Sun Java System Delegated Administrator 6.4 管理指南

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

文件号码 820–0521
2007 年 3 月

070521@17466

目录

表

图

前言

本指南介绍了如何配置和管理 Sun™ Java System Delegated Administrator。同时还介绍了 Delegated Administrator 命令，并提供了语法和示例。

Delegated Administrator 由一个控制台（图形用户界面）和一组命令行工具组成，它们用于使用 Sun Java System Access Manager 为 Sun Java System Messaging Server 和 Sun Java System Calendar Server 置备用户、组、域和资源。

目标读者

本书适用于负责在站点上管理、配置和部署 Delegated Administrator 的人员。

阅读本书之前

本书假定您负责管理此软件并且对以下内容有大致的了解：

- Internet 和万维网
- Messaging Server 协议
- Sun Java System Administration Server
- Sun Java System Directory Server 和 LDAP
- Sun Java System 控制台
- 以下平台上的系统管理和联网：
  - 用于 SPARC 和 x86 的 Solaris 10
  - 用于 SPARC 和 x86 的 Solaris 9
  - Red Hat Enterprise Linux 4.0 或任何 RHEL 4 更新
  - Red Hat Enterprise Linux 3.0 或任何 RHEL 3 更新

  常规部署体系结构

本书的结构

下表概要介绍了本书的内容。

表 P–1 本书的结构

章	说明
第 1 章	介绍了 Delegated Administrator 提供的目录组织、管理员角色和服务包。
第 2 章	介绍了安装和配置 Sun Java System Delegated Administrator 所需的步骤。
第 3 章	逐步介绍 Delegated Administrator 配置程序。
第 4 章	介绍了如何自定义 Delegated Administrator—例如，更改控制台的外观。
第 5 章	介绍了 `commadmin` 实用程序，并提供了语法和示例。
附录 A	介绍了服务提供商管理员角色以及由服务提供商管理员管理的供应商组织和业务组织。
附录 B	列出了特定命令行选项的属性值和时区值。
附录 C	列出了一些日志文件，可以检查这些文件来调试 Delegated Administrator。
附录 D	提供了针对 Delegated Administrator、Web 容器和 Directory Server 的调节技巧，用以提高 Delegated Administrator 的性能。
附录 E	介绍了如何在目录中合并 ACI 和删除未使用的 ACI 。

Communications Suite 文档集

可以通过 `http://docs.sun.com`SM 站点联机访问 Sun 技术文档。可以浏览文件集或查找某个特定的书名或主题。

Messaging Server 文档

可使用以下 URL 查看所有 Messaging Server 文档：

`http://docs.sun.com/coll/1312.1` 和 `http://docs.sun.com/coll/1392.1`

可以获取以下文档：

- Sun Java System Messaging Server 管理指南

- Sun Java System Messaging Server Administration Reference
- Sun Java System Messaging Server MTA Developer's Reference

Messaging Server 产品套件包含其他产品，例如 Sun Java™ System Directory Server。可以在以下 URL 中找到这些产品及其他产品的文档：

http://docs.sun.com/db/prod/sunone

除了软件文档之外，还可以查看 Messaging Server 软件论坛，以获取有关特定 Messaging Server 产品问题的技术帮助。可以在以下 URL 中找到该论坛：

http://swforum.sun.com/jive/forum.jsp?forum=15

Calendar Server 文档

可以使用以下 URL 查看所有 Calendar Server 文档：

http://docs.sun.com/coll/1313.1 和 http://docs.sun.com/coll/1387.1

可以获取以下文档：

- Sun Java System Calendar Server 管理指南
- Sun Java System Calendar Server Developer's Guide

Communications Suite 文档

可使用以下 URL 之一查看适用于所有 Communications Suite 产品的文档：

http://docs.sun.com/coll/1312.1 和 http://docs.sun.com/coll/1392.1

或者

http://docs.sun.com/coll/1313.1 和 http://docs.sun.com/coll/1387.1

可以获取以下文档：

- Sun Java Communications Suite Installation Guide
- Sun Java Communications Suite Upgrade Guide
- Sun Java Communications Suite 发行说明
- Sun Java System Delegated Administrator Administration Guide
- Sun Java Communications Suite Deployment Planning Guide
- Sun Java Communications Suite Schema Migration Guide
- Sun Java Communications Suite Schema Reference
- Sun Java Communications Suite Event Notification Service Guide
- Sun Java System Communications Express 管理指南
- Sun Java System Communications Express Customization Guide

默认的路径和文件名

下表介绍了本书中使用的默认路径和文件名。

表 P–2 默认的路径和文件名

占位符	说明	默认值
msg-svr-base	表示 Messaging Server 的基本安装目录。	Solaris 系统：`/opt/SUNWmsgsr` Linux 系统：`/opt/sun/messaging`
da-base	表示 Delegated Administrator 的基本安装目录。	Solaris 系统：`/opt/SUNWcomm` Linux 系统：`/opt/sun/comms/commcli`

印刷约定

下表介绍了本书中使用的印刷约定。

表 P–3 印刷约定

字体	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	保留未译的新词或术语以及要强调的词。要使用实名或值替换的命令行变量。	用于删除文件的命令是 `rm` *filename*。
新词术语强调	新词或术语以及要强调的词。	**高速缓存**是存储在本地的副本。 请**勿**保存文件。
《书名》	书名	请阅读用户指南中的第 6 章。

命令示例中的 shell 提示符

以下表格显示默认的系统提示符和超级用户提示符。

表 P–4 shell 提示符

shell	提示符
UNIX 和 Linux 系统上的 C shell	`machine_name%`
UNIX 和 Linux 系统上的 C shell 超级用户	`machine_name#`
UNIX 和 Linux 系统上的 Bourne shell 和 Korn shell	`$`
UNIX 和 Linux 系统上的 Bourne shell 和 Korn shell 超级用户	`#`
Microsoft Windows 命令行	`C:\`

符号约定

以下表格说明了本书中可能使用的符号。

表 P–5 符号约定

符号	说明	示例	含义
`[ ]`	包含可选的参数和命令选项。	`ls [-l]`	`-l` 选项不是必需的。
`{ | }`	包含所需命令选项的一组选择。	`-d {y|n}`	`-d` 选项要求使用 `y` 参数或 `n` 参数。
`${ }`	指示变量引用。	`${com.sun.javaRoot}`	引用变量 `com.sun.javaRoot` 的值。
-	将同时使用的多个键击连接在一起。	Ctrl-A	按下 Ctrl 键的同时按下 A 键。
+	将连续的多个键击连接在一起。	Ctrl+A+N	按下 Ctrl 键，释放它，然后再按下后面的键。
→	指示图形用户界面中的菜单项选择。	文件 → 新建 → 模板	从“文件”菜单中，选择“新建”。 从“新建”子菜单中，选择“模板”。

文档、支持和培训

Sun Web 站点提供关于以下附加资源的信息：

- 文档 (http://www.sun.com/documentation/)
- 支持 (http://www.sun.com/support/)
- 培训 (http://www.sun.com/training/)

第三方 Web 站点引用

本文档引用了第三方 URL 以提供其他相关信息。

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

Sun 欢迎您提出意见

Sun 致力于提高其文档的质量，并十分乐意收到您的意见和建议。要分享您的意见，请转至 http://docs.sun.com，然后单击“发送意见”。在联机表单中，请提供完整文档标题和文件号码。文件号码是 7 位或 9 位数字，您可以在本书的标题页或文档的 URL 中找到文件号码。例如，本书的文件号码是 820-0521。本书的标题为《Sun Java System Delegated Administrator 6.4 管理指南》。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 819-4438-10，文件标题为《Sun Java System Delegated Administrator 6.4 Administration Guide》。

◆ ◆ ◆ 第 1 章

1 Delegated Administrator 概述

Communications Suite Delegated Administrator 实用程序和控制台允许您在 Communications Suite 应用程序（例如 Messaging Server 和 Calendar Server）使用的 LDAP 目录中置备用户、组、域和资源。

本章介绍了以下主题：

Delegated Administrator 简介

使用 Delegated Administrator，您可以向有权管理 LDAP 目录中的指定组织的低级别管理员分配置备任务。委托用户进行管理这一功能具有以下优点：

- 使多个管理员共同分担可能较费时的置备大型目录的责任。对于包含成千上万个用户的目录，可以让数十或数百个管理员来管理其中的各个组织。
- 使您可以在目录结构中创建一些组织并将它们作为明确的（或独特的）单元来管理和置备。这些组织包含的用户可以是与客户业务有关的人员，也可以是公司各个部门或其他团体的成员。

Delegated Administrator 提供了两个界面，用于在目录中置备用户和组织：

下面几节对这两个界面进行了概括介绍。

Delegated Administrator 置备目录以支持 Messaging Server 和 Calendar Server。

另外，如果 Sun Java System Instant Messaging (IM) 部署在您的站点上，那么在 Delegated Administrator 中创建的用户可以访问 IM 服务。用户创建期间，会自动为用户指定基本的 IM 服务。

必须使用 Access Manager 控制台设置和管理 IM 用户访问级别。在本发行版中，Delegated Administrator 控制台不提供对 IM 服务的访问，也不提供管理 IM 用户访问级别的界面。

Delegated Administrator 实用程序

Delegated Administrator 实用程序是一组用于置备 Messaging Server 和 Calendar Server 组织、用户、组和日历资源的命令行工具。

注 – Delegated Administrator 实用程序没有提供命令来创建本书所介绍的服务提供商角色和组织。要创建和管理这些新的角色和组织，必须使用 Delegated Administrator 控制台。

可以使用 `commadmin` 命令来调用该实用程序。

有关 `commadmin` 实用程序中可用的语法和选项的信息，请参见第 5 章。

Delegated Administrator 控制台

Delegated Administrator 控制台是一个用于置备 Messaging Server 和 Calendar Server 组织、用户、组和日历资源的图形用户界面 (Graphical User Interface, GUI)。

有关如何使用该控制台的信息，请参见 Delegated Administrator 控制台联机帮助。

Delegated Administrator 与 LDAP 目录

Delegated Administrator 使您能够通过修改 LDAP 目录来置备用户。您并不需要直接修改该目录。但是，理解添加到该目录中的用户条目和高级节点的 Delegated Administrator 属性将会有所帮助。

有关支持 Delegated Administrator 的 LDAP 模式对象类和属性的信息，请参见*Sun Java System Communications Suite Schema Reference* 中的第 5 章 "Communications Suite Delegated Administrator Classes and Attributes (Schema 2)"。

置备用户的方案

根据业务需要，您可以创建简单目录结构并由单个管理员进行管理，也可以创建多层目录结构并将置备和管理任务委托给低级别管理员。

本节将介绍复杂程度依次提高的三种方案，然后介绍 Delegated Administrator 提供的可满足这些方案的要求的管理员角色和目录结构。

单层结构

在此方案中，公司或组织可包含数百或数千位员工或用户。所有用户都被分到单个组织中。由单个管理员查看和管理整个组。不存在管理任务委托情况。

图 1–1 显示了单个组织、单层结构中的管理员角色示例。

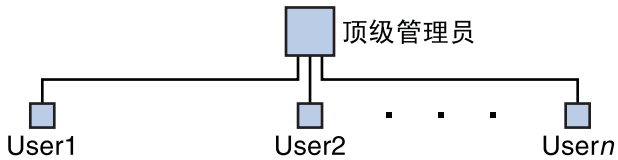

图 1–1 单层结构中的管理员角色

在单层结构中，管理员被称为顶级管理员 (Top-Level Administrator, TLA)。

在图 1–1 所示的示例中，TLA 直接管理和置备用户（User1、User2，一直到 Usern）。

如果您的目录中只有一个组织，则只需要 TLA 这一个管理员。

有关详细信息，请参见以下各节：

- 第 23 页中的 “支持单层结构的目录结构”
- 第 25 页中的 “顶级管理员角色”

两层结构

在此方案中，一个大公司（例如某个 Internet 服务提供商 [Internet Service Provider, ISP]）为多家公司提供服务。每家企业具有各自唯一的域，其中可能包含数千或数万个用户。

此方案并不是靠单个顶级管理员 (Top-Level Administrator, TLA) 来管理和置备所有域，而是允许将任务委托给低级别管理员。

在两层结构中，目录中包含多个组织。针对每个托管域，会创建一个单独的组织。

每个组织被指派给一个组织管理员 (Organization Administrator, OA)。每个 OA 负责所辖组织中的用户。OA 不能查看或修改该 OA 所辖组织以外的目录信息。

图 1–2 显示了两层结构中的管理员角色示例。

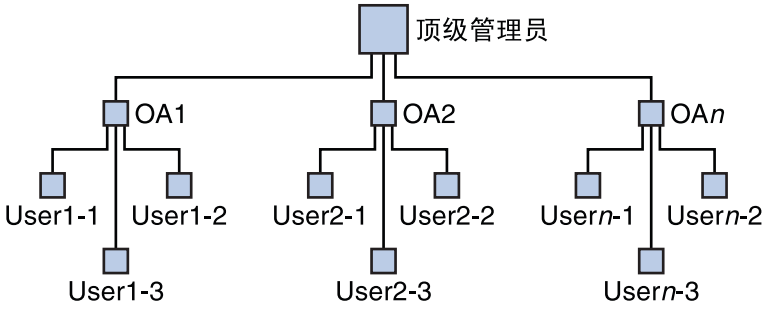

图 1–2 两层结构中的管理员角色

在图 1–2 所示的示例中，TLA 可创建和管理 OA1、OA2，一直到 OAn。每个 OA 管理一个组织中的用户。

如果您的目录中需要多个组织，则应当创建 TLA 和 OA 来管理各个组织及其用户。

有关详细信息，请参见以下各节：

- 第 24 页中的 “支持两层结构的目录结构”
- 第 25 页中的 “顶级管理员角色”
- 第 26 页中的 “组织管理员角色”

三层结构

在此方案中，一个公司（例如某个 ISP）为数百或数千家小型企业提供服务，每家企业都需要具有各自的组织。

ISP 可支持数百万需要邮件服务的最终用户。此外，ISP 还可能与管理最终用户业务的第三方转售商合作。

每天都可能需要向目录中添加许多新组织。

在两层结构中，TLA 将必须一一创建所有这些新组织。

而在三层结构中，则可以将管理任务委托给二级管理员。这种二级委托可以使得对大型 LDAP 目录所支持的大型客户库的管理容易一些。

为支持此分层结构，Delegated Administrator 引入了一个新的角色，服务提供商管理员 (Service Provider Administrator, SPA)。

SPA 的权限范围介于顶级管理员 (Top-Level Administrator, TLA) 与组织管理员 (Organization Administrator, OA) 的权限范围之间。

图 1–3 显示了三层结构中的管理员角色示例。

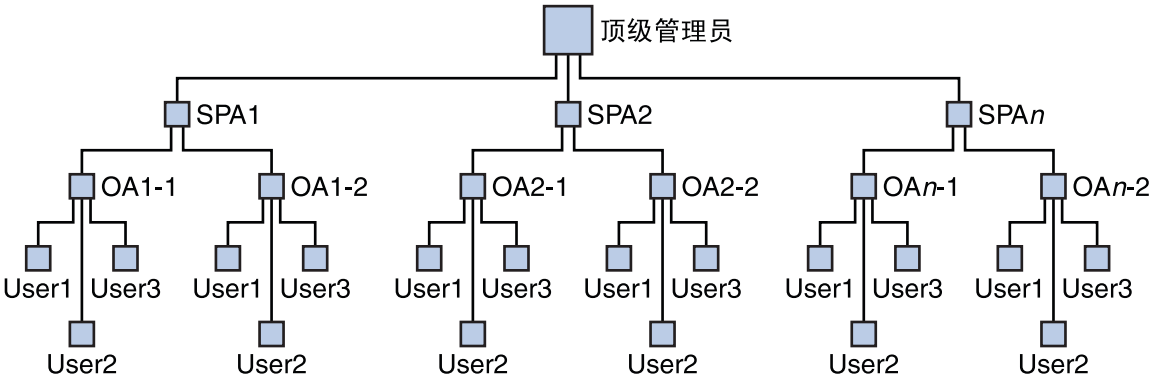

图 1–3 三层结构中的管理员角色

在三层结构中，TLA 可将管理权委托给服务提供商管理员 (Service Provider Administrator, SPA)。SPA 可以针对新客户创建下属组织并指派组织管理员 (Organization Administrator, OA) 来管理这些组织中的用户。

如果您需要的多个组织自身划分为各个子组或组织，那么您可以使用三层结构，从而可以实现 TLA、SPA 和 OA 角色。

有关 SPA 角色的信息，请参见附录 A。

管理员角色与目录分层结构

本节将显示可实现单层和两层结构的示例目录信息树，然后介绍可以由顶级管理员和组织管理员执行的任务。

支持单层结构的目录结构

当您通过运行配置程序 `config-commda` 对 Delegated Administrator 进行了配置后，就创建了顶级管理员 (Top-Level Administrator, TLA) 和默认组织。

单层结构：默认组织位于根后缀下

默认情况下，配置程序将默认组织放置在根后缀下。

目录信息树的外观将类似于图 1–4 中所示的示例。

图 1–4 显示了一个按单层结构（默认配置）组织的示例目录信息树。

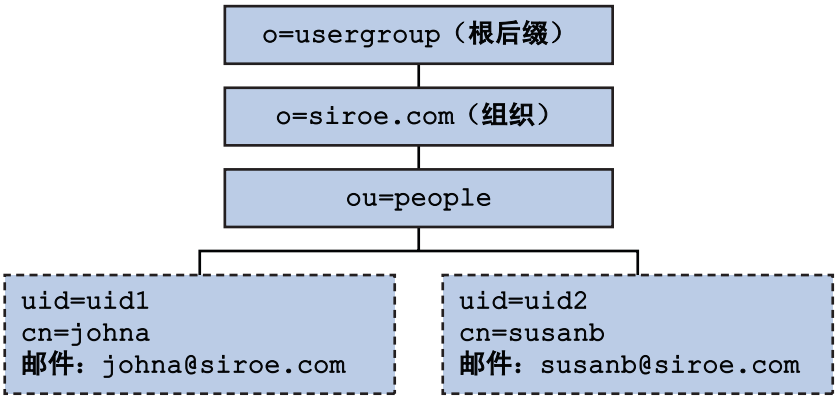

图 1–4 单层结构：示例目录信息树（默认）

单层结构：默认组织位于根后缀处

当运行配置程序 `config-commda` 时，您可以选择在根后缀处而不是在根后缀之下创建默认组织。有关配置的详细信息，请参见第 3 章中的第 65 页中的 “配置 Delegated Administrator 服务器” 。

