Sun Java System Access Manager 7 2005Q4 管理指南

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

文件号码 819–3482

060420@14774

目录

前言

《Sun Java System Access Manager 7 2005Q4 管理指南》说明如何使用 Sun Java™ System Access Manager 控制台以及如何通过命令行界面管理用户和服务数据。

Access Manager 是软件组件集合即 Sun Java Enterprise System (Java ES) 的一个组件，这些组件提供用于支持分布在网络或 Internet 环境中的企业应用程序所需的服务。

目标读者

本书的目标读者为使用 Sun Java System 服务器和软件实现 Web 访问平台的 IT 管理员和软件开发人员。

阅读本书之前

读者应该熟悉下列组件和概念：

- 《Sun Java System Access Manager 7 2005Q4 Technical Overview》中描述的 Access Manager 技术概念
- 部署平台：Solaris™ 或 Linux 操作系统
- 运行 Access Manager 的 Web 容器：Sun Java System Application Server、Sun Java System Web Server、BEA WebLogic 或 IBM WebSphere Application Server
- 技术概念：轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP)、Java 技术、JavaServer Pages (JSP) 技术、超文本传输协议 (HyperText Transfer Protocol, HTTP)、超文本标记语言 (HyperText Markup Language, HTML) 和可扩展标记语言 (eXtensible Markup Language, XML)

相关文档

可在如下位置获得相关文档：

- 第 14 页中的 “Access Manager 核心文档”
- 第 14 页中的 “Sun Java Enterprise System 产品文档”

Access Manager 核心文档

Access Manager 核心文档集包含以下文档：

- 产品发布以后，可获得联机的《Sun Java System Access Manager 7 2005Q4 发行说明》。该文档中收集了各种最新的信息，包括当前发行版的新功能说明、已知问题和限制、安装说明，以及报告有关软件或文档的问题的方法。
- 《Sun Java System Access Manager 7 2005Q4 Technical Overview》简单论述了 Access Manager 组件如何协同工作以完成访问控制功能，并保护企业信息和基于 Web 的应用程序。同时也解释了 Access Manager 的基本概念和术语。
- 《Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide》基于解决方案生命周期，为 Sun Java System Access Manager 提供计划和部署解决方案。
- 《Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide》提供关于如何微调 Access Manager 及其相关组件以获取最佳性能的信息。
- 《Sun Java System Access Manager 7 2005Q4 管理指南》描述如何使用 Access Manager 控制台以及如何通过命令行界面管理用户和服务数据。
- 《Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide》提供有关基于“Liberty 联盟计划”规范的“联合”模块的信息。其中包括有关基于这些规范的集成服务的信息、启用基于 Liberty 的环境的说明，并简单介绍了扩展框架的应用程序接口 (API)。
- 《Sun Java System Access Manager 7 2005Q4 Developer’s Guide》讲述如何自定义 Access Manager 以及把它的功能集成到组织当前的技术架构中。本指南还包含关于本产品及其 API 的程序方面的详细信息。
- 《Sun Java System Access Manager 7 2005Q4 C API Reference》概述了组成公共 Access Manager C API 的数据类型、结构和功能。
- Java API Reference（文件号码 819-2141）讲述有关在 Access Manager 中实现 Java 软件包的信息。
- 《Sun Java System Access Manager Policy Agent 2.2 User’s Guide》简单论述了策略功能和适用于 Access Manager 的策略代理。

在 Sun Java Enterprise System 文档站点的 Access Manager 页面中有发行说明的更新以及指向核心文档更正的链接。已更新的文档将会标记上修订日期。

Sun Java Enterprise System 产品文档

可在该文档中获得有关下列产品的有用信息：

- Directory Server
- Web Server
- Application Server
- Web Proxy Server

相关的第三方 Web 站点引用

本文档中引用了第三方 URL，其中提供附加的相关信息。

注 – Sun 对本文档中提到的第三方 Web 站点的可用性不承担任何责任。对于此类站点或资源中的（或通过它们获得的）任何内容、广告、产品或其他材料，Sun 并不表示认可，也不承担任何责任。对于因使用或依靠此类站点或资源中的（或通过它们获得的）任何内容、产品或服务而造成的或连带产生的实际或名义损坏或损失，Sun 概不负责，也不承担任何责任。

文档、支持和培训

Sun 功能	URL	说明
文档	http://www.sun.com/documentation/	下载 PDF 及 HTML 格式的文档，购买印刷文档
支持和培训	http://www.sun.com/supportraining/	获取技术支持、下载修补程序以及学习 Sun 提供的课程

印刷约定

下表介绍了本手册的印刷约定。

表 P–1 印刷约定

字体或符号	含义	示例
`AaBbCc123`	命令、文件和目录的名称；计算机屏幕输出	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `machine_name% you have mail.`
`AaBbCc123`	用户键入的内容，与计算机屏幕输出的显示不同	`machine_name%` **`su`** `Password:`
`aabbcc123`	要使用实名或值替换的命令行占位符	要删除文件，请键入 `rm` *filename*。

表 P–1 印刷约定 （续）

字体或符号	含义	示例
AaBbCc123	书名、新术语以及要强调的术语	阅读《用户指南》的第 6 章。 执行修补程序分析。 请勿保存文件。 [请注意：一些强调的项目以粗体字显示。]

命令中的 shell 提示符示例

下表列出了 C shell、Bourne shell 和 Korn shell 的默认系统提示符和超级用户提示符。

表 P–2 Shell 提示符

Shell	提示符
C shell 提示符	`machine_name%`
C shell 超级用户提示符	`machine_name#`
Bourne shell 和 Korn shell 提示符	`$`
Bourne shell 和 Korn shell 超级用户提示符	`#`

Sun 欢迎您提出宝贵意见

Sun 致力于提高其文档质量，并十分乐意收到您的意见和建议。

如果您要提出意见，请转到 `http://docs.sun.com`，然后单击“发送意见”(Send Comments)。请在联机表单中提供文档标题和文件号码。文件号码通常包含七位或九位数字，您可以在本书的标题页或文档最上部找到文件号码。

例如，本书的标题为《Sun Java System Access Manager 7 2005Q4 管理指南》，文件号码为 819-3482。提出意见时您还需要在表格中输入文件的英文文件号码和标题。本文件的英文文件号码是 819-2137-11，文件标题为《Sun Java System Access Manager 7 2005Q4 Administration Guide》。

第 I 部分

Access Manager 配置

这是《Sun Java System Access Manager™ 7 2005Q4 管理指南》的第一部分。本部分讨论安装 Access Manager 之后可以执行的配置选项。本部分包含以下各章：

◆ ◆ ◆ 第 1 章

Access Manager 7 2005Q4 配置脚本

本章介绍如何使用 `amconfig` 脚本和范例无提示模式输入文件 (`amsamplesilent`) 配置和部署 Sun Java™ System Access Manager。包括以下主题：

Access Manager 7 2005Q4 安装概述

对于新的安装，应始终运行 Sun Java Enterprise System (Java ES) 安装程序来安装 Access Manager 7 2005Q4 的第一个实例。当运行安装程序时，可以选择 Access Manager 的以下两个选项之一：

- “立即配置”选项允许在安装期间利用您在 Access Manager 安装面板上选择的选项（或默认值）安装和配置第一个实例。
- “以后再配置”选项可安装 Access Manager 7 2005Q4 组件，安装后，必须手动配置这些组件或运行 Access Manager 脚本（如第 33 页中的 “配置和重新配置 Access Manager 的实例”所述）。如果选择此选项，则不配置当前安装的任何产品。例如，如果选择安装 Access Manager 和 Application Server，并选择“以后再配置”选项，则将不配置这两个应用程序。

注 – 如果作为 Access Manager Web 容器安装 BEA WebLogic 或 IBM WebSphere Application Server，则在安装 Access Manager 时必须选择“以后再配置”选项。有关详细信息，请参阅第 2 章。

有关安装程序的信息，请参阅《Sun Java Enterprise System 2005Q4 Installation Guide for UNIX》。

Java Enterprise System 安装程序将 Access Manager 7 2005Q4 amconfig 脚本和范例无提示模式输入文件 (amsamplesilent) 安装在 Solaris 系统的 *AccessManager-base*/SUNWam/bin 目录中或 Linux 系统的 *AccessManager-base*/identity/bin 目录中。

AccessManager-base 代表 Access Manager 的基本安装目录。在 Solaris 系统中，默认的基本安装目录为 /opt， 在 Linux 系统中，默认基本安装目录为 /opt/sun。不过，如果愿意，您可以在运行安装程序时指定其他目录。

amconfig 脚本为顶级脚本，可根据需要调用其他脚本执行所请求的操作。有关详细信息，请参阅第 30 页中的 “Access Manager amconfig 脚本”。

此范例配置脚本输入文件 (amsamplesilent) 是一个模板，您可以使用该模板来创建在无提示模式下运行 amconfig 脚本时必须指定的输入文件。

此范例配置脚本输入文件是包含 Access Manager 配置变量的 ASCII 文本文件。运行 amconfig 脚本之前，先复制（如果需要，可重命名）amsamplesilent 文件，然后根据系统环境编辑文件中的变量。配置变量采用以下格式：

```
variable-name=value
```

例如：

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

有关可以在配置脚本输入文件中设置的变量列表，请参阅第 21 页中的 “Access Manager 范例配置脚本输入文件”。

注意 – 在无提示模式下运行 amconfig 脚本时，所使用的范例配置脚本输入文件的格式不遵循与 Java Enterprise System 无提示安装状态文件相同的格式，或没有必要使用与其相同的变量名。此文件包含敏感数据，如管理员密码。确保保护好此文件或适时地将其删除。

Access Manager amconfig 脚本操作

通过 Sun Java Enterprise System 安装程序安装 Access Manager 的第一个实例后，可以运行 amconfig 脚本来执行以下操作，具体取决于无提示模式输入文件中的变量值：

- 部署和配置 Access manager 的第一个实例或在同一个主机系统上部署和配置 Access Manager 的附加实例。例如，在配置 Web 容器的附加实例之后，即可为该 Web 容器实例部署和配置新的 Access Manager 实例。
- 重新配置 Access Manager 的第一个实例和任何附加实例。
- 部署和配置 Access Manager 完整的服务器服务或仅部署和配置 SDK 服务，将启用对以下产品的支持：
  - BEAWebLogic

- IBM WebSphere Application Server

  部署和配置特定 Access Manager 组件，如控制台或“联合管理”模块。
- 卸载使用 `amconfig` 脚本部署的 Access Manager 的实例和组件。

Access Manager 范例配置脚本输入文件

在运行 Java Enterprise System 安装程序后，Access Manager 范例配置脚本输入文件 (`amsamplesilent`) 在 Solaris 系统的 *AccessManager-base*`/SUNWam/bin` 目录中或在 Linux 系统的 *AccessManager-base*`/identity/bin` 目录中可用。

要设置配置变量，请首先复制并重命名 `amsamplesilent` 文件。然后为要执行的操作设置副本中的变量。有关此文件的示例，参见第 35 页中的 “示例配置脚本输入文件” 。

此范例无提示模式输入文件包含以下配置变量：

- 第 21 页中的 “部署模式变量”
- 第 22 页中的 “Access Manager 配置变量”
- 第 25 页中的 “Web 容器配置变量”
- 第 29 页中的 “Directory Server 配置变量”

部署模式变量

本节介绍 DEPLOY_LEVEL 变量的值，这是必需的变量。此变量确定需要 `amconfig` 脚本执行的操作。

表 1–1 Access Manager DEPLOY_LEVEL 变量

操作	DEPLOY_LEVEL 变量值和说明
安装	1 = 为新实例安装完整的 Access Manager（默认值） 2 = 仅安装 Access Manager 控制台 3 = 仅安装 Access Manager SDK 4 = 仅安装 SDK 并配置容器 5 = 仅安装“联合管理”模块 6 = 仅安装服务器 7= 安装 Access Manager 并配置容器以使用 Portal Server 部署。 注意： DEPLOY_MODE=7 仅适用于使用 Portal Server 部署 Access Manager。 对于某些部署，您可能想使用不同的 Web 容器在单个主机服务器上仅安装控制台或仅安装服务器。首先，运行 Java ES 安装程序以通过“以后再配置”选项来安装所有 Access Manager 子组件。然后，运行 `amconfig` 脚本来配置控制台和服务器实例。
卸载（取消配置）	11 = 完全卸载 12 = 仅卸载控制台 13 = 仅卸载 SDK 14 = 仅卸载 SDK 并取消容器配置 15 = 卸载“联合管理”模块 16 = 仅卸载服务器 使用 Portal Server 部署时，卸载 Access Manager 并取消配置容器。 注意： DEPLOY_MODE=7 仅在使用 Portal Server 部署 Access Manager 时使用。
重新安装 （也称为重新部署或重新配置）	21 = 重新部署所有（控制台、密码、服务和通用属性）Web 应用程序。 26 = 取消部署所有（控制台、密码、服务和通用属性） Web 应用程序。

Access Manager 配置变量

本节介绍 Access Manager 配置变量。

表 1–2 Access Manager 配置变量

变量	说明
AM_REALM	表示 Access Manager 模式： ■ 已启用：具有 Access Manager 7 2005Q4 功能和控制台的 Access Manager 在“领域”模式下运行。 ■ 已禁用：具有 Access Manager 6 2005Q1 功能和控制台的 Access Manager 在“传统”模式下运行。 默认值：已启用 **注意 –** 默认情况下启用 Access Manager 领域模式。如果使用 Portal Server、Messaging Server、Calendar Server、Delegated Administrator 或 Instant Messaging 部署 Access Manager，则必须在运行 `amconfig` 脚本之前选择“传统”模式（AM_REALM=已禁用）。
BASEDIR	Access Manager 软件包的基本安装目录。 默认值：PLATFORM_DEFAULT 对于 Solaris 系统，PLATFORM_DEFAULT 为 `/opt` 对于 Linux 系统，PLATFORM_DEFAULT 为 `/opt/sun`
SERVER_HOST	Access Manager 在其中运行（或将要安装）的系统的全限定主机名。 对于远程 SDK 安装，将此变量设置为安装（或将要安装）Access Manager 的主机，而不是远程客户机主机。 此变量应与 Web 容器配置中对应的变量相匹配。例如，对于 Application Server 8，此变量应与 AS81_HOST 相匹配。
SERVER_PORT	Access Manager 端口号。默认值：58080 对于远程 SDK 安装，将此变量设置为安装（或将要安装）Access Manager 的主机而不是远程客户机主机上的端口。 此变量应与 Web 容器配置中对应的变量相匹配。例如，对于 Application Server 8，此变量应与 AS81_PORT 相匹配。
SERVER_PROTOCOL	服务器协议：http 或 https。默认值：http 对于远程 SDK 安装，将此变量设置为安装（或将要安装）Access Manager 的主机而不是远程客户机主机上的协议。 此变量应与 Web 容器配置中对应的变量相匹配。例如，对于 Application Server 8，此变量应与 AS81_PROTOCOL 相匹配。
CONSOLE_HOST	安装控制台的服务器的全限定主机名。 默认值：为 Access Manager 主机提供的值
CONSOLE_PORT	控制台安装以及侦听连接所在 Web 容器的端口。 默认值：为 Access Manager 端口提供的值

表 1–2 Access Manager 配置变量 （续）

变量	说明
CONSOLE_PROTOCOL	控制台安装所在 Web 容器的协议。 默认值：服务器协议
CONSOLE_REMOTE	如果控制台远离 Access Manager 服务，则将其设置为 true。否则，设置为 false。默认值：false
DS_HOST	Directory Server 的全限定主机名。
DS_PORT	Directory Server 端口。默认值：389。
DS_DIRMGRDN	目录管理员 DN：可以无限制地访问 Directory Server 的用户。 默认值：`"cn=Directory Manager"`
DS_DIRMGRPASSWD	目录管理员的密码 请参阅第 22 页中的 “Access Manager 配置变量”的说明中有关特殊字符的注释。
ROOT_SUFFIX	目录的开首或根后缀。必须确保此值在所使用的 Directory Server 中存在。 请参阅第 22 页中的 “Access Manager 配置变量”的说明中有关特殊字符的注释。
ADMINPASSWD	管理员的密码 (`amadmin`)。必须与 `amldapuser` 的密码不同。 注意：如果密码包含特殊字符，如斜线 (/) 或反斜线 (\\)，则必须用单引号 (”) 将特殊字符引起来。例如： `ADMINPASSWD='\\\\\\\\\\\####///'` 但是，密码中不能包含单引号。
AMLDAPUSERPASSWD	`amldapuser` 的密码。必须与 `amadmin` 的密码不同。 请参阅第 22 页中的 “Access Manager 配置变量”的说明中有关特殊字符的注释。
CONSOLE_DEPLOY_URI	URI 前缀，用于访问与 Access Manager 管理控制台子组件相关联的 HTML 页面、类和 JAR 文件。 默认值：`/amconsole`
SERVER_DEPLOY_URI	URI 前缀，用于访问与身份管理和策略服务核心子组件相关联的 HTML 页面、类和 JAR 文件。 默认值：`/amserver`
PASSWORD_DEPLOY_URI	URI，用于确定运行 Access Manager 的 Web 容器要在您指定的字符串和对应的已部署应用程序之间使用的映射。 默认值：`/ampassword`

表 1–2 Access Manager 配置变量 （续）

变量	说明
COMMON_DEPLOY_URI	用于访问 Web 容器中公共域服务的 URI 前缀。 默认值：/amcommon
COOKIE_DOMAIN	Access Manager 在向用户授予会话 ID 时返回到浏览器的可信赖 DNS 域的名称。至少应有一个值。一般而言，采用的格式是在服务器域名前加上一个英文句点。 示例：.example.com
JAVA_HOME	JDK 安装目录的路径。默认值：/usr/jdk/entsys-j2se。此变量提供命令行界面（如 amadmin）的可执行文件使用的 JDK。版本必须为 1.4.2 或更高版本。
AM_ENC_PWD	密码加密密钥：Access Manager 用来加密用户密码的字符串。默认值：无。当此值被设置为 none 时，amconfig 将为用户生成密码加密密钥，因此将存在由用户指定或通过 amconfig 创建的用于安装的密码加密。 重要提示：如果部署 Access Manager 的多个实例或远程 SDK，则所有的实例必须使用相同的密码加密密钥。部署附加实例时，为第一个实例从 AMConfig.properties 文件中的 am.encryption.pwd **属性**复制值。
PLATFORM_LOCALE	平台的语言环境。默认值：en_US（美国英语）
NEW_OWNER	安装后 Access Manager 文件的新拥有者。默认值：root
NEW_GROUP	安装后 Access Manager 文件的新组。默认值：other 对于 Linux 安装，将 NEW_GROUP 设置为 root。
PAM_SERVICE_NAME	PAM 配置中 PAM 服务的名称或操作系统附带的并用于 Unix 验证模块的堆栈（通常，对于 Solaris 是 other，对于 Linux 是 password）。默认值：other。
XML_ENCODING	XML 编码。默认值：ISO-8859-1
NEW_INSTANCE	指定配置脚本是否应将 Access Manager 部署到新的用户创建的 Web 容器实例中： ■ true = 将 Access Manager 部署到新的用户创建的已存在实例以外的 Web 容器实例中。 ■ false = 配置第一个实例或重新配置实例。 默认值：false
SSL_PASSWORD	在此版本中不使用。

Web 容器配置变量

要指定 Access Manager 的 Web 容器，请设置无提示模式输入文件中的 WEB_CONTAINER 变量。有关 Access Manager 7 2005Q4 支持的 Web 容器的版本，请参阅《Sun Java System Access Manager 7 2005Q4 发行说明》。

表 1–3 Access Manager WEB_CONTAINER 变量

值	Web 容器
WS6（默认值）	第 26 页中的 “Sun Java System Web Server 6.1 SP5”
AS8	第 27 页中的 “Sun Java System Application Server 8.1”
WL8	第 28 页中的 “BEA WebLogic Server 8.1”
WAS5	第 29 页中的 “IBM WebSphere 5.1”

Sun Java System Web Server 6.1 SP5

本节介绍无提示模式输入文件中 Web Server 6.1 2005Q4 SP5 的配置变量 。

表 1–4 Web Server 6.1 配置变量

变量	说明
WS61_INSTANCE	将要在其中部署或取消部署 Access Manager 的 Web Server 实例的名称。 默认值： https-*web-server-instance-name* 其中， *web-server-instance-name* 为此 Access Manager 的主机 （第 22 页中的 “Access Manager 配置变量” 变量）
WS61_HOME	Web Server 基本安装目录。 默认值： `/opt/SUNWwbsvr`
WS61_PROTOCOL	将要在其中部署 Access Manager 的第 26 页中的 “Sun Java System Web Server 6.1 SP5” 变量设置的 Web Server 实例使用的协议： http 或 https。 默认值： Access Manager 协议（第 22 页中的 “Access Manager 配置变量” 变量）
WS61_HOST	Web Server 实例的全限定主机名（第 26 页中的 “Sun Java System Web Server 6.1 SP5” 变量）。 默认值： Access Manager 主机实例（第 22 页中的 “Access Manager 配置变量” 变量）
WS61_PORT	Web Server 侦听连接时所用的端口。 默认值： Access Manager 端口号（第 22 页中的 “Access Manager 配置变量” 变量）
WS61_ADMINPORT	“Web Server 管理服务器”侦听连接时所用的端口。 默认值： 8888
WS61_ADMIN	Web Server 管理员的用户 ID。 默认值： `"admin"`

Sun Java System Application Server 8.1

本节介绍无提示模式输入文件中 Application Server 8.1 的配置变量 。

表 1–5 Application Server 8.1 配置变量

变量	说明
AS81_HOME	Application Server 8.1 安装的目录的路径。 默认值：`/opt/SUNWappserver/appserver`
AS81_PROTOCOL	Application Server 实例使用的协议：http 或 https。 默认值：Access Manager 协议（第 22 页中的 “Access Manager 配置变量” 变量）
AS81_HOST	Application Server 实例侦听连接时所用的全限定域名 (FQDN)。 默认值：Access Manager 主机（第 22 页中的 “Access Manager 配置变量” 变量）
AS81_PORT	Application Server 实例侦听连接时所用的端口。 默认值：Access Manager 端口号（第 22 页中的 “Access Manager 配置变量” 变量）
AS81_ADMINPORT	Application Server 管理服务器侦听连接时所用的端口。 默认值：4849
AS81_ADMIN	Application Server 当前在其中显示的域的 Application Server 管理服务器管理员的用户名。 默认值：`admin`
AS81_ADMINPASSWD	Application Server 当前在其中显示的域的 Application Server 管理员的密码。 请参阅第 22 页中的 “Access Manager 配置变量”的说明中有关特殊字符的注释。
AS81_INSTANCE	将运行 Access Manager 的 Application Server 实例的名称。 默认值：`server`
AS81_DOMAIN	要在其中部署此 Access Manager 实例的域的 Application Server 目录的路径。 默认值：`domain1`
AS81_INSTANCE_DIR	Application Server 存储实例文件的目录的路径。 默认值：`/var/opt/SUNWappserver/domains/domain1`

表 1–5 Application Server 8.1 配置变量 （续）

变量	说明
AS81_DOCS_DIR	Application Server 用来存储内容文档的目录。 默认值：`/var/opt/SUNWappserver/domains/domain1/docroot`
AS81_ADMIN_IS_SECURE	指定 Application Server 管理实例是否正在使用 SSL： ■ true：启用安全端口（HTTPS 协议）。 ■ false：不启用安全端口（HTTP 协议）。 默认值：true（已启用） `ampsamplesilent` 中的附加设置指定了应用服务器管理端口是否安全： ■ true：应用服务器管理端口安全（HTTPS 协议）。 ■ false：应用服务器管理端口不安全（HTTP 协议）。 默认值：True（已启用）。

BEA WebLogic Server 8.1

本节介绍无提示模式输入文件中 BEA WebLogic Server 8.1 的配置变量。

表 1–6 BEA WebLogic Server 8.1 配置变量

变量	说明
WL8_HOME	WebLogic 起始目录。默认值：`/usr/local/bea`
WL8_PROJECT_DIR	WebLogic 项目目录。默认值：`user_projects`
WL8_DOMAIN	WebLogic 域名。默认值：`mydomain`
WL8_SERVER	WebLogic 服务器名。默认值：`myserver`
WL8_INSTANCE	WebLogic 实例名。默认值：`/usr/local/bea/weblogic81 ($WL8_HOME/weblogic81)`
WL8_PROTOCOL	WebLogic 协议。默认值：http
WL8_HOST	WebLogic 主机名。默认值：服务器主机名
WL8_PORT	WebLogic 端口。默认值：7001
WL8_SSLPORT	WebLogic SSL 端口。默认值：7002
WL8_ADMIN	WebLogic 管理员。默认值：`"weblogic"`
WL8_PASSWORD	WebLogic 管理员密码。 请参阅第 22 页中的 “Access Manager 配置变量”的说明中有关特殊字符的注释。
WL8_JDK_HOME	WebLogic JDK 起始目录。默认值：第 28 页中的 “BEA WebLogic Server 8.1” `/jdk142_04`

表 1–6 BEA WebLogic Server 8.1 配置变量 （续）

变量	说明
WL8_CONFIG_LOCATION	应设置为 WebLogic 启动脚本所在位置的父目录。

IBM WebSphere 5.1

本节介绍无提示模式输入文件中 IBM WebSphere Server 5.1 的配置变量。

表 1–7 IBM WebSphere 5.1 配置变量

变量	说明
WAS51_HOME	WebSphere 起始目录。默认值：`/opt/WebSphere/AppServer`
WAS51_JDK_HOME	WebSphere JDK 起始目录。默认值：`/opt/WebSphere/AppServer/java`
WAS51_CELL	WebSphere 单元。默认值：hostname 值
WAS51_NODE	WebSphere 节点名。默认值：WebSphere 安装服务器的主机名。默认值：hostname 值
WAS51_INSTANCE	WebSphere 实例名。默认值：`server1`
WAS51_PROTOCOL	WebSphere 协议。默认值：http
WAS51_HOST	WebSphere 主机名。默认值：服务器主机名
WAS51_PORT	WebSphere 端口。默认值：9080
WAS51_SSLPORT	WebSphere SSL 端口。默认值：9081
WAS51_ADMIN	WebSphere 管理员。默认值：`"admin"`
WAS51_ADMINPORT	WebSphere 管理员端口。默认值：9090

Directory Server 配置变量

有关 Access Manager 7 2005Q4 支持的 Directory Server 的版本，请参阅《Sun Java System Access Manager 7 2005Q4 发行说明》。本节介绍无提示模式输入文件中的 Directory Server 配置变量。

表 1–8 Directory Server 配置变量

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

Access Manager amconfig 脚本

在运行 Java Enterprise System 安装程序后，`amconfig` 脚本在 Solaris 系统的 *AccessManager-base*`/SUNWam/bin` 目录中或在 Linux 系统的 *AccessManager-base*`/identity/bin` 目录中可用。

`amconfig` 脚本读取无提示配置输入文件，然后根据需要在无提示模式下调用其他脚本，以执行请求的操作。

要运行 `amconfig` 脚本，请使用以下语法：

```
amconfig -s
          input-file
```

其中：

-s 在无提示模式下运行 `amconfig`。

`input-file` 为包含要执行的操作的配置变量的无提示配置输入文件。有关详细信息，请参阅第 21 页中的 “Access Manager 范例配置脚本输入文件”。

运行 `amconfig` 脚本的几个注意事项：

- 必须以超级用户 (`root`) 身份运行。
- 指定 `amsamplesilent` 文件（或该文件的副本）的完整路径。例如：

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

或

```
# ./amconfig -s /opt/SUNWam/bin/amsamplesilent
```

注 – 在 Access Manager 7 2005Q4 版本中，不支持以下脚本：

- 带有创建参数的 `amserver`
- `amserver.`*instance*

同样，默认情况下 `amserver` **启动**仅启动验证 `amsecuridd` 和 `amunixd` 帮助器。`amsecuridd` 帮助器仅在 Solaris OS SPARC 平台上可用。

Access Manager 部署方案

使用 Java Enterprise System 安装程序安装 Access Manager 的第一个实例后，可以通过编辑无提示配置输入文件中的配置变量，然后运行 `amconfig` 脚本来部署和配置附加 Access Manager 实例。

本节介绍以下方案：

- 第 32 页中的 “部署 Access Manager 的附加实例”
- 第 33 页中的 “配置和重新配置 Access Manager 的实例”
- 第 34 页中的 “卸载 Access Manager”
- 第 35 页中的 “卸载所有的 Access Manager 实例”

部署 Access Manager 的附加实例

在部署新的 Access Manager 实例之前，必须先使用 Web 容器的管理工具创建并启动新的 Web 容器实例。有关信息，请参阅特定 Web 容器文档：

- 有关 Web Server，请参阅 http://docs.sun.com/coll/1308.1
- 有关 Application Server，请参阅 http://docs.sun.com/coll/1310.1

本节介绍的步骤仅应用于使用“立即配置”选项安装的 Access Manager 实例。如果您计划将 WebLogic 或 WebSphere 用作 Web 容器，则必须在安装 Access Manager 时使用“以后再配置”选项。有关详细信息，请参阅第 2 章。

部署附加的 Access Manager 实例

本节介绍如何在不同的主机服务器上部署附加的 Access Manager 实例以及更新“平台服务器列表”。

▼ 部署附加的 Access Manager 实例

1 **以管理员身份登录，具体取决于实例的 Web 容器。例如，如果新实例的 Web 容器将是 Web Server 6.1，则以超级用户 (root) 身份或以“Web Server 管理服务器”的用户帐户登录均可。**

2 **将 amsamplesilent 文件复制到可写的目录，并将此目录作为当前目录。例如，可以创建名为 /newinstances 的目录。**

提示：重命名 amsamplesilent 文件的副本以描述要部署的新实例。例如，以下步骤使用名为 amnewws6instance 的输入文件为 Web Server 6.1 安装新实例。

3 **在新的 amnewws6instance 文件中设置以下变量：**

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

根据所要创建的新实例的需要设置 amnewws6instance 文件中的其他变量。有关这些变量的描述，请参阅以下各节中的表格：

- 第 22 页中的 “Access Manager 配置变量”
  - 第 25 页中的 “Web 容器配置变量”
  - 第 29 页中的 “Directory Server 配置变量”

    重要提示：所有 Access Manager 实例的密码加密密钥的值必须相同。要为此实例设置 AM_ENC_PWD 变量，应复制第一个实例的 AMConfig.properties 文件中的 am.encryption.pwd 属性值。

    为防以后卸载此实例，请保存 amnewws6instance 文件。

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

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./newinstances/amnewws6instance
```

-s 选项在无提示模式下运行 amconfig 脚本。

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

▼ 更新“平台服务器列表”

创建附加容器实例时，必须更新“Access Manager 平台服务器列表”以反映容器的附加内容。

1. **以顶级管理员身份登录到 Access Manager 控制台。**
2. **单击“服务配置”选项卡。**
3. **单击“平台”服务。**
4. **为“服务器列表”中的新实例输入以下信息：**

   protocol://*fqdn*:*port*|*instance-number*

   实例编号应为下一个尚未使用的可用编号。
5. **单击“添加”。**
6. **单击“保存”。**

配置和重新配置 Access Manager 的实例

通过运行 amconfig 脚本，可以配置使用 Java Enterprise System 安装程序中的“以后再配置”选项安装的某个 Access Manager 实例，或者重新配置使用“立即配置”选项安装的第一个实例。

例如，可能要重新配置实例以更改 Access Manager 拥有者和组。

▼ 配置或重新配置 Access Manager 的实例

1. **以管理员身份登录，具体取决于实例的 Web 容器。例如，如果 Web 容器为 Web Server 6.1，则以超级用户 (root) 身份或以“Web Server 管理服务器”的用户帐户登录均可。**
2. **将用来部署实例的无提示配置输入文件复制到可写的目录，并将此目录作为当前目录。例如，要重新配置 Web Server 6.1 的实例，以下步骤使用 /reconfig 目录中的名为 amnewinstanceforWS61 的输入文件。**
3. **在 amnewinstanceforWS61 文件中，将 DEPLOY_LEVEL 变量设置为描述第 21 页中的“部署模式变量”操作的值中的一个值。例如，设置 DEPLOY_LEVEL=21 可对完全安装进行重新配置。**
4. **在 amnewinstanceforWS61 文件中，将 NEW_INSTANCE 变量设置为 false：**

   ```
   NEW_INSTANCE=false
   ```

5 **设置 amnewinstanceforWS61 文件中的其他变量以重新配置实例。例如，要更改实例的所有者和组，请将 NEW_OWNER 和 NEW_GROUP 变量设置为各自的新值。**

有关其他变量的描述，请参阅以下各节中的表格：

- 第 22 页中的 “Access Manager 配置变量”
  - 第 25 页中的 “Web 容器配置变量”
  - 第 29 页中的 “Directory Server 配置变量”

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

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./reconfig/amnewinstanceforWS61
```

-s 选项在无提示模式下运行此脚本。amconfig 脚本根据需要调用其他配置脚本，使用 amnewinstanceforWS61 文件中的变量重新配置实例。

卸载 Access Manager

通过运行 amconfig 脚本，可以卸载以前安装的 Access Manager 实例。也可以临时取消配置 Access Manager 的实例，除非删除 Web 容器实例，否则它仍可用于以后重新部署其他的 Access Manager 实例。

▼ 卸载 Access Manager 的实例

1 **以管理员身份登录，具体取决于实例的 Web 容器。例如，如果 Web 容器为 Web Server 6.1，则以超级用户 (root) 身份或以“Web Server 管理服务器”的用户帐户登录均可。**

2 **将用来部署实例的无提示配置输入文件复制到可写的目录，并将此目录作为当前目录。例如，要取消配置 Web Server 6.1 的实例，以下步骤将使用 /unconfigure 目录中的名为 amnewinstanceforWS61 的输入文件。**

3 **在 amnewinstanceforWS61 文件中，将 DEPLOY_LEVEL 变量设置为描述第 21 页中的 “部署模式变量”操作的值中的一个值。例如，设置 DEPLOY_LEVEL=11 可对完全安装进行卸载（或取消配置）。**

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

```
# cd opt/SUNWam/bin/
 # ./amconfig -s ./unconfigure/aminstanceforWS61
```

-s 选项在无提示模式下运行此脚本。amconfig 脚本读取 amnewinstanceforWS61 文件，然后卸载此实例。

如果您以后想要使用 Web 容器实例来重新部署其他 Access Manager 实例，该 Web 容器实例将仍然可用。

卸载所有的 Access Manager 实例

此方案会彻底删除系统中的 Access Manager 7 2005Q4 实例和软件包。

▼ 彻底删除系统中的 Access Manager 7 2005Q4

1. **以超级用户 (root) 身份登录或成为超级用户。**

2. **在用来部署此实例的输入文件中，将 DEPLOY_LEVEL 变量设置为描述第 21 页中的“部署模式变量”操作的值中的一个值。例如，设置 DEPLOY_LEVEL=11 可对完全安装进行卸载（或取消配置）。**

3. **使用在第 35 页中的“卸载所有的 Access Manager 实例”中编辑的文件运行 `amconfig` 脚本。例如，在 Solaris 系统中：**

   ```
   # cd opt/SUNWam/bin/
   # ./amconfig -s ./newinstances/amnewws6instance
   ```

   以无提示模式运行 `amconfig` 脚本来卸载实例。

   为要卸载的任何其他 Access Manager 实例重复这些步骤，使用 Java Enterprise System 安装程序安装的第一个实例除外。

4. **要从系统中卸载第一个实例和删除所有的 Access Manager 软件包，请运行 Java Enterprise System 卸载程序。有关卸载程序的信息，请参阅《Sun Java Enterprise System 2005Q4 Installation Guide for UNIX》。**

示例配置脚本输入文件

下面一节包含使用 WebLogic 8.1 部署的 Access Manager 配置脚本输入文件的示例。

```
DEPLOY_LEVEL=1
BASEDIR=/opt
SERVER_HOST=ide-56.example.company.com
SERVER_PORT=7001
SERVER_PROTOCOL=http
CONSOLE_HOST=$SERVER_HOST
CONSOLE_PORT=$SERVER_PORT
CONSOLE_PROTOCOL=$SERVER_PROTOCOL
CONSOLE_REMOTE=false
DS_HOST=ide-56.example.company.com
DS_PORT=389
DS_DIRMGRDN=”cn=Directory Manager”
DS_DIRMGRPASSWD=11111111
ROOT_SUFFIX=”dc=company,dc=com”
ADMINPASSWD=11111111
```

```
AMLDAPUSERPASSWD=00000000
CONSOLE_DEPLOY_URI=/amconsole
SERVER_DEPLOY_URI=/amserver
PASSWORD_DEPLOY_URI=/ampassword
COMMON_DEPLOY_URI=/amcommon
COOKIE_DOMAIN=.iplanet.com
JAVA_HOME=/usr/jdk/entsys-j2se
AM_ENC_PWD=””
PLATFORM_LOCALE=en_US
NEW_OWNER=root
NEW_GROUP=other
XML_ENCODING=ISO-8859-1
NEW_INSTANCE=false
WEB_CONTAINER=WL8
WL8_HOME=/export/bea8
WL8_PROJECT_DIR=user_projects
WL8_DOMAIN=mydomain
WL8_CONFIG_LOCATION=$WL8_HOME/$WL8_PROJECT_DIR/domains
WL8_SERVER=myserver
WL8_INSTANCE=/export/bea8/weblogic81
WL8_PROTOCOL=http
WL8_HOST=ide-56.example.company.com
WL8_PORT=7001
WL8_SSLPORT=7002
WL8_ADMIN=”weblogic”
WL8_PASSWORD=”11111111”
WL8_JDK_HOME=$WL8_HOME/jdk142_04
DIRECTORY_MODE=1
USER_NAMING_ATTR=uid
ORG_NAMING_ATTR=o
ORG_OBJECT_CLASS=examplemanagedorganization
USER_OBJECT_CLASS=inetorgperson
DEFAULT_ORGANIZATION=
Sample Configuration Script Input File for WebLogic 8.1.x
```

◆ ◆ ◆ 第 2 章

2 安装和配置第三方 Web 容器

本章介绍安装和配置用 Sun Java™ System Access Manager 部署的第三方 Web 容器的步骤。对于此版本，Access Manager 支持 BEA WebLogic 8.1（及其最新的修补程序）和 IBM WebSphere 5.1（及其最新的修补程序）。

WebLogic 和 WebSphere 不是 Java Enterprise System 的一部分，因此不能使用 Java ES 安装程序进行安装和配置。大体步骤如下：

- 安装、配置和启动 Web 容器实例。
- 从 Java ES 安装程序安装 Directory Server。
- 在“以后再配置”模式下从 Java ES 安装程序安装 Access Manager，将使 Access Manager 保持为未配置状态。
- 运行 Access Manager 配置脚本，在 Web 容器中部署 Access Manager。
- 重新启动 Web 容器。

安装和配置 BEA WebLogic 8.1

安装 WebLogic 之前，请确保主机域名已在 DNS 中注册。另外，检查安装的 WebLogic 软件的版本是否正确。有关详细信息，请转至 BEA 产品站点：http://commerce.bea.com/index.jsp。

▼ 安装和配置 WebLogic 8.1

1 **将下载的 `.zip` 格式或 `.gz` 格式的软件映像解压缩。请确保所用的 zip/gzip 实用程序适用于当前平台，否则在解压缩期间将接收到校验和错误。**

2 **从目标系统的 shell 窗口运行安装程序。**

请遵循 WebLogic 安装实用程序（详细的安装说明位于 http://e-docs.bea.com/wls/docs81/）提供的步骤。

在安装过程中，请确保记录以下信息以便以后在 Access Manager 配置中使用：

- FQDN（在 WL8_HOST 参数中使用）
  - 安装位置
  - 端口号

3 **安装完成后，运行 WebLogic 配置工具，配置以下位置的域和服务器实例：**

WebLogic-base/WebLogic-instance/common/bin/quickstart.sh

默认情况下，WebLogic 将服务器实例定义为 myserver，将域定义为 mydomain。您不太可能会选择使用这些默认值。如要创建新的域和实例，请确保记录有关 Access Manager 配置和部署的信息。有关说明，请参阅 WebLogic 8.1 文档。

4 **如要在管理实例上安装，请使用以下位置的 startWebLogic.sh 实用程序启动 WebLogic：**

WebLogic-base/WebLogic-Userhome /domains/ *WebLogic-domain*/startWebLogic.sh

如要在受管实例上安装，请使用以下命令启动 WebLogic：

WebLogic-base /WebLogic-Userhome/domains/ WebLogic-domain /startManagedWebLogic WebLogic-managed-instancename admin-url

安装和配置 IBM WebSphere 5.1

安装 WebSphere 之前，请确保主机域名已在 DNS 中注册，并检查要安装的 WebSphere 软件的版本是否适用于当前平台。有关详细信息，请转至 IBM 产品支持网站：http://www-306.ibm.com/software/websphere/support/。

▼ 安装和配置 WebSphere 5.1

1 **将下载的 .zip 格式或 .gz 格式的软件映像解压缩。请确保所用的 zip/gzip 实用程序适用于当前平台，否则在解压缩期间将接收到校验和错误。**

2 **从目标系统的 shell 窗口运行安装程序。如果计划安装修补程序，请先安装 5.1 版本，然后再安装修补程序。详细的安装说明位于 http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp。**

在安装过程中，请确保记录以下信息以便以后在 Access Manager 配置中使用：

- 主机名
  - 域名
  - 单元名称
  - 节点名
  - 端口号

- 安装目录
- WebSphere 实例名
- 管理端口

  默认情况下，WebSphere 将服务器实例定义为 server1，尽管您未必会使用默认值。如果要创建新的实例，请确保记录有关 Access Manager 配置和部署的信息。有关说明，请参阅 WebSphere 5.1 文档。

3 **检验安装是否成功。**

   a. **确保** `server.xml` **文件在以下目录中：**

      `/opt/WebSphere/AppServer/config/cells/cell-name/noes/`

      `node-name/servers/server1`

   b. **使用** `startServer.sh` **命令启动服务器，例如：**

      `/opt/WebSphere/AppServer/bin/startServer.sh server1`

   c. **在 Web 浏览器中，输入以下格式的相应 URL 以查看范例 Web 应用程序：**

      `http://` *fqdn:portnumber/snoop*

4 **证实安装成功后，使用** `stopServer.sh` **实用程序关闭服务器。例如：**

`opt/WebSphere/AppServer/bin/stopServer.sh server1`

5 **如要安装 WebSphere 5.1 修补程序，则使用** `updateWizard.sh` **命令行实用程序在原始 5.1 实例上安装修补程序。**

6 **重新启动 WebSphere 并检查安装是否成功。**

使用 Java ES 安装 Directory Server 和 Access Manager

Access Manager 安装包括两次对 Java Enterprise System (Java ES) 安装程序的单独调用。

▼ 安装 Directory Server

1 **运行第一次 Java ES 调用并用"立即配置"选项安装 Directory Server（本地或远程）。"立即配置"选项允许在安装期间根据所作的选择（或默认值）配置第一个实例。**

2 **运行第二次 Java ES 调用并用“以后再配置”选项安装 Access Manager。此选项将安装 Access Manager 2005Q4 组件。安装之后，必须配置 Access Manager。**

WebLogic 和 WebSphere 的安装独立于 Java ES，因此安装程序不包含自动部署容器所需要的配置数据。为此，在安装 Access Manager 时必须选择“以后再配置”选项。此选项将使 Access Manager 部署处于以下状态：

- 活动的 Directory Server（本地或远程）不加载 Access Manager DIT 数据。
  - 不自动加载 Access Manager 配置文件。
  - 不生成 Access Manager Web 应用程序 `.war` 文件。
  - 不自动启动并运行 Access Manager 部署和安装后配置进程。

    有关详细的安装说明，请参阅 http://docs.sun.com/doc/819-0810 上的 Sun Java Enterprise System 安装指南。

配置 Access Manager

在目标系统的本地驱动器上完成 Access Manager 的安装之后，需要使用 WebLogic 8.1 或 WebSphere 5.1 手动配置 Access Manager。该过程分为三个步骤：

▼ 配置 Access Manager

1 **编辑配置脚本输入文件**

2 **运行配置脚本**

3 **重新启动 Web 容器**

创建配置脚本输入文件

Access Manager 配置脚本输入文件包含所有的部署级别、Access Manager、Web 容器和 Directory Server 变量的定义。Access Manager 包含一个范例配置脚本输入文件模板 (`amsamplesilent`)，它位于 Solaris 系统的 *AccessManager-base* `/SUNWam/bin` 目录中或在 Linux 系统的 *AccessManager-base* `/identity/bin` 目录中。

可以使用 `amsamplesilent` 模板构建配置脚本输入文件。第 21 页中的 “Access Manager 范例配置脚本输入文件”中介绍了编辑文件以及变量定义的说明。

在编辑文件之前，请确保 Web 容器安装中的以下信息可用：

BEA WebLogic 和 IBM WebSphere

- 安装位置
- 实例名和位置
- 主机名
- FQDN
- 侦听的端口号
- 管理 ID
- 使用的协议

仅 BEA WebLogic

- 管理密码
- 共享库位置
- 域名和位置
- 项目目录名
- JDK 位置

仅 IBM WebSphere

- 单元名称
- 节点名
- JDK 位置

运行配置脚本

保存配置脚本输入文件之后，运行 `amconfig` 脚本以完成配置过程。例如：

```
AccessManager-base/SUMWam/bin/amconfig -s silentfile
```

silentfile 应为配置输入文件的绝对路径。

运行此脚本可执行以下功能：

1. 将 Access Manager 模式载入活动的 Directory Server 实例。
2. 将 Access Manager 服务数据载入 Directory Server 实例。
3. 生成活动的 Access Manager 实例所用的 Access Manager 配置文件。
4. 将 Access Manager Web 应用程序数据部署到 Web 容器。
5. 自定义 Web 容器配置以符合 Access Manager 的要求。

重新启动 Web 容器

在完成配置过程之后，必须重新启动 Web 容器。有关说明，请参阅产品文档。

有关 BEA WebLogic 8.1 的信息，请参阅 http://e-docs.bea.com/wls/docs81。

有关 IBM WebSphere 5.1 的信息，请参阅 http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp。

◆ ◆ ◆ 第 3 章

3 在 SSL 模式下配置 Access Manager

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

- 使用安全 Web 容器配置 Access Manager
- 将 Access Manager 配置到安全的 Directory Server

使用安全 Sun Java Enterprise System Web Server 配置 Access Manager

要使用 Web Server 在 SSL 模式下配置 Access Manager，请参见以下步骤：

▼ 配置安全的 Web Server

1 **在 Access Manager 控制台中，转至“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，然后添加 `https://` 协议。单击“保存”。**

注 – 请务必单击“保存”。如果您没有单击“保存”，仍可以继续进行以下步骤，但是将丢失对配置所进行的全部更改，并且您将不能作为管理员登录来进行恢复。

步骤 2 到 24 介绍了 Web Server。

2 **登录 Web Server 控制台。默认端口为 8888。**

3 **选择在其上运行 Access Manager 的 Web Server 实例并单击“管理”。**
将显示一个弹出窗口，说明配置已更改。单击 “确定” 。

4 **单击屏幕右上角的“应用”按钮。**

5 **单击“应用更改”。**
Web Server 应当会自动重新启动。单击“确定”继续。

6 **停止选定的 Web Server 实例。**

7 **单击“安全”选项卡。**

8 **单击“创建数据库”。**

9 **输入新的数据库密码并单击“确定”。**
请务必将数据库密码记下来，以备将来使用。

10 **创建“证书数据库”后，单击“请求证书”。**

11 **在屏幕上的字段中输入数据。**
“密钥对字段密码”字段与在步骤 9 中输入的字段相同。在位置字段中，您需要完整写出位置。不能输入缩写（例如 CA）。必须定义所有字段。在“公共名称”字段中，输入您的 Web Server 的主机名。

12 **提交表单后，您将看到如下消息：**

```
--BEGIN CERTIFICATE REQUEST---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE REQUEST--
```

13 **复制并为证书请求提交该文本。**
确保您获取的是根 CA 证书。

14 **您将收到一个包含证书的证书响应，例如：**

```
--BEGIN CERTIFICATE---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE---
```

15 **将这些文本复制到剪贴板或保存到文件中。**

16 转至 Web Server 控制台并单击“安装证书”。

17 单击该服务器的“证书”。

18 在“密钥对文件密码”字段中，输入“证书数据库”密码。

19 将证书粘贴到提供的文本字段中或选中单选按钮，并在文本框中输入文件名。单击“提交”。
浏览器将显示证书，并提供用于添加证书的按钮。

20 单击“安装证书”。

21 单击“可信赖证书授权机构的证书”。

22 按照步骤 16 到 21 中所述的相同方式安装“根 CA 证书”。

23 安装完这两种证书后，单击 Web Server 控制台中的“首选项”选项卡。

24 如果要在其他端口上启用 SSL，请选择“添加侦听套接字”。然后，选择“编辑侦听套接字”。

25 将安全状态从“已禁用”更改为“已启用”，单击“确定”提交更改，然后单击“应用”和“应用更改”。
步骤 26 – 29 适用于 Access Manager。

26 打开 `AMConfig.properties` 文件。默认情况下，该文件的位置为 `etc/opt/SUNWam/config`。

27 将所有出现的 `http://` 协议替换为 `https://`，Web Server 实例目录使用的协议除外。这也在 `AMConfig.properties` 中指定，但必须保持相同。

28 保存 `AMConfig.properties` 文件。

29 在 Web Server 控制台中，单击 Access Manager 主机的 Web 服务器实例的“开/关”按钮。
Web Server 将在“启动/停止”页面中显示一个文本框。

30 在文本字段中输入“证书数据库”密码并选择“启动”。

使用安全 Sun Java System Application Server 配置 Access Manager

设置 Access Manager 以在启用了 SSL 的应用程序服务器上运行分为两个步骤。首先，将 Application Server 实例配置为安全实例，绑定到已安装的 Access Manager，然后配置 Access Manager。

以 SSL 设置 Application Server 6.2

本节描述了在 SSL 模式下设置 Application Server 6.2 的步骤。

▼ 保证 Application Server 实例的安全

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

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

   默认端口为 4848。

2. 输入在安装过程中输入的用户名和密码。

3. 选择已在其中安装（或将要安装）Access Manager 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. 输入新数据库密码并予以确认，然后单击“确定”按钮。请确保记下数据库密码，以备将来使用。

10. 创建“证书数据库”之后，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. 输入证书所需的以下“请求”数据

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

    b. 指定您要提交证书请求的方式。

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

       如果要从正在使用 Certificate Server 的内部 CA 申请证书，则单击 CA URL 并输入 Certificate Server 的 URL。此 URL 应指向处理证书请求的证书服务器的程序。

c. 输入密钥对文件的密码（这是在步骤 9 中指定的密码）。

d. 输入以下标识信息：

公共名称。服务器的全名，包括端口号。

请求者名称。请求者的名称。

电话号码。请求者的电话号码

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

电子邮件地址。管理员的电子邮件地址。

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

组织单位名称。组织的部门或其他运作单位的名称。

位置名称（城市）。城市或城镇的名称。

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

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

13 单击“确定”按钮。系统将显示一条消息，例如：

```
--BEGIN NEW CERTIFICATE REQUEST---
afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdfla
alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl
--END NEW CERTIFICATE REQUEST--
```

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

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

16 收到来自证书授权机构的数字证书后，您可以将文本复制到剪贴板或保存到文件中。

17 转到 Application Server 控制台并单击“安装”链接。

18 选择“此服务器的证书”。

19 在“密钥对文件密码”字段中，输入“证书数据库”密码。

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 按与上述相同的方式安装“根 CA 证书”。但要选择“可信赖证书授权机构的证书”。

24 证书安装都完成后，请展开左侧框中的“HTTP 服务器”节点。

25 选择“HTTP 服务器”下的“HTTP 侦听器”。

26 选择 `http-listener-1`。浏览器将显示套接字信息。

27 将 `http-listener-1` 使用的端口值从安装 Application Server 时输入的值更改为一个更合适的值，如 443。

28 选择“启用 SSL/TLS”。

29 选择“证书昵称”。

30 指定返回服务器。该名称应与在步骤 12 中指定的公共名称匹配。

31 单击“保存”。

32 选择将在其上安装 Access Manager 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”。应用服务器会自动重新启动。

以 SSL 配置 Application Server 8.1

以 SSL 配置 Application Server 8.1 的基本步骤如下。有关详细的说明，参见 Application Server 8.1 文档。

1. 通过 Application Server 管理控制台在 Application Server 上创建安全端口。有关详细信息，请参见位于以下地址的 Sun Java System Application Server Enterprise Edition 8.1 管理指南中的“配置安全性”：

   `http://docs.sun.com/app/docs/coll/1310.1` 及
   `http://docs.sun.com/app/docs/coll/1386.1`

2. 确认信任服务器证书的证书授权机构 (CA) 存在于 Web 容器的信任数据库中。然后，获取并安装该 Web 容器的服务器证书。有关详细信息，请参见位于以下地址的 Sun Java System Application Server Enterprise Edition 8.1 管理指南中的“使用证书和 SSL”：

   `http://docs.sun.com/app/docs/coll/1310.1` 及
   `http://docs.sun.com/app/docs/coll/1386.1`

3. 重新启动 Web 容器。

在 SSL 模式下配置 Access Manager

本节介绍在 SSL 模式下配置 Access Manager 的步骤。在设置 Access Manager 的 SSL 之前，请确保已为部署配置了 Web 容器。

▼ 在 SSL 模式下配置 Access Manager

1 **在 Access Manager 控制台中，转至"服务配置"模块并选择"平台"服务。在"服务器列表"属性中，添加 HTTPS 协议格式的相同 URL 和启用 SSL 的端口号。单击"保存"。**

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

---

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

`/etc/opt/SUNWam/config`。

3 **将所有出现的** `http://` **协议替换为** `https://`，**并将端口号更改为已启用 SSL 的端口号。**

4 **保存** `AMConfig.properties` **文件。**

5 **重新启动 Application Server。**

使用安全 BEA WebLogic Server 配置 AMSDK

在 SSL 模式下使用 AMSDK 配置 BEA WebLogic Server 之前，必须首先安装此服务器并将其作为 Web 容器进行配置。有关安装说明，请参阅 BEA WebLogic 服务器文档。要将 WebLogic 配置为 Access Manager 的 Web 容器，请参阅第 1 章。

▼ 配置安全 WebLogic 实例

1 **使用快速启动菜单创建域**

2 **转至 WebLogic 安装目录并生成证书请求。**

3 **通过将 CSR 文本文件用于 CA 来申请服务器证书。**

4 **将批准的证书保存到文本文件中。例如，**`approvedcert.txt` **文件。**

5 **使用以下命令在** `cacerts` **中加载根 CA：**

```
cd jdk141_03/jre/lib/security/
```

```
jdk141_03/jre/bin/keytool -keystore cacerts -keyalg RSA -import -trustcacerts -alias
"<alias name>" -storepass changeit -file /opt/bea81/cacert.txt
```

6 **使用以下命令加载服务器证书：**

```
jdk141_03/jre/bin/keytool -import -keystore <keystorename> -keyalg RSA -import
-trustcacerts -file approvedcert.txt -alias "mykey"
```

