管理指南

Sun™ ONE Identity Server

版本 6.1

817-4409-10
2003 年 12 月

目录

关于本指南

《*Sun*™ ONE *Identity Server* **管理指南**》介绍有关如何自定义 Sun ONE Identity Server 并将其功能集成到组织的当前技术基础结构当中的信息。本指南还包含关于产品及其 API 的程序方面的信息。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 ONE Server 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。管理员应具备以下知识：

- 轻便目录存取协议 (LDAP)
- Java™
- JavaServer Pages™ (JSP)
- 超文本传输协议 (HTTP)
- 超文本标记语言 (HTML)
- 可扩展标记语言 (XML)

由于 Identity Server 部署使用 Sun ONE Directory Server 作为数据存储库，因此，管理员还应该熟悉该产品附带的文档。可以联机查看最新的 Directory Server 文档。

Identity Server 6.1 文档集

Identity Server 文档集包括两套核心手册：Sun ONE Identity Server 6.1 核心应用程序手册和 Sun ONE Identity Server 策略代理手册。

Identity Server 核心文档

Identity Server 文档集包含下列书目：

- *Product Brief*，提供了 Identity Server 应用程序及其特征和功能的概述。
- **移植指南**，详细介绍了如何将现有数据和 Sun ONE 产品部署迁移到最新版本的 Identity Server。有关安装 Identity Server 的说明，请参见 *Sun Java Enterprise System 2003Q4 Installation Guide*。
- **管理指南**，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。
- *Customization and API Guide*，介绍如何自定义 Identity Server 的安装。它还提供如何使用公用 API 在应用程序中增加新服务的说明。
- *Deployment Guide*，介绍有关基于现有信息技术基础结构规划 Identity Server 部署的信息。
- **发行说明**，可以在产品发行后通过联机方式获得。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 Sun ONE 文档 Web 站点的 Identity Server 页面中找到**发行说明**的更新和到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 策略代理文档集

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。此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 Identity Server 策略代理，它可以保护各种托管的 J2EE 应用程序。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都有一个**发行说明**文件。这些**发行说明**中收集了各种最新的信息，包括此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 ONE 文档 Web 站点的策略代理页面中找到**发行说明**的更新和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，欢迎您提出宝贵的意见和建议。请您将意见和建议发送至 `docfeedback@sun.com`。

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

以下是一些在 Identity Server 文档集中通用的术语：

- *Identity Server* 指 Identity Server 和所有已安装的 Identity Server 软件实例。
- **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 ONE Directory Server 实例。
- *Application Server* 指已安装的 Sun ONE Application Server 实例。
- *Web Server* 指已安装的 Sun ONE Web Server 实例。
- *IdentityServer_base* 代表 Identity Server 所在的安装主目录的变量占位符。
- *DirectoryServer_base* 代表 Sun ONE Directory Server 所在的安装主目录的变量占位符。
- *ApplicationServer_base* 代表 Sun ONE Application Server 所在的安装主目录的变量占位符。
- *WebServer_base* 代表 Sun ONE Web Server 所在的安装主目录的变量占位符。
- **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）。

相关信息

除了 Identity Server 附带的文档之外，另外还有几种文档集也会对您有所帮助。表 0-1 列出了这些文档集和附加的信息源。

表 0-1 到何处去查找相关的 Sun ONE 资源

信息或资源	Internet 位置
Directory Server 文档	http://docs.sun.com/coll/S1_DirectoryServer_52
Web Server 文档	http://docs.sun.com/coll/S1_websvr61_en
Web Proxy Server 文档	http://docs.sun.com/prod/s1.webproxys#hic
Sun ONE 下载中心	http://wwws.sun.com/software/download/
Sun ONE 技术支持	http://www.sun.com/service/sunone/software/index.html
Sun ONE 专业服务信息	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

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、产品或其它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 1 部分

Identity Server 控制台指南

本部分是《*Sun™ ONE Identity Server* **管理指南**》的第一部分。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 1 章

产品概述

本章提供 Sun™ ONE Identity Server 的功能概述。本章包含以下内容：

Sun ONE Identity Server

Sun ONE Identity Server 技术是用于 Network Identity 的 Sun Open Net Environment (Sun ONE) Platform 的一部分。 Identity Server 是一组工具，用于发挥 Sun ONE Directory Server 的管理和安全功能 （基于轻便目录存取协议 [LDAP] 的数据存储）。 Identity Server 将 Directory Server 与用户验证及可增强数据安全性的单一登录功能集成在一起。它还允许管理员启动基于**角色**的用户条目管理，以及在用户条目中显示为属性的条目分组机制。最后，开发者还可以定义和管理多个缺省服务和自定义服务的配置参数。通过一个可自定义的图形用户界面 （即基于浏览器的 Identity Server 控制台）可以使用所有这三项功能。

Identity Server 的功能

Identity Server 是在 Directory Server 的安装的顶层建立的。旨在为目录管理员提供一个更直观一致的界面及用于扩展 Directory Server 的功能的功能。

服务配置

可以使用 Identity Server 服务管理组件指定缺省的和自定义的业务服务的配置参数。通过使用在 Identity Server 框架内定义的 XML 和 DTD，服务开发者可以定义企业服务 （如邮件服务、记账服务或日志服务）的参数，还可以管理服务的参数或**属性**。此外， Identity Server 还允许服务管理员定义这些属性的值。

策略管理

Identity Server 还提供定义、修改或删除规则的方法，这些方法用于控制对业务资源的访问。这些规则统称为**策略**。

SAML

Identity Server 使用安全断言标记语言 (SAML) 来交换安全信息。 SAML 定义了可扩展标记语言 (XML) 框架，以在提供此类信息的不同供应商平台之间实现相互可用性。 *Sun ONE Identity Server Customization and API Guide* 中介绍了 SAML 框架。

联合管理

Identity Server 集成了 “联合管理”模块，以使用由 Liberty Alliance Project 开发的适用于联合网络身份的开放标准。

验证

Identity Server 提供了用于用户验证的插件解决方案。验证特定用户所需的条件基于为 Identity Server 企业中的各个组织配置的验证服务。在能够访问 Identity Server 会话之前，用户必须成功地通过验证。

单一登录

用户通过验证之后，用于单一登录 (SSO) 的 Identity Server 的 API 将开始运行。已通过验证的用户每次尝试访问受保护的页面时， SSO API 将根据用户的验证凭证确定他们是否具有所需的权限。如果用户为有效用户，则无需进行其它验证即可访问该页面。如果用户不是有效用户，系统将提示用户再次进行验证。

策略代理

策略代理安装在 Web 容器 （Sun ONE Web Server 或 Sun ONE Application Server）上。它是 Identity Server 策略组件的特定实例。用户向受保护的 Web Server 上的 Web 资源发送请求时，此代理将作为附加验证步骤运行。此验证不属于资源必须执行的用户验证检查。该代理用于保护 Web Server，而资源由验证插件保护。

身份管理

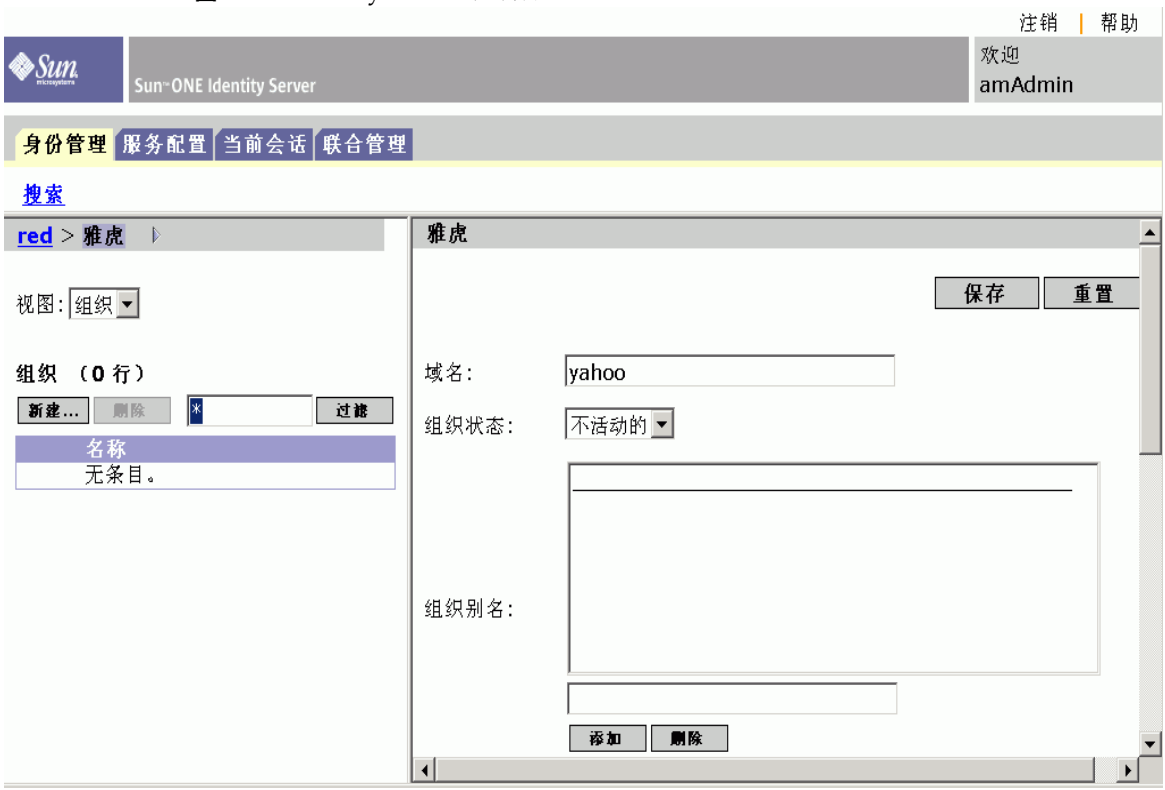
可以使用身份管理组件创建和管理与身份相关的对象。使用 Identity Server 控制台或命令行界面可以定义、修改或删除用户、角色、组、策略、组织、子组织和容器对象。控制台的缺省管理员具有不同等级的特权，这些特权用于创建和管理组织、组、容器、用户、服务和策略。（可以基于角色创建其他管理员。）管理员是在与 Identity Server 一起安装 Directory Server 时，在后者中进行定义的。这些管理员包括：

- 顶层管理员，对 Identity Server 企业内的所有条目具有读写权限。
- 顶层帮助台管理员，对 Identity Server 企业内的所有条目具有读取权限，并对用户密码属性具有写入权限。
- 组织管理员，对其组织内的所有条目具有读写权限。
- 组织帮助台管理员，对其组织内的所有条目具有读取权限。
- 容器管理员，对所有组管理员具有读写权限，而组管理员对其组的所有成员具有读写权限。

Identity Server 控制台

Identity Server 控制台分为三个部分：位置框、浏览框和数据框。通过使用这三个框，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 1-1 Identity Server 控制台



标题框

标题框位于控制台的顶部。标题框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 的缺省服务。
- “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”字段用于指明管理员在目录树中的位置。此路径用于进行浏览。

“欢迎进入”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”链接可以打开包含有关身份管理、当前会话、联合管理以及本文档的第 3 部分 “属性参考指南”的信息的浏览窗口。

“退出”链接允许用户从 Identity Server 中退出。

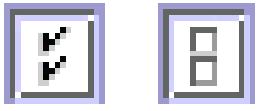
浏览框

浏览框是 Identity Server 控制台的左侧部分。**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。（浏览框中显示的大多数对象将具有相应的**属性**链接。选择此链接将在右侧的数据框中显示条目的属性。）“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。

数据框

数据框是控制台的右侧部分。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。



第 2 章

身份管理

本章介绍 Sun™ ONE Identity Server 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。本章包含以下内容：

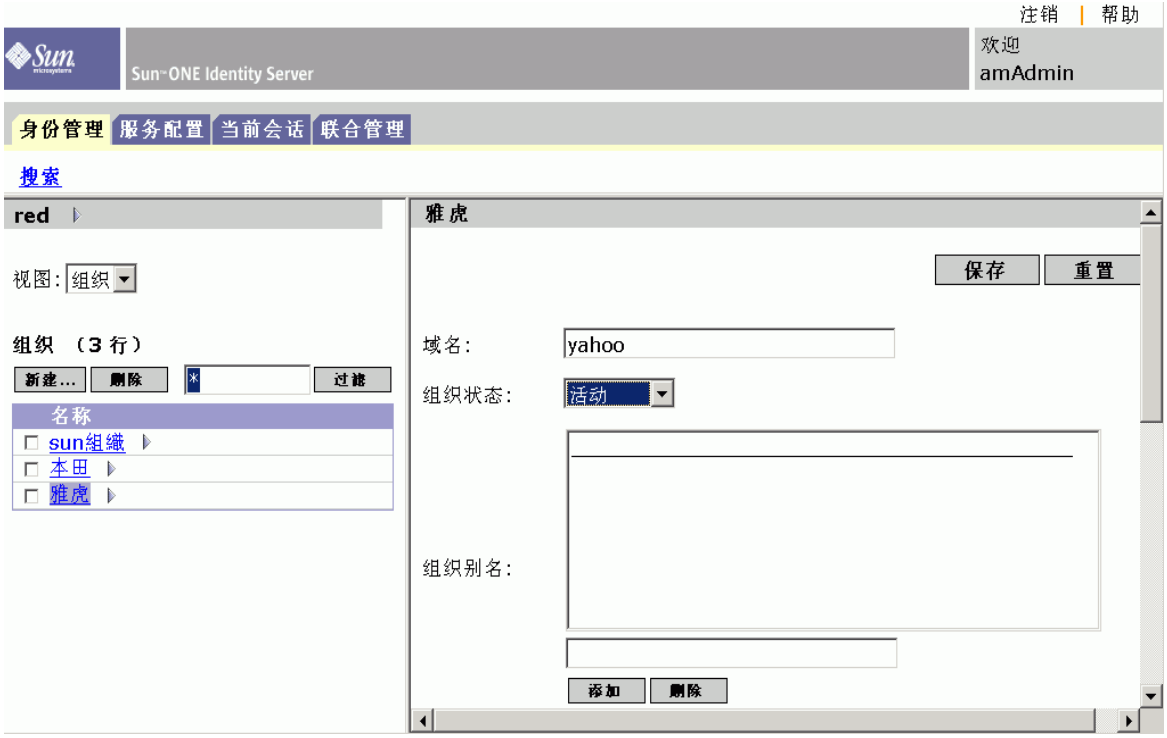
“身份管理”界面

Identity Server 图形用户界面有两种基本视图。用户可以访问 “身份管理”视图或“用户配置文件”视图，具体取决于用户登录的角色。

“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，其缺省视图为 “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。

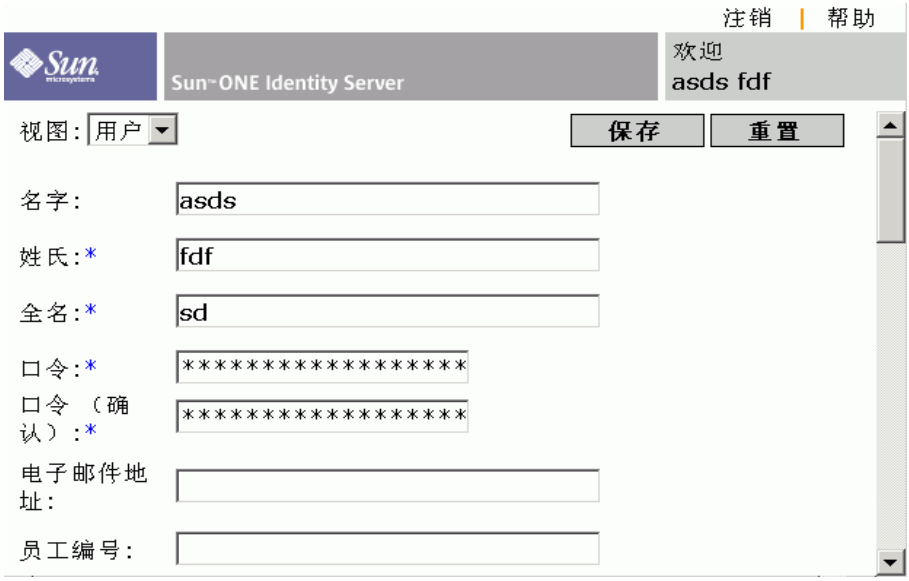
图 2-1 显示了组织属性的“身份管理”视图



“用户配置文件”视图

当未被指定管理角色的用户在 Identity Server 中进行验证时，缺省视图为用户自己的“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、家庭地址和密码。“用户配置文件”视图中显示的属性可以扩展。有关为对象和身份添加自定义属性的详细信息，请参见 *Sun ONE Identity Server Customization and API Guide*。

图 2-2 “用户配置文件”视图



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、角色和策略）所需的所有组件。本节说明对象类型及其详细配置方法。

属性函数

要查看或修改条目的属性，请单击对象名称旁边的 “属性”箭头。对象的属性和相应的值将显示在数据框中。不同的对象显示不同的属性。

有关如何扩展条目属性的信息，请参见 *Sun ONE Identity Server Customization and API Guide*。

组织

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

创建组织

1. 从 “身份管理” 模块的 “查看” 菜单中选择 “组织”。
2. 单击浏览框中的 “新建”。

   数据框中将显示 “新建组织” 模板。
3. 在 “新建组织” 模板中输入组织的名称。
4. 选择 “有效” 或 “无效” 状态。

   缺省值为 “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。
5. 根据需要输入其它可选字段的值。这些字段包括：

   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`，将 `123` 和 `abc` 定义为组织的别名，则可以使用以下任一 URL 登录到组织：