在这种情况下，目录信息树的外观将类似于图 1–5 中所示的示例。

但是，如果您在根后缀处创建默认组织，这种 LDAP 目录配置不支持多个托管域。要支持托管域，默认组织必须位于根后缀下。

图 1–5 显示了一个单层结构示例，其中，默认组织创建在根后缀处。

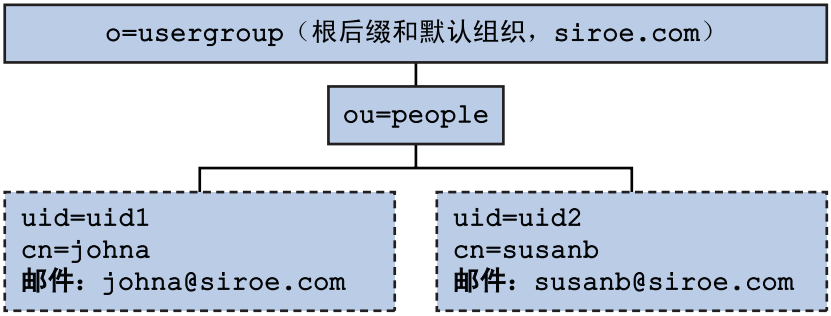

图 1–5 单层结构：默认组织位于根后缀处

支持两层结构的目录结构

使用 `config-commda` 程序对 Delegated Administrator 进行了配置后，TLA 就可以创建其他组织，如图 1–6 中所示。

图 1–6 显示了一个按两层结构组织的示例目录信息树。

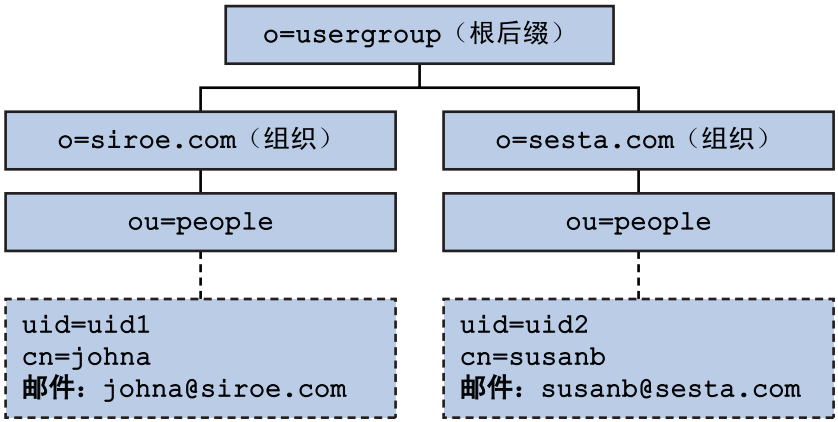

图 1–6 两层结构：示例目录信息树

顶级管理员角色

TLA 有权执行以下任务：

- 创建、删除和修改组织。

  在图 1–6 所示的示例中，TLA 可以修改或删除 siroe.com 或 sesta.com，并且可以创建其他组织。

  请注意，在此例中，两个组织也是两个独特（托管）域。
- 创建、删除和修改用户。
- 创建、删除和修改组。
- 创建、删除和修改日历资源。
- 将 OA 角色指派给用户。例如，TLA 可以将 OA 角色指派给 siroe.com 组织中的用户 johna。

  TLA 还可以撤消某个用户的 OA 角色。
- 将 TLA 角色指派给其他用户。TLA 还可以撤消某个用户的 TLA 角色。
- 将服务包指派给组织。

  有关服务包的信息，请参见本概述后面的第 27 页中的 “服务包”。

  TLA 可以将指定类型的服务包指派给一个组织，并且可以确定可用于该组织的每种服务包的最大数量。

  例如，TLA 可以指派以下服务包：

  - 在 siroe.com 组织中：

    1,000 个 gold 包

    500 个 platinum 包
  - 在 sesta.com 组织中：

2,000 个 silver 包

1,500 个 gold 包

100 个 platinum 包

TLA 可以通过使用 Delegated Administrator 控制台或通过执行 Delegated Administrator 实用程序 (commadmin) 命令来执行上述任务。

有关 commadmin 命令的说明，请参见第 5 章中的表 5–1。

组织管理员角色

OA 有权在其所辖的组织内执行以下任务：

- 创建、删除和修改用户。

  在图 1–6 所示的示例中，如果在 siroe.com 组织中将 OA 角色指派给用户 johna，则 johna 就可以管理 siroe.com 中的用户。
- 创建、删除和修改组。
- 创建、删除和修改日历资源。
- 将 OA 角色指派给其他用户。
- 为用户指派和撤消服务包。

OA 不能对其所辖组织以外的用户、组或资源执行这些任务中的任何一项。

例如，在图 1–6 中，如果 johna 是 siroe.com 的 OA，那么 johna 不能管理 sesta.com 中的用户、组或资源。

OA 可以通过使用 Delegated Administrator 控制台或通过执行 Delegated Administrator 实用程序 (commadmin) 命令来执行上述任务。

有关可供 OA 使用的 commadmin 命令的说明，请参见第 5 章中的表 5–1。

iPlanet Delegated Administrator 以前的用户的参考信息

Communications Suite Delegated Administrator 用于在 LDAP Schema 2 目录中置备用户。

早期版本的 Messaging Server（使用 LDAP Schema 1 目录）的用户可能使用过 iPlanet Delegated Administrator 这种已过时的工具。如果您仍使用 Schema 1 目录，则应使用 iPlanet Delegated Administrator 来置备用户。

iPlanet Delegated Administrator 使用的管理员角色的术语与 Communications Suite Delegated Administrator 当前所用的术语稍有不同。

表 1–1 列出并定义了每个 Delegated Administrator 版本中的管理员角色。

表 1–1 iPlanet Delegated Administrator 与 Communications Suite Delegated Administrator 中的管理员角色

iPlanet Delegated Administrator	Communications Suite Delegated Administrator 实用程序	Communications Suite Delegated Administrator 控制台	定义
站点管理员	顶级管理员 (Top-Level Administrator, TLA)	顶级管理员 (Top-Level Administrator, TLA)	管理 Delegated Administrator 所支持的整个目录，包括组织和用户*。
（无）	（此版本中没有这一项）	服务提供商管理员 (Service Provider Administrator, SPA)	管理提供商组织、提供商组织下承担部分或全部业务的商业组织以及这些商业组织中的用户。
域管理员	组织管理员 (Organization Administrator, OA)	组织管理员 (Organization Administrator, OA)	管理一个组织及该组织中的用户。
* 在此版本的 Delegated Administrator 中，TLA 不能在提供商组织下创建提供商组织或业务组织。			

服务包

服务包由 LDAP 目录中的服务类机制实现。此机制使您可以在配置 Delegated Administrator 时为目录中安装的预定义属性设置值。服务包会将服务的特征添加到用户或组条目。

Delegated Administrator 提供了服务类模板样例。

您也可以创建自己的服务包。

在 Delegated Administrator 控制台中，您可以将样例包和您自己的包指派给用户或组。

服务包类型

服务包包括以下组件：

- Access Manager 服务
- 服务束（邮件服务和/或日历服务）
- LDAP 对象（用户或组）

对于每一种服务定义，Delegated Administrator 都会自动提供 Access Manager 服务。当您将服务包指派给用户或组后，Delegated Administrator 会从服务定义中获取 Access Manager 对象类和属性，并将它们添加到 LDAP 条目。

请勿更改或删除任何服务包的 Access Manager 部分。

创建服务包后，您可以配置其服务束和 LDAP 对象。

服务束

Delegated Administrator 提供了两种服务：邮件服务和日历服务。

一个服务包可捆绑一项或多项服务，以及与该服务关联的一组属性。因此，单个服务包可以包含以下服务组合：

- 仅邮件服务
- 仅日历服务
- 邮件服务和日历服务

注 – 仅邮件服务包模板具有与邮件服务类定义相关联的 LDAP 属性。日历服务包模板不包括与日历服务定义相关联的属性。

为特殊 LDAP 对象定义的包

服务包要么是为用户定义的，要么是为组定义的。您不能将同一个服务包同时指派给用户和组。

Delegated Administrator 提供的服务包包含以下服务束和 LDAP 对象：

- 用户邮件服务
- 用户日历服务
- 用户邮件服务和日历服务
- 组邮件服务
- 组日历服务
- 组邮件服务和日历服务

关于组

在 Delegated Administrator 中，组是 LDAP 目录中的条目，它由一组用户组成。组的特征不会传递给该组的成员用户。例如，当您将服务包指派给某个组时，该组的成员不会继承服务包的属性。目录中的用户条目不会从属于（不“属于”）组条目。

将邮件服务包指派给某个组后，该组就成为一个由 Messaging Server 使用的邮递列表。

当将日历服务指派到组时，组成员共享由 Calendar Server 管理的组邀请和其他日历信息。

邮件组没有自己的邮箱，发送到组地址的消息会传送到各个组成员的邮箱。

但是，日历组拥有自己的日历，发送到组的邀请会显示在组日历和各个组成员的日历上。

Delegated Administrator 提供的服务包

配置 Delegated Administrator 时，您可以选择安装一组预定义的服务类模板样例。Delegated Administrator 控制台将显示这些模板。

（当您运行配置程序时，请选择**服务包和组织样例**面板中的**装入服务包样例**。）配置程序会将 `cos.sample.ldif` 文件添加到 LDAP 目录。

您可以使用模板样例向用户和组提供服务和邮件属性。有关模板及其属性值的列表，请参见第 33 页中的 “服务类模板样例”。

图 1–7 显示了用户服务包模板。

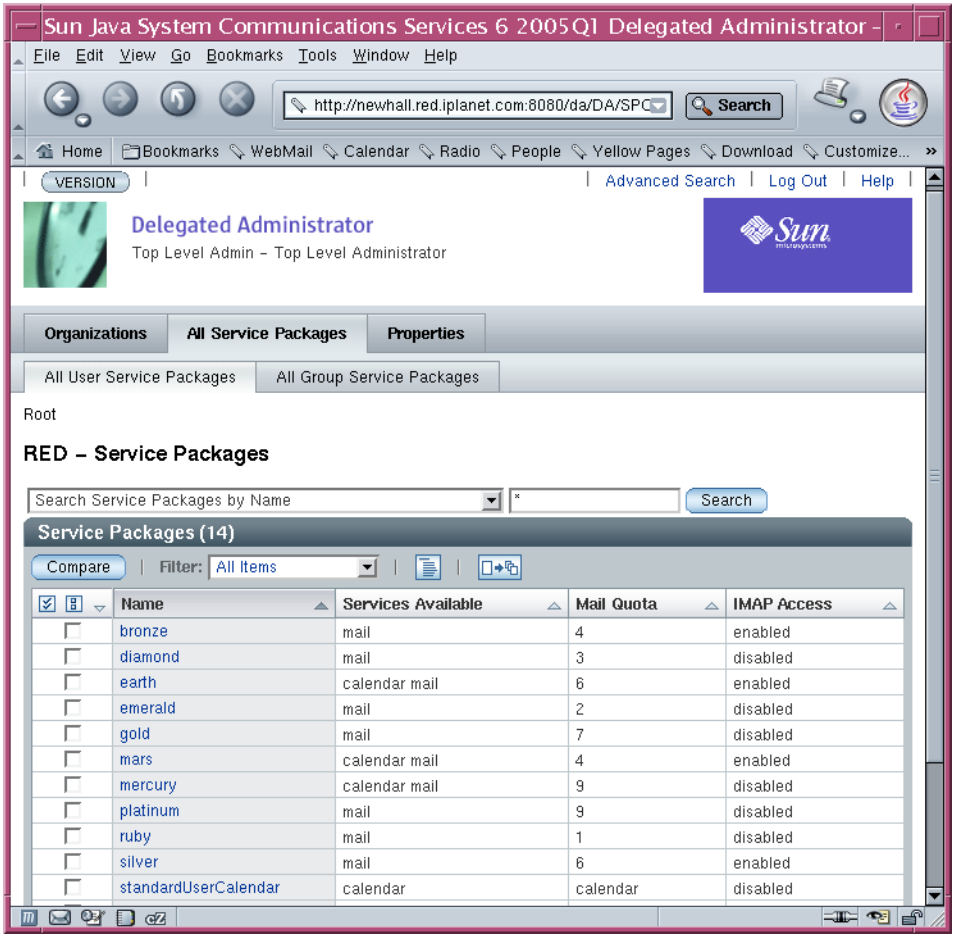

图 1–7 “全部用户服务软件包”页面—显示模板样例

图 1–8 显示了组服务包模板。

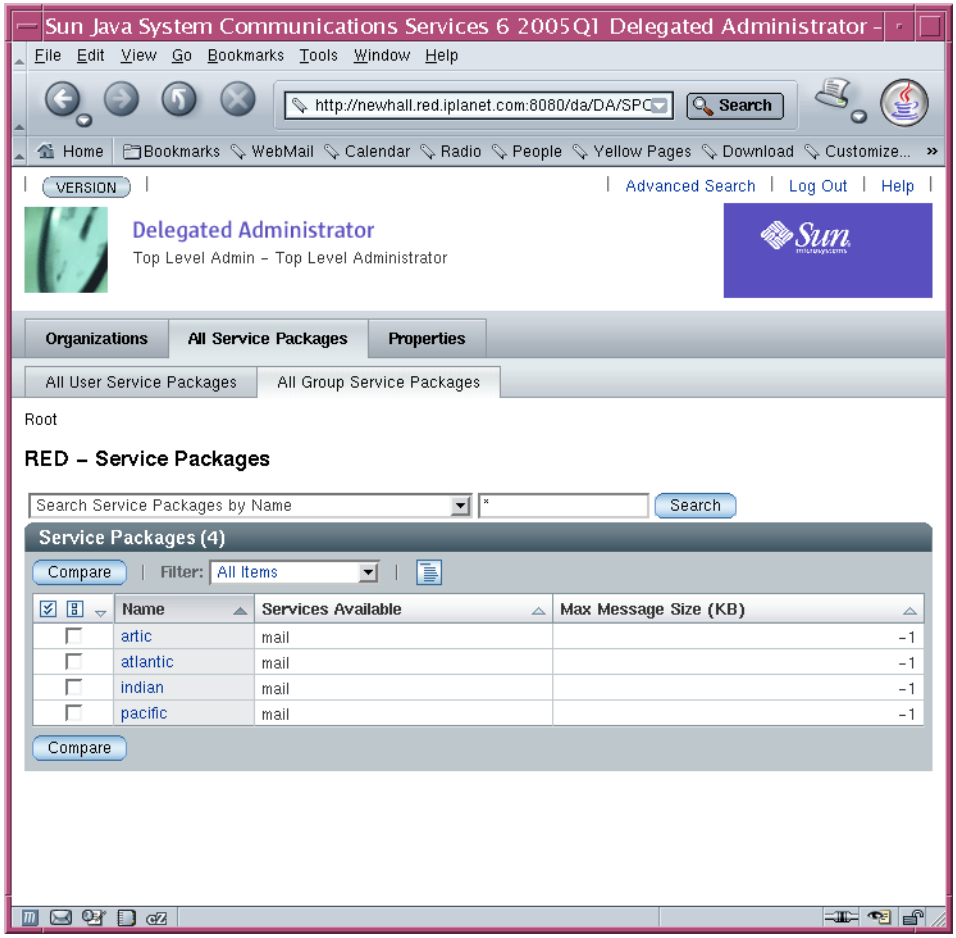

图 1–8 “全部组服务软件包”页面—显示模板样例

服务包任务

在 Delegated Administrator 控制台中，可执行以下服务包任务：

- 将服务包分配给各个组织。通过将部分（或全部）包分配给某个组织，将使这些包可供该组织中的用户或组使用。

  对于每种包类型，可分配指定数量的包。

  例如，可以为 ABC 组织分配 5000 个 gold 服务包、10000 个 venus 服务包和 500 个 atlantic 服务包。
- 将服务包指派给用户。
- 将服务包指派给组。

指派服务包的指导原则

- 分配给组织的服务包将构成一个池，可以从其中将服务包指派给该组织中的用户或组。
- 可以将多个服务包指派给一个用户或组。
- 将服务包指派给某个用户或组后，该服务包中的所有属性和值会自动被指派给该用户或组。
- 要仅将日历服务指派给用户，请使用 standardUserCalendar 服务包。日历服务不具有关联属性。

  指派 standardUserCalendar 服务包等同于使用 `commadmin user create` 或 `commadmin user modify` 命令中的 `-s cal` 选项。

有关如何分配和指派服务包的说明，请参见 Delegated Administrator 控制台联机帮助。

创建您自己的服务包

本章中介绍的服务类模板只是作为示例。您很可能会需要创建自己的服务包，以使其带有的属性值与您的安装中的用户和组相应。

要创建自己的服务包，您可以使用存储在 `da.cos.skeleton.ldif` 文件中的服务类模板。此文件是专门为用作编写服务包时的模板而创建的。配置 Delegated Administrator 时，未在 LDAP 目录中安装此文件。

您可以复制和编辑 `da.cos.skeleton.ldif` 文件并使用一个 LDAP 目录工具（例如 `ldapmodify`）在目录中安装自定义的服务类模板。

Delegated Administrator 控制台会将您的自定义模板与示例模板一起显示。在该控制台中，服务类模板被称为服务包。当您可以将服务包指派给用户或组时，Delegated Administrator 会用完整的服务包（包括 Access Manager 服务）来填充该用户或组 LDAP 条目。

有关使用 `da.cos.skeleton.ldif` 文件来配置您自己的服务包的说明，请参见第 3 章中第 74 页中的 “创建服务包” 。

查看扩展服务包时的限制

您可以通过将任何属性添加到定义条目来扩展 Delegated Administrator 服务包的定义。

但是，在此版本的 Delegated Administrator 中，控制台仅允许您查看 Delegated Administrator 配置好后所提供的预定义属性。Delegated Administrator 控制台不会显示您添加到服务包定义的任何属性。

此外，在此版本中，您也不应从 Delegated Administrator 提供的服务类定义中删除预定义属性。

指派给 LDAP 条目的服务包样例

使用 Delegated Administrator 将服务包指派给某个用户或组后，会在 LDAP 目录中为该用户或组条目添加单个属性 (inetCOS)。inetCOS 属性的值会将整个服务包（包括服务和与其关联的属性）指派给该用户或组。（inetCOS 是一个多值属性。）

例如，假设您将 platinum 包指派给某个用户。以下属性会被添加到该用户条目：

```
inetCOS: platinum
```

platinum 包将向该用户提供邮件服务。此包还包含以下邮件属性值。因此，指派 platinum 包等同于将以下属性添加到用户条目：

```
mailMsgMaxBlocks: 800
mailQuota: 10000000
mailMsgQuota: 6000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
```

Access Manager 服务定义提供了邮件服务和/或日历服务所需的对象类和属性。当您指派服务包时，Delegated Administrator 会将这些对象类和属性添加到用户或组条目。

服务类模板样例

本节列出了服务类模板样例和这些模板所提供的邮件属性值。

这些模板包含在 cos.sample.ldif 文件中。

邮件服务属性

邮件服务包括针对邮件用户定义的 LDAP 属性。表 1–2 中定义了这些属性。

表 1–2 可以在服务包中使用的邮件服务属性

属性	定义
mailMsgMaxBlocks	可以发送给用户或组的最大消息的大小，以 MTA 块为单位。
mailAllowedServiceAccess	一种过滤器，用于指定哪些客户机可以访问特定的服务。例如：+imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
mailMsgQuota	允许向某一用户发送的最大消息数量（包括所有用户文件夹）。
mailQuota	允许该用户的邮箱占用的磁盘空间（以字节为单位）。

有关这些属性的详细信息，请参见 *Sun Java System Communications Suite Schema Reference* 中的第 3 章 "Messaging Server and Calendar Server Attributes"。

用户邮件模板样例

Platinum

```
mailMsgMaxBlocks: 800
mailquota: 10000000
mailmsgquota: 6000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Gold

```
mailMsgMaxBlocks: 700
mailquota: 8000000
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Silver

```
mailMsgMaxBlocks: 300
mailquota: 6291456
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

Bronze

```
mailMsgMaxBlocks: 700
mailquota: 5242288
mailmsgquota: 3000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

Ruby

```
mailMsgMaxBlocks: 600
mailquota: 1048576
mailmsgquota: 2000
mailAllowedServiceAccess: +pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Emerald

```
mailMsgMaxBlocks: 600
mailquota: 2097152
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

Diamond

```
mailMsgMaxBlocks: 5000
mailquota: 3145728
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Topaz