7 **使用您的用户名和密码登录 WebLogic 控制台。**

8 **浏览到以下位置：**

“yourdomain”>“服务器”>“myserver”>“配置密钥库”

9 **选择“自定义身份”，然后选择“Java 标准信任”。**

10 **输入密钥库的位置。例如，**`/opt/bea81/keystore`。

11 **输入密钥库密码和密钥库密码短语。例如：**

密钥库密码：`JKS/Java Standard Trust`（对于 WL 8.1，此密码仅为 JKS）

密钥库密码短语：`changeit`

12 **检查 SSL 专用密钥设置、专用密钥别名和密码。**

注 – 必须使用全强度 SSL 许可证，否则 SSL 启动将会失败。

---

13 **在 Access Manager 中，**`AmConfig.properties`** 中的以下参数在安装期间自动配置。如果未配置，可以进行适当的编辑：**

```
com.sun.identity.jss.donotInstallAtHighestPriority=true [ this is not
 required for AM 6.3 and above]
com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.am.util.SecureRandomFactoryImpl
com.iplanet.security.SSLSocketFactoryImpl=netscape.ldap.factory.JSSESocketFactory
com.iplanet.security.encryptor=com.iplanet.services.util.JCEEncryption
```

如果 JDK 路径如下：

```
com.iplanet.am.jdk.path=/usr/jdk/entsys-j2se
```

则使用 keytool 实用程序导入证书数据库中的根 CA。例如：

```
/usr/jdk/entsys-j2se/jre/lib/security
/usr/jdk/entsys-j2se/jre/bin/keytool -keystore cacerts
-keyalg RSA -import -trustcacerts -alias "machinename" -storepass changeit -file
/opt/bea81/cacert.txt
```

keytool 实用程序位于以下目录：

```
/usr/jdk/entsys-j2se/jre/bin/keytool
```

14 从 **Access Manager** `amadmin` 命令行实用程序中删除 `-D"java.protocol.handler.pkgs=com.iplanet.services.comm"`。

15 在 **SSL** 模式下配置 **Access Manager**。有关详细信息，请参阅第 49 页中的“ 在 SSL 模式下配置 Access Manager ”。

使用安全 IBM WebSphere Application Server 配置 AMSDK

在 SSL 模式下使用 AMSDK 配置 IBM WebSphere Server 之前，必须首先安装此服务器并将其作为 Web 容器进行配置。有关安装说明，请参阅 WebSphere 服务器文档。要将 WebLogic 配置为 Access Manager 的 Web 容器，请参阅第 1 章。

▼ 配置安全 WebSphere 实例

1 启动 **Websphere** `/bin` 目录中的 `ikeyman.sh`。

2 从“签名者”菜单导入证书授权机构 (CA) 的证书。

3 从“个人证书”菜单生成 CSR。

4 检索上一步骤中创建的证书。

5 选择“个人证书”并导入服务器证书。

6 从 WebSphere 控制台更改默认的 SSL 设置并选择密码。

7 设置默认的 IBM JSSE SSL 提供者。

8 要从应用服务器 JVM 密钥库中刚创建的文件导入根 CA 证书，输入以下命令：

```
$ appserver_root-dir/java/bin/ keytool -import -trustcacerts -alias cmscacert
-keystore ../jre/lib/security/cacerts -file
/full_path_cacert_filename.txt
```

app-server-root-dir 为应用服务器的根目录，*full_path_cacert_filename.txt* 为包含此证书的文件的完整路径。

9 在 **Access Manager** 中更新 `AmConfig.properties` 中的以下参数以使用 **JSSE**：

```
com.sun.identity.jss.donotInstallAtHighestPriority=true
com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.
```

```
am.util.SecureRandomFactoryImpl
com.iplanet.security.SSLSocketFactorImpl=netscape.ldap.factory.
JSSESocketFactory
com.iplanet.security.encyptor=com.iplanet.services.unil.JCEEncryption
```

10 **在 SSL 模式下配置 Access Manager。有关详细信息，请参阅****第 49 页中的“ 在 SSL 模式下配置 Access Manager ”**。

在 SSL 模式下将 Access Manager 配置到 Directory Server

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

1. 获得并安装 Directory Server 的证书，然后配置 Directory Server，以信赖证书授权机构 (CA) 的证书。
2. 打开目录中的 SSL。
3. 配置验证、策略和平台服务，以连接到启用 SSL 的 Directory Server。
4. 配置 Access Manager，以安全地连接至 Directory Server 后端。

在 SSL 模式下配置 Directory Server

要在 SSL 模式下配置 Directory Server，必须获取并安装服务器证书、配置 Directory Server 以信赖 CA 的证书并启用 SSL。有关如何完成这些任务的详细说明，请参阅 *Directory Server* 管理指南的第 11 章，“管理验证和加密”。可在以下位置找到此文档：

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

如果 Directory Server 已经启用了 SSL，则转至下一节，以了解有关将 Access Manager 连接至 Directory Server 的详细信息。

将 Access Manager 连接至已启用 SSL 的 Directory Server

在 SSL 模式下配置完 Directory Server 后，需要将 Access Manager 安全地连接至 Directory Server 后端。

▼ 将 Access Manager 连接到 Directory Server

1 在 Access Manager 控制台中，转至“服务配置”模块中的“LDAP 验证”服务。

   a. 将 Directory Server 端口更改为 SSL 端口。

   b. 选择“对 LDAP 服务器启用 SSL 访问”属性。

2 转到“服务配置”模块中的“成员资格验证”服务。

   a. 将 Directory Server 端口更改为 SSL 端口。

   b. 选择“对 LDAP 服务器启用 SSL 访问”属性。

3 转至“服务配置”中的“策略配置”服务。

   a. 将 Directory Server 端口更改为 SSL 端口。

   b. 选择“启用 LDAP SSL”属性。

4 在文本编辑器中打开 `serverconfig.xml`。该文件位于：
`/etc/opt/SUNWam/config`

   a. 在 <服务> 元素中，更改以下值：
   `port` - 输入 Access Manager 侦听的安全端口的端口号（默认值为 636）。
   `type` - 将“SIMPLE”更改为“SSL”。

   b. 保存并关闭 `serverconfig.xml`。

5 从以下默认位置打开 `AMConfig.properties` 文件：
/etc/opt/ `SUNWam/config`。
更改以下属性：

   a. `com.iplanet.am.directory.port = 636`（如果使用默认值）

   b. `ssl.enabed = true`

   c. 保存 `AMConfig.properties`。

6 重新启动服务器

第 II 部分

访问控制

这是《Sun Java System Access Manager™ 7 2005Q4 管理指南》的第二部分。“访问控制”界面提供了一种创建和管理验证与验证服务的方法，从而保护和控制基于领域的资源。当企业用户请求信息时，Access Manager 会验证用户身份并授权用户访问其所请求的特定资源。本部分包含以下各章：

◆ ◆ ◆ 第 4 章

Access Manager 控制台

Access Manager 控制台是一个 Web 界面，它允许拥有不同访问级别的管理员（包括做其他事情）创建领域和组织、在这些领域中创建或删除用户，以及建立可保护和限制领域资源访问的强制策略。此外，管理员还可以查看和终止当前用户会话以及管理它们的联合配置（创建、删除和修改验证域和提供商）。另一方面，不拥有管理权限的用户可以管理个人信息（姓名、电子邮件地址、电话号码等）、更改他们的密码、订阅和取消订阅组以及查看他们的角色。 Access Manager 控制台拥有两个基本视图：

管理视图

拥有管理角色的用户通过 Access Manager 进行验证时，默认视图为“管理视图”。在该视图中，管理员可以执行与 Access Manager 相关的大多数管理任务。Access Manager 可以在两种不同模式（“领域”模式和“传统”模式）下进行安装。每种模式均拥有其各自的控制台。有关“领域模式”和“传统模式”的详细信息，请参阅 《Sun Java System Access Manager 7 2005Q4 Technical Overview》 。

领域模式控制台

“领域”模式控制台允许管理员管理基于领域的访问控制、默认服务配置、Web 服务和联合。要访问管理员登录屏幕，请在浏览器中使用以下地址语法：

protocol`://`*servername* `/amserver/UI/Login`

`protocol` 可以为 http 或 https，具体取决于您的部署。

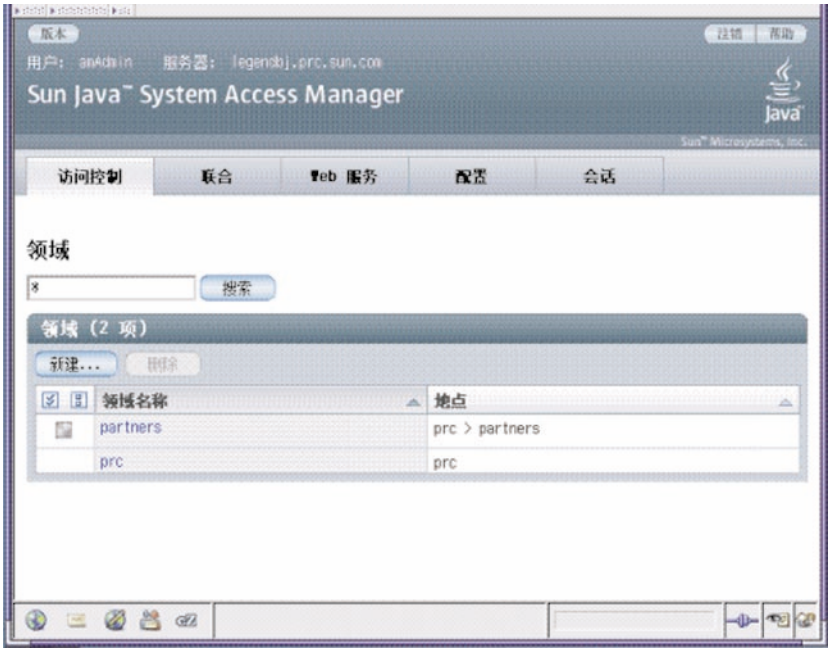

图 4–1 领域模式管理视图

传统模式控制台

“传统模式”控制台是基于 Access Manager 6.3 体系结构的。此传统 Access Manager 体系结构使用 Sun Java System Directory Server 自带的 LDAP 目录信息树 (DIT)。在“传统模式”下，用户信息和访问控制信息均存储于 LDAP 组织中。选择“传统模式”时，LDAP 组织等同于访问控制领域。领域信息集成在 LDAP 组织内。在“传统模式”下，“目录管理”选项卡可在基于 Access Manager 的身份管理中使用。

要访问管理员登录屏幕，请在浏览器中使用以下地址语法：

protocol`://`*servername* `/amserver/console`

`protocol` 可以为 http 或 https，具体取决于您的部署。

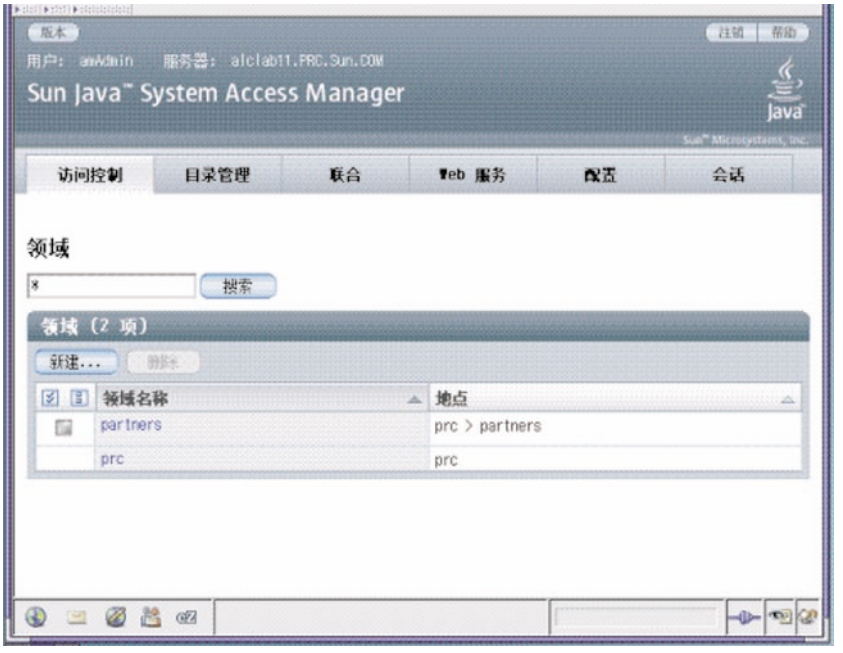

图 4–2 传统模式管理视图

传统模式 6.3 控制台

Access Manager 6.3 的某些功能在 Access Manager 7.0 控制台中不可用。因此，管理员可以通过 7.0 传统部署登录到 6.3 控制台。在将 Access Manager 建立在 Sun Java System Portal Server 或其他需要将 Sun Java System Directory Server 用作中心身份库的 Sun Java System 通信产品上的情况下，通常会使用此控制台。其他功能（如“委托管理”和“服务类”）只能通过此控制台进行访问。

注 – 请勿交换使用 6.3 传统模式控制台和 7.0 传统模式控制台。

要访问 6.3 控制台，请在浏览器中使用以下地址语法：

protocol`://`*servername* `/amconsole`

`protocol` 可以为 http 或 https，具体取决于您的部署。

图 4–3 基于传统 6.3 的控制台

用户概要文件视图

当尚未指定管理角色的用户向 Access Manager 进行验证时，默认视图为用户自己的“用户概要文件”视图。在“领域模式”或“传统模式”下均可访问“用户概要文件”视图。要访问该视图，用户必须在“登录”页面中输入自己的用户名和密码。

用户可以在该视图中修改用户的个人配置文件所特有的属性值。其中包括（但不限于）姓名、家庭地址和密码。“用户概要文件视图”中显示的属性可以扩展。

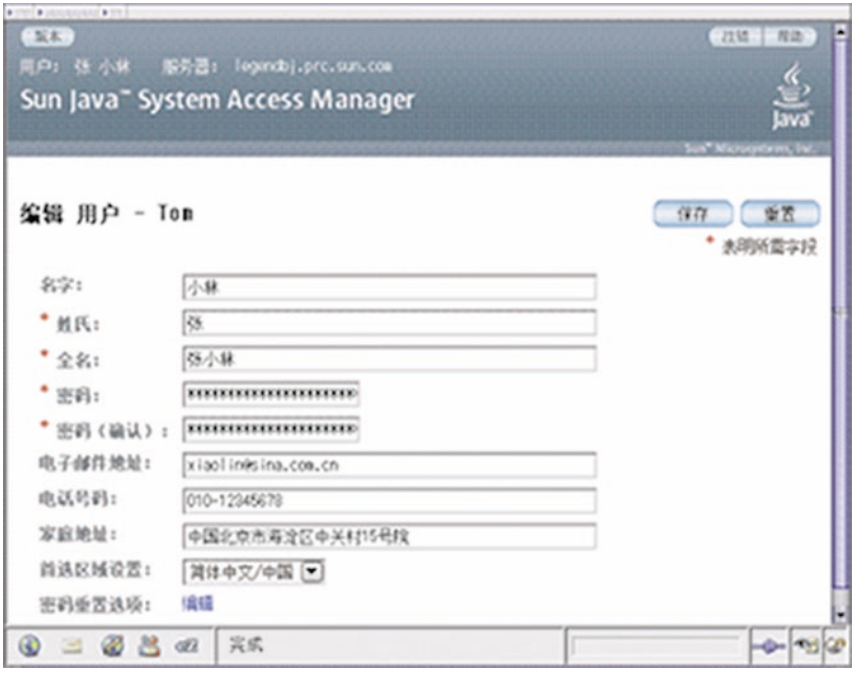

图 4–4 用户概要文件视图

◆ ◆ ◆ 第 5 章

管理领域

访问控制领域是可以与用户或用户组关联的一组验证属性和授权策略。领域数据存储在专用信息树中，该树由 Access Manager 在指定的数据存储库中创建。Access Manager 框架聚集了 Access Manager 信息树中各领域所包含的策略和属性。默认情况下，除用户数据外，Access Manager 7 将 Access Manager 信息树作为 Sun Java Enterprise System Directory Server 中的一个特殊分支自动插入。您可以在使用任何 LDAPv3 数据库的同时使用访问控制领域。

有关领域的详细信息，请参阅《Sun Java System Access Manager 7 2005Q4 Technical Overview》。

在“领域”选项卡中，可以配置访问控制的以下属性：

创建和管理领域

本节说明了如何创建和管理领域。

▼ 创建新的领域

1 **从“访问控制”选项卡下的“领域”列表中选择“新建”。**

2 **定义以下常规属性：**

名称　　输入领域名称。

父领域　　定义要创建的领域的位置。选择要在其中创建新领域的父领域。

3 **定义以下领域属性：**

领域状态	选择“活动”状态或“不活动”状态。默认值为“活动”。在领域的生命期内，可以随时通过选择“属性”图标来更改其状态。如果选择“不活动”，则当登录时，将禁止用户访问。
领域/DNS 别名	允许为领域的 DNS 名称添加别名。该属性只接受“真实的”域别名（不允许使用随机字符串）。

4 单击“确认”保存或单击“取消”返回上一页面。

常规属性

“常规属性”页面显示领域的基本属性。要修改这些属性，请从“访问控制”选项卡下的“领域名称”列表中单击某领域。然后编辑以下属性：

领域状态	选择“活动”状态或“不活动”状态。默认值为“活动”。在领域的生命期内，可以随时通过选择“属性”图标来更改其状态。如果选择“不活动”，则当登录时，将禁止用户访问。
领域/DNS 别名	允许为领域的 DNS 名称添加别名。该属性只接受“真实的”域别名（不允许使用随机字符串）。

编辑属性后，单击“保存”。

验证

在用户可以使用其他验证模块登录之前，常规验证服务必须注册为领域的服务。核心验证服务允许 Access Manager 7 管理员为领域的验证参数定义默认值。如果在指定的验证模块中没有定义覆盖值，则可以使用这些值。“核心验证服务”的默认值在 amAuth.xml 文件中进行定义，安装结束后将保存在 Directory Server 中。

有关详细信息，请参阅第 7 章

服务

在 Access Manager 中，服务是由 Access Manager 控制台同时管理的一组属性。属性可以仅仅是一些相关的信息，如雇员姓名、职务以及电子邮件地址。但是属性常被用作软件模块（如邮件应用程序或工资单服务）的配置参数。

您可以通过“服务”选项卡在领域中添加和配置许多 Access Manager 默认服务。您可以添加以下服务：

- 管理
- 搜索服务
- 全局化设置

- 密码重置
- 会话
- 用户

注 – Access Manager 要求服务 .xml 文件中的必需属性有一些默认值。如果服务的必需属性没有值，则需要添加默认值并重新加载服务。

▼ 将服务添加到领域

1. **单击要为其添加新服务的领域的名称。**
2. **选择“服务”选项卡。**
3. **单击“服务”列表中的“添加”。**
4. **选择要为领域添加的服务。**
5. **单击“下一步”。**
6. **通过定义领域属性来配置服务。有关服务属性的说明，请参阅联机帮助中的“配置”。**
7. **单击“完成”。**
8. **要编辑服务的属性，请在“服务”列表中单击其名称。**

权限

权限定义领域中现有的角色或组的访问权限。这些角色或组可用作“Access Manager 身份主题”类型的策略主题定义。单击您要进行编辑的角色或组的名称，可指定或修改权限。您可以指定的权限包括：

- 仅针对策略属性的读写访问权限
- 所有领域和策略属性的读写访问权限
- 所有属性和服务的只读访问权限

◆ ◆ ◆ 第 6 章

数据存储库

数据存储库是一个可用来存储用户属性和用户配置数据的数据库。

Access Manager 提供一个身份库插件，此插件可连接到身份库框架。使用这一新的模型可以不必在现有的用户数据库中做任何更改，便能查看和检索 Access Manager 用户信息。Access Manager 框架将来自身份库插件的数据和其他 Access Manager 插件的数据整合在一起，为每个用户形成一个虚拟身份。而后，Access Manager 能使用通用身份在多个身份库之间进行验证和授权过程。在用户会话结束后将会销毁虚拟用户身份。

LDAPv3 数据存储库

当在“领域”和“传统”模式下安装 Access Manager 时，可以为任何普通 LDAPv3 库创建新的数据存储库实例。应该在以下条件下选择 LDAPv3 库类型：

- 当不需要角色、服务类 (Cos) 以及与上一版本兼容时。
- 当要使用现有目录时。
- 当要将非 Sun Java System Directory Server 的目录服务器用于身份库时。
- 当不希望 Access Manager 写入身份库时。
- 当要使用平面目录信息树 (DIT) 时。

▼ 创建新的 LDAPv3 数据存储库

以下部分描述连接普通 LDAPv3 数据存储库的步骤。

1. **选择要为其添加新的数据存储库的领域。**
2. **单击“数据存储库”选项卡。**
3. **在“数据存储库”列表中，单击”新建”。**
4. **输入数据存储库的名称。**

5 定义 LDAPv3 库插件的属性。

6 单击“完成”。

LDAPv3 库插件属性

用于配置 LDAPv3 库插件的属性如下：

- 第 73 页中的 “重试之间的延时”
- 第 73 页中的 “需要重试的 LDAP 异常错误代码”

主 LDAP 服务器

输入要连接的 LDAP 服务器的名称。格式应为 hostname.domainname:portnumber。

如果输入了多个 host:portnumber 条目，将尝试连接列表中的第一个主机。仅当尝试连接当前主机失败时，才会尝试列表中的下一个条目。

LDAP 绑定 DN

指定 Access Manager 将用来向您当前连接的 LDAP 服务器进行验证的 DN 名称。拥有绑定 DN 名称的用户应该具有在“LDAPv3 支持的类型和操作”属性中配置的正确的添加/修改/删除权限。

LDAP 绑定密码

指定 Access Manager 将用来向您当前连接的 LDAP 服务器进行验证的 DN 名称

LDAP 绑定密码（ 确认 ）

确认密码。

LDAP 组织 DN

该数据存储库将映射到的 DN。它将成为在此数据存储库中执行的所有操作的基本 DN。

启用 LDAP SSL

如果启用该选项，Access Manager 将使用 HTTPS 协议连接到主服务器。

LDAP 连接池的最小尺寸

指定连接池中连接的初始数量。使用连接池可避免每次都必须创建新的连接。

LDAP 连接池的最大尺寸

指定允许的最大连接数。

搜索返回的结果的最大数目

指定搜索操作所返回的最大条目数。如果达到此限制，Directory Server 将返回与搜索要求相匹配的任何条目。

搜索超时

指定分配给搜索请求的最长时间（以秒计）。如果达到此限制，Directory Server 将返回与搜索要求相匹配的任何搜索条目。

LDAP 遵循候选组织

如果启用，此选项将指定自动遵循其他 LDAP 服务器的候选组织。

LDAPv3 库插件类名称

指定实现 LDAPv3 库的类文件的位置。

属性名称映射

将框架已知的公共属性映射到本地数据存储库。例如，如果框架使用 inetUserStatus 确定用户状态，则本地的数据存储库实际可能会使用 userStatus。属性定义区分大小写。

LDAPv3 插件支持的类型和操作

指定允许或可以在此 LDAP 服务器上执行的操作。默认操作是仅此 LDAPv3 库插件支持的操作。 LDAPv3 库插件支持以下操作：

- 组 -- 读取、创建、编辑、删除
- 领域 -- 读取、创建、编辑、删除、服务
- 用户 -- 读取、创建、编辑、删除、服务
- 代理 -- 读取、创建、编辑、删除

可以根据您的 LDAP 服务器设置和任务移除以上权限，但不能添加其他权限。

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。例如，如果用户的 DN 为 `uid=k user5,ou=people,dc=iplanet,dc=com`，则命名属性为 uid。`(uid=*)` 将附加到用户的搜索过滤器中。

LDAP 用户搜索过滤器

指定用于查找用户条目的搜索过滤器。例如，如果 LDAP 用户搜索属性为 uid 并且 LDAP 用户搜索过滤器为 `(objectClass=inetorgperson)`，则实际用户搜索过滤器为：`(&(uid=*)(objectClass=inetorgperson))`。

LDAP 用户对象类

指定用户的对象类。创建用户之后，此用户对象类列表将被添加到用户的属性列表中。

LDAP 用户属性

定义与用户相关的属性列表。禁止对不在列表之内的用户属性进行任何读/写尝试。属性区分大小写。在这里定义对象类和属性模式之前，必须先在 Directory Server 中定义对象类和属性模式。

LDAP 组搜索属性

该字段用于定义搜索组时使用的属性类型。例如，如果组 DN 为 `cn=group1,ou=groups,dc=iplanet,dc=com`，则组的命名属性为 `cn`，并且 `(cn=*)` 将附加到组搜索过滤器中。

LDAP 组搜索过滤器

指定用于查找组条目的搜索过滤器。例如，如果 LDAP 组搜索属性为 `cn` 并且 LDAP 组搜索过滤器为 `(objectclass=groupOfUniqueNames)`，则实际组搜索过滤器为 `(&(cn=*)(objectclass=groupOfUniqueNames))`。

LDAP 组容器命名属性

如果组驻留在容器中，则指定组容器的命名属性。否则，该属性保留为空。例如，如果组 DN `cn=group1,ou=groups,dc=iplanet,dc=com` 驻留在 `ou=groups` 中，则组容器命名属性为 `ou`。

LDAP 组容器值

指定组容器的值。例如，组 DN `cn=group1,ou=groups,dc=iplanet,dc=com` 驻留在容器名称 `ou=groups`中，则组容器值将为 `groups`。

LDAP 组对象类

指定组的对象类。创建组之后，此组对象类列表将被添加到组的属性列表中。

LDAP 组属性

定义与组相关的属性列表。禁止对不在列表之内的组属性进行任何读/写尝试。属性区分大小写。在这里定义对象类和属性模式之前，必须先在 Directory Server 中定义对象类和属性模式。

组成员资格的属性名称

指定属性名称，该属性的值为所有包含 DN 的组的名称。默认值为 `memberOf`。

组成员的属性名称

指定属性名称，该属性的值为该组所包含的某个 DN。默认值为 `uniqueMember`。

组成员 URL 的属性名称

指定属性名称，该属性的值为解析为该组所包含的成员的某个 LDAP URL。默认值为 `memberUrl`。

LDAP 人员容器命名属性

如果用户驻留在人员容器中，则指定该人员容器的命名属性。如果用户没有驻留在人员容器中，则将该字段保留为空。例如，假设用户 DN 为 `uid=kuser5,ou=people,dc=iplanet,dc=com`，如果人员容器的名称为 `ou=people`，则命名属性为 `ou`。

LDAP 人员容器值

指定人员容器的值。默认值为 `people`。例如，假设用户 DN 为 `uid=kuser5,ou=people,dc=iplanet,dc=com`，如果人员容器的名称为 `ou=people`，则命名属性为 `ou` 并且“LDAP 人员容器值”为 `people`。

LDAP 代理搜索属性

该字段用于定义搜索代理时使用的属性类型。默认值为 `uid`。例如，如果代理的 DN 为 `uid=kagent1,ou=agents,dc=iplanet,dc=com`，则代理的命名属性为 uid。`(uid=*)` 将附加到代理的搜索过滤器中。

LDAP 代理容器命名属性

如果代理驻留在代理容器中，则指定该代理容器的命名属性。如果代理没有驻留在代理容器中，则将该字段保留为空。例如，假设用户 DN 为 `uid=kagent1,ou=agents,dc=iplanet,dc=com`，则代理命名属性为 `ou`。

LDAP 代理容器值

指定代理容器的值。如果代理没有驻留在代理容器中，则将该字段保留为空。在前面的示例中，代理容器值为 `agents`。

LDAP 代理搜索过滤器

定义用于搜索代理的过滤器。“LDAP 代理搜索”属性将被置于此字段之前，以生成实际的代理搜索过滤器。

例如，如果“LDAP 代理搜索属性”为 `uid` 并且“LDAP 用户搜索过滤器”为 `(objectClass=sunIdentityServerDevice)`，则实际用户搜索过滤器为 `: (&(uid=*)(objectClass=sunIdentityServ erDevice))`

LDAP 代理对象类

定义代理的对象类。创建代理之后，用户对象类的列表将被添加到代理的属性列表中。

LDAP 代理属性

定义与代理相关的属性列表。禁止对不在列表之内的代理属性进行任何读/写尝试。属性区分大小写。在这里定义对象类和属性模式之前，必须先在 Directory Server 中定义对象类和属性模式。

持久搜索基本 DN

定义用于持久搜索的基本 DN。某些 LDAPv3 服务器仅在根后缀级别上支持持久搜索。

重新启动前的持久搜索最大空闲时间

定义重新启动持久搜索前的最大空闲时间。该值必须大于 1。如果小于或等于 1，重新启动搜索时将不会考虑连接的空闲时间。

如果部署 Access Manager 时包括负载平衡器，则某些负载平衡器会空闲指定的时间后超时。在这种情况下，您为“重新启动前的持久搜索最大空闲时间”设置的值应该小于为负载平衡器指定的空闲时间。

出现错误代码后的最大重试次数

定义持久搜索操作遇到在“需要重试的 LDAP 异常错误代码”中指定的错误代码时可以重试的最大次数。

重试之间的延时

指定每次重试之前的等待时间。仅适用于持久搜索连接。

需要重试的 LDAP 异常错误代码

指定可以重试持久搜索操作的错误代码。该属性仅适用于持久搜索，而非所有 LDAP 操作。

AMSDK 库插件

当在“传统”模式下安装 Access Manager 时，AMSDK 身份库会自动与 Access Manager 信息树混合。在“领域”模式下，可以选择安装 AMSDK 库，但身份库不会与 Access Manager 信息树混合。应该在以下条件下选择 AMSDK 库类型 :

- 需要使用 Sun Java System Directory Server 的特定功能，如角色和 CoS。
- 需要与上一版本的 Access Manager 兼容。

▼ 创建新的 AMSDK 库插件

1. **选择要在其中配置 Access Manager 库插件的领域。**
2. **单击“数据存储库”选项卡。**
3. **在“数据存储库”列表中，单击”新建”。**
4. **输入库插件的名称。**

5 选择“Access Manager 库插件”。

6 单击“下一步”。

7 定义以下字段：

Access Manager 插件类名称	指定实现 Access Manager 库插件的类文件的位置。
Access Manager 组织	指向 Directory Server 中由 Access Manager 管理的某组织 DN。它将成为在此数据存储库中执行的所有操作的基本 DN。

8 单击“完成”。

◆ ◆ ◆ 第 7 章

7 管理验证

“验证服务”为所有在 Access Manager 部署中安装的默认验证类型提供基于 Web 的用户界面。此界面在用户请求访问时显示登录要求屏幕（根据所调用的验证模块），为收集验证证书提供动态和可自定义的方法。该界面使用 Sun Java System™ 应用程序框架（有时称为 *JATO*）创建，该框架是一个用来帮助开发者创建功能性 Web 应用程序的 Java 2 Enterprise Edition (J2EE) 演示框架。

配置验证

本节介绍如何为部署配置验证。第一小节概述默认验证模块类型并提供所有必需的预配置说明。可以为领域、用户、角色等配置同一验证模块类型的多个配置实例。另外，可以添加验证链，这样验证必须满足多个实例的条件后才能成功。本节包括：

验证模块类型

验证模块是一个插件，可以收集用户信息（如用户 ID 和密码），然后根据数据库中的条目检查信息。如果用户提供的信息满足验证条件，则会批准该用户访问请求的资源。如果用户提供的信息不满足验证条件，则会拒绝该用户访问请求的资源。安装 Access Manager 时会随附 15 种类型的验证模块：

- 第 77 页中的 “LDAP”
- 第 78 页中的 “成员资格”
- 第 78 页中的 “MSISDN”
- 第 78 页中的 “RADIUS”
- 第 79 页中的 “SafeWord”
- 第 80 页中的 “SAML”
- 第 80 页中的 “SecurID”
- 第 81 页中的 “Windows 桌面 SSO”
- 第 83 页中的 “Windows NT”
- 第 81 页中的 “UNIX”

注 – 某些验证模块类型需要预配置然后才能用作验证实例。如有必要，配置步骤会在模块类型说明中列出。

核心

默认情况下，Access Manager 提供了十五个不同的验证模块和一个核心验证模块。核心验证模块提供验证模块的整体配置。在添加和启用活动目录验证模块、匿名验证模块、基于证书的验证模块、HTTP Basic 验证模块、JDBC 验证模块、LDAP 验证模块等验证模块之前，必须先添加和启用核心验证模块。对于默认领域，核心验证模块和 LDAP 验证模块自动启用。

单击“高级属性”按钮，可显示能为领域进行定义的核心验证属性。全局属性不适用于领域，因而不会显示出来。

活动目录

活动目录验证模块以类似于 LDAP 模块的方式执行验证，但是使用 Microsoft 的 Active Directory™ 服务器（LDAP 验证模块使用 Directory Server）。尽管 LDAP 验证模块可以被配置为使用活动目录服务器，但此模块允许在同一个领域下存在 LDAP 和活动目录验证。

注 – 对于此版本，活动目录验证模块仅支持用户验证。仅在 LDAP 验证模块中支持密码策略。

匿名

默认情况下，如果已启用此模块，则用户可以作为匿名用户登录 Access Manager。通过配置“有效匿名用户列表”属性，也可以为此模块定义一列匿名用户。允许匿名访问意味着无需提供密码即可访问该服务器。匿名访问可以限于特定的访问类型（例如，读取访问或搜索访问）、特定的子树或目录中的特定条目。

证书

基于证书的验证涉及到使用个人数字证书 (PDC) 确定用户的身份和验证用户。可以将 PDC 配置为要求用户提供的证书与 Directory Server 中存储的 PDC 相同，并且根据证书撤销列表进行验证。

将基于证书的验证模块添加到领域之前，需要完成许多操作。首先，需要确保与 Access Manager 一起安装的 Web 容器正常运行，并配置此 Web 容器使其适用于基于证书的验证。启用基于证书的模块之前，请参阅《*Sun ONE Web Server 6.1* 管理员指南》中的第 6 章“使用证书和密钥”，了解有关 Web 服务器的初始配置步骤。可以在以下位置找到此文档：

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

或参阅以下位置的 *Sun ONE Application Sever Administrator's Guide to Security*：

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

注 – 使用基于证书的模块进行验证的用户必须请求用户浏览器的 PDC。具体说明各不相同，视使用的浏览器而定。有关详细信息，请参阅浏览器的文档。

要添加此模块，必须作为领域管理员登录 Access Manager，将 Access Manager 和 Web 容器配置为 SSL，并且启用客户机验证。有关详细信息，请参阅第 3 章。

HTTP Basic

此模块使用基本验证，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。Access Manager 将检索用户名和密码，然后在内部根据 LDAP 验证模块验证用户。为使 HTTP Basic 正常工作，还必须添加 LDAP 验证模块（只添加 HTTP Basic 模块将无法正常工作）。用户成功进行验证后，可以在不提供用户名和密码的情况下重新进行验证。

JDBC

Java 数据库连接 (JDBC) 验证模块提供一种验证机制，允许 Access Manager 通过任何 SQL 数据库（提供 JDBC 技术辅助驱动程序）验证用户。可以直接通过 JDBC 驱动程序或 JNDI 连接池与 SQL 数据库连接。

注 – 此模块已在 MySQL4.0 和 Oracle 8i 上进行过测试。

LDAP

有了 LDAP 验证模块，用户登录时必须用特定用户 DN 和密码绑定至 LDAP 目录服务器。这是适用于所有基于领域的验证的默认验证模块。如果用户提供了 Directory Server 中的用户 ID 和密码，则建立并允许用户访问有效的 Access Manager 会话。对于默认领域，核心验证模块和 LDAP 验证模块自动启用

成员资格

成员资格验证的实现类似于个性化设置站点，如 my.site.com 或 mysun.sun.com。启用此模块时，用户可以在没有管理员帮助的情况下创建帐户并对其进行个性化设置。利用这个新帐户，用户可以作为已添加的用户来访问该服务。用户还可以访问作为授权数据和用户首选项保存在用户概要文件数据库中的查看器界面。

MSISDN

移动站集成服务数字网络 (MSISDN) 验证模块使用与设备（如移动电话）关联的移动用户 ISDN 来启用验证。它是一种非交互式模块。该模块检索用户 ISDN 并根据 Directory Server 对其进行验证，以查找与编号匹配的用户。

RADIUS

可以将 Access Manager 配置为与已安装的 RADIUS 服务器一起使用。如果企业中正在使用原有的 RADIUS 服务器进行验证，这样做很有用。RADIUS 验证模块的启用过程分为两个步骤：

1. 配置 RADIUS 服务器。

   有关详细说明，请参阅 RADIUS 服务器文档。

2. 注册和启用 RADIUS 验证模块。

使用 Sun Java System Application Server 配置 RADIUS

默认情况下，当 RADUIS 客户机与其服务器建立套接字连接时，Application Server 的 server.policy 文件中只允许 SocketPermission 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

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

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

| -portnumberportnumber-portnumber
```

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

端口（或端口范围）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。

侦听操作仅在与本地主机一起使用时才有意义。存在其他任意操作时，都暗含**解析**（解析主机/IP 名称服务查找）操作。

例如，当创建 SocketPermission 时，请注意如果将以下权限授予某个代码，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

可以配置 Access Manager 使其处理发送到 Secure Computing 的 SafeWord™ 或 SafeWord PremierAccess™ 验证服务器的 SafeWord 验证请求。Access Manager 提供 SafeWord 验证的客户机部分。SafeWord 服务器可能位于安装 Access Manager 的系统或单独的系统中

使用 Sun Java System Application Server 配置 SafeWord

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

- 接受
- 连接
- 侦听
- 解析

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

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

portnumber | -portnumberportnumber-[portnumber]
```

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

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

侦听操作仅在与本地主机一起使用时才有意义。存在其他任意操作时，都暗含**解析**（解析主机/IP 名称服务查找）操作。

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

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

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

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

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

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

SAML

安全声明标记语言 (SAML) 验证模块接收和验证目标服务器上的 SAML 声明。SAML SSO 仅在目标机器上配置了此模块后才会工作，包括升级后（例如从 Access Manager 2004Q2 升级到 Access Manager 2005Q1）。

SecurID

可以对 Access Manager 进行配置，以处理 RSA 的 ACE/Server 验证服务器的 SecureID 验证请求。Access Manager 提供 SecurID 验证的客户机部分。ACE/Server 可能位于安装 Access Manager 的系统或单独的系统中。要验证本地管理员的用户 ID（请参阅 admintool (1M)），必须具备超级用户 (root) 访问权限。

SecurID 验证使用验证帮助器 amsecuridd，这是独立于主 Access Manager 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 Access Manager 安装为以 nobody 运行，或以超级用户 (root) 以外的用户 ID 运行，*AccessManager-base*/SUNWam/share/bin/amsecuridd 进程必须仍以超级用户身份操作。有关 amsecuridd 帮助器的详细信息，请参阅第 20 章。

注 – 在此发行版本的 Access Manager 中，SecurID 验证模块不适用于 Linux 或 Solaris x86 平台，因此不能在这两个平台上注册、配置或启用。它仅适用于 SPARC 系统。

UNIX

可以配置 Access Manager 使其按照安装了 Access Manager 的 Solaris 或 Linux 系统已知的 Unix 用户 ID 和密码来处理验证请求。尽管 Unix 验证只有一个领域属性和几个全局属性，仍有一些面向系统的注意事项。要验证本地管理员的用户 ID（请参阅 `admintool` (1M)），必须具备超级用户 (root) 访问权限。

Unix 验证使用验证帮助器 `amunixd`，这是独立于主 Access Manager 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 Access Manager 只有一个 Unix 帮助器用于其所有领域。

如果将 Access Manager 安装为以 `nobody` 运行，或以超级用户外 (root) 以外的用户 ID 运行，*AccessManager-base*`/SUNWam/share/bin/amunixd` 进程必须仍以超级用户身份操作。Unix 验证模块通过打开到 `localhost:58946` 的套接字调用 `amunixd` 守护进程以侦听 Unix 验证请求。要在默认端口上运行 `amunixd` 帮助器进程，请输入以下命令：

```
./amunixd
```

要在非默认端口上运行 `amunixd`，请输入以下命令：

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

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

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

Windows 桌面 SSO

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

用户通过 SPNEGO（简单且受保护的 GSS-API 协商机制）协议向 Access Manager 提交 Kerberos 令牌。要通过此验证模块执行基于 Kerberos 的 Access Manager 单点登录，用户必须在客户机端支持 SPNEGO 协议以验证本身。一般而言，支持此协议的任何用户应该都能使用此模块验证 Access Manager。根据客户机端令牌的可用性，此模块提供 SPENGO 令牌或 Kerberos 令牌（这两种情况下协议是相同的）。 在 Windows 2000（或更高版本）上运行的 Microsoft Internet Explorer（5.01 或更高版本）当前支持此协议。此外，Solaris（9 和 10）上的 Mozilla 1.4 支持 SPNEGO，但返回的令牌只有一个 KERBEROS 令牌，因为 SPNEGO 在 Solaris 上不受支持。

注 – 必须使用 JDK 1.4 或更高版本利用 Kerberos V5 验证模块和 Java GSS API 的新功能，以执行此 SPNEGO 模块中基于 Kerberos 的 SSO。

Internet Explorer 的已知限制

如果在进行 WindowsDesktopSSO 验证时使用 Microsoft Internet Explorer 6.x，并且浏览器不能访问与 WindowsDesktopSSO 模块中配置的 (KDC) 领域匹配的用户 kerberos/SPNEGO 令牌，则浏览器在验证 WindowsDesktopSSO 模块失败后无法对其他模块实施正确的行为。问题的直接原因是：在 Internet Explorer 验证 WindowsDesktopSSO 模块失败后，浏览器若未重新启动，将无法传送回叫（其他模块的）给 Access Manager，即使系统提示该回叫。因此，WindowsDesktopSSO 后的所有模块都将因无效的用户证书而失败。

相关信息，请参阅以下文档：

http://support.microsoft.com/default.aspx?scid=kb;en-us;308074
(http://support.microsoft.com/default.aspx?scid=kb;en-us;308074)

http://www.wedgetail.com/jcsi/sso/doc/guide/troubleshooting.html#ieNTLM
(http://support.microsoft.com/default.aspx?scid=kb;en-us;308074)

配置 Windows 桌面 SSO

启用 Windows 桌面 SSO 验证分为两个步骤：

1. 在 Windows 2000 域控制器中创建用户。
2. 设置 Internet Explorer。

▼ 在 Windows 2000 域控制器中创建用户

1 在域控制器中，为 Access Manager 验证模块创建用户帐户。

a. 从“开始”菜单中，转至“程序”>“管理工具”。

b. 选择“活动目录用户”和“计算机”。

c. 以 Access Manager 主机名作为用户 ID（登录名）创建新用户。Access Manager 主机名不应该包含域名。

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

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

hostname.host.keytab

ktpass -princ HTTP/hostname.domainname@DCDOMAIN -pass

password -mapuser userName-out hostname

.HTTP.keytab
```

ktpass 命令接受以下参数：

hostname。运行 Access Manager 的主机名（不含域名）。

domainname。Access Manager 的域名。

DCDOMAIN。域控制器的域名。它可能与 Access Manager 域名不同。

password。用户帐户的密码。请确保密码正确，因为 ktpass 不校验密码。

userName。用户帐户 ID。它应与主机名相同。

注 – 确保两个键表文件都已安全保管。

服务模板的值应与以下示例类似：

服务负责人： `HTTP/machine1.EXAMPLE.COM@ISQA.EXAMPLE.COM`

Keytab 文件名：`/tmp/machine1.HTTP.keytab`

Kerberos 领域： `ISQA.EXAMPLE.COM`

Kerberos 服务器名：`machine2.EXAMPLE.com`

返回带有域名的负责人：`false`

验证级别： `22`

3 重新启动服务器。

▼ 设置 Internet Explorer

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

1 在“工具”菜单中，转至“Internet 选项”>“高级”/”安全”>“安全”。

2 选择“集成的 Windows 验证”选项。

3 转至“安全”>“本地 Intranet”。

a. 选择“自定义级别”。在“用户验证/登录”面板中，选择“只在 Intranet 区域自动登录”选项。

b. 转到“站点”并选择所有选项。

c. 单击“高级”，将 Access Manager 添加到本地区域（如果尚未添加）。

Windows NT

可以将 Access Manager 配置为与已安装的 Windows NT /Windows 2000 server 一起使用。Access Manager 提供 NT 验证的客户机部分。

1. 配置 NT 服务器。有关详细信息，请参阅 Windows NT server 文档。

2. 在添加和启用 Windows NT 验证模块之前，必须获取并安装 Samba 客户机，以与 Solaris 系统上的 Access Manager 进行通信。

安装 Samba 客户机

要激活 Windows NT 验证模块，必须下载 Samba 客户机2.2.2 并安装到以下目录：

```
AccessManager-base/SUNWam/bin
```

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

Red Hat Linux 随 Samba 客户机一起发行，它位于以下目录：

```
/usr/bin
```

为了使用 Windows NT 验证模块为 Linux 进行验证，请将客户机二进制文件复制到以下 Access Manager 目录：

AccessManager-base`/sun/identity/bin`

注 – 如果有多个界面，则需要额外配置。`smb.conf` 文件中的配置可以设置多个界面，以便传递到 `mbclient`。

验证模块实例

可以根据默认验证模块为领域创建多个验证模块实例。可以添加同一个验证模块的多个单独配置的实例。

▼ 创建新的验证模块实例

1 单击要为其添加新的验证模块实例的领域的名称。

2 选择“验证”选项卡。

注 – “管理员验证配置”按钮只能为管理员定义验证服务。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。在访问 Access Manager 控制台时，将使用该属性中配置的模块。

---

3 在“模块实例”列表中单击“新建”。

4 输入验证模块实例的名称。名称必须唯一。

5 选择领域验证模块的类型。

6 单击“创建”。

7 单击新建的模块实例名，并编辑该模块的属性。有关每种模块类型的属性的定义，请参阅联机帮助中的“验证”部分。

8 重复执行这些步骤可以添加多个模块实例。

验证链

可以配置一个或多个验证模块，用户必须将验证证书传递到这些验证模块中。这称为验证链。 Access Manager 的验证链是通过使用集成在验证服务中的 JAAS 框架实现的。模块链在“验证配置”服务下配置。

▼ 创建新的验证链

1 单击要为其添加新的验证链的领域的名称。

2 选择“验证”选项卡。

3 在“验证链”列表中单击“新建”。

4 输入验证链名称。

5 单击“创建”。

6 单击“添加”，定义您要在链里包含的验证模块实例。可以从“ 实例 ”列表中选择模块实例名完成此步骤。此列表中所显示的模块实例名都是在“模块实例”属性中创建的。

7 为验证链选择标准。这些标志建立了其定义的验证模块的执行标准。执行具有层次结构。“ 必需 ”位于最高层，“ 可选 ”位于最底层：

必要　要求模块实例必须成功。如果验证成功，将继续“验证链”列表中的下一个验证模块。如果验证失败，控制立即返回到应用程序（不继续“验证链”列表中的下一个验证模块）。

必需　要求对此模块的验证必须成功。如果链中的任一必需模块验证失败，则整个验证链将最终失败。然而，无论任一必需模块的验证是成功或失败，都将继续链中的下一个模块。

充足　不要求模块实例必须成功。如果验证成功，则立即返回到应用程序（不继续模块实例列表中的下一个验证模块）。如果验证失败，将继续“验证链”列表中的下一个验证模块。

可选　不要求模块实例必须成功。无论验证成功或失败，都将继续“验证链”列表中的下一个验证模块。

8　输入验证链的选项。这启用了模块的其他选项，格式为“关键字=值”对。多个选项之间用空格分隔。

9　定义以下属性：

成功登录 URL　指定用户在验证成功后，重新指向的 URL。

登录失败 URL　指定用户在验证失败后，重新指向的 URL。

验证后期处理类　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。

10　单击“保存”。

验证类型

“验证服务”提供了几种不同的验证方法。可通过指定登录 URL 参数或通过验证 API 来使用这些不同的验证方法《Sun Java System Access Manager 7 2005Q4 Developer’s Guide》中的第 5 章 “Using Authentication APIs and SPIs”一书的第 5 章，“Using Authentication APIs and SPIs”）。在能够配置验证模块之前，必须先修改核心验证服务属性“领域验证模块”以包含特定的验证模块名称。

验证配置服务用于定义以下任一验证类型的验证模块：

- 第 88 页中的 “基于领域的验证”
- 第 90 页中的 “基于组织的验证”
- 第 92 页中的 “基于角色的验证”
- 第 95 页中的 “基于服务的验证”
- 第 97 页中的 “基于用户的验证”
- 第 99 页中的 “基于验证级别的验证”
- 第 101 页中的 “基于模块的验证”

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。

验证类型如何确定访问

对于每种方法，用户验证都可能通过或失败。一旦确定，每种方法都遵守这一过程。步骤 1 到步骤 3 接着成功的验证执行；步骤 4 接着成功或失败的验证执行。

1. Access Manager 确认是否在 Directory Server 数据存储库中定义了验证的用户以及概要文件是否处于活动状态。

“核心验证”模块中的“用户概要文件”属性可以定义为**必需**、**动态**、**随用户别名动态变换**或**忽略**。在成功的验证之后，Access Manager 确认是否在 Directory Server 数据存储库中定义了验证的用户。如果“用户概要文件”值为**必需**，则确认用户概要文件是否处于活动状态。（这是默认情况。）如果“用户概要文件”是**动态配置**，“验证服务”将在 Directory Server 数据存储库中创建用户概要文件。如果“用户概要文件”被设置成**忽略**，将不进行用户验证。

2. 完成验证后期处理 SPI 的执行。

   “核心验证模块”包含一个“验证后期处理类”属性，该属性可以把验证后期处理类的名称作为自己的值。`AMPostAuthProcessInterface` 是后期处理接口。它可以在验证成功、验证失败或注销后执行。

3. 以下属性会被添加或更新到会话标记中，并且用户会话会被激活。

   领域。这是用户所属领域的 DN。

   负责人。这是用户的 DN。

   多个负责人。这是用户已经验证的名称的列表。（此属性可以有多个值，各值之间以管道符分隔。）

   用户 **ID**。这是模块返回的用户 DN，如果模块不是“LDAP”或“成员资格”，则为用户名。（所有的“负责人”必须映射到同一用户。用户 ID 是它们映射到的用户 DN。）

   注 – 该属性可能是一个非 DN 值。

   UserToken。这是一个用户名。（所有的“负责人”必须映射到同一用户。UserToken 是它们映射到的用户名。）

   主机。这是客户机的主机名或 IP 地址。

   authLevel。这是用户已经验证的最高级别。

   AuthType。这是用户已经验证的验证模块的管道符分隔列表（例如`module1|module2|module3`）。

   clientType。这是客户机浏览器的设备类型。

   语言环境。这是客户机的语言环境。

   字符集。这是为客户机确定的字符集。

   角色。仅适用于基于角色的验证，这是用户所属的角色。

   服务。仅适用于基于服务的验证，这是用户所属的服务。

4. 验证成功或失败后，会在该 URL 中查找信息，以重定向用户。

   URL 重定向可以是一个 Access Manager 页面或 URL。重定向取决于 Access Manager 根据验证方法查找重定向的优先顺序，以及验证是成功还是失败。此顺序在以下验证方法章节的 URL 重定向部分有详细描述。

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领域中，以便可以为角色、领域或用户进行配置。添加验证配置服务时，请确保添加一个验证模块，例如 LDAP - REQUIRED。

基于领域的验证

此验证方法允许用户向领域或子领域进行验证。这是 Access Manager 的默认验证方法。通过把“核心验证”模块注册到领域，并定义“领域验证配置”属性，可以设置领域的验证方法。

基于领域的验证登录 URL

通过在“用户界面登录 URL”中定义 `realm` 参数或 `domain` 参数可以指定验证的领域。请求验证的领域按优先级顺序由以下值确定：

1. `domain` 参数。
2. `realm` 参数。
3. “管理服务”中的 `DNS` **别名**属性的值。

   在调用正确的领域后，可以通过“核心验证服务”中的“领域验证配置”属性获取将验证用户的验证模块。用于指定和启动基于领域的验证的登录 URL 是：

   ```
   http://server_name.domain_name:port/amserver/UI/Login

   http://server_name.domain_name:port/amserver/UI/Login?domain=domain_name

   http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name
   ```

   如果没有定义参数，将由服务器主机和登录 URL 中指定的域确定领域。

基于领域的验证重定向 URL

在基于组织的验证成功或失败后，Access Manager 会查找信息以重定向用户。下面是应用程序查找这些信息的优先顺序。

成功的基于领域的验证重定向 URL

成功的基于领域的验证重定向 URL 通过按优先顺序检查以下位置来确定：

1. 验证模块设置的 URL。
2. `goto` 登录 URL 参数设置的 URL。
3. `clientType` 自定义文件中为用户概要文件 (`amUser.xml`) 的 `iplanet-am-user-success-url` 属性设置的 URL。

4. clientType 自定义文件中为用户角色条目的 iplanet-am-auth-login-success-url 属性设置的 URL。
5. clientType 自定义文件中为用户领域条目的 iplanet-am-auth-login-success-url 属性设置的 URL。
6. clientType 自定义文件中为 iplanet-am-auth-login-success-url 属性设置的作为全局默认值的 URL。
7. 用户概要文件 (amUser.xml) 的 iplanet-am-user-success-url 属性中设置的 URL。
8. 用户角色条目的 iplanet-am-auth-login-success-url 属性中设置的 URL。
9. 用户领域条目的 iplanet-am-auth-login-success-url 属性中设置的 URL。
10. iplanet-am-auth-login-success-url 属性中设置的作为全局默认值的 URL。

失败的基于领域的验证重定向 URL

失败的基于领域的验证重定向 URL 通过按下列顺序检查以下位置来确定：

1. 验证模块设置的 URL。
2. gotoOnFail 登录 URL 参数设置的 URL。
3. clientType 自定义文件中为用户条目 (amUser.xml) 的 iplanet-am-user-failure-url 属性设置的 URL。
4. clientType 自定义文件中为用户角色条目的 iplanet-am-user-failure-url 属性设置的 URL。
5. clientType 自定义文件中为用户领域条目的 iplanet-am-user-failure-url 属性设置的 URL。
6. clientType 自定义文件中为 iplanet-am-auth-login-failure-url 属性设置的作为全局默认值的 URL。
7. 为用户条目 (amUser.xml) 的 iplanet-am-user-failure-url 属性设置的 URL。
8. 为用户角色条目的 iplanet-am-auth-login-failure-url 属性设置的 URL。
9. 为用户领域条目的 iplanet-am-auth-login-failure-url 属性设置的 URL。
10. 为 iplanet-am-auth-login-failure-url 属性设置的作为全局默认值的 URL。

配置基于领域的验证

领域的验证模块是在首次将核心验证服务添加到该领域时设置的。

▼ 配置领域的验证属性

1 找到要为其添加“验证链”的领域。

2 单击“验证”选项卡。

3. **从下拉菜单中选择“默认验证链”。**
4. **从下拉菜单中选择“管理员验证链”。如果需要将管理员的验证模块与最终用户的验证模块区别开来，则可以使用该属性。默认验证模块为 LDAP。**
5. **定义验证链之后，单击“保存”。**

基于组织的验证

此验证类型只适用于在“传统”模式下安装的 Access Manager 部署。

此验证方法允许用户向组织或子组织进行验证。这是 Access Manager 的默认验证方法。通过把“核心验证”模块注册到组织，并定义“组织验证配置”属性，可以设置组织的验证方法。

基于组织的验证登录 URL

通过在“用户界面登录 URL”中定义 `org` 参数或 `domain` 参数可以指定验证的组织。请求验证的组织按优先顺序由以下值确定：

1. `domain` 参数。
2. `org` 参数。
3. “管理服务”中的 `DNS` **别名**（组织别名）属性值。

   在调用正确的组织后，可以通过核心验证服务中的“组织验证配置”属性获取将验证用户的验证模块。用来指定和启动基于组织的验证的登录 URL 是：

   ```
   http://server_name.domain_name:port/amserver/UI/Login

   http://server_name.domain_name:port/amserver/UI/Login?domain=domain_name

   http://server_name.domain_name:port/amserver/UI/Login?org=org_name
   ```

   如果没有定义参数，将由服务器主机和登录 URL 指定的域确定组织。

基于组织的验证重定向 URL

在基于组织的验证成功或失败后，Access Manager 会查找信息以重定向用户。下面是应用程序查找这些信息的优先顺序。

成功的基于组织的验证重定向 URL

成功的基于组织的验证重定向 URL 通过按优先顺序检查以下位置来确定：

1. 验证模块设置的 URL。
2. `goto` 登录 URL 参数设置的 URL。

3. clientType 自定义文件中为用户概要文件 (amUser.xml) 的 iplanet-am-user-success-url 属性设置的 URL。
4. clientType 自定义文件中为用户角色条目的 iplanet-am-auth-login-success-url 属性设置的 URL。
5. clientType **自定义文件中为用户组织条目的** iplanet-am-auth-login-success-url **属性设置的** URL。
6. clientType 自定义文件中为 iplanet-am-auth-login-success-url 属性设置的作为全局默认值的 URL。
7. 用户概要文件 (amUser.xml) 的 iplanet-am-user-success-url 属性中设置的 URL。
8. 用户角色条目的 iplanet-am-auth-login-success-url 属性中设置的 URL。
9. 用户组织条目的 iplanet-am-auth-login-success-url 属性中设置的 URL。
10. iplanet-am-auth-login-success-url 属性中设置的作为全局默认值的 URL。

失败的基于组织的验证重定向 URL

失败的基于组织的验证重定向 URL 通过按以下顺序检查以下位置来确定 :

1. 验证模块设置的 URL。
2. gotoOnFail 登录 URL 参数设置的 URL。
3. clientType 自定义文件中为用户条目 (amUser.xml) 的 iplanet-am-user-failure-url 属性设置的 URL。
4. clientType 自定义文件中为用户角色条目的 iplanet-am-user-failure-url 属性设置的 URL。
5. clientType 自定义文件中为用户组织条目的 iplanet-am-auth-login-failure-url 属性设置的 URL。
6. clientType 自定义文件中为 iplanet-am-auth-login-failure-url 属性设置的作为全局默认值的 URL。
7. 为用户条目 (amUser.xml) 的 iplanet-am-user-failure-url 属性设置的 URL。
8. 为用户角色条目的 iplanet-am-auth-login-failure-url 属性设置的 URL。
9. 为用户组织条目的 iplanet-am-auth-login-failure-url 属性设置的 URL。
10. 为 iplanet-am-auth-login-failure-url 属性设置的作为全局默认值的 URL。

配置基于组织的验证

组织的验证模块是在首次将核心验证服务添加到该组织时设置的。

▼ 配置组织的验证属性

1. **找到要为其添加“验证链”的组织。**
2. **单击“验证”选项卡。**
3. **从下拉菜单中选择“默认验证链”。**
4. **从下拉菜单中选择“管理员验证链”。如果需要将管理员的验证模块与最终用户的验证模块区别开来，则可以使用该属性。默认验证模块为 LDAP。**
5. **定义验证链之后，单击“保存”。**

基于角色的验证

此验证方法允许用户向领域或子领域内的角色（静态或过滤）进行验证。

注 – “验证配置服务”在作为实例注册到角色以前，必须首先注册到领域。

验证要想成功，用户必须属于该角色，并且必须向为该角色配置的“验证配置服”实例中定义的每个模块进行验证。每个基于角色验证的实例均可指定下列属性：

冲突解决级别。此属性为可能包含相同用户的两个不同角色定义的验证配置服务实例设置优先级级别。例如，如果 `User1` 同时分配给 `Role1` 和 `Role2`，则可以为 `Role1` 设置较高的冲突解决级别。这样，当用户试图进行验证时，`Role1` 将优先进行成功或失败重定向以及验证后期处理。

验证配置。此属性定义为角色验证过程配置的验证模块。

登录成功 **URL**。此属性定义在验证成功后用户被重定向到的 URL。

登录失败 **URL**。此属性定义在验证失败后用户被重定向到的 URL。

验证后期处理类。此属性定义验证后期界面。

基于角色的验证登录 URL

通过定义 role 参数，可以在“用户界面登录 URL”中指定基于角色的验证。在调用正确的角色后，可以通过为角色定义的“验证配置服务”实例获取将要验证用户的验证模块。

用于指定和启动基于角色的验证的登录 URL 是：