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

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

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

   域名。输入组织的完整域名系统 (DNS) 名称 （如果存在）。

   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`，则可以使用以下任一 URL 登录到组织：

   ```
   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，如果添加了指定电子邮件地址的唯一属性名，则不能创建具有相同电子邮件地址的两个用户。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 `PreferredDomain` 被定义为 `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。

6. 单击 “创建”。

   浏览框中将显示新创建的组织。

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 “过滤”。

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。当创建或修改策略时，可以在策略的 “主题”页面上将组织、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，请参见第 79 页中的 “修改策略”。

组

组代表具有共同功能、特性或利益的用户集合。通常来说，这种分组不会涉及特权。可以在两个级别创建组：组织中和其它被管理的组中 （作为子组）。可以静态或动态地 （通过过滤）将用户添加到管理的组中。

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，请参见第 153 页中的 “管理的组类型”。

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 缺省情况下，管理的组类型为动态的。您可以在 “管理”服务配置中更改此缺省设置。

创建管理的组

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. 从数据框中选择组类型。

   如果要创建静态订阅组，请选择 “按订阅指定成员”。

   a. 在 “名称”字段中输入组的名称。单击 “下一步”。
   b. 选择 “用户可以订阅该组”属性可以使用户自行订阅组。
   c. 从 “成员列表”中选择 “添加”可以将用户添加到组。
   d. 输入搜索条件并单击 “过滤”。当返回到用户列表时，选择要添加的用户并单击 “提交”。将用户添加到组是可选的。可以在创建完组后再添加用户。
   e. 单击 “创建”。

   如果要创建动态 （通过 LDAP 过滤的）组，请选择 “按过滤指定成员”。

   a. 在 “名称”字段中输入组的名称。单击 “下一步”。
   b. 构造 LDAP 搜索过滤器。
   c. 构造过滤器的字段使用 OR 或 AND 运算符。 UI 中列出的所有字段都会用到。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。
   d. 单击 “创建”。

删除管理的组

1. 找到要删除的组所在的组织。
2. 从 “查看”菜单中选择 “组”。
3. 选中要删除的组名称旁边的复选框。
4. 单击 “删除”。

注 应与 Directory Server 一同对 Identity Server 进行配置以使用引用完整性插件。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项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，请参见 《*Sun One Identity Server* **移植指南**》。

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。当创建或修改策略时，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，请参见第 79 页中的 “修改策略”。

用户

用户代表个人的身份。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，从角色和 / 或组中添加或删除用户，还可以给用户指定服务。

创建用户

1. 找到要在其中创建用户的组织、容器或人员容器 （也可以从 “用户创建” 页面选择人员容器）。
2. 从 “查看” 菜单中选择 “用户”。
3. 单击 “新建”。

   数据框中将显示 “新建用户” 页面。
4. 输入所需的属性值，并在所有可选字段中输入值。

   有关用户配置文件属性的信息，请参见第 263 页中的 “用户属性”。
5. 单击 “创建”。

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. 在浏览框中选择要修改的用户，然后单击属性箭头。
4. 从数据框的 “查看” 菜单中选择 “角色” 或 “组”。

   在 “用户” 视图中，您可以修改定义了用户服务的属性。

5. 选择要向其添加用户的角色或组，然后单击 “保存”。无法显示已过滤的角色和组。

将服务添加到用户

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. 在浏览框中选择要修改的用户，然后单击属性箭头。
4. 从数据框的 “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. 找到要删除的用户所在的组织。
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”。

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。当创建或修改策略时，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，请参见第 79 页中的 “修改策略”。

服务

激活组织或容器 （容器与组织的行为相同）的服务要通过两个步骤来完成。首先，需要将服务注册到组织。注册服务之后，必须创建一个专门为该组织配置的模板。有关其它信息，请参见第 3 章 “服务配置”。

注 新服务必须先通过命令行的 `amadmin` 命令导入到 Identity Server 中。有关导入服务的 XML 模式的信息，请参见 *Sun ONE Identity Server Customization and API Guide*。

注册服务

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”，然后从浏览框中选择组织。“位置”路径可以显示缺省的顶层组织和选定的组织。

2. 从“查看”菜单中选择“服务”。

3. 单击“注册”。

   数据框中将显示可注册到该组织的服务列表。

4. 选中要添加的服务旁边的复选框。

5. 单击“注册”。浏览框中将显示已注册的服务。

注 只有为顶层组织注册的服务才会在角色级别显示。

创建服务的模板

1. 找到注册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”，然后从浏览框中选择组织。

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。

   数据框中将显示消息**没有适用于此服务的模板。要创建模板吗？**

4. 单击“创建”。

   将为父组织或角色的该服务创建模板。数据框中将显示该服务的缺省属性和值。有关缺省服务属性的说明，请参见第 149 页中的“属性参考指南”。

5. 接受或修改缺省值，然后单击“保存”。

撤消注册服务

1. 找到要删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”，然后从浏览框中选择组织。

2. 从“查看”菜单中选择“服务”。

3. 选中要删除的服务的复选框。

4. 单击 “撤消注册”。

注 如果服务是在子组织级别注册的，则无法在父组织级别撤消注册该服务。

角色

角色是与**组**概念类似的 Directory Server 项机制。组有成员，角色也有成员。角色的成员是拥有该角色的 LDAP 项。角色本身的条件被定义为具有属性的 LDAP 项，由项的独特的名称 (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它 Directory Server 角色类型，只是它们不能被 Identity Server 控制台管理。其它 Directory Server 类型可以在策略的主题定义中使用。有关策略主题的详细信息，请参见第 76 页中的 “策略管理”。

用户可以拥有一个或多个角色。例如，可以创建具有 “会话服务”和 “URL 策略代理服务”中的属性的承包商角色。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。如果承包商随后将成为全职员工，管理员只需重新为用户指定其它的角色即可。

Identity Server 使用角色来应用访问控制指令。首次安装 Identity Server 时，Identity Server 会配置用于定义管理员权限的访问控制指令 (ACI)。这些 ACI 随后会被指定为角色 （例如，组织管理角色和组织帮助桌面管理角色），当这些角色被指定到用户时会定义用户的访问权限。

只有当管理服务中启用了 “显示用户的角色”属性时，用户才可以查看给他们指定的角色。有关详细信息，请参见第 160 页中的 “显示用户的角色”。

与组类似，角色也可以通过过滤创建，或者以静态方式创建。

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，所有用户都会被过滤器过滤并被指定到角色。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。

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。

创建过滤的角色

1. 在浏览框中，找到要在其中创建角色的组织。

2. 从 “查看” 菜单中选择 “角色”。

   在配置组织时会创建一组缺省角色，这些角色就显示在浏览框中。

   有关这些角色的说明，请参见 “属性参考” 一节中的第 156 页中的 “动态管理员角色 ACI”。

3. 单击浏览框中的 “新建”。数据框中将显示 “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，以确定在 DIT 中从何处启动用户。管理角色会通知控制台，角色的所有人拥有管理特权；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” 菜单中选择缺省的一组权限，以应用到角色。

   拥有这些权限，可以访问组织中的项。第 154 页中的 “缺省角色权限 (ACI)”一节中对这些权限进行了说明。（显示的缺省权限未按照特定顺序排列。）

   通常，“无权限 ACI” 会指定给服务角色，而缺省的 ACI 会指定给管理角色。

8. 输入搜索条件信息。这些字段包括：

   逻辑运算符。允许您使用逻辑运算符连接所有用于过滤的字段。 AND 将根据所有指定字段返回用户。 OR 将根据指定的任一字段返回用户。

   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=*))))
   ```

   如果过滤器保留为空，将缺省创建以下角色：

   ```
   (objectclass = inetorgperson)
   ```

   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。

9. 单击 “创建” 以启动基于过滤条件的搜索。通过过滤条件定义的用户会自动被指定到角色。

创建静态角色

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

   在配置组织时会创建一组缺省角色，这些角色就显示在浏览框中。

   有关这些角色的说明，请参见 “属性参考” 一节中的第 156 页中的 “动态管理员角色 ACI”。
3. 单击浏览框中的 “新建”。数据框中将显示 “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，以确定在 DIT 中从何处启动用户。管理角色会通知控制台，角色的所有人拥有管理特权；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” 菜单中选择缺省的一组权限，以应用到角色。

   拥有这些权限，可以访问组织中的项。第 154 页中的 “缺省角色权限 (ACI)” 一节中对这些权限进行了说明。（显示的缺省权限未按照特定顺序排列。）

   通常，“无权限 ACI” 会指定给服务角色，而缺省的 ACI 会指定给管理角色。
8. 单击 “创建”。

   创建的角色显示在浏览框中，角色的状态信息显示在数据框中。

   角色可用的服务是从角色的父组织中继承的。如果尚未创建服务模板，可以通过单击 “编辑” 链接为角色创建服务模板。如果已经存在服务模板，将显示服务属性，并且可以进行配置。有关详细信息，请参见第 46 页中的 “自定义角色的服务”。

向静态角色添加用户

1. 选择要修改的角色，然后单击属性箭头。
2. 从数据框中的 “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：

   逻辑运算符。允许您使用逻辑运算符连接所有用于过滤的字段。 AND 将根据所有指定的字段返回用户。 OR 将根据指定的任一字段返回用户。

   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。

   根据值返回用户。用于指定搜索要返回的值。

5. 单击 “过滤” 开始搜索。
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 “保存”。

   用户将被分配到角色。

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

从角色删除用户

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”，然后从浏览框中选择组织。

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. 选中要删除的用户的复选框。
6. 单击 “删除”。

   用户将从角色中删除。

注 应与 Directory Server 一同对 Identity Server 进行配置以使用引用完整性插件。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项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，请参见 《*Sun One Identity Server* **移植指南**》。

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。当创建或修改策略时，可以在策略的 “主题”页面上将组织、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，请参见第 79 页中的 “修改策略”。

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。使用 “常规”视图，管理员可以自定义 “服务”和 “用户”页面，并创建仅对特定服务拥有访问权限的服务管理员。例如，管理员可以拒绝某个给定角色对用户服务中的一个或多个属性拥有写权限，而拥有该角色的用户也不能修改这些属性。通过允许对所有策略服务进行访问，而拒绝对其它服务进行访问，可以创建策略管理员角色。拥有策略管理员角色的管理员将能够创建并指定策略，但无法执行用户管理任务。

您必须在组织级别注册服务，以便能显示这些服务。添加到角色的用户将继承该角色的服务属性。

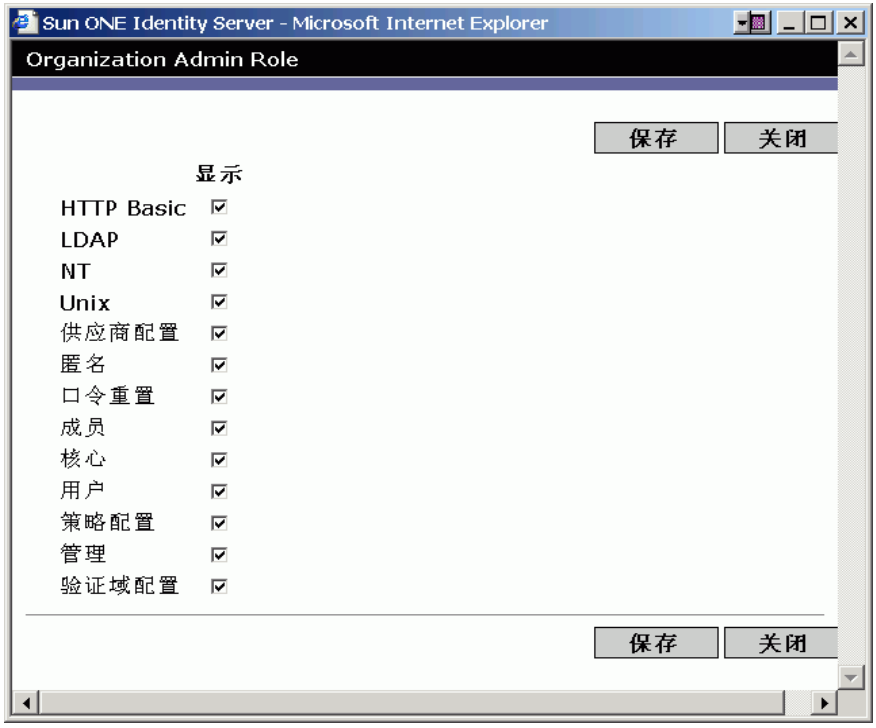
自定义服务访问

1. 单击要修改的角色的属性箭头。
2. 从 “查看”菜单中选择 “常规”。
3. 在 “角色属性”页面中，单击 “服务”列表中的 “编辑”。

   将显示 “服务访问”页面，如图 2-3 所示。
4. 单击 “显示”列中的服务名称，以选择允许角色访问的服务。缺省情况下，角色可以访问所有服务。
5. 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。

图 2-3 “服务访问”页面



自定义属性访问

1. 在“角色属性”页面中，单击“服务属性”列表中的“编辑”。将显示“属性访问”页面，如图 2-4 所示。
2. 使用“跳转”菜单以显示特定服务的属性。
3. 通过选中“读/写”或“只读”复选框，为属性指定访问级别。
4. 单击“保存”。

注 如果对于某项给定的属性，“读/写”和“只读”选项均未选中，则将拒绝对该属性的读和写访问。

图 2-4 “属性访问”页面

有关特定服务属性的详细信息，请参见本手册的第 3 部分 **“属性参考指南”**。

删除角色

1. 找到包含要删除的角色的组织。

   从“身份管理”模块的“查看”菜单中选择“组织”，然后从浏览框中选择组织。“位置”路径可以显示缺省的顶层组织和选定的组织。

2. 从“查看”菜单中选择“角色”。
3. 选中角色名称旁边的复选框。
4. 单击“删除”。

策略

策略定义用于保护组织的 Web 资源的规则。尽管策略的创建、修改和删除是通过“身份管理”模块来实现的，但是具体过程在第 76 页中的 “策略管理”中进行了说明。

容器

当由于对象类和属性的不同而无法使用组织项时，会使用容器项。有一点很重要，Identity Server 容器项和 Identity Server 组织项不必等同于 LDAP 对象类 `organizationalUnit` 和 `organization`。它们是抽象的身份项。理想情况下，将使用组织项而不使用容器项。

注 容器的显示是可选的。要查看容器，必须在 Identity Server 管理服务的 “菜单” 中选择 “显示容器”。有关详细信息，请参见第 152 页中的 “在菜单中显示容器”。

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”。

   数据框中将显示 “容器” 模板。

3. 输入要创建的容器的名称。

4. 单击 “创建”。

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。

人员容器

人员容器是缺省的 LDAP 组织单位。在组织中创建用户时，所有的用户都会被指定到该容器。人员容器位于组织级别和人员容器级别 （作为子人员容器）。它们只能包含其它人员容器和用户。如果需要，可以将其它人员容器添加到组织中。

注 人员容器的显示是可选的。要查看人员容器，必须在 Identity Server 管理服务中选择 “显示人员容器”。有关详细信息，请参见第 152 页中的 “显示人员容器”。

创建人员容器

1. 找到要在其中创建新人员容器的组织或人员容器。

   从 “查看”菜单中选择 “人员容器”。

2. 单击 “新建”。

   数据框中将显示 “人员容器”模板。

3. 输入要创建的人员容器的名称。
4. 单击 “创建”。

删除人员容器

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

注 删除人员容器会同时删除容器中存在的所有对象，包括所有用户和子人员容器。

组容器

组容器用来管理组。它只能包含组和其它组容器。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，可以添加其它组容器。

注 组容器的显示是可选的。要查看组容器，必须在 Identity Server 管理服务中选择 “显示组容器”。有关详细信息，请参见第 153 页中的 “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缺省组。
3. 单击“新建”。
4. 在“名称”字段中输入值，然后单击“创建”。

   浏览框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”。

   浏览框中将显示缺省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“删除选定”。

第 3 章

服务配置

本章介绍 Sun™ ONE Identity Server 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（缺省值和自定义值）的方法，以及配置 Identity Server 控制台显示设置的方法。本章包含以下内容：

服务的定义

服务是一组在通用名称下定义的属性。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。该文件位于以下目录：

IdentityServer_base`/SUNWam/dtd/`

有关定义 Identity Server 服务的详细信息，请参见 *Sun ONE Identity Server Customization and API Guide*。

Identity Server 服务

Identity Server 附带的缺省服务由位于以下目录中的 XML 文件来定义：

IdentityServer_base/SUNWamconfig/xml

或

/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，用于为该组织定义缺省值。

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

共有十个验证模块，其中一个是基本模块。这就允许管理员选择每个已定义的组织检验其用户授权的方法。

匿名

该模块允许在不指定用户名和密码的情况下登录。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

该模块允许通过个人数字证书 (PDC) 登录。

注 Application Server 6.1 版部署不支持证书验证服务。

核心

该模块是 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。它允许管理员定义缺省值，匿名服务、基于证书的服务、HTTP Basic 服务、 LDAP 服务、成员资格服务、 NT 服务、 RADIUS 服务、SafeWord 服务、 SecurID 服务和 Unix 服务中未专门进行设置的值将采用这些缺省值。

HTTP Basic

该模块使用基本验证，该验证是 HTTP 协议的内置验证支持。

LDAP

该模块允许使用 LDAP 绑定进行验证，LDAP 绑定是一种将密码与特定 LDAP 条目关联起来的操作。

成员资格 （自注册）

该模块允许新用户进行自注册，以使用登录和密码进行验证。

NT

该模块允许使用 Windows NT™/2000™ 服务器来验证用户。为了实现 NT 验证模块，必须下载并安装 Samba Client (smbclient) 2.2.2。

RADIUS

该模块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 ONE Application Server 一起正常工作，您必须配置 Application Server 的 `service.policy` 文件。有关此操作的说明，请参见第 87 页中的 “验证选项”。

SafeWord

该模块允许使用 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 ONE Application Server 一起正常工作，您必须配置 Application Server 的 `service.policy` 文件。有关此操作的说明，请参见第 87 页中的 “验证选项”。

SecurID

该模块允许使用 RSA ACE/Server® 验证软件和 SecurID® 认证器来验证用户。Solaris x86 不支持该服务。

Unix

该模块允许使用 Unix® 服务器来验证使用 UNIX 标识和密码的用户。

注 Windows 2000 平台不支持 Unix 验证服务。

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。

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。

全球化设置服务

全球化设置包含可以针对不同字符集配置 Identity Server 的属性。

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它 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。

密码重置服务

密码重置服务使用户能够接收遗忘的密码，或重置其用于访问受 Identity Server 保护的给定服务或应用程序的密码。密码重置服务属性由顶层管理员定义，它可以控制用户验证凭证 （以 “秘密问题” 形式）、控制新的或现有的密码通知机制，和设置不正确的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它选项中。

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

安全断言标记语言 (SAML) 服务定义了一个在各个安全授权机构之间交换安全断言的框架，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，例如最大会话时间和最大空闲时间。

用户服务

缺省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、员工编号和密码都是用户属性。可以通过修改 `amUser.xml` 文件来添加或删除用户服务中的用户属性。有关详细信息，请参见 *Sun ONE Identity Server Customization and API 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。并且，对象类与组织属性不相关。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

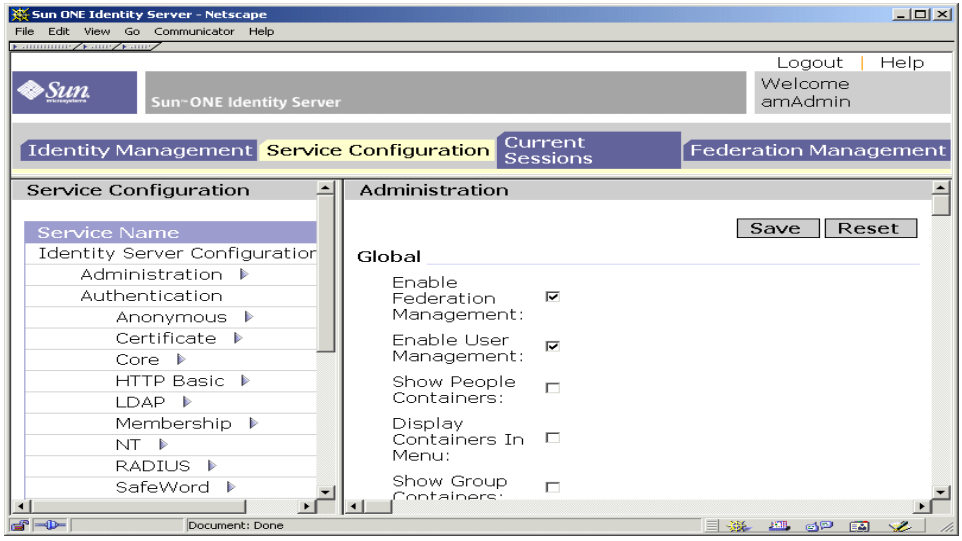
策略属性指定了与服务相关的访问控制操作 （或特权）。在将规则添加到策略时，这些属性将成为规则的一部分。