```
mailMsgMaxBlocks: 3000
mailquota: 4194304
mailmsgquota: 2000
mailAllowedServiceAccess: +imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

用户日历模板样例

无 (standardUserCalendar)

没有预定义服务类模板来提供日历服务和包含属性值。日历服务不具有关联属性。

因为不存在模板样例，所以 Delegated Administrator 会不使用模板而直接根据用户日历服务类定义来生成默认服务包。其名称与服务类定义的名称相同：standardUserCalendar。

此服务包仅提供日历服务。

用户邮件和日历模板样例

以下模板样例对邮件服务和日历服务均适用。

Mercury

```
mailMsgMaxBlocks: 800
mailquota: 10000000
mailmsgquota: 6000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

Venus

```
mailMsgMaxBlocks: 700
mailquota: 8000000
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

Earth

```
mailMsgMaxBlocks: 300
mailquota: 6291456
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

Mars

```
mailMsgMaxBlocks: 700
mailquota: 5242288
mailmsgquota: 3000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

组邮件模板样例

Atlantic

```
mailMsgMaxBlocks: 800
daServiceType: mail group
```

Pacific

```
mailMsgMaxBlocks: 900
daServiceType: mail group
```

Indian

```
mailMsgMaxBlocks: 1000
daServiceType: mail group
```

Arctic

```
mailMsgMaxBlocks: 1200
daServiceType: mail group
```

组日历模板样例

无 (standardGroupCalendar)

没有预定义服务类模板来向组提供日历服务和包含属性值。日历服务不具有关联属性。

因为不存在模板样例，所以 Delegated Administrator 会不使用模板而直接根据组日历服务类定义来生成默认服务包。其名称与服务类定义的名称相同：standardGroupCalendar。

此服务包仅（向组）提供日历服务。

组邮件和日历模板样例

以下模板样例将邮件服务和日历服务均应用于组。

Nile

```
mailMsgMaxBlocks: 1600
daServiceType: mail group
daServiceType: calendar group
```

Amazon

```
mailMsgMaxBlocks: 1800
daServiceType: mail group
daServiceType: calendar group
```

Thames

```
mailMsgMaxBlocks: 2000
daServiceType: mail group
daServiceType: calendar group
```

Danube

```
mailMsgMaxBlocks: 2200
daServiceType: mail group
daServiceType: calendar group
```

服务类定义

此版本的 Delegated Administrator 为每种服务包提供了服务类定义：

- 用户邮件服务
- 用户日历服务
- 用户邮件服务和日历服务
- 组邮件服务
- 组日历服务
- 组邮件服务和日历服务

当您对 Delegated Administrator 进行了配置，服务类定义就会安装在目录中。

在每个定义中，`daServiceType` 属性通过以下语法确定了服务包的类型：

```
daServiceType: <service type> <target>
```

其中 *service type* 为邮件服务、日历服务或邮件和日历服务，*target* 为用户或组。

用户邮件服务

用户邮件服务是在称为 `standardUserMail` 的服务类定义中的：

```
#
#  Definition for user mail service bundle
#
dn: cn=standardUserMail,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=mailuser,o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: mailAllowedServiceAccess
cosAttribute: mailMsgMaxBlocks
cosAttribute: mailquota
cosAttribute: mailmsgquota
daServiceType: mail user
```

注意：当 `Delegated Administrator` 配置程序在目录中安装 `standardUserMail` 定义时，上面显示的变量 `<ugldapbasedn>` 将替换为您的根后缀（如 `o=usergroup`）。

`daServiceType` 属性将此定义为用户邮件服务。

用户日历服务

用户日历服务是在称为 `standardUserCalendar` 的服务类定义中定义的：

```
#
#  Definition for user calendar service bundle
#
dn: cn=standardUserCalendar,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
```

```
cosTemplateDn: o=calendaruser,o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: icsPreferredHost
cosAttribute: icsDWPHost
cosAttribute: icsFirstDay
daServiceType: calendar user
```

注意：当 Delegated Administrator 配置程序在目录中安装 standardUserCalendar 定义时，上面显示的变量 <ugldapbasedn> 将替换为您的根后缀（如 o=usergroup）。

daServiceType 属性将此定义为用户日历服务。

注 – 日历服务定义还包括日历属性，例如 icsPreferredHost。

但是 Delegated Administrator 没有提供为这些属性指定值的服务包模板。Delegated Administrator 控制台提供了一个仅带有日历服务的服务包：standardUserCalendar 服务包。此包不包含日历属性。

用户邮件服务和日历服务

用户邮件服务和日历服务是在称为 standardUserMailCalendar 的服务类定义中定义的：

```
#
#  Definition for user mail and user calendar service bundle
#
dn: cn=standardUserMailCalendar,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=mailcalendaruser,o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: icsPreferredHost
cosAttribute: icsDWPHost
cosAttribute: icsFirstDay
cosAttribute: icsQuota
cosAttribute: mailAllowedServiceAccess
cosAttribute: mailMsgMaxBlocks
cosAttribute: mailquota
cosAttribute: mailmsgquota
daServiceType: calendar user
```

```
daServiceType: mail user
```

注意：当 Delegated Administrator 配置程序在目录中安装 standardUserMailCalendar 定义时，上面显示的变量 <ugldapbasedn> 将替换为您的根后缀。（如 o=usergroup）。

两个 daServiceType 属性条目将此定义为用户日历服务和邮件服务。

组邮件服务

组邮件服务是在称为 standardGroupMail 的服务类定义中定义的：

```
#
#  Definition for group mail service bundle
#
dn: cn=standardGroupMail,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=mailgroup,o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: mailMsgMaxBlocks
daServiceType: mail group
```

注意：当 Delegated Administrator 配置程序在目录中安装 standardGroupMail 定义时，上面显示的变量 <ugldapbasedn> 将替换为您的根后缀（如 o=usergroup）。

daServiceType 属性将此定义为组邮件服务。

组日历服务

组日历服务是在称为 standardGroupCalendar 的服务类定义中定义的：

```
#
#  Definition for group calendar service bundle
#
dn: cn=standardGroupCalendar,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
```

```
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=calendargroup,o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: icsdoublebooking
cosAttribute: icsautoaccept
daServiceType: calendar group
```

注意：当 Delegated Administrator 配置程序在目录中安装 standardGroupCalendar 定义时，上面显示的变量 <ugldapbasedn> 将替换为您的根后缀（如 o=usergroup）。

daServiceType 属性将此定义为组日历服务。

注 – 日历服务定义还包括日历属性，例如 icsdoublebooking。

但是 Delegated Administrator 没有提供为这些属性指定值的服务包模板。Delegated Administrator 控制台为组提供了一个仅带有日历服务的服务包：standardGroupCalendar 服务包。此包不包含日历属性。

组邮件服务和日历服务

用户邮件服务和日历服务是在称为 standardGroupMailCalendar 的服务类定义中定义的：

```
#
#  Definition for group mail and group calendar service bundle
#
dn: cn=standardGroupMailCalendar,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=mailcalendargroup,o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: mgrpMsgMaxSize
cosAttribute: mailMsgMaxBlocks
daServiceType: calendar group
daServiceType: mail group
```

注意：当 Delegated Administrator 配置程序在目录中安装 standardGroupMailCalendar 定义时，上面显示的变量

<ugldapbasedn> 将替换为您的根后缀（如 o=usergroup）。

这两个 daServiceType 属性条目将其定义为组日历服务和邮件服务。

服务类定义和包的位置

在 LDAP 目录信息树 (Directory Information Tree, DIT) 中，服务类定义位于根后缀下一层节点中。因为它们存储在 DIT 的顶层，因此可以将服务包指派给目录中的所有用户条目。

图 1–9 显示了服务定义和服务包在 DIT 中的位置。

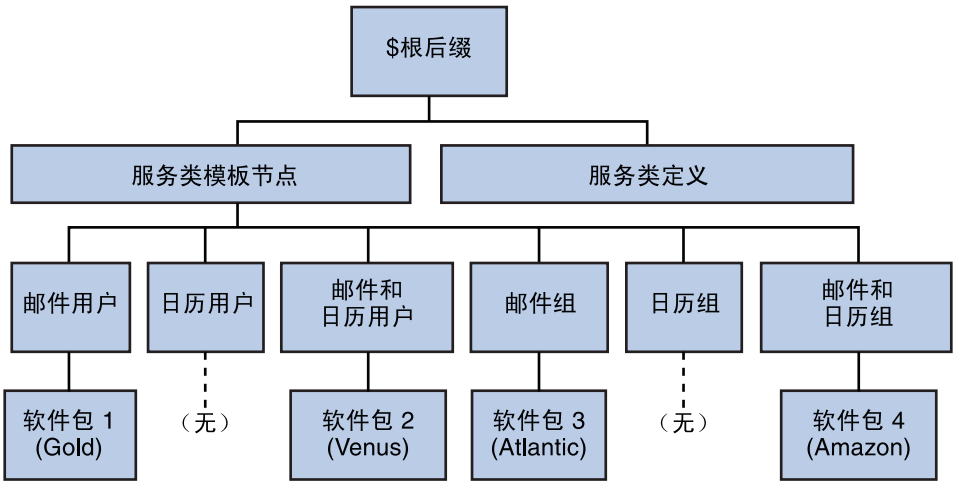

图 1–9 服务类定义和服务包在目录树中的位置

每种服务类模板位于各自的节点下。因此，为用户提供邮件服务的模板位于邮件用户节点下。这种结构使 Delegated Administrator 在将服务包指派给用户或组时能够使用正确的服务类定义（例如 standardUserMail）。

Delegated Administrator 使用典型的服务类定义。

有关服务类机制的详细信息，请参见 *Sun Java System Directory Server* **管理指南**。具体请参见第五章“管理身份和角色”中的“定义服务类 (CoS)”。

Sun Java System Directory Server **管理指南**中还介绍了相关的主题，例如，如果该单个用户条目中已经存在指派给用户的服务包所定义的属性，那么如何确定哪一个服务属性值优先。

◆ ◆ ◆ 第 2 章

2 安装和配置规划

要在 Solaris 系统上安装 Sun Java System Delegated Administrator，必须使用 Sun Java Communications Suite 安装程序，此安装程序也会安装其他 Communications Suite 组件产品。

要安装和配置 Delegated Administrator，请执行以下步骤：

1. 第 43 页中的 “收集 Delegated Administrator 的配置信息”
2. 第 47 页中的 “运行 Sun Java Communications Suite 安装程序”
3. 第 48 页中的 “运行 Directory Server 安装脚本”
4. 第 49 页中的 “配置 Delegated Administrator”
5. 第 49 页中的 “配置 Messaging Server 和 Calendar Server”

   有关 Delegated Administrator 的最新信息，请参见 Sun Java Communications Suite 发行说明。

收集 Delegated Administrator 的配置信息

Delegated Administrator 组件

Delegated Administrator 包含以下组件：

- **Delegated Administrator 实用程序（客户机）**—使用 `commadmin` 调用的命令行界面。

  必需。必须在所有安装 Delegated Administrator 的计算机上都配置此实用程序。
- **Delegated Administrator 服务器**—运行 Delegated Administrator 实用程序和控制台所需的 Delegated Administrator 服务器组件。

  必需。必须至少在一台计算机上配置 Delegated Administrator 服务器。
- **Delegated Administrator 控制台**—Delegated Administrator 图形用户界面 (Graphical User Interface, GUI)。

可选。如果只需要使用 Delegated Administrator 实用程序，则不必配置此控制台。

Web 容器

此外，还必须将 Delegated Administrator 服务器和控制台部署到 Web 容器。可以基于以下组件来配置 Delegated Administrator 控制台和服务器

- Sun Java System Web Server 6.*x*
- Sun Java System Web Server 7.*x*
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

配置时请遵循以下指导：

- 必须将 Delegated Administrator 服务器部署到 Access Manager 所使用的 Web 容器。
- 可以基于两个不同的 Web 容器、两个不同的 Web 容器实例或同一个 Web 容器来部署 Delegated Administrator 控制台和服务器。

配置信息

在配置 Delegated Administrator 之前，应该先收集配置信息。

表 2–1 列出了 Delegated Administrator 必需的配置选项。

表 2–2 列出了基于 Web Server 6.*x* 部署时的配置选项。

表 2–3 列出了基于 Web Server 7.*x* 部署时的配置选项。

表 2–4 列出了基于 Application Server 7.*x* 部署时的配置选项。

表 2–5 列出了基于 Application Server 8.*x* 部署时的配置选项。

表 2–1 Delegated Administrator：必需的配置选项

选项	说明
配置目录	用来存储配置和数据文件的目录。
Access Manager 主机名	安装 Access Manager 的主机名。Delegated Administrator 服务器应安装在同一服务器上。
Access Manager 端口号	Access Manager 的端口号。应当与 Web Server 端口号相同。
默认域	顶级管理员的默认域。在执行 `commadmin` 命令行实用程序时，如果没有通过 `-n` 选项显式指定某个域，则使用此域。

表 2–1 Delegated Administrator：必需的配置选项 （续）

选项	说明
默认 SSL 端口	Delegated Administrator 客户机所使用的 SSL 端口。
Access Manager 基本目录	Access Manager 的安装目录。默认目录为 `/opt/SUNWam`。
LDAP URL	用户和组的 Directory Server LDAP URL。
绑定为	用户和组的 Directory Server Directory Manager。例如 "cn=Directory Manager"。
LDAP 密码	用户和组的 Directory Manager 密码。
Access Manager 顶级管理员用户 ID 和密码	Access Manager 顶级管理员的用户 ID 和密码
Access Manager 内部 LDAP 验证用户的密码	由 Access Manager 创建的用户。此用户是 LDAP 服务的 BindDN 用户。
组织名	用于命名 LDAP 子树，属于默认电子邮件域的所有电子邮件用户和组均位于该子树下。
默认组织顶级管理员的用户 ID 和密码	将在默认组织中创建的顶级管理员的用户 ID 和密码 。
样例组织的首选邮件主机	安装 Messaging Server 的计算机名。如果您选择在您指定的目录下安装样例组织，则必须输入首选邮件主机。

表 2–2 Web Server 6.*x* 配置选项

选项	说明
Web Server 6.*x* 根（实例）目录	Web Server 6.*x* 实例所在的目录。有关 Web Server 实例的文件存储在 Web Server 安装目录下的 `https-`*host*`.`*domain* 目录中。
Web Server 6.*x* 实例标识符	Web Server 6.*x* 实例的全限定域名。可用 *host.domain* 名（例如 `west.sesta.com`）来指定此标识符。
虚拟服务器标识符	用 `https-`*host.domain* 名（例如 `https-west.sesta.com`）来指定。
HTTP 端口号	Web Server 6.*x* 的 HTTP 端口号。

表 2–3 Web Server 7.*x* 配置选项

选项	说明
Web Server 根目录	Web Server 7.*x* 服务器文件安装的目录。默认根目录是 `/opt/SUNWwbsvr7`。
Web Server 配置根目录	Web Server 7.*x* 配置文件安装的目录。默认配置根目录是 `/var/opt/SUNWwbsvr7`。

表 2–3 Web Server 7.*x* 配置选项 （续）

选项	说明
Web Server 实例标识符	Web Server 7.*x* 实例的全限定域名。可用 *host.domain* 名（例如 `west.sesta.com`）来指定此标识符。
虚拟服务器标识符	用 *host.domain* 名（例如 `west.sesta.com`）来指定。
HTTP 端口号	Web Server 7.*x* 的 HTTP 端口号。默认端口号是 `80`。
Administration Server 端口号	Web Server 7.*x* 的 Administration Server 实例的端口号。例如：`8800`。
Administration Server 管理员用户 ID	用户 ID 示例：`admin`
Administration Server 管理员密码	输入管理员用户 ID 的密码。
对 Administration Server 实例的 HTTP 或 HTTPS 访问	您将需要指定对 Administration Server 实例的 HTTP 访问是否安全。

表 2–4 Application Server 7.*x* 配置选项

选项	说明
Application Server 安装目录	Application Server 7.*x* 的安装目录。默认情况下，此目录为 `/opt/SUNWappserver7`。
Application Server 域目录	默认情况下，此目录为 `/var/opt/SUNWappserver7/domains/domain1`。
Application Server 文档根目录	默认情况下，此目录为 `/var/opt/SUNWappserver7/domains/domain1/server1/docroot`
Application Server 实例名	该实例的名称。例如：`server1`。
虚拟服务器标识符	Application Server 虚拟服务器标识符的名称。例如：`server1`。
Application Server 实例的 HTTP 端口号	Application Server 实例的 HTTP 端口号。
Administration Server 端口号	Application Server 7.*x* 的 Administration Server 实例的端口号。例如：`4848`。
Administration Server 管理员的用户 ID 和密码	Administration Server 管理员的用户 ID 和密码 。用户 ID 示例：`admin`
对 Administration Server 实例的 HTTP 或 HTTPS 访问	您将需要指定对 Administration Server 实例的 HTTP 访问是否安全。

表 2–5 Application Server 8.*x* 配置选项

选项	说明
Application Server 安装目录	Application Server 8.*x* 的安装目录。默认情况下，此目录为 `/opt/SUNWappserver/appserver`。
Application Server 域目录	默认情况下，此目录为 `/var/opt/SUNWappserver/domains/domain1`。
Application Server 文档根目录	默认情况下，此目录为 `/var/opt/SUNWappserver/domains/domain1/docroot`。
Application Server 目标名	该实例的名称。例如：`server`。
虚拟服务器标识符	Application Server 虚拟服务器标识符的名称。例如：`server`。
Application Server 目标的 HTTP 端口号	Application Server 目标的 HTTP 端口号。
Administration Server 端口号	Application Server 8.*x* 的 Administration Server 实例的端口号。例如：`4849`。
Administration Server 管理员的用户 ID 和密码	Administration Server 管理员的用户 ID 和密码 。用户 ID 示例：`admin`
对 Administration Server 实例的 HTTP 或 HTTPS 访问	您将需要指定对 Administration Server 实例的 HTTP 访问是否安全。

运行 Sun Java Communications Suite 安装程序

Communications Suite 安装程序将安装一系列交互操作的产品、共享组件和库。

要成功安装和配置 Delegated Administrator，需要通过运行 Communications Suite 安装程序来安装以下组件。或者，您的系统可能已经安装依赖的组件（如 Directory Server）。如果已经安装支持的版本，现在就不必重新进行安装。

以下列表包含所有支持的依赖组件的版本。如果使用当前的 Communications Suite 安装程序安装组件，仅能安装这些组件的最新版本。

- Sun Java System Directory Server 5.x 或 6.x。（当前的 Communications Suite 安装程序将安装版本 6.x。）
- Sun Java System Access Manager 6.x 或 7.x。（当前的 Communications Suite 安装程序将安装版本 7.x。）

  Access Manager 7 有两种安装类型：传统模式（默认）和领域模式。传统模式与 Delegated Administrator 兼容。

  运行 Communications Suite 安装程序时，必须在第一个 Access Manager 面板上选择“传统”模式作为安装类型。请不要选择“领域”模式。

  由于 Delegated Administrator 要求您使用 LDAP Schema 2 置备用户和组，因此您需要安装 Access Manager。

- 以下 Web 容器之一：
  - Sun Java System Web Server 6.*x*
  - Sun Java System Web Server 7.*x*（随当前的 Communications Suite 安装程序安装）
  - Sun Java System Application Server 7.*x*
  - Sun Java System Application Server 8.*x*（随当前的 Communications Suite 安装程序安装）

  Communications Suite 安装程序还会进行检查以确保您安装了 Directory Server 和以上列出的 Web 容器之一。
- Sun Java System Messaging Server 和 Sun Java System Calendar Server 中的一个或两个。