```
http://server_name.domain_name:port/amserver/UI/Login?role=role_name
```

```
http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name&role=role_name
```

如果没有配置 realm 参数，将通过在登录 URL 中指定的服务器主机和域来确定角色所属的领域。

基于角色的验证重定向 URL

在基于角色的验证成功或失败后，Access Manager 会查找信息以重定向用户。下面是应用程序查找这些信息的优先顺序。

成功的基于角色的验证重定向 URL

成功的基于角色的验证重定向 URL 通过按以下顺序检查以下位置来确定：

1. 验证模块设置的 URL。
2. `goto` 登录 URL 参数设置的 URL。
3. `clientType` 自定义文件中为用户概要文件 (`amUser.xml`) 的 `iplanet-am-user-success-url` 属性设置的 URL。
4. `clientType` 自定义文件中为用户已经验证的角色的 `iplanet-am-auth-login-success-url` 属性设置的 URL。
5. `clientType` 自定义文件中为已验证用户的另一个角色条目的 `iplanet-am-auth-login-success-url` 属性设置的 URL。（如果以前的重定向 URL 失败，此选项是一个替代方法。）
6. `clientType` 自定义文件中为用户领域条目的 `iplanet-am-auth-login-success-url` 属性设置的 URL。
7. `clientType` 自定义文件中为 `iplanet-am-auth-login-success-url` 属性设置的作为全局默认值的 URL。
8. 用户概要文件 (`amUser.xml`) 的 `iplanet-am-user-success-url` 属性中设置的 URL。
9. 用户已验证角色的 `iplanet-am-auth-login-success-url` 属性中设置的 URL。
10. 已验证用户的另一个角色条目的 `iplanet-am-auth-login-success-url` 属性中设置的 URL。（如果以前的重定向 URL 失败，此选项是一个替代方法。）
11. 用户领域条目的 `iplanet-am-auth-login-success-url` 属性中设置的 URL。
12. `iplanet-am-auth-login-success-url` 属性中设置的作为全局默认值的 URL。

失败的基于角色的验证重定向 URL

失败的基于角色的验证重定向 URL 通过按以下顺序检查以下位置来确定：

1. 验证模块设置的 URL。
2. `goto` 登录 URL 参数设置的 URL。
3. `clientType` 自定义文件中为用户概要文件 (`amUser.xml`) 的 `iplanet-am-user-failure-url` 属性设置的 URL。

4. clientType 自定义文件中为用户已验证的角色的 iplanet-am-auth-login-failure-url 属性设置的 URL。
5. clientType 自定义文件中为已验证用户的另一个角色条目的 iplanet-am-auth-login-failure-url 属性设置的 URL。（如果以前的重定向 URL 失败，此选项是一个替代方法。）
6. clientType 自定义文件中为用户领域条目的 iplanet-am-user-failure-url 属性设置的 URL。
7. clientType 自定义文件中为 iplanet-am-auth-login-failure-url 属性设置的作为全局默认值的 URL。
8. 用户概要文件 (amUser.xml) 的 iplanet-am-user-failure-url 属性中设置的 URL。
9. 用户已验证角色的 iplanet-am-auth-login-failure-url 属性中设置的 URL。
10. 已验证用户的另一个角色的 iplanet-am-auth-login-failure-url 属性中设置的 URL。（如果以前的重定向 URL 失败，此选项是一个替代方法。）
11. 用户领域条目的 iplanet-am-auth-login-failure-url 属性中设置的 URL。
12. iplanet-am-auth-login-failure-url 属性中设置的作为全局默认值的 URL。

▼ 配置基于角色的验证

1 找到要在其中添加验证配置服务的领域（或组织）。

2 单击“主题”选项卡。

3 “过滤的角色”或“角色”。

4 选择要为其设置验证配置的角色。

如果“验证配置”服务还没有添加到此角色，请单击“添加”，选择“验证服务”，然后单击“下一步”。

5 从下拉菜单中选择要启用的“默认验证链”。

6 单击“保存”。

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

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

基于服务的验证

此验证方法允许用户向在领域或子领域中注册的特定服务或应用程序进行验证。服务在验证配置服务内配置成“服务实例”，并且与“实例名称”关联。验证要想成功，用户必须向为服务配置的验证配置服务实例中定义的每个模块进行验证。每个基于服务验证的实例均可指定下列属性：

验证配置。此属性定义为服务验证进程配置的验证模块。

登录成功 **URL**。此属性定义在验证成功后用户被重定向到的 URL。

登录失败 **URL**。此属性定义在验证失败后用户被重定向到的 URL。

验证后期处理类。此属性定义验证后期界面。

基于服务的验证登录 URL

通过定义 service 参数，可以在“用户界面登录 URL”中指定基于服务的验证。在调用服务后，可以通过为服务定义的“验证配置服务”实例获取将要验证用户的验证模块。

用于指定和启动基于服务的验证的登录 URL 是：

```
http://server_name.domain_name:port/amserver/UI/

Login?service=auth-chain-name
```

和

```
http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name&service=auth-chain-name
```

e

如果没有配置 `org` 参数，将通过在登录 URL 中指定的服务器主机和域来确定用户所属的领域。

基于服务的验证重定向 URL

在基于服务的验证成功或失败后，Access Manager 会查找信息以重定向用户。下面是应用程序查找这些信息的优先顺序。

成功的基于服务的验证重定向 URL

成功的基于服务的验证重定向 URL 通过按以下顺序检查以下位置来确定：

1. 验证模块设置的 URL。
2. `goto` 登录 URL 参数设置的 URL。

3. clientType 自定义文件中为用户概要文件 (amUser.xml) 的 iplanet-am-user-success-url 属性设置的 URL。
4. clientType 自定义文件中为用户已验证服务的 iplanet-am-auth-login-success-url 属性设置的 URL。
5. clientType 自定义文件中为用户角色条目的 iplanet-am-auth-login-success-url 属性设置的 URL。
6. clientType 自定义文件中为用户领域条目的 iplanet-am-auth-login-success-url 属性设置的 URL。
7. clientType 自定义文件中为 iplanet-am-auth-login-success-url 属性设置的作为全局默认值的 URL。
8. 用户概要文件 (amUser.xml) 的 iplanet-am-user-success-url 属性中设置的 URL。
9. 用户已验证服务的 iplanet-am-auth-login-success-url 属性中设置的 URL。
10. 用户角色条目的 iplanet-am-auth-login-success-url 属性中设置的 URL。
11. 用户领域条目的 iplanet-am-auth-login-success-url 属性中设置的 URL。
12. iplanet-am-auth-login-success-url 属性中设置的作为全局默认值的 URL。

失败的基于服务的验证的重定向 URL

失败的基于服务的验证重定向 URL 通过按以下顺序检查以下位置来确定 :

1. 验证模块设置的 URL。
2. goto 登录 URL 参数设置的 URL。
3. clientType 自定义文件中为用户概要文件 (amUser.xml) 的 iplanet-am-user-failure-url 属性设置的 URL。
4. clientType 自定义文件中为用户已验证服务的 iplanet-am-auth-login-failure-url 属性设置的 URL。
5. clientType 自定义文件中为用户角色条目的 iplanet-am-user-failure-url 属性设置的 URL。
6. clientType 自定义文件中为用户领域条目的 iplanet-am-user-failure-url 属性设置的 URL。
7. clientType 自定义文件中为 iplanet-am-auth-login-failure-url 属性设置的作为全局默认值的 URL。
8. 用户概要文件 (amUser.xml) 的 iplanet-am-user-failure-url 属性中设置的 URL。
9. 用户已验证服务的 iplanet-am-auth-login-failure-url 属性中设置的 URL。
10. 用户角色条目的 iplanet-am-auth-login-failure-url 属性中设置的 URL。
11. 用户领域条目的 iplanet-am-auth-login-failure-url 属性中设置的 URL。
12. iplanet-am-auth-login-failure-url 属性中设置的作为全局默认值的 URL。

▼ 配置基于服务的验证

服务的验证模块是在添加了验证配置服务之后设置的。为此，请执行以下步骤：

1. **选择要配置基于服务的验证的领域。**
2. **单击"验证"选项卡。**
3. **创建验证模块实例。**
4. **创建验证链。**
5. **单击"保存"。**
6. **要访问领域的基于服务的验证，请输入以下地址：**

   `http://`*`server_name.domain_name:port`*`/amserver/UI/Login?realm=`*`realm_name&service=auth-chain-name`*

基于用户的验证

此验证方法允许用户向专门为其配置的验证进程进行验证。这个过程被配置成用户概要文件中的"用户验证配置"属性值。验证要想成功，用户必须向定义的每个模块验证。

基于用户的验证登录 URL

通过定义 user 参数，可以在"用户界面登录 URL"中指定基于用户的验证。在调用正确的用户后，可以通过为用户定义的"用户验证配置"实例获取将要验证用户的验证模块。

用于指定和启动基于角色的验证的登录 URL 是：

```
http://server_name.domain_name:port/amserver/UI/Login?user=user_name
```

```
http://server_name.domain_name:port/amserver/UI/Login?org=org_name&user=user_name
```

如果没有配置 realm 参数，将通过登录 URL 中指定的服务器主机和域来确定角色所属的领域。

用户别名列表属性

在收到基于用户的验证请求时，验证服务会先验证用户是否为有效的用户，然后为其检索验证配置数据。如果有多个与用户登录 URL 参数值关联的有效用户概要文件，则所有配置文件都必须映射到指定的用户。可以在用户概要文件的用户别名属性

(iplanet-am-user-alias-list) 中指定属于该用户的其他配置文件。如果映射失败，将拒绝该用户进行有效的会话。例外情况是，如果用户之一是顶级管理员，则不进行用户映射验证，并且用户被授予顶级管理员权限。

基于用户的验证重定向 URL

在基于模块的验证成功或失败后，Access Manager 会查找信息以重定向用户。下面是应用程序查找这些信息的优先顺序。

成功的基于用户的验证重定向 URL

成功的基于用户的验证重定向 URL 通过按优先顺序检查以下位置来确定：

1. 验证模块设置的 URL。
2. goto 登录 URL 参数设置的 URL。
3. clientType 自定义文件中为用户概要文件 (amUser.xml) 的 iplanet-am-user-success-url 属性设置的 URL。
4. clientType 自定义文件中为用户角色条目的 iplanet-am-auth-login-success-url 属性设置的 URL。
5. clientType 自定义文件中为用户领域条目的 iplanet-am-auth-login-success-url 属性设置的 URL。
6. clientType 自定义文件中为 iplanet-am-auth-login-success-url 属性设置的作为全局默认值的 URL。
7. 用户概要文件 (amUser.xml) 的 iplanet-am-user-success-url 属性中设置的 URL。
8. 用户角色条目的 iplanet-am-auth-login-success-url 属性中设置的 URL。
9. 用户领域条目的 iplanet-am-auth-login-success-url 属性中设置的 URL。
10. iplanet-am-auth-login-success-url 属性中设置的作为全局默认值的 URL。

失败的基于用户的重定向 URL

失败的基于用户的验证重定向 URL 通过按以下顺序检查以下位置来确定：

1. 验证模块设置的 URL。
2. gotoOnFail 登录 URL 参数设置的 URL。
3. clientType 自定义文件中为用户条目 (amUser.xml) 的 iplanet-am-user-failure-url 属性设置的 URL。
4. clientType 自定义文件中为用户角色条目的 iplanet-am-user-failure-url 属性设置的 URL。
5. clientType 自定义文件中为用户领域条目的 iplanet-am-user-failure-url 属性设置的 URL。

6. clientType 自定义文件中为 iplanet-am-auth-login-failure-url 属性设置的作为全局默认值的 URL。
7. 为用户条目 (amUser.xml) 的 iplanet-am-user-failure-url 属性设置的 URL。
8. 为用户角色条目的 iplanet-am-auth-login-failure-url 属性设置的 URL。
9. 为用户领域条目的 iplanet-am-auth-login-failure-url 属性设置的 URL。
10. 为 iplanet-am-auth-login-failure-url 属性设置的作为全局默认值的 URL。

▼ 配置基于用户的验证

1 找到要在其中为用户配置验证的领域。

2 单击“主题”选项卡，然后单击“用户”。

3 单击所要修改的用户的名称。

将显示“用户概要文件”。

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服务配置文件中的“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。

---

4 在“用户验证配置”属性中，选择您想要使用的验证链。

5 单击“保存”。

基于验证级别的验证

每个验证模块均可以与其验证级别的整数值相关联。单击“服务配置”中验证模块的属性箭头，然后更改模块的“验证级别”属性相应的值，可以指定验证级别。用户通过验证，获得了对一个或多个验证模块的访问权时，验证级别越高，则它为该用户定义的信任级别就越高。

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，使用户通过具有相应验证级别的验证模块进行访问。

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。如果只找到了一个匹配的模块，则会直接显示该验证模块的登录页。

此验证方法可让管理员指定验证身份的模块的安全级别。每个验证模块都有单独的“验证级别”属性，此属性的值可以定义为任何有效的整数。利用基于验证级别的验证，验证服务会显示一个模块登录页面，其中有一个菜单，包含验证级别等于或大于登录 URL 参数所指定的值的验证模块。用户可以从提供的列表中选择模块。在用户选择模块之后，剩余的进程取决于基于模块的验证。

基于验证级别的验证登录 URL

通过定义 authlevel 参数，可以在“用户界面登录 URL”中指定基于验证级别的验证。在调用含有相关模块列表的登录屏幕之后，用户必须选择一个用于验证的模块。用来指定和启动基于验证级别的验证的登录 URL 是：

```
http://server_name.domain_name:port/amserver/UI/Login?authlevel=authentication_level
```

和

```
http://server_name.domain_name:port/amserver/UI/
```

```
Login?realm=realm_name&authlevel=authentication_level
```

如果没有配置 `realm` 参数，将通过登录 URL 中指定的服务器主机和域来确定用户所属的领域。

基于验证级别的验证重定向 URL

在基于验证级别的验证成功或失败后，Access Manager 会查找信息以重定向用户。下面是应用程序查找这些信息的优先顺序。

成功的基于验证级别的验证重定向 URL

成功的基于验证级别的验证重定向 URL 通过按优先顺序检查以下位置来确定：

1. 验证模块设置的 URL。
2. `goto` 登录 URL 参数设置的 URL。
3. `clientType` 自定义文件中为用户概要文件 (`amUser.xml`) 的 `iplanet-am-user-success-url` 属性设置的 URL。
4. `clientType` 自定义文件中为用户角色条目的 `iplanet-am-auth-login-success-url` 属性设置的 URL。

5. clientType 自定义文件中为用户领域条目的 iplanet-am-auth-login-success-url 属性设置的 URL。
6. clientType 自定义文件中为 iplanet-am-auth-login-success-url 属性设置的作为全局默认值的 URL。
7. 用户概要文件 (amUser.xml) 的 iplanet-am-user-success-url 属性中设置的 URL。
8. 用户角色条目的 iplanet-am-auth-login-success-url 属性中设置的 URL。
9. 用户领域条目的 iplanet-am-auth-login-success-url 属性中设置的 URL。
10. iplanet-am-auth-login-success-url 属性中设置的作为全局默认值的 URL。

失败的基于验证级别的验证重定向 URL

失败的基于验证级别的验证重定向 URL 通过按以下顺序检查以下位置来确定 :

1. 验证模块设置的 URL。
2. gotoOnFail 登录 URL 参数设置的 URL。
3. clientType 自定义文件中为用户条目 (amUser.xml) 的 iplanet-am-user-failure-url 属性设置的 URL。
4. clientType 自定义文件中为用户角色条目的 iplanet-am-user-failure-url 属性设置的 URL。
5. clientType 自定义文件中为用户领域条目的 iplanet-am-user-failure-url 属性设置的 URL。
6. clientType 自定义文件中为 iplanet-am-auth-login-failure-url 属性设置的作为全局默认值的 URL。
7. 为用户条目 (amUser.xml) 的 iplanet-am-user-failure-url 属性设置的 URL。
8. 为用户角色条目的 iplanet-am-auth-login-failure-url 属性设置的 URL。
9. 为用户领域条目的 iplanet-am-auth-login-failure-url 属性设置的 URL。
10. 为 iplanet-am-auth-login-failure-url 属性设置的作为全局默认值的 URL。

基于模块的验证

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“领域验证模块”以包含该验证模块名称。如果此属性中不包含该验证模块名称，则当用户尝试进行验证时，将会显示“验证模块被拒绝”页面。

此验证方法允许用户指定用来进行验证的模块。指定的模块必须向用户正在访问的领域或子领域注册。这是在领域的“核心验证服务”的“领域验证模块”属性中进行配置的。在收到基于模块的验证请求时，验证服务会验证模块是否按要求正确配置，如果该模块未定义，将拒绝用户访问。

基于模块的验证登录 URL

通过定义 module 参数，可以在“用户界面登录 URL”中指定基于模块的验证。用来指定和启动基于模块的验证的登录 URL 是：

```
http://server_name.domain_name:port/amserver/UI/Login?module=authentication_module_name
```

```
http://server_name.domain_name:port/amserver/UI/
```

```
Login?org=org_name&module=authentication_module_name
```

如果没有配置 `org` 参数，将通过登录 URL 中指定的服务器主机和域来确定用户所属的领域。

基于模块的验证重定向 URL

在基于模块的验证成功或失败后，Access Manager 会查找信息以重定向用户。下面是应用程序查找这些信息的优先顺序。

成功的基于模块的验证重定向 URL

成功的基于模块的验证重定向 URL 通过按优先顺序检查以下位置来确定：

1. 验证模块设置的 URL。
2. `goto` 登录 URL 参数设置的 URL。
3. `clientType` 自定义文件中为用户概要文件 (`amUser.xml`) 的 `iplanet-am-user-success-url` 属性设置的 URL。
4. `clientType` 自定义文件中为用户角色条目的 `iplanet-am-auth-login-success-url` 属性设置的 URL。
5. `clientType` 自定义文件中为用户领域条目的 `iplanet-am-auth-login-success-url` 属性设置的 URL。
6. `clientType` 自定义文件中为 `iplanet-am-auth-login-success-url` 属性设置的作为全局默认值的 URL。
7. 用户概要文件 (`amUser.xml`) 的 `iplanet-am-user-success-url` 属性中设置的 URL。
8. 用户角色条目的 `iplanet-am-auth-login-success-url` 属性中设置的 URL。
9. 用户领域条目的 `iplanet-am-auth-login-success-url` 属性中设置的 URL。
10. `iplanet-am-auth-login-success-url` 属性中设置的作为全局默认值的 URL。

失败的基于模块的验证重定向 URL

失败的基于模块的验证重定向 URL 通过按以下顺序检查以下位置来确定：

1. 验证模块设置的 URL。
2. `gotoOnFail` 登录 URL 参数设置的 URL。
3. `clientType` 自定义文件中为用户条目 (`amUser.xml`) 的 `iplanet-am-user-failure-url` 属性设置的 URL。
4. `clientType` 自定义文件中为用户角色条目的 `iplanet-am-auth-login-failure-url` 属性设置的 URL。
5. `clientType` 自定义文件中为用户领域条目的 `iplanet-am-user-failure-url` 属性设置的 URL。
6. `clientType` 自定义文件中为 `iplanet-am-auth-login-failure-url` 属性设置的作为全局默认值的 URL。
7. 为用户角色条目的 `iplanet-am-auth-login-failure-url` 属性设置的 URL。
8. 为用户领域条目的 `iplanet-am-auth-login-failure-url` 属性设置的 URL。
9. 为 `iplanet-am-auth-login-failure-url` 属性设置的作为全局默认值的 URL。

用户界面登录 URL

在 Web 浏览器的地址栏中输入登录 URL 可访问“验证服务”用户界面。该 URL 是：

`http://`*AccessManager-root*`/`*.domain_name:port*` /`*service_deploy_uri*` /UI/Login`

注 – 在安装过程中，*service_deploy_uri* 被配置为 `amserver`。此默认服务部署 URI 将在本文档的全文中使用。

用户界面登录 URL 也可以附加登录 URL 参数来定义特定的验证方法或成功/失败的验证重定向 URL。

登录 URL 参数

URL 参数是附加在 URL 末尾的名称/值对。该参数以问号 (?) 开始，格式为 `name=value`。一个登录 URL 可以组合使用多个参数，如：

```
http://server_name.domain_name:port/amserver/UI/

Login?module=LDAP&locale=ja&goto=http://www.sun.com
```

如果存在多个参数，中间用与号 (&) 分隔。但组合必须遵守以下指导：

- 每个参数在一个 URL 中只能出现一次。例如，`module=LDAP&module=NT` 是不可计算的。
- `org` 参数和 `domain` 参数都可以确定登录领域。在这种情况下，登录 URL 中只能使用其中一个参数。如果同时使用两个参数且不指定优先级，将只有一个生效。
- 参数 `user`、`role`、`service`、`module` 和 `authlevel` 用于定义基于各自标准的验证模块。因此，登录 URL 中只能使用其中一个参数。如果同时使用多个参数且不指定优先级，将只有一个生效。

以下几节描述各参数，这些参数在附加至用户界面登录 URL 中并键入 Web 浏览器的地址栏中时，可获取不同的验证功能。

注 – 为简化在整个领域中分发验证 URL 和参数的过程，管理员可能会用简单的 URL 配置 HTML 页，该页面可链接到更复杂的登录 URL 以获取所有已配置的验证方法。

---

goto 参数

`goto=`*successful_authentication_URL* 参数覆写在“验证配置”服务的“登录成功 URL”中定义的值。当验证成功时，将链接到指定的 URL。`goto= logout_URL` 参数也可用于用户注销时链接到指定的 URL。成功的验证 URL 示例如下：

```
http://server_name.domain_name:port/amserver/

UI/Login?goto=http://www.sun.com/homepage.html
```

`goto` 注销 URL 的示例如下：

```
http://server_name.domain_name:port/amserver/

UI/Logout?goto=http://www.sun.com/logout.html.
```

注 – Access Manager 按优先顺序查找成功的验证重定向 URL。因为这些重定向 URL 及其顺序取决于验证方法，所以此顺序（和相关信息）将在“验证类型”部分中进行详细介绍。

---

gotoOnFail 参数

`gotoOnFail=failed_authentication_URL` 参数覆写在“验证配置”服务的“登录失败 URL”中定义的值。如果用户验证失败，将链接到指定的 URL。例如，`gotoOnFail URL` 可能是 `http://`*server_name.domain_name*`:`*port*`/amserver/UI/Login?gotoOnFail=http://www.sun.com/auth_fail.html`。

注 – Access Manager 按优先顺序查找失败的验证重定向 URL。因为这些重定向 URL 及其顺序取决于验证方法，所以此顺序（和相关信息）将在“验证类型”部分中进行详细介绍。

realm 参数

`org=`*realmName* 参数允许用户作为指定领域中的用户进行验证。

注 – 尚未成为指定领域成员的用户如果试图使用 `realm` 参数进行验证，会收到一则错误消息。如果以下所有条件均成立，则可在 Directory Server 中动态创建用户概要文件：

- 核心验证服务中的“用户概要文件”属性必须设置为**动态**或**随用户别名动态变换**。
- 用户必须成功通过所需模块的验证。
- 该用户在 Directory Server 中还没有配置文件。

使用此参数，将会显示正确的登录页面（基于领域及其语言环境设置）。如果未设置此参数，默认值是顶层领域。例如，`org` URL 可以是：

```
http://server_name.domain_name:port/amserver/UI/Login?realm=sun
```

org 参数

`org=`*orgName* 参数允许用户作为指定组织中的用户进行验证。

注 – 尚未成为指定域/组织成员的用户如果试图使用 `org` 参数进行验证，会收到一则错误消息。如果以下所有条件均成立，则可在 Directory Server 中动态创建用户概要文件：

- 核心验证服务中的“用户概要文件”属性必须设置为**动态**或**随用户别名动态变换**。
- 用户必须成功通过所需模块的验证。
- 该用户在 Directory Server 中还没有配置文件。

使用此参数，将会显示正确的登录页面（基于组织及其语言环境设置）。如果未设置此参数，默认值是顶层组织。例如，`org` URL 可以是：

```
http://server_name.domain_name:port/amserver/UI/Login?org=sun
```

user 参数

user=*userName* 参数强制使用在用户概要文件的“用户验证配置”属性中配置的模块进行验证。例如，某个用户的配置文件可能配置为使用“证书”模块进行验证，而另一个用户的配置文件可能配置为使用“LDAP”模块进行验证。添加此参数会将用户发送到其配置的验证进程，而非为其组织配置的方法。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?user=jsmith
```

role 参数

role=roleName 参数将用户发送至为指定角色配置的验证进程。尚未成为指定角色成员的用户如果试图用此参数进行验证，会收到一则错误消息。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?role=manager。
```

locale 参数

Access Manager 可为验证进程以及控制台本身显示本地化屏幕（翻译成英语以外的语言）。locale=*localeName* 参数使指定语言环境的优先级高于其他定义的语言环境。在以下位置按特定顺序搜索配置之后，客户机会显示登录语言环境：

1. 登录 URL 中的 locale 参数值

   locale=*localeName* 参数的值的优先级高于所有其他定义的语言环境。
2. 用户概要文件中定义的语言环境

   如果没有 URL 参数，则根据用户概要文件中“用户首选语言”属性的设置值显示语言环境。
3. HTTP 标题中定义的语言环境

   此语言环境由 Web 浏览器设置。
4. “核心验证服务”中定义的语言环境

   这是“核心验证”模块中“默认验证语言环境”属性的值。
5. “平台”服务中定义的语言环境

   这是“平台”服务中“平台语言环境”属性的值。

操作系统语言环境

从此等级派生的语言环境存储在用户的会话令牌中，Access Manager 使用此令牌只加载本地化验证模块。在成功验证之后，将使用用户概要文件中的“用户首选语言”属性定义的语言环境。如果没有设置，将继续使用验证所用的语言环境。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?locale=ja.
```

注 – 有关如何本地化屏幕文本和错误消息的信息可以在 Access Manager 中找到。

module 参数

`module=`*moduleName* 参数允许通过指定验证模块进行验证。可以指定任何模块，尽管它们必须首先在用户所属领域下注册并作为“核心验证”模块中该领域的验证模块之一被选定。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?module=Unix.
```

注 – 验证模块名称用在 URL 参数中时区分大小写。

service 参数

`service=`*serviceName* 参数允许用户通过服务的已配置验证模式进行验证。使用“验证配置”服务可以为不同的服务配置不同的验证方案。例如，一个联机薪金应用程序可能需要使用更安全的“证书验证”模块进行验证，而一个领域的员工目录应用程序可能只需要“LDAP 验证”模块。每个服务的验证模式都可以进行配置和命名。例如：

`http://`*server_name.domain_name*`:port/amserver/UI/Login?service=sv1.`

注 – “验证配置”服务用来为基于服务的验证定义方案。

arg 参数

`arg=`*newsession* 参数用于终止用户的当前会话并开始一个新会话。“验证服务”将销毁用户的现有会话标记，通过一个请求执行新的登录。此选项通常用于“匿名验证”模块。用户首先使用匿名会话进行验证，然后单击注册或登录链接。例如：

`http://`*server_name.domain_name*`:port/amserver/UI/Login?arg=newsession.`

authlevel 参数

`authlevel=`*value* 参数告知“验证服务”调用验证级别等于或大于指定验证级别值的模块。每个验证模块都定义了一个固定整数的验证级别。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?authlevel=1.
```

注 – “验证级别”设置在特定于每个模块的概要文件中。

domain 参数

此参数允许用户登录到标识为指定域的领域。指定域必须与领域配置文件的“域名”属性中定义的值相匹配。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?domain=sun.com.
```

注 – 尚未成为指定域/领域成员的用户如果试图使用 `org` 参数进行验证，会收到一则错误消息。如果以下所有条件均成立，则可在 Directory Server 中动态创建用户概要文件：

- 核心验证服务中的“用户概要文件”必须设置为**动态**或**随用户别名动态变换**。
- 用户必须成功通过所需模块的验证。
- 该用户在 Directory Server 中还没有配置文件。

iPSPCookie 参数

`iPSPCookie=yes` 参数允许用户使用持久 cookie 登录。当浏览器窗口关闭以后，持久 cookie 继续存在。要使用此参数，用户所登录的领域必须在其“核心验证”模块中启用“持久 Cookie”。一旦用户进行了验证并关闭了浏览器，用户可以使用新的浏览器会话登录并被定向至控制台而无需重新验证。这将一直有效，直到“核心服务”中指定的“持久 Cookie 最长时间”到期为止。例如：

```
http://server_name.domain_name:port/amserver/UI/Login?org=example&iPSPCookie=yes
```

IDTokenN 参数

此参数选项允许用户以 URL 或 HTML 形式传送验证证书。用户可使用 `IDTokenN=`*value* 参数通过验证，而无需访问“验证服务用户界面”。此进程称为零页面登录。零页面登录仅适用于使用一个登录页面的验证模块。`IDToken0`、`IDToken1`、...、`IDTokenN` 的值映射到验证模块登录页面上的字段。例如，LDAP 验证模块可能使用 `IDToken1` 作为 `userID` 信息，并使用 `IDToken2` 作为密码信息。在这种情况下，LDAP 模块 IDTokenN URL 是：

```
http://server_name.domain_name:port/amserver/UI/
Login?module=LDAP&IDToken1=userID&IDToken2=password
```

（如果 LDAP 为默认验证模块，则可以省略 `module=LDAP`。）

对于匿名验证，登录 URL 参数是：

`http://`*server_name.domain_name:port*`/amserver/UI/Login?module=Anonymous&IDToken1=anonymousUserID`。

注 – 令牌名称 `Login.Token0`、`Login.Token1`、`...`、`Login.TokenN`（来自先前的版本）仍受支持，但在以后的版本中将不再受支持。建议使用新的 `IDTokenN` 参数。

帐户锁定

“验证服务”提供这样一项功能：在验证失败 *n* 次后将锁定用户。此功能默认情况下是关闭的，但是可以使用 Access Manager 控制台启用它。

注 – 只有抛弃“密码无效异常”的模块可以使用“帐户锁定”功能。

核心验证服务包含用于启用和自定义此功能的属性，包括但不限于：

- 登录失败锁定模式，启用帐户锁定。
- 登录失败封锁计数，定义用户被锁定之前可以尝试验证的次数。此计数仅对单个用户 ID 有效；只有同一个用户 ID 失败指定的次数后才会被锁定。
- 登录失败锁定间隔，定义在锁定用户之前必须达到“登录失败封锁计数”值的时间（以分钟为单位）。
- 要发送封锁通知的电子邮件地址，指定接收用户封锁通知的电子邮件地址。
- **N** 次失败后警告用户，指定在向用户显示警告消息之前可以发生的验证失败次数。这允许管理员在用户得到即将锁定的警告之后设置附加的登录尝试次数。
- 登录失败锁定时间，定义用户在锁定后再次尝试验证所必须等待的时间（以分钟为单位）。
- 封锁属性名，定义用户概要文件中的哪一个 LDAP 属性针对物理锁定设置为**不活动**。
- 封锁属性值，定义在封锁属性名中指定的 LDAP 属性将设置为：**不活动**或**活动**。

有关任何帐户锁定的电子邮件通知都会发送给管理员。（还会记录帐户锁定活动。）

注 – 有关在 Microsoft® Windows 2000 操作系统上使用此功能的特殊说明，请参阅附录 A，“AMConfig.properties 文件”中的“简单邮件传输协议 (SMTP)”。

Access Manager 支持两种类型的帐户锁定：“物理锁定”和“内存锁定”，具体在以下几节中定义。

物理锁定

这是 Access Manager 的默认锁定行为。通过将用户概要文件中 LDAP 属性的状态更改为不活动可以启动此锁定。**封锁属性名**属性定义用来进行锁定的 LDAP 属性。

注 – 别名用户是通过配置 LDAP 配置文件中的“用户别名列表属性”(`amUser.xml` **中的** `iplanet-am-user-alias-list`) 被映射到现有 LDAP 用户概要文件的用户。别名用户可以通过把 `iplanet-am-user-alias-list` 添加到“核心验证服务”中的“别名搜索属性名称”字段来进行验证。也就是说，如果别名用户被锁定，则使用该用户别名的实际 LDAP 配置文件也将被锁定。这只适合于“LDAP”及“成员资格”以外的验证模块的物理锁定。

内存锁定

通过将**登录失败锁定时间**属性改为大于 0 的值来启用内存锁定。在指定的分钟数内将在内存中锁定用户帐户。帐户将在过了该时间段之后解除锁定。以下是使用内存锁定功能时的一些特殊注意事项：

- 如果重新启动 Access Manager，所有内存中锁定的帐户都将被解除锁定。
- 如果用户的帐户在内存中锁定，而管理员将帐户锁定机制改为物理锁定（通过将锁定时间设置回 0），用户的帐户将在内存中解除锁定，锁定计数也会重置。
- 内存锁定后，当使用非 LDAP 和成员资格验证模块时，如果用户尝试用正确的密码登录，将返回用户在此领域中没有配置文件错误，而不是用户处于不活动状态。错误。

注 – 如果在用户的配置文件中设置了“失败 URL”属性，则无论是锁定警告消息，还是表示其帐户已锁定的消息，都不会显示；用户将被重定向至定义的 URL。

验证服务故障转移

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

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

1. 验证服务 URL 将被传递给 AuthContext API。例如：

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

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

2. 验证环境将检查在 AMConfig.properties 文件的 com.iplanet.am.server* 属性中定义的服务器。
3. 如果步骤 2 失败，则验证环境将从提供有命名服务的服务器查询平台列表。此平台列表是在安装共享同一个 Directory Server 实例的多个 Access Manager 实例（通常是为故障转移目的）时自动创建的。

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

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

全限定域名映射

全限定域名 (FQDN) 映射可让“验证服务”在用户键入错误的 URL（例如指定部分主机名或 IP 地址来访问受保护的资源）时进行纠正。通过修改 AMConfig.properties 文件中 com.sun.identity.server.fqdnMap 属性来启用 FQDN 映射。用于指定此属性的格式为：

```
com.sun.identity.server.fqdnMap[invalid-name ]=valid-name
```

值 *invalid-name* 可能是用户键入的无效 FQDN 主机名，*valid-name* 是过滤器将用户重定向到的实际主机名。只要符合规定的要求，可以指定任意数量的映射（如“代码示例 1-1”所示）。如果未设置此属性，用户将被发送到 AMConfig.propertiess 文件的 com.iplanet.am.server.host=*server_name* 属性中配置的默认服务器名称。

示例 7–1 AMConfig.properties 中的 FQDN 映射属性

```
com.sun.identity.server.fqdnMap[isserver]=isserver.mydomain.com

com.sun.identity.server.fqdnMap[isserver.mydomain]=isserver.mydomain.com

com.sun.identity.server.fqdnMap[

        IP address]=isserver.mydomain.com
```

FQDN 映射的可能用途

此属性可用于为多个主机名创建映射，这可能是服务器上的应用程序可由多个主机名访问。此属性也可用于配置 Access Manager 使其对特定的 URL 不进行纠错。例如，如果使用 IP 地址访问应用程序的用户不需要重定向，可以通过指定如下映射条目来实现此功能：

`com.sun.identity.server.fqdnMap[`*IP address* `]=`*IP address*.

注 – 如果定义了多个映射，请确保无效的 FQDN 名称中没有重叠的值。否则可能导致无法访问应用程序。

持久 Cookie

持久 Cookie 在 Web 浏览器关闭之后继续存在，允许用户使用新的浏览器会话登录而无需重新验证。Cookie 的名称由 `AMConfig.properties` 中的 `com.iplanet.am.pcookie.name` 属性定义；默认值是 `DProPCookie`。Cookie 值是 3DES 加密字符串，包含用户 DN、领域名称、验证模块名称、最长会话时间、空闲时间和高速缓存时间。

▼ 启用持久 Cookie

1. **在核心验证模块中打开持久 `Cookie` 模式。**
2. **在核心验证模块中的持久 `Cookie` 最长时间属性配置时间值。**
3. **将值为 `yes` 的 iPSPCookie 参数附加到“用户界面登录 URL”。**

   一旦用户使用此 URL 进行验证，如果浏览器被关闭，用户可以打开新的浏览器窗口并被重定向到控制台而无需重新验证。这在到达步骤 2 所定义的时间之前一直有效。

   可以使用“验证 SPI”方法打开“持久 Cookie”模式：

   `AMLoginModule.setPersistentCookieOn()`。

传统模式中的多 LDAP 验证模块配置

Access Manager 控制台仅提供一个值字段时，作为故障转移的形式或为了给一个属性配置多个值，管理员可以在一个领域下定义多个 LDAP 验证模块配置。尽管这些附加配置无法通过控制台查看，但如果未找到对于请求用户的授权的初始搜索，这些配置将与主配置一起发挥作用。例如，一个领域可以定义在两个不同的域中搜索 LDAP 验证服务器，也可以在

一个域中配置多个用户命名属性。对于后者，控制台中只有一个文本字段，如果使用主要搜索条件找不到用户，LDAP 模块将使用第二个范围搜索。以下是配置其他 LDAP 配置的步骤。

▼ 添加其他 LDAP 配置

1 编写一个 XML 文件，在其中包括完整的属性集和第二个（或第三个）LDAP 验证配置所需的新值。

可以通过查看 `etc/opt/SUNWam/config/xml` 中的 `amAuthLDAP.xml` 来引用可用的属性。但此步骤创建的 XML 文件是基于 `amadmin.dtd` 结构的，这与 `amAuthLDAP.xml` 不同。可以为此文件定义任何或所有属性。代码示例 1-2 是子配置文件的示例，此文件包括 LDAP 验证配置所有可用属性的值。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!--

  Copyright (c) 2002 Sun Microsystems, Inc. All rights reserved.

  Use is subject to license terms.

-->

<!DOCTYPE Requests

    PUBLIC "-//iPlanet//Sun ONE Access Manager 6.0 Admin CLI DTD//EN"

    "jar://com/iplanet/am/admin/cli/amAdmin.dtd"

>

<!--

  Before adding subConfiguration load the schema with

GlobalConfiguration defined and replace corresponding

 serviceName and subConfigID in this sample file OR load

 serviceConfigurationRequests.xml before loading this sample

-->

<Requests>
```

```
<realmRequests DN="dc=iplanet,dc=com">

    <AddSubConfiguration subConfigName = "ssc"

        subConfigId = "serverconfig"

        priority = "0" serviceName="iPlanetAMAuthLDAPService">


              <AttributeValuePair>

            <Attribute name="iplanet-am-auth-ldap-server"/>

            <Value>vbrao.red.iplanet.com:389</Value>

        </AttributeValuePair>

        <AttributeValuePair>

            <Attribute name="iplanet-am-auth-ldap-base-dn"/>

            <Value>dc=iplanet,dc=com</Value>

        </AttributeValuePair>

        <AttributeValuePair>

            <Attribute name="planet-am-auth-ldap-bind-dn"/>

            <Value>cn=amldapuser,ou=DSAME Users,dc=iplanet,dc=com</Value>

        </AttributeValuePair>

        <AttributeValuePair>

            <Attribute name="iplanet-am-auth-ldap-bind-passwd"/>

            <Value>

                  plain text password</Value>

        </AttributeValuePair>

        <AttributeValuePair>

            <Attribute name="iplanet-am-auth-ldap-user-naming-attribute"/>
```

```
        <Value>uid</Value>
    </AttributeValuePair>
    <AttributeValuePair>
        <Attribute name="iplanet-am-auth-ldap-user-search-attributes"/>
        <Value>uid</Value>
    </AttributeValuePair>
    <AttributeValuePair>
        <Attribute name="iplanet-am-auth-ldap-search-scope"/>
        <Value>SUBTREE</Value>
    </AttributeValuePair>
    <AttributeValuePair>
        <Attribute name="iplanet-am-auth-ldap-ssl-enabled"/>
        <Value>false</Value>
    </AttributeValuePair>
    <AttributeValuePair>
        <Attribute name="iplanet-am-auth-ldap-return-user-dn"/>
        <Value>true</Value>
    </AttributeValuePair>
    <AttributeValuePair>
        <Attribute name="iplanet-am-auth-ldap-auth-level"/>
        <Value>0</Value>
    </AttributeValuePair>
    <AttributeValuePair>
```

```
            <Attribute name="iplanet-am-auth-ldap-server-check"/>

            <Value>15</Value>

        </AttributeValuePair>


    </AddSubConfiguration>


</realmRequests>

</Requests>
```

2 **将纯文本密码作为在步骤 1 中创建的 XML 文件中的 iplanet-am-auth-ldap-bind-passwd 的值进行复制。**

在代码示例中，此属性的值被格式化为粗体。

3 **使用 `amadmin` 命令行工具装入 XML 文件。**

```
./amadmin -u amadmin -w administrator_password -v -t name_of_XML_file.
```

请注意，第二个 LDAP 配置不可见，也不能用控制台修改。

提示 – 多个 LDAP 配置有可供使用的样例。请参阅 `/AccessManager-base /SUNWam/samples/admin/cli/bulk-ops/` 中的`serviceAddMultipleLDAPConfigurationRequests .xml` 命令行模板。可以在 `/AccesManager-base/SUNWam/samples/admin/cli/` 的 `Readme.html` 中找到说明。

会话升级

验证服务允许根据同一用户向一个领域执行的第二次成功验证来升级有效的会话标记。如果拥有有效会话标记的用户尝试向其当前领域保护的资源验证，并且这第二次验证请求成功，则该会话将用基于新验证的新属性更新。如果验证失败，则会返回当前会话，而不升级。如果拥有有效会话的用户尝试向不同领域保护的资源验证，该用户将会收到一则询问

他们是否要向新领域验证的消息。此时用户可以保持当前的会话，也可以尝试向新领域进行验证。成功的验证将损坏原来的会话，并创建新会话。

在会话升级期间，如果登录页面超时，就会重定向到原来的成功 URL。超时值取决于：

- 每个模块的页面超时值设置（默认值为 1 分钟）
- `AMConfig.properties` 中的 `com.iplanet.am.invalidMaxSessionTime` 属性（默认值为 10 分钟）
- `iplanet-am-max-session-time` （默认值为 120 分钟）

`com.iplanet.am.invalidMaxSessionTimeout` 和 `iplanet-am-max-session-time` 的值应大于页面超时值，否则在会话升级期间的有效会话信息将丢失，URL 重定向到以前的成功 URL 也将失败。

验证插件接口

管理员可以编写适用于其领域的用户名或密码验证逻辑，并将其插入“验证服务”。（只有“LDAP”和“成员资格”验证模块支持此项功能。）在验证用户或更改密码之前，Access Manager 将调用此插件。如果验证成功，验证将会继续；如果验证失败，将会抛弃验证失败页面。此插件扩展了作为“服务管理 SDK”一部分的 `com.iplanet.am.sdk.AMUserPasswordValidation` 类。有关此 SDK 的信息，参见 `com.iplanet.am.sdk` 软件包。

▼ 编写和配置验证插件

1. **新的插件类将扩展 `com.iplanet.am.sdk.AMUserPasswordValidation` 类，并实现 `validateUserID()` 和 `validatePassword()` 方法。如果验证失败，将抛出 `AMException`。**
2. **编译插件类并将 `.class` 文件放置到所需的位置。更新类路径，使其在运行时可供 Access Manager 访问。**
3. **以顶级管理员身份登录 Access Manager 控制台。单击“服务管理”选项卡，访问管理服务的属性。在用户 `ID` 和密码验证插件类字段中键入插件类的名称（包括软件包的名称）。**
4. **注销，然后登录。**

JAAS 共享状态

JAAS 共享状态可在验证模块之间共享用户 ID 和密码。为以下每个验证模块都定义了选项：

- 领域（或组织）
- 用户
- 服务
- 角色

如果失败，模块会提示所需的证书。在验证失败后，模块会停止运行，或者清除注销共享状态。

启用 JAAS 共享状态

配置 JAAS 共享状态：

- 使用 `iplanet-am-auth-shared-state-enabled` 选项。
- 共享状态选项的用法为：`iplanet-am-auth-shared-state-enabled=true`
- 此选项的默认值为 true。
- 此变量在验证链配置的“选项”栏中指定。

在失败时，验证模块会根据 JAAS 规范中建议的 `tryFirstPass` 选项行为提示提供所需的证书。

JAAS 共享状态存储选项

配置 JAAS 共享状态存储选项：

- 使用 `iplanet-amauth-store-shared-state-enabled` 选项。
- 存储共享状态选项的用法为：`iplanet-am-auth-store-shared-state-enabled=true`
- 此选项的默认值为 false。
- 此变量在验证链配置的“选项”栏中指定。

在提交、中止或注销后，将清除共享状态。

◆ ◆ ◆ 第 8 章

管理策略

本章介绍 Sun Java™ System Access Manager 的“策略管理”功能。Access Manager 的“策略管理”功能使顶级管理员或顶级策略管理员能够查看、创建、删除和修改可在所有领域中使用的特定服务的策略。它还为领域管理员、子领域管理员或策略管理员提供了一种在领域级别查看、创建、删除和修改策略的方法。

本章包括以下内容：

概述

策略定义了若干规则，这些规则将指定对某一组织受保护资源的访问权限。企业拥有各种需要进行保护、管理和监视的资源、应用程序和服务。“策略”通过定义用户对给定的资源进行操作的时间和方式，从而控制对这些资源的访问权限和使用方式。策略定义了特定负责人的资源。

注 – 负责人可以是个人、公司、角色或组等具有某种身份的任何对象。有关详细信息，请参阅 Java™ 2 Platform Standard Edition Javadoc (`http://java.sun.com/j2se/1.4.2/docs/api/java/security/Principal.html`)。

单个策略能定义二进制或非二进制的决策。二进制决策为 *yes*/*no*、*true*/ *false* 或 *allow*/*deny*。非二进制决策代表某个属性的值。例如，邮件服务可能包含一个 `mailboxQuota` 属性，其中为每个用户都设置了最大存储量的值。通常说来，配置策略可以定义某负责人在什么条件下可以对什么资源执行什么操作。

策略管理功能

“策略管理”功能提供了用于创建和管理策略的策略服务。策略服务允许管理员定义、修改、授予、撤消和删除权限，以保护 Access Manager 部署内部的资源。通常，策略服务包括一个数据存储库、一个允许创建、管理和评估策略的界面库以及一个策略执行程序或策略代理。默认情况下，Access Manager 使用 Sun Java Enterprise System Directory Server 进行数据存储，并提供用于策略评估和策略服务自定义的 Java 和 C API（有关详细信息，请参阅《Sun Java System Access Manager 7 2005Q4 Developer’s Guide》）。它也允许管理员将 Access Manager 控制台用于策略管理。Access Manager 提供了一种启用策略的服务 －“URL 策略代理”服务，该服务使用可下载策略代理执行策略。

URL 策略代理服务

安装时，Access Manager 会提供“URL 策略代理”服务来定义策略以保护 HTTP URL。 该服务允许管理员通过策略强制程序或策略代理来创建和管理策略。

策略代理

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

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

最新的“Access Manager 策略代理”可以从“Sun Microsystems 下载中心”下载。

有关安装和管理策略代理的详细信息，可在 《Sun Java System Access Manager Policy Agent 2.2 User’s Guide》中找到。

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

Access Manager 策略代理仅在 Web URL（`http://...` 或 `https//...`）上执行决策。但是，可以使用 Java 和 C Policy Evaluation API 编写代理，以在其他资源上强制执行策略。

此外，还需要将“策略配置服务”中的“资源比较器”属性由其默认配置更改为：

```
serviceType=Name_of_LDAPService
|class=com.sun.identity.policy.plugins.SuffixResourceName|wildcard=*

|delimiter=,|caseSensitive=false
```

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

策略代理过程

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

如果代理已截取请求并验证了现有的会话标记，随后将发生以下过程。

1. 如果会话标记有效，则允许或拒绝用户的访问。如果会话标记无效，则用户将被重定向到“验证服务”，如下列各步骤所述。

   假设代理截取了某一请求，而对于该请求不存在任何现有会话标记，则代理将用户重定向到登录页面，即使用不同验证方法保护资源也是如此。
2. 正确验证用户凭证后，代理会向定义用于连接到 Access Manager 内部服务的 URL 的“命名服务”发布请求。
3. 如果资源与在代理处配置的非执行列表匹配，则允许访问。
4. “命名服务”返回策略服务、会话服务和日志记录服务的定位器。
5. 代理将请求发送到“策略服务”以获取适用于用户的策略决策。
6. 是允许用户访问还是拒绝用户访问，需根据当前访问资源的策略决策而定。如果对策略决策的建议指示出不同的验证级别或验证机制，代理会将请求重定向到“验证服务”，直到所有条件都经过验证为止。

策略类型

有两种类型的策略可以使用 Access Manager 进行配置：

- 第 121 页中的 “标准策略”
- 第 125 页中的 “候选策略”

标准策略

在 Access Manager 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、条件和响应提供者组成。

规则

一条规则包含一个资源、一项或多项操作以及一个值。每个操作均可拥有一个或多个值。

- 资源定义受保护的特定对象，例如 HTML 页或使用人力资源服务访问的用户工资信息。
- 操作是可在资源上执行的操作的名称，例如 Web 服务器操作的示例有 POST 或 GET。 例如，针对人力资源服务的一项可行的操作可以更改家庭电话号码。

- 值用于定义操作的权限，例如，允许或拒绝。

注 – 可以不使用某些服务的资源来定义操作。

主题

主题定义策略所影响的用户或用户集合（例如，一个组或某个特定角色的拥有者）。主题将被分配给策略。主题的常规规则是：只有当用户至少是策略中的其中一个主题的成员时，才能够应用策略。默认主题包括：