“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 缺省服务包中未包含的特定于组织的服务，然后将其添加到 “其它配置”标题下的界面中。您可以在第 3 部分 “属性参考指南”中找到有关如何进行此操作的说明，这部分内容介绍了缺省的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）的缺省配置的视图。当组织注册并激活了某项服务后，指定给该服务的初始缺省数据将显示在该服务的 “服务配置”页面中。图 3-1 显示了图形用户界面。

图 3-1 “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。要为服务设置全局缺省值，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 4 章

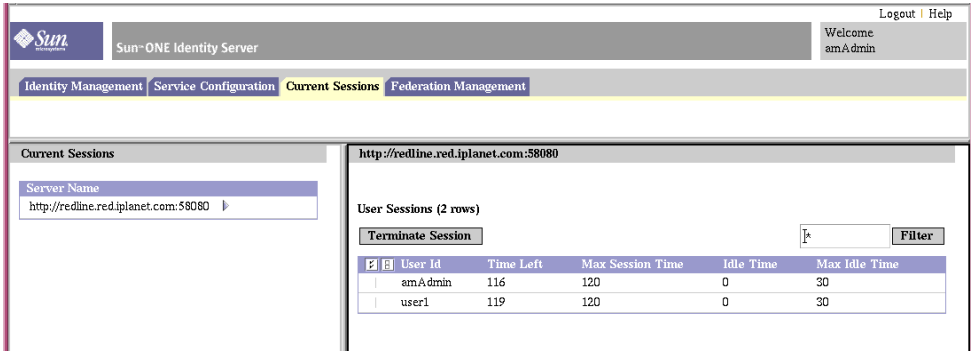
当前会话

本章介绍 Sun™ ONE Identity Server 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。

“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 4-1 “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，请参见第 261 页中的“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 5 章

联合管理

本章介绍 Sun™ ONE Identity Server 的联合管理界面功能。“联合管理”界面提供了查看、管理和配置有关验证域和提供商的元数据的方法。

不再支持 LIberty Alliance Project 规范 1.0 中介绍的功能。因为实际上没有 1.0 部署，所以不会造成严重影响。

本章包含以下内容：

注 本章中所述的属性字段的示例数据均可以在以下缺省位置找到：

IdentityServer_base/SUNWam/samples/liberty

验证域和提供商概述

“联合管理”模块提供了用于创建、修改和删除验证域、远程提供商和代管提供商的界面。以下步骤示范了一个基本的联合管理模型：

1. 创建一个验证域。
2. 创建一个或多个属于已创建的验证域的代管提供商。
3. 创建一个或多个属于已创建的验证域的远程提供商。还必须将远程提供商的元数据包含在内。
4. 在提供商之间建立可信赖的关系。代管提供商可以选择信任属于同一验证域的代管提供商或远程提供商的子集。

以下各节分别说明了如何创建和配置验证域、远程提供商和代管提供商。

验证域

本节说明如何创建、修改和删除验证域。

创建验证域

1. 从 “联合管理”模块的 “查看”菜单中选择 “验证域”。
2. 单击浏览框中的 “新建”。

   数据框中将显示 “创建验证域”。
3. 在 “创建验证域”窗口中输入验证域的名称。
4. 输入用于说明验证域的值。
5. 输入记录器服务 URL 的值。

   记录器服务 URL 用于指定在 “通用域”写入 Cookie 的记录器服务的位置。例如，如果 example.com 为通用域，则 URL 可能为：

   ```
   http://example.com:8080/liberty/WriterServlet
   ```
6. 输入读取程序服务 URL 的值。

   读取程序服务 URL 用于指定从 “通用域”读取 Cookie 的读取程序服务的位置。
7. 选择 “有效”或 “无效”状态。

   缺省值为 “有效”。在验证域生效期间，通过选择属性图标可以随时更改该状态。选择 “无效”将禁用验证域中与当前安装的 Identity Server 有关的 “特权”通信。
8. 单击 “创建”。

   浏览框中将显示新创建的验证域。

修改验证域

1. 单击您要修改的验证域旁边的属性箭头。

   数据框中将显示验证域的属性。

2. 修改验证域的属性。

3. 单击 “保存”。

删除验证域

删除验证域时不会删除属于该验证域的提供商。如果提供商属于已删除的验证域，则在这些提供商被明确删除以前，他们仍是验证域的一部分。您无法在已删除的验证域中添加其他提供商。

1. 从 “联合管理”模块的 “查看”菜单中选择 “验证域”。

   浏览框中将显示所有创建的验证域。

2. 选中您要删除的验证域名称旁边的复选框。

3. 单击 “删除选定”。

注 执行删除时不会显示警告消息。

提供商

本节说明如何创建、修改和删除远程提供商及代管提供商。

创建远程提供商

远程提供商是接收负责人 （指与系统进行交互的组织或个人）发出的元数据的实体。要创建远程提供商，请执行以下步骤：

1. 从 “联合管理”模块的 “查看”菜单中选择 “远程提供商”。

   缺省情况下，创建的提供商为服务提供商。您也可以通过选择步骤 15 中所述的选项将远程提供商创建为身份提供商。

2. 单击 “新建”。屏幕上将显示 “创建远程提供商”窗口。

3. 输入“提供商 ID”的值。

   “提供商 ID”应指定提供商的 URL 标识符。“提供商 ID”的值在所有远程和代管提供商范围内必须是唯一的。

4. 输入远程提供商的说明。

5. 输入“安全密钥”。

   “安全密钥”定义了安全证书的别名。证书以别名保存在 JKS 密钥库中。这个别名（即安全密钥）用于获取所需的证书。

6. 输入“SOAP 终点 URL”。

   该字段指定 SOAP 请求接收方的位置。它用于通过 SOAP 在反向信道上通信（非浏览器通信）。

7. 输入“单一注销服务 URL”。

   服务提供商或身份提供商使用“单一注销服务 URL”来发送和接收注销请求。

8. 输入“单一注销返回 URL”。

   该字段指定注销请求在被处理后重定向的 URL。

9. 输入“联合终止服务 URL”。

   该字段指定接收联合终止请求的 URL。

10. 输入“联合终止返回 URL”的值。

    该字段指定联合终止请求在被处理后重定向的 URL。

11. 定义“单一登录服务 URL”。

    该字段定义服务提供商在联合和 SSO 期间将请求发送到的身份提供商 URL。只有在启用“作为身份提供商”选项时才有必要定义该字段。

12. 输入名称注册服务 URL。

    该字段使用的名称注册协议是服务提供商与身份提供商通信时注册其名称标识符所用的协议。注册只在建立联合会话后进行。该字段用于定义服务提供商向身份提供商注册名称标识符时使用的服务 URL。

13. 输入名称注册返回 URL。

    该字段使用的名称注册协议是服务提供商与身份提供商通信时注册其名称标识符所用的协议。注册只在建立联合会话后进行。名称注册返回 URL 是身份提供商向其发送注册状态的 URL。

14. 输入 “断言用户 URL”。

    该字段定义身份提供商将 SAML 断言发送到的服务提供商终点。

15. 确定是否将远程提供商定义为身份提供商。缺省情况下，所有提供商都是服务提供商。如果选择 “作为身份提供商”选项，远程提供商将被另外定义为身份提供商。

16. 单击 “创建”。

    浏览框中将显示新创建的提供商。

修改远程提供商

一旦创建远程主机，您便可随时对其进行修改。为此，请执行以下步骤：

1. 从 “查看”菜单的浏览框中选择 “远程提供商”。

2. 选择您要修改的提供商配置文件，然后单击 “编辑”箭头。

    缺省情况下，浏览框中显示 “常规”视图。“常规”视图中显示的大部分字段包含创建远程提供商期间输入的数据。可以修改以下其它字段：

    提供商 Succinct ID。该字段是区别服务提供商与身份提供商的唯一标志。

    Succinct ID 应为 SHA1 编码字符串。为了保证唯一性，提供商 ID 字符串应当用作编码的值。要生成 SHA1 编码，请使用 OpenSSL 命令行工具语法：

    ```
    $ echo providerID | openssl sha1
    ```

    如果修改任何字段，请单击 “保存”保存修改。

    状态。“有效”状态使远程提供商可以参与联合和 SSO。“无效”状态则使远程提供商不可用，且不会对任何请求作出响应。

3. 要修改 “服务提供商”字段，请从 “查看”菜单中选择 “服务提供商”。

    “断言用户 URL”字段包含您在创建远程提供商期间输入的数据。但是，您还可以修改其它字段：

    联合后的名称注册。如果启用该选项，服务提供商则可以在联合之后参与名称注册。名称注册是一个配置文件，服务提供商依据该文件来指定负责人的名称标识符，身份提供商将使用该名称标识与服务提供商通信。

    作为已签署验证请求。如果启用该选项，则指定远程提供商发送已签署的验证和联合请求。身份提供商将不会处理服务提供商发出的未签署请求。

    断言用户 URL。该字段定义身份提供商将 SAML 断言发送到的提供商终点。

联合终止配置文件。您可以选择“SOAP”或“HTTP/ 重定向”。该字段指定 SOAP 或 HTTP/ 重定向配置文件是否用于通知联合终止信息。在提供商生效期间可以随时更改该字段。

单一注销配置文件。您可以选择“SOAP”或“HTTP 重定向”。该字段指定 SOAP 或重定向 HTTP 是否用于通知注销事件。在提供商生效期间可以随时更改该字段。

名称注册配置文件。您可以选择“SOAP”或“HTTP/ 重定向”。该字段指定 SOAP 或 HTTP/ 重定向配置文件是否用于名称注册。在提供商生效期间可以随时更改该字段。

4. 单击“保存”。

5. 如果远程提供商在创建期间被定义为身份提供商，则您可以通过选择“查看”菜单中的“身份提供商”来修改以下字段：

   作为身份提供商。该字段指定远程提供商是否将被定义为身份提供商。缺省情况下，所有提供商都是服务提供商。如果选择“作为身份提供商”选项，远程提供商将被另外定义为身份提供商。

   SSO 过程中的名称注册。如果启用该选项，则在 SSO 过程中，身份提供商可以参与名称注册。名称注册是一个配置文件，服务提供商依据该文件来指定负责人的名称标识符，身份提供商将使用该名称标识与服务提供商通信。

   单一登录服务 URL。该字段定义服务提供商在联合和 SSO 期间将请求发送到的身份提供商 URL。只有在启用“作为身份提供商”选项时才有必要定义该字段。

6. 选择“查看”菜单中的“验证域”，编辑远程提供商所属的验证域。

   使用方向箭头将选定的验证域移到“可用”列表中。单击“保存”。这样就将提供商指定给该验证域。一个提供商可以属于一个或多个验证域，但是没有指定验证域的提供商不能参与“特权”通信。单击“保存”。

创建代管提供商

代管提供商是指一个实体，它可以创建、维护和管理负责人的身份信息，并向验证域中的其他服务提供商提供负责人验证。要创建代管提供商，请执行以下步骤：

1. 从“联合管理”模块的“查看”菜单中选择“代管提供商”。

   缺省情况下，创建的提供商为服务提供商。您也可以通过选择步骤 6 中所述的选项将远程提供商创建为身份提供商。

2. 单击“新建”。屏幕上将显示“创建代管提供商”窗口。

3. 输入 “提供商 ID”的值。

   “提供商 ID”指定提供商的 URL 标识符。“提供商 ID”的值在所有远程和代管提供商范围内必须是唯一的。

4. 输入代管提供商的说明。

5. 输入提供商的别名。

   对于每个代管提供商，该字段中提供的别名将被添加到一个名为 metaAlias 的字符串中。然后该字符串被添加到代管提供商的自动填充 URL 中。这些 URL 称为 “元数据 URL”。在以下示例中， `sunAlias` 是提供商的别名：

   联合终止服务 URL

   ```
   http://www.example.com:58080/amserver/ProcessTermination/metaAlias/sunAlias
   ```

   SOAP 终点 URL

   ```
   http://www.example.com:58080/amserver/SOAPReceiver/metaAlias/sunAlias
   ```

6. 确定是否将远程提供商定义为身份提供商。缺省情况下，所有提供商都是服务提供商。如果选择 “作为身份提供商”选项，远程提供商将被另外定义为身份提供商。

7. 输入 “安全密钥”。

   “安全密钥”定义了安全证书的别名。证书以别名保存在 JKS 密钥库中。这个别名 （即安全密钥）用于获取所需的证书。

8. 输入 “提供商 URL”。

   该字段指定发送元数据的 URL。

9. 确定是否将代管提供商定义为身份提供商。缺省情况下，所有提供商都是服务提供商。如果选择 “作为身份提供商”选项，代管提供商将被另外定义为身份提供商。

10. 单击 “创建”。

    浏览框中将显示新创建的提供商。

修改代管提供商

1. 选择您要修改的提供商配置文件，然后单击 “编辑”箭头。

   缺省情况下，浏览框中显示 “常规”视图。“常规”视图中显示的大部分字段包含创建代管提供商期间输入的数据。可以修改以下其它字段：

   SOAP 终点 URL。该字段指定 SOAP 请求接收方的位置。它用于通过 SOAP 在反向信道上通信 （非浏览器通信）。

   单一注销服务 URL。服务提供商或身份提供商使用 “单一注销服务 URL”来发送和接收注销请求。

   单一注销返回 URL。该字段指定注销请求在被处理后重定向的 URL。

   联合终止服务 URL。该字段指定接收联合终止请求的 URL。

   联合终止返回 URL。该字段指定联合终止请求在被处理后重定向的 URL。

   名称注册服务 URL。该字段使用的名称注册协议是服务提供商与身份提供商通信时注册其名称标识符所用的协议。注册只在建立联合会话后进行。该字段用于定义服务提供商向身份提供商注册名称标识符时使用的服务 URL。

   名称注册返回 URL。该字段使用的名称注册协议是服务提供商与身份提供商通信时注册其名称标识符所用的协议。注册只在建立联合会话后进行。名称注册返回 URL 是身份提供商向其发送注册状态的 URL。

   如果您修改了任何一个字段，请单击 “保存”。

2. 要修改 “服务提供商”字段，请从 “查看”菜单中选择 “服务提供商”。

   “断言用户 URL”字段包含您在创建远程提供商期间输入的数据。您可以修改以下其它字段：

   联合后的名称注册。如果启用该选项，服务提供商则可以在联合之后参与名称注册。名称注册是一个配置文件，服务提供商依据该文件来指定负责人的名称标识符，身份提供商将使用该名称标识与服务提供商通信。

   作为已签署验证请求。如果启用该选项，则指定代管提供商发送已签署的验证和联合请求。身份提供商将不会处理服务提供商发出的未签署请求。

   联合终止配置文件。您可以选择 “SOAP”或 “HTTP/ 重定向”。该字段指定 SOAP 或 HTTP/ 重定向配置文件是否用于通知联合终止信息。在提供商生效期间可以随时更改该字段。

   单一注销配置文件。您可以选择 “SOAP”或 “HTTP 重定向”。该字段指定 SOAP 或重定向 HTTP 是否用于通知注销事件。在提供商生效期间可以随时更改该字段。

名称注册配置文件。您可以选择 “SOAP”或 “HTTP/ 重定向”。该字段指定 SOAP 或 HTTP/ 重定向配置文件是否用于名称注册。在提供商生效期间可以随时更改该字段。

验证环境。该字段允许您为要使用的验证环境指定验证级别。

如果您修改了任何一个字段，请单击 “保存”。

3. 如果代管提供商在创建期间被定义为身份提供商，则您可以通过选择 “查看”菜单中的 “身份提供商”来修改这些字段。这些字段中的数据是在创建提供商时输入的数据。您可以修改以下字段：

   作为身份提供商。该字段指定远程提供商是否将被定义为身份提供商。缺省情况下，所有提供商都是服务提供商。如果选择 “作为身份提供商”选项，远程提供商将被另外定义为身份提供商。

   SSO 过程中的名称注册。如果启用该选项，则在 SSO 过程中，身份提供商可以参与名称注册。名称注册是一个配置文件，服务提供商依据该文件来指定负责人的名称标识符，身份提供商将使用该名称标识与服务提供商通信。

   单一登录服务 URL。该字段定义服务提供商在联合和 SSO 期间将请求发送到的身份提供商 URL。只有在启用 “作为身份提供商”选项时才有必要定义该字段。

   支持。指定身份提供商是否支持验证环境。身份提供商应至少支持一种验证环境。

   环境参考。定义验证环境的名称。“特权”协议中定义了十种环境。

   关键字。发送给 /UI/Login （Identity Server 验证 servlet）的查询字符串中将包含 “关键字 - 值”对，用于识别将要使用的验证机制。关键字值可为：

   - 模块
   - 级别
   - 角色
   - 服务
   - 用户

   值。为验证机制定义 “关键字 - 值”对的值。

   优先级。指明定义 “特权”的验证环境的排列次序，由身份提供商确定。如果身份提供商不支持服务提供商在验证请求过程中要求的验证环境，则可以使用同级或更高优先级的其它任何验证环境。

   单击 “保存”保存更改。

4. 选择 “查看”菜单中的 “验证域”，编辑远程提供商所属的验证域。

   使用方向箭头将选定的验证域移到 “可用”列表中。单击 “保存”。这样就将提供商指定给该验证域。一个提供商可以属于一个或多个验证域，但是没有指定验证域的提供商不能参与 “特权”通信。

5. 从 “查看”菜单中选择 “可信赖提供商”。

   远程提供商将只接受这组提供商发出的请求，而忽略其他提供商发出的请求。要创建可信赖的提供商列表，请从 “可用”字段中选择提供商并使用 “添加”按钮将这些提供商添加到 “选定”字段。（另外，您也可使用 “删除”按钮删除提供商。）单击 “保存”。

6. 选择 “Identity Server 配置属性”。

   包括以下字段：

   验证类型。远程/本地 — 指定代管提供商在收到验证请求时是联系身份提供商（远程）还是否由代管提供商自己 （本地）来完成验证。

   单一登录/联合配置文件。指定代管提供商用于发送验证请求的配置文件。Identity Server 提供了以下协议：

   - 浏览器 Post — 指定基于 http POST 的正向信道协议。
   - 浏览器辅件 — 基于 SOAP 的反向信道 （非浏览器）协议。

   缺省验证环境。指定当身份提供商未在服务提供商请求中接收到验证环境时将要使用的验证环境。它还指定在未知用户试图访问受保护的资源时服务提供商所用的验证环境。缺省值包括：

   - Previous-Session
   - Time-Sync-Token
   - Smartcard
   - MobileUnregistered
   - Smartcard-PKI
   - MobileContract
   - Password
   - Password-ProtectedTransport
   - MobileDigitalID