  Delegated Administrator 是用于 Messaging Server 和 Calendar Server 的置备工具。因此，要成功使用 Delegated Administrator，您应该安装这两种应用程序中的一个或两个。

  有关配置 Messaging Server 的说明，请参见 Sun Java System Messaging Server 管理指南。有关配置 Calendar Server 的说明，请参见 Sun Java System Calendar Server 管理指南。
- Delegated Administrator

  Communications Suite 安装程序中会有一个面板询问是否安装 Delegated Administrator。请在此面板中指定要安装 Delegated Administrator。

  安装程序将把 Delegated Administrator 安装在被称为 *da-base* 的目录（例如，默认为 `/opt/SUNWcomm`）中。

有关 Communications Suite 安装程序的信息，请参阅 Sun Java Communications Suite Installation Guide。

注 – 如果要从早期版本的 Sun Java 升级 Delegated Administrator，请参见 Sun Java Communications Suite Upgrade Guide 中名为 "Upgrading Delegated Administrator" 的章节。

运行 Directory Server 安装脚本

在配置 Delegated Administrator、Messaging Server 或 Calendar Server 之前，必须先运行 Directory Server Preparation Tool 脚本 (`comm_dssetup.pl`)。您只需运行 `comm_dssetup.pl` 脚本一次。

此脚本可将 LDAP Directory Server 配置为与 Delegated Administrator、Messaging Server 或 Calendar Server 配置一起工作。`comm_dssetup.pl` 脚本通过设置新的模式、索引和配置数据来准备 Directory Server。

有关 `comm_dssetup.pl` 脚本的说明和选项，请参见 Sun Java System Messaging Server 管理指南或 Sun Java System Calendar Server 管理指南。

要运行 Delegated Administrator，在运行 `comm_dssetup.pl` 脚本时必须选择 "Schema 2" 模式类型。

合并目录中的 ACI

在 Access Manager、Messaging Server 和 LDAP Schema 2 目录的大规模安装中，您可能需要合并目录中的访问控制指令 (Access Control Instruction, ACI)。

当您将 Access Manager 与 Messaging Server 一起安装后，目录中一开始会安装大量的 ACI。很多默认的 ACI 对 Messaging Server 来说是不需要的或用不到。您可以通过合并目录中的默认 ACI 和精简其数量来提高 Directory Server 的性能，从而提高 Messaging Server 的查找性能。

有关如何合并和放弃未使用的 ACI 的信息，请参见本指南后面的附录 E。

配置 Delegated Administrator

安装了 Delegated Administrator 之后，请使用第 43 页中的 “收集 Delegated Administrator 的配置信息”中提供的信息来运行 Delegated Administrator 配置程序。

有关运行该配置程序的信息，请参见第 3 章。

配置 Messaging Server 和 Calendar Server

有关配置 Messaging Server 的说明，请参见 Sun Java System Messaging Server 管理指南。有关配置 Calendar Server 的说明，请参见 Sun Java System Calendar Server 管理指南。

◆ ◆ ◆ 第 3 章

3 配置 Delegated Administrator

Delegated Administrator 配置程序 (`config-commda`) 可根据您的特定要求来创建新的配置。此初始运行时配置程序执行的是最小配置。

运行此程序之后，应执行第 72 页中的 “配置后任务”中所述的步骤来完成初始配置。

通过执行第 4 章中所述的任务，您可以进一步自定义 Delegated Administrator 配置。

可能还会需要执行其他配置，如 Sun Java System Messaging Server 管理指南中所述。

本章介绍了以下主题：

如果要从早期版本的 Delegated Administrator 进行升级

如果您是首次配置 Delegated Administrator，则可以跳过本节，直接转到第 55 页中的 “选择要配置的组件”一节。

如果要从早期版本升级到此版本的 Delegated Administrator，则在配置 Delegated Administrator 之前可能需要执行以下任务：

有关如何从早期版本的 Sun Java 升级到 Delegated Administrator 的说明，请参见 Sun Java Communications Suite Upgrade Guide 中名为 "Upgrading Delegated Administrator" 的章节。

保留现有配置

本节仅针对以前安装并配置了 Delegated Administrator，并自定义了 Delegated Administrator 配置的用户。

如果您具有自定义配置并且重新运行 Delegated Administrator 配置程序 `config-commda`，则配置文件中的属性将重置为其默认值。这些文件列在下面的第 52 页中的 “Delegated Administrator 属性文件”中。

有关如何自定义 Delegated Administrator 的信息，请参见第 4 章。

在升级 Delegated Administrator 或由于任何其他原因而重新运行 Delegated Administrator 配置程序之前，应保留自定义配置。

Delegated Administrator 属性文件

Delegated Administrator 安装了以下属性文件：

- Delegated Administrator 实用程序
  - `cli-usrprefs.properties`

    位置：*da-base*`/data/config`
- Delegated Administrator 控制台
  - `daconfig.properties`
  - `logger.properties`
  - `Resources.properties`
  - `Security.properties`

  有关 Delegated Administrator 控制台文件的默认位置，请参见第 90 页中的 “配置文件的原始（标准）位置”。
- Delegated Administrator 服务器
  - `resource.properties`

    有关 `resource.properties` 文件的默认位置，请参见第 90 页中的 “配置文件的原始（标准）位置”。

▼ 保留现有配置的步骤

1. **备份已自定义的属性文件。**

   有关属性文件的列表，请参见第 52 页中的 “Delegated Administrator 属性文件”。

2. **运行 `config-commda` 程序，如以下几节所述。**

   剩下的步骤将使用 `resource.properties` 文件作为示例。您可以对每个自定义的文件重复这些步骤。

3 **如下所示编辑由 `config-commda` 程序创建的新 `resource.properties` 文件：**

a. **打开该新 `resource.properties` 文件。**

确保编辑位于 Delegated Administrator 安装目录原始（标准）位置的 `resource.properties` 文件，而不是部署到 Delegated Administrator 服务器所使用的 Web 容器的文件。

b. **打开 `resource.properties` 文件的备份副本。**

c. **找到在该备份副本中自定义的属性。将自定义值应用于新 `resource.properties` 文件中的相应属性。**

不要简单地用整个备份副本覆写新 `resource.properties` 文件。该新文件可能包含为支持此版本的 Delegated Administrator 而创建的新属性。

4 **将编辑的 `resource.properties` 文件重新部署到 Delegated Administrator 服务器使用的 Web 容器。**

必须运行脚本将自定义的 `resource.properties` 文件部署到您的 Web 容器，更改才会生效。

有关如何将自定义的属性文件部署到特定 Web 容器的说明，请参见第 92 页中的 “部署自定义配置文件”。

升级自定义服务包

本节仅针对从 Communications Services 6 2005Q4 Delegated Administrator 升级到 Delegated Administrator 6.4（当前版本），并且在前一个版本 (6 2005Q4) 中创建了自定义服务包的用户。

在 Delegated Administrator 6.4 中，服务包模板在目录中所处的节点与前一个版本 (6 2005Q4) 不同。

服务类模板样例

运行 Delegated Administrator 配置程序后，以前由 Delegated Administrator 配置程序安装的服务类模板样例将自动升级。（在此配置程序中，应选择**服务包和组织样例**中的**装入样例服务包**。）

如果仅使用样例模板来向用户和组分配服务包，则不需要执行任何操作。

自定义服务包

配置程序不会升级在 6 2005Q4 版本中创建的自定义服务包。您必须手动升级自定义服务包。

有关如何创建自定义服务包的信息，请参见第 74 页中的 “创建您自己的服务包”。

▼ 升级自定义服务包的步骤

对 LDAP 目录执行以下操作：

1 将您的服务包模板从此目录节点：

`o=cosTemplates,o=`*rootsuffix*

复制到此目录节点：

`o=`*service_target*`,o=cosTemplates,o=`*rootsuffix*

其中 *service_target* 为下列之一：

```
mailuser
calendaruser
mailcalendaruser
mailgroup
```

例如，如果某个服务包模板名为 `myservicepackage`，并且向用户提供邮件服务，则服务包模板的新 `dn` 应为：

`o=myservicepackage,o=mailuser,o=cosTemplates,o=`*rootsuffix*

2 从如下的原始目录节点删除服务包模板的条目：

`o=cosTemplates,o=`*rootsuffix*

3 通过将以下行添加到用于定义服务包的 ldif 文件来编辑每个自定义服务包：

`daServiceType:` *service type target*

注 – 如果您的 ldif 文件已经包含 `daServiceType` 属性，可跳过此步骤。

`daServiceType` 属性定义服务包提供的服务类型和服务包的服务目标。

service 可以是 `mail` 或 `calendar`。

target 可以是 `users` 或 `groups`。

例如：

```
daServiceType: mail user
```

以下示例显示了编辑后的 ldif 文件的外观：

```
dn: cn=myservicepackage,o=mailuser,o=cosTemplates,o=mycompanysuffix
changetype: modify
replace: daServiceType
daServiceType: mail user
```

更多信息 **使用 LDAP 目录工具 `ldapmodify` 来更新目录中的服务包。**

例如，可以运行以下命令：

```
ldapmodify -D <directory manager> -w <password> -f myservicepackagemodldif
```

其中

`<directory manager>` 是 Directory Server 管理员的名称。

`<password>` 是 Directory Server 管理员的密码。

`myservicepackagemodldif` 是包含之前步骤所述修改的 ldif 文件的名称。

选择要配置的组件

配置程序中的第三个面板会询问您要配置哪些 Delegated Administrator 组件：

- **Delegated Administrator 实用程序（客户机）**—使用 `commadmin` 调用的命令行界面。
- **Delegated Administrator 服务器**—运行 Delegated Administrator 实用程序和控制台必需的 Delegated Administrator 服务器组件。
- **Delegated Administrator 控制台**—Delegated Administrator 图形用户界面 (Graphical User Interface, GUI)。

配置程序将根据您选择的组件显示不同的面板。

以下步骤对配置选项进行了概要介绍。每个摘要步骤（如下）可链接到本章后面的一节，该部分逐步介绍了配置面板的实际情况。

▼ 配置选项摘要

1. **第 57 页中的“ 开始进行配置 ”**
   输入这些面板中请求的信息，从而开始进行配置。

2. **第 58 页中的“ 配置 Delegated Administrator 实用程序 ”**
   这些面板紧跟在**选择要配置的组件**面板后面。它们将请求用于配置 Delegated Administrator 实用程序的信息。

   - 标准方法是将 Delegated Administrator 实用程序和其他两个组件（服务器和控制台）配置在同一台计算机上。

     必须在所有要安装 Delegated Administrator 服务器的计算机上都配置 Delegated Administrator 实用程序 。
   - 也可以在单独的计算机上配置 Delegated Administrator 实用程序和控制台。在要配置实用程序和控制台的计算机上，只能在**选择要配置的组件**面板中选择这些组件。

在这种情况下，必须在要配置服务器的计算机上再次运行配置程序。

3 **第 59 页中的 “ 配置 Delegated Administrator 控制台 ”**

这些面板出现在用于配置实用程序的面板后面。

您可以选择是否配置 Delegated Administrator 控制台。

- 如果将 Delegated Administrator 控制台和服务器配置在同一台计算机上，则应当在**选择要配置的组件**面板中同时选择控制台和服务器。
- 也可以将 Delegated Administrator 控制台和服务器配置在不同的计算机上。

  在要配置控制台的计算机上，只能在**选择要配置的组件**面板中选择控制台。此实用程序默认为选定，请确保它保持选定状态。

  在这种情况下，必须在要配置服务器的计算机上再次运行配置程序。

  如果将控制台和服务器配置在不同的计算机上，则在**两台**计算机上都要配置此实用程序。

根据您为控制台选择的 Web 容器，配置程序将显示不同的面板。您可以部署到以下 Web 容器之一：

- Sun Java System Web Server 6.*x*
- Sun Java System Web Server 7.*x*
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

如果将 Delegated Administrator 服务器和控制台配置在同一计算机上，则要按上述说明操作**两次**（一次针对服务器，一次针对控制台）。

4 **第 65 页中的 “ 配置 Delegated Administrator 服务器 ”**

这些面板出现在用于配置控制台的面板后面。

您可以选择是否在给定的计算机上配置 Delegated Administrator 服务器。

如果选择不在给定计算机上配置该服务器，配置程序将警告您必须在另一台计算机上配置该服务器。要运行实用程序和控制台，该服务器组件是必需的。

部署该服务器时的其他所有注意事项与部署控制台时的注意事项（如第 59 页中的 “配置 Delegated Administrator 控制台”中所述）相同。

注 – Delegated Administrator 服务器与 Access Manager 使用同一 Web 容器。配置程序会在请求 Access Manager 基本目录后请求 Web 容器信息。

---

5 **第 67 页中的 “ 完成配置 ”**

输入这些面板中请求的信息，从而完成配置。

运行配置程序

本节中介绍的步骤将指导您逐步配置 Delegated Administrator。

启动配置程序

要运行配置程序，请作为（或成为）超级用户来登录，并转到 `/opt/SUNWcomm/sbin` 目录。然后输入以下命令：

```
# ./config-commda
```

运行 `config-commda` 命令之后，就会启动配置程序。

配置程序控制台会显示当前 Delegated Administrator 产品的版本：6.4。

以下几节将逐步向您介绍各个配置面板。

开始进行配置

必须输入第一批配置程序面板中请求的信息。

▼ 开始进行配置的步骤

1 欢迎

配置程序中的第一个面板为版权页。单击**下一步**继续或单击**取消**退出。

2 选择用于存储配置和数据文件的目录

选择要用来存储 Delegated Administrator 配置和数据文件的目录。默认的配置目录为 `/var/opt/SUNWcomm`。此目录应当与 *da-base* 目录（默认为 `/opt/SUNWcomm`）分开。

输入此目录的名称，或保留默认名称，然后单击**下一步**继续。

如果指定的目录不存在，将会出现一个对话框，询问您是要创建该目录还是选择一个新目录。单击**创建目录**以创建目录或**选择新目录**以输入一个新目录。

将出现一个对话框，指出正在装入组件。这可能需要几分钟的时间。

3 选择要配置的组件

在“组件”面板上选择一个或多个要配置的组件。

- **Delegated Administrator 实用程序（客户机）**—使用 `commadmin` 调用的命令行界面。此组件是必需的组件，默认情况下处于选定状态。无法取消选定该组件。
- **Delegated Administrator 服务器**—运行 Delegated Administrator 控制台必需的 Delegated Administrator 服务器组件。

- **Delegated Administrator 控制台**—Delegated Administrator 图形用户界面 (Graphical User Interface, GUI)。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

有关如何选择组件的详细信息，请参见第 55 页中的 “选择要配置的组件”

如果选择不配置 Delegated Administrator 服务器，则会出现一个对话框，提醒您注意必须在另一台计算机上配置 Delegated Administrator 服务器。必须配置该服务器才能使用 Delegated Administrator 实用程序和控制台。

配置 Delegated Administrator 实用程序

必须在所有要安装 Delegated Administrator 组件（服务器或控制台）的计算机上都配置 Delegated Administrator 实用程序 。

▼ 配置 Delegated Administrator 实用程序的步骤

1 Access Manager 主机名和端口号

输入 Access Manager 主机名和端口号。如果要安装 Delegated Administrator 服务器组件，则必须将其与 Access Manager 安装在同一台主机上。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或又单击**取消**退出。

2 默认域

输入顶级管理员的默认域。在执行 `commadmin` 命令行实用程序时，如果没有通过 `-n` 选项显式指定某个域，则使用此域。它也称为默认组织。如果目录中不存在指定的域，将会创建该域。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

3 默认的客户机 SSL 端口

输入 Delegated Administrator 实用程序使用的默认 SSL 端口。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

4 如果选择仅配置 Delegated Administrator 实用程序 ，请转至

第 67 页中的 “完成配置”

如果选择配置 Delegated Administrator 控制台和服务器，或者选择仅配置该控制台，请转至

第 59 页中的 “配置 Delegated Administrator 控制台”

如果选择仅配置 Delegated Administrator 服务器（以及必需的 Delegated Administrator 实用程序），请转至

第 65 页中的 “配置 Delegated Administrator 服务器”

配置 Delegated Administrator 控制台

现在，配置程序将显示以下面板：

为 Delegated Administrator 选择 Web 容器

选择部署 Delegated Administrator 控制台所基于的 Web 容器。可以基于以下组件来配置 Delegated Administrator

- Sun Java System Web Server 6.*x*
- Sun Java System Web Server 7.*x*
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

此面板以及接下来的几个面板用于收集有关 Delegated Administrator 控制台的 Web 容器的信息。请按照相应部分中的说明执行操作：

- 第 59 页中的 “Web Server 6.*x* 配置”
- 第 61 页中的 “Web Server 7.*x* 配置”
- 第 62 页中的 “Application Server 7.*x* 配置”
- 第 63 页中的 “Application Server 8.*x* 配置”

可以基于两个不同的 Web 容器、两个不同的 Web 容器实例或同一个 Web 容器来部署 Delegated Administrator 控制台和服务器。

如果选择在面板 3 中配置 Delegated Administrator 控制台和 Delegated Administrator 服务器，则另一系列的面板将会请求有关该服务器的 Web 容器的信息。

因此，您会两次看到 Web 容器配置面板。请按照相应的说明来部署每个 Delegated Administrator 组件。

当您完成 Web 容器配置面板后，执行下列操作之一：

- 如果选择配置 Delegated Administrator 控制台和服务器，请转至
  第 65 页中的 “配置 Delegated Administrator 服务器”
- 如果选择仅配置 Delegated Administrator 控制台（以及必需的 Delegated Administrator 实用程序），请转至
  第 67 页中的 “完成配置”

Web Server 6.*x* 配置

如果要在 Web Server 6.*x* 上部署 Delegated Administrator 服务器或控制台，请按照本节所述的步骤进行操作。

▼ 配置 Web Server 6.*x*

1 Web Server 6.x 配置详细信息

此面板文本用于告知您是在为 Delegated Administrator 服务器还是控制台提供 Web Server 6.*x* 配置信息。

输入 Web Server 6.*x* 的根目录。可以通过浏览来选择该目录。

输入 Web Server 6.*x* 实例标识符。可用 *host.domain* 名（例如 `west.sesta.com`）来指定此标识符。

输入虚拟服务器标识符。可以用 `https-`*host.domain* 名（例如 `https-west.sesta.com`）来指定。

有关 Web Server 6.*x* 实例标识符和虚拟服务器标识符的详细信息，请参见 Web Server 文档。

Web Server 6.*x* 实例的相关文件存储在 Web Server 6.*x* 安装目录下的 `https-`*host*`.`*domain* 目录中，例如 `/opt/SUNWwbsvr/https-west.sesta.com`。

输入指定的虚拟服务器侦听的 HTTP 端口号。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

配置程序将检查您指定的值是否有效。如果某个目录或标识符无效或不存在，将会出现一个对话框，通知您选择新值。

然后，配置程序将检查 Web Server 6.*x* 实例连接是否处于活动状态。如果不是，将会出现一个对话框，警告您配置程序无法连接到指定的实例，配置可能无法完成。您可以接受指定的值，也可以选择新的 Web Server 6.*x* 配置值。

2 默认的域分隔符

此面板只有在配置 Delegated Administrator 控制台时才会显示。在配置控制台时需要使用域分隔符；此信息与 Web 容器无关。

输入用于在用户登录时进行验证的默认域分隔符。例如：`@`。

域分隔符值包含在 `daconfig.properties` 文件中。可以在运行配置程序之后编辑此属性值。有关详细信息，请参见第 4 章。

3 如果配置 Delegated Administrator 控制台，请执行下列操作之一：

- 如果选择配置 Delegated Administrator 控制台和服务器，请转至
  第 65 页中的 “配置 Delegated Administrator 服务器”
- 如果选择仅配置 Delegated Administrator 控制台（以及必需的 Delegated Administrator 实用程序），请转至
  第 67 页中的 “完成配置”

