	29	服务管理器异常。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
statusmsg15	30	模式文件输入流异常。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
statusmsg30	31	策略管理器异常 （SSO 异常）。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
statusmsg31	32	策略管理器异常。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
dbugerror	33	指定了多个调试选项。	只能指定一个调试选项。
loginFalied	34	登录失败。	amadmin 会产生异常消息以表明特定错误。请参考这些消息来评估问题。
levelerr	36	属性值无效。	检查为 LDAP 搜索设置的级别。该级别应为 SCOPE_SUB 或 SCOPE_ONE。
failToGetObjType	37	获得对象类型时出现的错误。	确保 XML 文件中的 DN 有效且包含正确的对象类型。
invalidOrgDN	38	组织 DN 无效。	确保 XML 文件中的 DN 有效并为组织对象。

表 A-4 amadmin 错误代码

错误消息	代码	说明 / 可能的原因	操作
invalidRoleDN	39	角色 DN 无效。	确保 XML 文件中的 DN 有效并为角色对象。
invalidStaticGroupDN	40	静态组 DN 无效。	确保 XML 文件中的 DN 有效并为静态组对象。
invalidPeopleContainerDN	41	用户容器 DN 无效。	确保 XML 文件中的 DN 有效并为用户容器对象。
invalidOrgUnitDN	42	组织单元 DN 无效。	确保 XML 文件中的 DN 有效并为容器对象。
invalidServiceHostName	43	服务主机名无效。	确保用于检索有效会话的主机名正确。
subschemaexception	44	子模式错误。	只有全局属性和组织属性支持子模式。
serviceschemaexception	45	无法定位服务的服务模式。	确保 XML 文件中的子模式有效。
roletemplateexception	46	仅当模式类型为动态时，角色模板才可以为 true。	确保 XML 文件中的角色模板有效。
cannotAddusersToFileredRole	47	无法将用户添加到过滤的角色。	确保 XML 文件中的角色 DN 不是过滤的角色。
templateDoesNotExist	48	模板不存在。	确保 XML 文件中的服务模板有效。
cannotAdduUersToDynamicGroup	49	无法将用户添加到动态组。	确保 XML 文件中的组 DN 不是动态组。
cannotCreatePolicyUnderContainer	50	无法在容器的子组织中创建策略。	确保要在其中创建策略的组织不是容器的子组织。
defaultGroupContainerNotFound	51	未找到组容器。	创建父组织或容器的组容器。
cannotRemoveUserFromFilteredRole	52	无法从过滤的角色中移除用户。	确保 XML 文件中的角色 DN 不是过滤的角色。
cannotRemoveUsersFromDynamicGroup	53	无法从动态组中移除用户。	确保 XML 文件中的组 DN 不是动态组。
subSchemStringDoesNotExist	54	子模式字符串不存在。	确保 XML 文件中存在子模式字符串。

表 A-4 amadmin 错误代码

错误消息	代码	说明 / 可能的原因	操作
defaultPeopleContainerNotFound	59	您正尝试向组织或容器添加用户。而组织或容器中不存在默认用户容器。	请确保存在默认用户容器。
nodefaulturlprefix	60	在 --defaultURLPrefix 参数后未找到默认 URL 前缀	请相应提供默认的 URL 前缀。
nometaalias	61	在 --metaalias 参数后未找到元数据别名	请相应提供元数据别名。
missingEntityName	62	未指定实体名称。	请提供实体名称。
missingLibertyMetaInputFile	63	缺少用于导入元数据的文件名。	请提供包含元数据的文件名称。
missingLibertyMetaOutputFile	64	缺少用于存储已导出元数据的文件名。	请提供用于存储元数据的文件名称。
cannotObtainMetaHandler	65	无法获得元数据属性的处理程序。指定的用户名和口令可能不正确。	确保用户名和口令正确。
missingResourceBundleName	66	添加、查看或删除存储在目录服务器中的资源包时，缺少资源包名称。	请提供资源包名称
missingResourceFileName	67	向目录服务器中添加资源包时，缺少包含资源字符串的文件的文件名。	请提供有效文件名。
failLoadLibertyMeta	68	无法将特权元数据加载到 Directory Server。	再次加载元数据之前，请重新检查元数据。

术语表

有关本文档集中所使用术语的列表，参见最新的 《*Sun Java™ Enterprise System Glossary*》，网址为：

http://docs.sun.com/doc/816-6873

A

B

C

D

F

G

H

I

J

K

L

M

N

P

Q

R

S

T

U

V

W

X

Y

Z

Z