AM 身份主题	在“领域主题”选项卡下创建和管理的身份可作为主体的值进行添加。
Access Manager 角色	任意 LDAP 角色均可作为该主题的值进行添加。“LDAP 角色”是使用 Directory Server 角色功能的任意角色定义。这些角色具有通过 Directory Server 角色定义授权的对象类。可以在“策略配置服务”中修改“LDAP 角色搜索”过滤器以缩小范围并提高性能。
验证的用户	任何拥有有效 SSO 令牌的用户均为该主题的成员。所有通过验证的用户都是此“主题”的成员，即使他们已经通过其他组织（而不是定义策略的组织）的验证。如果资源拥有者要开放一些资源（为其他组织的用户所管理的资源）的访问权时，这将非常有用。
LDAP 组	任意 LDAP 组成员均可作为该主题的值进行添加。
LDAP 角色	任意 LDAP 角色均可作为该主题的值进行添加。“LDAP 角色”是使用 Directory Server 角色功能的任意角色定义。这些角色具有通过 Directory Server 角色定义授权的对象类。可以在“策略配置服务”中修改“LDAP 角色搜索”过滤器以缩小范围并提高性能。
LDAP 用户	任意 LDAP 用户均可作为该主题的值进行添加。
组织	任意组织成员均为该主题的成员
Web 服务客户机	有效值为本地 JKS 密钥库中的可信赖证书（对应于可信赖 WSC 证书）的 DN。此主题取决于“Liberty Web 服务框架”，并且只能由“Liberty 服务提供者”用来对 WSC 进行授权。如果 SSO 令牌中包含的负责人的 DN 与此主题的任意选定值匹配，则由该 SSO 令牌标识的 Web 服务客户机 (WSC) 是此主题的成员。 请确保将此“主题”添加到策略之前，您已经创建了密钥库。您可以从以下位置找到有关设置密钥库的信息： *AccessManager-base* `/SUNWam/samples/saml/xmlsig/keytool.html`

Access Manager 角色与 LDAP 角色

Access Manager 角色是由 Access Manager 创建的。这些角色所具有的对象类由 Access Manager 进行授权。LDAP 角色是使用 Directory Server 角色功能的任意角色定义。这些角色具有通过 Directory Server 角色定义授权的对象类。所有 Access Manager 角色均可被用作 Directory Server 角色。但是，Directory Server 角色并不一定都是 Access Manager 角色。可通过配置第 137 页中的 “策略配置服务”从现有目录利用 LDAP 角色。 Access Manager 角色只能通过所属的“Access Manager 策略服务”进行访问。可以在“策略配置服务”中修改“LDAP 角色搜索”过滤器以缩小范围并提高性能。

嵌套角色

嵌套角色可作为策略定义主题中的“LDAP 角色”正确评估。

条件

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

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

注 – 候选、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*。

可以添加的默认条件是：

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

此属性指明验证的信任级别。

可以使用验证级别条件来指定领域中已注册的验证模块级别之外的级别。当对已通过其他领域验证的用户应用某个策略时，这将非常有用。

对于“LE 验证”，如果用户的验证级别低于或等于条件中设置的验证级别，则应用该策略。可以使用验证级别条件来指定领域中已注册的验证模块级别之外的级别。当对已通过其他领域验证的用户应用某个策略时，这将非常有用。

验证模式　　从下拉菜单中选择条件的验证模式。 这些验证模式即为在领域的核心验证服务中定义的验证模块。

IP 地址　基于“IP 地址”的范围设置此条件。 您可以定义的字段包括：

- 起始/结束 IP 地址 — 指定 IP 地址范围。
- DNS 名称 — 指定 DNS 名称。此字段可以是全限定主机名，也可以是采用以下格式之一的字符串：

  domainname

  **.domainname*

会话　基于用户的会话数据设置此条件。您可以修改的字段包括：

- 最长会话时间 — 指定在发起会话时，策略可应用的最长持续时间。
- 终止会话 — 如果选择该字段，当会话时间超过在“最长会话时间”字段中定义的最长允许时间时，系统将终止该用户会话。

  可使用该条件保护敏感资源以使其仅在验证后的有限时间内可用。

会话属性　根据用户的 Access Manager 会话中设置的属性值决定策略是否适用于请求。在策略评估期间，仅当用户会话的每个属性值均符合条件中的定义时，条件才会返回 true。对于在条件中定义了多个值的属性，令牌只要具有条件的属性中列出的一个值就足够了。例如，可使用该条件来应用基于外部库属性的策略。 验证后期插件可设置基于外部属性的会话属性。

时间　基于时间限制设置此条件。这些字段包括：

- 起始/结束日期 — 指定日期范围。
- 时间 — 指定一天内的时间范围。
- 天数 — 指定表示天数的范围。
- 时区 — 指定一个标准的或自定义的时区。自定义的时区只能是可由 Java 识别的时区 ID（例如，PST）。如果未指定值，默认值为 Access Manager JVM 中设置的时区。

响应提供者

响应提供者是提供基于策略的响应属性的插件。响应提供者属性与策略决策一起发送到 PEP。 Access Manager 包括一个实现，`IDResponseProvider`。该版本的 Access Manager 不支持自定义的响应提供者。 代理和 PEP 通常会将这些响应属性作为标题传递给应用程序。 应用程序通常会使用这些属性来自定义应用程序页面（如门户页面）。

策略建议

如果根据条件判定策略不适用，该条件可能会产生建议消息，指明策略不适用于请求的原因。这些建议消息在策略决策内传播到“策略强制点”。“策略强制点”可以检索此建议并采取适当的行动，例如将用户重定向回验证机制以进行更高级别的验证。 如果策略适用，系统在针对建议采取适当的操作后可能会提示用户进行更高级别的验证，用户或许可以访问资源。

可从以下类中找到更多信息：

```
com.sun.identity.policy.ConditionDecision.getAdvices()
```

如果条件不满足，则只有 `AuthLevelCondiiton` 和 `AuthSchemeCondition` 提供建议。

`AuthLevelCondition` 建议与下列关键字相关：

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_LEVEL_CONDITION_ADVICE
```

`AuthSchemeCondition` 建议与下列关键字相关：

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_SCHEME_CONDITION_ADVICE
```

自定义的条件也可以提供建议。但是，“Access Manager 策略代理”只对“验证级别建议”和“验证模式建议”做出响应。 可以编写自定义的代理来理解和响应更多建议，也可以扩展现有的 Access Manager 代理来理解和响应更多建议。有关详细信息，参见《Sun Java System Access Manager Policy Agent 2.2 User’s Guide》。

候选策略

管理员可能需要将一个领域的策略定义和决策委托给另一个领域。（另外，还可以将资源的策略决策委托给其他策略产品）。 候选策略控制着对策略创建和评估的委托授权。该策略由一个或多个规则或一个或多个候选项组成。

规则

规则定义策略定义和评估相关的资源。

候选项

候选组织定义当前与策略评估相关的组织。默认情况下，有两种候选项类型：对等领域和子领域。 它们分别代表同级领域和子级领域。 有关详细信息，请参阅第 131 页中的 “为对等领域和子领域创建策略 ”。

注 – 相关领域只能为那些已相关的资源（或子资源）定义或评估策略。但是，该限制并不适用于顶层领域。

策略定义类型文档

一旦创建并配置了策略，它就会以 XML 形式存储于 Directory Server 中。在 Directory Server 中，XML 编码的数据存储在一个位置。尽管策略是使用 amAdmin.dtd（或控制台）进行定义和配置，但它实际上是作为基于 policy.dtd 的 XML 被存储在 Directory Server 中。policy.dtd 包含从 amAdmin.dtd（无策略创建标记）中提取的策略元素标记。因此，“策略服务”从 Directory Server 加载策略时，它将根据 policy.dtd 分析 XML。只有在使用命令行创建策略时，才使用 amAdmin.dtd。本节介绍 policy.dtd 的结构。policy.dtd 存在于下列位置：

```
AccessManager-base/SUNWam/dtd (Solairs)
AccessManager-base/identity/dtd (Linux)
```

注 – 在本章中的余下部分将只给出 Solaris 目录信息。请注意 Linux 的目录结构有所不同。

Policy 元素

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

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

Rule 元素

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

注 – 已定义的策略也可以不包括定义的 *ResourceName* 元素。

ServiceName 元素

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

ResourceName 元素

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

AttributeValuePair 元素

AttributeValuePair 元素定义操作及其值。它被用作 第 128 页中的 “Subject 元素” 、第 128 页中的 “Referral 元素”和第 129 页中的 “Condition 元素”的子元素。它包含 *Attribute* 和 *Value* 元素但没有 XML 服务属性。

Attribute 元素

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

Value 元素

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

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

Subjects 元素

Subjects 子元素确定策略所适用的负责人集合；根据组中的成员资格、角色所有权或个别用户选择该集合。它接受 *Subject* 子元素。可以定义的 XML 属性有：

name。它定义集合的名称。

description。它定义主题的说明。

includeType。当前未使用此项。

Subject 元素

Subject 子元素确定策略所适用的负责人集合；该集合可从 Subject 元素所定义的集合中准确找出更具体的对象。成员资格可基于角色、组成员资格或仅仅基于个别用户的列表。它包含子元素第 127 页中的 “AttributeValuePair 元素”。所需 XML 属性是 `type`，它确定一个通用的对象集合，具体定义的主题从该集合中提取。其他 XML 属性包括定义集合名称的 `name` 和 `includeType`，后者规定集合是否如定义的那样，用于确定策略是否用于“不”属于该主题成员的用户。

注 – 定义了多个主题时，要使策略得以应用，至少要有一个主题应该应用于用户。将 `includeType` 设置为 false 来定义主题时，用户不应为应用策略的主题成员。

Referrals 元素

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

Referral 元素

Referral 子元素确定特定的策略候选项。它接受子元素第 127 页中的 “AttributeValuePair 元素”。它必需的 XML 属性是 `type`，该属性确定一个通用的任务集合，具体定义的候选项从该集合中提取。它还可以包含定义集合名称的 `name` 属性。

Conditions 元素

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

注 – Condition 元素是策略中的可选元素。

Condition 元素

Condition 子元素标识特定策略限制（时间范围、验证级别等）。它接受子元素第 127 页中的 "AttributeValuePair 元素"。它必需的 XML 属性是 `type`，该属性确定一个通用的限制集合，具体定义的条件从该集合中提取。它还可以包含定义集合名称的 `name` 属性。

添加"已启用策略服务"

只有当服务模式拥有配置到 `sms.dtd` 的 `<Policy>` 元素时才可定义给定服务的资源策略。

默认情况下，Access Manager 会提供"URL 策略代理"服务 (`iPlanetAMWebAgentService`)。此服务在位于以下目录的 XML 文件中定义：

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

但是，您可以向 Access Manager 添加附加的策略服务。一旦创建了策略服务，就可以通过 `amadmin` 命令行实用程序把它添加到 Access Manager。

▼ 添加新的已启用策略服务

1 **在基于 `sms.dtd` 的 XML 文件里开发新的策略服务。Access Manager 提供两个策略服务 XML 文件，用户可能希望将其用作新策略服务文件的基础：**

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

`SampleWebService.xml` - 这是位于 `AccessManager-base/samples/policy` 的范例策略服务文件。

2 **将该 XML 文件保存到您将从中加载新策略服务的目录。例如：**

```
/config/xml/newPolicyService.xml
```

3 **用 `amadmin` 命令行实用程序加载新策略服务。例如：**

```
AccessManager-base/SUNWam/bin/amadmin
    --runasdn "uid=amAdmin,ou=People,default_org,
root_suffix
    --password password
    --schema /config/xml/newPolicyService.xml
```

4 **加载新策略服务后，可通过 Access Manager 控制台或使用 `amadmin` 加载新策略来制定策略定义的规则。**

创建策略

您可以通过“策略 API”和 Access Manager 控制台创建、修改和删除策略，并通过 `amadmin` 命令行工具创建和删除策略。 您也可以使用 `amadmin` 实用程序获取和列出 XML 格式的策略。本节重点介绍如何通过 `amadmin` 命令行实用程序和 Access Manager 控制台创建策略。有关“策略 API”的详细信息，请参阅《Sun Java System Access Manager 7 2005Q4 Developer’s Guide》。

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

通常情况下，策略是在领域（或子领域）级别创建以在整个领域树中使用的。

▼ 使用 amadmin 创建策略

1 **创建基于 `amadmin.dtd` 的策略 XML 文件。该文件位于以下目录中：**

AccessManager-base `/SUNWam/dtd`

2 **策略 XML 文件生成之后，便可使用以下命令加载它：**

AccessManager-base`/SUNWam/bin/amadmin`
`--runasdn "uid=amAdmin,ou=People,`*default_org*`,`
root_suffix`"`
`--password` *password*
`--data` *policy.xml*

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

通过 `amadmin` 创建策略时，确保验证模块在创建验证模式条件时已注册到领域；创建领域、LDAP 组、LDAP 角色和 LDAP 用户主题时存在相应的 LDAP 对象领域、组、角色和用户；创建 `IdentityServerRoles` 主题时存在 Access Manager 角色；以及创建子领域或对等领域候选项时存在相关领域。

请注意，`SubrealmReferral`、`PeerRealmReferral`、`Realm` 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完整 DN。

▼ 使用 Access Manager 控制台创建标准策略

1 选择要为其创建策略的领域。

2 单击“策略”选项卡。

3 在“ 策略 ”列表中单击“ 新建策略 ”。

4 为策略添加名称和说明。

5 如果您希望激活此策略，请在“活动”属性里选中“是”。

6 此时，您不必为标准策略定义所有字段。您可以在创建策略之后再添加规则、主题、条件和响应提供者等内容。有关详细信息，请参见第 132 页中的“ 管理策略 ”。

7 单击“创建”。

▼ 使用 Access Manager 控制台创建候选策略

1 选择要为其创建策略的领域。

2 在“策略”选项卡中单击“新建候选项”。

3 为策略添加名称和说明。

4 如果您希望激活此策略，请在“活动”属性里选中“是”。

5 此时，您不必为候选策略定义所有字段。 您可以在创建策略之后再添加规则、候选项等内容。有关详细信息，请参阅第 132 页中的“ 管理策略 ”。

6 单击“创建”。

为对等领域和子领域创建策略

要为对等领域或子领域创建策略，必须首先在父领域（或其他对等领域）中创建候选策略。 候选策略的规则定义中必须包含子领域所管理的资源前缀。 一旦在父领域（或其他对等领域）中创建了候选策略，便可在子领域（或对等领域）创建标准策略。

在本示例中，`o=isp` 是父领域，`o=example.com` 是管理 `http://www.example.com` 的资源和子资源的子领域。

▼ 为子领域创建策略

1 **在 o=isp 中创建候选策略。有关候选策略的信息，请参阅第 135 页中的“ 修改候选策略 ”过程。**

候选策略必须将 http://www.example.com 定义为规则中的资源，并且必须包含一个以 example.com 作为候选项中的值的 SubRealmReferral。

2 **找到子领域 example.com。**

3 **既然资源是通过 isp 引用 example.com，就可以为资源 http://www.example.com，或任何以 http://www.example.com 开头的资源创建标准策略。**

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

管理策略

一旦创建了标准或候选策略并将其添加到 Access Manager，您就可以使用 Access Manager 控制台通过修改规则、主题、条件和候选项来管理策略。

修改标准策略

通过“策略”选项卡，可以修改定义访问权限的标准策略。您可以定义和配置多个规则、主题、条件和资源比较器。本节列出并介绍相关操作步骤。

▼ 在标准策略中添加或修改规则

1 **如果已创建了策略，请单击要为其添加规则的策略的名称。否则，请参阅第 131 页中的“ 使用 Access Manager 控制台创建标准策略 ”。**

2 **在“规则”菜单中单击“新建”。**

3 **为规则选择以下任一默认服务类型。如果策略可用的服务较多时，您看到的列表可能会比较长：**

搜索服务	为搜索服务查询定义授权操作并通过指定资源的 Web 服务客户机修改调用的协议。
Liberty 个人配置文件服务	为“Liberty 个人配置文件”服务查询定义授权操作并通过指定资源的 Web 服务客户机修改调用的协议。
URL 策略代理	为策略强制提供“URL 策略代理”服务。该服务允许管理员通过策略强制程序或策略代理来创建和管理策略。

4 **单击“下一步”。**

5 **输入规则的名称及其资源名称。**

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。

主机、端口和资源名称都支持通配符。 例如：

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

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

6 **为规则选择操作。如果您使用的是“URL 策略代理”服务，则可以选择以下选项：**

- GET
- POST

7 **选择操作值。**

- 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。
- 拒绝规则始终优先于允许规则。 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。策略定义过程应只使用允许规则。 如果没有适用于资源的策略，则自动拒绝访问。

  当采用了显式拒绝规则时，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，则被分配了“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 `authentication level` 条件，其中“经理”角色在更高验证级别进行验证。

8 **单击“完成”。**

▼ 在标准策略中添加或修改主题

1 **如果已创建了策略，请单击要为其添加主题的策略的名称。如果尚未创建策略，请参阅**第 131 页中的“ 使用 Access Manager 控制台创建标准策略 ”**。**

2 **在“主题”列表中单击“新建”。**

3 **选择以下任一默认主题类型。有关主题类型的说明，请参阅**第 122 页中的“ 主题 ”

4 单击“下一步”。

5 输入主题的名称。

6 选择或取消选择“排除”字段。

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

如果策略中存在多个主题，则当身份属于至少一个主题的成员时，策略将应用到该身份。

7 执行搜索以显示要添加到主题的身份。此步骤不适用于“验证的用户”主题或“Web 服务客户机”主题。

默认 (*) 搜索模式将显示所有条目。

8 选择要为主题添加的各个身份，或单击“全部添加”一次添加所有身份。单击“添加”将这些身份移至“选定”列表中。此步骤不适用于“验证的用户”主题。

9 单击“完成”。

10 要从策略中移除主题，请选择相应主题并单击“删除”。您可以通过单击主题名称来编辑任何主题定义。

▼ 将条件添加到标准策略

1 如果已创建了策略，请单击要为其添加条件的策略的名称。如果尚未创建策略，请参阅第 131 页中的“ 使用 Access Manager 控制台创建标准策略 ”

2 在“条件”列表中单击“新建”。

3 选择条件类型，然后单击“下一步”。

4 定义条件类型字段。有关条件类型的说明，请参阅第 123 页中的“ 条件 ”。

5 单击“完成”。

▼ 将响应提供者添加到标准策略

1 如果已创建了策略，请单击要为其添加响应提供者的策略的名称。如果尚未创建策略，请参阅第 131 页中的“ 使用 Access Manager 控制台创建标准策略 ”。

2 在“响应提供者”列表中单击“新建”。

3 输入响应提供者的名称。

4 **定义以下值：**

StaticAttribute	该响应属性的名称和值在实例 `IDResponseProvider` 中定义并在策略中存储。
DynamicAttribute	应首先在相应领域的“策略配置服务”中定义此处所选择的响应属性。定义的属性名称应与已配置数据存储库中已有的属性名称相同。有关如何定义属性的详细信息，参见 Access Manager 联机帮助中的“策略配置”属性定义。

5 **单击“完成”。**

6 **要从策略中删除响应提供者，请选择相应主题，然后单击“删除”。您可以通过单击响应提供者名称来编辑任何响应提供者的定义。**

修改候选策略

可将领域的策略定义和决策委托给使用候选策略的不同领域。自定义候选项可用于从任意策略目标点获取策略决策。一旦创建了候选策略，便可添加或修改相关的规则、候选项和资源提供者。

▼ 在候选策略中添加或修改规则

1 **如果已创建了策略，请单击要为其添加规则的策略的名称。否则，请参阅第 131 页中的“使用 Access Manager 控制台创建候选策略”。**

2 **在“规则”列表中单击“新建”。**

3 **为规则选择以下任一默认服务类型。如果策略可用的服务较多时，您看到的列表可能会比较长：**

搜索服务	为搜索服务查询定义授权操作并通过指定资源的 Web 服务客户机修改调用的协议。
Liberty 个人配置文件服务	为“Liberty 个人配置文件”服务查询定义授权操作并通过指定资源的 Web 服务客户机修改调用的协议。
URL 策略代理	为策略强制提供“URL 策略代理”服务。该服务允许管理员通过策略强制程序或策略代理来创建和管理策略。

4 **单击“下一步”。**

5 **输入规则的名称及其资源名称。**

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

资源名称、端口号和协议都支持通配符。例如：

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

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

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

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

6 **单击“完成”。**

▼ 在策略中添加或修改候选项

1 **如果已经创建了策略，请单击要为其添加响应提供者的策略的名称。如果尚未创建策略，请参阅**第 131 页中的“ 使用 Access Manager 控制台创建候选策略 ”**。**

2 **在“规则”列表中单击“新建”。**

3 **选择“服务类型”。**

4 **在“规则”字段中定义资源。这些字段包括：**

候选项— 显示当前候选项类型。

名称— 输入候选项的名称。

资源名称— 输入资源的名称。

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

值 — 选择该候选项的组织名称。

5 **单击“完成”。**

要从策略中移除候选项，请选择该候选项，然后单击“删除”。

您可以通过单击候选项名称旁边的“编辑”链接来编辑任何候选项定义。

▼ 将响应提供者添加到候选策略

1 **如果已创建了策略，请单击要为其添加响应提供者的策略的名称。如果尚未创建策略，请参阅**第 131 页中的“ 使用 Access Manager 控制台创建标准策略 ”**。**

2 **在“响应提供者”列表中单击“新建”。**

3 **输入响应提供者的名称。**

4 **定义以下值：**

StaticAttribute　该响应属性的名称和值在实例 `IDResponseProvider` 中定义并在策略中存储。

DynamicAttribute　该响应属性只有名称是在策略的实例 `IDResponseProvider` 中选定。在策略评估期间，根据用户身份请求从 `IDRepostitories` 读取属性值。

5 **单击"完成"。**

6 **要从策略中移除响应提供者，请选择相应主题，然后单击"删除"。您可以通过单击响应提供者名称来编辑任何响应提供者的定义。**

策略配置服务

"策略配置"服务用于通过 Access Manager 控制台为每个组织配置与策略相关的属性。 也可以定义资源名称实现和与 Access Manager 策略框架一同使用的 Directory Server 数据存储库。在"策略配置服务"中指定的 Directory Server 用于 LDAP 用户、LDAP 组、LDAP 角色以及组织策略主题的成员资格评估。

主题结果的生存时间

为了提高策略评估的性能，成员资格评估将被缓存一段时间，具体时间长短如"策略配置"服务中的"主题结果的生存时间"属性定义。 在达到"主题结果的生存时间"属性中所定义的时间之前，将持续使用这些缓存的成员资格决策。在此之后的成员资格评估用于反映目录中用户的当前状态。

动态属性

这些是所允许的动态属性名称，它们显示在列表中，并且可通过选择它们来定义策略响应提供者的动态属性。所定义的名称需与数据系统信息库中定义的属性名称相同。

amldapuser 定义

`amldapuser` 是默认情况下安装"策略配置"服务中指定的 Directory Server 期间创建的用户。如有必要，管理员或领域的策略管理员可以对其进行更改。

添加策略配置服务

创建领域时，将为领域自动设置“策略配置”服务属性。 但是，必要时也可修改属性。

基于资源的验证

某些组织需要高级验证方案，其中用户将根据他们尝试要访问的资源用特定模块进行验证。基于资源的验证是 Access Manager 的一项功能，该功能要求用户必须通过用于保护资源的特定验证模块而非默认验证模块进行验证。 此功能仅适用于首次用户验证。

注 – 该功能与第 116 页中的 “会话升级”中所描述的基于资源的验证不同。后者不具有任何限制。

限制

基于资源的验证包含以下限制：

- 如果适用于此资源的策略包含多个验证模块，系统将任意选择一个验证模块。
- 级别和模式是可为此策略定义的仅有的两个条件。
- 此功能在不同的 DNS 域中不起作用。

▼ 配置基于资源的验证

一旦安装了 Access Manager 和策略代理，便可对基于资源的验证进行配置。 要执行此操作，需要将 Access Manager 指向网关 servlet。

1 **打开** `AMAgent.properties`。

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

2 **注释掉以下行：**

```
#com.sun.am.policy.am.loginURL = http://Access
Manager_server_host.domain_name:port/amserver/UI/Login
```

。

3 **将以下行添加到 文件：**

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

注 – 网关 servlet 是使用“策略评估 API”开发的，可使用它来编写用于完成基于资源的验证的自定义机制。《Sun Java System Access Manager 7 2005Q4 Developer’s Guide》中的第 6 章 “Using the Policy APIs”一书中的第 6 章，“Using the Policy APIs”。

4 **重新启动代理。**

◆ ◆ ◆ 第 9 章

9 管理主题

“主题”界面可用于领域中的基本身份管理。任何在“主题”界面中创建的身份都能在策略（使用“Access Manager 身份主题”类型创建）的主题定义中使用。

你可以创建和修改的身份包括：

用户

用户代表个体身份。可以创建或删除组的用户，也可以从角色和/或组添加或移除用户。此外，还可以将服务指定给用户。

▼ 创建或修改用户

1 **单击“用户”选项卡。**

2 **单击“新建”。**

3 **为以下字段输入数据：**

用户 **ID**。此字段中应填入用户用来登录到 Access Manager 的名称。该属性可能是一个非 DN 值。

名字。此字段中应填入用户的名字。

姓氏。此字段中应填入用户的姓氏。

全名 —此字段中应填入用户的全名。

密码。— 此字段中应填入“用户 ID”字段中指定的名称的密码。

密码（确认） —确认密码。

用户状态。此选项指示是否允许用户通过 Access Manager 进行验证。

4 单击“创建”。

5 创建用户之后，您可以单击用户的名称来编辑用户信息。有关用户属性的信息，请参阅“用户”属性。您可以进行的其他修改包括：

- 第 141 页中的 “创建或修改用户”
- 第 142 页中的 “将用户添加到角色和组”
- 第 142 页中的 “将服务添加到身份”

▼ 将用户添加到角色和组

1 单击所要修改的用户的名称。

2 选择“角色”或“组”。仅显示已被指定给用户的那些角色和组。

3 从“可用”列表中选择角色或组，然后单击“添加”。

4 当“选定”列表中显示了所选的角色或组时，单击“保存”。

▼ 将服务添加到身份

1 选择您要添加服务的身份。

2 单击“服务”选项卡。

3 单击“添加”。

4 根据您所选择的身份类型，将显示以下服务列表：

- 验证配置
- 搜索服务
- Liberty 个人配置文件服务
- 会话
- 用户

5 选择您要添加的服务，然后单击“下一步”。

6 编辑服务的属性。有关服务的说明，请单击步骤 4 中的服务名称。

7 **单击“完成”。**

代理

Access Manager 策略代理可以保护 Web 服务器和 Web 代理服务器上的内容不受未授权的侵入。它们控制对基于策略（由管理员配置）的服务和 Web 资源的访问。

代理对象定义了“策略代理”配置文件，并允许 Access Manager 存储验证和其他有关保护 Access Manager 资源的特定代理的配置文件信息。通过 Access Manager 控制台，管理员可以查看、创建、修改和删除代理配置文件。

可以在代理对象创建页面定义代理用于通过 Access Manager 进行验证的 UID/密码。如果有多个 AM/WS 设置使用相同的 Access Manager，您可以选择为不同的代理启用多个 ID 并且可以从 Access Manager 单独将其启用和禁用。您也可以集中管理代理的一些首选项值，而不必在每台计算机上都编辑 `AMAgent.properties`。

▼ 创建或修改代理

1 **单击“代理”选项卡。**

2 **单击“新建”。**

3 **输入以下字段的值：**

名称。输入代理的名称或身份。此为代理将用来登录 Access Manager 的名称。不接受多字节名称。

密码。输入代理的密码。此密码必须与在 LDAP 验证过程中代理所使用的密码不同。

确认密码。确认密码。

设备状态。输入代理的设备状态。如果将状态设置为“活动”，代理将能够通过 Access Manager 进行验证并与之进行通信。如果将状态设置为“不活动”，代理将无法通过 Access Manager 进行验证。

4 **单击“创建”。**

5 **创建代理之后，您可以另外编辑以下字段：**

说明。输入代理的简短说明。例如，可以输入代理实例名称或此代理保护的应用程序名称。

代理关键字值。使用关键字/值对设置代理属性。Access Manager 使用此属性接收有关用户的证书声明的代理请求。通常仅一个属性有效，所有其他属性都将被忽略。请使用以下格式：

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

创建唯一策略代理身份

默认情况下，当在一个可信赖环境中创建多个策略代理时，这些策略代理包含的 UID 和密码相同。因为 UID 和密码是共享的，所以 Access Manager 不能区分各个代理，这可能导致会话 Cookie 容易被截取。

当“身份提供者”为第三方或企业中未授权组开发的应用程序（或“服务提供者”）提供验证、授权和有关用户的配置文件信息时，这个缺点可能会出现。可能的安全问题包括：

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

▼ 创建唯一策略代理身份

1 使用 Access Manager 管理控制台为每个代理设置一个条目。

2 运行以下有关密码的命令，此密码是在创建代理过程中输入的。此命令应该在安装代理的主机上调用。

```
AccessManager-base/SUNWam/agents/bin/crypt_util agent123
```

此时输出以下信息：

```
WnmKUCg/y3l404ivWY6HPQ==
```

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

```
# The username and password to use for the Application

authentication module.



com.sun.am.policy.am.username = agent123

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



# Cross-Domain Single Sign On URL

# Is CDSSO enabled.

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

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

# in a CDSSO Scenario.

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

/amserver/cdcservlet
```

4 **更改安装有 Access Manager 的** `AMConfig.properties` **以反映新值，然后重新启动 Access Manager。示例：**

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

com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer



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

5 **在 Access Manager 控制台中，选择"配置">"平台"。**

6 **在"Cookie 域"列表中更改 Cookie 域名：**

a. **选择默认** `iplanet.com` **域，然后单击"删除"。**

b. **输入 Access Manager 安装的主机名，然后单击"添加"。**

示例：`server.example.com`

应该会在浏览器上看见两个 Cookie 集：

- iPlanetDirectoryPro – server.example.com（主机名）
- sunIdentityServerAuthNServer – example.com（主机名）

过滤的角色

过滤的角色是 LDAP 过滤器创建的动态角色。在创建角色时，会通过过滤器过滤所有用户并为其分配该角色。过滤器会搜索条目中的所有属性值对（例如，`ca=user*`），并自动将包含该属性的用户分配给角色。

▼ 创建过滤的角色

1. 在“浏览”窗格中，找到要在其中创建角色的组织。
2. 单击“新建”。
3. 输入过滤的角色的名称。
4. 输入搜索条件信息。
   例如，
   ```
   (&(uid=user1)(|(inetuserstatus=active)(!(inetuserstatus=*))))
   ```
   如果过滤器保留为空，将默认创建以下角色：
   ```
   (objectclass = inetorgperson)
   ```
5. 单击“创建”以基于过滤条件启动搜索。通过过滤条件定义的身份将会自动指定给角色。
6. 创建过滤的角色后，单击角色的名称来查看属于该角色的用户。此外，还可以通过单击“服务”选项卡将服务添加到角色。

角色

角色的成员是指拥有该角色的 LDAP 条目。角色本身的条件被定义为具有属性的 LDAP 条目，由条目的区别名 (DN) 属性来标识。 创建角色后，可以手动添加服务和用户。

▼ 创建或修改角色

1. 单击“角色”选项卡。
2. 在“角色”列表中单击“新建”。
3. 输入角色的名称。
4. 单击“创建”。

▼ 将用户添加到角色或组

1. 单击要为其添加用户的角色或组的名称。
2. 单击“用户”选项卡。

3 从“可用”列表中选择您要添加的用户，并单击“添加”。

4 当“选定”列表中显示了所选的用户时，单击“保存”。

组

组代表具有共同功能、特性或利益的用户集合。通常来说，这种分组不会涉及权限。组可存在于两个级别，分别是组织和其他受管组中。

▼ 创建或修改组

1 单击“组”选项卡。

2 在“组”列表中单击“新建”。

3 输入组的名称。

4 单击“创建”。

创建组之后，您可以单击组的名称，然后单击“用户”选项卡，将用户添加到组。

第 III 部分

目录管理和默认服务

这是《Sun Java System Access Manager 7 2005Q4 管理指南》的第三部分。“目录管理”一章介绍当 Access Manager 在“传统模式”下部署时如何管理“目录”对象。其他几章介绍如何配置和使用 Access Manager 的一些默认服务。本部分包含以下各章：

◆ ◆ ◆ 第 10 章

10 目录管理

“目录管理”选项卡只有在“传统”模式下安装 Access Manager 时才显示。此目录管理功能可以为已启用了 Sun Java System Directory Server 的 Access Manager 部署提供身份管理解决方案。

有关“传统模式”安装选项的详细信息，参见《Sun Java Enterprise System 2005Q4 Installation Guide for UNIX》

管理目录对象

“目录管理”选项卡包含查看和管理 Directory Server 对象所需的所有组件。本部分说明对象类型及其详细配置方法。使用 Access Manager 控制台或命令行界面可以定义、修改或删除用户、角色、组、组织、子组织和容器对象。控制台有默认的管理员，他们拥有不同的权限级别以创建和管理目录对象。（可以基于角色创建其他管理员。）与 Access Manager 一起安装时，在 Directory Server 中会定义管理员。 可以管理的 Directory Server 对象有：

组织

在企业用来管理部门和资源的层次结构中，组织代表其最高一级。Access Manager 在安装时会动态创建一个顶级组织（在安装期间定义）来管理 Access Manager 企业配置。 安装后可以创建其他组织，以管理单独的企业。创建的所有组织都位列顶级组织之下。

▼ 创建组织

1 **单击“目录管理”选项卡。**

2 **在“组织”列表中，单击“新建”。**

3 **输入字段的值。仅“名称”是必需字段。这些字段包括：**

名称 输入组织名称的值。

域名 输入组织的完整域名系统 (DNS) 名称（如果存在）。

组织状态 选择**不活动**或**活动**状态。默认值为**活动**。在组织的生命期内，可以随时选择“属性”图标来更改该状态。 如果选择**不活动**状态，则当登录到组织时，将禁止用户访问。

组织别名 该字段定义组织的别名，以允许您在通过 URL 登录时使用别名进行验证。 For example, if you have an organization named `exampleorg`, and define `123` and `abc` as aliases, you can log into the organization using any of the following URLs:

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

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

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

组织别名在组织中必须唯一。可以使用“唯一属性列表”来强制执行唯一性。

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

```
http://machine.example.com/amserver/UI/

Login?org=exampleorg

http://machine.example1.com/amserver/

UI/Login?org=exampleorg

http://machine.example2.com/amserver/

UI/Login?org=exampleorg
```

唯一属性列表 用于添加组织中用户的唯一属性名列表。例如，如果添加用于指定电子邮件地址的唯一属性名，则不能创建两个使用相同电子邮件地址的用

户。也可以在该字段中输入以逗号分隔的列表。列表中的任一属性名均定义了唯一性。例如，如果该字段包含以下属性名列表：

```
PreferredDomain, AssociatedDomain
```

并且针对特定用户 `PreferredDomain` 被定义为 `http://www.example.com`，则整个以逗号分隔的列表在该 URL 中唯一。将命名属性 'ou' 添加到 "唯一属性列表" 并不会强制执行默认组和人员容器的唯一性。(ou=Groups,ou=People)。

对于所有子组织都强制执行唯一性。

4 **单击 "确定"。**

新组织将显示在"组织"列表中。 要编辑在创建组织过程中定义的属性，请单击要编辑的组织的名称，更改属性，然后单击"保存"。

▼ 删除组织

1 **选中要删除的组织名称旁边的复选框。**

2 **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 Access Manager 对象添加到策略中。创建或修改策略时，组织、角色、组和用户可以被定义为主题。定义了主题后，策略将被应用到对象。有关详细信息，请参阅第 132 页中的 "管理策略"。

容器

当由于对象类和属性的不同而无法使用组织条目时，将使用容器条目。请切记 Access Manager 容器条目和 Access Manager 组织条目不必等同于 LDAP 对象类 `organizationalUnit` 和 `organization`。它们是抽象身份条目。理想情况下，将使用组织条目而不使用容器条目。

注 – 容器的显示是可选的。要查看容器，必须选择"配置">"控制台属性"下方"管理"服务中的"显示容器"。

▼ 创建容器

1. 选择将在其中创建新容器的组织或容器的位置链接。
2. 单击“容器”选项卡。
3. 在“容器”列表中单击“新建”。
4. 输入要创建的容器的名称。
5. 单击“确定”。

▼ 删除容器

1. 单击“容器”选项卡。
2. 选中要删除的容器名称旁边的复选框。
3. 单击“删除”。

注 – 如果删除某个容器，就会删除该容器中存在的所有对象，包括所有对象和子容器。

组容器

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

注 – 组容器的显示是可选的。要查看组容器，必须选择“配置”>“控制台属性”下方“管理”服务中的“启用组容器”。

▼ 创建组容器

1. 选择将包含新的组容器的组织或组容器的位置链接。
2. 选择“组容器”选项卡。
3. 在“组容器”列表中单击“新建”。
4. 在“名称”字段中输入值，然后单击“确定”。新的组容器将显示在“组容器”列表中。

▼ 删除组容器

1. **找到包含要删除的组容器的组织。**
2. **选择“组容器”选项卡。**
3. **选中要删除的组容器旁边的复选框。**
4. **单击“删除”。**

组

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

Access Manager 还支持嵌套组，它“代表”了单个组中所包含的现有组。与子组不同，嵌套组可以存在于 DIT 中的任何位置。使用嵌套组可以快速地为多个用户设置访问权限。

可以创建两种类型的组：静态组和动态组。只能手动将用户添加到静态组，动态组则通过过滤器控制用户的添加。这两种类型的组中都可以添加嵌套组或子组。

静态组

静态组是根据您指定的“受管组类型”创建的组。 使用 `groupOfNames` 或 `groupOfUniqueNames` 对象类将组成员添加到组条目中。

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

动态组

动态组是通过使用 LDAP 过滤器创建的。所有条目均由过滤器过滤并动态分配给组。过滤器将查找条目中的任何属性，并返回那些包含特定属性的条目。例如，如果您要根据构建号创建组，则可以使用过滤器返回一组包含该构建号属性的用户。

注 – 要使用参考完整性插件，应将 Access Manager 与 Directory Server 一起进行配置。当启用参照完整性插件后，它将直接在删除或重命名操作后对指定属性执行完整性更新。这将确保在整个数据库中维持相关条目之间的关系。数据库索引则增强了 Directory Server 中的搜索性能。有关启用插件的详细信息，参见《Sun Java System Access Manager 6 2005Q1 Migration Guide》。

▼ 创建静态组

1. **找到要在其中创建新组的组织、组或组容器。**
2. **在"组"列表中，单击"新建静态"。**
3. **在"名称"字段中输入组的名称。单击"下一步"。**
4. **选择"用户可以订阅此组"属性可以使用户自行订阅组。**
5. **单击"确定"。**
   组创建完毕后，可以通过选择组的名称并单击"常规"选项卡来编辑"用户可以订阅此组"属性。

▼ 向静态组添加成员或从中移除

1. **在"组"列表中，选择要添加成员的组。**
2. **在"选择操作"菜单中选择要执行的操作。可以执行以下操作：**

   新建用户　保存用户信息时，此操作将创建新用户并将该用户添加到组。

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

   搜索标准创建完毕后，单击"下一步"。从返回的用户列表中，选择要添加的用户并单击"完成"。

   添加组　此操作可以将嵌套组添加到当前组。选择此操作时要创建搜索条件，包括搜索范围、组的名称（允许使用通配符"*"），并且可指定用户是否可以自行订阅组。信息输入完毕后，单击"下一步"。从返回的组列表中，选择要添加的组并单击"完成"。

   移除成员　此操作将从组中移除成员（包括用户和组），但不会将其删除。选择要移除的成员并从"选择操作"菜单中选择"移除成员"。

   删除成员　此操作将永久删除所选成员。选择要删除的成员，然后选择"删除成员"。

▼ 创建动态组

1. **找到要在其中创建新组的组织或组。**
2. **单击"组"选项卡。**

3 **单击“新建动态”。**

4 **在“名称”字段中输入组的名称。**

5 **构造 LDAP 搜索过滤器。**

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

6 **单击“确定”后，系统会自动将与搜索条件匹配的所有用户添加到组。**

▼ 向动态组添加成员或从中移除

1 **在“组”列表中，单击要添加成员的组的名称。**

2 **在“选择操作”菜单中选择要执行的操作。可以执行以下操作：**

添加组	此操作可以将嵌套组添加到当前组。选择此操作时要创建搜索条件，包括搜索范围、组的名称（允许使用通配符“*”），并且可指定用户是否可以自行订阅组。信息输入完毕后，单击“下一步”。 从返回的组列表中，选择要添加的组并单击“完成”。
移除成员	此操作将从组中移除成员（包括组），但不会将其删除。 选择要移除的成员，然后选择“移除成员”
删除成员	此操作将永久删除所选成员。选择要删除的成员，然后选择“删除成员”。

将组添加到策略

可以通过定义策略的主题将 Access Manager 对象添加到策略中。在创建或修改策略时，可以在策略的“主题”页面中将组织、角色、组和用户定义为主题。定义了主题后，策略将被应用到对象。有关详细信息，请参阅第 132 页中的 “管理策略” 。

人员容器

人员容器是默认的 LDAP 组织单位。在组织中创建用户时，所有的用户都将被指定到该容器。 人员容器位于组织级别和人员容器级别（作为子人员容器）。它们只能包含其他人员容器和用户。如果需要，可以将其他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“管理服务”中选择“启用人员容器”。

▼ 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。
2. 在“人员容器”列表中单击“新建”。
3. 输入要创建的人员容器的名称。
4. 单击“确定”。

▼ 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. 选中要删除的人员容器名称旁边的复选框。
3. 单击“删除”。

注 – 删除人员容器将删除该人员容器中存在的所有对象， 包括所有用户和子人员容器。

用户

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

注 – 如果在子组织中创建的用户使用了与 `amadmin` 相同的用户 ID，登录 `amadmin` 时将失败。如果发生了这样的问题，管理员应该通过 Directory Server 控制台更改用户 ID。这样可使管理员登录到默认组织。另外，验证服务中的“起始用户搜索的 DN”可以设置为人员容器 DN，以确保在登录过程中返回唯一匹配项。

▼ 创建用户

1. 找到要在其中创建用户的组织、容器或人员容器。
2. 单击“用户”选项卡。
3. 在“用户”列表中单击“新建”。
4. 为以下值输入数据：

用户 ID	此字段中应填入用户用来登录到 Access Manager 的名称。该属性可能是一个非 DN 值。
名字	此字段中应填入用户的名字。“名字”值和“姓氏”值可以标识“当前已登录”字段中的用户。 此值不用必须填写。
姓氏	此字段中应填入用户的姓氏。“名字”值和“姓氏”值可以标识用户。
全名	此字段中应填入用户的全名。
密码	此字段中应填入“用户 ID”字段中所指定名称的密码。
密码（确认）	确认密码。
用户状态	此选项指示是否允许用户通过 Access manager 进行验证。只有活动用户才能进行验证。默认值为**活动**。

5 单击“确定”。

▼ 编辑用户概要文件

当某个尚未指定管理角色的用户通过 Access Manager 进行验证时，默认视图为用户自己的“用户概要文件”视图。 另外，具有适当权限的管理员可以编辑用户概要文件。 在该视图中，用户可以修改其个人概要文件的属性值。“用户概要文件”视图中显示的属性可以扩展。 有关添加对象和身份的自定义属性的详细信息，请参阅 Access Manager Developer’s Guide。

1 选择要对其概要文件进行编辑的用户。 默认情况下，屏幕上将显示“常规”视图。

2 编辑以下字段：

名字	此字段中应填入用户的名字。
姓氏	此字段中应填入用户的姓氏。
全名	此字段中应填入用户的全名。
密码	单击“编辑”链接以添加和确认用户密码。
电子邮件地址	此字段中应填入用户的电子邮件地址。
员工编号	此字段中应填入用户的员工编号。
电话号码	此字段中应填入用户的电话号码。
家庭地址	此字段中应填入用户的家庭地址。
用户状态	此选项指示是否允许用户通过 Access Manager 进行验证。只有活动用户才能通过 Access Manager 进行验证。默认值为“活动”。可以从下拉菜单中选择以下任意一个选项：。 ■ 活动 — 用户可通过 Access Manager 进行验证。

- 不活动 — 用户不能通过 Access Manager 进行验证，但用户概要文件仍会存储在目录中。

注 – 将用户状态更改为“不活动”仅影响通过 Access Manager 进行的验证。 Directory Server 使用 *nsAccountLock* 属性来确定用户帐户的状态。 禁用 Access Manager 验证的用户帐户仍然可以执行不需要 Access Manager 的任务。要禁用目录中的某个用户帐户，而不仅仅是禁用 Access Manager 验证，应将 *nsAccountLock* 的值设置为 false。 如果站点的委托管理员要定期禁用用户，应考虑将 *nsAccountLock* 属性添加到“Access Manager 用户概要文件”页面。有关详细信息，请参阅《Sun Java System Access Manager 7 2005Q4 Developer’s Guide》 。

帐户失效日期	如果存在此属性，则当前日期和时间超过指定的“帐户失效日期”时，验证服务将不允许进行登录。 此属性的格式为 *mm/dd/yyyy hh:mm*。
用户验证配置	此属性设置用户的验证链。
用户别名列表	此字段定义了一组应用于用户的别名。 要使用此属性中配置的别名，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	此字段指定用户的语言环境。
成功 URL	此属性指定用户在验证成功后，重新指向的 URL。
失败 URL。	此属性指定用户在验证失败后，重新指向的 URL。
密码重置选项	此字段用于选择要在忘记密码页面中使用的问题，该页面用来恢复忘记的密码。
用户搜索资源提供	设置用户的“用户搜索”服务的资源提供。
MSISDN 号码	使用 MSISDN 验证时，定义用户的 MSISDN 号码。

▼ 将用户添加到角色和组

1. **单击“用户”选项卡。**
2. **单击所要修改的用户的名称。**
3. **选择“角色”或“组”选项卡。**
4. **选择要向其添加用户的角色或组，然后单击“添加”。**
5. **单击“保存”。**

注 – 要从“角色”或“组”中移除用户，请选择角色或组并单击“移除”，然后单击“保存”。

将用户添加到策略

可以通过定义策略的主题将 Access Manager 对象添加到策略中。在创建或修改策略时，可以在策略的“主题”页面中将组织、角色、组和用户定义为主题。定义了主题后，策略将被应用到对象。有关详细信息，请参阅第 132 页中的 “管理策略”。

角色

角色是与组的概念类似的 Directory Server 条目机制。组有成员，角色也有成员。角色的成员是指拥有该角色的 LDAP 条目。角色本身的条件被定义为具有属性的 LDAP 条目，由条目的区别名 (DN) 属性来标识。 Directory Server 具有许多不同类型的角色，但 Access Manager 只能管理其中的一种：被管理的角色。

注 – 在目录部署中还可以使用其他的 Directory Server 角色类型，只是它们不能被 Access Manager 控制台管理。还可以在策略的主题定义中使用其他的 Directory Server 类型。有关策略主题的详细信息，请参阅第 130 页中的 “创建策略”。

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

Access Manager 使用角色来应用访问控制指令。首次安装时，Access Manager 会配置定义管理员权限的访问控制指令 (ACI)。然后在角色（如“组织管理员角色”和“组织帮助台管理员角色”）中指定这些 ACI，当这些角色被指定到用户时，可定义用户的访问权限。

仅当“管理服务”中启用了“在用户概要文件页面中显示角色”属性时，用户才可查看为其分配的角色。

注 – 要使用参考完整性插件，应将 Access Manager 与 Directory Server 一起进行配置。当启用参照完整性插件后，它将直接在删除或重命名操作后对指定属性执行完整性更新。这将确保在整个数据库中维持相关条目之间的关系。数据库索引则增强了 Directory Server 中的搜索性能。有关启用插件的详细信息，参见《Sun Java System Access Manager 6 2005Q1 Migration Guide》。

有两种类型的角色：

- 静态 — 静态角色在创建时可以不添加用户。角色创建之后，您可以在其中添加特定用户。这样，在向给定角色添加特定用户时，您可以更好的进行控制。
- 动态 – 动态角色是通过使用 LDAP 过滤器创建的。在创建角色时，会通过过滤器过滤所有用户并为其分配该角色。 过滤器会搜索条目中的所有属性值对（例如，`ca=user*`），并自动将包含该属性的用户分配给角色。

▼ 创建静态角色

1 转到要在其中创建角色的组织。

2 单击“角色”选项卡。

“角色”列表中将显示在配置组织时创建的一组默认角色。默认角色包括：

容器帮助台管理员。“容器帮助台管理员”角色拥有对组织单位中所有条目的读取权限，但仅对自身容器单位中用户条目的 `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 – 在创建子组织时，请记住管理角色是在子组织而不是父组织中创建的。

容器管理员。“容器管理员”角色拥有对 LDAP 组织单位中所有条目的读写权限。 在 Access Manager 中，LDAP 组织单位通常被称为容器。

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。

人员管理员。默认情况下，新创建的组织中的所有用户条目都是该组织的成员。“人员管理员”拥有对组织中所有用户条目的读写权限。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或组的属性，也不能从角色或组中移除用户。

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

组管理员。创建组时所创建的“组管理员”拥有对特定组所有成员的读写权限，可以创建新用户、将用户指定到自己所管理的组以及删除自己创建的用户。

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

顶级管理员。“顶级管理员”拥有对顶级组织中所有条目的读写权限。换句话说，“顶级管理员”角色具有 Access Manager 应用程序内所有配置负责人所拥有的权限。

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

3 **单击“新建静态”按钮。**

4 **输入角色的名称。**

5 **输入角色的说明。**

6 **从“类型”菜单中选择角色类型。**

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

7 **从“访问权限”菜单中选择默认的一组权限，以应用到角色。拥有这些权限，可以访问组织中的条目。显示的默认权限未按照特定顺序排列。这些权限包括：**

无权限	对角色不设置权限。
组织管理员	“组织管理员”拥有对已配置的组织中所有条目的读写权限。
组织帮助台管理员	“组织帮助台管理员”拥有对已配置的组织中所有条目的读取权限以及对 `userPassword` 属性的写入权限。
组织策略管理员	“组织策略管理员”拥有对组织中所有策略的读写权限。“组织策略管理员”不能创建对等组织的侯选策略。 通常，“无权限 ACI”会指定给“服务”角色，而默认的 ACI 会指定给“管理”角色。

▼ 将用户添加到静态角色

1 **单击要为其添加用户的角色的名称。**

2 **在“成员”列表中，从“选择操作”菜单选择“添加用户”。**

3 **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：**

匹配	允许选择过滤器要包含的字段。`ALL` 将根据所有指定的字段向用户返回结果。`ANY` 将根据所指定的任一字段向用户返回结果。
名字	按照用户的名字搜索用户。
用户 ID	按照用户 ID 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（活动或不活动）搜索用户。

4 **单击“下一步”开始搜索。将显示搜索结果。**

5 **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。**

6 **单击“完成”。**
用户将被分配到角色。

▼ 创建动态角色

1 **转到要在其中创建角色的组织。**

2 **单击“角色”选项卡。**
“角色”列表中将显示在配置组织时创建的一组默认角色。默认角色包括：

容器帮助台管理员。“容器帮助台管理员”角色拥有对组织单位中所有条目的读取权限，但仅对自身容器单位中用户条目的 `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 – 在创建子组织时，请记住管理角色是在子组织而不是父组织中创建的。

容器管理员。“容器管理员”角色拥有对 LDAP 组织单位中所有条目的读写权限。 在 Access Manager 中，LDAP 组织单位通常被称为容器。

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。

人员管理员。默认情况下，新创建的组织中的所有用户条目都是该组织的成员。“人员管理员”拥有对组织中所有用户条目的读写权限。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或组的属性，也不能从角色或组中移除用户。

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

组管理员。创建组时所创建的“组管理员”拥有对特定组所有成员的读写权限，可以创建新用户、将用户指定到自己所管理的组以及删除自己创建的用户。

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

顶级管理员。“顶级管理员”拥有对顶级组织中所有条目的读写权限。换句话说，“顶级管理员”角色具有 Access Manager 应用程序内所有配置负责人所拥有的权限。

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

3 单击“新建动态”按钮。

4 输入角色的名称。

5 输入角色的说明。

6 从“类型”菜单中选择角色类型。

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

7 从“访问权限”菜单中选择默认的一组权限，以应用到角色。拥有这些权限，可以访问组织中的条目。显示的默认权限未按照特定顺序排列。这些权限包括：

无权限	对角色不设置权限。
组织管理员	“组织管理员”拥有对已配置的组织中所有条目的读写权限。
组织帮助台管理员	“组织帮助台管理员”拥有对已配置的组织中所有条目的读取权限以及对 `userPassword` 属性的写入权限。
组织策略管理员	“组织策略管理员”拥有对组织中所有策略的读写权限。“组织策略管理员”不能创建对等组织的侯选策略。 通常，“无权限 ACI”会指定给“服务”角色，而默认的 ACI 会指定给“管理”角色。

8 输入搜索条件信息。这些字段包括：

匹配	允许您使用运算符来连接所有用于过滤的字段。`ALL` 将根据所有指定的字段向用户返回结果。`ANY` 将根据所指定的任一字段向用户返回结果。
名字	按照用户的名字搜索用户。
用户 ID	按照用户 ID 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（活动或不活动）搜索用户。

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

▼ 从角色中移除用户

1. **找到包含要修改的角色的组织。**
   从“身份管理”模块的“查看”菜单中选择“组织”，然后选择“角色”选项卡。
2. **选择要修改的角色。**
3. **从“查看”菜单中选择“用户”。**
4. **选中每个要移除的用户旁边的复选框。**
5. **单击“选择操作”菜单中的“移除用户”。**
   用户将从角色中移除。

将角色添加到策略

可以通过定义策略的主题将 Access Manager 对象添加到策略中。在创建或修改策略时，可以在策略的“主题”页面中将组织、角色、组和用户定义为主题。定义了主题后，策略将被应用到对象。有关详细信息，请参阅第 132 页中的 “管理策略”。

◆ ◆ ◆ 第 11 章

11 当前会话

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

当前会话界面

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

会话管理

“会话管理”窗格显示当前所管理的 Access Manager 的名称。

会话信息

“会话信息”窗口显示当前登录到 Access Manager 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）。

最长会话时间。显示会话过期之前用户可以登录的最长时间（以分钟为单位），过期后用户就必须重新验证才能重新获得访问权。

空闲时间。显示用户处于空闲状态的时间（以分钟为单位）。

最大空闲时间。显示用户在需要重新验证之前，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。

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。

▼ 终止会话

1. **选择要终止的用户会话。**
2. **单击“终止”。**

◆ ◆ ◆ 第 12 章

密码重置服务

Access Manager 提供的“密码重置”服务允许用户重新设置用于访问给定服务或受 Access Manager 保护的应用程序的密码。顶级管理员定义的“密码重置”服务属性控制了用户验证证书（以密码提示问题的形式），还控制了新的或现有密码通知的机制，以及为不正确用户验证设置可能的封锁间隔。

本章包括以下内容：

注册密码重置服务

用户所在领域无需注册“密码重置”服务。如果用户所在组织中不存在“密码重置”服务，它将继承为“服务配置”中的服务定义的值。

▼ 为不同领域中的用户注册密码重置

1. **找到要为用户注册密码的领域。**
2. **单击领域名称，然后单击“服务”选项卡。**
   如果尚未将其添加到领域，请单击“添加”按钮。
3. **选择“密码重置”，然后单击“下一步”**
   将显示“密码重置”服务属性。有关属性定义的信息，请参阅联机帮助。
4. **单击“完成”。**