如果要配置 Delegated Administrator 服务器：

请转至

第 65 页中的 “配置 Delegated Administrator 服务器”中的步骤 3。

Web Server 7.*x* 配置

如果要在 Web Server 7.*x* 上部署 Delegated Administrator 服务器或控制台，请按照本节所述的步骤进行操作。

▼ 配置 Web Server 7.*x*

1 Web Server 7.x 配置详细信息

此面板文本用于告知您是在为 Delegated Administrator 服务器还是控制台提供 Web Server 7.*x* 配置信息。

输入 Web Server 7.*x* 服务器的根目录。Web Server 软件文件将安装到此目录中。可以通过浏览来选择该目录。默认值为 `/opt/SUNWwbsvr7`。

输入 Web Server 7.*x* 配置的根目录。Web Server 配置文件将安装到此目录中。可以通过浏览来选择该目录。默认值为 `/var/opt/SUNWwbsvr7`。

输入 Web Server 7.*x* 实例标识符。可用 *host.domain* 名（例如 `west.sesta.com`）来指定。

输入虚拟服务器标识符。可用 *host.domain* 名（例如 `west.sesta.com`）来指定。

有关 Web Server 7.*x* 实例标识符和虚拟服务器标识符的详细信息，请参见 Web Server 文档。

Web Server 7.*x* 实例的相关文件存储在 Web Server 7.*x* 安装目录下的 `https-`*host*`.`*domain* 目录中，例如 `/var/opt/SUNWwbsvr7/https-west.sesta.com`。

输入指定的虚拟服务器侦听的 HTTP 端口号。例如：`80`。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

配置程序将检查您指定的值是否有效。如果某个目录或标识符无效或不存在，将会出现一个对话框，通知您选择新值。

然后，配置程序将检查 Web Server 7.*x* 实例连接是否处于活动状态。如果不是，将会出现一个对话框，警告您配置程序无法连接到指定的实例，配置可能无法完成。您可以接受指定的值，也可以选择新的 Web Server 7.*x* 配置值。

2 Web Server 7.x：管理实例详细信息

输入 Administration Server 端口号。例如：`8800`

输入 Administration Server 管理员的用户 ID。例如：`admin`

输入管理员的用户密码。

如果要使用安全的 Administration Server 实例，应选中**安全 Administration Server 实例**框。如果不需要使用安全实例，则将此框保留为未选中状态。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

3 **默认的域分隔符**

此面板只有在配置 Delegated Administrator 控制台时才会显示。在配置控制台时需要使用域分隔符；此信息与 Web 容器无关。

输入用于在用户登录时进行验证的默认域分隔符。例如：`@`。

域分隔符值包含在 `daconfig.properties` 文件中。可以在运行配置程序之后编辑此属性值。有关详细信息，请参见第 4 章。

4 **如果配置 Delegated Administrator 控制台，请执行下列操作之一：**

- 如果选择配置 Delegated Administrator 控制台和服务器，请转至
  第 65 页中的 “配置 Delegated Administrator 服务器”
- 如果选择仅配置 Delegated Administrator 控制台（以及必需的 Delegated Administrator 实用程序），请转至
  第 67 页中的 “完成配置”

如果要配置 Delegated Administrator 服务器：

请转至

第 65 页中的 “配置 Delegated Administrator 服务器”中的步骤 3。

Application Server 7.*x* 配置

如果要在 Application Server 7.*x* 上部署 Delegated Administrator 服务器或控制台，请按照本节所述的步骤进行操作。

▼ 配置 Application Server 7.*x* 的步骤

1 **Application Server 7.x 配置详细信息**

此面板文本用于告知您是否在为 Delegated Administrator 服务器或控制台提供 Application Server 7. *x* 配置信息。

输入 Application Server 安装目录。默认情况下，此目录为 `/opt/SUNWappserver7`。

输入 Application Server 域目录。默认情况下，此目录为 `/var/opt/SUNWappserver7/domains/domain1`。

输入 Application Server 文档根目录。默认情况下，此目录为 `/var/opt/SUNWappserver7/domains/domain1/server1/docroot`。

可以通过浏览来选择这些目录中的任何一个。

输入 Application Server 实例名称。例如：`server1`。

输入 Application Server 虚拟服务器标识符。例如：`server1`。

输入 Application Server 实例的 HTTP 端口号。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或又单击**取消**退出。

配置程序将检查您指定的目录是否有效。如果某个目录无效或不存在，将会出现一个对话框，通知您选择新目录。

然后，配置程序将检查 Application Server 实例连接是否处于活动状态。如果不是，将会出现一个对话框，警告您配置程序无法连接到指定的实例，配置可能无法完成。您可以接受指定的值，也可以选择新的 Application Server 配置值。

2 Application Server 7.x：管理实例详细信息

输入 Administration Server 端口号。例如：`4848`

输入 Administration Server 管理员的用户 ID。例如：`admin`

输入管理员的用户密码。

如果要使用安全的 Administration Server 实例，应选中**安全 Administration Server 实例**框。如果不需要使用安全实例，则将此框保留为未选中状态。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

3 默认的域分隔符

此面板只有在配置 Delegated Administrator 控制台时才会显示。在配置控制台时需要使用域分隔符；此信息与 Web 容器无关。

输入用于在用户登录时进行验证的默认域分隔符。例如：`@`。

4 如果配置 Delegated Administrator 控制台，请执行下列操作之一：

- 如果选择配置 Delegated Administrator 控制台和服务器，请转至
  第 65 页中的 “配置 Delegated Administrator 服务器”
- 如果选择仅配置 Delegated Administrator 控制台（以及必需的 Delegated Administrator 实用程序），请转至
  第 67 页中的 “完成配置”

如果要配置 Delegated Administrator 服务器：

请转至

第 65 页中的 “配置 Delegated Administrator 服务器”中的步骤 3。

Application Server 8.*x* 配置

如果要在 Application Server 8.*x* 上部署 Delegated Administrator 服务器或控制台，请按照本节所述的步骤进行操作。

▼ 配置 Application Server 8.*x* 的步骤

1 Application Server 8.x 配置详细信息

此面板文本用于告知您是否在为 Delegated Administrator 服务器或控制台提供 Application Server 8. *x* 配置信息。

输入 Application Server 安装目录。默认情况下，此目录为 `/opt/SUNWappserver/appserver`。

输入 Application Server 域目录。默认情况下，此目录为 `/var/opt/SUNWappserver/domains/domain1`。

输入 Application Server 文档根目录。默认情况下，此目录为 `/var/opt/SUNWappserver/domains/domain1/docroot`。

可以通过浏览来选择这些目录中的任何一个。

输入 Application Server 目标名称。例如：`server`。

输入 Application Server 虚拟服务器标识符。例如：`server`。

注 – 如果要运行 `config-commda` 程序升级 Delegated Administrator，而且已经将 Application Server 从版本 7 升级到版本 8.*x*，那么要为 Application Server 目标名称和虚拟服务器标识符指定以下值：

- 目标名称：`server1`
- 虚拟服务器标识符：`server`

您必须指定这些值，因为 `asupgrade` 实用程序会将 Application Server 7 `server1` 实例迁移到运行在节点代理下的 Application Server 8.*x* `server1` 目标。但是，`asupgrade` 会将虚拟服务器的值从 Application Server 7 中的 `server1` 更改为 Application Server 8.*x* 中的 `server`。

输入 Application Server 目标的 HTTP 端口号。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

配置程序将检查您指定的目录是否有效。如果某个目录无效或不存在，将会出现一个对话框，通知您选择新目录。

然后，配置程序将检查 Application Server 目标连接是否处于活动状态。如果不是，将会出现一个对话框，警告您配置程序无法连接到指定的目标，配置可能无法完成。您可以接受指定的值，也可以选择新的 Application Server 配置值。

2 Application Server 8.x：管理实例详细信息

输入 Administration Server 端口号。例如：`4849`

输入 Administration Server 管理员的用户 ID。例如：`admin`

输入管理员的用户密码。

如果要使用安全的 Administration Server 实例，应选中**安全 Administration Server 实例**框。如果不需要使用安全实例，则将此框保留为未选中状态。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

3 **默认的域分隔符**

此面板只有在配置 Delegated Administrator 控制台时才会显示。在配置控制台时需要使用域分隔符；此信息与 Web 容器无关。

输入用于在用户登录时进行验证的默认域分隔符。例如：`@`。

4 **如果配置 Delegated Administrator 控制台，请执行下列操作之一：**

- 如果选择配置 Delegated Administrator 控制台和服务器，请转至
  第 65 页中的 “配置 Delegated Administrator 服务器”
- 如果选择仅配置 Delegated Administrator 控制台（以及必需的 Delegated Administrator 实用程序），请转至
  第 67 页中的 “完成配置”

如果要配置 Delegated Administrator 服务器：

请转至

第 65 页中的 “配置 Delegated Administrator 服务器”中的步骤 3。

配置 Delegated Administrator 服务器

如果您选择配置 Delegated Administrator 服务器，则配置程序将显示以下面板。

▼ 配置 Delegated Administrator 服务器的步骤

1 **Access Manager 基本目录**

输入 Access Manager 基本目录。默认目录为 `/opt/SUNWam`。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或又单击**取消**退出。

配置程序将检查指定的 Access Manager 基本目录是否有效。如果无效，将会出现一个对话框，指出必须选择现有的 Access Manager 基本目录。

2 **然后，将显示 Web 容器的配置详细信息面板。**

如果选择了配置控制台和服务器，则这是第二次出现 Web 容器的**配置详细信息**面板。

Delegated Administrator 服务器将与 Access Manager 部署到同一 Web 容器。（无法为 Delegated Administrator 服务器选择 Web 容器。）

请按照相应部分中的说明执行操作：

- 第 59 页中的 “Web Server 6.*x* 配置”
- 第 62 页中的 “Application Server 7.*x* 配置”
- 第 63 页中的 “Application Server 8.*x* 配置”

3 Directory (LDAP) Server

此面板将请求有关连接到 LDAP Directory Server 的信息来作为用户/组后缀。

在相应的文本框中输入用户和组 Directory Server LDAP URL (**LdapURL**)、Directory Manager（**绑定为**）以及密码。

Directory Manager 对 Directory Server 以及使用 Directory Server 的所有 Sun Java System 服务器（例如 Delegated Administrator）具有总体管理员权限，并对 Directory Server 中的所有条目具有完全管理权限。默认推荐的标识名 (Distinguished Name, DN) 为 `cn=Directory Manager`。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

4 Access Manager 顶级管理员

输入 Access Manager 顶级管理员的用户 ID 和密码。在安装 Access Manager 时会创建该用户 ID 和密码。默认的用户 ID 为 `amadmin`。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

5 Access Manager 内部 LDAP 验证密码

输入 Access Manager 内部 LDAP 验证用户的密码。

验证用户名被硬编码为 `amldapuser`。它由 Access Manager 安装程序创建，并且是 LDAP 服务的绑定 DN 用户。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

6 组织标识名 (Distinguished Name, DN)

输入默认域的组织 DN。例如，如果组织 DN 为 `o=siroe.com`，则该组织中的所有用户都将放在 LDAP DN `o=siroe.com, o=usergroup` 下，其中 `o=usergroup` 为根后缀。

默认情况下，配置程序会在 LDAP 目录中的根后缀下添加默认域。

如果要在根后缀处（而不是在其下）创建默认域，请从显示在**组织标识名 (Distinguished Name, DN)** 文本框中的 DN 中删除组织名称。

例如，如果组织 DN 为 `o=siroe.com`，根后缀为 `o=usergroup`，则从文本框内的 DN 中删除 `"o=siroe.com"`，仅保留 `o=usergroup`。

如果选择在根后缀处创建默认域，则以后决定使用托管域时，可能会很难迁移到托管域配置。`config-commda` 程序将会显示以下警告：

“您选择的组织 DN 是用户/组后缀。尽管这是一个有效选项，但当您决定使用托管域时，将很难进行迁移。如果您一定要使用托管域，请指定比用户/组后缀低一级的 DN。”

有关详细信息，请参见第 23 页中的 “支持单层结构的目录结构” 。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

7 默认组织的顶级管理员

为要在默认域（组织）中创建的顶级管理员输入用户 ID 和密码。

确认密码字段要求您再次输入该密码。

单击**下一步**继续，或单击**上一步**返回到前一个面板，或者单击**取消**退出。

8 服务包和组织样例

您可以选择向 LDAP 目录中添加样例服务包和样例组织。

装入样例服务包。如果要使用或修改样例服务包模板来创建您自己的服务类包，则选中此选项。

装入样例组织。如果要在 LDAP 目录树中包含样例提供商组织节点和下属组织节点，则选中此选项。

您可以选择

- 同时选中样例服务包和样例组织
- 仅选中其中一个选项
- 不选中任何选项

用于样例的首选邮件主机。输入安装了 Messaging Server 的计算机的名称。

例如：`mymachine.siroe.com`

如果选择将样例组织装入到 LDAP 目录中，则必须为这些样例输入首选邮件主机名。

有关服务包和组织的信息，请参见第 2 章： “Delegated Administrator 概述” 。

运行配置程序之后，必须修改服务包模板来创建您自己的服务类包。有关此配置后任务的信息，请参见第 74 页中的 “创建服务包” 。

完成配置

执行本节所述的步骤来完成配置程序。

▼ 完成配置的步骤

1 准备配置

验证面板会显示将要配置的项目。

单击**立即配置**开始进行配置，或单击**上一步**返回到前面任意一个面板以更改信息，或者单击**取消**退出。

2 **任务序列**

"任务序列"面板上会显示要执行的任务序列。此时将会实际开始进行配置。

当面板显示"所有任务已通过"时，您可以单击**下一步**继续或单击**取消**停止执行任务并退出。

将会出现一个对话框，提醒您要重新启动 Web 容器才能使配置更改生效。

3 **安装摘要**

"安装摘要"面板显示了安装的产品，并且具有**详细信息...**按钮，单击该按钮可显示有关此配置的详细信息。

将在 `/opt/SUNWcomm/install` 目录中创建 `config-commda` 程序的日志文件。该日志文件的名称为 `commda-config_`*YYYYMMDDHHMMSS*`.log`，其中 *YYYYMMDDHHMMSS* 标识了配置的年（4 位数）、月、日、小时、分钟和秒钟。

单击**关闭**以完成配置。

重新启动 Web 容器

完成 Delegated Administrator 配置后，必须重新启动将 Delegated Administrator 部署到的 Web 容器（以下之一）：

- Sun Java System Web Server 6.*x*
- Sun Java System Web Server 7.*x*
- Application Server 7.x
- Application Server 8.x

由 `config-commda` 程序部署的配置文件和日志文件

配置文件

通过使用您在面板中提供的信息，`config-commda` 程序将为三个 Delegated Administrator 组件部署以下配置文件：

- Delegated Administrator 实用程序：
  - `cli-usrprefs.properties`

    位置：*da-base*`/data/config`
- Delegated Administrator 服务器：
  - `resource.properties`
- Delegated Administrator 控制台：
  - `daconfig.properties`

- Resources.properties
- Security.properties
- logger.properties

  （logger.properties 文件指定日志文件的位置，以及是否启用日志记录。它是配置文件，不是日志文件。）

config-commda 程序会将配置文件部署到已部署 Delegated Administrator 的 Web 容器的应用程序系统信息库中。有关文件部署位置的列表，请参见第 90 页中的 “配置文件的部署位置”。

有关配置文件包含的属性以及如何编辑这些属性以自定义配置的信息，请参见第 4 章。

日志文件

Delegated Administrator 控制台会创建运行时日志文件：

默认日志文件名：da.log

默认位置：/opt/SUNWcomm/log

有关此日志文件以及其他 Delegated Administrator 日志文件的详细信息，请参见附录 C。

执行无提示安装

Delegated Administrator 实用程序初始运行时配置程序将会自动创建无提示安装状态文件（称为 saveState）。此文件包含有关配置程序的内部信息，用于运行无提示安装。

无提示安装 saveState 文件存储在 /opt/SUNWcomm/data/setup/commda-config_*YYYYMMDDHHMMSS*/ 目录中，其中 *YYYYMMDDHHMMSS* 标识了 saveState 文件的年（4 位数）、月、日、小时、分钟和秒钟。

例如，一旦运行了一次 config-commda 程序后，就可以在无提示安装模式下运行该程序：

```
da-base/sbin/config-commda -nodisplay -noconsole -state
 fullpath/saveState
```

fullpath 变量是 saveState 文件所在位置的完整目录路径。

运行 Delegated Administrator 控制台和实用程序

启动控制台

通过访问将 Delegated Administrator 控制台部署到的 Web 容器可启动该 Delegated Administrator 控制台。

▼ 启动 Delegated Administrator 控制台的步骤

1 **转至以下 url：**

`http://` *host*`:`*port*`/da`

其中

host 为 Web 容器主机

port 是 Web 容器端口

例如：

```
http://siroe.com:8080/da
```

Delegated Administrator 控制台登录窗口将会出现。

注 – 在以前版本的 Delegated Administrator 中，控制台是从以下 url 启动的：

`http://` *host*`:`*port*`/da/DA/Login`

在当前版本中可以继续使用此 url。

---

2 **登录到 Delegated Administrator 控制台。**

可以使用在 Delegated Administrator 配置程序中指定的顶级管理员 (Top-Level Administrator, TLA) 的用户 ID 和密码。此信息是在以下面板中请求的：

默认组织的顶级管理员

注 – 运行 Delegated Administrator 控制台时，可以使用在 Access Manager 中设置的值来确定会话超时值。有关会话超时值的信息，请参见 *Sun Java System Access Manager* **管理指南**中的“会话服务属性”。有关在 Access Manager 控制台中查看这些值的信息，请参见 *Sun Java System Access Manager* **管理指南**中的“当前会话”。

注 – 不要将浏览器设置为显示 JavaScript 控制台或弹出 JavaScript 错误。这样做会显示对 Delegated Administrator 控制台正常运转没有影响的 JavaScript 错误。要禁用 JavaScript 错误，执行以下步骤：

- 在 Internet Explorer 中，禁用以下选项：**工具** —> **Internet 选项** —> **高级** —> “显示每个脚本错误的通知”。
- 在 Mozilla 中，不要显式打开以下选项：**工具** —> **JavaScript 控制台**

运行命令行实用程序

可以通过在终端窗口中输入命令名称 `commadmin` 来运行 Delegated Administrator 实用程序。

▼ 运行命令行实用程序的步骤

1. **转至 *da-base*`/bin/` 目录。例如，转至 `/opt/SUNWcomm/bin/`。**
2. **输入 `commadmin` 命令。**

示例 3–1 使用 `commadmin` 搜索用户

以下命令将搜索 `varrius.com` 域中的用户：

```
commadmin user search -D chris -w bolton -d varrius.com -n sesta.com
```