- Software-PKI

强制验证身份提供商。指明身份提供商在收到验证请求时是否必须进行重新验证 （即使在活动的会话期间）。

请求身份提供商为被动。如果选择该字段，则要求身份提供商不与负责人相互通信，而必须与用户相互通信。

组织 DN。如果各个代管提供商选择在不同组织之间管理用户 （形成支持的模型），则该字段用于指定组织 DN 的存储位置。

特权版本 URI。指定 “特权”规格的版本。

名称标识符实现。允许服务提供商选择是否参与名称注册。名称注册是一个配置文件，服务提供商依据该文件来指定负责人的名称标识符，身份提供商将使用该名称标识与服务提供商通信。

提供商主页 URL。指定提供商的主页。

单一登录失败重定向 URL。指定发生故障的 SSO 的重定向 URL。

断言时间间隔。指定身份提供商所发布断言的有效时间间隔。在断言时间间隔到期之前，身份提供商始终会验证负责人。

清除时间间隔。指定清除存储在身份提供商处的断言的时间间隔。

辅件超时。指定断言辅件在身份提供商处的超时时间。

断言限制。指定身份提供商可以发布或存储的断言数量。

7. 单击 “保存”。

删除提供商

1. 从 “联合管理”的 “查看”菜单中选择 “提供商”。

   浏览框中将显示所有创建的提供商。

2. 选中您要删除的提供商的复选框。

3. 单击 “删除选定”。

注 执行删除时不会显示警告消息。

第 6 章

策略管理

本章介绍 Sun™ ONE Identity Server 的策略服务管理功能。策略管理提供了查看、管理和配置所有 Identity Server 策略的方法。

本章包含以下内容：

策略类型

使用 Identity Server 可以配置两种类型的策略：**标准**策略和**参照策略**。标准策略由**规则**、**主题**和**条件**组成。参照策略由**规则**和**候选组织**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。

规则由一种**资源**、一组或多组**操作**以及一个**值**组成。资源用于定义被保护的对象，操作是可以在资源上执行的操作的名称，值则用于定义权限。

注 允许定义不带资源的操作。

不能将策略指定到身份，而可以将**主题**指定到策略。主题就是指定且应用了策略的身份对象。

条件定义的是策略适用的情况。例如，如果策略中有一个 7 AM 到 10 AM 的时间条件，则表示该策略只能在 7 AM 到 10 AM 之间使用。

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。这些术语在 *Sun ONE Identity Server Customization and API Guide* 中做了进一步介绍。

参照策略

通常来说，管理员可能会需要将一个组织的策略定义和决策授权给另一个组织。（另外，还可以将资源的策略决策授权给其它策略产品）。**参照**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。规则定义策略定义和评估相关的资源。候选组织定义当前与策略定义和评估相关的组织。

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。

Identity Server 捆绑了两种候选组织：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，请参见第 85 页中的 “为对等组织和子组织创建策略”。

策略管理

您可以通过策略 API、 `amadmin` 命令行工具和 Identity Server 控制台创建、删除和修改策略。

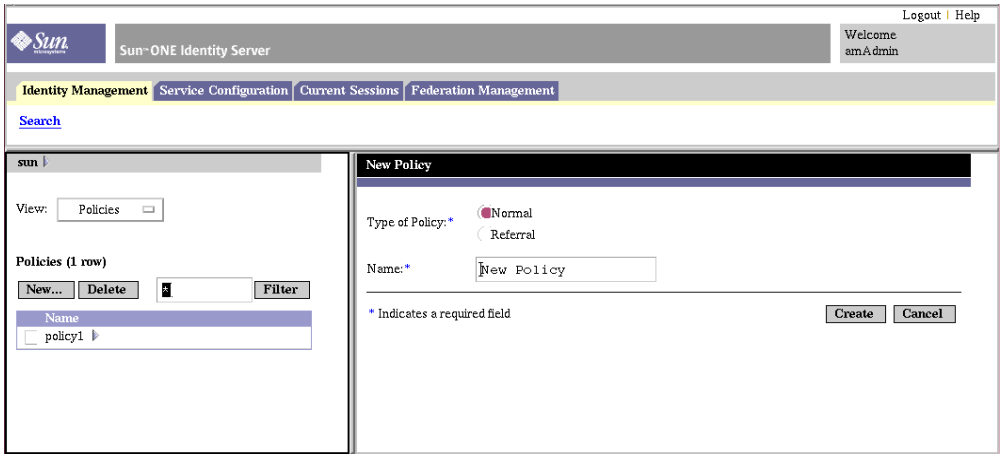
本章重点介绍通过控制台创建策略。有关 `amadmin` 的详细信息，请参见第 121 页中的 “amadmin 命令行工具”。有关策略 API 的详细信息，请参见 *Sun ONE Identity Server Customization and API Guide* 中的 “Policy Service” 一章。

策略是通过 “身份管理” 界面配置的。此界面提供了进行以下操作的方法：

- 顶层管理员查看、创建、删除和修改能够在所有组织范围内使用的特定服务的策略。
- 组织或子组织的管理员查看、创建、删除和修改组织专用的策略。

通常来说，策略在组织 （或子组织）级别创建并用于整个组织树。

图 6-1 策略视图



注册策略配置服务

注册策略配置服务与注册其它任何类型的服务一样，只不过是它在 “身份管理” 界面中完成。缺省情况下，系统会自动向顶级组织注册策略配置服务。您所创建的任何策略服务都必须向所有组织注册。无论何时注册策略配置服务，均必须在模板中输入 LDAP 绑定密码，以使所有策略在组织内生效。

1. 找到 “身份管理” 界面。

   在打开控制台时，缺省界面是 “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。缺省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 “注册”。

   数据框中将显示尚未向该组织注册的服务列表。

5. 在数据框的 “注册服务” 窗口中，选择 “策略配置”，然后单击 “注册”。

   “策略配置服务” 会添加到浏览框的服务列表中。

6. 单击属性箭头配置策略服务。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。

   要配置策略服务，请单击 “创建”。修改策略配置属性。有关这些属性的说明，请参见第 245 页中的 “策略配置服务属性”。单击 “保存”。

   现在已向选定组织注册了策略配置服务。

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。

创建策略

策略是通过 “身份管理”界面创建的。

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”。

   缺省情况下，“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。

   如果子组织没有相应的参照策略，则不能为该子组织创建任何策略。有关详细信息，请参见第 85 页中的 “为对等组织和子组织创建策略”。

   此时，您不必为标准或参照策略定义所有字段。您可以在创建策略之后再添加规则、主题、候选组织等字段。有关配置标准策略和参照策略的信息，请参见第 79 页中的 “修改策略”。

6. 键入策略的名称，然后单击 “创建”。

   在创建的策略名称下面将会显示新的策略规则窗口。

7. 缺省情况下，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”完成对策略的配置。

修改策略

一旦创建了标准或参照策略，您就可以修改规则、主题、条件和候选组织。

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。

   缺省情况下，屏幕上将显示 “常规”视图。

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缺省字段。

添加规则

“规则”用于定义策略的资源、操作和操作值。

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。

   缺省情况下，屏幕上将显示 “常规”视图。

3. 要定义策略的规则，请从 “查看”菜单中选择 “规则”，然后单击 “添加”。

   如果存在多个服务，这些服务会在数据框中列出。选择要为其创建策略的服务，然后单击 “下一步”。屏幕上将显示 “添加规则”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：

   服务。显示所创建策略的服务。缺省值为 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.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。例如：

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

对于 “URL 策略代理”服务，如果未输入端口号，则 http:// 的缺省端口号为 80， https:// 的缺省端口号为 443。

选择操作。对于 “URL 策略代理”服务，您可以选择以下两项缺省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缺省的拒绝规则。

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，请参见第 82 页中的 “添加条件”。

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 “创建”保存规则。

6. 重复步骤 1 至 5 以创建其它规则。
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。

   要从策略中删除规则，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。

添加主题

“主题” 用于定义策略所应用的主题。

1. 要定义策略的主题，请从 “查看” 菜单中选择 “主题”，然后单击 “添加”。
2. 选择以下任一缺省主题类型：
   - Identity Server 角色
   - LDAP 组
   - LDAP 角色
   - LDAP 用户
   - 组织

   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 （缺省），策略应用到的身份为主题成员。如果选择该字段，策略应用到的身份为非主题成员。

   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。无论是否选择了 “专用” 字段，满足策略中定义的所有条件时，策略就可以应用到身份。
5. 执行搜索以显示要添加到主题的身份。

   缺省 (*) 搜索模式将显示所有符合条件的条目。
6. 选择要添加到主题中的身份，然后单击 “添加” 将它们移到 “选定” 列表框中。（或选择 “全部添加” 添加所有身份。）
7. 单击 “创建”。

8. 主题的名称、类型和专用状态都显示在 “主题” 视图的表中。单击 “保存”。

   要从策略中删除主题，请选择该主题并单击 “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。

要将条件添加到标准策略，请执行以下步骤：

1. 定义策略的条件。从 “查看” 菜单中选择 “条件”。单击 “添加” 添加新的条件，或单击 “编辑” 链接编辑现有的条件。
2. 选择以下缺省条件之一：
   - 验证级别
   - 验证方案
   - IP 地址
   - 会话
   - 时间

   单击 “下一步”。

3. 在 “规则”字段中定义给定条件的值。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。

   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）。

   会话

   最大会话时间。指定应用策略的最大用户会话时间。

   终止会话。当选中该字段后，如果会话时间超过 “最大会话时间”字段中定义的最大许可时间，将终止用户会话。

4. 定义条件后，单击 “创建”。

5. 为该策略创建的所有条件均显示在 “条件”视图的表中。单击 “保存”。

   要从策略中删除条件，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。

修改参照策略

通过 “身份管理”界面，您可以将一个组织的策略定义和决策授权给另一个组织。（您还可以将资源的策略决策授权给其它策略产品。）**参照策略**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。如果策略服务包括不需要资源的操作，则不能为子组织创建参照策略。

添加规则

“规则”用于定义策略的资源。

1. 要定义策略的规则，请从 “查看”菜单中选择 “规则”。单击 “添加”添加新的规则，或单击 “编辑”链接编辑现有的规则。
2. 在 “规则”字段中定义资源。这些字段包括：

   服务。显示可用于所创建策略的策略服务

   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://` 的缺省端口号为 80， `https://` 的缺省端口号为 443。
3. 单击 “创建”保存规则。
4. 重复步骤 1 - 3 创建其它规则。
5. 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”。

   要从策略中删除规则，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

候选组织定义当前与策略评估相关的组织。缺省情况下，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。

1. 要定义策略的候选组织，请从 “查看”菜单中选择 “候选组织”。单击 “添加”添加新的候选组织，或单击 “编辑”链接编辑现有的候选组织。
2. 在 “规则”字段中定义资源。这些字段包括：

   候选组织。显示当前的候选组织。

   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。缺省情况下，该字段将显示所有组织名称。

   值。输入候选组织的组织名称。

3. 单击 “创建”，然后单击 “保存”。

   要从策略中删除候选组织，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。

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 （或其它对等组织）中创建参照策略。另外，还应该注册策略配置服务并在子组织中创建模板。参照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 （或其它对等组织）中创建了参照策略，就可以在子组织 （或对等组织）中创建标准策略。

如果操作名称不包含资源名称，则 Identity Server 策略框架不允许创建参照策略。换句话说，如果操作不包括任何资源名称，则只能在根组织下创建策略，而不能在子组织下创建。

在本示例中， `o=isp` 为父组织， `o=sun.com` 为子组织并管理 `http://www.example.com` 的资源和子资源。要为该子组织创建策略，请执行以下步骤：

1. 在 `o=isp` 中创建参照策略。有关参照策略的信息，请参见第 83 页中的 “修改参照策略”过程。

   此参照策略必须将 `http://www.sun.com` 定义为规则中的资源，并将候选组织中的 SubOrgReferral 的值设置为 `sun.com`。

2. 转到 “组织”视图并找到子组织 `sun.com`。

3. 确保在子组织级别 （即 `sun.com`）上注册策略配置服务。有关信息，请参见第 77 页中的 “注册策略配置服务”。

4. 现在， `isp` 已将资源关联到 `sun.com`，因此可为资源 `http://www.sun.com` 或所有以 `http://www.sun.com` 开头的资源创建标准策略。

   有关创建标准策略的信息，请参见第 79 页中的 “修改标准策略”过程。

   要为 `sun.com` 管理的其它资源定义策略，必须在 `o=isp` 中创建其它参照策略。

第 7 章

验证选项

Sun™ ONE Identity Server 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 控制台或任何其它受 Identity Server 保护的资源之前，用户必须通过验证进程。验证是通过用于验证用户身份的插件来实现的。（*Sun ONE Identity Server Customization and API Guide* 中更全面地介绍了此插件体系结构。）

Identity Server 控制台用于设置缺省值，这些缺省值用于注册验证服务、创建验证模板及启用服务。本章提供关于验证服务的概述和注册这些验证服务的说明。本章包含以下内容：

- URL 重定向

核心验证

缺省情况下，除了核心验证服务以外， Identity Server 还提供了十种不同的验证服务。核心验证服务为验证服务提供总体配置。在注册和启用匿名验证、基于证书的验证、 HTTP Basic 验证、 LDAP 验证、成员资格验证、 NT 验证、 RADIUS 验证、 SafeWord 验证、 SecurID 验证和 Unix 验证之前，必须先注册和启用核心验证。第 19 章 “核心验证属性”中包含核心属性的详细列表。

注册和启用核心服务

1. 找到要为其注册核心服务的组织的浏览框。
2. 从 “查看”菜单中选择 “服务”。
3. 单击浏览框中的 “添加”。

   数据框中将显示可用服务的列表。
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框中，向管理员表明已注册该服务。
5. 单击核心验证的属性箭头。

   数据框中将显示消息**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”。

   数据框中将显示核心属性。根据需要修改这些属性。您可以在第 19 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

缺省情况下，如果启用了此模块，用户可以以 *anonymous* 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（请参见第 171 页）。允许匿名访问意味着无需提供密码即可访问该服务器。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。

注册和启用匿名验证

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

1. 找到要为其注册匿名验证的组织的浏览框。
2. 从 “查看” 菜单中选择 “服务”。

   如果已经注册了核心服务，则该服务将显示在浏览框中。如果未注册该服务，则可以与匿名验证服务一同注册。
3. 单击浏览框中的 “添加”。

   数据框中将显示可用服务的列表。
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框中，向管理员表明已注册该服务。
5. 单击匿名验证的属性箭头。

   数据框中将显示消息**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”。

   数据框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 17 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 182 页中的 “组织验证模块”）以定义匿名验证。这可以确保用户登录时使用 `http(s)://hostname:port/DEPLOY_URI/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/DEPLOY_URI/Login?module=Anonymous&org=org_name&IDTolken1=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缺省模块，则无需在 URL 中指定模块名称。

注 匿名验证服务中的 “缺省匿名用户名” 属性值为 anonymous。这是用户登录时使用的名称。必须在组织中创建缺省的匿名用户。用户 ID 应当与在匿名验证属性中指定的用户名相同。

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注册到组织之前，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，请先查阅 《*Sun ONE Web Server 6.1* **管理员指南**》中的第 6 章 “使用证书和密钥” 中的这些初始 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，对于安全性，请查阅以下位置的 Sun ONE Application Sever Administrator's Guide to Security：

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

注 每个将使用基于证书的服务进行验证的用户均必须请求一个适用于用户浏览器的 PDC。使用的浏览器不同，具体的说明也不同。有关详细信息，请参见浏览器的文档。

注册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. 找到要为其注册基于证书的验证的组织的浏览框。
2. 从 “查看” 菜单中选择 “服务”。

   如果已经注册了核心服务，则该服务将显示在浏览框中。如果未注册该服务，则可以与基于证书的验证服务一同注册。
3. 单击浏览框中的 “添加”。

   数据框中将显示可用服务的列表。

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框中，向管理员表明已注册该服务。

5. 单击基于证书的验证的属性箭头。

   数据框中将显示消息**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”。

   数据框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 18 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”。

为基于证书的验证添加平台服务器列表

为了进行添加，您必须以组织管理员身份登录到 Identity Server。

1. 选择 “服务配置”模块。
2. 从可用服务的列表中选择 “平台”服务。
3. 在 “服务器列表”属性中添加服务器信息。有关其它服务器属性的详细信息，请参见第 33 章 “平台服务属性”。

使用基于证书的验证登录

为了使基于证书的验证成为缺省验证方法，必须修改核心验证服务属性 “组织验证模块”（请参见第 182 页）。这可以确保当用户使用 `https://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缺省模块，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，该验证是 HTTP 协议的内置验证支持。 Web server 发出对用户名和密码的客户机请求，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 将检索用户名和密码，然后在 LDAP 验证模块中内部验证该用户。为使 HTTP Basic 验证正常工作，还必须注册 LDAP 验证模块 （只注册 HTTP Basic 模块将无法正常工作）。有关详细信息，请参见第 93 页中的 “注册和启用 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密码的情况下重新进行验证。

注册和启用 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 中。

1. 找到要为其注册 HTTP Basic 验证的组织的浏览框。
2. 从 “查看” 菜单中选择 “服务”。

   如果已经注册了核心服务，则该服务将显示在浏览框中。如果未注册该服务，则可以与 HTTP Basic 验证服务一同注册。
3. 单击浏览框中的 “添加”。

   数据框中将显示可用服务的列表。
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框中，向管理员表明已注册该服务。
5. 单击 HTTP Basic 验证的属性箭头。

   数据框中将显示消息**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”。

   数据框中将显示 HTTP Basic 验证属性。根据需要修改这些属性。您可以在第 20 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 HTTP Basic 验证登录，必须修改核心验证服务属性 （第 182 页中的 “组织验证模块”）以定义 HTTP Basic 验证。这可以确保当用户使用 `http://hostname:port/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缺省模块，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。

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 和密码绑定到 LDAP Directory Server 上。这是所有基于组织的验证的缺省验证模块。如果用户提供的用户 ID 和密码在 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。缺省情况下，安装 Identity Server 时将启用 LDAP 验证。在禁用该服务的事件中提供了以下说明。

注册和启用 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. 找到要为其注册 LDAP 验证的组织的浏览框。
2. 从 “查看” 菜单中选择 “服务”。

   如果已经注册了核心服务，则该服务将显示在浏览框中。如果未注册该服务，则可以与 LDAP 验证服务一同注册。
3. 单击浏览框中的 “添加”。

   数据框中将显示可用服务的列表。
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框中，向管理员表明已注册该服务。
5. 单击 LDAP 验证的属性箭头。

   数据框中将显示消息**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”。

   数据框中将显示 LDAP 验证属性。根据需要修改这些属性。您可以在第 21 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 “root 用户绑定的密码”属性中输入密码。缺省情况下，安装过程中输入的 `amldapuser` 密码将用作绑定用户。

   要使用其它绑定用户，请在 “root 用户绑定的 DN”属性中更改用户的 DN，并在 “root 用户绑定的密码”属性中输入该用户的密码。

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 182 页中的 “组织验证模块”）以定义 LDAP 验证。这可以确保当用户使用 `http://`*`hostname:port/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缺省模块，则无需在 URL 中指定模块名称。

启用 LDAP 验证故障切换

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，请参见 LDAP 属性第 194 页中的 “主 LDAP 服务器和端口”和第 194 页中的 “辅助 LDAP 服务器和端口”。