配置密码重置服务

注册“密码重置”服务之后，必须由拥有管理员权限的用户配置该服务。

▼ 配置服务

1. **选择已注册“密码重置”服务的领域。**
2. **单击“服务”选项卡。**
3. **单击服务列表中的“密码重置”。**
4. **出现“密码重置”属性，它允许定义“密码重置”服务的要求。确保启用“密码重置”服务（默认情况下）。必须至少定义以下属性：**
   - 用户验证
     - 密码提示问题
     - 绑定 DN
     - 绑定密码

     “绑定 DN”属性必须包含拥有重置密码权限的用户（例如，帮助台管理员）。由于 Directory Server 中存在限制，因此当绑定 DN 为 `cn=Directory Manager` 时，“密码重置”将不生效。

     剩余属性则为可选。有关服务属性的说明，请参阅联机帮助。

   注 – Access Manager 将自动安装可随机生成密码的“密码重置”Web 应用程序。 但是，您也可写入自己的密码生成和密码通知插件类。有关这些插件类的范例，请参阅位于以下位置的 Readme.html 文件。

   PasswordGenerator :

   ```
   AccessManager-base/SUNWam/samples/console/PasswordGenerator
   ```

   NotifyPassword :

   ```
   AccessManager-base/SUNWam/samples/console/NotifyPassword
   ```

   ---

5. **如果用户要定义他/她的唯一个人问题，则选择“已启用个人问题”属性。定义属性后，单击“保存”。**

密码重置封锁

“密码重置”服务包含封锁功能，该功能限制了用户尝试正确回答其密码提示问题的次数。封锁功能是通过“密码重置”服务属性来配置的。有关服务属性的说明，请参阅联机帮助。“密码重置”支持两种类型的封锁：内存封锁和物理封锁。

内存封锁

这是一种临时封锁，仅当“密码重置失败封锁时间”属性中的值大于零且启用了“启用密码重置失败封锁”属性时才有效。该封锁将阻止用户通过“密码重置”Web 应用程序重置他们的密码。该封锁将持续到“密码重置失败封锁时间”中指定的时间，或是重新启动服务器前。有关服务属性的说明，请参阅联机帮助。

物理封锁

这是一种更为永久性的封锁。如果将“密码重置失败封锁计数”属性中的值设置为 0 且启用了“启用密码重置失败封锁”属性，则当用户未能正确回答密码提示问题时，其用户帐户的状态将变为不活动。有关服务属性的说明，请参阅联机帮助。

最终用户的密码重置

以下几节介绍“密码重置”服务的用户体验。

自定义密码重置

一旦启用了“密码重置”服务并且管理员定义了属性，用户便可登录到 Access Manager 控制台自定义他们的密码提示问题。

▼ 自定义密码重置

1. **用户登录到 Access Manager 控制台，假设“用户名”和“密码”已验证成功。**
2. **在“用户概要文件”页面上，用户选择“密码重置”选项。此时将显示“可用问题答案”屏幕。**
3. **用户可看到管理员为服务定义的可用问题，如：**
   - 您的宠物名称?
     - 您喜欢哪个电视节目?
     - 您母亲的娘家姓?
     - 您喜欢哪家餐馆?
4. **用户选择密码提示问题，最多可选择管理员为领域定义问题的最大数目（“密码重置服务”定义的最大量）。然后，用户提供所选问题的答案。这些问题和答案会成为重置用户密码的**

基础（请参阅下一节）。如果管理员选择了“已启用个人问题”属性，则提供的文本字段将允许用户输入唯一密码提示问题并提供其答案。

5 **用户单击“保存”。**

重置忘记密码

如果用户忘记他们的密码，Access Manager 将使用“密码重置”Web 应用程序来随机生成新密码并将其告知用户。忘记密码的典型方案如下：

▼ 重置忘记密码

1 **用户通过管理员赋予他们的 URL 登录到“密码重置”Web 应用程序。例如：**

`http://hostname:port /ampassword`（适用于默认领域）

或

`http://hostname: port/`*deploy_uri* `/UI/PWResetUserValidation?realm=realmname`， 其中 realmname 为领域名称。

注 – 如果没有为父领域但为子领域启用了“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?realm=realmname`

---

2 **用户输入用户 ID。**

3 **用户将看到在“密码重置”服务中定义以及自定义期间由用户选择的个人问题。如果用户先前没有登录到“用户概要文件”页面且未自定义个人问题，将不会生成密码。**

一旦用户正确回答了问题，便会生成新密码并通过电子邮件发送给用户。无论用户是否正确回答了问题都将为用户发送尝试通知。为确保接收到新密码和尝试通知，用户必须在“用户概要文件”页面上输入他们的电子邮件地址。

密码策略

安全密码策略可通过执行以下操作将与易被猜中密码相关的风险降至最低：

- 用户必须定期更改他们的密码。
- 用户必须提供较复杂的密码。
- 使用错误密码多次进行绑定可能会导致帐户被锁定。

Directory Server 提供了多种在树中的任意节点设置密码策略的方式，此外还有多种策略设置方式。有关详细信息，请参阅以下 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 13 章

13 日志记录服务

Sun Java™ System Access Manager 7 2005Q4 提供了可记录信息（如用户活动、流量模式和授权违规）的“日志记录服务”。此外，调试文件允许管理员排除其安装故障。

日志文件

日志文件为其监视的每项服务记录大量事件。管理员应定期查看这些文件。SPARC 系统的默认日志文件目录为 `/var/opt/SUNWam/logs`，Linux 系统的则为 `/var/opt/sun/identity`。通过使用 Access Manager 控制台可以在“日志记录服务”中配置日志文件目录。

《Sun Java System Access Manager 7 2005Q4 Technical Overview》中的“How the Logging Feature Works”一书中的“How the Logging Feature Works”，以获取默认日志文件类型、所记录的信息和日志文件格式的详细列表。

有关“日志记录服务”的属性定义，请单击 Access Manager 控制台中的“帮助”按钮查看联机帮助。

Access Manager 服务日志

有两种不同类型的服务日志文件：访问日志文件和错误日志文件。访问日志文件可能包含操作尝试和成功结果的记录。错误日志文件记录 Access Manager 服务中出现的错误。平面日志文件附加有 `.error` 或 `.access` 扩展名。Oracle 数据库的数据库列名以 `_ERROR` 或 `_ACCESS` 结尾，而 MySQL 数据库的则是以 `_error` 或 `_access` 结尾。例如，记录控制台事件日志的平面文件名为 `amConsole.access`，而记录相同事件日志的数据库列名为 `AMCONSOLE_ACCESS`。以下各节介绍“日志记录服务”记录的日志文件。

会话日志

“日志记录服务”记录以下“会话服务”事件：

- 登录

- 注销
- 会话空闲超时
- 会话最长超时
- 登录失败
- 会话重新激活
- 会话损坏

会话日志的前缀为 amSSO。

控制台日志

Access Manager 控制台日志记录对与身份相关的对象、策略和服务（其中包括组织、组织单位、用户、角色、策略、组）的创建、删除和修改操作。它还记录对用户属性（包括密码）的修改以及向角色和组中添加用户或从中移除的操作。另外，控制台日志写入委托操作和数据存储库操作。控制台日志的前缀为 amConsole。

验证日志

“验证”组件记录用户登录和注销日志。验证日志的前缀为 amAuthentication。

联合日志

“联合”组件记录与联合相关的事件的日志，其中包括（但不限于）创建“验证域”和创建“托管供应商”。联合日志的前缀为 amFederation。

策略日志

“策略”组件记录与策略相关的事件，其中包括（但不限于）策略管理（策略创建、删除和修改）和策略评估。策略日志的前缀为 amPolicy。

代理日志

策略代理日志负责记录关于允许或拒绝用户访问的日志资源的异常日志。代理日志的前缀为 amAgent。amAgent 日志仅驻留在代理服务器上。代理事件被记录在 Access Manager 服务器上的“验证日志”中。有关该功能的详细信息，请参阅论述策略代理的文档。

SAML 日志

SAML 组件记录与 SAML 相关的事件，其中包括（但不限于）创建或移除声明和辅件、响应和请求的详细信息以及 SOAP 错误。会话日志的前缀为 amSAML。

amAdmin 日志

命令行日志记录使用命令行工具进行操作期间出现的事件错误。其中包括（但不限于）加载服务模式、创建策略和删除用户。命令行日志的前缀为 amAdmin。

日志记录功能

“日志记录服务”具有许多特殊功能，启用它们可以实现附加功能。其中包括“启用安全日志”、“命令行日志”和“远程日志”。

安全日志

此可选功能可以将其他安全性添加到日志记录功能中。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。无需特殊编码即可使用此功能。“安全日志”是通过使用系统管理员配置的预注册证书来完成的。此“清单分析和证书”(Manifest Analysis and Certification, MAC) 是为每个日志记录生成和存储的。定期插入的特殊“签名”日志记录代表了写入该点的日志内容签名。两个记录的组合可以确保日志未被篡改。

▼ 启用安全日志

1. **创建一个名为 Logger 的证书，然后将其安装于运行 Access Manager 的部署容器内。有关详细信息，请参阅部署容器文档。**

2. **使用 Access Manager 控制台打开“日志记录服务”配置中的“安全日志”，然后保存更改。管理员也可修改“日志记录服务”中其他属性的默认值。**

   如果日志目录从默认值 (/var/opt/SUMWam/logs) 进行了更改，则确保将权限设置为 0700。日志记录服务将创建目录（如果不存在），但它会按设置权限为 0755 的情况来创建目录。

   另外，如果指定了与默认目录不同的其他目录，则必须将 Web 容器的 server.policy 文件中的以下参数更改为新的目录：

   ```
   permission java.io.FilePermission “/var/opt/SUNWam/logs/*”,”delete,write”
   ```

3. **在包含证书数据库密码的 *AccessManager-base*/SUNWam/config 目录下创建一个文件，然后将其命名为 .wtpass。**

注 – 可在 AMConfig.properties 文件中配置其文件名和路径。有关详细信息，请参阅附录 A中的“证书数据库”。

出于安全考虑，应确保部署容器用户是唯一拥有读取该文件权限的管理员。

---

4 **重新启动服务器。**

由于某些可导致误解的验证错误在安全日志启动时可能会被写入 `/var/opt/SUNWam/debug/amLog` 文件，因此应清空安全日志目录。

要检测未授权的更改或安全日志篡改，请查找由验证操作写入 `/var/opt/SUNWam/debug/amLog` 的错误信息。要手动检查篡改，请运行 `VerifyArchive` 实用程序。有关详细信息，请参阅第 19 章。

命令行日志

`amadmin` 命令行工具能够在 Directory Server 中创建、修改或删除身份对象（例如，组织、用户和角色）。该工具也可加载、创建和注册服务模板。“日志记录服务”可通过调用 `-t` 选项来记录这些操作。如果 `AMConfig.properties` 中的 `com.iplanet.am.logstatus` 属性被启用 (ACTIVE)，将创建日志记录。（默认情况下将启用该属性。）命令行日志的前缀为 `amAdmin`。有关详细信息，请参阅第 14 章。

日志属性

在 `AMConfig.properties` 文件中有影响日志输出的属性：

`com.iplanet.am.logstatus=ACTIVE`	该属性将启用或禁用日志。默认为 ACTIVE。
`iplanet-am-logging.`*service*`.level=` *level*	*service* 是服务的常规调试文件名。*level* 是 `java.util.logging.Level` 的值之一，表示日志中所记录的详细信息的级别。级别分为：SEVERE、WARNING、INFO、CONFIG、FINE、FINER 和 FINEST。大多数服务不记录详细信息级别高于 INFO 的日志。

远程日志

Access Manager 支持远程日志。这样就允许客户机应用程序使用安装有 Access Manager SDK 的主机，在部署在远程计算机上的 Access Manager 实例中创建日志记录。采用以下任意方案均可启动远程日志：

1. 当 Access Manager 实例的“命名服务”中的日志 URL 指向远程实例，并且在两者之间有已配置的信任关系时，日志将被写入远程 Access Manager 实例。
2. 当根据远程 Access Manager 实例安装 Access Manager SDK，并且在 SDK 服务器上运行的客户机（或简单 Java 类）使用日志 API 时，日志将被写入远程 Access Manager 计算机。
3. 当 Access Manager 代理使用日志 API 时。

▼ 启用远程日志

1 **如果您使用的是 Sun Java System Web Server，则需要在 `server.xml` 配置文件中设置以下环境变量：**

- `java.util.logging.manager=com.sun.identity.log.LogManager`
- `java.util.logging.config.file=/` *AccessManager-base* `/SUNwam/lib/LogConfig.properties`
- 如果正在使用的 Java™ 2 Platform, Standard Edition 为 1.4 或更高版本，此操作需要通过调用以下命令行来完成：

  `java -cp /`*AccessManager-base*`/SUNWam/lib/am_logging.jar:/` *AccessManager-base* `/SUNWam/lib/xercesImpl.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/jaas.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/servlet.jar:/` *AccessManager-base* `/SUNWam/locale:/` *AccessManager-base*`/SUNWam/lib/am_services.jar:/` *AccessManager-base*`/SUNWam/lib/am_sdk.jar:/` *AccessManager-base*`/SUNWam/lib/jss311.jar:/` *AccessManager-base*`/SUNWam/lib:.`

  `-Djava.util.logging.manager=com.sun.identity.log.LogManager`

  `-Djava.util.logging.config.file=/` *AccessManager-base* `/SUNwam/lib/LogConfig.properties <logTestClass>`
- 如果正在使用的 Java 2 Platform, Standard Edition 的版本低于 1.4，此操作需要通过调用以下命令行来完成：

  `java -Xbootclasspath/a:/`*AccessManager-base* `/SUNWam/lib/jdk_logging.jar -cp /` *AccessManager-base* `/SUNWam/lib/am_logging.jar:/` *AccessManager-base* `/SUNWam/lib/xercesImpl.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/jaas.jar:/` *AccessManager-base* `/SUNWam/lib/xmlParserAPIs.jar:/` *AccessManager-base* `/SUNWam/lib/servlet.jar:/` *AccessManager-base* `/SUNWam/locale:/` *AccessManager-base*`/SUNWam/lib/am_services.jar:/` *AccessManager-base*`/SUNWam/lib/am_sdk.jar:/` *AccessManager-base*`/SUNWam/lib/jss311.jar:/` *AccessManager-base*`/SUNWam/lib:.`

  `-Djava.util.logging.manager=com.sun.identity.log.LogManager`

  `-Djava.util.logging.config.file=/` *AccessManager-base* `/SUNwam/lib/LogConfig.properties <logTestClass>`

2 **确保以下各参数是在位于 *AccessManager-base*`/SUNWam/lib` 中的 `LogConfig.properties` 内配置的：**

- `iplanet-am-logging-remote-handler=com.sun.identity.`

  `log.handlers.RemoteHandler`
- `iplanet-am-logging-remote-formatter=com.sun.`

identity.log.handlers.RemoteFormatter

- iplanet-am-logging-remote-buffer-size=1

  远程日志以日志记录数目为基础支持缓冲技术。该值根据记录数目定义日志缓冲区的大小。缓冲区满后，将刷新所有已缓冲的记录到服务器。

- iplanet-am-logging-buffer-time-in-seconds=3600

  该值定义超时期限，可在其中调用日志缓冲区清理程序线程。

- iplanet-am-logging-time-buffering-status=OFF

  该值定义是否启用日志缓冲技术（和缓冲区清理程序线程）。默认情况下，此功能被关闭。

注 – 每当日志文件为空，安全日志记录便可能显示“验证失败。”这是由于创建的文件数量等于归档大小时，安全日志记录将从此组归档并重新启动。在大部分实例中，可忽略此错误。一旦记录数等于归档大小，将不显示此错误。

错误日志和访问日志

存在两种类型的 Access Manager 日志文件：访问日志文件和错误日志文件。

访问日志文件记录与 Access Manager 部署有关的常见审计信息。日志可能包含某事件的单个记录，如验证成功。日志也可能包含同一事件的多个记录。例如，在管理员使用控制台更改属性值时，“日志记录服务”会将此更改尝试记录到一条记录中。“日志记录服务”还会将执行更改的结果记录到第二条记录中。

错误日志文件记录应用程序中发生的错误。将操作错误记录到错误日志的同时，操作尝试将被记录到访问日志文件中。

平面日志文件附加有 .error 或 .access 扩展名。数据库列名以 _ERROR 或 _ACCESS 结尾。例如：记录控制台事件的平面文件名称为 amConsole.access，而记录同样事件的数据库列则命名为 AMCONSOLE_ACCESS 或 amConsole_access。

下表对每个 Access Manager 组件所产生的日志文件进行了简要说明。

表 13–1 Access Manager 组件日志

组件	日志文件名前缀	记录的信息
会话	amSSO	会话管理属性值（如：登录时间、注销时间、超时限制）。
管理控制台	amConsole	通过管理控制台执行的用户操作（如：创建、删除和修改与身份相关的对象、领域和策略）。

表 13–1 Access Manager 组件日志 （续）

组件	日志文件名前缀	记录的信息
验证	amAuthentication	用户登录和注销。
身份联合	amFederation	与联合相关的事件（如：“验证域”的创建以及“托管提供者”的创建）。联合日志的前缀为 amFederation。
验证（策略）	amPolicy	与策略相关的事件（如：策略创建、删除或修改以及策略评估）。
策略代理	amAgent	与资源相关的异常，这些资源被用户访问过，或拒绝用户访问。amAgent 日志驻留在安装策略代理的服务器上。代理事件记录在 Access Manager 计算机上的“验证日志”中。
SAML	amSAML	与 SAML 相关的事件（如：声明和辅件的创建或删除、响应和请求详细信息以及 SOAP 错误）。
命令行	amAdmin	使用命令行工具的操作过程中发生的事件错误。例如：加载服务模式、创建策略以及删除用户。

有关 Access Manager 日志文件列表和描述的详细信息，参见附录 C。

调试文件

调试文件不是“日志记录服务”的某一功能。使用独立于日志 API 的不同 API 可将其写入。调试文件存储在 /var/opt/SUNWam/debug 中。可在 *AccessManager-base*/SUNWam/lib/ 目录下的 AMConfig.properties 文件中配置该存储位置和调试信息的级别。有关调试属性的详细信息，请参阅附录 A。

调试级别

有多个可记录到调试文件的信息级别。调试级别是通过 AMConfig.properties 中的 com.iplanet.services.debug.level 属性来设置的。

1. 关 — 未记录任何调试信息。
2. 错误 — 该级别已用于产品。在生产期间，调试文件中不应有错误。
3. 警告 — 建议当前不使用该级别。
4. 消息 — 该级别可对使用代码跟踪的可能问题发出警报。大多数 Access Manager 模块使用该级别发送调试消息。

注 – 不应在产品中使用“警告”级别和“消息”级别。它们会导致性能严重降低并生成大量调试消息。

调试输出文件

模块对调试文件进行写入操作前不会创建调试文件。因此，在默认的**错误**模式下，可能不生成任何调试文件。在设置调试级别为**消息**的基本登录上所创建的调试文件包括：

- amAuth
- amAuthConfig
- amAuthContextLocal
- amAuthLDAP
- amCallback
- amClientDetection
- amConsole
- amFileLookup
- amJSS
- amLog
- amLoginModule
- amLoginViewBean
- amNaming
- amProfile
- amSDK
- amSSOProvider
- amSessionEncodeURL
- amThreadManager

最常用的文件为 `amSDK`、`amProfile` 以及所有与验证有关的文件。捕获的信息包括日期、时间和消息类型（错误、警告和消息）。

使用调试文件

默认情况下，调试级别设置为**错误**。出现以下情况时，调试文件对于管理员来说可能是有用的：

- 写入自定义验证模块。
- 使用 Access Manager SDK 写入自定义应用程序。`amProfile` 调试文件和 `amSDK` 调试文件捕获此信息。
- 使用控制台或 SDK 时排除访问权限故障。`amProfile` 调试文件和 `amSDK` 调试文件也捕获此信息。
- 排除 SSL 故障。
- 排除 LDAP 验证模块故障。`amAuthLDAP` 调试文件捕获此类信息。

调试文件应与可能在将来拥有的任意故障排除指南同步。例如当 SSL 失败时，某人可能会打开消息调试，然后在 amJSS 调试文件中查找任意特定的证书错误。

多个 Access Manager 实例和调试文件

Access Manager 包含可用于配置服务器大量实例的 ammultiserverinstall 脚本。 如果配置了多个服务器实例以使用不同的调试目录，则每个单独的实例都必须同时拥有调试目录的读写权限。

第 IV 部分

命令行参考

这是“命令行参考”，《Sun Java System Access Manager 7 2005Q4 管理指南》的第四部分。

本部分中介绍的所有命令行工具都可以在以下默认位置找到：

```
AccessManager-base/SUNWam/bin (Solairs)

AccessManager-base/identity/bin (Linux)
```

本部分包含以下各章：

◆ ◆ ◆ 第 14 章

amadmin 命令行工具

本章介绍有关 amadmin 命令行工具的信息。

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 服务文件加载到数据存储库中，以及在 DIT 上执行批管理任务。amadmin 位于 AccessManager-base/SUNWam/bin 中，可用来：

- 加载 XML 服务文件 - 管理员将服务加载到使用在 sms.dtd 中定义的 XML 服务文件格式的 Access Manager 中。所有服务都必须使用 amadmin 加载；它们无法通过 Access Manager 控制台导入。

注 – XML 服务文件作为 Access Manager 所引用 XML 数据的静态 *blobs* 存储在数据存储库中。此信息对 Directory Server 不适用，它只帮助了解 LDAP。

- 执行 DIT 身份对象的批更新 - 管理员可使用在 amadmin.dtd 中定义的批处理 XML 文件格式对 Directory Server DIT 执行批更新。例如，如果管理员要创建 10 个组织、1000 个用户和 100 个组，将请求放入一个或多个批处理 XML 文件中，然后用 amadmin 加载这些文件即可。

注 – amadmin 仅支持 Access Manager 控制台所支持的部分功能，且不可完全替代 Access Manager。建议将控制台用于小型管理任务，将 amadmin 用于大型管理任务。

---

amadmin 语法

要使用 amadmin，必须遵循许多的结构规则。使用该工具的通用语法是：

- 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

以下是 amadmin 命令行参数选项的定义：

--runasdn (-u)

--runasdn 用于验证访问 LDAP 服务器的用户。此参数的值等于被授权运行 amadmin 的用户的区别名 (DN) 的值；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 是一个强制性选项，其值等于用 --runasdn 选项指定的 DN 密码的值。

--locale (-l)

--locale 选项的值等于语言环境名称的值。此选项可用于自定义消息语言。如果没有提供此选项，则使用默认语言环境 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，如果要同时加载三个 XML 文件，并且第一个 XML 文件加载失败，amadmin 将继续加载其余的文件。continue 选项仅应用于独立请求。

--session (-m)

--session (-m) 选项可管理会话或显示当前会话。当指定 --runasdn 时，其值必须与 AMConfig.properties 中超级用户的 DN 相同，或与顶级管理员用户的 ID 相同。

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 模式

该模式可以是一个通配符 (*)。如果此模式 (pattern) 使用通配符 (*)，则必须在 Shell（命令解释器）中用元字符 (\\) 对其进行换码。

--debug (-d)

--debug 选项可以将消息写入在 /var/opt/SUNWam/debug 目录下创建的 amAdmin 文件中。这些消息在技术上很详细，但与 i18n 不兼容。要生成 amadmin 操作日志，应在记入数据库时，手动添加数据库驱动程序的类路径。 例如，当以 amadmin 记入 mysql 时，需添加以下行：

```
CLASSPATH=$CLASSPATH:/opt/IS61/SUNWam/lib/mysql-connector-java-3.0.6-stable-bin.jar
export CLASSPATH
```

--verbose (-v)

--verbose 选项可在屏幕上显示 amadmin 命令的总体进度。它不会将详细信息打印到文件中。输出到命令行的消息与 i18n 兼容。

--data (-t)

--data 选项将正在导入的批处理 XML 文件的名称作为它的值。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。

--schema (-s)

--schema 选项可将 Access Manager 服务的属性加载到 Directory Server 中。它的变量值为在其中定义服务属性的 XML 服务文件。此 XML 服务文件是基于 sms.dtd 的。可以指定一个或多个 XML 文件。

注 – 根据是要对 DIT 配置批更新还是要加载服务模式和配置数据，必须指定 `--data` 或 `--schema` 选项。

--deleteservice (-r)

`--deleteservice` 选项仅用于删除服务及其模式。

--serviceName

`--serviceName` 选项的值等于在 XML 服务文件 `Service name=...` 标签中定义的服务名称。此部分显示在第 190 页中的 “--serviceName” 中。

示例 14–1 `sampleMailService.xml` 的一部分

```
...
<ServicesConfiguration>
    <Service name="sampleMailService" version="1.0">
        <Schema
 serviceHierarchy="/other.configuration/sampleMailService"
            i18nFileName="sampleMailService"
            i18nKey="iplanet-am-sample-mail-service-description">
...
```

--help (-h)

`--help` 参数显示 `amadmin` 命令的语法。

--version (-n)

`--version` 参数显示实用程序名称、产品名称、产品版本和法律声明。

使用 amadmin 进行联合管理

本节列出供“联合管理”使用的 amadmin 参数。有关“联合管理”的详细信息，请参阅 Access Manager Federation Management Guide。

将 Liberty 元数据符合性 XML 装入 Directory Server

```
amadmin -u|--runasdn <user's DN>
-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-g|--import <xmlfile>
```

--runasdn (-u)

用户 DN

--password (-w)

用户密码。

--passwordfile (-f)

包含用户密码的文件的名称。

--entityname (-e)

实体名称。例如，`http://www.example.com`。某一实体应只属于一个组织。

--import (-g)

包含元数据信息的 XML 文件的名称。此文件应该符合 Liberty 元数据规范和 XSD。

将实体导出到 XML 文件（无 XML 数字签名）

amadmin -u|--runasdn <user's DN>

```
-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-o|--export <filename>
```

--runasdn (-u)

用户 DN

--password (-w)

用户密码。

--passwordfile (-f)

包含用户密码的文件的名称。

--entityname (--e)

驻留在 Directory Server 中的实体的名称

--export (-o)

要包含实体的 XML 的文件名称。XML 应符合 Liberty 元数据 XSD。

将实体导出到 XML 文件（有 XML 数字签名）

```
amadmin -u|--runasdn <user's DN>
-w|--password <password> or -f|--passwordfile <passwordfile>
-e|--entityname <entity name>
-q|--exportwithsig <filename>
```

--runasdn (-u)

用户 DN

--password (-w)

用户密码。

--passwordfile (-f)

包含用户密码的文件的名称。

--entityname (--e)

驻留在 Directory Server 中的实体的名称

--exportwithsig (-o)

要包含实体的 XML 的文件名称。此文件已经过数字签名。XML 必须符合 Liberty 元数据 XSD。

将 amadmin 用于资源包

以下章节说明了用于添加、查找和移除资源包的 amadmin 语法。

添加资源包。

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-b|--addresourcebundle <name-of-resource-bundle>

-i|--resourcebundlefilename <resource-bundle-file-name>

[-R|--resourcelocale] <locale>
```

获取资源字符串。

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-z|--getresourcestrings <name-of-resource-bundle>

[-R|--resourcelocale] <locale>
```

移除资源包。

```
amadmin -u|--runasdn <user-dn> -w|--password <user-password>

-j|--deleteresourcebundle <name-of-resource-bundle>

[-R|--resourcelocale] <locale>
```

◆ ◆ ◆ 第 15 章

15 ampassword 命令行工具

本章介绍有关 amPassword 命令行工具的信息，包括下面一节：

ampassword 命令行可执行文件

Access Manager 包含一个 ampassword 实用程序，此程序在 SPARC 系统中位于 /opt/SUNWam/bin 下，在 Linux 系统中位于 /opt/sun/Identity/bin 下。利用该实用程序，您可以更改管理员或用户的 Directory Server 密码。

▼ 用 Access Manager 在 SSL 模式下运行 ampassword

1. **修改位于以下目录的 serverconfig.xml 文件：**

   AccessManager-base/SUNWam/config/

2. **更改 Access Manager 运行的 SSL 端口的 port 服务器属性。**

3. **更改 SSL 的 type 属性。**

   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。 您需要手动更改 ServerConfig.xml 中的密码以及 Access Manager 的所有验证模板。

◆ ◆ ◆ 第 16 章

bak2am 命令行工具

本章介绍有关 bak2am 命令行工具的信息，包含下面一节：

bak2am 命令行可执行文件

Access Manager 在 AccessManager-base/SUNWam/bin 下包含 bak2am 实用程序。此实用程序执行由 am2back 实用程序备份的 Access Manager 组件的恢复。

bak2am 语法

在 Solaris 操作系统下使用 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 操作系统下使用 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` 指定 `tar.gz` 格式的备份文件的完整路径和文件名。默认情况下，此路径为 `AccessManager-base/backup`。此选项仅适用于 Solaris。

--tar *backup-name*

`--tar` 指定 `tar` 格式的备份文件的完整路径和文件名。默认情况下，此路径为 `AccessManager-base/backup`。此选项仅适用于 Solaris。

--verbose

`--verbose` 用于在详细模式下运行备份实用程序。

--directory

`--directory` 指定备份目录。默认情况下，此路径为 `AccessManager-base/backup`。此选项仅适用于 Windows 2000。

--help

`--help` 参数显示 `bak2am` 命令的语法。

--version

`--version` 参数显示实用程序名称、产品名称、产品版本和法律声明。

◆ ◆ ◆ 第 17 章

17 am2bak 命令行工具

本章介绍有关 am2bak 命令行工具的信息。

am2bak 命令行可执行文件

Access Manager 包含一个 am2bak 实用程序，此程序位于 AccessManager-base/SUNWam/bin 下。该实用程序可以对 Access Manager 的全部或部分组件进行备份。在备份日志时必须运行 Directory Server。

am2bak 语法

在 Solaris 操作系统上使用 am2bak 工具的通用语法是：

```
./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 操作系统上使用 am2bak 工具的通用语法是：

```
am2bak [ -v | --verbose ] [ -k | --backup backup-name ] [ -l | --location location ] [[-c
| --config] | [-b | --debug] | [-g | --log] | [-t | --cert] | [-d | --ds] | [-a |
--all]]*

am2bak -h | --help

am2bak -n | --version
```

注 – 必须完全按照语法中所示，输入两个连字符。

am2bak 选项

--verbose (-v)

--verbose 用于在详细模式下运行备份实用程序。

--backup *backup-name (-k)*

--backup *backup-name* 定义备份文件的名称。默认名称为 ambak。

--location (-l)

--location 指定备份文件的目录位置。默认位置为 AccessManager-base/backup。

--config (-c)

--config 指定仅为配置文件备份。

--debug (-b)

--debug 指定仅为调试文件备份。

--log (-g)

--log 指定仅为日志文件备份。

--cert (-t)

--cert 指定仅为证书数据库文件备份。

--ds (-d)

--ds 指定仅为 Directory Server 备份。

--all (-a)

--all 指定对整个 Access Manager 进行完整备份。

--help (-h)

--help 参数显示 am2bak 命令的语法。

--version (-n)

`--version` 参数显示实用程序名称、产品名称、产品版本和法律声明。

▼ 运行备份程序

1 以超级用户身份登录。
运行此脚本的用户必须具有超级用户权限。

2 如果需要，运行确保使用正确路径的脚本。
此脚本将会备份以下 Solaris™ 操作环境文件：

- 配置文件和自定义文件：
  - `AccessManager-base/SUNWam/config/`
    - `AccessManager-base/SUNWam/locale/`
    - `AccessManager-base/SUNWam/servers/httpacl`
    - `AccessManager-base/SUNWam/lib/*.properties`（Java 属性文件）
    - `AccessManager-base/SUNWam/bin/amserver.` *instance-name*
    - `AccessManager-base/SUNWam/servers/https-` *all_instances*
    - `AccessManager-base/SUNWam/servers/web-apps-` *all_instances*
    - `AccessManager-base/SUNWam/web-apps/services/WEB-INF/config`
    - `AccessManager-base/SUNWam/web-apps/services/config`
    - `AccessManager-base/SUNWam/web-apps/applications/WEB-INF/classes`
    - `AccessManager-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`
    - `Access Manager/slapd-` *host* `/config/dse.ldif`

    日志文件和调试文件：

    - `var/opt/SUNWam/logs`（Access Manager 日志文件）
    - `var/opt/SUNWam/install`（Access Manager 安装日志文件）
    - `var/opt/SUNWam/debug`（Access Manager 调试文件）

    证书：

    - `Access Manager/SUNWam/servers/alias`
    - `Access Manager/alias`

      此脚本还将备份以下 Microsoft® Windows 2000 操作系统文件：

    配置文件和自定义文件：

    - `AccessManager-base/web-apps/services/WEB-INF/config/*`
    - `AccessManager-base/locale/*`

- AccessManager-base/web-apps/applications/WEB-INF/classes/*.properties（java 属性文件）
- AccessManager-base/servers/https-*host*/config/jvm12.conf
- AccessManager-base/servers/https-*host*/config/magnus.conf
- AccessManager-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（Access Manager 日志文件）
- var/opt/debug（Access Manager 调试文件）

证书：

- AccessManager-base/servers/alias
- AccessManager/alias

◆ ◆ ◆ 第 18 章

18 amserver 命令行工具

本章介绍有关 amserver 命令行工具的信息。本章包含下面一节：

amserver 命令行可执行文件

amserver 命令行可执行文件启动和停止 amunixd 与 amsercuridd 帮助器，它们分别与 Unix 和 SecurID 验证模块相关。

amserver 语法

使用该工具的通用语法为：

```
./amserver { start | stop }
```

start

start 为启动帮助器的命令。

stop

stop 为停止帮助器的命令。

◆ ◆ ◆ 第 19 章

19 VerifyArchive 命令行工具

本章提供有关 VerifyArchive 命令行工具的信息，包含下面一节：

VerifyArchive 命令行可执行文件

VerifyArchive 用来检验日志归档文件。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。

对于给定 logName，VerifyArchive 会提取所有归档文件集和属于每个归档文件集的所有文件。执行检测时，VerifyArchive 搜索每个日志记录是否进行了篡改。如果检测到篡改，则将打印一条消息，指定已被篡改的文件和记录编号。

VerifyArchive 也检查所有从归档文件集中删除的文件。如果检测到文件被删除，则将打印一条消息，说明验证已失败。如果未检测到文件被篡改或被删除，将返回一条消息，说明归档文件的验证已成功完成。

注 – 如果以无管理员权限的用户身份运行 amverifyarchive，可能会出错。

VerifyArchive 语法

所有的参数选项都是必需的。其语法如下所示：

```
amverifyarchive -l logName -p path -u
uname -w password
```

VerifyArchive 选项

logName

logName 指要验证的日志的名称（如 amConsole、amAuthentication 等）。VerifyArchive 验证给定 logName 的访问和错误日志。例如，如果指定了 amConsole，则验证程序将验证 amConsole.access 和 amConsole.error 文件。logName 也可以指定为 amConsole.access 或 amConsole.error，以限制只验证某些日志。

path

path 是存放日志文件的完整目录路径。

uname

uname 是 Access Manager 管理员的用户 ID。

password

password 是 Access Manager 管理员的密码。

◆ ◆ ◆ 第 20 章

20 amsecuridd 帮助器

本章介绍有关 amsecuiridd 帮助器的信息，包含以下章节：

amsecuridd 帮助器命令行可执行文件

通过安全动态 ACE/客户机 C API 和 amsecruidd 帮助器实现 Access Manager SecurID 验证模块，该帮助器在 Access Manager SecurID 验证模块和 SecurID 服务器之间通信。SecurID 验证模块通过打开套接字 localhost:57943 调用 amsecuridd 守护进程来侦听 SecurID 验证请求。

注 – 57943 为默认端口号。如果此端口号已被使用，可以在 SecurID 验证模块中的“SecurID 帮助器验证端口”属性中指定不同的端口号。此端口号在所有组织中必须唯一。

---

amsecuridd 的接口以明文形式通过 stdin，因此仅允许本地主机连接。amsecuridd 在后台使用 SecurID 远程 API（版本 5.x）进行数据加密。

amsecuridd 帮助器在端口号为 58943（默认）的端口上侦听，以接收其配置信息。如果此端口已被使用，可以在 AMConfig.properties 文件（默认情况下，位于 AccessManager-base /SUNWam/config/）中的 securidHelper.ports 属性中对其进行更改。securidHelp.ports 属性包含每个 amsecuridd 帮助器实例的端口列表（以空格分隔）。保存对 AMConfig.properties 所作的更改后，重新启动 Access Manager。

注 – 应为每个组织运行 amsecuridd 的单独实例，此组织与单独的 ACE/Server（包含不同的 sdconf.rec 文件）进行通信。

---

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，然后登录到 /var/opt/SUNWam/debug/securidd_client.debug 。

configure portnumber (-c portnm)

配置侦听端口号。默认端口为 58943。

运行 amsecuridd 帮助器

默认情况下，amsecuridd 位于 *AccessManager-base* /SUNWam/share/bin。要在默认端口上运行帮助器，请输入以下命令（不需要选项）：

```
./amsecuridd
```

要在非默认端口上运行帮助器，请输入以下命令：

```
./amsecuridd [-v] [-c portnm]
```

amsecuridd 也可以通过 amserver 命令行实用程序运行，但其只能在默认端口上运行。

必需的库

为了运行帮助器，需要以下的库（多数库位于操作系统的 /usr/lib/ ）：

- 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 *AccessManager-base* /Sunwam/lib/ 以找到 libaceclnt.so。

第 V 部分

附录

这是《Sun Java System Access Manager 7 2005Q4 管理指南》的第五部分，包含错误代码列表和文件参考。本部分包含以下附录：

- 附录 A
- 附录 B
- 附录 C
- 附录 D

◆ ◆ ◆ 附 录 A

AMConfig.properties 文件

AMConfig.properties 是 Access Manager 的主配置文件。您可以配置此文件中的某些属性而不是全部属性。本章提供了在 AMConfig.properties 中包含的属性说明、默认属性值以及有关修改某些值的说明（这些值可以被更改而不会导致 Access Manager 不可用）。

本章包括以下内容：

- 第 233 页中的 “SMTP”
- 第 233 页中的 “统计服务”

关于 AMConfig.properties 文件

在安装期间，AMConfig.properties 位于以下目录：/etc/opt/SUNWam/config。

AMConfig.properties 每行包含一个属性，每个属性都有一个对应的值。属性和值区分大小写。以斜杠和星号 (/*) 开始的行为注释，应用程序会忽略这种注释。注释的最后一行以星号和斜杠(*/)结尾。

修改 AMConfig.properties 中的属性后，必须重新启动 Access Manager 以激活更改。

Access Manager 控制台

- com.iplanet.am.console.deploymentDescriptor

  其值在安装期间设置。示例：/amconsole
- com.iplanet.am.console.host

  其值在安装期间设置。示例：*hostName.domain.Name*.com
- com.iplanet.am.console.port

  其值在安装期间设置。示例：80
- com.iplanet.am.console.protocol

  其值在安装期间设置。示例：http

Access Manager 服务器安装

- com.iplanet.am.install.basedir

  此为“只读”属性。不要修改属性值。

  其值在安装期间设置。示例：/opt/SUNWam/web-src/services/WEB-INF
- com.iplanet.am.install.vardir

  此为“只读”属性。不要修改属性值。

  其值在安装期间设置。示例：/var/opt/SUNWam
- com.iplanet.am.installdir

  此为“只读”属性。不要修改属性值。

  其值在安装期间设置。示例：/opt/SUNWam
- com.iplanet.am.jdk.path

  其值在安装期间设置。示例：/usr/jdk/entsys-j2se

- `com.iplanet.am.locale`

  其值在安装期间设置。示例：`en_US`

- `com.iplanet.am.server.host`

  其值在安装期间设置。示例：*hostName.domainName*`.com`

- `com.iplanet.am.server.port`

  其值在安装期间设置。示例：`80`

- `com.iplanet.am.server.protocol`

  其值在安装期间设置。示例：`http`

- `com.iplanet.am.version`

  其值在安装期间设置。示例：`7 2005Q4`

- `com.sun.identity.server.fqdnMap[ ]`

  启用 Access Manager 验证服务可以使 Access Manager 在用户输入了错误的 URL 时进行纠错。例如，当用户指定了部分主机名或使用 IP 地址访问受保护的资源时，这很有用。

  该属性的语法表示无效的 FQDN 值被映射到相应的有效值。此属性使用以下格式：`com.sun.identity.server.fqdnMap[`*invalid-name*`]=`*valid—name* 。在此示例中，*invalid-name* 是用户可能使用的无效的 FQDN 主机名，*valid—name* 是过滤器将用户重定向到的 FQDN 主机名。如果同一个无效的 FQDN 存在重叠值，则应用程序可能会无法访问。使用此属性的无效值也可以导致应用程序无法访问。可以使用此属性映射多个主机名。当服务器托管的应用程序能用多个主机名访问时，这很有用。

  可以使用此属性配置 Access Manager，以便不对特定主机名的 URL 进行修正操作。这在要求不进行修正操作（如不对使用原始 IP 地址访问应用程序资源的用户进行重定向）时会很有帮助。

  可以指定映射条目，如：`com.sun.identity.server.fqdnMap[`*IP* `]=`*IP* .

  可以指定任意数量的此类属性，只要它们是有效属性并且符合上述要求。示例：
  `com.sun.identity.server.fqdnMap[`*isserver*`]=`*isserver.mydomain.com*
  `com.sun.identity.server.fqdnMap[`*isserver.mydomain*`]=`*isserver.mydomain.com*
  `com.sun.identity.server.fqdnMap[`*IP address*`]=`*isserver.mydomain.com*

am.util

- `com.iplanet.am.util.xml.validating`

  默认值为 `no`。当使用 Access Manager `XMLUtils` 类解析 XML 文档时，确定是否需要进行验证。此属性仅在 `com.iplanet.services.debug.level` 属性的值设置为 `warning` 或 `message` 时才有效。允许的值为 `yes` 和 `no`。仅当此属性的值为 `yes`，并且 `com.iplanet.services.debug.level` 属性设置为 `warning` 或 `message` 时，才会启用 XML 文档验证。

amSDK

每个 SDK 高速缓存条目存储用户的一组 AMObject 属性值。

- com.iplanet.am.sdk.cache.maxSize

  默认值为 10000。指定启用缓存时 SDK 高速缓存的大小。请使用大于 0 的整数，或者使用默认大小（10000 个用户）。

- com.iplanet.am.sdk.userEntryProcessingImpl

  此属性指定实现 com.iplanet.am.sdk.AMUserEntryProcessed 接口的插件以执行用户创建、删除和修改操作的一些后期处理。如果使用此属性，应指定实现以上接口的全限定类名。

- com.iplanet.am.sdk.caching.enabled

  将此属性设置为 true 将启用高速缓存，设置为 false 则禁用高速缓存。默认值为 false。

Application Server 安装

- com.iplanet.am.iASConfig

  其值在安装期间设置。示例：APPSERVERDEPLOYMENT

  此属性用来确定 Access Manager 是否在 iPlanet Application Server 上运行。

验证

- com.sun.identity.auth.cookieName

  默认值为 AMAuthCookie。指定用于“验证服务”的 Cookie 名称以设置验证过程中的会话处理程序 ID。一旦此过程完成（成功或失败），此 Cookie 就被会清除或删除。

- com.sun.identity.authentication.ocsp.responder.nickname

  其值在安装期间设置。该响应器的证书授权机构 (CA) 证书昵称。示例：**证书管理器** - sun。如果设置了该值，则 CA 证书必须出现在 Web 服务器的证书数据库中。

- com.sun.identity.authentication.ocsp.responder.url

  其值在安装期间设置。示例： http://ocsp.sun.com/ocsp

  指定此实例的全局 OCSP 响应器 URL。 如果设置了 OCSP 响应器 URL，也必须设置 OCSP 响应器的昵称。否则此二者将被忽略。如果二者都没有设置，则用户证书中出现的 OCSP 响应器 URL 将用于 OCSP 验证。 如果 OCSP 响应器 URL 没有出现在用户证书中，则不会执行 OCSP 验证。

- com.sun.identity.authentication.ocspCheck

  默认值为 true。启用或禁用 OCSP 检查的全局参数。 如果该值为 false，则不能使用“证书验证”模块类型中的 OCSP 功能。。

- com.sun.identity.authentication.special.users

其值在安装期间设置。示例：`cn=dsameuser,ou=DSAME Users,o=AMRoot|cn=amService-UrlAccessAgent,ou=DSAME Users,o=AMRoot`

确定此 Access Manager 验证组件的特殊用户或用户组。“客户机 API”使用此用户根据完整用户 DN 向 Access Manager 服务器验证远程应用程序。始终根据本地目录服务器验证此用户。此特殊用户 DN 的多个值用管道字符 (|) 分隔开。 此属性仅限“验证”组件使用。

- `com.sun.identity.authentication.super.user`

  其值在安装期间设置。示例：`uid=amAdmin,ou=People,o=AMRoot`

  确定此 Access Manager 实例的超级用户。此用户必须使用 LDAP 登录，并且必须使用完整 DN。始终根据本地 Directory Server 验证此用户。

- `com.sun.identity.authentication.uniqueCookieDomain`

  用于设置上述 Cookie 名称的 Cookie 域。此 Cookie 域的设置应包含网络中安装的 CDC（跨域控制器）服务的所有实例。例如 `.example.com`，如果所有 Access Manager 实例都在域 `example.com` 中。

- `com.sun.identity.authentication.uniqueCookieName`

  默认值为 `sunIdentityServerAuthNServer`。 指定当 Access Manager 遭遇会话 Cookie 劫持时设置给 Access Manager 服务器主机 URL 的 Cookie 名称。

- `com.iplanet.am.auth.ldap.createUserAttrList`

  指定将“验证服务”配置为动态创建用户时包含在 LDAP 验证期间将从外部 Directory Server 检索的值的用户属性列表。在本地 Directory Server 中创建的新用户将具有从外部 Directory Server 检索的属性的值。

  示例：*attribute1*, *attribute2*, *attribute3*

证书数据库

当为 SSL 配置 iPlanet Web 服务器时，设置这些属性可以初始化 JSS Socket Factory。

- `com.iplanet.am.admin.cli.certdb.dir`

  其值在安装期间设置。示例：`/opt/SUNWwbsvr/alias`

  指定证书数据库路径。

- `com.iplanet.am.admin.cli.certdb.passfile`

  其值在安装期间设置。示例：`/etc/opt/SUNWam/config/.wtpass`

  指定证书数据库密码文件。

- `com.iplanet.am.admin.cli.certdb.prefix`

  其值在安装期间设置。示例：`https-`*`hostName.domainName`*`.com-`*`hostName`*`-`

  指定证书数据库前缀。

Cookie

- com.iplanet.am.cookie.encode

  此属性允许 Access Manager URL **编码** Cookie 值，即将字符转换为 HTTP 能够解读的字符。

  其值在安装期间设置。示例：false

- com.iplanet.am.cookie.name

  默认值为 iPlanetDirectoryPro。“验证服务”用于设置有效会话处理程序 ID 的 Cookie 名称。此 Cookie 名称的值可用于检索有效会话信息。

- com.iplanet.am.cookie.secure

  允许在安全模式下设置 Access Manager Cookie，在此模式下，当使用安全协议（如 HTTP(s)）时，浏览器将仅返回 Cookie。

  默认值为 false。

- com.iplanet.am.console.remote

  其值在安装期间设置。示例：false

  确定控制台是安装在远程机上还是安装在本地机上供验证控制台使用。

- com.iplanet.am.pcookie.name

  指定持久 Cookie 的 Cookie 名称。当浏览器窗口关闭以后，持久 Cookie 继续存在。这使用户能够用新的浏览器会话登录而无需重新验证。默认值为 DProPCookie。

- com.sun.identity.cookieRewritingInPath

  默认值为 true。当 Access Manager 被配置为在 Cookieless 模式下运行时，此属性由“验证服务”读取。此属性指定需要使用以下格式将 Cookie 作为附加路径信息重新写入 URL 中：protocol://server:port/uri;*cookiename*= cookieValue?queryString. 如果未指定此属性，则 Cookie 将作为查询字符串的一部分写入。

- com.sun.identity.enableUniqueSSOTokenCookie

  默认值为 false。当值设置为 true 时，表示 Access Manager 遭遇了会话 Cookie 劫持。

调试

- com.iplanet.services.debug.directory

  指定将在其中创建调试文件的输出目录。其值在安装期间设置。示例：/var/opt/SUNWam/debug

- com.iplanet.services.debug.level

  指定调试级别。默认值为 error。可能的值包括：

off	不创建调试文件。
error	仅记录错误消息。
warning	仅记录警告消息。

`message` 记录错误、警告和通知消息。

Directory Server 安装

- `com.iplanet.am.defaultOrg`
  其值在安装期间设置。示例：`o=AMRoot`
  指定 Access Manager 信息树中的顶级领域或组织。
- `com.iplanet.am.directory.host`
  其值在安装期间设置。示例：*DirectoryServerHost.domainName*.com
  指定 Directory Server 的全限定主机名。
- `com.iplanet.am.directory.port`
  其值在安装期间设置。示例：`389`
  指定 Directory Server 端口号。
- `com.iplanet.am.directory.ssl.enabled`
  默认值为 `false`。指明安全套接字层 (SSL) 是否已启用。
- `com.iplanet.am.domaincomponent`
  其值在安装期间设置。示例：`o=AMRoot`
  指定 Access Manager 信息树的域组件 (dc) 属性。
- `com.iplanet.am.rootsuffix`
  其值在安装期间设置。示例：`o=AMRoot`

事件连接

- `com.iplanet.am.event.connection.delay.between.retries`
  默认值为 3000。 指定重试重新建立事件服务连接之间的延时（以毫秒为单位）。
- `com.iplanet.am.event.connection.ldap.error.codes.retries`
  默认值为 `80`、`81`、`91`。指定重试重新建立事件服务连接将触发的 LDAP 异常错误代码。
- `com.iplanet.am.event.connection.num.retries`
  默认值为 `3`。指定尝试成功重新建立事件服务连接的次数。
- `com.sun.am.event.connection.idle.timeout`
  默认值为 `0`。指定重新启动持久搜索之前的分钟数。

该属性在负载平衡器或防火墙位于策略代理和 Directory Server 之间并且持久搜索连接因 TCP `idle timeout` 断开时使用。此属性的值应小于负载平衡器或防火墙 TCP 超时的值。这样可以确保在连接断开之前重新启动持久搜索。值 `0` 表示不重新启动持久搜索。仅重置超时的连接。

全局服务管理

- `com.iplanet.am.service.secret`

  其值在安装期间设置。示例：`AQICPX9e1cxSxB2RSy1WG1+O4msWpt/6djZl`
- `com.iplanet.am.services.deploymentDescriptor`

  其值在安装期间设置。示例：`/amserver`
- `com.iplanet.services.comm.server.pllrequest.maxContentLength`

  默认值为 `16384` 或 16k。指定 Access Manager 接受的 `HttpRequest` 的最大内容长度。
- `com.iplanet.services.configpath`

  其值在安装期间设置。示例：`/etc/opt/SUNWam/config`

帮助器守护进程

- `com.iplanet.am.daemons`

  默认值为 `unix securid`。说明
- `securidHelper.ports`

  默认值为 `58943`。该属性采用以空格分隔的列表，用于 SecurID 验证模块和帮助器。
- `unixHelper.ipaddrs`

  其值在安装期间设置。指定 IP 地址列表，当启动帮助器时，`amserver` 脚本读取此列表并将其传送给 UNIX 帮助器。此属性包含以空格分隔的可信赖 IPv4 格式 IP 地址列表。
- `unixHelper.port`

  默认值为 58946。用于 UNIX 验证模块类型。

身份联合

- `com.sun.identity.federation.alliance.cache.enabled`

  默认值为 `true`。如果为 `true`，联合元数据将在内部缓存。
- `com.sun.identity.federation.fedCookieName`

  默认值为 `fedCookie`。指定联合服务 Cookie 的名称。
- `com.sun.identity.federation.proxyfinder`

默认值为 com.sun.identity.federation.services.FSIDPProxyImpl。定义实现以查找要被代理的首选身份提供者。

- com.sun.identity.federation.services.signingOn

  默认值为 false。指定 Liberty 请求和响应的签名验证级别。

  true　Liberty 请求和响应将在发送时签署，并且接收的 Liberty 请求和响应将进行签名有效性验证。

  false　发送和接收的 Liberty 请求和响应将不进行签名验证。

  optional　仅当联合配置文件要求时，Liberty 请求和响应才会进行签署或验证。

- com.sun.identity.password.deploymentDescriptor

  其值在安装期间设置。示例：/ampassword

- com.sun.identity.policy.Policy.policy_evaluation_weights

  默认值为 10:10:10。指定评估策略主题、规则和条件的比例处理成本。指定的值将影响策略的主题、规则和条件的评估顺序。此值用三个代表主题、规则和条件的整数来表示。此值以冒号 (:) 分隔，指示评估策略主题、规则和条件的比例处理成本。

- com.sun.identity.session.application.maxCacheTime

  默认值为 3。指定“应用程序会话”缓存时间的最大分钟数。默认情况下，如果不启用该属性高速缓存就不会终止。

- com.sun.identity.sm.ldap.enableProxy

  默认值为 false。指定连接要使用的“代理服务器”。如果后端存储器支持 LDAPProxy，则将该值设为 true。如果为 true，则为连接使用“代理服务器”；如果为 false，则不为连接使用“代理服务器”。

- com.sun.identity.webcontainer

  其值在安装期间设置。示例：WEB_CONTAINER

  指定 Web 容器的名称。尽管 servlet 或 JSP 与 Web 容器无关，但 Access Manager 仍然使用 servlet 2.3 API request.setCharacterEncoding() 对收到的非英语字符正确解码。如果将 Access Manager 部署在 Sun Java System Web Server 6.1 上，这些 API 将不会运行。Access Manager 使用 gx_charset 机制正确解码 Sun Java System Web 服务器版本 6.1 和 S1AS7.0 中接收的数据。可能的值包括 BEA6.1、BEA 8.1、IBM5.1 或 IAS7.0。如果 Web 容器为 Sun Java System Web Server，则不替换标记。

JSS 代理

这些属性标识了 SSL ApprovalCallback 的值。如果启用了 checkSubjectAltName 或 resolveIPAddress 功能，则必须在 com.iplanet.am.admin.cli.certdb.dir 目录中创建带有前缀值 com.iplanet.am.admin.cli.certdb.prefix 的 cert7.db 和 key3.db。然后重新启动 Access Manager。

- com.iplanet.am.jssproxy.checkSubjectAltName

默认值为 false。当启用时，服务器证书包括“主题替换名”(SubjectAltName) 扩展名， 并且 Access Manager 会检查扩展名中的所有名称条目。如果 SubjectAltName 扩展名中的名称之一与服务器 FQDN 相同，则 Access Manager 将继续进行 SSL 信息交换。要启用此属性，请将其设置为用逗号分隔的可信赖 FQDN 列表。例如

: com.iplanet.am.jssproxy.checkSubjectAltName=
amserv1.example.com,amserv2.example.com

- com.iplanet.am.jssproxy.resolveIPAddress

  默认值为 false。

- com.iplanet.am.jssproxy.trustAllServerCerts

  默认值为 false。如果启用 (true)，Access Manager 将忽略所有与证书相关的问题（如名称冲突）并继续进行 SSL 信息交换。为防止可能的安全性风险，请仅在测试时，或企业网被严密控制时启用此属性。如果可能会出现安全性风险（例如，如果服务器连接到不同网络的服务器），请避免启用此属性。

- com.iplanet.am.jssproxy.SSLTrustHostList 如果设置了此属性，则 Access Manager 将检查正在被访问的服务器主机的 “平台服务器” 列表。如果 “平台服务器” 列表中两台服务器的服务器 FQDN 匹配，Access Manager 将继续 SSL 握手。使用以下语法来设置属性：

  com.iplanet.am.jssproxy.SSLTrustHostList = *fqdn_am_server1* ,*fqdn_am_server2*, *fqdn_am_server3*

- com.sun.identity.jss.donotInstallAtHighestPriority

  默认值为 false。确定是否以最高优先级将 JSS 添加到 JCE。如果应使用其他 JCE 提供者进行数字签名和加密，则将该值设置为 true。

LDAP 连接

- com.iplanet.am.ldap.connection.delay.between.retries

  默认值为 1000。指定重试间隔的毫秒数。

- com.iplanet.am.ldap.connection.ldap.error.codes.retries

  默认值为 80、81、91。指定重试重新建立 LDAP 连接将触发的 LDAPException 错误代码。

- com.iplanet.am.ldap.connection.num.retries

  默认值为 3。指定尝试成功重新建立 LDAP 连接的次数。

Liberty 联盟交互

- com.sun.identity.liberty.interaction.htmlStyleSheetLocation

  其值在安装期间设置。示例： /opt/SUNWam/lib/is-html.xsl

  指定生成 HTML 交互页面的样式表的路径。

- com.sun.identity.liberty.interaction.wmlStyleSheetLocation

  其值在安装期间设置。示例： /opt/SUNWam/lib/is-wml.xsl

  指定提供 WML 格式的交互页面的样式表路径。

- com.sun.identity.liberty.interaction.wscSpecifiedInteractionChoice

  默认值为 interactIfNeeded。指明 Web 服务使用方是否参与交互。允许的值为：

interactIfNeeded	仅在必要时进行交互。还在指定的值无效时使用。
doNotInteract	无交互。
doNotInteractForData	无数据交互。

- com.sun.identity.liberty.interaction.wscSpecifiedMaxInteractionTime

  默认值为 80。Web 服务使用方对于可接受交互持续时间的首选项。该值以秒表示。 如果没有指定值或指定了非整数的值，则使用默认值。

- com.sun.identity.liberty.interaction.wscWillEnforceHttpsCheck

  默认值为 yes。指明 Web 服务使用方是否强制执行重定向至 URL 的请求使用 HTTPS 的要求。有效值为 yes 和 no。不区分大小写。Liberty 规范要求值为 yes。如果没有指定值，则将使用默认值。

- com.sun.identity.liberty.interaction.wscWillInlcudeUserInteractionHeader

  默认值为 yes。如果没有指定值，则将使用默认值。指示 Web 服务使用方是否包括 userInteractionHeader。允许的值为 yes 和 no。不区分大小写。

- com.sun.identity.liberty.interaction.wscWillRedirect

  默认值为 yes。指示 Web 服务使用方是否重定向用户以进行交互。有效值为 yes 和 no。如果没有指定值，则将使用默认值。

- com.sun.identity.liberty.interaction.wspRedirectHandler

  其值在安装期间设置。示例：
  http://*hostName.domainName*.com:*portNumber*/amserver/WSPRedirectHandler

  指定用来处理基于用户代理重定向的 Liberty WSF WSP 资源拥有者交互的 URL WSPRedirectHandlerServlet。这应与 Liberty 服务提供者运行于同一个 JVM 上。

- com.sun.identity.liberty.interaction.wspRedirectTime

  默认值为 30。Web 服务提供者预期的交互持续时间。 以秒表示。如果没有指定值或指定了非整数值，则使用默认值。

- com.sun.identity.liberty.interaction.wspWillEnforceHttpsCheck

默认值为 yes。如果没有指定值，则将使用默认值。指明 Web 服务使用方是否强制执行 returnToURL 使用 HTTPS 的要求。有效值为 yes 和 no。（不区分大小写）Liberty 规范要求值为 yes。

- com.sun.identity.liberty.interaction.

  wspWillEnforceReturnToHostEqualsRequestHost

  Liberty 规范要求值为 yes。 指示 Web 服务使用方是否强制要求 returnToHost 和 requestHost 相同。有效值为 yes 和 no。

- com.sun.identity.liberty.interaction.wspWillRedirect

  默认值为 yes。如果没有指定值，则将使用默认值。指示 Web 服务提供者是否重定向用户以进行交互。有效值为 yes 和 no。不区分大小写。

- com.sun.identity.liberty.interaction.wspWillRedirectForData

  默认值为 yes。如果没有指定值，则将使用默认值。指明 Web 服务提供者是否重定向用户以进行数据交互。有效值为 yes 和 no。不区分大小写。

- com.sun.identity.liberty.ws.interaction.enable

  默认值为 false。

- com.sun.identity.liberty.ws.jaxb.namespacePrefixMappingList

  默认值为