有关此 `commadmin` 命令的详细信息，请参见 第 151 页中的 “commadmin user search”。

更多信息 `commadmin` 返回码

提示 – 当 `commadmin` 操作成功时，命令行将显示“确定”消息。

如果操作失败，则显示以下消息：

```
FAIL
<message>
```

其中 <*message*> 显示错误文本。

配置后任务

运行 Delegated Administrator 配置程序之后，应执行以下任务：

仅当在 Schema 2 兼容性模式下使用 LDAP 目录时，才需执行以下任务：

向默认域添加邮件服务和日历服务

`config-commda` 程序会创建一个默认域。

如果要在该默认域中创建具有邮件服务或日历服务的用户，首先必须向该域添加邮件服务和日历服务。

要执行此任务，请使用带有 `-S mail` 和 `-S cal` 选项的 `commadmin domain modify` 命令。

以下示例显示了如何使用 `commadmin domain modify` 来向默认域添加邮件服务和日历服务：

```
commadmin domain modify -D chris -w bolton -n sesta.com -d siroe.com
 -S mail,cal -H test.siroe.com
```

有关 `commadmin` 命令的语法和详细信息，请参见第 5 章。

对邮件属性强制使用唯一值

Messaging Server 使用以下邮件属性来识别用户的电子邮件地址和备用邮件地址：

- `mail`
- `mailAlternateAddress`
- `mailEquivalentAddress`

每个用户的邮件属性在目录范围内应该是唯一的。

以下过程显示了如何修改 Directory Server ldif 文件来强制保证这些属性的唯一性。只要 Delegated Administrator（或任何 LDAP 工具）添加条目或修改邮件属性，ldif 插件就会检查邮件属性值是否唯一。如果操作会导致两个条目具有相同的邮件属性值，那么会终止该操作。

有关邮件属性的定义，请参见《Sun Java Communications Suite 5 Schema Reference》中的第 3 章 “Messaging Server and Calendar Server Attributes”。

▼ 强制邮件属性唯一性

开始之前

注 – 如果运行的是 Directory Server 5.2.5 (Java ES Release 4) 或更新版本，请遵循如下所述的过程。

如果运行的是 Directory Server 5.2.4 (Java ES Release 4)，则需要在开始以下过程之前应用 5.2_Patch_4_6313027 修补程序。

如果运行的是 Directory Server 的更早版本，则需要在开始之前升级到 Directory Server 5.2.5 或更新版本。

要访问 Directory Server 修补程序，转至 http://sunsolve.sun.com。

1. **创建一个文本文件，并写入以下内容。将文件中显示的参数替换为您的安装特定的值：**

```
dn: cn=Uniqueness in Attribute Set,cn=plugins,cn=config
objectClass: top
objectClass: nsSlapdPlugin
objectClass: ds-signedPlugin
objectClass: extensibleObject
cn: Uniqueness in Attribute Set
nssldap-pluginPath: server_root/lif/uid-plugin.so
nsslapd-pluginInitfunc: NSUniqueAttrSet_Init
nsslapd-pluginType: preoperation
nsslapd-pluginEnabled: on
nsslapd-pluginarg0: attributeset=mail,mailalternateaddress,mailequivalentaddress
nsslapd-pluginarg1: ugldapbasedn
nsslapd-plugin-depends-on-type: database
nsslapd-pluginId: NSUniqueAttrSet
nsslapd-pluginVersion: 5.2
nsslapd-pluginVendor: Sun Microsystems, Inc.
nsslapd-pluginDescription: Enforce unique values among an attribute set
```

   更改以下参数：

   将 *server_root* 替换为 Directory Server 安装目录的上一级目录。例如：`/var/opt/mps/serverroot`

   将 *ugldapbasedn* 替换为您的根后缀。此后缀下的所有条目都会执行唯一性检查。

2. **停止 Directory Server。**

3. **将您修改过的文本文件添加到 Directory Server `dse.ldif` 文件中。**

   `dse.ldif` 文件的位置：

   `dse.ldif` 文件位于以下目录：

   server_root`/slapd-`*machine_name*`/config`

其中

server_root 是 Directory Server 安装目录的上一级目录。例如：`/var/opt/mps/serverroot`

machine_name 是安装 Directory Server 的主机的名称。

添加文本文件的位置：

将文本文件添加到 `dse.ldif` 文件的 `uid uniqueness` 部分之后。此部分的第一行 (`dn`) 内容如下：

```
dn: cn=uid uniquenss,cn=plugins,cn=config
```

4 **重新启动 Directory Server。**

当 Directory Server 启动时，它会在目录中安装修改过的 `dse.ldif` 文件。

故障排除 如果 Directory Server 因为 `dse.ldif` 文件产生错误而没有启动，那么检查您用来替换范例文本文件中参数的值。您用来进行安装的 LDAP 根后缀、Directory Server 安装路径与主机必须正确无误。

如果 Directory Server 仍然没有启动，最后，您可以从 `dse.ldif` 文件中删除文本文件并重新启动 Directory Server。

创建服务包

使用 Delegated Administrator 在 LDAP 目录中置备的每个用户和组都应具有服务包。一个用户或组可以具有多个服务包。

预定义的服务类模板

在运行 Delegated Administrator 配置程序 (`config-commda`) 时，可以选择让 `config-commda` 程序在目录中安装服务类模板样例。

有关服务类模板样例以及服务包中的可用邮件属性的信息，请参见第 1 章中的第 27 页中的 “服务包”。

您可以使用服务类模板样例来创建和分配服务包；但是这些模板样例只是一些示例。

创建您自己的服务包

您很可能会需要根据自定义的服务类模板来创建自己的服务包，使属性值适用于您的安装中的用户和组。

要创建您自己的服务包，可使用存储在 `da.cos.skeleton.ldif` 文件中的服务类模板，它位于以下目录中：

da-base`/lib/config-templates`

此文件是专门作为编写自定义服务类模板时所用的模板而创建的。配置 Delegated Administrator 时，未在 LDAP 目录中安装此文件。

`da.cos.skeleton.ldif` 文件包含参数化模板，对应于 Delegated Administrator 所提供的每个服务类定义：

- `standardUserMail`
- `standardUserCalendar`
- `standardUserMailCalendar`
- `standardGroupMail`
- `standardGroupCalendar`
- `standardGroupMailCalendar`

您可以通过使用 `da.cos.skeleton.ldif` 文件中的一个或多个参数化模板来创建自己的服务类模板。

`da.cos.skeleton.ldif` 文件中的服务类模板如下：

```
# Templates for creating COS templates for service packages.
#
# There are six COS definitions :
#   standardUserMail
#   standardUserCalendar
#   standardUserMailCalendar
#   standardGroupMail
#   standardGroupCalendar
#   standardGroupMailCalendar
#
# Each definition can have zero or more COS templates which
# define specific values for the attributes listed in the
# COS definition.
#
# Each COS definition points to a corresponding subdirectory
# in which COS templates for that definition (and no other
# definition) are found.  The templates directory structure
# is as follows:
# standardUserMail          => o=mailuser,o=costemplates,<ugldapbasedn>
# standardUserCalendar      => o=calendaruser,o=costemplates,
#                              <ugldapbasedn>
# standardUserMailCalendar  => o=mailcalendaruser,o=costemplates,
#                              <ugldapbasedn>
# standardGroupMail          => o=mailgroup,o=costemplates,
#                              <ugldapbasedn>
# standardGroupCalendar      => o=calendargroup,o=costemplates,
#                              <ugldapbasedn>
# standardGroupMailCalendar => o=mailcalendargroup,o=costemplates,
#                              <ugldapbasedn>
#
```

```
# Thus, all COS templates for the user mail service are found in the
# o=mailuser,o=costemplates,<ugldapbasedn> directory, etc.
#
# It is not necessary to have any templates for a given definition.
# In that case default values are assumed for those attributes defined
# in the COS definition.
#
# If a template is created for a definition there should be at least
# one attribute with a defined value.
#
# Consult documentation for values for the attributes.
# Documentation includes units and default values.
#
# The finished COS derived from this skeleton is added to the
# directory with the following command:
#
# ldapmodify -D <directory manager> -w <password>
# -f <cos.finished.template.ldif>
#
#
############################################################
#
#    standardMailUser COS template
#
############################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
# - mailQuota
# - mailMsgQuota
# - mailAllowedServiceAccess
#
dn: cn=<service package name>,o=mailuser,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
mailQuota: <ma:ilQuotaValue>
mailMsgQuota: <mailMsgQuotaValue>
mailAllowedServiceAccess: <mailAllowedServiceAccessValue>
daServiceType: mail user#
#
############################################################
#
#    standardCalendarUser COS template
```

```
#
#############################################################
# There must be a least one of the following attributes:
# - icsPreferredHost
# - icsDWPHost
# - icsFirstDay
#
dn: cn=<service package name>,o=calendaruser,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
icsPreferredHost: <preferredHostValue>
icsDWPHost: <dwpHostValue>
icsFirstDay: <firstDayValue>
daServiceType: calendar user
#
#
#############################################################
#
#    standardMailCalendarUser COS template
#
#############################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
# - mailQuota
# - mailMsgQuota
# - mailAllowedServiceAccess
#
dn: cn=<service package name>,o=mailcalendaruser,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
mailquota: <mailQuotaValue>
mailmsgquota: <mailMsgQuotaValue>
mailAllowedServiceAccess: <mailAllowedServiceAccessValue>
daServiceType: calendar user
daServiceType: mail user
#
#
```

```
############################################################
#
#    standardMailGroup COS template
#
############################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
#
#
dn: cn=<service package name>,o=mailgroup,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
daServiceType: mail group
#
#
############################################################
#
#    standardCalendarGroup COS template
#
############################################################
# There must be a least one of the following attributes:
# - icsdoublebooking
# - icsautoaccept
#
#
dn: cn=<service package name>,o=calendargroup,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
icsdoublebooking: <doubleBookingValue>
icsautoaccept: <autoAcceptValue>
daServiceType: calendar group
#
#
############################################################
#
#    standardMailCalendarGroup COS template
#
```

```
#############################################################
# There must be a least one of the following attributes:
# - icsdoublebooking
# - icsautoaccept
# - mailMsgMaxBlocks
#
#
dn: cn=<service package name>,o=mailcalendargroup,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailmsgmaxblocks: <mailMsgMaxBlocksValue>
icsdoublebooking: <doubleBookingValue>
icsautoaccept: <autoAcceptValue>
daServiceType: calendar group
daServiceType: mail group
```

▼ 创建您自己的服务包的步骤

1 **复制并重命名** `da.cos.skeleton.ldif` **文件中的某一个参数化模板。**

安装了 Delegated Administrator 后，`da.cos.skeleton.ldif` 文件将被安装在以下目录中：

da-base`/lib/config-templates`

选择 `da.cos.skeleton.ldif` 文件中的以下模板之一来进行复制和重命名：

```
standardUserMail
standardUserCalendar
standardUserMailCalendar
standardGroupMail
```

2 **在模板副本中编辑以下参数：**

- `<ugldapbasedn>`

  将根后缀参数 `<rootSuffix>` 更改为您的根后缀（例如 `o=usergroup`）。

  `<ugldapbasedn>` 参数将显示在 DN 中。

- `<service package name>`

  将 `<service package name>` 参数更改为您自己的服务包名称。

  `<service package name>` 参数将显示在 DN 和 `cn` 中。

- 邮件属性值：

```
<mailMsgMaxBlocksValue>
<mailQuotaValue>
<mailMsgQuotaValue>
<mailAllowedServiceAccessValue>
```

编辑这些值使其符合您的特定要求。

例如，可以为邮件属性输入以下值：

```
mailMsgMaxBlocks: 400
mailQuota: 400000000
mailMsgQuota: 5000
mailAllowedServiceAccess: imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
```

- 日历属性值：

```
<preferredHostValue>
<dwpHostValue>
<firstDayValue>
```

这些参数代表 LDAP 属性 `icsPreferredHost`、`icsDWPHost` 和 `icsFirstDay` 的值。

编辑这些值使其符合您的特定要求。

有关这些属性的定义和说明，请参见 *Sun Java Communications Suite Schema Reference* 中的第 3 章 "Messaging Server and Calendar Server Attributes"。

在自定义的服务类模板中，必须至少使用一个属性；但不必在自定义模板中使用全部四个邮件属性。可以从服务包中删除一个或多个属性。

3 **使用 LDAP 目录工具 `ldapmodify` 将服务包安装到目录中。**

例如，可以运行以下命令：

```
ldapmodify -D <directory manager> -w <password> -f <cos.finished.template.ldif>
```

其中

`<directory manager>` 是 Directory Server 管理员的用户名。

`<password>` 是 Directory Server 管理员的密码。

`<cos.finished.template.ldif>` 是编辑的 ldif 文件的名称，该文件要作为服务包安装在目录中。

为 Schema 2 兼容性模式添加 ACI

如果要在 Schema 2 兼容性模式下使用 LDAP 目录，则必须手动向该目录中添加 ACI，以便能够在您的目录中置备 Delegated Administrator。请执行以下步骤：

▼ 为 Schema 2 兼容性模式添加 ACI

1 **将以下两个 ACI 添加到 OSI 根目录。可以在位于 `/opt/SUNWcomm/config` 目录中的 `usergroup.ldif` 文件中找到以下两个 ACI。**

请确保用您的用户组后缀来替换 `ugldapbasedn`。将编辑后的 `usergroup.ldif` 文件添加到 LDAP 目录中。

```
#
# acis to limit Org Admin Role
#
########################################
# dn: <local.ugldapbasedn>
########################################
dn: <ugldapbasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<ugldapbasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)

dn: <ugldapbasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<ugldapbasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read
to org node";
allow (read,search) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)
```

2 **将以下两个 ACI 添加到 DC 树根后缀。可以在位于 `/opt/SUNWcomm/lib/config-templates` 目录的 `dctree.ldif` 文件中找到以下两个 ACI。**

请确保用您的 DC 树根后缀来替换 *dctreebasedn*，用您的用户组后缀来替换 *ugldapbasedn*。将编辑后的 `dctree.ldif` 文件添加到 LDAP 目录中。

```
#
# acis to limit Org Admin Role
#
########################################
# dn: <dctreebasedn>
########################################
dn: <dctreebasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<dctreebasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access deny to dc node";
```

```
deny (write,add,delete) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)

dn: <dctreebasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<dctreebasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to dc
node"; allow (read,search) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)
```

3 **将以下附加 ACI 添加到 DC 树根后缀。（这些 ACI 不在 `dctree.ldif` 文件中。）**

```
dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS Proxy user rights"; allow (proxy)
userdn = "ldap:///cn=puser,ou=DSAME Users,<ugldapbasedn>";)

dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the
root suffix"; allow (all) userdn ="ldap:///cn=dsameuser,ou=DSAME
Users,<ugldapbasedn>";)

dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS Top-level admin rights";
allow (all) roledn = "ldap:///cn=Top-level Admin
Role,<ugldapbasedn>";)
```

4 **将 `AMConfig.properties` 文件中的 `com.iplanet.am.domaincomponent` 属性设置为您的 DC 树根后缀。**

例如，修改 <*AM_base_directory*>`/lib/AMConfig.properties` 文件中的以下行：

从

```
com.iplanet.am.domaincomponent=o=isp
```

改为

```
com.iplanet.am.domaincomponent=o=internet
```

5 **配置 Access Manager 以使用兼容性模式。**

在 Access Manager 控制台中，选中（启用）“管理控制台服务”页中的**启用域组件树**复选框。

6 **将 `inetdomain` 对象类添加到所有 DC 树节点（例如 `dc=com,o=internet`），如以下示例所示：**

```
/var/mps/serverroot/shared/bin 298% ./ldapmodify
-D "cn=Directory Manager" -w password
dn: dc=com,o=internet
changetype: modify
add: objectclass
objectclass: inetdomain
```

7 **重新启动 Web 容器。**

配置 Web Server 以在 SSL 模式下运行 Delegated Administrator

如果将 Delegated Administrator 控制台部署到 Web Server 6 或 Web Server 7.*x*，则您能够在 SSL 模式下通过安全端口运行 Delegated Administrator 控制台。

如果将 Delegated Administrator 服务器部署到 Web Server 6 或 Web Server 7.*x*，则您能够在 SSL 模式下运行 Delegated Administrator 实用程序 (`commadmin`)。

要使 Delegated Administrator 控制台和实用程序能够使用 SSL 访问：

- 对于控制台，完成在 SSL 配置过程中的所有步骤即可。
- 对于实用程序，只需完成 SSL 配置过程中的步骤 1 即可。使用 `commadmin` 命令及 `-s` 选项以在 SSL 模式下运行。

对于 Web Server 6，遵循以下过程：

- 第 84 页中的 “配置 Web Server 6 以使 Delegated Administrator 能在 SSL 模式下运行”

对于 Web Server 7.*x*，遵循以下过程：

- 第 86 页中的 “配置 Web Server 7.x 以使 Delegated Administrator 能在 SSL 模式下运行”

▼ 配置 Web Server 6 以使 Delegated Administrator 能在 SSL 模式下运行

在此过程中，会在 Delegated Administrator 配置目录中创建证书 truststore。例如 : `/var/opt/SUNWcomm/config`

1 请求并安装证书。

在生产环境中，必须从向您颁发证书的证书授权机构 (Certificate Authority, CA) 请求证书。然后安装该证书。

在测试环境中，可以创建并安装自签名的证书。

有关为 Web Server 6 请求和安装证书的信息，请参见《Sun Java System Web Server 6.1 SP6 Administrator's Guide》中的 "Using Certificates and Keys"。

完成此步骤后，即可在 SSL 模式下运行 Delegated Administrator 实用程序。

2 导出以 ASCII 编码的特定证书。

例如 :

```
/opt/SUNWwbsvr/bin/https/admin/bin/certutil -L -n Server-Cert -d \
-P https-host.domain-host-
/opt/SUNWwbsvr/alias -a > /tmp/host.cert
```

其中

- `Server-Cert` 是由管理界面创建的默认名称
- *host* 是运行 Web Server 6 的计算机的主机名称。例如 : `myhost`。
- *host.domain* 是运行 Web Server 6 的计算机的主机名和域名。例如 : `myhost.siroe.com`。

3 使用 java `keytool` 实用程序将证书导入到 truststore。

此步骤假设您在 Delegated Administrator 配置目录中创建了新的 truststore。

a. 导入证书。

例如 :

```
cd /var/opt/SUNWcomm/config

keytool -import -alias Server-Cert -file /tmp/host.cert
-keystore truststore
```

b. 当 `keytool` 提示您输入密码时，请输入密码。

4 **为 Web Server 6 实例配置定义 JVM 设置中的 `ssl.truststore` 属性。**

例如：

```
-Djavax.net.ssl.trustStore=/var/opt/SUNWcomm/config/truststore

Djavax.net.ssl.trustStorePassword=password
```

其中 *password* 是您在 `keytool` 提示时输入的密码。

5 **为 Web Server 6 实例配置修改以下 JVM 设置中的属性。**

将

```
-Djava.protocol.handler.pkgs=com.iplanet.services.comm
```

更改为以下值：

```
-Djava.protocol.handler.pkgs=com.sun.identity.protocol
```

6 **更改 `daconfig.properties` 文件中的以下属性：**

a. **在文本编辑器中打开 `daconfig.properties` 文件。**

`daconfig.properties` 文件默认保存在 Delegated Administrator 配置目录：

da-base/data/da/WEB-INF/classes/com/sun/comm/da/resources

（在稍后的步骤中，`daconfig.properties` 文件将被部署到 Web Server 6 配置目录。）

b. **如下所示更改属性值：**

```
commadminserver.host=host.domain

commadminserver.port=port

commadminserver.usessl=true
```

其中 *host.domain* 是运行 Web Server 6 的计算机的主机名和域名。例如：`myhost.siroe.com`。

其中 *port* 是 SSL 端口。例如：443。

7 **部署 Web Server 6 配置并重新启动实例：**

a. **运行 Web Server 6 部署脚本：**

```
/opt/SUNWcomm/sbin/config-wbsvr-da
```

b. **重新启动 Web Server 6 实例。**

▼ 配置 Web Server 7.x 以使 Delegated Administrator 能在 SSL 模式下运行

在此过程中，会在 Delegated Administrator 配置目录中创建证书 truststore。例如 `: /var/opt/SUNWcomm/config`