多个 LDAP 配置

管理员可以在一个组织下定义多个 LDAP 配置，作为故障切换的形式或者在 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从控制台查看，但如果未找到搜索请求用户的验证的初始搜索，这些配置将与主配置一起发挥作用。有关多个 LDAP 配置的信息，请参见 *Sun ONE Identity Server Customization and API Guide* 中的 “多个 LDAP 配置”。

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。用户可以以注册用户的身份访问此新帐户。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。

注册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. 找到要为其注册成员资格验证的组织的浏览框。
2. 从 “查看” 菜单中选择 “服务”。

   如果已经注册了核心服务，则该服务将显示在浏览框中。如果未注册该服务，则可以与成员资格验证服务一同注册。
3. 单击浏览框中的 “添加”。

   数据框中将显示可用服务的列表。
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框中，向管理员表明已注册该服务。
5. 单击成员资格验证的属性箭头。

   数据框中将显示消息**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”。

   数据框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 22 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 “root 用户绑定的密码” 属性中输入密码。缺省情况下，安装过程中输入的 `amldapuser` 密码将用作绑定用户。

   要使用其它绑定用户，请在 “root 用户绑定的 DN” 属性中更改用户的 DN，并在 “root 用户绑定的密码” 属性中输入该用户的密码。
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 182 页中的 “组织验证模块”）以定义成员资格验证。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缺省模块，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. 必须先获得并安装用于在 Solaris 系统中与 Identity Server 通信的 Samba 客户机，才能注册和启用 NT 验证服务。有关详细信息，请参见第 205 页中的 “NT 验证属性”。

3. 注册和启用 NT 验证服务。

注册和启用 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. 找到要为其注册 NT 验证的组织的浏览框。
2. 从 “查看”菜单中选择 “服务”。

   如果已经注册了核心服务，则该服务将显示在浏览框中。如果未注册该服务，则可以与 NT 验证服务一同注册。

3. 单击浏览框中的 “添加”。

   数据框中将显示可用服务的列表。

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框中，向管理员表明已注册该服务。

5. 单击 NT 验证的属性箭头。

   数据框中将显示消息**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”。

   数据框中将显示 NT 验证属性。根据需要修改这些属性。您可以在第 23 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 182 页中的“组织验证模块”）以定义 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缺省模块，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。

注册和启用 RADIUS 验证

您必须以组织管理员身份登录到 Identity Server 中。

1. 找到要为其注册 RADIUS 验证的组织的浏览框。

2. 从 “查看” 菜单中选择 “服务”。

   如果已经注册了核心服务，则该服务将显示在浏览框中。如果未注册该服务，则可以与 RADIUS 验证服务一同注册。

3. 单击浏览框中的 “添加”。

   数据框中将显示可用服务的列表。

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框中，向管理员表明已注册该服务。

5. 单击 RADIUS 验证的属性箭头。

   数据框中将显示消息**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”。

   数据框中将显示 RADIUS 验证属性。根据需要修改这些属性。您可以在第 24 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 182 页中的 “组织验证模块”）以定义 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缺省模块，则无需在 URL 中指定模块名称。

使用 Sun ONE Application Server 配置 RADIUS

缺省情况下， 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 的连接权限。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

要授予套接字连接的权限，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）。 DNS 名称主机规范中可以包含通配符 “*”（只能出现一次）。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。任意其它操作存在时， `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

可以配置 Identity Server 以处理对 Secure Computing 的 SafeWord™ 或 SafeWord PremierAccess™ 验证服务器的 SafeWord 验证请求。 Identity Server 提供了 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。

注册和启用 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. 找到要为其注册 SafeWord 验证的组织的浏览框。
2. 从 “查看” 菜单中选择 “服务”。

   如果已经注册了核心服务，则该服务将显示在浏览框中。如果未注册该服务，则可以与 SafeWord 验证服务一同注册。
3. 单击浏览框中的 “添加”。

   数据框中将显示可用服务的列表。
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框中，向管理员表明已注册该服务。
5. 单击 SafeWord 验证的属性箭头。

   数据框中将显示消息**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”。

   数据框中将显示 SafeWord 验证属性。根据需要修改这些属性。您可以在第 24 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 182 页中的 “组织验证模块”）以定义 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缺省模块，则无需在 URL 中指定模块名称。

使用 Sun ONE Application Server 配置 SafeWord

缺省情况下， 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 的 `connect` 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

要授予套接字连接的权限，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）。 DNS 名称主机规范中可以包含通配符 “*”（只能出现一次）。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。任意其它操作存在时， `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。

SecurID 验证

可以配置 Identity Server 以处理对 RSA 的 ACE/Server 验证服务器的 SecureID 验证请求。Identity Server 提供了 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 145 页中的“amsecuridd 帮助器”。

注册和启用 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. 找到要为其注册 SecurID 验证的组织的浏览框。
2. 从“查看”菜单中选择“服务”。

如果已经注册了核心服务，则该服务将显示在浏览框中。如果未注册该服务，则可以与 SecurID 验证服务一同注册。

3. 单击浏览框中的 “添加”。

   数据框中将显示可用服务的列表。

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框中，向管理员表明已注册该服务。

5. 单击 SecurID 验证的属性箭头。

   数据框中将显示消息**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”。

   数据框中将显示 SecurID 验证属性。根据需要修改这些属性。您可以在第 25 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 182 页中的 “组织验证模块”）以定义 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缺省模块，则无需在 URL 中指定模块名称。

Unix 验证

可以将 Identity Server 配置为通过与安装了 Identity Server 的 Solaris 系统已知的 Unix 用户 ID 和密码相比较来处理验证请求。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。要在缺省端口上运行 amunixd 帮助器进程，请输入以下命令：

```
./amunixd
```

要在非缺省端口上运行 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。

无法在 Windows 平台上使用 Unix 验证服务。

注册和启用 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 26 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. 找到要为其注册 Unix 验证的组织的浏览框。
5. 从 “查看”菜单中选择 “服务”。

   如果已经注册了核心服务，则该服务将显示在浏览框中。如果未注册该服务，则可以与 Unix 验证服务一同注册。
6. 单击浏览框中的 “添加”。

   数据框中将显示可用服务的列表。

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框中，向管理员表明已注册该服务。

8. 单击 Unix 验证的属性箭头。

   数据框中将显示消息**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”。

   数据框中将显示 Unix 验证组织属性。根据需要修改验证级别属性。您可以在第 26 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 验证服务已经启用。

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 182 页中的 “组织验证模块”）以定义 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缺省模块，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. 在对象的验证配置属性旁边的 “编辑”链接上单击将显示 “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）。缺省情况下，这些模块包括：

- LDAP
- 证书
- 匿名
- SafeWord
- SecurID
- HTTPBasic
- 成员资格
- NT
- RADIUS
- Unix

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：

- REQUIRED — 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。
- REQUISITE — 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）。
- SUFFICIENT — 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。

- OPTIONAL — 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。

这些标志为定义了它们的验证模块建立了执行标准。执行是有等级的：REQUIRED 等级最高， OPTION 等级最低。

例如，如果管理员使用 REQUIRED 标志定义 LDAP 模块，则用户凭证必须通过 LADP 验证要求才能访问给定资源。

如果添加多个验证模块，并将每个模块的 “标志”都设置成 REQUIRED，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。还可以以 “关键字 = 值”对的形式为模块增加其它选项。多个选项之间用空格分隔。

图 7-1 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。

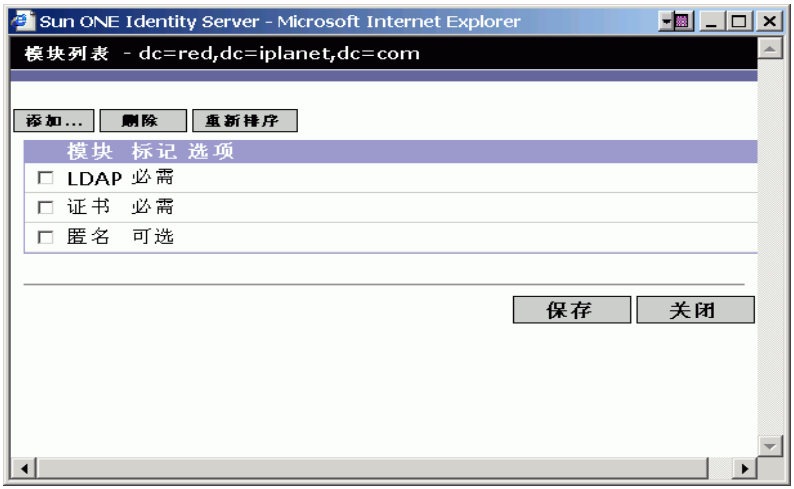
   要更改验证模块的顺序，请执行以下步骤：

   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”按钮将其放置到所需的位置。

图 7-2 用于用户的 “模块列表”窗口



4. 要从列表中删除任一验证模块，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

第一次将核心验证服务注册到组织时将设置用于组织的验证模块。

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。

   数据框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。缺省验证模块为 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。缺省验证模块为 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

在角色级别注册了验证配置服务之后，将设置用于角色的验证模块。

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。

   数据框中将显示角色的属性。

4. 从数据框中的 “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 27 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 验证模块保留为缺省设置，因为不需要配置成员资格。

用于服务的验证配置

注册了验证配置服务之后，将设置用于服务的验证模块。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”。

   将显示已注册服务的列表。如果未注册验证配置服务，请继续执行以下的步骤。如果已注册该服务，请转到步骤 4。

2. 单击浏览框中的 “添加”。

   数据框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框中，向管理员表明已注册该服务。

4. 单击验证配置的属性箭头。

   数据框中将显示 “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”。您可以在第 27 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”。

   浏览框中将显示用户列表。

2. 选择要修改的用户，然后单击属性箭头。

   数据框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. 从数据框中的 “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”。

按验证级别验证

每个验证模块均可以与其**验证级别**的整数值相关联。通过单击“服务配置”中验证模块的属性箭头并更改相应的模块验证级别属性的值，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。

按模块验证

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。如果此属性中未包含该验证模块名称，则当用户试图进行验证时将显示“验证模块被拒绝”页面。有关详细信息，请参见第 182 页中的“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 - REQUIRED。有关为身份对象注册验证配置服务的信息，请参见第 105 页中的“验证配置”。

第 8 章

密码重置服务

Sun™ ONE Identity Server 提供密码重置服务，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密码。密码重置服务属性由顶层管理员定义，它可以控制用户验证凭证 （以**秘密问题**形式）、控制新的或现有的密码通知机制，和设置不正确的用户验证的可能的锁定间隔。

本章包含以下内容：

注册密码重置服务

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

要为其它组织中的用户注册密码重置服务，请执行以下操作：

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. 选中密码重置的复选框并单击 “注册”。

   密码重置服务将显示在浏览框中，向管理员表明已注册该服务。

配置密码重置服务

注册密码重置服务后，必须由具有管理员特权的用户来配置该服务。要配置服务，请执行以下操作：

1. 选择要为其注册密码重置服务的组织。
2. 单击密码重置属性的箭头。

   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. 数据框中将显示密码重置属性，使您可以定义密码重置服务的要求。确保启用密码重置服务 （此为缺省情况）。至少必须定义以下属性：

   - 用户验证
   - 秘密问题
   - 绑定 DN
   - 绑定密码

   绑定 DN 属性必须包含具有重置密码特权的用户 （例如，帮助台管理员）。

   其它属性是可选的。您可以在第 235 页中的 “密码重置服务属性”中，或通过单击控制台右上角的 “帮助”链接找到有关密码重置属性的说明。

注 Identity Server 会自动为随机密码生成安装密码重置 Web 应用程序。但是，您可以写自己的密码生成和密码通知插件类。有关这些插件类的样例，请参见以下位置中的 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”。

密码重置锁定

密码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。锁定功能通过密码重置服务属性配置。有关这些属性的说明，请参见第 235 页中的 “密码重置服务属性”。密码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 “密码重置失败锁定持续时间 （分钟）” 属性中的值大于零并启用了 “密码重置失败锁定模式” 属性时才有效。该锁定功能可以防止用户通过密码重置 Web 应用程序重置其密码。锁定将持续 “密码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 “密码重置失败锁定计数” 属性中的值设置为 0 并启用了 “密码重置失败锁定模式” 属性，则当用户不能正确回答秘密问题时，用户的帐户状态将更改为无效。

最终用户密码重置

以下各节说明了用户使用密码重置服务的经过。

自定义密码重置

启用密码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，提供用户名和密码并成功通过验证。
2. 在 “用户配置文件” 页面中，用户选择密码重置选项。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？
    - 您最喜欢哪一家餐馆？

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 （最大数目在密码重置服务中定义）。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密码 （请参见下节）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 8-1 已启用私人问题的 “可用问题答案”屏幕

5. 用户单击 “保存”。

重置遗忘密码

在用户忘记其密码的情况下， Identity Server 将使用密码重置 Web 应用程序随机生成新密码并将其通知用户。一般的遗忘密码解决方案如下：

1. 用户从管理员为其提供的 URL 登录到密码重置 Web 应用程序。例如：

   `http://`*`hostname:port`*`/ampassword` （对于缺省组织）

   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密码重置服务，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. 系统将显示在密码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，将不会生成密码。

图 8-2 “用户的密码问题”屏幕

用户正确回答问题后，将生成新密码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，才能接收新密码和尝试通知。

密码策略

安全密码策略通过强制实施以下措施将与易猜测的密码相关的风险降到最低程度：

- 用户必须定期更改其密码。
- 用户必须提供不常见的密码。
- 输入一定次数的错误密码之后，可以锁定帐户。

Directory Server 提供了几种在树中的任一节点设置密码策略的方法，并且有几种方法设置策略。有关详细信息，请参见以下 Directory Server 文档：

http://docs.sun.com/source/816-6700-10/aci.html#14773

http://docs.sun.com/source/816-6698-10/useracct.html#14386

第 2 部分

命令行参考指南

本部分是 《Sun™ ONE Identity Server 管理指南》的第二部分 “命令行参考指南”。本部分包含以下各章：

- amadmin 命令行工具
- amserver 命令行工具
- ampassword 命令行工具
- am2bak 命令行工具
- bak2am 命令行工具
- VerifyArchive 命令行工具
- amsecuridd 帮助器

本部分中所述的所有命令行工具均可在以下缺省位置找到：

```
IdentityServer_base/SUNWam/bin
```

第 9 章

amadmin 命令行工具

本章介绍有关 amadmin 命令行工具的信息，包含以下内容：

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，请参见 *Sun One Identity Server Programmer'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 的密码。

--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，将使用缺省的语言环境 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 (*)，必须用元字符 (\) 使其脱离开命令解释器。

--debug (-d)

--debug 选项用于将消息写入在 *IdentityServer_base*/var/opt/SUNWam/debug 目录下创建的 amadmin 文件。这些消息在技术上已详化，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-st
able-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。它不将详细信息保存到文件中。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。有关可以传递给此选项的 XML 文件的类型的详细信息，请参见 *Sun ONE Identity Server Programmer'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。第 124 页中的代码示例 9-1 中显示了此部分。

代码示例 9-1 `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、产品版本和法律通告。

使用 amadmin 创建策略

可以通过 `amadmin` 管理策略，但是不能直接使用 amadmin 修改策略。要修改策略，必须先删除该策略，然后使用 amadmin 添加已修改的策略。

要使用 `amadmin` 添加策略，必须按照 `policy.dtd` 开发策略 XML 文件。（*Sun ONE Identity Server Customization and API Guide* 中介绍了 `policy.dtd`）开发了策略的 XML 文件之后，可以使用以下命令装入该文件：

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，请确保在创建验证模式条件时使用组织注册验证模块；确保在创建组织、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候选时，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。

第 10 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 { create | delete [instance_name] | startall | start | stop |
stopall | version }
```

适用于 Solaris 的 amserver 命令

create

create 命令用于创建新的 Identity Server 实例。应当以 root 用户身份运行 amserver 脚本。要创建实例，请运行 amserver 脚本 ./amserver create。第 129 页中的 “使用 amserver 进行多服务器安装程序管理 （仅用于 Web Server 实例）” 介绍了创建多个服务器实例的详细步骤。该命令只适用于 Web Server 实例。

startall

`startall` 命令用于启动所有的 Identity Server 实例。要启动单个实例，请运行以下命令：

```
IdentityServer_base/SUNWam/bin/amserver.instance_name start
```

stopall

`stopall` 命令用于停止所有的 Identity Server 实例。要停止单个 Identity Server 实例，请运行以下命令：

```
/opt/SUNWam/bin/amserver.instance_name stop
```

delete

`delete` 命令用于删除由 `create` 选项创建的实例。

适用于 Windows 2000 的 amserver 命令

Windows 2000 平台上的 amserver 仅支持以下命令：

start

`start` 命令用于启动 Identity Server。

stop

`stop` 命令用于停止 Identity Server。

注 `stop` 和 `start` 在新的与容器无关的部署中可能会运行不正常。如果遇到这种情况，请在容器中使用 `stop` 和 `start`。

restart

`restart` 命令用于重新启动 Identity Server。

`amserver` 不能停止或启动 Directory Server。可能需要手动重新启动它。 amserver 只能重新启动 Web Server 实例。对于其它 Web 容器，该命令仅重新启动验证帮助器。

使用 amserver 进行多服务器安装程序管理（仅用于 Web Server 实例）

可以使用 amserver 命令行实用程序安装和管理 Identity Server 的多个实例。在安装 Identity Server 的多个实例之前，您必须先以 root 用户身份登录。在 IdentityServer_base/SUNWam/bin 中可以找到以下步骤中涉及到的脚本。

要安装多个实例，请执行以下步骤：

1. 通过输入 ./amserver create 使用 amServer 创建一个新的服务器实例。

   例如，如果要创建侦听端口：81 的名为 instance1 的实例，脚本的输出可能会如下所示：

```
###################################################################
#####
请输入服务器实例的名称：instance1
请输入端口号：81
是否要创建更多的服务器实例？ y/[n]
正在安装 ... 请稍候 ....
###################################################################
##
```

   a. 随后将为每个 Web Server 实例创建一个目录。示例：

      IdentityServer_base/SUNWam/servers/https-*instance_name*

   b. Identity Server 应用程序将被部署到以下位置：

      IdentityServer_base/SUNWam/servers/web-apps-*instance_name*

   c. IdentityServer_base/SUNWam/bin 目录包含 amServer 的实例特定版本。例如：

      amserver.*instance_name*

d. 将在 IdentityServer_base/SUNWam/lib/AMConfig-*instance_name*.properties 中创建 Identity Server 配置文件的副本。

e. 文件 /etc/rc3.d 包含初始化文件的实例特定版本：

S55amserver.*instance_name*

K55amserver.*instance_name*

注 请勿在创建实例名称时使用 “_”（下划线 _）或 “.”（句点）

2. 通过输入以下命令启动所有的 Identity Server 实例 （包括原先的服务器实例）：

```
./amserver startall
```

也可以使用以下命令启动单个服务器：

IdentityServer_base/SUNWam/bin/amserver.*instance_name* start

现在应该可以通过浏览器调用所有实例的 Identity Server 登录屏幕。

3. 通过输入以下命令停止所有的服务器实例 （包括原先的实例）：