  ```
  =S=http://schemas.xmlsoap.org/soap/envelope/|sb=urn:liberty:sb:2003-08

  |pp=urn:liberty:id-sis-pp:2003-08|ispp=http://www.sun.com/identity/

  liberty/pp|is=urn:liberty:is:2003-08
  ```

  。指定将 JAXB 内容树结构化为 DOM 树时使用的名称空间前缀映射。语法为 prefix=namespace|prefix=namespace|...

- com.sun.identity.liberty.ws.jaxb.packageList

  指定构建 JAXBContext 时使用的 JAXB 软件包列表。每个软件包必须用冒号 (:) 分隔。

- com.sun.identity.liberty.ws.security.TokenProviderImpl

  默认值为 com.sun.identity.liberty.ws.security.AMSecurityTokenProviderDescription。

- com.sun.identity.liberty.ws.soap.certalias

  其值在安装期间设置。SSL 连接中将用于“Liberty SOAP 绑定”的客户机证书别名。

- com.sun.identity.liberty.ws.soap.messageIDCacheCleanupInterval

  默认值为 60000。指定缓存清理事件开始前所需时间的毫秒数。存储在高速缓存中的每条消息都带有自身的 messageID 以免消息重复。当消息的当前时间减去接收的时间超出 staleTimeLimit 值时，此消息将被从高速缓存中删除。

- com.sun.identity.liberty.ws.soap.staleTimeLimit

默认值为 300000。确定消息是否过时从而不再值得信赖。如果消息的时间戳比当前时间戳早指定毫秒数，则该消息将被视为过时。

- com.sun.identity.liberty.ws.soap.supportedActors

  默认值为 http://schemas.xmlsoap.org/soap/actor/next。指定支持的 SOAP 参与者。各个参与者之间必须用管道字符 (|) 分隔开。

- com.sun.identity.liberty.ws.ta.certalias

  其值在安装期间设置。为将用于签署 SAML 或 SAML 的可信赖授权机构指定证书别名。响应消息的 BEARER 令牌。

- com.sun.identity.liberty.ws.wsc.certalias

  其值在安装期间设置。为此 Web 服务客户机指定用于发布 Web 服务安全令牌的默认证书别名。

- com.sun.identity.liberty.ws.ta.certalias

  其值在安装期间设置。为将用于签署 SAML 或 SAML 的可信赖授权机构指定证书别名。响应消息的 BEARER 令牌。

- com.sun.identity.liberty.ws.trustedca.certaliases

  其值在安装期间设置。

  为可信赖的 CA 指定证书别名。接收的请求的 SAML 或 SAML BEARER 令牌。消息必须由此列表中的可信赖 CA 签署。语法为
  cert alias 1[:*issuer 1*]|*cert alias 2*[:*issuer 2*]|....。
  示例： myalias1:myissuer1|myalias2|myalias3:myissuer3。
  当签名中没有令牌的 KeyInfo 时，将使用值 issuer。令牌的发布者必须在此列表中，相应的证书别名将用于验证签名。如果 KeyInfo 存在，则关键字库必须包含与此 KeyInfo 相匹配的证书别名，并且该证书别名必须在此列表中。

- com.sun.identity.liberty.ws.security.TokenProviderImpl

  其值在安装期间设置。指定安全令牌提供者的实现。

- com.sun.identity.saml.removeassertion

  默认值为 true。该标记指示是否应该从缓存中删除去除引用的声明。适用于已创建的与辅件相关联且已去除引用的声明。

日志记录服务

- com.iplanet.am.logstatus

  指定是打开 (ACTIVE) 还是关闭 (INACTIVE) 日志。在安装过程中，该值被设置为 ACTIVE。

可以添加到 AMConfig.properties 的日志属性

通过在 AMConfig.properties 文件中添加属性，可以配置包含在特定日志文件中的信息的详细程度。请使用以下格式：

iplanet-am-logging.*logfileName* .level=*java.util.logging.Level*，此处，*logfileName* 为 Access Manager 服务（参见表 1）的日志文件名，*java.util.logging.Level* 为允许的属性值。Access Manager 服务在 INFO 级别记录日志。SAML 和身份联合服务也在更详细的级别 (FINE、FINER、FINEST) 记录日志。示例：

```
iplanet-am-logging.amSSO.access.level=FINER
```

也可以关闭登录到某个特定日志文件。示例：

```
iplanet-am-logging.amConsole.access.evel=OFF
```

表 A–1 Access Manager 日志文件

日志文件名	记录的记录
amAdmin.access	成功的 amadmin 命令行事件
amAdmin.error	amadmin 命令行错误事件
amAuthLog.access	与 Access Manager 策略代理相关的事件。请参阅此表后的注释。
amAuthentication.access	成功的验证事件
amAuthentication.error	验证失败
amConsole.access	控制台事件
amConsole.error	控制台错误事件。
amFederation.access	成功的联合事件。
amFederation.error	联合错误事件。
amPolicy.access	策略存储允许事件
amPolicy.error	策略存储拒绝事件
amSAML.access	成功的 SAML 事件
amSAML.error	SAME 错误事件
amLiberty.access	成功的 Liberty 事件
amLiberty.error	Liberty 错误事件
amSSO.access	单点登录的创建和破坏
amSSO.error	单点登录错误事件

注 – amAuthLog 文件名取决于 AMAgent.properties 中的“策略代理”属性。对于“Web 策略代理”，此属性为 com.sun.am.policy.agents.config.remote.log。对于“J2EE 策略代理”，此属性为 com.sun.identity.agents.config.remote.logfile。默认为 amAuthLog.*host.domain.port*，其中 *host.domain* 是运行“策略代理”Web 服务器的主机的全限定主机名，*port* 是该 Web 服务器的端口号。如果部署了多个“策略代理”，则可以有此文件的多个实例。属性 com.sun.identity.agents.config.audit.accesstype（适用于 Web 和 J2EE 代理）用于确定哪些数据将被远程记录。记录的数据可以包括策略允许、策略拒绝、允许和拒绝或既不允许也不拒绝。

命名服务

- com.iplanet.am.naming.failover.url

  此属性在 Access Manager 7.0 中不再使用。

- com.iplanet.am.naming.url

  其值在安装期间设置。示例：http://*hostName.domainName*.com:*portNumber*/amserver/namingservice

  指定要使用的命名服务 URL。

通知服务

使用以下关键字配置通知线程池。

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

  默认值为 10。通过指定总线程数定义线程池的大小。

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

  默认值为 100。指定任务队列最大长度。

  通知任务到达后，被发送至任务队列等待处理。如果队列达到最大长度，则以后接收的请求将被拒绝，并出现 ThreadPoolException，直到队列出现空缺。

- com.iplanet.am.notification.url

  其值在安装期间设置。示例：http://*hostName.domainName*.com:*portNumber*/amserver/notificationservice

策略代理

- com.iplanet.am.policy.agents.url.deploymentDescriptor

  其值在安装期间设置。示例： AGENT_DEPLOY_URI

- com.sun.identity.agents.app.username

  默认值为 UrlAccessAgent。为应用程序验证模块指定要使用的用户名。

- com.sun.identity.agents.cache.size

  默认值为 1000。指定资源结果高速缓存的大小。在安装策略代理的服务器上创建高速缓存。

- com.sun.identity.agents.header.attributes

  默认值为 cn、ou、o、mail、employeenumber、c。指定策略评估者要返回的策略属性。使用格式 a[,...]。在本示例中，a 是数据存储库中要获取的属性。

- com.sun.identity.agents.logging.level

  默认值为 NONE。控制策略客户机 API 日志记录级别的粒度。默认值为 NONE。可能的值包括：

  ALLOW　记录**允许的访问**请求。

  DENY　记录**拒绝的访问**请求。

  BOTH　记录**允许的访问**和**拒绝的访问**请求。

  NONE　不记录请求。

- com.sun.identity.agents.notification.enabled

  默认值为 false。为策略客户机 API 启用或禁用通知。

- com.sun.identity.agents.notification.url

  策略代理 SDK 将其用于注册策略更改通知。 错误配置此属性将导致策略通知被禁用。

- com.sun.identity.agents.polling.interval

  默认值为 3。指定轮询间隔，该间隔为条目从客户机 API 高速缓存断开之前的分钟数。

- com.sun.identity.agents.resource.caseSensitive

  默认值为 false。说明

  指示策略评估期间是开启还是关闭区分大小写。

- com.sun.identity.agents.true.value

  指示策略操作的真实值。如果应用程序不需要访问 PolicyEvaluator.isAllowed 方法，则可以忽略该值。该值表示应如何解释 Access Manager 的策略决策。默认值为 allow。

- com.sun.identity.agents.resource.comparator.class

  默认值为 com.sun.identity.policy.plugins.URLResourceName

指定资源比较类名。 可用的实现类包括
：com.sun.identity.policy.plugins.PrefixResourceName 和
com.sun.identity.policy.plugins.URLResourceName.

- com.sun.identity.agents.resource.delimiter

  默认值为反斜线 (/)。为资源名称指定分隔符。

- com.sun.identity.agents.resource.wildcard

  默认值为 *。为资源名称指定通配符。

- com.sun.identity.agents.server.log.file.name

  默认值为 amRemotePolicyLog。指定将消息记录到 Access Manager 要使用的日志文件名。只需指定文件名。 文件目录由其他 Access Manager 配置设置决定。

- com.sun.identity.agents.use.wildcard

  默认值为 true。指示是否将通配符用于资源名称比较。

策略客户机 API

- com.sun.identity.policy.client.booleanActionValues

  iPlanetAMWebAgentService|POST|allow|deny

  默认值为 iPlanetAMWebAgentService|GET|allow|deny:。

  为策略操作名称指定布尔操作值。使用格式
  serviceName|actionName|trueValue|falseValue。操作名称的值用冒号 (:) 分隔。

- com.sun.identity.policy.client.cacheMode

  默认值为 self。为客户机策略评估者指定高速缓存模式。有效值为 subtree 和 self。如果设置为 subtree，则策略评估者可以从服务器获得来自实际请求的资源根目录的所有资源的策略决策。如果设置为 self，则策略评估者仅可从服务器获得实际请求的资源的策略决策。

- com.sun.identity.policy.client.clockSkew

  调整策略客户机机器和策略服务器之间的时间差。如果该属性不存在，并且策略代理时间不同于策略服务器时间，则会偶尔遇到错误的策略决策。必须运行时间同步服务，以使策略服务器上的时间和策略客户机上的时间尽量保持一致。使用此属性调整微小的时间差，不考虑运行时间同步服务。时钟相位差（以秒计） = agentTime - serverTime。注释掉策略服务器上的属性。不注释行，设置策略客户机或运行策略代理代理 - 服务器时钟相位差（以秒计）的机器上适当的值。

- com.sun.identity.policy.client.resourceComparators=

  serviceType=iPlanetAMWebAgentService|class=

  指定用于不同服务名的 ResourceComparators。 从 Access Manager 控制台复制值。 转到 **服务配置** > **策略配置** > **全局** : **资源比较器**。从 Access Manager 中连接多个值，使用冒号 (:) 作为分隔符。

- com.sun.identity.policy.plugins.URLResourceName|wildcard

  默认值为 *|delimiter=/|caseSensitive=trueDescription

配置文件服务

- com.iplanet.am.profile.host

  此属性在 Access Manager 7 中不再使用。提供此属性只是为了向下兼容。 其值在安装期间设置。示例： *hostName.domainName*.com

- com.iplanet.am.profile.port

  此属性在 Access Manager 7 中不再使用。提供此属性只是为了向下兼容。 其值在安装期间设置。示例： 80

复制

使用以下关键字配置复制设置。

- com.iplanet.am.replica.delay.between.retries

  默认值为 1000。指定重试间隔的毫秒数。

- com.iplanet.am.replica.num.retries

  默认值为 0。指定重试次数。

SAML 服务

- com.sun.identity.saml.assertion.version

  默认值为 1.1。指定所用的默认的 SAML 版本。可能的值是 1.0 或 1.1。

- com.sun.identity.saml.checkcert

  默认值为 on。根据关键字库中的证书检查嵌入 KeyInfo 的证书的标志。由 com.sun.identity.saml.xmlsig.keystore 属性指定关键字库中的证书。可能的值包括：on|off。如果标志为“on”，则 XML 签名验证使用的 * 证书必须存在于关键字库中*。如果标志为“off”，则跳过 * 存在检查*/。

  on　　XML 签名验证使用的证书必须出现在关键字库中。

  off　　跳过存在检查。

- com.sun.identity.saml.protocol.version

  默认值为 1.1。指定所用的默认的 SAML 版本。可能的值是 1.0 或 1.1。

- com.sun.identity.saml.removeassertion

- com.sun.identity.saml.request.maxContentLength

  默认值为 16384。指定在 SAML 中使用的 HTTP **请求**的最大内容长度。

- com.sun.identity.saml.xmlsig.certalias

  默认值为 test。说明

- com.sun.identity.saml.xmlsig.keypass

  其值在安装期间设置。示例：/etc/opt/SUNWam/config/.keypass

  指定 SAML XML 关键字密码文件的路径。

- com.sun.identity.saml.xmlsig.keystore

  其值在安装期间设置。示例：/etc/opt/SUNWam/config/keystore.jks

  指定 SAML XML 关键字库密码文件的路径。

- com.sun.identity.saml.xmlsig.storepass

  其值在安装期间设置。示例：/etc/opt/SUNWam/config/.storepass

  指定 SAML XML 关键字库密码文件的路径。

安全

- com.iplanet.security.encryptor

  默认值为 com.iplanet.services.util.JSSEncryption。指定加密类实现。可用的类包括：com.iplanet.services.util.JCEEncryption and com.iplanet.services.util.JSSEncryption。

- com.iplanet.security.SecureRandomFactoryImpl

  默认值为 com.iplanet.am.util.JSSSecureRandomFactoryImpl。指定 SecureRandomFactory 的工厂类名。可用的实现类有：使用 JSS 的 com.iplanet.am.util.JSSSecureRandomFactoryImpl 和使用纯粹 Java 的 com.iplanet.am.util.SecureRandomFactoryImpl。

- com.iplanet.security.SSLSocketFactoryImpl

  默认值为 com.iplanet.services.ldap.JSSSocketFactory。指定 LDAPSocketFactory 的工厂类名。可用的类包括：使用 JSS 的 com.iplanet.services.ldap.JSSSocketFactory 和使用纯粹 Java 的 netscape.ldap.factory.JSSESocketFactory。

- com.sun.identity.security.checkcaller

  默认值为 false。为 Access Manager 启用或禁用 Java 安全管理器权限检查。默认情况下，此设置处于禁用状态。如果启用此设置，则应对容器（Access Manager 部署在该容器中）的 Java 策略文件进行适当的更改。这样，Access Manager JAR 文件可以信赖，可以用来执行敏感操作。有关详细信息，请参阅 com.sun.identity.security 的 Java API Reference (Javadoc) 条目。

- am.encryption.pwd

  其值在安装期间设置。示例：dSB9LkwPCSoXfIKHVMhIt3bKgibtsggd

指定用于加密和解密密码的密钥。

会话服务

- com.iplanet.am.clientIPCheckEnabled

  默认值为 false。指定是否在所有的 SSOToken 创建或验证中检查客户机的 IP 地址。

- com.iplanet.am.session.client.polling.enable

  此为“只读”属性。请勿修改属性值。

  默认值为 false。启用客户端会话轮询。 请注意，会话轮询模式和会话通知模式是互斥的。 如果启用轮询模式，则自动关闭会话通知，反之亦然。

- com.iplanet.am.session.client.polling.period

  默认值为 180。指定轮询周期的秒数。

- com.iplanet.am.session.httpSession.enabled

  默认值为 true。启用或禁用 USING httpSession。

- com.iplanet.am.session.invalidsessionmaxtime

  默认值为 10。指定当创建了会话且用户没有登录时，从会话表中删除无效会话前的分钟数。该值应始终大于验证模块属性文件中超时的值。

- com.iplanet.am.session.maxSessions

  默认值为 5000。指定允许的并发会话的最大数目。

  如果最大并发会话值超出此数目，登录时将发送“最大会话数”错误。

- com.iplanet.am.session.purgedelay

  默认值为 60。指定清除会话操作延迟的分钟数。

  会话超时后，这是延长的时间长度，在此期间会话继续驻留在会话服务器中。客户机应用程序使用此属性检查通过 SSO API 的会话是否超时。此延长时间结束时，会话被销毁。如果用户注销或会话直接被 Access Manager 组件销毁，则此会话不会在延长的时间长度内保留。在此延长时间内，会话处于 INVALID 状态。

- com.sun.am.session.caseInsensitiveDN

  默认值为 true。比较代理 DN。如果值为 false，则比较区分大小写。

- com.sun.am.session.enableHostLookUp

  默认值为 false。启用或禁用在会话记录期间进行主机查找。

SMTP

- com.iplanet.am.smtphost

  默认值为 localhost。指定邮件服务器主机。

- com.iplanet.am.smtpport

  默认值为 25。指定邮件服务器端口。

统计服务

- com.iplanet.am.stats.interval

  默认值为 60。指定统计记录时间间隔的分钟数。最短 5 秒钟，以免 CPU 饱和。Access Manager 将任何小于 5 秒的值都假设为 5 秒。

- com.iplanet.services.stats.directory

  其值在安装期间设置。示例：/var/opt/SUNWam/stats 指定在其中创建调试文件的目录。

- com.iplanet.services.stats.state

  默认值为 file。指定统计日志的位置。可能的值包括：

off	没有记录统计信息。
file	统计信息被写入指定目录下的文件。
console	统计信息被写入 Web Server 日志文件。

◆ ◆ ◆ 附 录 B

serverconfig.xml 文件

serverconfig.xml 文件为 Sun Java™ System Access Manager 提供了有关将 Directory Server 用作自身数据存储库的配置信息。本章说明了该文件的各个元素，以及如何针对故障转移配置该文件、如何拥有多个实例、如何对控制台解除部署以及从服务器中删除控制台文件。包括以下各节：

概述

serverconfig.xml 位于 */ AccessManager-base* /SUNWam/config/ums 中。它包含“标识 SDK”在建立到 Directory Server 的 LDAP 连接池时所使用的参数。此产品的其他功能不使用该文件。该文件中定义了两个用户：user1 为 Directory Server 代理用户，而 user2 则为 Directory Server 管理员。

代理用户

代理用户可以具有任一用户的权限（如组织管理员或最终用户）。绑定到代理用户的连接形成连接池。Access Manager 使用形为 cn=puser,ou=DSAME Users,dc=example,dc=com 的 DN 来创建代理用户。该用户用于所有针对 Directory Server 进行的查询。由于它受益于 Directory Server 中已配置的代理用户 ACI，因此必要时也可代表用户来执行操作。它保持开放式连接，通过此连接可传送所有查询（如服务配置、组织信息等的检索）。代理用户密码始终是加密的。第 235 页中的 “代理用户” 举例说明了加密密码在 serverconfig.xml 中的位置。

示例 B–1 serverconfig.xml 中的代理用户

```
<User name="User1" type="proxy">
<DirDN>
cn=puser,ou=DSAME Users,dc=example,dc=com
```

示例 B–1 serverconfig.xml 中的代理用户 （续）

```
</DirDN>
<DirPassword>
AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
</DirPassword>
</User>
```

管理员用户

当 Access Manager SDK 在未链接到特定用户的 Directory Server 上执行操作（例如，检索服务配置信息）时，dsameuser 可用于绑定。第 235 页中的 “代理用户” 可代表 dsameuser 执行这些操作，但是绑定必须首先验证 dsameuser 证书。在安装期间，Access Manager 将创建 cn=dsameuser,ou=DSAME Users,dc=example,dc=com。第 235 页中的 “代理用户” 举例说明了已加密的 dsameuser 密码在 serverconfig.xml 中的位置。

示例 B–2 serverconfig.xml 中的管理员用户

```
<User name="User2" type="admin">
<DirDN>
cn=dsameuser,ou=DSAME Users,dc=example,dc=com
</DirDN>
<DirPassword>
AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
</DirPassword>
</User>
```

服务器配置定义类型文档

server-config.dtd 定义 serverconfig.xml 的结构。它位于 *AccessManager-base* /SUNWam/dtd 中。本节定义 DTD 的主要元素。第 238 页中的 “MiscConfig 元素” 是 serverconfig.xml 文件的一个示例。

iPlanetDataAccessLayer 元素

iPlanetDataAccessLayer 是根元素。此根元素允许为每个 XML 文件定义多个服务器组。此根元素的直接子元素为第 237 页中的 “ServerGroup 元素” 。此根元素不包含任何属性。

ServerGroup 元素

ServerGroup 定义了指向一个或多个目录服务器的指针。它们可以是主服务器或复制服务器。限定 *ServerGroup* 的子元素包括第 237 页中的 “Server 元素”、第 237 页中的 “User 元素”、第 238 页中的 “BaseDN 元素”和第 238 页中的 “MiscConfig 元素”。*ServerGroup* 的 XML 属性是服务器组的名称、*minConnPool* 和 *maxConnPool*，后两者分别定义可以为 LDAP 连接池打开的连接的最小数目 (1) 和最大数目 (10)。不支持多个已定义的 ServerGroup 元素。

注 – Access Manager 使用连接池来访问 Directory Server。Access Manager 已启动且尚未关闭时会开启所有连接。这些连接可以重复使用。

Server 元素

服务器定义了特定 Directory Server 实例。它不包含子元素。服务器的必需 XML 属性是服务器的用户友好名称、主机名和运行 Directory Server 的端口号，以及必须打开的 LDAP 连接的类型（简单或 SSL）。

注 – 有关使用 Server 元素进行自动故障转移的示例，请参阅第 239 页中的 “故障转移或多主体配置”。

User 元素

User 包含定义了用户（为 Directory Server 实例配置的）的子元素。限定 *User* 的子元素包括 *DirDN* 和 *DirPassword*。User 元素的必需 XML 属性是用户名和用户类型。类型的值标识用户的权限，以及将为 Directory Server 实例打开的连接的类型。选项包括：

- 验证—定义通过 Directory Server 进行验证的用户。
- 代理—定义 Directory Server 代理用户。有关详细信息，请参阅第 235 页中的 “代理用户”。
- 重新绑定—定义拥有可用于重新绑定的证书的用户。
- 管理员—定义拥有 Directory Server 管理权限的用户。有关详细信息，请参阅第 236 页中的 “管理员用户”。

DirDN 元素

DirDN 包括已定义用户的 LDAP 区别名。

DirPassword 元素

DirPassword 包括已定义用户的加密密码。

注意 – 在整个部署过程中，密码和加密密钥必须保持一致。例如，在此元素内定义的密码也存储于 Directory Server 中。如果要在一个地方更改密码，则两个地方的密码都必须更新。此外，此密码是加密的。如果 `am.encryption.pwd` 属性中定义的加密密钥被更改，则 `serverconfig.xml` 中所有的密码必须使用 `ampassword --encrypt` 密码重新加密。

BaseDN 元素

BaseDN 定义服务器组的基本区别名。此元素不包含子元素和 XML 属性。

MiscConfig 元素

MiscConfig 是一个占位符，用于定义任一 LDAP JDK 特性（如高速缓存大小）。它不包含子元素。它的必需 XML 属性是特性的名称及其定义的值。

示例 B–3 serverconfig.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!--
 Copyright (c) 2002 Sun Microsystems, Inc. All rights reserved.

 Use is subject to license terms.

-->
<iPlanetDataAccessLayer>
        <ServerGroup name="default" minConnPool="1" maxConnPool="10">
                <Server name="Server1" host="
               ishost.domain_name" port="389"
type="SIMPLE" />
                <User name="User1" type="proxy">
                        <DirDN>
                                cn=puser,ou=DSAME Users,dc=example,dc=com
                        </DirDN>
                        <DirPassword>
                                AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
                        </DirPassword>
                </User>
                <User name="User2" type="admin">
                        <DirDN>
                                cn=dsameuser,ou=DSAME Users,dc=example,dc=com
                        </DirDN>
                        <DirPassword>
                                AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
                        </DirPassword>
```

示例 B–3 serverconfig.xml （续）

```
                </User>
                <BaseDN>
                        dc=example,dc=com
                </BaseDN>
        </ServerGroup>
</iPlanetDataAccessLayer>
```

故障转移或多主体配置

Access Manager 允许自动故障转移至任何在 serverconfig.xml 中定义为第 237 页中的 “ServerGroup 元素”第 237 页中的 “Server 元素”的 Directory Server。可以为故障转移或多主体配置多个服务器。如果最初配置的服务器停止运行，则随后配置的服务器将接替最初配置的服务器继续运行。第 239 页中的 “故障转移或多主体配置”举例说明了含有自动故障转移配置的 serverconfig.xml。

示例 B–4 serverconfig.xml 中配置的故障转移

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<!--
PROPRIETARY/CONFIDENTIAL. Use of this product is subject to license terms.
Copyright 2002 Sun Microsystems, Inc. All rights reserved.
-->
<iPlanetDataAccessLayer>
     <ServerGroup name="default" minConnPool="1" maxConnPool="10">
          <Server name="Server1" host="
            amhost1.domain_name" port="389" type="SIMPLE" />
          <Server name="Server2" host="
            amhost2.domain_name" port="389" type="SIMPLE" />
          <Server name="Server3" host="
            amhost3.domain_name" port="390" type="SIMPLE" />
          <User name="User1" type="proxy">
               <DirDN>
                    cn=puser,ou=DSAME Users,dc=example,dc=com
               </DirDN>
               <DirPassword>
                    AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
               </DirPassword>
          </User>
          <User name="User2" type="admin">
               <DirDN>
                    cn=dsameuser,ou=DSAME Users,dc=example,dc=com
```

示例 B–4 serverconfig.xml 中配置的故障转移 （续）