1 请求并安装证书。

在生产环境中，必须从向您颁发证书的证书授权机构 (Certificate Authority, CA) 请求证书。然后安装该证书。

在测试环境中，可以创建并安装自签名的证书。

有关为 Web Server 7.*x* 请求和安装证书的信息，请参见《Sun Java System Web Server 7.0 Administrator's Guide》中的"Managing Certificates"。

完成此步骤后，即可在 SSL 模式下运行 Delegated Administrator 实用程序。

2 运行 `certutil` 实用程序来列出证书数据库中的所有证书。

例如：

```
cd /var/opt/SUNWcomm/config

/usr/sfw/bin/certutil -L -d
/var/opt/SUNWwbsvr7/https-host.domain/config
```

其中 *host.domain* 是运行 Web Server 7.*x* 的计算机的主机名和域名。例如 `: myhost.siroe.com`

3 导出以 ASCII 编码的特定证书。

例如：

```
/usr/sfw/bin/certutil -L -n cert-host.domain -d
/var/opt/SUNWwbsvr7/https-host.domain/config
-a > host.cert
```

其中 *host* 和 *host.domain* 是运行 Web Server 7.*x* 的计算机的主机名或主机名和域名。

4 使用 java `keytool` 实用程序将证书导入到 truststore。

此步骤假设您在 Delegated Administrator 配置目录中创建了新的 truststore。

a. 导入该证书。

例如：

```
keytool -import -alias cert-host.domain -file host.cert
-keystore truststore
```

b. 当 `keytool` 提示您输入密码时，请输入密码。

5 **为 Web Server 7.*x* 实例配置定义 JVM 设置中的 `ssl.truststore` 属性。**

例如：

```
-Djavax.net.ssl.trustStore=/var/opt/SUNWcomm/config/truststore

-Djavax.net.ssl.trustStorePassword=password
```

其中 *password* 是您在 `keytool` 提示时输入的密码。

6 **为 Web Server 7.*x* 实例配置修改以下 JVM 设置中的属性。**

将

```
-Djava.protocol.handler.pkgs=com.iplanet.services.comm
```

更改为以下值：

```
-Djava.protocol.handler.pkgs=com.sun.identity.protocol
```

7 **更改 `daconfig.properties` 文件中的以下属性：**

a. **在文本编辑器中打开 `daconfig.properties` 文件。**

`daconfig.properties` 文件默认情况下位于 Delegated Administrator 配置目录：

da-base`/data/da/WEB-INF/classes/com/sun/comm/da/resources`

（在稍后的步骤中，将 `daconfig.properties` 文件部署到 Web Server 7.*x* 配置目录。）

b. **如下所示更改以下属性值：**

```
commadminserver.port=port

commadminserver.usessl=true
```

其中 *port* 是 SSL 端口。例如：443。

8 **部署 Web Server 7.*x* 配置并重新启动实例：**

a. **运行 Web Server 7.*x* 部署脚本：**

```
/opt/SUNWcomm/sbin/config-wbsvr7x-da
```

b. **重新启动 Web Server 7.*x* 实例。**

◆ ◆ ◆ 第 4 章

4 自定义 Delegated Administrator

当您利用配置程序 (`config-commda`) 安装和配置 Delegated Administrator 之后，可以根据需要自定义您的配置。本章提供了有关如何自定义 Delegated Administrator 某些功能的示例。

开始自定义配置之前，您应该对所有现有 Delegated Administrator 配置文件进行备份。

此外，在升级 Delegated Administrator 时也可能会丢失自定义配置数据。因此，在升级 Delegated Administrator 或重新运行 Delegated Administrator 配置程序之前，您也应该保存自定义配置。有关详细信息，请参见第 52 页中的 “保留现有配置”。

本章首先列出配置文件的位置，并说明如何将自定义文件重新部署到正确的位置。然后说明如何自定义特定的功能。包括以下主题：

部署自定义配置文件

当使用 `config-commda` 程序配置 Delegated Administrator 时，`config-commda` 会将配置文件保存在 Delegated Administrator 安装目录中的配置数据标准位置。然后，`config-commda` 程序将配置文件部署到已部署 Delegated Administrator 的 Web 容器的应用程序系统信息库中。

因此，配置文件的部署位置会根据您所使用的 Web 容器不同而各异。

在运行时，Delegated Administrator 使用配置文件的属性值，这些配置文件位于其部署位置——也就是部署 Delegated Administrator 的 Web 容器的系统信息库。

要自定义配置文件，执行以下步骤：

1. 编辑位于 Delegated Administrator 安装目录中的原始配置文件。
2. 使用 Delegated Administrator 提供的脚本将配置文件重新部署到 Web 容器。

自定义配置文件时，在将文件重新部署到 Web 容器之前，新值不会生效。

本节的剩余部分说明以下主题：

- 第 90 页中的 “配置文件的原始（标准）位置”
- 第 90 页中的 “配置文件的部署位置”
- 第 92 页中的 “部署自定义配置文件”
- 第 92 页中的 “配置文件部署脚本”

配置文件的原始（标准）位置

Delegated Administrator 配置完成后（在您运行 `config-commda` 程序之后），配置文件位于以下目录中：

- Delegated Administrator 实用程序：
  - `cli-usrprefs.properties`

    位置：*da-base*`/data/config`

    注：`cli-usrprefs.properties` 文件不会部署到 Web 容器。它保留在 Delegated Administrator 安装路径中。
- Delegated Administrator 服务器：
  - `resource.properties`

    位置：*da-base*`/data/WEB-INF/classes/sun/comm/cli/server/servlet`
- Delegated Administrator 控制台：
  - `daconfig.properties`
  - `Resources.properties`
  - `Security.properties`
  - `logger.properties`

    位置：*da-base*`/data/da/WEB-INF/classes/com/sun/comm/da/resources`

配置文件的部署位置

运行 `config-commda` 程序后，根据您所选的部署 Delegated Administrator 的 Web 容器，配置文件会部署到以下位置。

Delegated Administrator 服务器文件 (resource.properties) 的部署位置

将 resource.properties 文件部署到以下默认位置之一：

Web Server 6.*x*

```
/opt/SUNWwbsvr/https-hostname/webapps/https-hostname \
/commcli/WEB-INF/classes/sun/comm/cli/server/servlet
```

Web Server 7.*x*

```
/var/opt/SUNWwbsvr7/https-hostname/webapps/hostname \
/commcli/WEB-INF/classes/sun/comm/cli/server/servlet
```

Application Server 7.*x*

```
/var/opt/SUNWappserver7/domains/domain1/server1 \
/applications/j2ee-modules \
/commcli/WEB-INF/classes/sun/comm/cli/server/servlet
```

Application Server 8.*x*

```
/var/opt/SUNWappserver/domains/domain1 \
/applications/j2ee-modules \
/commcli/WEB-INF/classes/sun/comm/cli/server/servlet
```

Delegated Administrator 控制台配置文件的部署位置

以下文件部署到同一默认位置：

- daconfig.properties
- logger.properties
- Resources.properties
- Security.properties

根据您所选的部署 Delegated Administrator 的 Web 容器，这些属性文件会被部署到以下默认位置之一：

Web Server 6.*x*

```
/opt/SUNWwbsvr/https-hostname/webapps/https-hostname \
/da/WEB-INF/classes/com/sun/comm/da/resources
```

Web Server 7.*x*

```
/var/opt/SUNWwbsvr7/https-hostname/webapps/hostname \
/da/WEB-INF/classes/com/sun/comm/da/resources
```

Application Server 7.*x*

```
/var/opt/SUNWappserver7/domains/domain1/server1 \
/applications/j2ee-modules \
/Delegated_Administrator/WEB-INF \
/classes/com/sun/comm/da/resources
```

Application Server 8.*x*

```
/var/opt/SUNWappserver/domains/domain1 \
/applications/j2ee-modules \
/Delegated_Administrator/WEB-INF \
/classes/com/sun/comm/da/resources
```

▼ 部署自定义配置文件

1 **以超级用户身份（或成为超级用户）登录并转至以下目录：**

`/opt/SUNWcomm/sbin`

2 **运行适当的部署脚本将您的自定义配置文件重新部署到 Delegated Administrator 所使用的 Web 容器。**

必须将配置文件重新部署到上次运行 Delegated Administrator 配置程序 (`config-commda`) 将 Delegated Administrator 部署到的 Web 容器中。

使用可同时应用到您的自定义配置文件和正确的 Web 容器的部署脚本。

例如，要将 `resource.properties` 文件重新部署到 Web Server 6，运行此命令：

```
# ./config-wbsvr-commcli
```

有关部署脚本的列表，请参见第 92 页中的 “配置文件部署脚本”。

配置文件部署脚本

每个 Web 容器有两个部署脚本。一个脚本部署 Delegated Administrator 服务器文件。另一个部署 Delegated Administrator 控制台文件：

- Delegated Administrator 服务器配置文件：`resource.properties`。
- Delegated Administrator 控制台配置文件：`daconfig.properties`、`Security.properties`、`Resources.properties` 和 `logger.properties`。

部署脚本如下所示：

Web Server 6

- 适用于 Delegated Administrator 服务器文件 (`resource.properties`) 的部署脚本：

  `config-wbsvr-commcli`

- 适用于 Delegated Administrator 控制台文件的部署脚本：

  `config-wbsvr-da`

要运行脚本，输入以下命令：

```
# ./config-wbsvr-commcli
# ./config-wbsvr-da
```

Web Server 7.x

- 适用于 Delegated Administrator 服务器文件 (`resource.properties`) 的部署脚本：

  `config-wbsvr7x-commcli`

- 适用于 Delegated Administrator 控制台文件的部署脚本：

  `config-wbsvr7x-da`

要运行脚本，输入以下命令：

```
# ./config-wbsvr7x-commcli
# ./config-wbsvr7x-da
```

Application Server 7.x

- 适用于 Delegated Administrator 服务器文件 (`resource.properties`) 的部署脚本：

  `config-appsvr-commcli`

- 适用于 Delegated Administrator 控制台文件的部署脚本：

  `config-appsvr-da`

要运行脚本，输入以下命令：

```
# ./config-appsvr-commcli deploy
# ./config-appsvr-da deploy
```

必须使用参数 `deploy` 运行这些命令。

Application Server 8.x

- 适用于 Delegated Administrator 服务器文件 (`resource.properties`) 的部署脚本：

  ```
  config-appsvr8x-commcli
  ```

- 适用于 Delegated Administrator 控制台文件的部署脚本：

  ```
  config-appsvr8x-da
  ```

要运行脚本，输入以下命令：

```
# ./config-appsvr8x-commcli deploy
# ./config-appsvr8x-da deploy
```

必须使用参数 `deploy` 运行这些命令。

使用服务范围默认值配置首选邮件主机

如果要使用服务器范围的默认值来设置“首选邮件主机”和“首选邮件存储库”，可以执行本节中所述的任务。

如果需要从控制台（具体来讲，是从“新建组织”向导和“组织属性”屏幕）删除“首选邮件主机”字段，可以执行以下步骤：

- 编辑 `Security.properties` 文件。此步骤将在本节中进行介绍。
- 启用 MailHostStorePlugin。此步骤将在下一节第 96 页中的 “为 Delegated Administrator 添加插件”中进行介绍。

`Security.properties` 文件允许您为所有角色或个别角色自定义 Delegated Administrator 控制台。

▼ 从控制台删除首选邮件主机

1 将以下的内容添加到 `Security.properties` 文件中。

```
# Remove Preferred Mail Host from UI
*.NewOrganizationPage6.PreferredMailHostProperty=INVISIBLE
*.NewOrganizationSummaryPage.PreferredMailHostSummaryProperty=INVISIBLE
*.OrgProperties.MailHostName=INVISIBLE
*.OrgProperties.MailHostNameText=INVISIBLE
*.OrgProperties.MailHostValue=INVISIBLE
```

`Security.properties` 文件位于以下目录：

da-base/data/da/WEB-INF/classes/com/sun/comm/da/resources

注意：您可以向此文件中添加行以进行自定义，但是不能编辑已有的行。编辑现有的行会导致控制台中抛出异常。

2 **将编辑的 Security.properties 文件重新部署到 Delegated Administrator 控制台使用的 Web 容器。**

必须运行脚本将自定义 Security.properties 文件部署到您的 Web 容器，更改才会生效。

有关如何将自定义的属性文件部署到特定 Web 容器的说明，请参见第 92 页中的 “部署自定义配置文件”。

Security.properties 文件属性的语法和值

文件中的属性的格式为：*Security Element Name=Permission*

安全元素名的格式为：**角色名.容器视图名.控制台元素名**

安全元素指定了要定义其权限的控制台元素和角色。如果不知道元素名称，请查看页来源，以使该页上的名称与您所需的控制台元素相匹配。

页面上的名称是全限定名。您只需挑选名称的后两个元素，其格式为**容器视图名.控制台元素名**。

Delegated Administrator 的有效角色名如下：

"ProviderAdminRole" (SPA) 有关此角色的信息，请参见附录 A。

"OrganizationAdminRole" (OA)

"Top-levelAdminRole" (TLA)

"*"（将权限应用于所有角色，除非对于某一特定角色，该权限被忽略）

权限必须是以下字符串之一：

- EDITABLE–表示该安全元素可编辑。
- NONEDITABLE–表示该安全元素是只读的。
- VISIBLE–表示该安全元素可见并且是只读的。
- INVISIBLE–表示该安全元素不可见。

为 Delegated Administrator 添加插件

您可以自定义 Delegated Administrator 以支持以下插件：

- `MailHostStorePlugin`

  默认情况下禁用此插件。如果在创建了业务组织后没有提供 `preferredmailhost`，将会出现异常。如果禁用此插件，则仅当缺少相应属性时才会使用平面文件（本节后面对此进行了说明）中的值。

- `MailDomainReportAddressPlugin`

  可使用域值返回预期的 DSN 地址。默认实现将会返回字符串 `MAILER-DAEMON@<`*domain*`>`。

- `UidPlugin`

  可生成惟一 ID 字符串。默认实现将会生成 GUID 来返回到调用方。

启用插件

要启用这些插件，请编辑 `commcli servlet resource.properties` 文件，该文件位于以下目录：

```
da-base/data/WEB-INF/classes/sun/comm/cli/server/servlet/ \
resource.properties
```

（默认情况下，*da-base* 为 `/opt/SUNWcomm`。）

这些插件位于 `resource.properties` 文件中标题如下的部分：

```
########################
# Plugin Configuration #
########################
```

每个插件均带有 `"plugin"` 后缀。当前的列表如下所示：

```
jdapi-mailhoststoreplugin=disabled

jdapi-mailhoststorepluginclass=sun.comm.cli.server.util.MailHostStorePlugin
jdapi-mailhoststorepluginfile=/tmp/mailhostmailstore
jdapi-maildomainreportaddressplugin=enabled
jdapi-maildomainreportaddresspluginclass=sun.comm.cli.server.
  util.MailDomainReportAddressPlugin
jdapi-uidautogenerationplugin=disabled
jdapi-uidautogenerationpluginclass=sun.comm.cli.server.util.UidPlugin
```

在编辑 resource.properties 文件后，将它重新部署到 Delegated Administrator 服务器所使用的 Web 容器。

必须运行脚本将自定义 resource.properties 文件部署到您的 Web 容器，更改才会生效。

有关如何将自定义的属性文件部署到特定 Web 容器的说明，请参见第 92 页中的 “部署自定义配置文件” 。

插件格式

每个插件至少具有两行，其格式如下：

- jdapi-<*name*>plugin= "enabled" | "disabled"
-

```
jdapi-<name>pluginclass=sun.comm.cli.server.util/ \
<java class name>
```

要启用插件，请将 "disabled" 改为 "enabled"。

本节中列出的所有插件的插件类均已提供。这些类位于以下目录：

da-base/data/WEB-INF/classes/sun/comm/cli/server/util

您不需要对这些类进行任何操作。

MailHostStorePlugin 所需的其他平面文件

MailHostStorePlugin 需要另外一个平面文件，该文件将包含在插件的第三行中。插件将读取该平面文件中的值并使用该值来设置各个属性值。如果启用了此插件，则该文件必须存在，否则将发生错误。

-

```
jdapi-mailhoststoreplugin
    o jdapi-mailhoststorepluginginf=<full file name>
    o file has one line
    o value is that for :
        o preferredmailhost attribute
        o preferredmailmessagestore attribute
    o form
        o <mailhost>:<mailpartition>
```

创建 LDAP 对象时添加自定义对象类

您可以启用 Delegated Administrator 来向新的用户、组、资源或组织的 LDAP 条目中添加自定义类。要完成此任务，可自定义由 Access Manager 安装在目录中的相应的对象创建模板。

例如，BasicUser 创建模板决定了在创建新用户时要向用户条目中添加哪些对象类和属性。您可以利用自定义对象类来更新 BasicUser 创建模板。此后，该自定义对象类会与标准对象类一起添加到每个新的用户条目中。

以下过程说明了如何自定义 BasicUser 模板。您可以按照相同的过程来自定义 BasicGroup、BasicResource 和 BasicOrganization 创建模板。

▼ 在用户创建进程中添加自定义对象类

1 **请确保您在目录模式下定义了自定义对象类。**

2 **查找以下目录条目：**

```
ou=basicuser,ou=creationtemplates,ou=templates,ou=default,
ou=globalconfig,ou=1.0,ou=dai,ou=services,
o=$Root_Suffix
```

其中 *$Root_Suffix* 是您的目录的根后缀。

3 **将以下 *attribute:value* 添加到该条目中：**

```
sunkeyValue:required=objectClass=$Your_Custom_Objectclass.
```

其中 *$Your_Custom_Objectclass* 是您的自定义的对象类。

自定义用户登录帐户

当您运行 Delegated Administrator 配置程序 (`config-commda`) 时，用来登录到 Delegated Administrator 的值被设置为 `uid`。

例如，如果您打算作为 TLA 登录，而 TLA 的 `uid` 为 `john.doe`，那么就要使用 `john.doe` 登录到 Delegated Administrator。

您可以自定义 Delegated Administrator 以便能够使用其他值作为用户登录帐户。例如，可以添加邮件地址 (`mail`)。

如何设置用户登录帐户值

config-commda 程序可利用 resource.properties 文件中的 loginAuth-idAttr 属性将此值设置为 uid，如以下示例所示：

```
loginAuth-searchBase=<$rootSuffix>
servicepackage-cosdefbasedn = <$rootSuffix>
loginAuth-idAttr-1=uid
```

其中 <*$rootSuffix*> 是您的目录的根后缀。

添加用户登录帐户值

通过编辑 resource.properties 文件，您可以设置其他值来作为用户登录帐户。

resource.properties 文件所在的位置为

```
da-base/data/WEB-INF/classes/sun/comm/cli/server/servlet/ \
resource.properties
```

例如，要能够使用邮件地址（例如 john.doe@sesta.com）来登录，您可以向 resource.properties 文件中添加以下行：

```
loginAuth-searchBase=<$rootSuffix>
servicepackage-cosdefbasedn = <$rootSuffix>
loginAuth-idAttr-1=uid
loginAuth-idAttr-2=mail
```

其中 <*$rootSuffix*> 是您的目录的根后缀。

请注意，每个新的 loginAuth-idAttr 属性值必须是递增的。在本例中，添加的是第二个值，因此应向 loginAuth-idAttr 中添加 -2。

可以添加多个 loginAuth-idAttr 属性实例：

```
loginAuth-idAttr-1=uid
loginAuth-idAttr-2=mail
|
loginAuth-idAttr-n=<login-in value>
```