```
./amserver stopall
```

也可以使用以下命令停止单个服务器：

IdentityServer_base/SUNWam/bin/amserver.*instance_name* stop

4. 通过输入以下命令调用 Delete 命令选项：

```
./amserver delete
```

由 Create 命令创建的所有文件应该已被删除。如果使用 Identity Server 卸载实用程序，则由脚本生成的文件不会被删除。

5. 通过输入以下命令指定调试文件的目录：

Edit IdentityServer_base/SUNWam/lib/AMConfig-*instance_name*.properties

确保将 com.iplanet.services.debug.directory 属性更改为您的指定目录。

6. 通过使用以下语法调用 ammultiserverinstall 实用程序：

   ammultiserverinstall [*server-instance-name*] [*port*]

   如果应用需要安装多个 Identity Server 实例，但是倾向于使用非交互式界面，请使用 ammultiserverinstall 实用程序。如果 ammultiserverinstall 失败，将以值 1 退出。

7. amserver 将自动将服务器实例添加到 “平台服务器”列表中。

8. 将 Identity Server 配置为在 SSL 模式中运行。有关此操作的说明，请参见本手册的附录 B “在 SSL 模式中配置 Identity Server”。

9. 输入以下命令以启动所有的 Identity Server 实例：

   ./amserver startall

   也可以使用以下命令启动单个 Identity Server 实例：

   ./amserver-*instance* start

第 11 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。缺省值为 ambak。

--location (-l)

--location 指定备份的目录位置。缺省位置为 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、产品版本和法律通告。

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

该脚本还将备份以下 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 12 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。缺省情况下，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。缺省情况下，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。缺省情况下，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、产品版本和法律通告。

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 13 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 $installroot/SUNWam/bin 下。该实用程序允许您更改管理员或用户的 Identity Server 密码。

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 用于更改管理密码。

--proxy (-p)

--proxy 用于更改代理服务器密码。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 用于加密密码。该选项被打印到命令行。

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/ums

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 中的密码。您必须手动更改 `ServerConfig.xml` 和 Identity Server 的所有验证模板中的密码。

第 14 章

VerifyArchive 命令行工具

本章介绍有关 VerifyArchive 命令行工具的信息，包含以下内容：

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被从归档文件集中删除了。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。

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 管理员的密码。

第 15 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 为缺省端口号。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它端口号。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 （缺省情况下）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 （缺省情况下，位于 *IdentityServer_base*/SUNWam/lib/）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。缺省端口为 58943。

运行 amsecuridd 帮助器

缺省情况下， amsecuridd 位于 *IdentityServer_base*/SUNWam/share/bin。要在缺省端口上运行帮助器，请输入以下命令 （不需要选项）：

```
./amsecuridd
```

要在非缺省端口上运行帮助器，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 （但它只在缺省端口上运行）。

所需的库

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 3 部分

属性参考指南

本部分是 《Sun ONE Identity Server 管理指南》的第三部分 “属性参考指南”。其中介绍了在 Identity Server 的缺省服务中配置的属性。本部分包含以下各章：

- 平台服务属性
- 策略配置服务属性
- SAML 服务属性
- 会话服务属性
- 用户属性

第 16 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 ONE 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缺省值，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
- 组织属性

全局属性

管理服务中的全局属性包括：

- 启用联合管理
- 启用用户管理
- 显示人员容器
- 在菜单中显示容器
- 显示组容器
- 管理的组类型
- 缺省角色权限 (ACI)
- 启用域组件树
- 启用管理员组
- 启用符合用户删除

- 动态管理员角色 ACI
- 用户配置文件服务类
- DC 节点属性列表
- 用于删除的对象的搜索过滤器

启用联合管理

选中该字段将启用联合管理。缺省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。缺省情况下将启用该字段。

显示人员容器

该属性用于指定是否在 Identity Server 控制台中显示 “人员容器”。如果选中该选项，组织、容器和组容器的 “查看”菜单中将显示 “人员容器”菜单选项。仅在平面结构的 DIT 的顶层才会显示 “人员容器”。

人员容器是包含用户配置文件的组织单元。建议在 DIT 中只使用一个人员容器，并利用角色的灵活性来管理帐户和服务。 Identity Server 控制台在缺省情况下会隐藏人员容器。但是，如果 DIT 中有多个人员容器，请选择 “显示人员容器”以将人员容器显示为 Identity Server 控制台中的管理对象。

在菜单中显示容器

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。缺省值是 `false`。管理员可以选择以下两个值之一：

- `false` （未选中复选框）— 位于组织和其它容器顶层的 “查看”菜单的菜单选项中将不列出容器。
- `true` （选中复选框）— 位于组织和其它容器顶层的 “查看”菜单的菜单选项中将列出容器。

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。）缺省值是 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` — 使用 “订阅成员”选项创建的是动态组。
- `Static` — 使用 “订阅成员”选项创建的是静态组。

缺省角色权限 (ACI)

该属性定义用于在创建新角色时授予管理员特权的缺省访问控制指令 (ACI) 或**权限**列表。可以根据所需的特权级别来选择某个 ACI。 Identity Server 在出厂时设置了四种缺省角色权限：

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 或其它目录概念。

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，以将其用作缺省角色。当基于某个缺省角色创建角色时， 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 ONE 组件使用的特定 DIT 结构，用于在 DNS 名称和组织条目之间建立映射。

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。缺省情况下，它将被设置成 Identity Server 的根。如果需要其它后缀，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。

启用管理员组

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删除该用户。但是该操作不能反向进行。在某个组中添加或删除用户时，用户关联的角色中不会添加或删除该用户。

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

该选项指定是否从目录中删除用户条目或只是将用户条目标记为已删除。如果在选中该选项 (true) 的情况下删除用户条目，则用户条目将仍然存在于目录中，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。如果未选中该选项，将从目录中删除用户条目。

动态管理员角色 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缺省 ACI。

注意 组织级别的管理员拥有比组管理员更大的权限。但是，如果在缺省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密码，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。

人员容器管理员

缺省情况下，新创建的组织中的所有用户条目都是该组织的人员容器的成员。人员容器管理员对该组织的人员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删除用户。

注 可以使用 Identity Server 配置其它容器，以包含用户条目、组条目甚至其它容器。要将管理员角色应用到配置组织之后创建的容器，请使用缺省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特权，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负责人所拥有的特权。

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特权。

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，由控制台生成的缺省显示不能完全满足需要。该属性可为任何服务创建自定义显示，利用它可以完全控制服务信息的显示内容和显示方式。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。缺省参数包括：

- 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删除模式时，用于要删除的对象的搜索过滤器。

组织属性

管理服务中的组织属性包括：

- 组缺省人员容器
- 组人员容器列表
- 用户配置文件显示类
- 显示用户的角色
- 显示用户的组
- 用户组自订阅
- 用户配置文件显示选项
- 用户创建缺省角色
- 查看菜单条目
- 搜索返回的结果的最大数目
- 搜索的超时时间 （秒）
- JSP 目录名称
- 联机帮助文档
- 所需的服务
- 用户搜索关键字
- 用户搜索返回属性
- 用户创建通知列表
- 用户删除通知列表
- 用户修改通知列表
- 每页的最大条目数目
- 显示选项
- 事件侦听程序类
- 处理前和处理后的类
- 启用外部属性获取

组缺省人员容器

该字段用于指定在创建用户时，用户将被放到缺省人员容器中。该字段没有缺省值。其有效值是人员容器的 DN。有关人员容器属性为空时的替代顺序，请参见组人员容器列表属性下的说明。

组人员容器列表

该字段用于指定人员容器列表，组管理员在创建新用户时会从中选择人员容器。如果目录树中存在多个人员容器，则可以使用该列表。（如果没有在这个列表和 “组缺省人员容器” 字段中指定 “人员容器”，则将在缺省的 Identity Server 人员容器 `ou=people` 中创建用户。）该字段不存在缺省值。该属性的语法如下所示：

group name|*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 “组缺省人员容器” 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。

显示用户的角色

该选项用于指定是否在用户的 “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。缺省值是 `false`。

显示用户的组

该选项用于指定是否在用户的 “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。缺省值是 `false`。

用户组自订阅

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。缺省值是 `false`。

注 仅当选中“显示用户的组”选项时，该选项才可用。

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”方案属性。

  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，请参见 *Sun ONE Identity Server Customization and API Guide*。

- `Combined` — 显示指定给用户的服务的可查看“用户”和“动态”方案属性。

用户创建缺省角色

该列表用于定义将被自动指定给新创建的用户的角色。该字段没有缺省值。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。

查看菜单条目

该字段列出控制台顶部的“查看”菜单中要显示的服务的 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。缺省值是 100。

注意 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，请参见以下位置的 *Sun ONE Directory Server Installation and Tuning Guide*：

`http://docs.sun.com/db/doc/816-6697-10`

搜索的超时时间 （秒）

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。缺省值是 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，其它应用程序也可以在 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 | 单击时要装入的 *html* 页 | *i18n* 属性文件

例如：

`IdentityServer Help | /AMAdminHelp.html | amAdminModuleMsgs`

所需的服务

该字段列出创建用户条目时动态添加的服务。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

该属性用于定义在 “导航”页中进行搜索时依据的属性名称。该属性的缺省值是 cn。例如，如果该属性使用缺省值，则：

在 “导航”框中的 “名称”字段内输入 j* 后，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，缺省值为 uid cn。这将显示用户 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。为避免性能下降，应使用在用户条目中设置了属性值的属性。

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，请参见第 185 页中的表 19-1。

注 通过修改 amProfile.properties（缺省情况下位于 IdentityServer_base/Identity-Server/SUNWam/locale ）中的属性 497，可以更改发送者电子邮件 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，请参见第 185 页中的表 19-1。

注 通过修改 amProfile.properties（缺省情况下位于 IdentityServer_base/Identity-Server/SUNWam/locale ）中的属性 497，可以更改发送者电子邮件 ID。缺省的发送者 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，请参见第 185 页中的表 19-1。

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。

每页的最大条目数目

该属性允许您定义每页可以显示的最大行数。缺省值是 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。

显示选项

该属性用于添加值，以配置 Identity Server 控制台中的显示选项。输入值并单击“添加”以配置显示选项。值可以为：

表 16-1 显示选项值

参数	说明和语法
generateUserCN	如果设置为 true，该参数会在创建用户时动态生成用户 CN。缺省值为 false。 语法： `generateUserCN=[false|true]`
userAttributeNameForProfileTitle	确定在“用户配置文件”页面的标题上显示的用户属性值。缺省值为 uid。 语法： `userAttributeNameForProflleTitle=[uid|`*`userAttribute`*`]`
autoSelect	当设置为 true （缺省值）时，该参数允许 Identity Server 自动选择“浏览”视图中给定的身份对象类型的第一项。 语法： `autoselect=[true|false]`

参数	说明和语法
disableIntitialSearch	该值将禁用搜索一个或多个身份对象类型的初始 Identity Server 搜索。禁用初始搜索可以缩短显示 Identity Server 控制台的时间。控制台中与此指令对应的服务属性是 “显示选项”，它是管理服务中的一项组织属性。该控制台选项的优先权要高于在 `com.iplanet.am.console.display.off` 中定义的值。如果在 `AMConfig.properties` 中配置该属性，就不要使用控制台配置它 （反之亦然）。 语法 （多个值之间用逗号分隔）： `disableInitialSearch=[users|organizaitons|peopleContainers|organizationalUnits|roles|groups|policies]`
defaultUserView	该参数用于设置 “用户配置文件”页面 “视图”菜单中的缺省视图。缺省情况下会设置所有值。 语法： `defaultUserView=[roles|groups|services|IplanetAMUserService|`*`service name`*`]`
defaultGroupView	该参数用于设置 “组配置文件”页面 “视图”菜单中的缺省视图。缺省情况下会设置所有值。 语法： `defaultGroupView=[general|users]`
defaultRoleView	该参数用于设置 “角色配置文件”页面 “视图”菜单中的缺省视图。缺省情况下会设置所有值。 语法： `defaultRoleView=[general|users|services]`

参数	说明和语法
defaultPolicyView	该参数用于设置 “策略配置文件”页面 “视图”菜单中的缺省视图。缺省情况下会设置所有值。 语法： `defaultPolicyView=[general|rules|subjects|referrals|conditions]`
defaultFederationHostedProviderView	该参数用于设置 “联合管理”模块的 “代管提供商配置文件”页面 “视图”菜单中的缺省视图。缺省情况下会设置所有值。 语法： `defaultFederationHostedProviderView=[general|serviceProvider|identityProvider|authenticaionDomain|trustedProviders|identityServerConfiguration]`
defaultFederationRemoteProviderView	该参数用于设置 “联合管理”模块的 “远程提供商配置文件”页面 “视图”菜单中的缺省视图。缺省情况下会设置所有值。 语法： `defaultFederationRemoteProviderView=[general|serviceProvider|identityProvider|authenticaionDomain]`
rootNavMenu	该参数用于设置根后缀浏览视图中身份对象的缺省视图。缺省情况下会设置所有值。 语法： `rootNavMenu=[organizations|organizationalUnits|groupContainers|peopleContainers|roles|groups|users|policies]`

参数	说明和语法
organizationNavMenu	该参数用于设置 “组织”浏览视图中身份对象的缺省视图。缺省情况下会设置所有值。 语法： `organizationNavMenu=[organizations|organizationalUnits|groupContainers|peopleContainers|roles|groups|users|policies]`
groupContainerNavMenu	该参数用于设置 “组容器”浏览视图中身份对象的缺省视图。缺省情况下会设置所有值。 语法： `groupContainerNavMenu=[groupContainers|groups]`
peopleContainerNavMenu	该参数用于设置 “人员容器”浏览视图中身份对象的缺省视图。缺省情况下会设置所有值。 语法： `peopleContainerNavMenu=[peopleContainers|users]`
federationNavMenu	该参数用于设置 “联合管理”模块浏览视图中身份对象的缺省视图。缺省情况下会设置所有值。 语法： `federationNavMenu=[authenticationDomains|hostedProviders|remoteProviders]`
userProfileMenu	该参数用于设置 “用户配置文件”页面中子视图的菜单条目。缺省情况下会设置所有值。 语法： `userProfileMenu=[roles|groups|services|iPlanetAMUserService|`*`service name`*`]`

参数	说明和语法
groupProfileMenu	该参数用于设置 “组配置文件”页面中子视图的菜单条目。缺省情况下会设置所有值。 语法： `groupProfileMenu=[general|users]`
roleProfileMenu	该参数用于设置 “角色配置文件”页面中子视图的菜单条目。缺省情况下会设置所有值。 语法： `roleProfileMenu=[general|users|services]`
policyProfileMenu	该参数用于设置 “策略配置文件”页面中子视图的菜单条目。缺省情况下会设置所有值。 语法： `policyProfileMenu=[general|rules|subjects|referrals|conditions]`
federationRemoteProviderProfileMenu	该参数用于设置 “联合远程提供商配置文件”页面中子视图的菜单条目。缺省情况下会设置所有值。 语法： `federationRemoteProviderProfileMenu=[general|serviceProvider|identityProvider|authenticationDomain]`
FederationHostedProviderProfileMenu	该参数用于设置 “联合代管提供商配置文件”页面中子视图的菜单条目。缺省情况下会设置所有值。 语法： `federationHostedProviderProfileMenu=[general|serviceProvider|identityProvider|authenticationDomain|trustedProviders|identityServerConfiguration]`

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 （从安装 Identity Server 时的基础组织），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。缺省情况下，不启用该选项。

第 17 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缺省值。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缺省值。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
- 用户名区分大小写
- 缺省匿名用户名
- 验证级别

有效匿名用户列表

该字段包含登录时不需要提供凭证的用户 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指定给指定的用户 ID。

如果此列表为空，访问以下缺省模块登录 URL 将作为缺省匿名用户名被验证：

```
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，访问缺省模块登录 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 >
```

用户名区分大小写

如果启用，该选项允许对用户 ID 区分大小写。缺省情况下，不启用该属性。

缺省匿名用户名

该字段用于定义当有效匿名用户列表为空且访问以下缺省模块登录 URL 时，为会话指定的用户 ID：

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name
```