```
                </DirDN>
                <DirPassword>
                     AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
                </DirPassword>
           </User>
           <BaseDN>
                o=isp
           </BaseDN>
     </ServerGroup>
</iPlanetDataAccessLayer>
```

◆ ◆ ◆ 附 录 C

日志文件参考

本附录列出了每个 Access Manager 功能区域的可能日志文件。本附录中的表记录了以下日志文件项：

- Id — 日志标识号。
- 日志级别 — 消息的“日志级别”属性。
- 说明 — 日志消息的说明。
- 数据 — 消息所属的数据类型。
- 触发 — 日志文件消息的原因。
- 操作 — 获取详细信息要执行的操作。

日志文件的定义和位置均在《Sun Java System Access Manager 7 2005Q4 Technical Overview》中进行介绍。

表 C–1 amAdmin 命令行实用程序的日志参考

Id	日志级别	说明	数据	触发	操作
1	INFO	用户登录不成功。	用户 ID	用户登录不成功。	
2 TEST	INFO	收到管理异常	元素名错误消息	在处理管理请求时收到管理异常。	有关详细信息，请查阅 amAdmin 调试文件。
3	INFO	会话已破坏	用户名	会话已破坏。	
11	INFO	服务模式已加载	模式名称	已成功加载服务模式。	
12	INFO	服务已删除	服务名	已成功删除服务。	
13	INFO	属性已添加	属性名	已成功添加属性。	

表 C–1 amAdmin 命令行实用程序的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
21	INFO	此服务没有策略	服务名	指定了“删除策略规则标志”，但服务没有策略。	
22	INFO	找不到“服务的策略模式”	服务名	指定了“删除策略规则标志”，但没有找到服务的策略模式	
23	INFO	正在删除服务策略	服务名	指定了“正在删除带有删除策略规则标志的服务”。	
24	INFO	已完成删除服务策略	服务名	指定了“正在删除带有删除策略规则标志的服务”。	
25	INFO	已在组织中创建策略	策略名组织 *DN*	已在组织 DN 中创建策略。	
26	INFO	已从组织中删除策略	策略名组织 *DN*	已从组织 DN 中删除策略。	
31	INFO	将语言环境资源包添加到 Directory Server	资源包名称资源语言环境	语言环境资源包已成功存储到 Directory Server。	
32	INFO	将默认资源包添加到 Directory Server	资源包名称	默认资源包已成功存储到 Directory Server。	
33	INFO	已从 Directory Server 中删除语言环境资源包	资源包名称资源语言环境	已从 Directory Server 中成功删除语言环境资源包。	
34	INFO	已从 Directory Server 中删除默认语言环境资源包	资源包名称	已从 Directory Server 中成功删除默认资源包。	
41	INFO	已修改服务的服务模式	服务名	已成功修改服务的服务模式。	

表 C–1 amAdmin 命令行实用程序的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
42	INFO	已删除服务的服务子模式	子模式名称服务名	已成功删除服务的服务子模式。	
43	INFO	已将服务子模式添加到服务。	服务名	已将服务子模式成功添加到服务。	
44	INFO	已将子配置添加到服务。	子配置名称服务名	已将子配置成功添加到服务。	
45	INFO	已修改服务的子配置	子配置名称服务名	已成功修改服务的子配置。	
46	INFO	已删除服务的子配置	子配置名称服务名	已成功删除服务的子配置。	
47	INFO	已删除服务的所有服务配置。	服务名	已成功删除服务的所有服务配置。	
91	INFO	修改组织中的服务子配置	子配置名称服务名组织 *DN*	已成功修改组织中的服务子配置。	
92	INFO	已添加组织中的服务子配置	子配置名称服务名组织 *DN*	已成功添加组织中的服务子配置。	
93	INFO	已删除组织中的服务子配置	子配置名称服务名组织 *DN*	已成功删除组织中的服务子配置。	
94	INFO	已在组织中创建远程提供者	提供者名称组织 *DN*	已在组织中成功创建远程提供者。	
95	INFO	已修改组织中的远程提供者	提供者名称组织 *DN*	已成功修改组织中的远程提供者。	
96	INFO	已修改组织中的托管提供者	提供者名称组织 *DN*	已成功修改组织中的托管提供者。	
97	INFO	已在组织中创建托管提供者	提供者名称组织 *DN*	已在组织中成功创建托管提供者。	有关详细信息，请查阅身份库日志。

表 C–1 amAdmin 命令行实用程序的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
98	INFO	已删除组织中的远程提供者	提供者名称组织 *DN*	已成功删除组织中的远程提供者。	
99	INFO	已在组织中创建验证域	信任圈名称组织 *DN*	已在组织中成功创建验证域。	
100	INFO	已删除组织中的验证域。	信任圈名称组织 *DN*	已成功删除组织中的验证域。	
101	INFO	已修改组织中的验证域。	信任圈名称组织 *DN*	已成功修改组织中的验证域。	
102	INFO	尝试修改服务模板	服务模板的 DN	已尝试修改服务模板。	
103	INFO	已修改服务模板	服务模板的 DN	已成功修改服务模板。	
104	INFO	尝试移除服务模板	服务模板的 DN	已尝试移除服务模板。	
105	INFO	已移除服务模板	服务模板的 DN	已成功移除服务模板。	
106	INFO	尝试添加服务模板	服务模板的 DN	已尝试添加服务模板。	
107	INFO	已添加服务模板	服务模板的 DN	已成功添加服务模板。	
108	INFO	尝试将嵌套组添加到组	要添加的组名包含组的 *DN*	已尝试将嵌套组添加到组。	
109	INFO	已将嵌套组添加到组	要添加的组名包含组的 *DN*	已将嵌套组成功添加到组。	
110	INFO	尝试将用户添加到组或角色	用户名目标组或角色	已尝试将用户添加到组或角色。	
111	INFO	已将用户添加到组或角色	用户名目标组或角色	已将用户成功添加到组或角色。	
112	INFO	尝试创建实体。	实体的 DN	已尝试创建实体。	

表 C–1 amAdmin 命令行实用程序的日志参考　（续）

Id	日志级别	说明	数据	触发	操作
113	INFO	已创建实体。	实体的本地化名称实体的 *DN*	已创建实体。	
114	INFO	尝试创建角色	角色 DN	已尝试创建角色。	
115	INFO	已创建角色	角色名	已创建角色。	
116	INFO	尝试创建组容器	组容器名	已尝试创建组容器。	
117	INFO	创建组容器	组容器名	已创建组容器。	
118	INFO	尝试创建组。	组名	已尝试创建组。	
119	INFO	创建组。	组名	已创建组。	
120	INFO	尝试创建人员容器。	人员容器的 DN	已尝试创建人员容器。	
121	INFO	创建人员容器。	人员容器的 DN	已创建人员容器。	
122	INFO	尝试在组织或角色中创建服务模板	服务模板名称组织或角色名	已尝试在组织或角色中创建服务模板。	
123	INFO	在组织或角色中创建服务模板	服务模板名称组织或角色名	已在组织或角色中创建服务模板。	
124	INFO	尝试创建容器	容器名	已尝试创建容器。	
125	INFO	创建容器	容器名	已创建容器。	
126	INFO	尝试创建用户。	用户名	已尝试创建用户。	
127	INFO	创建用户。	用户名	已创建用户。	
128	INFO	尝试删除实体。	实体的 DN	已尝试删除实体。	
129	INFO	删除实体。	实体的本地化名称实体的 *DN*	已删除实体。	
130	INFO	尝试删除人员容器	人员容器的 DN	已尝试删除人员容器。	

表 C–1 amAdmin 命令行实用程序的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
131	INFO	删除人员容器	人员容器的 DN	已删除人员容器。	
132	INFO	尝试删除角色	角色名	已尝试删除角色。	
133	INFO	删除角色	角色名	已删除角色。	
134	INFO	尝试删除组织中的服务模板	服务模板名组织名	已尝试删除组织中的服务模板。	
135	INFO	删除组织中的服务模板	服务模板名组织名	已删除组织中的服务模板。	
136	INFO	尝试删除容器。	容器名	已尝试删除容器。	
137	INFO	删除容器。	容器名	已删除容器。	
138	INFO	尝试修改实体	实体的本地化名称实体的 *DN*	已尝试修改实体。	
139	INFO	修改实体	实体的本地化名称实体的 *DN*	已修改实体。	
140	INFO	尝试修改人员容器。	人员容器的 DN	已尝试修改人员容器。	
141	INFO	修改人员容器。	人员容器的 DN	已修改人员容器。	
142	INFO	尝试修改容器。	容器名	已尝试修改容器。	
143	INFO	修改容器。	容器名	已修改容器。	
144	INFO	尝试在组织下注册服务。	服务名组织名	已尝试在组织下注册服务	
145	INFO	在组织下注册服务。	服务名组织名	已在组织下注册服务	
146	INFO	尝试在组织下取消注册服务。	服务名组织名	已尝试在组织下取消注册服务	
147	INFO	在组织下取消注册服务。	服务名组织名	已在组织下取消注册服务	
148	INFO	尝试修改组。	组名	已尝试修改组	

表 C–1 amAdmin 命令行实用程序的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
149	INFO	修改组。	组名	已修改组	
150	INFO	尝试从组中移除嵌套组。	嵌套组名称组名	已尝试从组中移除嵌套组。	
151	INFO	从组中移除嵌套组。	嵌套组名称组名	已从组中移除嵌套组。	
152	INFO	尝试删除组	组名	已尝试删除组。	
153	INFO	删除组	组名	已删除组。	
154	INFO	尝试从角色中移除用户	用户名角色名	已尝试从角色中移除用户。	
155	INFO	从角色中移除用户	用户名角色名	已从角色中移除用户。	
156	INFO	尝试从组中移除用户	用户名组名	已尝试从组中移除用户。	
157	INFO	从组中移除用户	用户名组名	已从组中移除用户。	
201	INFO	尝试将身份添加到领域中的身份	要添加的身份名要添加的身份类型要添加到的身份名要添加到的身份类型领域名	已尝试将身份添加到领域中的身份。	
202	INFO	将身份添加到领域中的身份	要添加的身份名要添加的身份类型要添加到的身份名要添加到的身份类型领域名	已将身份添加到领域中的身份。	
203	INFO	尝试将服务指定到领域中的身份。	服务名身份名身份类型领域名	已尝试将服务指定到领域中的身份。	
204	INFO	将服务指定到领域中的身份。	服务名身份名身份类型领域名	已将服务指定到领域中的身份。	

表 C–1 amAdmin 命令行实用程序的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
205	INFO	尝试在领域中创建某种类型的多个身份。	身份类型领域名	已尝试在领域中创建某种类型的多个身份。	
206	INFO	在领域中创建某种类型的多个身份。	身份类型领域名	已在领域中创建某种类型的多个身份。	
207	INFO	尝试在领域中创建某种类型的身份。	身份名身份类型领域名	已尝试在领域中创建某种类型的身份。	
208	INFO	在领域中创建某种类型的身份。	身份名身份类型领域名	已在领域中创建某种类型的身份。	
209	INFO	尝试删除领域中某种类型的身份	身份名身份类型领域名	已尝试删除领域中某种类型的身份。	
210	INFO	删除领域中某种类型的身份	身份名身份类型领域名	已删除领域中某种类型的身份。	
211	INFO	尝试修改领域中身份的服务	服务名身份类型身份名领域名	已尝试修改领域中身份的服务。	
212	INFO	修改领域中身份的服务	服务名身份类型身份名领域名	已修改领域中身份的服务。	
213	INFO	尝试从领域中的身份移除身份	要移除的身份名要移除的身份类型要从中移除的身份名要从中移除的身份类型领域名	已尝试从领域中的身份移除身份。	
214	INFO	从领域中的身份移除身份	要移除的身份名要移除的身份类型要从中移除的身份名要从中移除的身份类型领域名	已从领域中的身份移除身份。	

表 C–1 amAdmin 命令行实用程序的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
215	INFO	尝试设置领域中身份的服务属性	服务名身份类型身份名领域名	已尝试设置领域中身份的服务属性。	
216	INFO	设置领域中身份的服务属性	服务名身份类型身份名领域名	已设置领域中身份的服务属性。	
217	INFO	尝试从领域中的身份取消指定服务	服务名身份类型身份名领域名	已尝试从领域中的身份取消指定服务。	
218	INFO	从领域中的身份取消指定服务	服务名身份类型身份名领域名	已从领域中的身份取消指定服务。	
219	INFO	尝试创建组织	组织名	已尝试创建组织。	
220	INFO	创建组织	组织名	已创建组织。	
221	INFO	尝试删除子配置	组织名	已尝试删除子组织。	
222	INFO	删除子组织。	组织名	已删除子组织。	
223	INFO	尝试修改角色	角色名	已尝试修改角色。	
224	INFO	修改角色	角色名	已修改角色。	
225	INFO	尝试修改子组织。	组织名	已尝试修改子组织。	
226	INFO	修改子组织。	组织名	已修改子组织。	
227	INFO	尝试删除用户。	用户名	已尝试删除用户。	
228	INFO	删除用户。	用户名	已删除用户。	
229	INFO	尝试修改用户。	用户名	已尝试修改用户。	
230	INFO	修改用户。	用户名	已修改用户。	
231	INFO	尝试在领域的服务属性中添加值。	属性名服务名领域名	已尝试在领域的服务属性中添加值。	

表 C–1 amAdmin 命令行实用程序的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
232	INFO	在领域的服务属性中添加值。	属性名服务名领域名	已在领域的服务属性中添加值。	
233	INFO	尝试将服务指定到领域	服务名领域名	已尝试将服务指定到领域。	
234	INFO	将服务指定到领域	服务名领域名	已将服务指定到领域。	
235	INFO	尝试创建领域	已创建的领域名父领域名	已尝试创建领域。	
236	INFO	创建领域	已创建的领域名父领域名	已创建领域。	
237	INFO	删除领域。	是否递归已删除的领域名	已删除领域。	
238	INFO	删除领域。	是否递归已删除的领域名	已删除领域。	
239	INFO	尝试修改领域中的服务。	服务名领域名	已尝试修改领域中的服务。	
240	INFO	修改领域中的服务。	服务名领域名	已修改领域中的服务。	
241	INFO	尝试移除领域中服务的属性	属性名服务名领域名	已尝试移除领域中服务的属性。	
242	INFO	从领域中的服务移除属性	属性名服务名领域名	已从领域中的服务移除属性。	
243	INFO	尝试从领域中服务的属性移除值	属性名服务名领域名	已尝试从领域中服务的属性移除值。	
244	INFO	从领域中服务的属性移除值	属性名服务名领域名	已从领域中服务的属性移除值。	
245	INFO	尝试设置领域中服务的属性。	服务名领域名	已尝试设置领域中服务的属性。	
246	INFO	设置领域中服务的属性。	服务名领域名	设置领域中服务的属性。	

表 C–1 amAdmin 命令行实用程序的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
247	INFO	尝试从领域取消指定服务。	服务名领域名	已尝试从领域取消指定服务。	
248	INFO	从领域取消指定服务。	服务名领域名	已从领域取消指定服务。	
249	INFO	尝试将服务指定到组织配置	服务名领域名	已尝试将服务指定到组织配置。	
250	INFO	将服务指定到组织配置	服务名领域名	已将服务指定到组织配置。	
251	INFO	将服务指定到组织配置未完成	服务名领域名	已将服务指定到组织配置，但此服务不是组织配置的可指定服务。	
252	INFO	将服务指定到领域未完成	服务名领域名	已将服务指定到领域，但此服务不是领域的可指定服务。	
253	INFO	尝试从组织配置取消指定服务。	服务名领域名	已尝试从组织配置取消指定服务。	
254	INFO	从组织配置取消指定服务。	服务名领域名	已从组织配置取消指定服务。	
255	INFO	取消指定非组织配置或领域中的服务。	服务名领域名	已请求取消指定非组织配置或领域中的服务。	
256	INFO	尝试修改组织配置中的服务。	服务名领域名	已尝试修改组织配置中的服务。	
257	INFO	修改组织配置中的服务。	服务名领域名	已修改组织配置中的服务。	
258	INFO	修改非组织配置或领域中的服务。	服务名领域名	已尝试修改非组织配置或领域中的服务。	

表 C–2 验证的日志参考

Id	日志级别	说明	数据	触发	操作
100	INFO	验证成功	消息	用户使用有效凭证验证	
101	INFO	基于用户的验证成功	消息验证类型 用户名	用户使用有效凭证验证	
102	INFO	基于角色的验证成功	消息验证类型 角色名	属于角色的用户使用有效凭证验证	
103	INFO	基于服务的验证成功	消息验证类型 服务名	用户使用有效凭证向领域下的已配置服务进行验证	
104	INFO	基于验证级别的验证成功	消息验证类型 验证级别值	用户使用有效凭证向一个或多个验证级别值大于或等于指定验证级别的验证模块进行验证	
105	INFO	基于模块的验证成功	消息验证类型 模块名	用户使用有效凭证向领域下的验证模块进行验证	
200	INFO	验证失败	错误消息	提交了错误/无效凭证用户被锁定/未激活	向必需的验证模块输入正确/有效凭证
201	INFO	验证失败	错误消息	输入了无效凭证。	请输入正确的密码。
202	INFO	验证失败	错误消息	命名的配置（验证链）不存在。	请为此组织创建并配置命名的配置。
203	INFO	验证失败	错误消息	未找到此用户的用户概要文件。	用户在已配置的数据存储库插件中不存在，因此，请正确配置此领域/组织的数据存储库插件。

表 C–2 验证的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
204	INFO	验证失败	错误消息	此用户处于不活动状态。	请激活此用户。
205	INFO	验证失败	错误消息	超过失败尝试的最大次数。用户已被锁定。	请联系系统管理员。
206	INFO	验证失败	错误消息	用户帐户已过期。	请联系系统管理员。
207	INFO	验证失败	错误消息	登录超时。	请再次尝试登录。
208	INFO	验证失败	错误消息	验证模块被拒绝。	请配置此模块或使用其他模块。
209	INFO	验证失败	错误消息	已达到允许的会话最大数量限制。	请注销会话或增加限制。
210	INFO	验证失败	错误消息	组织/领域不存在。	请使用有效的组织/领域。
211	INFO	验证失败	错误消息	组织/领域未激活。	请激活组织/领域。
212	INFO	验证失败	错误消息	无法创建会话。	请确保已配置会话服务且未达到最大会话数量。
213	INFO	基于用户的验证失败	错误消息验证类型用户名	没有为用户配置任何验证配置（一个或多个验证模块链）提交了错误/无效凭证用户被锁定/未激活	请为用户配置验证配置（一个或多个验证模块链）向必需的验证模块输入正确/有效凭证
214	INFO	验证失败	错误消息验证类型用户名	基于用户的验证。输入了无效凭证。	请输入正确的密码。
215	INFO	验证失败	错误消息验证类型用户名	此用户的命名的配置（验证链）不存在	请为此用户创建并配置命名的配置

表 C–2 验证的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
216	INFO	验证失败	错误消息验证类型用户名	基于用户的验证。未找到此用户的用户概要文件。	用户在已配置的数据存储库插件中不存在，因此，请正确配置此领域/组织的数据存储库插件。
217	INFO	验证失败	错误消息验证类型用户名	基于用户的验证。此用户处于不活动状态。	请激活此用户。
218	INFO	验证失败	错误消息验证类型用户名	基于用户的验证。超过失败尝试的最大次数。用户已被锁定。	请联系系统管理员。
219	INFO	验证失败	错误消息验证类型用户名	基于用户的验证。用户帐户已过期。	请联系系统管理员。
220	INFO	验证失败	错误消息验证类型用户名	基于用户的验证。登录超时。	请再次尝试登录。
221	INFO	验证失败	错误消息验证类型用户名	基于用户的验证。验证模块被拒绝。	请配置此模块或使用其他模块。
222	INFO	验证失败	错误消息验证类型用户名	基于用户的验证。已达到允许的会话最大数量限制。	请注销会话或增加限制。
223	INFO	验证失败	错误消息验证类型用户名	基于用户的验证。组织/领域不存在。	请使用有效的组织/领域。
224	INFO	验证失败	错误消息验证类型用户名	基于用户的验证。组织/领域未激活。	请激活组织/领域。
225	INFO	验证失败	错误消息验证类型用户名	基于用户的验证。无法创建会话。	请确保已配置会话服务且未达到最大会话数量。

表 C–2 验证的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
226	INFO	基于角色的验证失败	错误消息验证类型角色名	没有为角色配置任何验证配置（一个或多个验证模块链）提交了错误/无效凭证用户不属于此角色用户被锁定/未激活	请为角色配置验证配置（一个或多个验证模块链）向必需的验证模块输入正确/有效凭证将此角色指定到验证用户
227	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。输入了无效凭证。	请输入正确的密码。
228	INFO	验证失败	错误消息验证类型角色名	此角色的命名的配置（验证链）不存在。	请为此角色创建并配置命名的配置。
229	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。未找到此用户的用户概要文件。	用户在已配置的数据存储库插件中不存在，因此，请正确配置此领域/组织的数据存储库插件。
230	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。此用户处于不活动状态。	请激活此用户。
231	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。超过失败尝试的最大次数。用户已被锁定。	请联系系统管理员。
232	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。用户帐户已过期。	请联系系统管理员。
233	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。登录超时。	请再次尝试登录。
234	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。验证模块被拒绝。	请配置此模块或使用其他模块。

表 C–2 验证的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
235	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。已达到允许的会话最大数量限制。	请注销会话或增加限制。
236	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。组织/领域不存在。	请使用有效的组织/领域。
237	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。组织/领域未激活。	请激活组织/领域。
238	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。无法创建会话。	请确保已配置会话服务且未达到最大会话数量。
239	INFO	验证失败	错误消息验证类型角色名	基于角色的验证。用户不属于此角色。	请将用户添加到此角色。
240	INFO	基于服务的验证失败	错误消息验证类型服务名	没有为服务配置任何验证配置（一个或多个验证模块链）提交了错误/无效凭证用户被锁定/未激活	请为服务配置验证配置（一个或多个验证模块链）向必需的验证模块输入正确/有效凭证
241	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。输入了无效凭证。	请输入正确的密码。
242	INFO	验证失败	错误消息验证类型服务名	具有此服务名的命名的配置（验证链）不存在。	请创建并配置命名的配置。
243	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。未找到此用户的用户概要文件。	用户在已配置的数据存储库插件中不存在，因此，请正确配置此领域/组织的数据存储库插件。

表 C–2 验证的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
244	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。此用户处于不活动状态。	请激活此用户。
245	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。超过失败尝试的最大次数。用户已被锁定。	请联系系统管理员。
246	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。用户帐户已过期。	请联系系统管理员。
247	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。登录超时。	请再次尝试登录。
248	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。验证模块被拒绝。	请配置此模块或使用其他模块。
249	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。服务不存在。	请仅使用有效服务。
250	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。已达到允许的会话最大数量限制。	请注销会话或增加限制。
251	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。组织/领域不存在。	请使用有效的组织/领域。
252	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。组织/领域未激活。	请激活组织/领域。
253	INFO	验证失败	错误消息验证类型服务名	基于服务的验证。无法创建会话。	请确保已配置会话服务且未达到最大会话数量。

表 C–2 验证的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
254	INFO	基于验证级别的验证失败	错误消息验证类型验证级别值	没有验证级别值大于或等于指定验证级别的验证模块向一个或多个验证级别高于或等于指定验证级别的验证模块提交了错误/无效凭证用户被锁定/未激活	请配置一个或多个验证级别值大于或等于必需的验证级别的验证模块向一个或多个验证级别高于或等于指定验证级别的验证模块输入正确/有效凭证
255	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。输入了无效凭证。	请输入正确的密码。
256	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。没有可用的验证配置。	请创建验证配置。
257	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。未找到此用户的用户概要文件。	用户在已配置的数据存储库插件中不存在，因此，请正确配置此领域/组织的数据存储库插件。
258	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。此用户处于不活动状态。	请激活此用户。
259	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。超过失败尝试的最大次数。用户已被锁定。	请联系系统管理员。
260	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。用户帐户已过期。	请联系系统管理员。
261	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。登录超时。	请再次尝试登录。

表 C–2 验证的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
262	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。验证模块被拒绝。	请配置此模块或使用其他模块。
263	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。验证级别无效。	请指定有效的验证级别。
264	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。已达到允许的会话最大数量限制。	请注销会话或增加限制。
265	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。组织/领域不存在。	请使用有效的组织/领域。
266	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。组织/领域未激活。	请激活组织/领域。
267	INFO	验证失败	错误消息验证类型验证级别值	基于级别的验证。无法创建会话。	请确保已配置会话服务且未达到最大会话数量。
268	INFO	基于模块的验证失败	错误消息验证类型模块名	未在领域下注册/配置模块提交了错误/无效凭证用户被锁定/未激活	请在领域下注册/配置验证模块向验证模块输入正确/有效凭证
269	INFO	验证失败	错误消息验证类型模块名	基于模块的验证。输入了无效凭证。	请输入正确的密码。
270	INFO	验证失败	错误消息验证类型模块名	基于模块的验证。未找到此用户的用户概要文件。	用户在已配置的数据存储库插件中不存在，因此，请正确配置此领域/组织的数据存储库插件。
271	INFO	验证失败	错误消息验证类型模块名	基于模块的验证。此用户处于不活动状态。	请激活此用户。

表 C–2 验证的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
272	INFO	验证失败	错误消息验证类型模块名	基于模块的验证。超过失败尝试的最大次数。用户已被锁定。	请联系系统管理员。
273	INFO	验证失败	错误消息验证类型模块名	基于模块的验证。用户帐户已过期。	请联系系统管理员。
274	INFO	验证失败	错误消息验证类型模块名	基于模块的验证。登录超时。	请再次尝试登录。
275	INFO	验证失败	错误消息验证类型模块名	基于模块的验证。验证模块被拒绝。	请配置此模块或使用其他模块。
276	INFO	验证失败	错误消息验证类型模块名	基于模块的验证。已达到允许的会话最大数量限制。	请注销会话或增加限制。
277	INFO	验证失败	错误消息验证类型模块名	基于模块的验证。组织/领域不存在。	请使用有效的组织/领域。
278	INFO	验证失败	错误消息验证类型模块名	基于模块的验证。组织/领域未激活。	请激活组织/领域。
279	INFO	验证失败	错误消息验证类型模块名	基于模块的验证。无法创建会话。	请确保已配置会话服务且未达到最大会话数量。
300	INFO	用户注销成功	消息	用户已注销	
301	INFO	用户从基于用户的验证注销成功	消息验证类型用户名	用户已注销	
302	INFO	用户从基于角色的验证注销成功	消息验证类型角色名	属于此角色的用户已注销	
303	INFO	用户从基于服务的验证注销成功	消息验证类型服务名	用户已从领域下的已配置服务中注销	

表 C–2 验证的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
304	INFO	用户从基于验证级别的验证注销成功	消息验证类型 验证级别值	用户已从一个或多个验证级别值大于或等于指定验证级别的验证模块注销	
305	INFO	用户从基于模块的验证注销成功	消息验证类型 模块名	用户已从领域下的验证模块中注销	

表 C–3 Access Manager 控制台的日志参考

Id	日志级别	说明	数据	触发	操作
1	INFO	尝试创建身份	身份名身份类型领域名	单击“领域创建”页面中的“创建”按钮。	
2	INFO	创建身份成功。	身份名身份类型领域名	单击“领域创建”页面中的“创建”按钮。	
3	SEVERE	创建身份失败	身份名身份类型领域名 错误消息	无法在领域下创建身份。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
4	SEVERE	创建身份失败	身份名身份类型领域名 错误消息	由于数据存储库错误，无法在领域下创建身份。	有关详细信息，请查阅数据存储库日志。
11	INFO	尝试搜索身份	基本领域身份类型搜索模式 搜索大小限制 搜索时间限制	单击“身份搜索”视图中的“搜索”按钮。	
12	INFO	搜索身份成功	基本领域身份类型搜索模式 搜索大小限制 搜索时间限制	单击“身份搜索”视图中的“搜索”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
13	SEVERE	搜索身份失败	身份名身份类型领域名 错误消息	无法对领域下的身份执行搜索操作。 这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
14	SEVERE	搜索身份失败	身份名身份类型领域名 错误消息	由于数据存储库错误，无法对领域下的身份执行搜索操作。	有关详细信息，请查阅数据存储库日志。
21	INFO	尝试读取身份的属性值	身份名属性名	查看身份配置文件视图。	
22	INFO	读取身份的属性值成功	身份名属性名	查看身份配置文件视图。	
23	SEVERE	读取身份的属性值失败	身份名属性名 错误消息	无法读取身份的属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
24	SEVERE	读取身份的属性值失败	身份名属性名 错误消息	由于数据存储库错误，无法读取身份的属性值。	有关详细信息，请查阅数据存储库日志。
25	SEVERE	读取身份的属性值失败	身份名属性名 错误消息	由于服务管理器 API 异常，无法读取身份的属性值。	有关详细信息，请查阅服务管理日志。
31	INFO	尝试修改身份的属性值	身份名属性名	单击“身份配置文件”视图中的“保存”按钮。	
32	INFO	修改身份的属性值成功	身份名属性名	单击“身份配置文件”视图中的“保存”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
33	SEVERE	修改身份的属性值失败	身份名属性名错误消息	无法修改身份的属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
34	SEVERE	修改身份的属性值失败	身份名属性名错误消息	由于数据存储库错误，无法修改身份的属性值。	有关详细信息，请查阅数据存储库日志。
41	INFO	尝试删除身份	领域名要删除的身份名	单击“身份搜索”视图中的“删除”按钮。	
42	INFO	删除身份成功	领域名要删除的身份名	单击“身份搜索”视图中的“删除”按钮。	
43	SEVERE	删除身份失败	领域名要删除的身份名错误消息	无法删除身份。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
44	SEVERE	删除身份失败	领域名要删除的身份名错误消息	由于数据存储库错误，无法删除身份。	有关详细信息，请查阅数据存储库日志。
51	INFO	尝试读取身份的成员资格信息	身份名成员资格身份类型	查看身份的成员资格页面。	
52	INFO	读取身份的成员资格信息成功	身份名成员资格身份类型	查看身份的成员资格页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
53	SEVERE	读取身份的成员资格信息失败。	身份名成员资格身份类型错误消息	无法读取身份的成员资格信息。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
54	SEVERE	读取身份的成员资格信息失败。	身份名成员资格身份类型错误消息	由于数据存储库错误，无法读取身份的成员资格信息。	有关详细信息，请查阅数据存储库日志。
61	INFO	尝试读取身份的成员信息	身份名成员身份类型	查看身份的成员页面。	
62	INFO	读取身份的成员信息成功	身份名成员身份类型	查看身份的成员页面。	
63	SEVERE	读取身份的成员信息失败。	身份名成员身份类型错误消息	无法读取身份的成员信息。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
64	SEVERE	读取身份的成员信息失败。	身份名成员身份类型错误消息	由于数据存储库错误，无法读取身份的成员信息。	有关详细信息，请查阅数据存储库日志。
71	INFO	尝试将成员添加到身份	身份名要添加的身份名。	选择要添加到身份的成员。	
72	INFO	将成员添加到身份成功	身份名已添加的身份名。	选择要添加到身份的成员。	
73	SEVERE	将成员添加到身份失败。	身份名要添加的身份名。错误消息	无法将成员添加到身份。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
74	SEVERE	将成员添加到身份失败。	身份名要添加的身份名。错误消息	由于数据存储库错误，无法将成员添加到身份。	有关详细信息，请查阅数据存储库日志。
81	INFO	尝试从身份中移除成员	身份名要移除的身份名。	选择要从身份中移除的成员。	
82	INFO	从身份中移除成员成功	身份名已移除的身份名。	选择要从身份中移除的成员。	
83	SEVERE	从身份中移除成员失败。	身份名要移除的身份名。错误消息	无法从身份中移除成员。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
84	SEVERE	从身份中移除成员失败。	身份名要移除的身份名。错误消息	由于数据存储库错误，无法从身份中移除成员。	有关详细信息，请查阅数据存储库日志。
91	INFO	尝试读取身份的指定服务名	身份名	单击身份的服务指定视图中的“添加”按钮。	
92	INFO	读取身份的指定服务名成功	身份名	单击身份的服务指定视图中的“添加”按钮。	
93	SEVERE	读取身份的指定服务名失败。	身份名错误消息	无法读取身份的指定服务名。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
94	SEVERE	读取身份的指定服务名失败。	身份名错误消息	由于数据存储库错误，无法读取身份的指定服务名。	有关详细信息，请查阅数据存储库日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
101	INFO	尝试读取身份的可指定服务名	身份名	查看身份的服务页面。	
102	INFO	读取身份的可指定服务名成功	身份名	查看身份的服务页面。	
103	SEVERE	读取身份的可指定服务名失败。	身份名错误消息	无法读取身份的可指定服务名。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
104	SEVERE	读取身份的可指定服务名失败。	身份名错误消息	由于数据存储库错误，无法读取身份的可指定服务名。	有关详细信息，请查阅数据存储库日志。
111	INFO	尝试将服务指定到身份	身份名服务名	单击身份的服务视图中的“添加”按钮。	
112	INFO	将服务指定到身份成功	身份名服务名	单击身份的服务视图中的“添加”按钮。	
113	SEVERE	将服务指定到身份失败。	身份名服务名错误消息	无法将服务指定到身份。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
114	SEVERE	将服务指定到身份失败。	身份名服务名错误消息	由于数据存储库错误，无法将服务指定到身份。	有关详细信息，请查阅数据存储库日志。
121	INFO	尝试从身份取消指定服务	身份名服务名	单击身份的服务视图中的“移除”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
122	INFO	从身份取消指定服务成功	身份名服务名	单击身份的服务视图中的“移除”按钮。	
123	SEVERE	从身份取消指定服务失败。	身份名服务名错误消息	无法从身份取消指定服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
124	SEVERE	从身份取消指定服务失败。	身份名服务名错误消息	由于数据存储库错误，无法从身份取消指定服务。	有关详细信息，请查阅数据存储库日志。
131	INFO	尝试读取身份的服务属性值	身份名服务名	查看身份的服务配置文件视图。	
132	INFO	读取身份的服务属性值成功	身份名服务名	查看身份的服务配置文件视图。	
133	SEVERE	读取身份的服务属性值失败。	身份名服务名错误消息	无法读取身份的服务属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
134	SEVERE	读取身份的服务属性值失败。	身份名服务名错误消息	由于数据存储库错误，无法读取身份的服务属性值。	有关详细信息，请查阅数据存储库日志。
141	INFO	尝试向身份写入服务属性值	身份名服务名	单击身份的服务配置文件视图中的“保存”按钮。	
142	INFO	向身份写入服务属性值成功	身份名服务名	单击身份的服务配置文件视图中的“保存”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
143	SEVERE	向身份写入服务属性值失败。	身份名服务名错误消息	无法向身份写入服务属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
144	SEVERE	向身份写入服务属性值失败。	身份名服务名错误消息	由于数据存储库错误，无法向身份写入服务属性值。	有关详细信息，请查阅数据存储库日志。
201	INFO	尝试读取所有全局服务的默认属性值	服务名	查看服务的全局配置视图。	
202	INFO	读取所有全局服务的默认属性值成功	服务名	查看服务的全局配置视图。	
203	INFO	尝试读取全局服务的默认属性值	服务名属性名	查看服务的全局配置视图。	
204	INFO	读取全局服务的默认属性值成功	服务名属性名	查看服务的全局配置视图。	
205	INFO	读取全局服务的默认属性值失败	服务名属性名	查看服务的全局配置视图。	有关详细信息，请查阅服务管理日志。
211	INFO	尝试写入全局服务的默认属性值	服务名属性名	单击服务的全局配置视图中的“保存”按钮。	
212	INFO	写入全局服务的默认属性值成功	服务名属性名	单击服务的全局配置视图中的“保存”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
213	SEVERE	写入全局服务的默认属性值失败。	服务名属性名错误消息	无法写入全局服务的默认属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
214	SEVERE	写入全局服务的默认属性值失败。	服务名属性名错误消息	由于服务管理错误，无法写入服务默认属性值。	有关详细信息，请查阅服务管理日志。
221	INFO	尝试获取子配置名称	服务名基本全局子配置名称	查看其服务具有子模式的全局服务视图。	
222	INFO	读取全局子配置名称成功	服务名基本全局子配置名称	查看其服务具有子模式的全局服务视图。	
223	SEVERE	读取全局子配置名称失败。	服务名基本全局子配置名称错误消息	无法获取全局子配置名称。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
224	SEVERE	读取全局子配置名称失败。	服务名基本全局子配置名称错误消息	由于服务管理错误，无法获取全局子配置名称。	有关详细信息，请查阅服务管理日志。
231	INFO	尝试删除子配置	服务名基本全局子配置名称要删除的子配置名称	单击全局服务配置文件视图中的“删除选定”按钮。	
232	INFO	删除子配置成功	服务名基本全局子配置名称要删除的子配置名称	单击全局服务配置文件视图中的“删除选定”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
233	SEVERE	删除子配置失败。	服务名基本全局子配置名称要删除的子配置名称错误消息	无法删除子配置。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
234	SEVERE	删除子配置失败。	服务名基本全局子配置名称要删除的子配置名称错误消息	由于服务管理错误，无法删除子配置。	有关详细信息，请查阅服务管理日志。
241	INFO	尝试创建子配置	服务名基本全局子配置名称要创建的子配置名称要创建的子模式名称	单击创建子配置视图中的“添加”按钮。	
242	INFO	创建子配置成功	服务名基本全局子配置名称要创建的子配置名称要创建的子模式名称	单击创建子配置视图中的“添加”按钮。	
243	SEVERE	创建子配置失败。	服务名基本全局子配置名称要创建的子配置名称要创建的子模式名称错误消息	无法创建子配置。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
244	SEVERE	创建子配置失败。	服务名基本全局子配置名称要创建的子配置名称要创建的子模式名称错误消息	由于服务管理错误，无法创建子配置。	有关详细信息，请查阅服务管理日志。
251	INFO	读取子配置的属性值成功	服务名子配置名称	查看子配置配置文件视图。	
261	INFO	尝试写入子配置的属性值	服务名子配置名称	单击子配置配置文件视图中的“保存”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
262	INFO	写入子配置的属性值成功	服务名子配置名称	单击子配置配置文件视图中的“保存”按钮。	
263	SEVERE	写入子配置的属性值失败。	服务名子配置名称错误消息	无法写入子配置的属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
264	SEVERE	写入子配置的属性值失败。	服务名子配置名称错误消息	由于服务管理错误，无法写入子配置的属性值。	有关详细信息，请查阅服务管理日志。
301	INFO	尝试获取领域下的策略名。	领域名	查看策略主页。	
302	INFO	获取领域下的策略名成功	领域名	查看策略主页。	
303	SEVERE	获取领域下的策略名失败。	领域名错误消息	无法获取领域下的策略名。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅策略日志。
304	SEVERE	获取领域下的策略名失败。	领域名错误消息	由于与策略 SDK 相关的错误，无法获取领域下的策略名。	有关详细信息，请查阅策略日志。
311	INFO	尝试在领域下创建策略。	领域名策略名	单击策略创建页面中的“新建”按钮。	
312	INFO	创建策略成功	领域名策略名	单击策略创建页面中的“新建”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
313	SEVERE	创建策略失败。	领域名策略名错误消息	无法在领域下创建策略。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅策略日志。
314	SEVERE	创建策略失败。	领域名策略名错误消息	由于与策略 SDK 相关的错误，无法在领域下创建策略。	有关详细信息，请查阅策略日志。
321	INFO	尝试修改策略。	领域名策略名	单击策略配置文件页面中的“保存”按钮。	
322	INFO	修改策略成功	领域名策略名	单击策略配置文件页面中的“保存”按钮。	
323	SEVERE	修改策略失败。	领域名策略名错误消息	无法修改领域下的策略。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅策略日志。
324	SEVERE	修改策略失败。	领域名策略名错误消息	由于与策略 SDK 相关的错误，无法修改策略。	有关详细信息，请查阅策略日志。
331	INFO	尝试删除策略。	领域名策略名	单击策略主页中的“删除”按钮。	
332	INFO	删除策略成功	领域名策略名	单击策略主页中的“删除”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
333	SEVERE	删除策略失败。	领域名策略名错误消息	无法删除策略。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅策略日志。
334	SEVERE	删除策略失败。	领域名策略名错误消息	由于与策略 SDK 相关的错误，无法删除策略。	有关详细信息，请查阅策略日志。
401	INFO	尝试获取领域名	父领域名	查看领域主页。	
402	INFO	获取领域名成功。	父领域名	查看领域主页。	
403	SEVERE	获取领域名失败。	父领域名错误消息	由于服务管理 SDK 异常，无法获取领域名。	有关详细信息，请查阅服务管理日志。
411	INFO	尝试创建领域	父领域名新领域名	单击创建领域页面中的“新建”按钮。	
412	INFO	创建领域成功。	父领域名新领域名	单击创建领域页面中的“新建”按钮。	
413	SEVERE	创建领域失败。	父领域名新领域名错误消息	由于服务管理 SDK 异常，无法创建新领域。	有关详细信息，请查阅服务管理日志。
421	INFO	尝试删除领域	父领域名要删除的领域名	单击领域主页中的“删除”按钮。	
422	INFO	删除领域成功。	父领域名要删除的领域名	单击领域主页中的“删除”按钮。	
423	SEVERE	删除领域失败。	父领域名要删除的领域名错误消息	由于服务管理 SDK 异常，无法删除领域。	有关详细信息，请查阅服务管理日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
431	INFO	尝试获取领域的属性值	领域名	查看领域配置文件页面。	
432	INFO	获取领域的属性值成功。	领域名	查看领域配置文件页面。	
433	SEVERE	获取领域的属性值失败。	领域名错误消息	由于服务管理 SDK 异常，无法获取领域的属性值。	有关详细信息，请查阅服务管理日志。
441	INFO	尝试修改领域的配置文件	领域名	单击领域配置文件页面中的“保存”按钮。	
442	INFO	修改领域的配置文件成功。	领域名	单击领域配置文件页面中的“保存”按钮。	
443	SEVERE	修改领域的配置文件失败。	领域名错误消息	由于服务管理 SDK 异常，无法修改领域的配置文件。	有关详细信息，请查阅服务管理日志。
501	INFO	尝试获取领域下的委托主题	领域名搜索模式	查看委托主页。	
502	INFO	获取领域下的委托主题成功。	领域名搜索模式	查看委托主页。	
503	SEVERE	获取领域下的委托主题失败。	领域名搜索模式错误消息	无法获取委托主题。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅委托管理日志。
504	SEVERE	获取领域下的委托主题失败。	领域名搜索模式错误消息	由于与委托管理 SDK 相关的错误，无法获取委托主题。	有关详细信息，请查阅委托管理日志。
511	INFO	尝试获取委托主题的权限	领域名委托主题的 *ID*	查看委托主题配置文件页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
512	INFO	获取委托主题的权限成功。	领域名委托主题的 *ID*	查看委托主题配置文件页面。	
513	SEVERE	获取委托主题的权限失败。	领域名委托主题的 *ID* 错误消息	无法获取委托主题的权限。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅委托管理日志。
514	SEVERE	获取委托主题的权限失败。	领域名委托主题的 *ID* 错误消息	由于与委托管理 SDK 相关的错误，无法获取委托主题的权限。	有关详细信息，请查阅委托管理日志。
521	INFO	尝试修改委托权限	领域名委托权限的 *ID* 主题 *ID*	单击委托主题配置文件页面中的“保存”按钮。	
522	INFO	修改委托权限成功。	领域名委托权限的 *ID* 主题 *ID*	单击委托主题配置文件页面中的“保存”按钮。	
523	SEVERE	修改委托权限失败。	领域名委托权限的 *ID* 主题 *ID* 错误消息	无法修改委托权限。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅委托管理日志。
524	SEVERE	修改委托权限失败。	领域名委托权限的 *ID* 主题 *ID* 错误消息	由于与委托管理 SDK 相关的错误，无法修改委托权限。	有关详细信息，请查阅委托管理日志。
601	INFO	尝试获取数据存储库名称	领域名	查看数据存储库主页。	
602	INFO	获取数据存储库名称成功。	领域名	查看数据存储库主页。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
603	SEVERE	获取数据存储库名称失败。	领域名错误消息	无法获取数据存储库名称。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
604	SEVERE	获取数据存储库名称失败。	领域名错误消息	由于服务管理 SDK 异常，无法获取数据存储库名称。	有关详细信息，请查阅服务管理日志。
611	INFO	尝试获取身份库的属性值	领域名身份库名	查看数据存储库配置文件页面。	
612	INFO	获取数据存储库的属性值成功。	领域名身份库名	查看数据存储库配置文件页面。	
613	SEVERE	获取数据存储库的属性值失败。	领域名身份库名错误消息	无法获取身份库的属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
614	SEVERE	获取数据存储库的属性值失败。	领域名身份库名错误消息	由于服务管理 SDK 异常，无法获取数据存储库的属性值。	有关详细信息，请查阅服务管理日志。
621	INFO	尝试创建身份库	领域名身份库名身份库类型	单击数据存储库创建页面中的“新建”按钮。	
622	INFO	创建数据存储库成功。	领域名身份库名身份库类型	单击数据存储库创建页面中的“新建”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
623	SEVERE	创建数据存储库失败。	领域名身份库名身份库类型错误消息	无法创建身份库。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
624	SEVERE	创建数据存储库失败。	领域名身份库名身份库类型错误消息	由于服务管理 SDK 异常，无法创建数据存储库。	有关详细信息，请查阅服务管理日志。
631	INFO	尝试删除身份库	领域名身份库名	单击数据存储库主页中的“删除”按钮。	
632	INFO	删除数据存储库成功。	领域名身份库名	单击数据存储库主页中的“删除”按钮。	
633	SEVERE	删除数据存储库失败。	领域名身份库名错误消息	无法删除身份库。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
634	SEVERE	删除数据存储库失败。	领域名身份库名错误消息	由于服务管理 SDK 异常，无法删除数据存储库。	有关详细信息，请查阅服务管理日志。
641	INFO	尝试修改身份库	领域名身份库名	单击数据存储库配置文件页面中的“保存”按钮。	
642	INFO	修改数据存储库成功。	领域名身份库名	单击数据存储库配置文件页面中的“保存”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
643	SEVERE	修改数据存储库失败。	领域名身份库名错误消息	无法修改身份库。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
644	SEVERE	修改数据存储库失败。	领域名身份库名错误消息	由于服务管理 SDK 异常，无法修改数据存储库。	有关详细信息，请查阅服务管理日志。
701	INFO	尝试获取领域的指定服务	领域名	查看领域的服务主页。	
702	INFO	获取领域的指定服务成功。	领域名	查看领域的服务主页。	
703	SEVERE	获取领域的指定服务失败。	领域名错误消息	由于验证配置异常，无法获取领域的指定服务。	有关详细信息，请查阅验证日志。
704	SEVERE	获取领域的指定服务失败。	领域名错误消息	由于服务管理 SDK 异常，无法获取领域的指定服务。	有关详细信息，请查阅服务管理日志。
705	SEVERE	获取领域的指定服务失败。	领域名错误消息	由于数据存储库 SDK 异常，无法获取领域的指定服务。	有关详细信息，请查阅服务管理日志。
706	SEVERE	获取领域的指定服务失败。	领域名错误消息	无法获取领域的指定服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
711	INFO	尝试获取领域的可指定服务	领域名	查看领域的服务主页。	
712	INFO	获取领域的可指定服务成功。	领域名	查看领域的服务主页。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
713	SEVERE	获取领域的可指定服务失败。	领域名错误消息	由于验证配置异常，无法获取领域的可指定服务。	有关详细信息，请查阅验证日志。
714	SEVERE	获取领域的可指定服务失败。	领域名错误消息	由于服务管理 SDK 异常，无法获取领域的可指定服务。	有关详细信息，请查阅服务管理日志。
715	SEVERE	获取领域的可指定服务失败。	领域名错误消息	由于 ID 库管理 SDK 异常，无法获取领域的可指定服务。	有关详细信息，请查阅 ID 库管理日志。
716	SEVERE	获取领域的可指定服务失败。	领域名错误消息	无法获取领域的可指定服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
721	INFO	尝试从领域取消指定服务	领域名服务名	单击领域的服务页面中的“取消指定”按钮。	
722	INFO	从领域取消指定服务成功。	领域名服务名	单击领域的服务页面中的“取消指定”按钮。	
723	SEVERE	从领域取消指定服务失败。	领域名服务名错误消息	由于服务管理 SDK 异常，无法从领域取消指定服务。	有关详细信息，请查阅服务管理日志。
725	SEVERE	从领域取消指定服务失败。	领域名服务名错误消息	无法从领域取消指定服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库管理日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
724	SEVERE	从领域取消指定服务失败。	领域名服务名错误消息	由于数据存储库管理 SDK 异常，无法从领域取消指定服务。	有关详细信息，请查阅数据存储库管理日志。
731	INFO	尝试将服务指定到领域	领域名服务名	单击领域的服务页面中的“指定”按钮。	
732	INFO	将服务指定到领域成功。	领域名服务名	单击领域的服务页面中的“指定”按钮。	
733	SEVERE	将服务指定到领域失败。	领域名服务名错误消息	由于服务管理 SDK 异常，无法将服务指定到领域。	有关详细信息，请查阅服务管理日志。
734	SEVERE	将服务指定到领域失败。	领域名服务名错误消息	无法将服务指定到领域。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
735	SEVERE	将服务指定到领域失败。	领域名服务名错误消息	由于数据存储库 SDK 异常，无法将服务指定到领域。	有关详细信息，请查阅服务管理日志。
741	INFO	尝试获取领域中服务的属性值	领域名服务名属性模式名称	查看领域的服务配置文件页面。	
742	INFO	获取领域下服务的属性值成功。	领域名服务名属性模式名称	查看领域的服务配置文件页面。	
743	SEVERE	获取领域下服务的属性值失败。	领域名服务名属性模式名称错误消息	由于服务管理 SDK 异常，无法获取服务的属性值。	有关详细信息，请查阅服务管理日志。
744	INFO	获取领域下服务的属性值失败。	领域名服务名属性模式名称错误消息	由于数据存储库 SDK 异常，无法获取服务的属性值。	有关详细信息，请查阅服务管理日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
745	SEVERE	获取领域下服务的属性值失败。	领域名服务名属性模式名称错误消息	无法获取服务的属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
751	INFO	尝试修改领域中服务的属性值	领域名服务名	单击领域的服务配置文件页面中的“保存”按钮。	
752	INFO	修改领域下服务的属性值成功。	领域名服务名	单击领域的服务配置文件页面中的“保存”按钮。	
753	SEVERE	修改领域下服务的属性值失败。	领域名服务名错误消息	由于服务管理 SDK 异常，无法修改服务的属性值。	有关详细信息，请查阅服务管理日志。
754	SEVERE	修改领域下服务的属性值失败。	领域名服务名错误消息	由于数据存储库错误，无法修改服务的属性值。	有关详细信息，请查阅数据存储库日志。
755	SEVERE	修改领域下服务的属性值失败。	领域名服务名错误消息	无法修改服务的属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅数据存储库日志。
801	INFO	尝试获取验证类型		查看验证配置文件页面。	
802	INFO	获取验证类型成功。		查看验证配置文件页面。	
803	SEVERE	获取验证类型失败。	错误消息	由于验证配置 SDK 异常，无法获取验证类型。	有关详细信息，请查阅验证管理日志。
811	INFO	尝试获取领域下的验证实例	领域名	查看验证配置文件页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
812	INFO	获取领域下的验证实例成功。	领域名	查看验证配置文件页面。	
813	SEVERE	获取领域下的验证实例失败。	领域名错误消息	由于验证配置 SDK 异常，无法获取验证实例。	有关详细信息，请查阅验证管理日志。
821	INFO	尝试移除领域下的验证实例	领域名验证实例名	查看验证配置文件页面。	
822	INFO	移除领域下的验证实例成功。	领域名验证实例名	查看验证配置文件页面。	
823	SEVERE	移除领域下的验证实例失败。	领域名验证实例名错误消息	由于验证配置 SDK 异常，无法移除验证实例。	有关详细信息，请查阅验证管理日志。
831	INFO	尝试在领域下创建验证实例	领域名验证实例名验证实例类型	单击验证创建页面中的“新建”按钮。	
832	INFO	在领域下创建验证实例成功。	领域名验证实例名验证实例类型	单击验证创建页面中的“新建”按钮。	
833	SEVERE	在领域下创建验证实例失败。	领域名验证实例名验证实例类型错误消息	由于验证配置异常，无法创建验证实例。	有关详细信息，请查阅验证配置日志。
841	INFO	尝试修改验证实例	领域名验证服务名	单击验证配置文件页面中的“保存”按钮。	
842	INFO	修改验证实例成功。	领域名验证服务名	单击验证配置文件页面中的“保存”按钮。	
843	SEVERE	修改验证实例失败。	领域名验证服务名错误消息	由于服务管理 SDK 异常，无法修改验证实例。	有关详细信息，请查阅服务管理日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
844	SEVERE	修改验证实例失败。	领域名验证服务名错误消息	无法修改验证实例。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
851	INFO	尝试获取验证实例配置文件	领域名验证实例名	查看验证实例配置文件页面。	
852	INFO	获取验证实例配置文件成功。	领域名验证实例名	查看验证实例配置文件页面。	
853	SEVERE	获取验证实例配置文件失败。	领域名验证实例名错误消息	由于验证配置 SDK 异常，无法获取验证实例配置文件。	有关详细信息，请查阅验证管理日志。
861	INFO	尝试修改验证实例配置文件	领域名验证实例名	单击验证实例配置文件页面中的“保存”按钮。	
862	INFO	修改验证实例配置文件成功。	领域名验证实例名	单击验证实例配置文件页面中的“保存”按钮。	
863	SEVERE	修改验证实例配置文件失败。	领域名验证实例名错误消息	由于验证配置 SDK 异常，无法修改验证实例配置文件。	有关详细信息，请查阅验证管理日志。
864	SEVERE	修改验证实例配置文件失败。	领域名验证实例名错误消息	由于服务管理 SDK 异常，无法修改验证实例配置文件。	有关详细信息，请查阅服务管理日志。
864	SEVERE	修改验证实例配置文件失败。	领域名验证实例名错误消息	无法修改验证实例配置文件。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
871	INFO	尝试获取领域下的验证配置文件	领域名	查看领域页面下的验证配置文件。	
872	INFO	获取领域下的验证配置文件成功。	领域名	查看领域页面下的验证配置文件。	
873	SEVERE	获取领域下的验证配置文件失败。	领域名错误消息	由于服务管理 SDK 异常，无法获取领域下的验证配置文件。	有关详细信息，请查阅服务管理日志。
881	INFO	尝试获取验证配置配置文件	领域名验证配置名称	查看验证配置配置文件页面。	
882	INFO	获取验证配置配置文件成功。	领域名验证配置名称	查看验证配置配置文件页面。	
883	SEVERE	获取验证配置配置文件失败。	领域名验证配置名称错误消息	无法获取验证配置配置文件。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
884	SEVERE	获取验证配置配置文件失败。	领域名验证配置名称错误消息	由于服务管理 SDK 异常，无法获取验证配置配置文件。	有关详细信息，请查阅服务管理日志。
885	SEVERE	获取验证配置配置文件失败。	领域名验证配置名称错误消息	由于验证配置 SDK 异常，无法获取验证配置配置文件。	有关详细信息，请查阅验证配置日志。
891	INFO	尝试修改验证配置配置文件	领域名验证配置名称	单击验证配置配置文件页面中的“保存”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
892	INFO	修改验证配置配置文件成功。	领域名验证配置名称	单击验证配置配置文件页面中的“保存”按钮。	
893	SEVERE	修改验证配置配置文件失败。	领域名验证配置名称错误消息	无法修改验证配置配置文件。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
894	SEVERE	修改验证配置配置文件失败。	领域名验证配置名称错误消息	由于服务管理 SDK 异常，无法修改验证配置配置文件。	有关详细信息，请查阅服务管理日志。
895	SEVERE	修改验证配置配置文件失败。	领域名验证配置名称错误消息	由于验证配置 SDK 异常，无法修改验证配置配置文件。	有关详细信息，请查阅验证配置日志。
901	INFO	尝试创建验证配置	领域名验证配置名称	单击验证配置创建页面中的“新建”按钮。	
902	INFO	创建验证配置成功。	领域名验证配置名称	单击验证配置创建页面中的“新建”按钮。	
903	SEVERE	创建验证配置失败。	领域名验证配置名称错误消息	无法创建验证配置。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
904	SEVERE	创建验证配置失败。	领域名验证配置名称错误消息	由于服务管理 SDK 异常，无法创建验证配置。	有关详细信息，请查阅服务管理日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
905	SEVERE	创建验证配置失败。	领域名验证配置名称错误消息	由于验证配置 SDK 异常，无法创建验证配置。	有关详细信息，请查阅验证配置日志。
1001	INFO	尝试获取实体描述符名称。	搜索模式	查看实体描述符主页。	
1002	INFO	获取实体描述符名称成功	搜索模式	查看实体描述符主页。	
1003	SEVERE	获取实体描述符名称失败。	搜索模式错误消息	由于与联合 SDK 相关的错误，无法获取实体描述符名称。	有关详细信息，请查阅联合日志。
1011	INFO	尝试创建实体描述符。	描述符名称描述符类型	单击实体描述符创建页面中的“新建”按钮。	
1012	INFO	创建实体描述符成功	描述符名称描述符类型	单击实体描述符创建页面中的“新建”按钮。	
1013	SEVERE	创建实体描述符失败。	描述符名称描述符类型错误消息	由于与联合 SDK 相关的错误，无法创建实体描述符。	有关详细信息，请查阅联合日志。
1021	INFO	尝试删除实体描述符。	描述符名称	单击实体描述符主页中的“删除”按钮。	
1022	INFO	删除实体描述符成功	描述符名称	单击实体描述符主页中的“删除”按钮。	
1023	SEVERE	删除实体描述符失败。	描述符名称错误消息	由于与联合 SDK 相关的错误，无法删除实体描述符。	有关详细信息，请查阅联合日志。
1031	INFO	尝试获取联合提供者实体描述符的属性值。	描述符名称	查看联合提供者实体描述符配置文件页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
1032	INFO	获取联合提供者实体描述符的属性值成功。	描述符名称	查看联合提供者实体描述符配置文件页面。	
1033	SEVERE	获取联合提供者实体描述符的属性值失败。	描述符名称错误消息	由于与联合 SDK 相关的错误，无法获取联合提供者实体描述符的属性值。	有关详细信息，请查阅联合日志。
1041	INFO	尝试修改联合提供者实体描述符。	描述符名称	单击联合提供者实体描述符配置文件页面中的“保存”按钮。	
1042	INFO	修改联合提供者实体描述符成功。	描述符名称	单击联合提供者实体描述符配置文件页面中的“保存”按钮。	
1043	SEVERE	修改联合提供者实体描述符失败。	描述符名称错误消息	由于与联合 SDK 相关的错误，无法修改联合提供者实体描述符。	有关详细信息，请查阅联合日志。
1044	SEVERE	修改联合提供者实体描述符失败。	描述符名称错误消息	由于一个或多个属性值的编号格式错误，无法修改联合提供者实体描述符。	有关详细信息，请查阅联合日志。
1051	INFO	尝试获取实体描述符的属性值。	描述符名称	查看实体描述符配置文件页面。	
1052	INFO	获取实体描述符的属性值成功。	描述符名称	查看实体描述符配置文件页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
1053	SEVERE	获取实体描述符的属性值失败。	描述符名称错误消息	由于与联合 SDK 相关的错误，无法获取实体描述符的属性值。	有关详细信息，请查阅联合日志。
1061	INFO	尝试修改实体描述符。	描述符名称	单击实体描述符配置文件页面中的“保存”按钮。	
1062	INFO	修改实体描述符成功。	描述符名称	单击实体描述符配置文件页面中的“保存”按钮。	
1063	SEVERE	修改实体描述符失败。	描述符名称错误消息	由于与联合 SDK 相关的错误，无法修改实体描述符。	有关详细信息，请查阅联合日志。
1101	INFO	尝试获取验证域名。	搜索模式	查看验证域主页。	
1102	INFO	获取验证域名成功。	搜索模式	查看验证域主页。	
1103	SEVERE	获取验证域名失败。	搜索模式错误消息	由于与联合 SDK 相关的错误，无法获取验证域名。	有关详细信息，请查阅联合日志。
1111	INFO	尝试创建验证域	验证域名	单击验证域创建页面中的“新建”按钮。	
1112	INFO	创建验证域成功。	验证域名	单击验证域创建页面中的“新建”按钮。	
1113	SEVERE	创建验证域失败。	验证域名错误消息	由于与联合 SDK 相关的错误，无法创建验证域。	有关详细信息，请查阅联合日志。
1121	INFO	尝试删除验证域	验证域名	单击验证域主页中的“删除”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
1122	INFO	删除验证域成功。	验证域名	单击验证域主页中的“删除”按钮。	
1123	SEVERE	删除验证域失败。	验证域名错误消息	由于与联合 SDK 相关的错误，无法删除验证域。	有关详细信息，请查阅联合日志。
1131	INFO	尝试获取验证域的属性值	验证域名	查看验证域配置文件页面。	
1132	INFO	获取验证域的属性值成功。	验证域名	查看验证域配置文件页面。	
1133	SEVERE	获取验证域的属性值失败。	验证域名错误消息	由于与联合 SDK 相关的错误，无法获取验证域的属性值。	有关详细信息，请查阅联合日志。
1141	INFO	尝试修改验证域	验证域名	单击验证域配置文件页面中的“保存”按钮。	
1142	INFO	修改验证域成功。	验证域名	单击验证域配置文件页面中的“保存”按钮。	
1143	SEVERE	修改验证域失败。	验证域名错误消息	由于与联合 SDK 相关的错误，无法修改验证域。	有关详细信息，请查阅联合日志。
1151	INFO	尝试获取所有提供者名称		查看验证域配置文件页面。	
1152	INFO	获取所有提供者名称成功。		查看验证域配置文件页面。	
1153	SEVERE	获取所有提供者名称失败。	错误消息	由于与联合 SDK 相关的错误，无法获取所有提供者名称。	有关详细信息，请查阅联合日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
1161	INFO	尝试获取验证域下的提供者名称	验证域名	查看验证域配置文件页面。	
1162	INFO	获取验证域下的提供者名称成功。	验证域名	查看验证域配置文件页面。	
1163	SEVERE	获取验证域下的提供者名称失败。	验证域名错误消息	由于与联合 SDK 相关的错误，无法获取验证域下的提供者名称。	有关详细信息，请查阅联合日志。
1171	INFO	尝试将提供者添加到验证域	验证域名提供者名称	单击提供者分配页面中的“保存”按钮。	
1172	INFO	将提供者添加到验证域成功。	验证域名提供者名称	单击提供者分配页面中的“保存”按钮。	
1173	SEVERE	将提供者添加到验证域失败。	验证域名提供者名称错误消息	由于与联合 SDK 相关的错误，无法将提供者添加到验证域。	有关详细信息，请查阅联合日志。
1181	INFO	尝试从验证域移除提供者。	验证域名提供者名称	单击提供者分配页面中的“保存”按钮。	
1182	INFO	从验证域删除提供者成功。	验证域名提供者名称	单击提供者分配页面中的“保存”按钮。	
1183	SEVERE	从验证域删除提供者失败。	验证域名提供者名称错误消息	由于与联合 SDK 相关的错误，无法从验证域中移除提供者。	有关详细信息，请查阅联合日志。
1301	INFO	尝试创建提供者	提供者名称提供者角色提供者类型	单击提供者分配页面中的“保存”按钮。	
1302	INFO	创建提供者成功。	提供者名称提供者角色提供者类型	单击提供者分配页面中的“保存”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
1303	SEVERE	创建提供者失败。	提供者名称提供者角色提供者类型错误消息	由于与联合 SDK 相关的错误，无法创建提供者。	有关详细信息，请查阅联合日志。
1303	SEVERE	创建提供者失败。	提供者名称提供者角色提供者类型错误消息	由于与联合 SDK 相关的错误，无法创建提供者。	有关详细信息，请查阅联合日志。
1304	SEVERE	创建提供者失败。	提供者名称提供者角色提供者类型错误消息	由于管理控制台无法找到为此提供者设置值的适当方法，因此无法创建提供者。	这是 Web 应用程序错误。请联系 Sun 技术支持获得帮助。
1311	INFO	尝试获取提供者的属性值	提供者名称提供者角色提供者类型	查看提供者配置文件页面。	
1312	INFO	获取提供者的属性值成功。	提供者名称提供者角色提供者类型	查看提供者配置文件页面。	
1321	INFO	尝试获取提供者的处理程序	提供者名称提供者角色	查看提供者配置文件页面。	
1322	INFO	获取提供者处理程序成功。	提供者名称提供者角色	查看提供者配置文件页面。	
1323	SEVERE	获取提供者处理程序失败。	提供者名称提供者角色错误消息	由于与联合 SDK 相关的错误，无法获取提供者处理程序。	有关详细信息，请查阅联合日志。
1331	INFO	尝试修改提供者	提供者名称提供者角色	单击提供者配置文件页面中的“保存”按钮。	
1332	INFO	修改提供者成功。	提供者名称提供者角色	单击提供者配置文件页面中的“保存”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
1333	SEVERE	修改提供者失败。	提供者名称提供者角色错误消息	由于与联合 SDK 相关的错误，无法修改提供者。	有关详细信息，请查阅联合日志。
1334	SEVERE	修改提供者失败。	提供者名称提供者角色错误消息	由于管理控制台无法找到为此提供者设置值的适当方法，因此无法修改提供者。	这是 Web 应用程序错误。请联系 Sun 技术支持获得帮助。
1341	INFO	尝试删除提供者	提供者名称提供者角色	单击提供者配置文件页面中的“删除提供者”按钮。	
1342	INFO	删除提供者成功。	提供者名称提供者角色	单击提供者配置文件页面中的“删除提供者”按钮。	
1343	SEVERE	删除提供者失败。	提供者名称提供者角色错误消息	由于与联合 SDK 相关的错误，无法删除提供者。	有关详细信息，请查阅联合日志。
1351	INFO	尝试获取预期的可信赖提供者	提供者名称提供者角色	查看添加可信赖提供者页面。	
1352	INFO	获取预期的可信赖提供者成功。	提供者名称提供者角色	查看添加可信赖提供者页面。	
1353	SEVERE	获取预期的可信赖提供者失败。	提供者名称提供者角色错误消息	由于与联合 SDK 相关的错误，无法获取预期的可信赖提供者。	有关详细信息，请查阅联合日志。
2001	INFO	尝试获取服务模式的模式类型的属性值	服务名模式类型名称属性模式名称	查看服务配置文件页面。	
2002	INFO	获取服务模式的模式类型的属性值成功。	服务名模式类型名称属性模式名称	查看服务配置文件页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
2003	SEVERE	获取服务模式的模式类型的属性值失败。	服务名模式类型名称属性类型名称错误消息	无法获取服务模式的模式类型的属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
2004	SEVERE	获取服务模式的模式类型的属性值失败。	服务名模式类型名称属性类型名称错误消息	由于与服务管理 SDK 相关的错误，无法获取服务模式的模式类型的属性值。	有关详细信息，请查阅服务管理日志。
2005	INFO	获取服务模式的模式类型的属性值失败。	服务名模式类型名称属性模式名称	查看服务配置文件页面。	无需对此事件执行任何操作。控制台尝试从服务获取模式，但模式不存在。
2011	INFO	尝试获取服务模式的模式类型的属性模式的属性值	服务名模式类型名称属性模式名称	查看服务配置文件页面。	
2012	INFO	获取服务模式的模式类型的属性模式的属性值成功。	服务名模式类型名称属性模式名称	查看服务配置文件页面。	
2013	SEVERE	获取服务模式的模式类型的属性模式的属性值失败。	服务名模式类型名称属性类型名称错误消息	无法获取服务模式的模式类型的属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
2014	SEVERE	获取服务模式的模式类型的属性模式的属性值失败。	服务名模式类型名称属性类型名称错误消息	由于与服务管理 SDK 相关的错误，无法获取服务模式的模式类型的属性值。	有关详细信息，请查阅服务管理日志。
2021	INFO	尝试修改服务模式的模式类型的属性模式的属性值	服务名模式类型名称属性模式名称	单击服务配置文件页面中的“保存”按钮。	
2022	INFO	修改服务模式的模式类型的属性模式的属性值成功。	服务名模式类型名称属性模式名称	单击服务配置文件页面中的“保存”按钮。	
2023	SEVERE	修改服务模式的模式类型的属性模式的属性值失败。	服务名模式类型名称属性类型名称错误消息	无法修改服务模式的模式类型的属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅服务管理日志。
2024	SEVERE	修改服务模式的模式类型的属性模式的属性值失败。	服务名模式类型名称属性类型名称错误消息	由于与服务管理 SDK 相关的错误，无法修改服务模式的模式类型的属性值。	有关详细信息，请查阅服务管理日志。
2501	INFO	尝试获取客户机检测服务的设备名称	配置文件名样式名搜索模式	查看客户机配置文件页面。	
2502	INFO	获取客户机检测服务的设备名称成功。	配置文件名样式名搜索模式	查看客户机配置文件页面。	
2511	INFO	尝试删除客户机检测服务中的客户机	客户机类型	单击客户机类型删除超级链接页面。	