缺省值是 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，则可以使用缺省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=<缺省匿名用户名>
```

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所需的最小级别，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。缺省值为 0。

注 如果未指定任何验证级别，核心验证属性 “缺省验证级别” 中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 189 页中的 “缺省验证级别”。

第 18 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缺省值。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缺省值。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：

- 在 LDAP 中匹配证书
- 主题 DN 中用于搜索 LDAP 的属性
- 将证书与 CRL 匹配
- 发布者 DN 中用于搜索 CRL 的属性
- 启用 OCSP 验证
- LDAP 服务器和端口
- LDAP 起始搜索 DN
- LDAP Server 主要用户
- LDAP Server 主要密码
- 配置文件 ID 的 LDAP 属性
- 使用 SSL 访问 LDAP
- 证书中用于访问用户配置文件的字段
- 证书中用于访问用户配置文件的其它字段
- 可信赖的远程主机
- SSL 端口号
- 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，且不需要其它验证，则允许用户访问。在缺省情况下，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 174 页中的 “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。

主题 DN 中用于搜索 LDAP 的属性

该字段用于指定证书的 SubjectDN 属性的值，该值将用于在 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。缺省值是 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 中的属性名称定位。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。在缺省情况下，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。

发布者 DN 中用于搜索 CRL 的属性

该字段用于指定接收到的证书的发布者 SubjectDN 属性的值，该值将用于在 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。缺省值是 CN。

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

LDAP 服务器和端口

该字段用于指定存储证书的 LDAP 服务器的名称和端口号。缺省值是安装 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

该字段用于指定节点的 DN，将从该 DN 开始搜索用户证书。该字段没有缺省值。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。

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。该字段没有缺省值，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 主要密码

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 密码。该字段没有缺省值，它接受指定主要用户的有效 LDAP 密码。

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。该字段不存在缺省值，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 访问 LDAP

该选项用于指定是否使用 SSL 来访问 LDAP 服务器。在缺省情况下，证书验证服务不使用 SSL 来访问 LDAP 服务器。

证书中用于访问用户配置文件的字段

该菜单用于指定应该使用证书的主题 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。缺省字段是 `subject CN`。该列表包含以下内容：

- email address
- subject CN
- subject DN
- subject UID
- other

证书中用于访问用户配置文件的其它字段

如果将 “证书中用于访问用户配置文件的字段”属性的值设置为 `other`，则该字段用于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。该配置仅与 Sun ONE Portal Server 一起使用。

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。添加或更改 SSL 端口号之前，请参见 Sun ONE Identity Server Customization and API 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所需的最小级别，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。缺省值为 `0`。

注 如果未指定任何验证级别，核心验证属性 “缺省验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 189 页中的 “缺省验证级别”。

第 19 章

核心验证属性

核心验证服务是所有缺省验证服务的基本服务，也是使用验证 SPI 创建的自定义验证服务的基本服务。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 ONE 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缺省值。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缺省值。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
- 组织属性

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
- 客户机支持的验证模块
- LDAP 连接池大小
- LDAP 连接池的缺省大小

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。缺省情况下，包括 LDAP、 SafeWord、 SecurID、应用程序、匿名、 HTTP Basic、成员资格、 Unix、证书、 NT 和 RADIUS。 Identity Server 还包括可用于添加其它验证服务的公共 SPI。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 连接池的缺省大小

该属性用于设置要与所有 LDAP 验证模块配置一起使用的缺省最小连接池和最大连接池。如果 “LDAP 连接池大小”属性中存在主机和端口条目，则不会使用 “LDAP 连接池的缺省大小”中的最小及最大设置。

组织属性

核心验证服务中的组织属性包括：

- 组织验证模块
- 用户配置文件
- 管理员验证
- 用户配置文件动态创建缺省角色
- 持久 Cookie 模式
- 持久 Cookie 最长时间 （秒）
- 所有用户的人员容器
- 别名搜索属性名称
- 缺省验证级别
- 用户命名属性
- 缺省验证语言环境
- 组织验证配置
- 登录失败锁定模式
- 登录失败锁定计数
- 登录失败锁定间隔 （分钟）
- 用于发送锁定通知的电子邮件地址
- N 次失败后警告用户
- 登录失败锁定时间 （分钟）
- 锁定属性名称
- 锁定属性值
- 缺省成功登录 URL
- 缺省失败登录 URL
- 验证后处理类
- 用户名生成器模式
- 可插接用户名生成器类

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。缺省验证模块为 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

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

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。

用户配置文件动态创建缺省角色

如果在第 182 页中的 “用户配置文件”特征中选中了 “动态创建”，则该字段将指定指派给创建了配置文件的新用户的角色。该字段没有缺省值。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。

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 “持久 Cookie 模式”可以保留用户会话。当启用 “持久 Cookie 模式”时，在用户会话的持久 Cookie 过期后或用户明确注销后，用户会话才会过期。过期时间是在 “持久 Cookie 最长时间 （秒）”中指定的。缺省值为未启用 “持久 Cookie 模式”，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 （秒）

该字段用于指定经过多长时间后持久 Cookie 过期。（必须已通过选中相应复选框启用 “持久 Cookie 模式”。）该时间间隔从成功验证用户的会话时开始计算。缺省值为 `2147483` （以秒为单位）。该字段可以是 `0` 与 `2147483` 之间的任意整数值。

所有用户的人员容器

在用户进行成功验证后，将检索用户配置文件。该字段中的值用于指定搜索配置文件的位置。通常情况下，该值将是缺省人员容器的 DN。添加到组织的所有用户条目被自动添加到组织的缺省人员容器中。缺省值是 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：

- 在缺省的人员容器中搜索，然后
- 在缺省的组织中搜索，然后
- 使用 “别名搜索属性名称”属性在缺省组织中搜索用户。

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

在用户进行成功验证后，将检索用户配置文件。该字段用于指定次 LDAP 属性，当根据第 184 页中的 “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。该属性不存在缺省值，它可以接受任何有效的 LDAP 属性 （例如 cn）。

用户命名属性

在用户进行成功验证后，将检索用户配置文件。该属性的值指定用于进行搜索的 LDAP 属性。缺省情况下， Identity Server 假定用户条目是由 uid 属性标识的。如果您的 Directory Server 使用的是其它属性 （例如 givenname），请在该字段中指明属性名称。

缺省验证语言环境

该字段用于指定验证服务要使用的缺省语言子类型。缺省值为 en_US。可以在表 19-1 中找到有效语言子类型的列表。

为了使用其它语言环境，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 *Sun ONE Identity Server Customization and API Guide* 中的第三章 “Authentication Service”。

表 19-1 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
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

表 19-1 支持的语言环境 （续）

语言标记	语言
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。缺省验证模块为 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 Sun ONE Identity Server Customization and API Guide。

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。缺省情况下，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 （分钟）”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 （分钟）

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 （分钟）

该属性用于启用内存锁定。缺省情况下，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。缺省情况下，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，缺省实现值为 `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。缺省情况下，对于 inetuserstatus 值设置为 0。

缺省成功登录 URL

该字段用于指定验证成功后用户被重定向到的 URL，它可以接受任何有效的 URL。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 *Sun ONE Identity Server Customization and API Guide*。

缺省失败登录 URL

该字段用于指定验证失败后用户被重定向到的 URL，它可以接受任何有效的 URL。失败登录 URL 设置于 remote-auth.dtd 中的 LoginStatus 元素中。有关详细信息，请参见 *Sun ONE Identity Server Customization and API Guide*。

验证后处理类

该字段指定用于为成功或不成功登录自定义登记验证过程的 Java 类的名称。示例：

```
com.abc.authentication.PostProcessClass
```

该 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。

用户名生成器模式

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 “用户名生成器模式” 时，用来生成用户 ID 的 Java 类的名称。

缺省验证级别

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所需的最小级别，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。

验证级别应该在组织的特定验证模板中进行设置。这里所描述的 “缺省验证级别” 值只有在 “验证级别” 字段中没有为特定组织的验证模板指定验证级别时才适用。“缺省验证级别” 的缺省值为 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。）

第 20 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 验证模板的缺省值。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缺省值。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所需的最小级别，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。缺省值为 0。

注 如果未指定任何验证级别，核心验证属性 “缺省验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 189 页中的 “缺省验证级别”。

第 21 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 验证模板的缺省值。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缺省值。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 服务器和端口
- 辅助 LDAP 服务器和端口
- 起始用户搜索的 DN
- root 用户绑定的 DN
- root 用户绑定的密码
- root 用户绑定的密码 （确认）
- 用户命名属性
- 用户条目搜索属性
- 用户搜索过滤器
- 搜索范围
- 对 LDAP 服务器启用 SSL
- 将用户 DN 返回到验证
- LDAP 服务器检查间隔
- 用户创建属性列表
- 验证级别

主 LDAP 服务器和端口

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 服务器和端口

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。

注意 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。）缺省值是目录树的根。可以接受任何有效的 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。

root 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。验证服务需要以该 DN 进行绑定，以便基于用户的登录 ID 来搜索匹配的用户 DN。缺省值为 `amldapuser`。可以接受任何有效的 DN。

在注销之前，请确保密码正确。因为如果密码不正确，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。缺省情况下，这就是您通常登录时所使用的 amAdmin 帐户，不过您要使用完整的 DN。例如：

`uid_amAdmin,ou=People,`*`IdentityServer_base`*

root 用户绑定的密码

该字段的取值为在 “root 用户绑定的 DN”字段中所指定的管理员配置文件密码。该字段没有缺省值。只接受管理员的有效 LDAP 密码。

root 用户绑定的密码 （确认）

对密码进行确认。

用户命名属性

在用户进行成功验证后，将检索用户配置文件。该属性的值用于执行搜索。该字段指定要使用的 LDAP 属性。缺省情况下， Identity Server 假定用户条目是由 `uid` 属性标识的。如果您的 Directory Server 使用的是其它属性 （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 “用户条目命名属性”的组合。

用户条目搜索属性

该字段列出用于为将被验证的用户形成搜索过滤器的属性，并允许用户在用户条目中使用多个属性进行验证。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。该字段没有缺省值。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 195 页中的 “起始用户搜索的 DN”属性中指定的节点开始搜索。缺省值为 `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

注意 即使子组织处于无效状态，子组织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

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。缺省情况下，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。

将用户 DN 返回到验证

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。它用于定义检验 LDAP 主服务器是否正在运行之前，线程将 “休眠”的秒数。

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。只有当 “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所需的最小级别，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。缺省值为 0。

注 如果未指定任何验证级别，核心验证属性 “缺省验证级别” 中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 189 页中的 “缺省验证级别”。

第 22 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缺省值。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缺省值。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：

- 最小密码长度
- 缺省用户角色
- 注册后的用户状态
- 主 LDAP 服务器和端口
- 辅助 LDAP 服务器和端口
- 起始用户搜索的 DN
- root 用户绑定的 DN
- root 用户绑定的密码
- root 用户绑定的密码 （确认）
- 用户命名属性
- 用户条目搜索属性
- 用户搜索过滤器
- 搜索范围
- 对 LDAP 服务器启用 SSL
- 将用户 DN 返回到验证
- 验证级别

最小密码长度

该字段用于指定自注册过程中设置密码时要求的最小字符数。缺省值为 8。

如果更改了该值，还应在以下文件的注册和错误文本中对其进行更改：

IdentitySever_base/locale/amAuthMembership.properties (PasswdMinChars *entry)*

缺省用户角色

该字段用于指定分配给新用户的角色，这些用户的配置文件是通过自注册创建的。该字段没有缺省值。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。所有其它 DN 将被忽略。

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。缺省值为 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 服务器和端口

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 服务器和端口

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。

注意 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。）缺省值是目录树的根。可以接受任何有效的 DN。如果使用了多个条目，条目前面必须带有本地服务器名称。

注 如果有多个用户与同一个搜索相匹配，则验证将会失败。

root 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。验证服务需要以该 DN 进行绑定，以便基于用户的登录 ID 来搜索匹配的用户 DN。缺省值为 `amldapuser`。可以接受任何有效的 DN。

root 用户绑定的密码

该字段的取值为在 “root 用户绑定的 DN”字段中所指定的管理员配置文件密码。该字段没有缺省值。仅接受管理员的有效 LDAP 密码。

root 用户绑定的密码 （确认）

对密码进行确认。

用户命名属性

该字段用于指定用户条目命名惯例的属性。缺省情况下， Identity Server 假定用户条目是由 `uid` 属性标识的。如果您的 Directory Server 使用的是其它属性 （例如 `givenname`），请在该字段中指明属性名称。

用户条目搜索属性

该字段列出用于为将被验证的用户形成搜索过滤器的属性，并允许用户在用户条目中使用多个属性进行验证。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。该字段没有缺省值。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 201 页中的 “起始用户搜索的 DN”属性中指定的节点开始搜索。缺省值为 `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

对 LDAP 服务器启用 SSL

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。缺省情况下未选中该复选框， SSL 协议不用于访问 Directory Server。

将用户 DN 返回到验证

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所需的最小级别，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。缺省值为 `0`。

注 如果未指定任何验证级别，核心验证属性 “缺省验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 189 页中的 “缺省验证级别”。

第 23 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 验证模板的缺省值。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缺省值。组织属性不会被组织子树中的条目继承。

只有 Solaris 版的 Identity Server 支持 NT 验证。为了实现 NT 验证模块，必须下载并安装 Samba Client 2.2.2。 Samba Client 是文件与打印服务器，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。要了解有关详情以及下载该软件，请访问 http://wwws.sun.com/software/download/products/3e3af224.html。

NT 验证属性包括：

- NT 验证域
- NT 验证主机
- 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)。缺省情况下， 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所需的最小级别，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。缺省值为 `0`。

注 如果未指定任何验证级别，核心验证属性 “缺省验证级别” 中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 189 页中的 “缺省验证级别”。

第 24 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 验证模板的缺省值。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缺省值。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
- RADIUS 服务器 2
- RADIUS 共享秘密
- RADIUS 共享秘密 （确认）
- RADIUS 服务器的端口
- 超时 （秒）
- 验证级别

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。缺省的 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)。该服务器用于进行故障切换，当联系不上主服务器时将联系该服务器。缺省的 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。共享秘密的合格条件应与选择得当的密码相同。该字段不存在缺省值。

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。缺省值为 `1645`。

注 如果未指定任何验证级别，核心验证属性 “缺省验证级别” 中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 189 页中的 “缺省验证级别”。

超时 （秒）

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。缺省值为 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所需的最小级别，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。缺省值为 0。

注 如果未指定任何验证级别，核心验证属性 “缺省验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 189 页中的 “缺省验证级别”。

第 24 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 验证模板的缺省值。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缺省值。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 服务器规范
- SafeWord 系统名
- SafeWord 服务器验证文件路径
- SafeWord 日志级别
- SafeWord 日志路径
- 验证级别

SafeWord 服务器规范

该字段指定 SafeWord 或 SafeWord PremiereAccess 服务器的名称和端口。端口 7482 为 SafeWord 服务器的缺省端口。SafeWord PremierAccess 服务器的缺省端口号为 5030。

SafeWord 系统名

该字段用于指定 SafeWord 服务器中配置的系统名。缺省的系统名为 `STANDARD`。

SafeWord 服务器验证文件路径

该字段用于指定 SafeWord 客户机库放置其验证文件的目录。缺省路径如下所示：

```
/var/opt/SUNWam/auth/safeword/serverVerification
```

如果该字段中指定的是其它目录，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 日志路径

该属性用于指定 SafeWord 客户机日志的目录路径和日志文件名。缺省路径如下所示：

```
/var/opt/SUNWam/auth/safeword/safe.log
```

如果指定的是其它路径或文件名，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所需的最小级别，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。缺省值为 0。

注 如果未指定任何验证级别，核心验证属性 “缺省验证级别” 中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 189 页中的 “缺省验证级别”。

第 25 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 验证模板的缺省值。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缺省值。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：

- SecurID ACE/Server 配置路径
- SecurID 帮助器配置端口
- SecurID 帮助器验证端口
- 验证级别

注 在 Identity Server 6.1 中， 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。缺省路径如下所示：

```
/opt/ace/data
```

如果该字段中指定的是其它目录，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。缺省端口为 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。缺省端口为 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所需的最小级别，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。缺省值为 `0`。

注 如果未指定任何验证级别，核心验证属性 “缺省验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 189 页中的 “缺省验证级别”。

第 26 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 ONE 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缺省值，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：

- 全局属性
- 组织属性

注 Windows 2000 平台不支持 Unix 验证服务。

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
- Unix 帮助器验证端口
- Unix 帮助器超时 （分钟）
- Unix 帮助器线程

Unix 帮助器配置端口

该属性用于指定当启动 “Unix 帮助器验证端口”、“Unix 帮助器超时 （分钟）” 和 “Unix 帮助器线程” 属性中包含的配置信息时， Unix 帮助器 “侦听” 的端口。缺省端口为 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

该属性用于指定 Unix 帮助器 “侦听”的端口，以获取配置后的验证请求。缺省端口为 57946。

Unix 帮助器超时 （分钟）

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。缺省时间为 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。缺省值为 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所需的最小级别，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。缺省值为 0。

注 如果未指定任何验证级别，核心验证属性 “缺省验证级别”中指定的值将会存储到 SSO 令牌中。有关详细信息，请参见第 189 页中的 “缺省验证级别”。

第 27 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，则在缺省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
- 登录成功 URL
- 登录失败 URL
- 验证后处理类

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 可以使用的缺省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： • REQUIRED — 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。 • REQUISITE — 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）。 • SUFFICIENT — 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。 • OPTIONAL — 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。 这些标志为定义了它们的验证模块建立了执行标准。执行是有等级的：REQUIRED 等级最高， OPTION 等级最低。 例如，如果管理员使用 REQUIRED 标志定义 LDAP 模块，则用户凭证必须通过 LADP 验证要求才能访问给定资源。 如果添加多个验证模块，并将每个模块的“标志”都设置成 REQUIRED，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	还可以以“关键字 = 值”对的形式为模块增加其它选项。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 28 章

客户机检测服务属性

客户机检测服务属性是全局属性。全局化设置属性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。

最初使用时，可供基于 HTML 的浏览器使用的仅有的已配置 Identity Server 客户机数据被定义为总体模式 genericHTML 及其父 HTML 的子配置。

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缺省属性。

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、操作系统和已安装的软件的属性。

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。

其它属性。允许您添加设备的其它属性。

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 “**”字符表示该设备已被自定义。使用 “缺省”链接可以删除自定义的属性并将设备重置为缺省设置。

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/terms.asp?doc=WAP-248-UAProf-20011020-a.pdf

要复制设备及其属性，请单击 “复制”链接。设备名称必须唯一。缺省情况下，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。

缺省客户机类型

该属性定义 “客户机类型”属性中客户机类型列表的缺省客户机类型。缺省值为 `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。缺省的客户机检测类为 `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，则由 “客户机检测类”属性中指定的类来路由各个请求。

缺省情况下，对除 genericHTML 之外的所有客户机类型均禁用客户机检测功能。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 29 章

全球化设置服务属性

全球化设置服务属性是全局属性。全球化设置属性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。）全球化设置属性包括：

- 各个语言环境支持的字符集
- 字符集别名
- 自动生成的通用名称格式

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、复制和删除字符集。

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来形成 java 字符集与 IANA 字符集之间的映射。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、复制和删除字符集别名。

自动生成的通用名称格式

利用该显示选项可以定义名称自动生成的方式，以使名称格式与不同的语言环境和字符集相适应。缺省语法如下 （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，如果要采用中文字符集为具有 uid (11111) 的用户 (User One) 显示新的名称格式，请使用以下形式：

```
zh = {sn}{givenname}({uid})
```

这将显示为：

```
OneUser 11111
```

第 30 章

日志服务属性

日志服务属性是全局属性。日志属性所采用的值将被应用到整个 Sun ONE 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：

- 最大日志大小
- 历史文件数目
- 日志位置
- 日志类型
- 数据库用户名
- 数据库用户密码
- 数据库用户密码 （确认）
- 数据库驱动程序名
- 可配置日志字段
- 日志验证时间
- 日志签名时间
- 安全日志
- 最大记录数目
- 每个归档文件中的文件数目
- 缓冲区大小
- 缓冲时间
- 缓冲时间

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）。缺省值为 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。缺省值为 3。

日志位置

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。缺省位置为：

/var/opt/SUNWam/logs

如果使用了非缺省目录，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。

数据库用户密码

当 “日志类型”属性设置为 “DB”时，该属性采用数据库用户密码。

数据库用户密码 （确认）

确认数据库密码。

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。缺省情况下，将记录以下字段：

- Domain
- Hostname
- IPAddress
- LoggedBy
- Loglevel
- LoginID
- ModuleName

日志验证时间

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）。缺省时间为 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）。缺省时间为 900 秒。该参数仅适用于安全日志。

安全日志

该属性用于指定是否启用安全日志。缺省情况下，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。缺省情况下，该属性被设置成 500。日志 API 的调用者可以通过 LogQuery 参数来覆盖该属性。

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。缺省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。缺省情况下是一条记录。

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。缺省值是 3600 秒。

缓冲时间

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 31 章

命名服务属性

命名服务属性是全局属性。 SAML 属性所采用的值将被应用到整个 Sun ONE 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
- 会话服务 URL
- 日志服务 URL
- 策略服务 URL
- 验证服务 URL
- SAML Web 配置 / 辅件服务 URL
- SAML SOAP 服务 URL
- SAML Web 配置 /POST 服务 URL
- SAML 断言管理器服务 URL
- 联合断言管理器服务 URL
- 身份 SDK 服务 URL

配置服务 URL

该字段采用的值为

%protocol://%host:%port/*Server_DEPLOY_URI*/profileservice

该语法允许基于特定会话参数动态替换配置 URL。

会话服务 URL

该字段采用的值为

%protocol://%host:%port/*Server_DEPLOY_URI*/sessionservice

该语法允许基于特定会话参数动态替换会话 URL。

日志服务 URL

该字段采用的值为

%protocol://%host:%port/*Server_DEPLOY_URI*/loggingservice

该语法允许基于特定会话参数动态替换日志 URL。

策略服务 URL

该字段采用的值为

%protocol://%host:%port/*Server_DEPLOY_URI*/policyservice

该语法允许基于特定会话参数动态替换策略 URL。

验证服务 URL

该字段采用的值为

%protocol://%host:%port/*Server_DEPLOY_URI*/authservice

该语法允许基于特定会话参数动态替换验证 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

该语法允许基于特定会话参数动态替换 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

该语法允许基于特定会话参数动态替换 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

该语法允许基于特定会话参数动态替换 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

该语法允许基于特定会话参数动态替换 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/FSAssertionManagerIF

该语法允许基于特定会话参数动态替换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/
```

该语法允许基于特定会话参数动态替换身份 SDK 服务 URL。

第 32 章

密码重置服务属性

密码重置服务属性是组织属性。在“服务配置”下密码重置属性所采用的值将成为给定组织中密码重置服务的缺省值。组织属性不会被组织子树中的条目继承。

密码重置属性包括：

- 用户验证
- 秘密问题
- 搜索过滤器
- 基本 DN
- 绑定 DN
- 绑定密码
- 密码重置选项
- 密码更改通知选项
- 启用密码重置
- 启用私人问题
- 问题数目
- 密码重置失败锁定计数
- 密码重置失败锁定间隔 （分钟）
- 用于发送锁定通知的电子邮件地址
- N 次失败后警告用户
- 密码重置失败锁定持续时间 （分钟）
- 密码重置失败锁定模式

- 密码重置锁定属性名称
- 密码重置锁定属性值

用户验证

该属性指定搜索要重置其密码的用户时使用的值。

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密码。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密码。

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 “绑定密码”来重置用户密码。

绑定密码

可以同时使用该属性值与 “绑定 DN”来重置用户密码。

密码重置选项

该属性用于确定重置密码时使用的类名。缺省的类名为：

```
com.sun.identity.password.RandomPasswordGenerator
```

可以通过插件自定义密码重置类，这个类需要由 `PasswordGenerator` 接口实现。有关详细信息，请参见 *Sun ONE Identity Server Customization and API Guide*。

密码更改通知选项

该属性用于确定重置密码时通知用户的方法。缺省的类名为：

```
com.sun.identity.password.EmailPassword
```

可以通过插件自定义密码通知类，这个类需要由 `NotifyPassword` 接口实现。有关详细信息，请参见 *Sun ONE Identity Server Customization and API Guide*。

启用密码重置

选择该属性将启用密码重置功能。

启用私人问题

选择该属性将允许用户创建独特的密码重置问题。

问题数目

该值用于指定最多可以在密码重置页面上提多少个问题。

密码重置失败锁定计数

该属性用于定义在 “密码重置失败锁定间隔”中指定的时间间隔内，用户在被锁定之前可以重置密码的次数。

例如，如果将 “密码重置失败锁定计数”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 次密码。

密码重置失败锁定间隔 （分钟）

该属性用于定义用户在被锁定之前，可以尝试重置密码 （重置次数在 “密码重置失败锁定计数”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密码重置服务锁定时接收通知的电子邮件地址。可以采用以空格分隔的列表形式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，允许的密码重置失败的次数。

密码重置失败锁定持续时间 （分钟）

该属性定义在发生锁定之后，用户不能重置密码的持续时间 （以分钟为单位）。

密码重置失败锁定模式

该属性指定如果用户最初重置密码 （使用密码重置应用程序）失败，是否禁止用户重置其密码。缺省情况下，不启用该功能。

密码重置锁定属性名称

该属性包含 “密码重置锁定属性值”中设置的 `inetuserstatus` 值。如果用户在密码重置中被锁定，且 “密码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，以禁止用户重置其密码。

密码重置锁定属性值

该属性用于将用户状态的 inetuserstatus 值 （包含在 “密码重置锁定属性名称” 中）指定为有效或无效。如果用户在密码重置中被锁定，且 “密码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，以禁止用户重置其密码。

第 33 章

平台服务属性

平台服务属性是全局属性。 SAML 属性所采用的值将被应用到整个 Sun ONE 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
- 平台语言环境
- Cookie 域
- 登录服务 URL
- 注销服务 URL
- 可用的语言环境
- 客户机字符集

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 工作，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。列表中的第一个值用于指定安装过程中指定的服务器的主机名称和端口。列表的结尾是一个两字节的值，该值唯一标识服务器。参与平衡负荷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。

平台语言环境

平台语言环境的值是安装 Identity Server 时使用的缺省语言子类型。验证、记录和管理服务是用该缺省值的语言进行管理的。缺省值为 `en_US`。有关所有支持的语言子类型的列表，请参见第 185 页中的表 19-1。

Cookie 域

这是一个域列表，当在验证过程中将 Cookie 设置到用户的浏览器时， 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 将只会发送到 Identity Server 本身，而不发送到域中的其它服务器。如果域中的其它服务器需要 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。该字段的缺省值是安装的 Identity Server 的域。

登录服务 URL

该字段用于指定登录页面的 URL。该属性的缺省值为 */Service_DEPLOY_URI*`/UI/Login`。

注销服务 URL

该字段用于指定注销页面的 URL。该属性的缺省值为 */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 34 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 ONE 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缺省值。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缺省值。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
- 组织属性

全局属性

策略配置服务中的全局属性为：

- 资源比较器

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大小写还是忽略大小写。`False` 表示忽略大小写， `True` 表示考虑大小写。

组织属性

策略配置服务中的组织属性包括：

- LDAP 服务器和端口
- LDAP 基本 DN
- LDAP 用户基本 DN
- Identity Server 角色基本 DN
- LDAP 绑定 DN
- LDAP 绑定密码
- LDAP 绑定密码 （确认）
- LDAP 组织搜索过滤器
- LDAP 组织搜索范围
- LDAP 组搜索过滤器
- LDAP 组搜索范围
- LDAP 用户搜索过滤器
- LDAP 用户搜索范围
- LDAP 角色搜索过滤器

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 服务器主机的故障切换配置，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

对于故障切换配置：

machine1.example1.com|machine1.example1.com:389 machine2.example.com1:389

machine1.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。缺省情况下，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。缺省情况下，它是安装 Identity Server 时的基础组织的顶级组织。

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。缺省情况下，它是安装 Identity Server 时的基础组织的顶级组织。

LDAP 绑定 DN

该字段指定 LDAP 服务器中的绑定 DN。

LDAP 绑定密码

该属性定义用于绑定 LDAP 服务器的密码。缺省情况下，安装过程中输入的 amldapuser 密码将用作绑定用户。

LDAP 绑定密码 （确认）

确认 LDAP 绑定密码。

LDAP 组织搜索过滤器

指定用于查找组织条目的搜索过滤器。缺省值为 (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 （缺省值）

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。缺省值为 (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 （缺省值）

LDAP 用户搜索过滤器

指定用于查找用户条目的搜索过滤器。缺省值为 (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 （缺省值）

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。缺省值为 (&(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 （缺省值）

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 （缺省值）

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。缺省值为 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。缺省值为 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。缺省值为 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。缺省值为 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。缺省值为 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 （秒）

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（缺省）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。缺省值为 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。缺省值为 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来基于单一登录令牌评估同一策略请求。

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。以 SSO 令牌 ID 作为关键字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策略、同一 SSO 令牌 ID 进行另一次评估，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=luser`），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 35 章

SAML 服务属性

安全断言标记语言 (SAML) 服务属性是全局属性。 SAML 属性所采用的值将被应用到整个 Sun ONE 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，请参见 *Sun ONE Identity Server Customization and API Guide*。

SAML 属性包括：

- 站点 ID 和站点发布者姓名
- 签名请求
- 签名响应
- 签名断言
- 辅件名
- 目标说明符
- 辅件超时 （秒）
- 断言不早于偏差因数
- 断言超时 （秒）
- 可信赖的伙伴站点
- 发送给目标 URL 的 POST

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。缺省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//。

签名请求

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。

签名响应

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。

辅件名

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。缺省值为 SAMLart。例如，使用缺省 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。缺省值为 `Target`。

辅件超时 （秒）

该属性指定为辅件创建的断言超时。缺省值为 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 （缺省值为 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 （秒）

该属性指定经过多少秒后发生断言超时。缺省值为 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 35-1 可信赖的伙伴站点参数

SourceID	该参数为长 20 字节的序列，它是站点 ID 和发布者姓名的一部分。
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，缺省值为 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。
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的站点中的该列表中，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。它的缺省值为： com.sun.identity.saml.plugins.DefaultAccountMapper
attributeMapper	指定一个类，该类包含 attributeMapper 所在的路径。可以在应用程序中开发一个 attributeMapper 来通过查询获得一个 SSOToken ID 或获得一个包含 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。可以在应用程序中开发一个 actionMapper 来通过查询获得一个 SSOToken ID 或获得一个包含 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定。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。可以在应用程序中开发一个 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]
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 或任何其它的 URL。

第 36 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，则在缺省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缺省会话值。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缺省值的值，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
- 搜索的超时时间 （秒）

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。缺省值为 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。缺省值为 5 秒。

动态属性

动态属性包括：

- 最大会话时间 （分钟）
- 最大空闲时间 （分钟）
- 最大缓存时间 （分钟）

最大会话时间 （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 1）的值。缺省值为 120。（为了同时实现安全和方便两方面的要求，可以考虑将 “最大会话时间”的时间间隔设置为一个较大的值，而将 “最大空闲时间”的时间间隔设置为一个相对小的值。）“最大会话时间”限制了会话的有效性。会话不能超过设定的 “最大会话时间”。

最大空闲时间 （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 1）的值。缺省值为 30。（为了同时实现安全和方便两方面的要求，可以考虑将 “最大会话时间”的时间间隔设置为一个较大的值，而将 “最大空闲时间”的时间间隔设置为一个相对小的值。）

最大缓存时间 （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。缺省值为 3。建议最大缓存时间应始终小于最大空闲时间。

第 37 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缺省属性。“用户管理”窗口中包含用户项属性。

- 用户服务属性
- 用户配置文件属性
- 唯一用户 ID

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指派到 Identity Server 中配置的角色或组织。当角色被指定给用户，或用户被指定到组织时，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 DN 起始视图
- 缺省用户状态

缺省的用户值是为所有 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 （非缺省值）。

用户首选语言

该字段指定用户选择的在 Identity Server 控制台中显示的文本语言。缺省值为 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。该字段没有缺省值。

继承的语言环境

该字段指定用户的语言环境。缺省值为 en_US。可以使用第 185 页中的表 19-1 中的任何值。

管理 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。该字段没有缺省值。可以使用用户至少拥有读取权限的有效 DN。

缺省用户状态

该选项用于指示新创建的用户的缺省状态。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。缺省值为 “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，选择值并将其应用到角色，然后将该角色添加到用户配置文件中。

用户配置文件属性

用户配置文件属性是用户配置文件的缺省属性。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，请参见 *Sun ONE Identity Server Customization and API 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`。但管理员可以配置 Sun ONE 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，请参见本章结尾处的“唯一用户 ID”，或 *Sun One Directory Server Administrator's Guide*。

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。

密码

该字段中是在“用户 ID”字段中指定的名称的密码。

密码（确认）

对密码进行确认。

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。缺省值为 “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`。如果您指派的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，请参见 *Sun ONE Identity Server Customization and API 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。缺省的验证方法是 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。缺省值为 `en_US`。可以使用第 185 页中的表 19-1 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

该属性指定用户在验证成功后，重新指向的 URL。

失败 URL

该属性指定用户在验证失败后，重新指向的 URL。

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。缺省状态下，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 ONE Identity Server 生成的错误消息的列表。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 ONE 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：	当前用户删除该对象之前，该对象可能已被其他用户删除。	重新显示正试图删除的对象，然后再次尝试删除操作。
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。请与管理员联系。	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 “goto” 查询参数并结合像管理控制台 URL 这样的值。
logout.failure.	用户无法退出 Identity Server。	重新启动服务器。
uncaught_exception	由于处理程序不正确，出现验证异常。	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 容器的错误日志以查看是否有错误。
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	输入的密码无效。	密码必须包含至少 8 个字符。检查密码是否包含相应数量的字符并确保其未过期。
auth.failed	验证失败。这是缺省登录失败模板中显示的通用错误消息。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/密码（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	输入密码的字符数不足。登录到成员资格/自注册验证模块时，可能显示此错误。	缺省情况下，登录密码必须包含至少 8 个字符 （此数目可通过成员资格验证模块配置）。
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 “密码” 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。	确保用户名和密码不相同。
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。

表 A-2 验证错误代码

错误消息	说明/可能的原因	操作
no.password	未输入密码。登录到成员资格/自注册验证模块时，可能显示此错误。	确保输入密码。
missing.confirm.passwd	遗漏确认密码字段。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 “确认密码”字段中输入密码。
password.mismatch	密码与确认密码不匹配。登录到成员资格/自注册验证模块时，可能显示此错误。	确保密码与确认密码匹配。
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。	
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。	确保所需的验证模块在所需的组织下注册，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所需的验证方法。
cookie.notpersistent	持久 Cookie 域中不存在持久 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	未填写其中的某个必填字段。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。	使用其它名称创建策略。
rule_name_already_present	另一个具有给定名称的规则已存在。	使用其它规则名称创建策略。
rule_already_present	具有相同规则值的规则已存在。	使用其它规则值。
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 绑定密码无效。	策略配置中定义的 LDAP 绑定用户的密码不正确。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。
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。

表 A-3 策略错误代码

错误消息	说明/可能的原因	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 命令行工具生成到 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 值中缺少密码。	在 --password 值中提供密码。
nolocalename	6	未提供语言环境名称。缺省语言环境为 en_US。	有关语言环境的列表，请参见缺省验证语言环境。
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。

表 A-4 amadmin 错误代码

错误消息	代码	说明/可能的原因	操作
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。
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 和密码正确。
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。
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、密码、主机名或端口号无效导致 LDAP 验证失败。	确保用户 DN 和密码正确。

表 A-4 amadmin 错误代码

错误消息	代码	说明/可能的原因	操作
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。
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	人员容器 DN 无效。	确保 XML 文件中的 DN 有效并为人员容器对象。
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。

表 A-4 amadmin 错误代码

错误消息	代码	说明/可能的原因	操作
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删除用户。	确保 XML 文件中的角色 DN 不是过滤的角色。
cannotRemoveUsersFromDynamicGroup	53	无法从动态组中删除用户。	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。

在 SSL 模式中配置 Identity Server

使用安全套接字层 (SSL) 和简单验证可以保密，并能够保证数据的完整性。

Identity Server 可以同时进行 SSL 和非 SSL 通信。这就意味着您不必在 SSL 通信和非 SSL 通信之间进行选择，而是可以同时使用它们。

以下各节说明了使用四种不同的 Web 容器在 SSL 模式中配置 Identity Server 的步骤：

使用安全 Sun ONE Web Server 配置 Identity Server

要使用 Sun ONE Web Server 在 SSL 模式中配置 Identity Server，请参见以下步骤：

1. 在 Identity Server 控制台中，单击顶层组织 （安装过程中创建）的属性箭头。

   数据框中将显示 “组织属性”窗口。

2. 单击 “保存”保存更改。

3. 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，删除 `http://` 协议，并添加 `https://` 协议。单击 “保存”。

注 请务必单击 “保存”。如果未保存，您将仍能够继续下面的步骤，但是所作的所有配置更改将会丢失，并且您将不能够以管理员身份登录来改正此错误。

步骤 4 至步骤 27 对 Sun ONE Web Server 进行了说明。

4. 登录到 Web Server 控制台。缺省端口为 58888。
5. 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”。
6. 单击屏幕右上角的 “应用”按钮。
7. 单击 “应用设置”。

   Web Server 应当会自动重新启动。单击 “确定”继续。
8. 停止选定的 Web Server 实例。
9. 单击 “安全”选项卡。
10. 单击 “创建数据库”。
11. 输入新数据库的密码并单击 “确定”。

    请务必将数据库密码记下来，以备将来使用。
12. 创建证书数据库后，单击 “请求证书”。
13. 在屏幕上的字段中输入数据。

    在 “密钥对字段密码”字段中输入您在步骤 11 中输入的密码。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 “通用名称”字段中，输入您的 Web Server 的主机名。
14. 提交表单后，您将看到如下消息：

```
--BEGIN CERTIFICATE REQUEST---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE REQUEST--
```

15. 复制并为证书请求提交该文本。

    确保您获取的是根 CA 证书。

16. 您将收到一个包含证书的证书响应，例如：

```
--BEGIN CERTIFICATE---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE---
```

17. 将这些文本复制到剪贴板或保存到文件中。
18. 转到 Web Server 控制台并单击 “安装证书”。
19. 单击该服务器的 “证书”。
20. 在 “密钥对文件密码”字段中，输入证书数据库的密码。
21. 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。
22. 单击 “安装证书”。
23. 单击 “信任的认证机构的证书”。
24. 按照步骤 18 至步骤 23 中所述的方法安装根 CA 证书。
25. 安装完这两种证书后，单击 Web Server 控制台中的 “首选项”选项卡。
26. 如果要在其它端口上启用 SSL，请选择 “添加侦听套接字”。然后，选择 “编辑侦听套接字”。
27. 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 28 至步骤 30 对 Identity Server 进行了说明。

28. 打开 `AMConfig.properties` 文件。缺省情况下，该文件位于 `/opt/SUNWam/lib` 中。
29. 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。

30. 保存 `AMConfig.properties` 文件。
31. 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。
32. 在文本字段输入证书数据库密码并选择 “启动”。

使用安全 Sun ONE Application Server 配置 Identity Server

将 Identity Server 设置为在启用 SSL 的 Sun ONE Application Server 上运行要通过两个步骤来完成。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

要使 Application Server 实例安全

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

   `http://fullservername:port`

   缺省端口为 4848。
2. 输入在安装过程中输入的用户名和密码。
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. 输入新数据库的密码并确认，然后单击 “确定”按钮。请确保记下数据库的密码，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，一些认证机构 (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 “可用的认证机构列表”。

       如果是向使用 Sun ONE 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. 输入密钥对文件的密码 （即您在步骤 9 中指定的密码）。

    d. 输入以下标识信息：

       通用名称。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。

       通用名称。要在其上安装数字证书的 Sun One 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。认证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。组织的部门或其它运作单位的名称。

       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。您的国家的两个字母的 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. 收到来自认证机构的数字证书后，您可以将文本复制到剪贴板或保存到文件中。
17. 转到 Sun ONE 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 “密钥对文件密码”字段中，输入证书数据库的密码。（该密码与您在步骤 9 中输入的密码相同。）
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 “信任的认证机构的证书”。
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 侦听程序”。
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 中指定的通用名称匹配。
31. 单击 “保存”。
32. 选择您要在其上安装 Sun ONE 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。

配置 Identity Server 处于 SSL 模式

要配置 Identity Server，使 WebLogic 处于 SSL 模式，请执行以下步骤：

1. 在 Identity Server 控制台中，单击顶层组织 （安装过程中创建）的属性箭头。数据框中将显示 “组织属性”窗口。
2. 单击 “保存”保存更改。
3. 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”。
4. 从以下缺省位置打开 `AMConfig.properties` 文件：

   `/opt/SUNWam/lib`。
5. 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。
6. 保存 `AMConfig.properties` 文件。
7. 重新启动 Application Server。

索引

符号

英文

A

B

C

D

F

G

H

J

K

L

M

N

P

Q

R

S

T

W

X

Y

Z

Z