2512	INFO	删除客户机检测服务中的客户机成功。	客户机类型	单击客户机类型删除超级链接页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
2513	SEVERE	删除客户机检测服务中的客户机失败。	客户机类型错误消息	由于与客户机检测 SDK 相关的错误，无法删除客户机。	有关详细信息，请查阅客户机检测管理日志。
2521	INFO	尝试创建客户机检测服务中的客户机	客户机类型	单击“客户机创建”页面中的“新建”按钮。	
2522	INFO	创建客户机检测服务中的客户机成功。	客户机类型	单击“客户机创建”页面中的“新建”按钮。	
2523	SEVERE	创建客户机检测服务中的客户机失败。	客户机类型错误消息	由于与客户机检测 SDK 相关的错误，无法创建客户机。	有关详细信息，请查阅客户机检测管理日志。
2524	INFO	创建客户机检测服务中的客户机失败。	客户机类型错误消息	由于客户机类型无效，因此无法创建客户机。	创建前请再次检查客户机类型。
2531	INFO	尝试获取客户机检测服务中的客户机配置文件	客户机类型分类	查看客户机配置文件页面。	
2532	INFO	获取客户机检测服务中的客户机配置文件成功。	客户机类型分类	查看客户机配置文件页面。	
2541	INFO	尝试修改客户机检测服务中的客户机配置文件	客户机类型	单击客户机配置文件页面中的“保存”按钮。	
2542	INFO	修改客户机检测服务中的客户机配置文件成功。	客户机类型	单击客户机配置文件页面中的“保存”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
2543	SEVERE	修改客户机检测服务中的客户机配置文件失败。	客户机类型错误消息	由于与客户机检测 SDK 相关的错误，无法修改客户机配置文件。	有关详细信息，请查阅客户机检测管理日志。
3001	INFO	尝试获取当前会话	服务器名搜索模式	查看会话主页。	
3002	INFO	获取当前会话成功。	服务器名搜索模式	查看会话主页。	
3003	SEVERE	获取当前会话失败。	服务器名领域名错误消息	由于会话 SDK 异常，无法获取当前会话。	有关详细信息，请查阅会话管理日志。
3011	INFO	尝试使会话无效	服务器名会话 *ID*	单击会话主页中的“使无效”按钮。	
3012	INFO	使会话无效成功。	服务器名会话 *ID*	单击会话主页中的“使无效”按钮。	
3013	SEVERE	使会话无效失败。	服务器名会话 *ID* 错误消息	由于会话 SDK 异常，无法使会话无效。	有关详细信息，请查阅会话管理日志。
10001	INFO	尝试从组织搜索容器	组织 DN 搜索模式	单击组织的容器页面中的“搜索”按钮。	
10002	INFO	从组织搜索容器成功。	组织 DN 搜索模式	单击组织的容器页面中的“搜索”按钮。	
10003	SEVERE	从组织搜索容器失败。	组织 DN 搜索模式错误消息	无法搜索容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10004	SEVERE	从组织搜索容器失败。	组织 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索容器。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10011	INFO	尝试从容器搜索容器	容器 DN 搜索模式	单击容器的子容器页面中的“搜索”按钮。	
10012	INFO	从容器搜索容器成功。	容器 DN 搜索模式	单击容器的子容器页面中的“搜索”按钮。	
10013	SEVERE	从容器搜索容器失败。	容器 DN 搜索模式错误消息	无法搜索容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10014	SEVERE	从容器搜索容器失败。	容器 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索容器。	有关详细信息，请查阅访问管理 SDK 日志。
10021	INFO	尝试在组织下创建容器	组织 DN 容器名	单击“容器创建”页面中的“新建”按钮。	
10022	INFO	在组织下创建容器成功。	组织 DN 容器名	单击“容器创建”页面中的“新建”按钮。	
10023	SEVERE	在组织下创建容器失败。	组织 DN 容器名错误消息	无法创建容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10024	SEVERE	在组织下创建容器失败。	组织 DN 容器名错误消息	由于访问管理 SDK 异常，无法创建容器。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10031	INFO	尝试在容器下创建容器	容器 DN 容器名	单击“容器创建”页面中的“新建”按钮。	
10032	INFO	在容器下创建容器成功。	容器 DN 容器名	单击“容器创建”页面中的“新建”按钮。	
10033	SEVERE	在容器下创建容器失败。	容器 DN 容器名错误消息	无法创建容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10034	SEVERE	在容器下创建容器失败。	容器 DN 容器名错误消息	由于访问管理 SDK 异常，无法创建容器。	有关详细信息，请查阅访问管理 SDK 日志。
10041	INFO	尝试获取容器的指定服务	容器 DN	查看容器的服务配置文件页面。	
10042	INFO	获取容器的指定服务成功。	容器 DN	查看容器的服务配置文件页面。	
10043	SEVERE	获取容器的指定服务失败。	容器 DN 错误消息	无法获取指定给容器的服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10044	SEVERE	获取容器的指定服务失败。	容器 DN 错误消息	由于访问管理 SDK 异常，无法获取指定给容器的服务。	有关详细信息，请查阅访问管理 SDK 日志。
10101	INFO	尝试获取组织下的服务模板	组织 DN 服务名模板类型	查看组织的服务配置文件页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10102	INFO	获取组织下的服务模板成功。	组织 DN 服务名模板类型	查看组织的服务配置文件页面。	
10103	SEVERE	获取组织下的服务模板失败。	组织 DN 服务名模板类型错误消息	无法获取服务模板。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10104	SEVERE	获取组织下的服务模板失败。	组织 DN 服务名模板类型错误消息	由于访问管理 SDK 异常，无法获取服务模板。	有关详细信息，请查阅访问管理 SDK 日志。
10111	INFO	尝试获取容器下的服务模板	容器 DN 服务名模板类型	查看容器的服务配置文件页面。	
10112	INFO	获取容器下的服务模板成功。	容器 DN 服务名模板类型	查看容器的服务配置文件页面。	
10113	SEVERE	获取容器下的服务模板失败。	容器 DN 服务名模板类型错误消息	无法获取服务模板。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10114	SEVERE	获取容器下的服务模板失败。	容器 DN 服务名模板类型错误消息	由于访问管理 SDK 异常，无法获取服务模板。	有关详细信息，请查阅访问管理 SDK 日志。
10121	INFO	尝试删除目录对象	对象名	单击对象主页中的“删除”按钮。	
10122	INFO	删除目录对象成功。	对象名	单击对象主页中的“删除”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10123	SEVERE	删除目录对象失败。	对象名错误消息	无法删除目录对象。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10124	SEVERE	删除目录对象失败。	对象名错误消息	由于访问管理 SDK 异常，无法删除目录对象。	有关详细信息，请查阅访问管理 SDK 日志。
10131	INFO	尝试修改目录对象	对象 DN	单击对象配置文件页面。	
10132	INFO	修改目录对象成功。	对象 DN	单击对象配置文件页面。	
10133	SEVERE	修改目录对象失败。	对象 DN 错误消息	由于访问管理 SDK 异常，无法修改目录对象。	有关详细信息，请查阅访问管理 SDK 日志。
10141	INFO	尝试从组织中删除服务	组织 DN 服务名	单击组织的服务页面中的“取消指定”按钮。	
10142	INFO	从组织中删除服务成功。	组织 DN 服务名	单击组织的服务页面中的“取消指定”按钮。	
10143	SEVERE	从组织中删除服务失败。	组织 DN 服务名错误消息	无法删除服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10144	SEVERE	从组织中删除服务失败。	组织 DN 服务名错误消息	由于访问管理 SDK 异常，无法删除服务。	有关详细信息，请查阅访问管理 SDK 日志。
10151	INFO	尝试从容器中删除服务	容器 DN 服务名	单击容器的服务页面中的“取消指定”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10152	INFO	从容器中删除服务成功。	容器 DN 服务名	单击容器的服务页面中的“取消指定”按钮。	
10153	SEVERE	从容器中删除服务失败。	容器 DN 服务名错误消息	无法删除服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10154	SEVERE	从容器中删除服务失败。	容器 DN 服务名错误消息	由于访问管理 SDK 异常，无法删除服务。	有关详细信息，请查阅访问管理 SDK 日志。
10201	INFO	尝试搜索组织下的组容器	组织 DN 搜索模式	单击组织的组容器页面中的“搜索”按钮。	
10202	INFO	搜索组织下的组容器成功。	组织 DN 搜索模式	单击组织的组容器页面中的“搜索”按钮。	
10203	SEVERE	搜索组织下的组容器失败。	组织 DN 搜索模式错误消息	无法搜索组容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10204	SEVERE	搜索组织下的组容器失败。	组织 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索组容器。	有关详细信息，请查阅访问管理 SDK 日志。
10211	INFO	尝试搜索容器下的组容器	容器 DN 搜索模式	单击容器的组容器页面中的“搜索”按钮。	
10212	INFO	搜索容器下的组容器成功。	容器 DN 搜索模式	单击容器的组容器页面中的“搜索”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10213	SEVERE	搜索容器下的组容器失败。	容器 DN 搜索模式错误消息	无法搜索组容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10214	SEVERE	搜索容器下的组容器失败。	容器 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索组容器。	有关详细信息，请查阅访问管理 SDK 日志。
10221	INFO	尝试搜索组容器下的组容器	组容器 DN 搜索模式	单击组容器的组容器页面中的“搜索”按钮。	
10222	INFO	搜索组容器下的组容器成功。	组容器 DN 搜索模式	单击组容器的组容器页面中的“搜索”按钮。	
10223	SEVERE	搜索组容器下的组容器失败。	组容器 DN 搜索模式错误消息	无法搜索组容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10224	SEVERE	搜索组容器下的组容器失败。	组容器 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索组容器。	有关详细信息，请查阅访问管理 SDK 日志。
10231	INFO	尝试在组织中创建组容器	组织 DN 组容器名	单击组容器创建页面中的“新建”按钮。	
10232	INFO	在组织下创建组容器成功。	组织 DN 组容器名	单击组容器创建页面中的“新建”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10233	SEVERE	在组织下创建组容器失败。	组织 DN 组容器名错误消息	无法创建组容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10234	SEVERE	在组织下创建组容器失败。	组织 DN 组容器名错误消息	由于访问管理 SDK 异常，无法创建组容器。	有关详细信息，请查阅访问管理 SDK 日志。
10241	INFO	尝试在容器中创建组容器	容器 DN 组容器名	单击组容器创建页面中的“新建”按钮。	
10242	INFO	在容器下创建组容器成功。	容器 DN 组容器名	单击组容器创建页面中的“新建”按钮。	
10243	SEVERE	在容器下创建组容器失败。	容器 DN 组容器名错误消息	无法创建组容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10244	SEVERE	在容器下创建组容器失败。	容器 DN 组容器名错误消息	由于访问管理 SDK 异常，无法创建组容器。	有关详细信息，请查阅访问管理 SDK 日志。
10251	INFO	尝试在组容器中创建组容器	组容器 DN 组容器名	单击组容器创建页面中的“新建”按钮。	
10252	INFO	在组容器下创建组容器成功。	组容器 DN 组容器名	单击组容器创建页面中的“新建”按钮。	
10253	SEVERE	在组容器下创建组容器失败。	组容器 DN 组容器名错误消息	无法创建组容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10254	SEVERE	在组容器下创建组容器失败。	组容器 DN 组容器名错误消息	由于访问管理 SDK 异常，无法创建组容器。	有关详细信息，请查阅访问管理 SDK 日志。
10301	INFO	尝试搜索组织下的组	组织 DN 搜索模式	单击组织的组页面中的“搜索”按钮。	
10302	INFO	搜索组织下的组成功。	组织 DN 搜索模式	单击组织的组页面中的“搜索”按钮。	
10303	SEVERE	搜索组织下的组失败。	组织 DN 搜索模式错误消息	无法搜索组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10304	SEVERE	搜索组织下的组失败。	组织 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索组。	有关详细信息，请查阅访问管理 SDK 日志。
10311	INFO	尝试搜索容器下的组	容器 DN 搜索模式	单击容器的组页面中的“搜索”按钮。	
10312	INFO	搜索容器下的组成功。	容器 DN 搜索模式	单击容器的组页面中的“搜索”按钮。	
10313	SEVERE	搜索容器下的组失败。	容器 DN 搜索模式错误消息	无法搜索组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10314	SEVERE	搜索容器下的组失败。	容器 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索组。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10321	INFO	尝试搜索静态组下的组	静态组 DN 搜索模式	单击静态组的组页面中的“搜索”按钮。	
10322	INFO	搜索静态组下的组成功。	静态组 DN 搜索模式	单击静态组的组页面中的“搜索”按钮。	
10323	SEVERE	搜索静态组下的组失败。	静态组 DN 搜索模式错误消息	无法搜索组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10324	SEVERE	搜索静态组下的组失败。	静态组 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索组。	有关详细信息，请查阅访问管理 SDK 日志。
10331	INFO	尝试搜索动态组下的组	动态组 DN 搜索模式	单击动态组的组页面中的“搜索”按钮。	
10332	INFO	搜索动态组下的组成功。	动态组 DN 搜索模式	单击动态组的组页面中的“搜索”按钮。	
10333	SEVERE	搜索动态组下的组失败。	动态组 DN 搜索模式错误消息	无法搜索组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10334	SEVERE	搜索动态组下的组失败。	动态组 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索组。	有关详细信息，请查阅访问管理 SDK 日志。
10341	INFO	尝试搜索可指定动态组下的组	可指定动态组 DN 搜索模式	单击可指定动态组的组页面中的“搜索”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10342	INFO	搜索可指定动态组下的组成功。	可指定动态组 DN 搜索模式	单击可指定动态组的组页面中的“搜索”按钮。	
10343	SEVERE	搜索可指定动态组下的组失败。	可指定动态组 DN 搜索模式错误消息	无法搜索组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10344	SEVERE	搜索可指定动态组下的组失败。	可指定动态组 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索组。	有关详细信息，请查阅访问管理 SDK 日志。
10351	INFO	尝试在组织下创建组	组织 DN 组名	单击组创建页面中的“新建”按钮。	
10352	INFO	在组织下创建组成功。	组织 DN 组名	单击组创建页面中的“新建”按钮。	
10353	SEVERE	在组织下创建组失败。	组织 DN 组名错误消息	无法创建组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10354	SEVERE	在组织下创建组失败。	组织 DN 组名错误消息	由于访问管理 SDK 异常，无法创建组。	有关详细信息，请查阅访问管理 SDK 日志。
10361	INFO	尝试在容器下创建组	容器 DN 组名	单击组创建页面中的“新建”按钮。	
10362	INFO	在容器下创建组成功。	容器 DN 组名	单击组创建页面中的“新建”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10363	SEVERE	在容器下创建组失败。	容器 DN 组名错误消息	无法创建组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10364	SEVERE	在容器下创建组失败。	容器 DN 组名错误消息	由于访问管理 SDK 异常，无法创建组。	有关详细信息，请查阅访问管理 SDK 日志。
10371	INFO	尝试在组容器下创建组	组容器 DN 组名	单击组创建页面中的“新建”按钮。	
10372	INFO	在组容器下创建组成功。	组容器 DN 组名	单击组创建页面中的“新建”按钮。	
10373	SEVERE	在组容器下创建组失败。	组容器 DN 组名错误消息	无法创建组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10374	SEVERE	在组容器下创建组失败。	组容器 DN 组名错误消息	由于访问管理 SDK 异常，无法创建组。	有关详细信息，请查阅访问管理 SDK 日志。
10381	INFO	尝试在动态组下创建组	动态组 DN 组名	单击组创建页面中的“新建”按钮。	
10382	INFO	在动态组下创建组成功。	动态组 DN 组名	单击组创建页面中的“新建”按钮。	
10383	SEVERE	在动态组下创建组失败。	动态组 DN 组名错误消息	无法创建组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10384	SEVERE	在动态组下创建组失败。	动态组 DN 组名错误消息	由于访问管理 SDK 异常，无法创建组。	有关详细信息，请查阅访问管理 SDK 日志。
10391	INFO	尝试在静态组下创建组	静态组 DN 组名	单击组创建页面中的“新建”按钮。	
10392	INFO	在静态组下创建组成功。	静态组 DN 组名	单击组创建页面中的“新建”按钮。	
10393	SEVERE	在静态组下创建组失败。	静态组 DN 组名错误消息	无法创建组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10394	SEVERE	在静态组下创建组失败。	静态组 DN 组名错误消息	由于访问管理 SDK 异常，无法创建组。	有关详细信息，请查阅访问管理 SDK 日志。
10401	INFO	尝试在可指定动态组下创建组	可指定动态组 DN 组名	单击组创建页面中的“新建”按钮。	
10402	INFO	在可指定动态组下创建组成功。	可指定动态组 DN 组名	单击组创建页面中的“新建”按钮。	
10403	SEVERE	在可指定动态组下创建组失败。	可指定动态组 DN 组名错误消息	无法创建组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10404	SEVERE	在可指定动态组下创建组失败。	可指定动态组 DN 组名错误消息	由于访问管理 SDK 异常，无法创建组。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10411	INFO	尝试修改组	组 DN	单击组配置文件页面中的“保存”按钮。	
10412	INFO	修改组成功。	组 DN	单击组配置文件页面中的“保存”按钮。	
10414	SEVERE	修改组失败。	可指定动态组 DN 组名错误消息	由于访问管理 SDK 异常，无法修改组。	有关详细信息，请查阅访问管理 SDK 日志。
10421	INFO	尝试在组中搜索用户	组 DN 搜索模式	查看组的用户页面。	
10422	INFO	在组中搜索用户成功。	组 DN 搜索模式	查看组的用户页面。	
10423	SEVERE	在组中搜索用户失败。	组 DN 搜索模式错误消息	无法搜索用户。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10424	SEVERE	在组中搜索用户失败。	组 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索用户。	有关详细信息，请查阅访问管理 SDK 日志。
10431	INFO	尝试获取嵌套组	组 DN	查看组的成员页面。	
10432	INFO	获取嵌套组成功。	组 DN	查看组的成员页面。	
10433	SEVERE	获取嵌套组失败。	组 DN 错误消息	无法获取嵌套组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10434	SEVERE	获取嵌套组失败。	组 DN 错误消息	由于访问管理 SDK 异常，无法获取嵌套组。	有关详细信息，请查阅访问管理 SDK 日志。
10441	INFO	尝试移除嵌套组	组 DN 嵌套组 *DN*	单击组的成员页面中的“移除”按钮。	
10442	INFO	移除嵌套组成功。	组 DN 嵌套组 *DN*	单击组的成员页面中的“移除”按钮。	
10443	SEVERE	移除嵌套组失败。	组 DN 嵌套组 *DN* 错误消息	无法移除嵌套组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10444	SEVERE	移除嵌套组失败。	组 DN 嵌套组 *DN* 错误消息	由于访问管理 SDK 异常，无法移除嵌套组。	有关详细信息，请查阅访问管理 SDK 日志。
10451	INFO	尝试从组中移除用户	组 DN 用户 *DN*	单击组的成员页面中的“移除”按钮。	
10452	INFO	从组中移除用户成功。	组 DN 用户 *DN*	单击组的成员页面中的“移除”按钮。	
10453	SEVERE	从组中移除用户失败。	组 DN 用户 *DN* 错误消息	无法移除用户。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10454	SEVERE	从组中移除用户失败。	组 DN 用户 *DN* 错误消息	由于访问管理 SDK 异常，无法移除用户。	有关详细信息，请查阅访问管理 SDK 日志。
10501	INFO	尝试在组织中搜索人员容器	组织 DN 搜索模式	查看组织的人员容器页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10502	INFO	在组织中搜索人员容器成功。	组织 DN 搜索模式	查看组织的人员容器页面。	
10503	SEVERE	在组织中搜索人员容器失败。	组织 DN 搜索模式错误消息	无法搜索人员容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10504	SEVERE	在组织中搜索人员容器失败。	组织 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索人员容器。	有关详细信息，请查阅访问管理 SDK 日志。
10511	INFO	尝试在容器中搜索人员容器	容器 DN 搜索模式	查看容器的人员容器页面。	
10512	INFO	在容器中搜索人员容器成功。	容器 DN 搜索模式	查看容器的人员容器页面。	
10513	SEVERE	在容器中搜索人员容器失败。	容器 DN 搜索模式错误消息	无法搜索人员容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10514	SEVERE	在容器中搜索人员容器失败。	容器 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索人员容器。	有关详细信息，请查阅访问管理 SDK 日志。
10521	INFO	尝试在人员容器中搜索人员容器	人员容器 DN 搜索模式	查看人员容器的人员容器页面。	
10522	INFO	在人员容器中搜索人员容器成功。	人员容器 DN 搜索模式	查看人员容器的人员容器页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10523	SEVERE	在人员容器中搜索人员容器失败。	人员容器 DN 搜索模式错误消息	无法搜索人员容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10524	SEVERE	在人员容器中搜索人员容器失败。	人员容器 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索人员容器。	有关详细信息，请查阅访问管理 SDK 日志。
10531	INFO	尝试在组织中创建人员容器	组织 DN 人员容器名	单击人员容器创建页面中的“新建”按钮。	
10532	INFO	在组织中创建人员容器成功。	组织 DN 人员容器名	单击人员容器创建页面中的“新建”按钮。	
10533	SEVERE	在组织中创建人员容器失败。	组织 DN 人员容器名错误消息	无法创建人员容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10534	SEVERE	在组织中创建人员容器失败。	组织 DN 人员容器名错误消息	由于访问管理 SDK 异常，无法创建人员容器。	有关详细信息，请查阅访问管理 SDK 日志。
10541	INFO	尝试在容器中创建人员容器	容器 DN 人员容器名	单击人员容器创建页面中的“新建”按钮。	
10542	INFO	在容器中创建人员容器成功。	容器 DN 人员容器名	单击人员容器创建页面中的“新建”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10543	SEVERE	在容器中创建人员容器失败。	容器 DN 人员容器名错误消息	无法创建人员容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10544	SEVERE	在容器中创建人员容器失败。	容器 DN 人员容器名错误消息	由于访问管理 SDK 异常，无法创建人员容器。	有关详细信息，请查阅访问管理 SDK 日志。
10551	INFO	尝试在人员容器中创建人员容器	人员容器 DN 人员容器名	单击人员容器创建页面中的“新建”按钮。	
10552	INFO	在人员容器中创建人员容器成功。	人员容器 DN 人员容器名	单击人员容器创建页面中的“新建”按钮。	
10553	SEVERE	在人员容器中创建人员容器失败。	人员容器 DN 人员容器名错误消息	无法创建人员容器。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10554	SEVERE	在人员容器中创建人员容器失败。	人员容器 DN 人员容器名错误消息	由于访问管理 SDK 异常，无法创建人员容器。	有关详细信息，请查阅访问管理 SDK 日志。
10601	INFO	尝试获取组织的指定服务	组织 DN	查看组织的服务配置文件页面。	
10602	INFO	获取组织的指定服务成功。	组织 DN	查看组织的服务配置文件页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10603	SEVERE	获取组织的指定服务失败。	组织 DN 错误消息	无法获取指定服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10604	SEVERE	获取组织的指定服务失败。	组织 DN 错误消息	由于访问管理 SDK 异常，无法获取指定服务。	有关详细信息，请查阅访问管理 SDK 日志。
10611	INFO	尝试从组织中移除服务	组织 DN 服务名	单击组织的服务配置文件页面中的“取消指定”按钮。	
10612	INFO	从组织中移除服务成功。	组织 DN 服务名	单击组织的服务配置文件页面中的“取消指定”按钮。	
10613	SEVERE	从组织中移除服务失败。	组织 DN 服务名错误消息	无法移除服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10614	SEVERE	从组织中移除服务失败。	组织 DN 服务名错误消息	由于访问管理 SDK 异常，无法移除服务。	有关详细信息，请查阅访问管理 SDK 日志。
10621	INFO	尝试在组织中搜索组织	组织 DN 搜索模式	查看组织的子组织页面。	
10622	INFO	在组织中搜索组织成功。	组织 DN 搜索模式	查看组织的子组织页面。	
10623	SEVERE	在组织中搜索组织失败。	组织 DN 搜索模式错误消息	无法搜索组织。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10624	SEVERE	在组织中搜索组织失败。	组织 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索组织。	有关详细信息，请查阅访问管理 SDK 日志。
10631	INFO	尝试修改组织	组织 DN	单击组织配置文件页面中的“保存”按钮。	
10632	INFO	修改组织成功。	组织 DN	单击组织配置文件页面中的“保存”按钮。	
10633	SEVERE	修改组织失败。	组织 DN 错误消息	无法修改组织。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10634	SEVERE	修改组织失败。	组织 DN 错误消息	由于访问管理 SDK 异常，无法修改组织。	有关详细信息，请查阅访问管理 SDK 日志。
10641	INFO	尝试在组织中创建组织	组织 DN 新组织名	单击组织创建页面中的“新建”按钮。	
10642	INFO	在组织中创建组织成功。	组织 DN 新组织名	单击组织创建页面中的“新建”按钮。	
10643	SEVERE	在组织中创建组织失败。	组织 DN 新组织名错误消息	无法创建组织。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10644	SEVERE	在组织中创建组织失败。	组织 DN 新组织名错误消息	由于访问管理 SDK 异常，无法创建组织。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10651	INFO	尝试获取组织的属性值	组织 DN	查看组织配置文件页面。	
10652	INFO	获取组织的属性值成功。	组织 DN	查看组织配置文件页面。	
10653	SEVERE	获取组织的属性值失败。	组织 DN 错误消息	无法获取组织的属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10654	SEVERE	获取组织的属性值失败。	组织 DN 错误消息	由于访问管理 SDK 异常，无法获取组织的属性值。	有关详细信息，请查阅访问管理 SDK 日志。
10661	INFO	尝试将服务添加到组织	组织 DN 服务名	单击组织的服务页面中的“指定”按钮。	
10662	INFO	将服务添加到组织成功。	组织 DN 服务名	单击组织的服务页面中的“指定”按钮。	
10663	SEVERE	将服务添加到组织失败。	组织 DN 服务名错误消息	无法将服务添加到组织。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10664	SEVERE	将服务添加到组织失败。	组织 DN 服务名错误消息	由于访问管理 SDK 异常，无法将服务添加到组织。	有关详细信息，请查阅访问管理 SDK 日志。
10701	INFO	尝试从角色中移除用户	角色 DN 用户名	单击角色的用户页面中的“移除”按钮。	
10702	INFO	从角色中移除用户成功。	角色 DN 用户名	单击角色的用户页面中的“移除”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10703	SEVERE	从角色中移除用户失败。	角色 DN 用户名错误消息	无法移除用户。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10704	SEVERE	从角色中移除用户失败。	角色 DN 用户名错误消息	由于访问管理 SDK 异常，无法移除用户。	有关详细信息，请查阅访问管理 SDK 日志。
10711	INFO	尝试获取角色的属性值	角色 DN	查看角色配置文件页面。	
10712	INFO	获取角色的属性值成功。	角色 DN	查看角色配置文件页面。	
10713	SEVERE	获取角色的属性值失败。	角色 DN 错误消息	无法获取属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10714	SEVERE	获取角色的属性值失败。	角色 DN 错误消息	由于访问管理 SDK 异常，无法获取属性值。	有关详细信息，请查阅访问管理 SDK 日志。
10721	INFO	尝试修改角色	角色 DN	单击角色配置文件页面中的“保存”按钮。	
10722	INFO	修改角色成功。	角色 DN	单击角色配置文件页面中的“保存”按钮。	
10723	SEVERE	修改角色失败。	角色 DN 错误消息	无法修改角色。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10724	SEVERE	修改角色失败。	角色 DN 错误消息	由于访问管理 SDK 异常，无法修改角色。	有关详细信息，请查阅访问管理 SDK 日志。
10731	INFO	尝试获取角色中的成员	角色 DN 搜索模式	查看角色的成员页面。	
10732	INFO	获取角色中的成员成功。	角色 DN 搜索模式	查看角色的成员页面。	
10733	SEVERE	获取角色中的成员失败。	角色 DN 搜索模式错误消息	无法获取成员。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10734	SEVERE	获取角色中的成员失败。	角色 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法获取成员。	有关详细信息，请查阅访问管理 SDK 日志。
10741	INFO	尝试获取组织中的角色	角色 DN 搜索模式	查看组织的角色页面。	
10742	INFO	获取组织中的角色成功。	角色 DN 搜索模式查看角色的成员页面。	查看组织的角色页面。	
10743	SEVERE	获取组织中的角色失败。	角色 DN 搜索模式错误消息	无法获取角色。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10744	SEVERE	获取组织中的角色失败。	角色 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法获取角色。	有关详细信息，请查阅访问管理 SDK 日志。
10751	INFO	尝试获取容器中的角色	角色 DN 搜索模式	查看容器的角色页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10752	INFO	获取容器中的角色成功。	角色 DN 搜索模式查看角色的成员页面。	查看容器的角色页面。	
10753	SEVERE	获取容器中的角色失败。	角色 DN 搜索模式错误消息	无法获取角色。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10754	SEVERE	获取容器中的角色失败。	角色 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法获取角色。	有关详细信息，请查阅访问管理 SDK 日志。
10761	INFO	尝试在容器中创建角色	容器 DN 角色名	单击角色创建页面中的“新建”按钮。	
10762	INFO	在容器中创建角色成功。	容器 DN 角色名	单击角色创建页面中的“新建”按钮。	
10763	SEVERE	在容器中创建角色失败。	容器 DN 角色名	无法创建角色。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10764	SEVERE	在容器中创建角色失败。	容器 DN 角色名错误消息	由于访问管理 SDK 异常，无法创建角色。	有关详细信息，请查阅访问管理 SDK 日志。
10771	INFO	尝试在组织中创建角色	组织 DN 角色名	单击角色创建页面中的“新建”按钮。	
10772	INFO	在组织中创建角色成功。	组织 DN 角色名	单击角色创建页面中的“新建”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10773	SEVERE	在组织中创建角色失败。	组织 DN 角色名	无法创建角色。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10774	SEVERE	在组织中创建角色失败。	组织 DN 角色名错误消息	由于访问管理 SDK 异常，无法创建角色。	有关详细信息，请查阅访问管理 SDK 日志。
10781	INFO	尝试获取角色中的指定服务	角色 DN	查看角色的服务页面。	
10782	INFO	获取角色中的指定服务成功。	角色 DN	查看角色的服务页面。	
10783	SEVERE	获取角色中的指定服务失败。	角色 DN 错误消息	无法获取角色中的服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10784	SEVERE	获取角色中的指定服务失败。	角色 DN 错误消息	由于访问管理 SDK 异常，无法获取角色中的服务。	有关详细信息，请查阅访问管理 SDK 日志。
10791	INFO	尝试从角色中移除服务	角色 DN 服务名	单击角色的服务页面中的“取消指定”按钮。	
10792	INFO	从角色中移除服务成功。	角色 DN 服务名	单击角色的服务页面中的“取消指定”按钮。	
10793	SEVERE	从角色中移除服务失败。	角色 DN 服务名错误消息	无法从角色中移除服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10794	SEVERE	从角色中移除服务失败。	角色 DN 服务名错误消息	由于访问管理 SDK 异常，无法从角色中移除服务。	有关详细信息，请查阅访问管理 SDK 日志。
10801	INFO	尝试将服务添加到角色	角色 DN 服务名	单击角色的服务页面中的“指定”按钮。	
10802	INFO	将服务添加到角色成功。	角色 DN 服务名	单击角色的服务页面中的“指定”按钮。	
10803	SEVERE	将服务添加到角色失败。	角色 DN 服务名错误消息	无法将服务添加到角色。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10804	SEVERE	将服务添加到角色失败。	角色 DN 服务名错误消息	由于访问管理 SDK 异常，无法将服务添加到角色。	有关详细信息，请查阅访问管理 SDK 日志。
10901	INFO	尝试获取用户的指定角色	用户 DN	查看用户的角色页面。	
10902	INFO	获取用户的指定角色成功。	用户 DN	查看用户的角色页面。	
10903	SEVERE	获取用户的指定角色失败。	用户 DN 错误消息	无法获取指定角色。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10904	SEVERE	获取用户的指定角色失败。	用户 DN 服务名错误消息	由于访问管理 SDK 异常，无法获取指定角色。	有关详细信息，请查阅访问管理 SDK 日志。
10911	INFO	尝试从用户中移除角色	用户 DN 角色 *DN*	单击用户的角色页面中的“删除”按钮。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10912	INFO	从用户中移除角色成功。	用户 DN 角色 *DN*	单击用户的角色页面中的“删除”按钮。	
10913	SEVERE	从用户中移除角色失败。	用户 DN 角色 *DN* 错误消息	无法移除角色。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10914	SEVERE	从用户中移除角色失败。	用户 DN 角色 *DN* 服务名错误消息	由于访问管理 SDK 异常，无法移除角色。	有关详细信息，请查阅访问管理 SDK 日志。
10921	INFO	尝试将角色添加到用户	用户 DN 角色 *DN*	单击用户的角色页面中的“添加”按钮。	
10922	INFO	将角色添加到用户成功。	用户 DN 角色 *DN*	单击用户的角色页面中的“添加”按钮。	
10923	SEVERE	将角色添加到用户失败。	用户 DN 角色 *DN* 错误消息	无法添加角色。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10924	SEVERE	将角色添加到用户失败。	用户 DN 角色 *DN* 服务名错误消息	由于访问管理 SDK 异常，无法添加角色。	有关详细信息，请查阅访问管理 SDK 日志。
10931	INFO	尝试获取用户的指定服务	用户 DN	查看用户的服务页面。	
10932	INFO	获取用户的指定服务成功。	用户 DN	查看用户的服务页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10933	SEVERE	获取用户的指定服务失败。	用户 DN 错误消息	无法获取服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10934	SEVERE	获取用户的指定服务失败。	用户 DN 错误消息	由于访问管理 SDK 异常，无法获取服务。	有关详细信息，请查阅访问管理 SDK 日志。
10941	INFO	尝试从用户中移除服务	用户 DN 服务名	单击用户的服务页面中的“移除”按钮。	
10942	INFO	从用户中移除服务成功。	用户 DN 服务名	单击用户的服务页面中的“移除”按钮。	
10943	SEVERE	从用户中移除服务失败。	用户 DN 服务名错误消息	无法移除服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10944	SEVERE	从用户中移除服务失败。	用户 DN 服务名错误消息	由于访问管理 SDK 异常，无法移除服务。	有关详细信息，请查阅访问管理 SDK 日志。
10951	INFO	尝试在组织中搜索用户	组织 DN 搜索模式	查看组织的用户页面。	
10952	INFO	在组织中搜索用户成功。	组织 DN 搜索模式	查看组织的用户页面。	
10953	SEVERE	在组织中搜索用户失败。	组织 DN 搜索模式错误消息	无法搜索用户。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10954	SEVERE	在组织中搜索用户失败。	组织 DN 搜索模式错误消息	由于访问管理 SDK 异常，无法搜索用户。	有关详细信息，请查阅访问管理 SDK 日志。
10961	INFO	尝试修改用户	用户 DN	单击用户概要文件页面中的“保存”按钮。	
10962	INFO	修改用户概要文件成功。	用户 DN	单击用户概要文件页面中的“保存”按钮。	
10963	SEVERE	修改用户概要文件失败。	用户 DN 错误消息	无法修改用户。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10964	SEVERE	修改用户概要文件失败。	用户 DN 错误消息	由于访问管理 SDK 异常，无法修改用户。	有关详细信息，请查阅访问管理 SDK 日志。
10971	INFO	尝试创建用户	人员容器 DN 用户名	单击用户创建页面中的“添加”按钮。	
10972	INFO	创建用户成功。	人员容器 DN 用户名	单击用户创建页面中的“添加”按钮。	
10973	SEVERE	创建用户失败。	人员容器 DN 用户名错误消息	无法创建用户。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10974	SEVERE	创建用户失败。	人员容器 DN 用户名错误消息	由于访问管理 SDK 异常，无法创建用户。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
10981	INFO	尝试获取用户的属性值	用户 DN	查看用户概要文件页面。	
10982	INFO	获取用户的属性值成功。	用户 DN	查看用户概要文件页面。	
10983	SEVERE	获取用户的属性值失败。	用户 DN 错误消息	无法获取属性值。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10984	SEVERE	获取用户的属性值失败。	用户 DN 错误消息	由于访问管理 SDK 异常，无法获取属性值。	有关详细信息，请查阅访问管理 SDK 日志。
10991	INFO	尝试将服务添加到用户	用户 DN 服务名	单击用户的服务页面中的“添加”按钮。	
10992	INFO	将服务添加到用户成功。	用户 DN 服务名	单击用户的服务页面中的“添加”按钮。	
10993	SEVERE	将服务添加到用户失败。	用户 DN 服务名错误消息	无法添加服务。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
10994	SEVERE	将服务添加到用户失败。	用户 DN 服务名错误消息	由于访问管理 SDK 异常，无法添加服务。	有关详细信息，请查阅访问管理 SDK 日志。
11001	INFO	尝试获取用户的指定组	用户 DN	查看用户的组页面。	
11002	INFO	获取用户的指定组成功。	用户 DN	查看用户的组页面。	

表 C–3 Access Manager 控制台的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
11003	SEVERE	获取用户的指定组失败。	用户 DN 错误消息	无法获取指定组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
11004	SEVERE	获取用户的指定组失败。	用户 DN 错误消息	由于访问管理 SDK 异常，无法获取指定组。	有关详细信息，请查阅访问管理 SDK 日志。
11011	INFO	尝试从用户中移除组	用户 DN 组 *DN*	单击用户的组页面中的“移除”按钮。	
11012	INFO	从用户中移除组成功。	用户 DN 组 *DN*	单击用户的组页面中的“移除”按钮。	
11013	SEVERE	从用户中移除组失败。	用户 DN 组 *DN* 错误消息	无法移除组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。
11014	SEVERE	从用户中移除组失败。	用户 DN 组 *DN* 错误消息	由于访问管理 SDK 异常，无法移除组。	有关详细信息，请查阅访问管理 SDK 日志。
11021	INFO	尝试将组添加到用户	用户 DN 组 *DN*	单击用户的组页面中的“添加”按钮。	
11022	INFO	将组添加到用户成功。	用户 DN 组 *DN*	单击用户的组页面中的“添加”按钮。	
11023	SEVERE	将组添加到用户失败。	用户 DN 组 *DN* 错误消息	无法添加组。这可能是用户的单点登录令牌已过期；或者用户没有权限执行此操作。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–3 Access Manager 控制台的日志参考　（续）

Id	日志级别	说明	数据	触发	操作
11024	SEVERE	将组添加到用户失败。	用户 DN 组 *DN* 错误消息	由于访问管理 SDK 异常，无法添加组。	有关详细信息，请查阅访问管理 SDK 日志。

表 C–4 联合的日志参考

Id	日志级别	说明	数据	触发	操作
1	INFO	验证域创建	验证域名	已创建验证域	
2	INFO	验证域删除	验证域名	已删除验证域	
3	INFO	修改验证域	验证域名	已修改验证域	
4	INFO	远程提供者创建	提供者 ID	已创建远程提供者	
5	INFO	托管提供者创建	提供者 ID	已创建托管提供者	
6	INFO	已删除联合提供者	联合提供者 ID	已删除联合提供者	
7	INFO	删除实体	实体 ID	已删除实体	
8	INFO	已删除提供者	提供者 ID	已删除提供者	
9	INFO	修改实体	实体 ID	已修改实体	
10	INFO	修改联合提供者	联合提供者 ID	已修改联合提供者	
11	INFO	修改提供者	提供者 ID	已修改提供者	
12	INFO	创建实体	实体 ID	已创建实体	
13	INFO	创建联合提供者	联合提供者 ID	已创建联合提供者	
14	INFO	写入帐户联合信息	用户 DN 联合信息密钥联合信息值	带有密钥的帐户联合信息已添加到用户	
15	INFO	移除帐户联合信息	用户 DN 提供者 *ID* 现有联合信息密钥	带有密钥的帐户联合信息已从用户中移除	
16	FINER	创建声明	声明 ID 或字符串	已创建声明	

表 C–4 联合的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
17	INFO	Liberty 未启用。	消息	Liberty 未启用。 无法处理请求。	请登录到管理控制台以启用管理控制台服务中的联合管理。
18	INFO	注销请求处理失败。	消息	注销请求处理失败	
19	INFO	终止请求处理失败	消息	终止请求处理失败	
20	INFO	无法创建 SOAP URL 端点。	SOAP 端点 URL	无法创建 SOAP URL 端点	
21	INFO	验证类型和协议（基于 SOAP URL）不匹配。	协议验证类型	验证类型和协议（基于 SOAP URL）不匹配。	
22	INFO	验证类型错误	验证类型	验证类型错误	
23	FINER	SAML SOAP 接收方 URL	soap url	SAML SOAP 接收方 URL	
24	INFO	SOAP 响应无效	消息	SOAP 响应无效。	
25	INFO	声明无效	消息	此声明无效	
26	INFO	单点登录失败	消息	单点登录失败	
27	INFO	授予权限后重定向到 URL。	重定向 URL	授予权限后重定向到 URL。	
28	INFO	缺少验证响应	消息	未找到验证响应	
29	INFO	帐户联合失败	消息	帐户联合失败	
30	INFO	SSO 令牌生成失败	消息	无法生成 SSO 令牌	
31	INFO	验证响应无效	验证响应无效	验证响应无效	
32	INFO	验证请求处理失败	消息	验证请求处理失败。	
33	INFO	签名验证失败。	消息	签名验证失败。	

表 C–4 联合的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
34	FINER	已创建 SAML 响应	SAML 响应	已创建 SAML 响应	
35	FINER	重定向 URL	重定向 URL	重定向到 :	
36	INFO	未找到公共域服务信息	消息	未找到公共域服务信息。	
37	INFO	提供者不被信赖	提供者 ID	提供者不被信赖。	
38	INFO	验证请求无效	消息	验证请求无效	
39	INFO	未找到用户的帐户联合信息	用户名	未找到用户的帐户联合信息 :	
40	INFO	找不到用户。	用户名	找不到用户。	
41	INFO	不支持注销配置文件。	注销配置文件	不支持注销配置文件。	验证元数据是否正确。
42	INFO	注销成功。	用户名	注销成功。	
43	INFO	由于错误的 URL 导致注销无法重定向。	消息	由于错误的 URL 导致注销无法重定向。	
44	INFO	注销请求格式不正确。	用户名	注销请求格式不正确。	
45	INFO	未能获取 Pre/Logout 处理程序。	注销 URL	未能获取 Pre/Logout 处理程序。	
46	INFO	单一注销失败。	用户名	单一注销失败。	
47	INFO	无法创建 SPProvidedNameIdentifier。	消息	无法创建 SPProvidedNameIdentifier。	
48	INFO	签名无效。	消息	签名无效。	
49	INFO	联合终止失败。	用户名	联合终止失败。 无法更新帐户。	
50	FINER	联合终止成功。	用户 DN	联合终止成功。 用户帐户已更新。	
51	INFO	响应无效	SAML 响应	SAML 响应无效。	
52	INFO	提供者注册无效。	提供者 ID	提供者无效。	

表 C–5 Liberty的日志参考

Id	日志级别	说明	数据	触发	操作
1	INFO	无法处理 SASL 请求	消息 ID 验证机制验证 *ID* 建议验证 *ID*	无法处理 SASL 请求。	
2	INFO	SASL 响应正常	消息 ID 验证机制验证 *ID* 建议验证 *ID*	SASL 响应正常。	
3	INFO	返回 SASL 验证响应	消息 ID 验证机制验证 *ID* 建议验证 *ID*	已返回 SASL 响应，继续验证。	
4	INFO	未在数据存储库中找到用户	用户名	未在数据存储库中找到用户	
5	INFO	已在数据存储库中找到用户	用户名	已在数据存储库中找到用户	
6	INFO	无法从资源 ID 找到用户	资源 ID	无法从资源 ID 找到用户	
7	INFO	已成功更新用户概要文件	用户名	已成功更新用户概要文件	
8	INFO	未授权。无法查询个人配置文件服务	资源 ID	无法查询个人配置文件服务	
9	INFO	交互式操作失败	资源 ID	与个人配置文件服务的交互失败	
10	INFO	已成功查询 PP 服务	资源 ID	个人配置文件服务查询成功	
11	INFO	修改失败	资源 ID	无法修改个人配置文件服务	
12	INFO	修改成功	资源 ID	个人配置文件服务修改成功。	
13	INFO	交互式操作成功	交互式操作成功消息	与个人配置文件服务交互成功	
14	INFO	正在发送消息	请求消息 ID	正向 WSP 发送 SOAP 请求消息。	

表 C–5 Liberty的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
15	INFO	正在返回响应消息	响应消息 ID 请求消息 *ID*	正在返回 SOAP 请求的响应消息。	
16	INFO	正在重新发送消息	消息 ID	正向 WSP 重新发送 SOAP 请求消息	
17	INFO	交互式管理器正在将用户代理重定向到交互式服务	请求消息 ID	交互式管理器正在将用户代理重定向到交互式服务	
18	INFO	交互式管理器正在返回响应元素	消息 ID 参考消息 *ID* 高速缓存条目状态	交互式管理器正在返回响应元素	
19	INFO	已向用户代理提交交互式查询	消息 ID	已向用户代理提交交互式查询	
20	INFO	用户代理已响应交互式查询	消息 ID	用户代理已响应交互式查询	
21	INFO	用户代理已重定向至 SP	消息 ID	用户代理已重定向至 SP	
22	INFO	Web 服务成功	消息 ID 处理程序密钥	Web 服务成功。	
23	INFO	Web 服务失败	错误消息	Web 服务失败。	

表 C–6 策略的日志参考

Id	日志级别	说明	数据	触发	操作
1	INFO	评估策略成功	策略名领域名服务类型名称资源名操作名策略决策	正在评估策略。	
2	INFO	获取受保护的策略资源成功	负责人名称资源名保护策略	正在获取受保护的策略资源。	
3	INFO	在领域中创建策略成功	策略名领域名	正在领域中创建策略。	

表 C–6 策略的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
4	INFO	修改领域中的策略成功。	策略名领域名	正在修改领域中的策略。	
5	INFO	从领域中移除策略成功	策略名领域名	正在从领域中移除策略。	
6	INFO	策略已存在于领域中	策略名领域名	正在领域中创建策略。	
7	INFO	在领域中创建策略失败	策略名领域名	正在领域中创建策略。	请检查用户是否有在领域中创建策略的权限。
8	INFO	替换领域中的策略失败	策略名领域名	正在替换领域中的策略。	请检查用户是否有替换领域中策略的权限。
81	INFO	未替换策略 - 领域中已经存在具有此新名称的其他策略	新的策略名领域名	正在替换领域中的策略	
9	INFO	从领域中移除策略失败	策略名领域名	正在从领域中移除策略。	请检查用户是否有从领域中移除策略的权限。
10	INFO	管理员计算策略决策成功	管理员名称负责人名称资源名策略决策	管理员正在计算策略决策。	
11	INFO	管理员计算忽略主题的策略决策成功	管理员名称资源名策略决策	管理员正在计算忽略主题的策略决策。	

表 C–7 SAML的日志参考

Id	日志级别	说明	数据	触发	操作
1	INFO	已创建新声明	消息 ID 当日志级别为 *LL_FINER* 时的声明 *ID* 或声明	浏览器附件配置文件浏览器 *POST* 配置文件创建声明辅件验证查询属性查询验证决策查询	

表 C–7 SAML的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
2	INFO	已创建新的声明辅件	消息 ID 声明辅件与辅件对应的声明 *ID*	浏览器附件配置文件创建声明辅件	
3	FINE	已从映射中移除声明辅件	消息 ID 声明辅件	SAML 辅件查询声明辅件过期	
4	FINE	已从映射中移除声明	消息 ID 声明 *ID*	SAML 辅件查询声明过期	
5	INFO	已验证声明辅件的访问权限	消息 ID 声明辅件	SAML 辅件查询	
6	INFO	已配置的验证类型和实际的 SOAP 协议不匹配。	消息 ID	SAML SOAP 查询	请登录到控制台，转到“联合”，然后转到“SAML”，编辑“可信赖伙伴配置”，检查选中的“验证类型”字段，确保与 SOAP URL 字段中指定的协议相匹配。
7	INFO	验证类型无效	消息 ID	SAML SOAP 查询	请登录到控制台，转到“联合”，然后转到“SAML”，编辑“可信赖伙伴配置”，选择“验证类型”字段的其中一个值，然后保存。
8	FINE	远程 SOAP 接收方 URL	消息 ID *SOAP* 接收方 *URL*	SAML SOAP 查询	
9	INFO	SAML 响应中没有声明	消息 ID *SAML* 响应	SAML 辅件查询	如有错误，请联系远程伙伴
10	INFO	SAML 响应中的声明数目不等于 SAML 请求中的辅件数目。	消息 ID *SAML* 响应	SAML 辅件查询	如有错误，请联系远程伙伴
11	INFO	要发送到远程伙伴的辅件	消息 ID *SAML* 辅件	SAML 辅件查询	

表 C–7 SAML的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
12	INFO	可信赖伙伴配置中的 SOAP URL 错误	消息 ID	SAML 辅件查询	请登录到控制台，转到“联合”，然后转到“SAML”，编辑“可信赖伙伴配置”，输入 SOAP URL 字段的值，然后保存。
13	FINE	SAML 辅件查询 SOAP 请求	消息 ID *SAML* 辅件查询消息	SAML 辅件查询	
14	INFO	没有来自远程 SAML SOAP 接收方的回复	消息 ID	SAML 辅件查询	如有错误，请向远程伙伴核实
15	FINE	SAML 辅件查询响应	消息 ID *SAML* 辅件查询响应消息	SAML 辅件查询	
16	INFO	SOAP 响应中没有 SAML 响应	消息 ID	SAML 辅件查询	如有错误，请向远程伙伴核实
17	INFO	SAML 响应的 XML 签名无效	消息 ID	SAML 辅件查询	如有关于 XML 数字签名的错误，请向远程伙伴核实
18	INFO	获取 SAML 响应状态代码时出错	消息 ID	SAML 辅件查询	如有关于响应状态代码的错误，请向远程伙伴核实
19	INFO	请求中缺少 TARGET 参数	消息 ID	SAML 辅件配置文件*SAML POST* 配置文件	请在请求中将“TARGET=target_url”作为查询参数添加
20	INFO	SAML 辅件源站点中的重定向 URL	消息 ID 目标重定向 *URL* 当 *POST* 配置文件和日志级别为 *LL_FINER* 时的 *SAML* 响应消息	SAML 辅件配置文件源*SAML POST* 配置文件源	
21	INFO	禁止访问指定的目标站点	消息 ID 目标 *URL*	SAML 辅件配置文件源*SAML POST* 配置文件源	任何可信赖伙伴都不能处理请求中指定的 TARGET URL，请检查 TARGET URL，确保与可信赖伙伴站点中配置的目标 URL 之一相匹配

表 C–7 SAML的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
22	INFO	无法创建单点登录令牌	消息 ID	SAML 辅件配置文件目标*SAML POST* 配置文件目标	验证组件无法创建 SSO 令牌，有关详细信息，请检查验证日志和调试
23	INFO	单点登录成功，已批准访问目标的权限	消息 ID 当 *POST* 配置文件和日志级别为 *LL_FINER* 或更高时的响应消息	SAML 辅件配置文件目标*SAML POST* 配置文件目标	
24	INFO	servlet 请求或响应为空	消息 ID	SAML 辅件配置文件*SAML POST* 配置文件	有关详细信息，请检查 Web 容器错误日志
25	INFO	POST 主体中缺少 SAML 响应	消息 ID	SAML POST 配置文件目标	请向远程 SAML 伙伴核实，以查看 HTTP POST 主体中缺少 SAML 响应对象的原因
26	INFO	响应消息出错	消息 ID	SAML POST 配置文件目标	无法将已编码的 POST 主体属性转换为 SAML 响应对象，请向远程 SAML 伙伴核实，以查看 SAML 响应创建是否存在错误，例如，编码错误、响应子元素无效等
27	INFO	响应无效	消息 ID	SAML POST 配置文件目标	SAML 响应中的收件人属性与此站点的 POST 配置文件 URL 不匹配响应状态代码为 *NOT SUCCESS*
28	INFO	无法获得消息工厂的实例	消息 ID	SAML SOAP 接收方初始化	请检查 SOAP 工厂属性 (javax.xml.soap.MessageFactory)，以确保使用的是有效的 SOAP 工厂实现

表 C–7 SAML的日志参考 （续）

Id	日志级别	说明	数据	触发	操作
29	INFO	接收到来自不可信站点的请求	消息 ID 远程站点主机名或 *IP* 地址	SAML SOAP 查询	请登录到控制台，转到“联合”，然后转到“SAML”服务，编辑“可信赖伙伴配置”，检查“主机列表”字段，确保远程主机/IP 地址的值是其中之一。 如果是带有客户机验证的 SSL，请确保“主机列表”包含远程站点的客户机证书别名。
30	INFO	来自远程伙伴站点的请求无效	消息 ID 和请求主机名/IP 地址返回响应	SAML SOAP 查询	请向远程伙伴站点的管理员核实
31	FINE	来自伙伴站点的请求消息	消息 ID 和请求主机名/IP 地址请求 *XML*	SAML SOAP 查询	
32	INFO	由于内部服务器错误，无法生成响应	消息 ID	SAML SOAP 查询	请检查调试消息以查看失败的原因，例如，无法创建响应状态、主要/次要版本错误等
33	INFO	正在向伙伴站点发送 SAML 响应	消息 ID *SAML* 响应或响应 *ID*	SAML SOAP 查询	
32	INFO	无法生成 SOAP 故障响应主体	消息 ID	SAML SOAP 查询	请检查调试消息以查看失败的原因，例如，无法创建 SOAP 故障等。

表 C–8 会话的日志参考

Id	日志级别	说明	数据	触发	操作
1	INFO	会话已创建	用户 ID	用户已验证。	
2	INFO	会话有空闲超时	用户 ID	用户会话已长时间空闲。	
3	INFO	会话已过期	用户 ID	用户会话已达到其最大时间限制。	
4	INFO	用户已注销	用户 ID	用户已从系统注销。	

表 C–8 会话的日志参考　（续）

Id	日志级别	说明	数据	触发	操作
5	INFO	会话已重新激活	用户 ID	用户会话状态为活动。	
6	INFO	会话已破坏	用户 ID	用户会话已破坏且不能引用。	
7	INFO	会话的属性已更改。	用户 ID	用户已更改会话的不受保护的属性。	
8	INFO	会话收到未知事件	用户 ID	未知会话事件	
9	INFO	尝试设置受保护的属性	用户 ID	尝试设置受保护的属性	
10	INFO	用户的会话配额已用尽。	用户 ID	会话配额已用尽	
11	INFO	用于会话故障转移和会话约束的会话数据库不可用。	用户 ID	无法连接会话数据库。	
12	INFO	会话数据库重新联机。	用户 ID	会话数据库重新联机。	
13	INFO	AM 服务器上托管的有效会话总数已达到最大限制。	用户 ID	已达到会话最大限制。	

◆ ◆ ◆ 附 录 D

错误代码

本附录提供一个由 Access Manager 生成的错误消息列表。此列表并不全面，但本章提供的信息可作为解决一般问题的良好开端。本附录中列出的表格提供了错误代码、错误说明和/或可能的原因，并介绍了为解决所遇到的问题可以采取的操作。

本附录列出了以下功能方面的错误代码：

如果在诊断错误时需要更多帮助，请与 Sun 技术支持联系：

http://www.sun.com/service/sunone/software/index.html

Access Manager 控制台错误

下表描述由 Access Manager 控制台生成并显示的错误代码。

表 D–1 Access Manager 控制台错误

错误消息	说明/可能的原因	操作
删除下列对象时出错：	当前用户移除该对象之前，该对象可能已被其他用户移除。	重新显示正试图删除的对象，然后再次尝试删除操作。
您输入的 URL 无效	如果在 Access Manager 控制台窗口输入的 URL 不正确，则显示上述消息。	
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的任何对象都不匹配。	输入另一组参数，然后再次运行搜索

表 D–1 Access Manager 控制台错误 （续）

错误消息	说明/可能的原因	操作
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。	
没有为此服务显示的信息。	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	
超出搜索范围限制。请改进搜索。	搜索中指定的参数所返回的条目数超过了允许返回的条目数	将“管理”服务中的“搜索返回的结果的最大数目”属性修改为一个更大的值。您也可以修改搜索参数以加强限制。
已超出搜索时间限制。请改进搜索。	指定参数的搜索所耗费的时间已超出允许的范围。	将“管理”服务中的“搜索的超时时间”属性修改为一个更大的值。您也可以修改搜索参数，使其放宽限制，以返回更多的值。
用户的起始位置无效。请联系您的管理员。	用户条目中的起始位置 DN 已无效	在“用户概要文件”页面中，将起始 DN 的值更改为有效 DN。
不能建立身份对象。用户没有足够的访问权限。	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 D–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。	请注销，或通过 Access Manager 控制台设置登录成功重定向 URL。使用以“管理控制台 URL”作为参数值的“goto”查询参数。
logout.failure.	用户不能注销 Access Manager。	重新启动服务器。
uncaught_exception	由于不正确的处理程序而抛出验证异常	检查登录 URL 是否包含无效或特殊字符。
redirect.error	Access Manager 不能转向成功或失败重定向 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。	

表 D–2 验证错误代码 （续）

错误消息	说明/可能的原因	操作
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。这是显示在默认登录失败模板中的一般错误消息。最常见的原因是凭证无效/不正确。	输入有效并正确的用户名/密码（被调用的验证模块所需要的证书。）
nouser.profile	在给定组织中未找到匹配输入的用户名的用户概要文件。登录到成员资格/自注册验证模块时，可能显示此错误。	请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够。登录到成员资格/自注册验证模块时，可能显示此错误。	默认情况下，登录密码必须包含至少 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。
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	缺少确认密码字段。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	密码和确认密码不匹配。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。
存储用户概要文件时出错。	存储用户概要文件时出错。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` 文件里自注册的属性和元素是有效和正确的。
orginactive	此组织未激活。	将组织的状态从**不活动**转变到**活动**，通过 Access Manager 控制台激活该组织。
internal.auth.error	内部验证错误。这是一个通用验证错误，可能是由不同和多个环境和/或配置问题所导致。	

表 D–2 验证错误代码 （续）

错误消息	说明/可能的原因	操作
usernot.active	用户已不处于活动状态。	将用户的状态从**不活动**转变到**活动**，通过 Admin 控制台激活该用户。 如果用户已通过“内存锁定”被封锁，请重新启动服务器。
user.not.inrole	用户不属于指定的角色。进行基于角色的验证时显示此错误。	确保登录用户属于为基于角色的验证指定的角色。
session.timeout	用户会话已超时。	请重新登录。
authmodule.denied	指定的验证模块被拒绝。	确保必需的验证模块在必需的组织下注册，并为该模块创建和保存模板，还要在“核心验证”模块的“组织验证模块”列表中选择该模块。
noconfig.found	未找到任何配置。	检查验证配置服务以查找必需的验证方法。
cookie.notpersistent	持久 Cookie 用户名在持久 Cookie 域中不存在。	
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概要文件。	确保用户在本地 Directory Server 中的指定的组织中存在并且有效。
reqfield.missing	未完成某一必需字段。请确保在所有必需字段中均输入值。	确保在所有必需字段中均输入值。
session.max.limit	达到最大会话数限制。	注销，然后再次登录。

策略错误代码

下表描述由策略框架生成的并在 Access Manager 控制台中显示的错误代码。

表 D–3 策略错误代码

错误消息	说明/可能的原因	操作
illegal_character_/_in_name	策略名称中含有非法字符“/”。	确保策略名称中不包含“/”字符。
policy_already_exists_in_org	具有相同名称的规则已存在。	使用其他名称创建策略。
rule_name_already_present	同名的另一个规则已经存在	使用其他规则名称创建策略。
rule_already_present	具有相同规则值的规则已存在。	使用其他规则值。

表 D–3 策略错误代码 （续）

错误消息	说明/可能的原因	操作
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。	请更改搜索控制参数中的搜索模式或组织的策略配置。“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。	请更改搜索控制参数中的搜索模式或组织的策略配置。“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。	该插件的属性值应该是整数。
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	用户没有足够的访问权限。用户不具有执行策略操作的足够权限。	具有相应访问权限的用户才能执行策略操作。
invalid_ldap_server_host	LDAP 服务器主机无效。	更改在策略配置服务中输入的无效 LDAP 服务器主机。

amadmin 错误代码

下表描述由 amadmin 命令行工具为 Access Manager 的调试文件生成的错误代码。

表 D–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必需参数（--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	缺少 --runasdn 值的用户 DN。	提供 --runasdn 值的用户 DN。
noservicename	4	缺少 --deletservice 值的服务名称。	提供 --deleteservice 值的服务名称。
nopwdforadmin	5	缺少 --password 值的密码。	提供 --password 值的密码。
nolocalename	6	未提供语言环境名称。默认语言环境为 en_US。	参见联机帮助里的语言环境列表。
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。要获得一组有效的参数，键入 amadmin --help。
oprfailed	9	操作失败。	当 amadmin 失败时，会产生更明确的错误代码指明特定错误。请参考这些错误代码来评估问题。
execfailed	10	无法处理请求。	当 amadmin 失败时，会产生更明确的错误代码指明特定错误。请参考这些错误代码来评估问题。
policycreatexception	12	无法创建策略。	amadmin 产生异常消息以指示特定错误。请参考这些消息来评估问题。
policydelexception	13	无法删除策略。	amadmin 产生异常消息以指示特定错误。请参考这些消息来评估问题。
smsdelexception	14	无法删除服务。	amadmin 产生异常消息以指示特定错误。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 格式正确且遵守 amAdmin.dtd。

表 D–4 amadmin 错误代码 （续）

错误消息	代码	说明/可能的原因	操作
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 格式正确且遵守 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 产生异常消息以指示特定错误。请参考这些消息来评估问题。
ioexception	19	无法读取输入 XML 文件。	amadmin 产生异常消息以指示特定错误。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 产生异常消息以指示特定错误。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 产生异常消息以指示特定错误。请参考这些消息来评估问题。
failedToProcessXML	23	无法处理 XML 文件。	amadmin 产生异常消息以指示特定错误。请参考这些消息来评估问题。
nodataschemawarning	24	--data 或 --schema 选项都不在命令中。	检查是否所有变量均有效。要获得一组有效的参数，键入 amadmin --help。
doctyperror	25	XML 文件不符合正确的 DTD。	查看 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。
statusmsg13	28	服务管理器异常（SSO 异常）。	amadmin 产生异常消息以指示特定错误。请参考这些消息来评估问题。
statusmsg14	29	服务管理器异常。	amadmin 产生异常消息以指示特定错误。请参考这些消息来评估问题。
statusmsg15	30	模式文件输入流异常。	amadmin 产生异常消息以指示特定错误。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 产生异常消息以指示特定错误。请参考这些消息来评估问题。
statusmsg31	32	策略管理器异常。	amadmin 产生异常消息以指示特定错误。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 产生异常消息以指示特定错误。请参考这些消息来评估问题。

表 D–4 amadmin 错误代码 （续）

错误消息	代码	说明/可能的原因	操作
levelerr	36	属性值无效。	检查为 LDAP 搜索设置的级别。应该是 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。
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。
cannotAdduUersToDynamic-Group	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。
cannotCreatePolicyUnder-Container	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。
defaultGroupContainer-NotFound	51	未找到组容器。	创建父组织或容器的组容器。
cannotRemoveUserFrom-FilteredRole	52	无法从过滤的角色中移除用户。	确保 XML 文件中的角色 DN 不是过滤的角色。
cannotRemoveUsersFrom-DynamicGroup	53	无法从动态组中移除用户。	确保 XML 文件中的组 DN 不是动态组。

表 D–4 amadmin 错误代码 （续）

错误消息	代码	说明/可能的原因	操作
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。
defaultPeopleContainer-NotFound	59	您正尝试向组织或容器添加用户。而组织或容器中不存在默认人员容器。	请确保存在默认人员容器。
nodefaulturlprefix	60	在 --defaultURLPrefix 参数后未找到默认 URL 前缀	请相应提供默认的 URL 前缀。
nometaalias	61	在 --metaalias 参数后未找到元数据别名	请相应提供元数据别名。
missingEntityName	62	未指定实体名称。	请提供实体名称。
missingLibertyMetaInputFile	63	缺少用于导入元数据的文件名。	请提供包含元数据的文件名。
missingLibertyMetaOutputFile	64	缺少用于存储导出的元数据的文件名。	请提供用于存储元数据的文件名。
cannotObtainMetaHandler	65	无法获得元数据属性的处理程序。指定的用户名和密码可能不正确。	确保用户名和密码正确。
missingResourceBundleName	66	添加、查看或删除存储在目录服务器中的资源包时，缺少资源包名称。	请提供资源包名称
missingResourceFileName	67	向目录服务器中添加资源包时，缺少包含资源字符串的文件的文件名。	请提供有效文件名。
failLoadLibertyMeta	68	无法将 Liberty 元数据加载到 Directory Server。	再次加载元数据之前，请重新检查元数据。

索引

重

主

状

组