在编辑 resource.properties 文件后，将它重新部署到 Delegated Administrator 服务器所使用的 Web 容器。

必须运行脚本将自定义 resource.properties 文件部署到您的 Web 容器，更改才会生效。

有关如何将自定义的属性文件部署到特定 Web 容器的说明，请参见第 92 页中的 “部署自定义配置文件” 。

要求为新用户指派服务包

默认情况下，Delegated Administrator 允许您创建新用户而不为该用户指派服务包。

您可以更改默认设置，以便要求必须为每个新用户至少指派一个服务包。

▼ 要求为新用户指派服务包的步骤

1 **在一个文本编辑器中打开 `daconfig.properties` 文件。**

`daconfig.properties` 文件默认情况下位于以下目录：

da-base`/data/da/WEB-INF/classes/com/sun/comm/da/resources`

2 **将 `user.atleastOneServicePackage` 属性值从 `false` 改为 `true`。**

默认情况下，此值为 `false`。

例如：

```
user.atleastOneServicePackage=true
```

将此值设置为 `true` 之后，当使用 Delegated Administrator 控制台中的“创建新用户”向导时，就必须为成功创建的新用户至少指派一个服务包。

3 **将编辑的 `daconfig.properties` 文件重新部署到 Delegated Administrator 控制台所使用的 Web 容器。**

必须运行脚本将自定义 `daconfig.properties` 文件部署到您的 Web 容器，更改才会生效。

有关如何将自定义的属性文件部署到特定 Web 容器的说明，请参见第 92 页中的 “部署自定义配置文件” 。

添加新的日历时区

您可以通过添加新的 Calendar Server 时区来自定义 Delegated Administrator。这样，Delegated Administrator 就可以使用该新时区来置备组织、用户、组和资源。

要添加新时区，执行以下任务。要使用 Delegated Administrator 实用程序管理新时区，仅执行第一个任务。要通过 Delegated Administrator 控制台管理新时区，必须执行两个任务。

- 第 101 页中的 “在 Delegated Administrator 中添加新时区的步骤”
- 第 102 页中的 “在 Delegated Administrator 控制台中显示和管理新时区”

时区添加之后，可通过执行以下任务，将它设置为新创建用户的默认时区：

- 第 104 页中的 “更改 Delegated Administrator 中的默认时区的步骤”

▼ 在 Delegated Administrator 中添加新时区的步骤

必须执行此任务，您才能使用 `commadmin` 实用程序或 Delegated Administrator 控制台来按照新时区置备用户。此任务会用新时区值更新 Access Manager。此任务完成后，可使用 `commadmin` 将新时区指定给用户。

1 **在 Calendar Server 中添加新时区。**

要完成此步骤，必须编辑 `timezones.ics` 文件和其他 Calendar Server 文件。有关说明，请参见 Sun Java System Calendar Server 管理指南中 “管理 Calendar Server 的时区” 的 “添加新时区” 一节。

2 **备份 `UserCalendarService.xml` 和 `DomainCalendarService.xml` 文件。**

xml 文件默认情况下位于以下目录：

da-base`/lib/services`

3 **编辑 `UserCalendarService.xml` 和 `DomainCalendarService.xml` 文件以便在 Delegated Administrator 中添加新时区。**

- 在 `UserCalendarService.xml` 和 `DomainCalendarService.xml` 文件中，都找到以下条目标题：

```
<AttributeSchema name="icstimezone"
                            type="single choice"
                            syntax="string"
                            any="optional|adminDisplay">
                            <ChoiceValues>
```

- 将新时区值添加到 `<ChoiceValues>` 列表中。

4 **运行 Access Manager amadmin 实用程序以删除当前的服务并添加更新的服务。**

对 UserCalendarService.xml 和 DomainCalendarService.xml 文件都运行以下 amadmin 命令：

```
./amadmin -u <admin> -w <password> -r CalendarService

./amadmin -u <admin> -w <password>
-s da_base/lib/services/CalendarService.xml
```

其中 *CalendarService* 为 UserCalendarService 或 DomainCalendarService 之一。

注 – 如果您还打算将新时区设置为默认时区，则可以在执行上述两个任务之后运行这些 amadmin 命令。有关详细信息，请参见第 104 页中的 “更改 Delegated Administrator 中的默认时区的步骤”。

---

5 **重新启动您的 Web 容器以使所做的更改生效。**

6 **要使 Delegated Administrator 控制台能显示新时区，请参见第 102 页中的 “在 Delegated Administrator 控制台中显示和管理新时区”。**

▼ 在 Delegated Administrator 控制台中显示和管理新时区

此任务向控制台显示的时区列表中添加新时区。然后，此任务将在目录中保存新时区值。

要在控制台中显示时区，必须向 Resources.properties 文件添加新值。

要允许控制台在目录中存储时区，必须向 daconfig.properties 文件中的两个列表添加新值。第一个列表指定存储在 LDAP 目录中的实际值。第二个列表使控制台能够将时区的显示值（可能已本地化）映射到存储的值。

1 **编辑 Resources.properties 文件，该文件位于 Delegated Administrator 数据目录下。**

Resources.properties 文件默认情况下位于以下目录：

```
da-base/data/da/WEB-INF/classes/com/sun/ \
comm/da/resources
```

要编辑 Resources.properties，请搜索 rsrc.Timezone 属性并将新时区添加到相应的列表中。您可以本地化这个新时区的显示值。

2 **找到位于 Delegated Administrator 数据目录下的 daconfig.properties 文件中的时区值列表。**

daconfig.properties 文件默认情况下位于以下目录：

```
da-base/data/da/WEB-INF/classes/com/sun/ \
comm/da/resources
```

要查找时区值的列表，搜索以下内容：

```
#Timezone values - only English
```

这些是存储在 LDAP 目录中的值。新时区必须以英文书写，这是存储在目录中的值必需的格式。

3 **将新时区添加到列表。**

例如，要将 America/Miami 添加到列表，假设 Timezone1 目前有 24 个值，那么您应该添加

```
rsrc.Timezone1-25=America/Miami
```

此值将是显示在控制台中的 Americas 下拉列表中的第 25 个时区。注意，根据前述任务中您在 Resources.properties 文件中指定的内容不同，时区可能以别的语言显示。

4 **找到 daconfig.properties 文件中的反向时区映射列表。**

该列表提供了本地化时区值（在控制台中显示）与您在上述步骤 2 中指定的实际值的映射关系。

要查找反向映射的列表，搜索以下内容：

```
#reverse timezone mappings - used by DA in getting localized tz value
```

5 **向反向映射列表添加新值。**

例如，要将 America/Miami 添加到列表，您应该添加

```
rsrcKey-America-Miami=rsrc.Timezone1-25
```

6 **将编辑的 daconfig.properties 和 Resources.properties 文件重新部署到 Delegated Administrator 控制台所使用的 Web 容器。**

必须运行脚本将自定义 daconfig.properties 文件部署到您的 Web 容器，更改才会生效。

有关如何将自定义的属性文件部署到特定 Web 容器的说明，请参见第 92 页中的 “部署自定义配置文件” 。

编辑并重新部署 daconfig.properties 和 Resources.properties 文件后，新时区会显示在 Delegated Administrator 控制台中的相应列表框内。只要您在 Delegated Administrator 控制台中选择该时区并单击“保存”，它就会被保存在目录中。

▼ 更改 Delegated Administrator 中的默认时区的步骤

1 **在 `UserCalendarService.xml` 和 `DomainCalendarService.xml` 文件中，编辑以下值：**

```
<DefaultValues>
                <Value>America/Denver</Value>
</DefaultValues>
```

可以在 xml 文件中的以下条目下找到 `<DefaultValues>`：

```
<AttributeSchema name="icstimezone"
```

2 **运行 Access Manager `amadmin` 实用程序以删除当前的服务并添加更新的服务。**

对 `UserCalendarService.xml` 和 `DomainCalendarService.xml` 文件，运行以下 `amadmin` 命令：

```
./amadmin -u <admin> -w <password> -r DomainCalendarService

./amadmin -u <admin> -w <password>
-s da_base/lib/services/DomainCalendarService.xml
```

3 **重新启动您的 Web 容器以使所做的更改生效。**

防止新用户访问 Instant Messaging

如果已安装 Sun Java System Instant Messaging (IM)，并将其配置为使用 LDAP 存储用户属性，那么当 Delegated Administrator 创建新用户时，访问 IM 服务所必需的对象类会自动添加到该用户的 LDAP 条目。

可以阻止新用户在用户创建期间被授予必需的 IM 对象类。要做到这一点，可更改 Delegated Administrator 服务器的 `resource.properties` 文件中的一个属性值。

▼ 禁用新用户的 Instant Messaging 服务

1 **在文本编辑器中打开 `resource.properties` 文件。**

`resource.properties` 文件默认情况下位于 Delegated Administrator 安装路径中的原始（标准）位置：

da-base`/data/WEB-INF/classes/sun/comm/cli/server/servlet`

2 **将 `im-provision` 属性的值从 `true` 更改为 `false`。**

默认情况下，此值为 `true`。

例如：

```
im-provision=false
```

3 **将编辑的 `resource.properties` 文件重新部署到 Delegated Administrator 服务器使用的 Web 容器。**

必须运行脚本将自定义的 `resource.properties` 文件部署到您的 Web 容器，更改才会生效。

有关如何将自定义的属性文件部署到特定 Web 容器的说明，请参见第 92 页中的 “部署自定义配置文件” 。

◆ ◆ ◆ 第 5 章

5 命令行实用程序

Delegated Administrator 命令行实用程序使管理员能够针对用户、组、域和组织管理各种通信服务。本章将介绍用于执行批量操作（例如创建、修改、删除和搜索用户、组、域和组织）的命令行工具集。

命令

命令列在以下所示的表中。该表包含三列，第一列列出了命令，第二列列出了对命令的说明，第三列列出了允许执行该命令的管理员类型。

`commadmin` 实用程序位于 `/opt/SUNWcomm/bin` 目录中。

表 5–1 Delegated Administrator 命令行界面

命令	说明	有权执行*
第 110 页中的 “commadmin admin add”	向用户授予组织管理员权限	顶级管理员
第 112 页中的 “commadmin admin remove”	撤消用户的组织管理员权限	顶级管理员
第 113 页中的 “commadmin admin search”	搜索并显示具有组织管理员权限的用户	顶级管理员、组织管理员
第 114 页中的 “commadmin debug log”	创建调试日志	顶级管理员
第 115 页中的 “commadmin domain create”	创建域	顶级管理员
第 118 页中的 “commadmin domain delete”	删除域	顶级管理员
第 119 页中的 “commadmin domain modify”	修改域	顶级管理员

表 5–1 Delegated Administrator 命令行界面 （续）

命令	说明	有权执行*
第 121 页中的 “commadmin domain purge”	清除域	顶级管理员
第 126 页中的 “commadmin domain search”	搜索域	顶级管理员
第 127 页中的 “commadmin group create”	创建组	顶级管理员、组织管理员
第 130 页中的 “commadmin group delete”	删除组	顶级管理员、组织管理员
第 132 页中的 “commadmin group modify”	修改组	顶级管理员、组织管理员
第 136 页中的 “commadmin group search”	搜索组	任何人
第 137 页中的 “commadmin resource create”	创建资源	顶级管理员、组织管理员
第 141 页中的 “commadmin resource modify”	修改资源	顶级管理员、组织管理员
第 140 页中的 “commadmin resource delete”	删除资源	顶级管理员、组织管理员
第 142 页中的 “commadmin resource search”	搜索资源	任何人
第 144 页中的 “commadmin user create”	创建用户	顶级管理员、组织管理员
第 147 页中的 “commadmin user delete”	删除用户	顶级管理员、组织管理员
第 151 页中的 “commadmin user search”	搜索用户	任何人
第 149 页中的 “commadmin user modify”	修改用户	顶级管理员、组织管理员
*本版 Delegated Administrator 不支持服务提供商管理员使用 `commadmin` 实用程序。		

执行模式

命令行执行模式有三种：

- 使用在文件中指定的选项执行

  ```
  commadmin object task -i inputfile
  ```

  分析 *inputfile* 并执行该文件。
- 交互式执行

  ```
  commadmin object task
  ```

  可向管理员查询其他选项和属性。

- 立即执行或 shell 执行

```
commadmin object task [options]
```

如果 `commadmin` 操作成功，命令行将显示一条“确定”消息。

如果操作失败，则显示以下消息：

```
FAIL
<message>
```

其中 <*message*> 显示错误文本。

命令文件格式

通过使用 `-i` 选项可以在文件中指定选项。

在文件中，选项名称与选项值用空格来分隔。选项值是从第一个非空格字符到行尾字符之间的内容。各个选项集用空行来分隔。

常规语法为：

```
<选项名称><空格>[选项值，如果有]
<选项名称><空格>[选项值，如果有]
...
<选项名称><空格>[选项值，如果有]
<空行>
<选项名称><空格>[选项值，如果有]
<选项名称><空格>[选项值，如果有]
...
<选项名称><空格>[选项值，如果有]
```

命令行中给出的选项值将成为每个选项集的默认值；或者，也可以分别为每个选项集指定这些选项。该值将覆盖命令行上指定的任何默认值。

以下示例显示了用 `-i` 选项为 `commadmin user create` 命令指定的文件的格式和语法。

```
l newuser1
F new
L user1
W secret

l newuser2
F new
L user2
W secret
```

```
l newuser3
F new
L user3
W secret

<等等...>
```

命令说明

本节提供了命令行工具的说明、语法和示例。

强制性 commadmin 选项

以下是用于验证管理员或用户的强制性选项。

选项	说明
-D *userid*	用来绑定到目录的用户 ID。
-w *password*	用来验证绑定到目录的用户 ID 的密码。 还可以通过文本文件 *password*.txt 来指定 *password*。 例如，如果您指定 -w mypassword.txt，而 mypassword.txt 文件的内容是 secret，那么 commadmin 实用程序将字符串 secret 作为密码。 注意，如果您指定 -w mypassword.txt，而 mypassword.txt 文件不存在，那么 commadmin 实用程序将字符串 mypassword.txt 本身作为密码。
-n *domain*	管理员所属的域。（有关更多信息，参见本表格下面显示的**注**。）

安装过程中指定 Access Manager 主机 (-X)、Access Manager 端口 (-p) 和默认域 (-n) 的值，并存储在 cli-userprefs.properties 文件中。

注 – 如果在执行 commadmin 命令时没有指定-X、-p 和 -n 选项，则采用它们存储在 cli-userprefs.properties 文件中的值。

commadmin admin add

commadmin admin add 命令用于向用户授予对特定域的组织管理员权限。只有顶级管理员或 ISP 管理员才能执行此命令。

语法

```
commadmin admin add -D login -l login -n domain -w password -d domain [-h] [-i inputfile]
[-p AM port] [-X AM host] [-?] [-s] [-v] [-V]
```

选项

以下选项是强制性选项：

选项	说明
-D *login*	顶级管理员的用户 ID。
-l *login*	要向其授予组织管理权限的用户的用户 ID。该用户应当位于目录中，并且属于 -d 选项所指定的域。
-n *domain*	顶级管理员所属的域。如果没有指定，则使用存储在 cli-userprefs.properties 文件中的默认域。
-w *password*	顶级管理员的密码。
-d *domain*	要授予管理权限的域。如果没有指定，则使用 -n 选项所指定的域。

以下选项是非强制性选项：

选项	说明
-i *inputfile*	从文件中而不是命令行中读取命令信息。
-p *AM port*	使用此选项可指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*。
-h, -?	打印命令用法语法。
-V	打印关于该实用程序及其版本的信息。
-s	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
-v	启用调试输出。

示例

以下命令将向用户 ID 为 admin1 的用户授予组织管理员权限。

```
commadmin admin add -D chris -n sesta.com -w bolton -l admin1 \
-d florizel.com
```

以下命令将向域 `florizel.com` 中用户 ID 为 `admin2` 的用户授予组织管理员权限。

```
commadmin add admin -D chris -w bolton -l admin2 -n varrius.com \
-d florizel.com
```

commadmin admin remove

`commadmin admin remove` 命令用于撤消现有组织管理员的组织管理员权限。只有顶级管理员才能执行此命令。

要撤消多个用户的组织管理员权限，请使用 `-i` 选项。

语法

`commadmin admin remove -D` *login* `-l` *login* `-n` *domain* `-w` *password* `-d` *domain name* `[-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-X` *AM host*`] [-s] [-v] [-V]`

选项

以下选项是强制性选项：

选项	说明
`-D` *login*	顶级管理员的用户 ID。
`-l` *login*	要撤消其管理员权限的用户 ID。
`-n` *domain*	顶级管理员所属的域。
`-w` *password*	顶级管理员的密码。
`-d` *domain name*	要撤消管理员权限的域。如果没有指定 `-d`，则使用 `-n` 所指定的域。

以下选项是非强制性选项：

选项	说明
`-h, -?`	打印命令用法语法。
`-i` *inputfile*	从文件中而不是命令行中读取命令信息。

选项	说明
-p *AM port*	使用此选项可指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。
-s	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。

示例

以下命令将撤消用户 ID 为 admin5 的管理员的组织管理员权限：

```
commadmin admin remove -D chris -n sesta.com -w bolton -l admin5 -d test.com
```

commadmin admin search

commadmin admin search 命令用于搜索并显示某个域的特定或全部组织管理员。

语法

commadmin admin search -D *login* -n *domain* -w *password* [-l *login*] [-d *domain*]

选项

以下选项是强制性选项：

选项	说明
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	-D 选项所指定用户所属的域。
-w *password*	-D 选项所指定用户的密码。

以下选项是非强制性选项：

选项	说明
`-l` *login*	要搜索的组织管理员的用户 ID。如果没有指定 `-l`，或者与通配符一起指定了 `-l`（ `-l\\*` 或 `-l '*'`），将会显示该域的所有组织管理员。
`-d` *domain*	搜索对指定的域具有组织管理员权限的用户。如果没有指定 `-d`，则使用 `-n` 所指定的域。

示例

要搜索 `test.com` 域的所有组织管理员，可使用以下命令：

```
commadmin admin search -D chris -n sesta.com -w bolton -d test.com
```

commadmin debug log

`commadmin debug log` 命令创建 Delegated Administrator 服务器日志，其中包含由安装在 Web 容器中的 Delegated Administrator servlet 生成的调试语句。

语法

`commadmin debug log -D` *login* `-n` *domain* `-w` *password* `-t [ on|off ] -f` *path and file name*

选项

以下选项是强制性选项：

选项	说明
`-D` *login*	顶级管理员的用户 ID。
`-n` *domain*	顶级管理员所属的域。
`-t [ on|off ]`	在打开调试日志和关闭调试日志之间切换。 值 `on` 会导致服务器开始向日志写入调试语句。值 `off` 会导致服务器停止向日志写入调试语句。 如果您指定 `-t on` 以向现有日志文件写入调试日志记录，新的调试语句会附加到现有文件的末尾。
`-w` *password*	顶级管理员的密码。

以下选项是非强制性选项：

选项	说明

-f *path and file name*	创建日志的完整路径，包括日志的文件名。
	path 必须是以下两个目录之一：
	`/tmp/`
	`/var/tmp/`
	file name 可以为任意文件名。
	如果未指定 `-f` 选项，则默认值为 `/tmp/commcli.log`。

示例

要创建新的调试日志，输入以下命令：

```
commadmin debug log -D paul -n sesta.com -w bolton \
-t on -f /tmp/debug.log
```

要关闭对现有日志文件的日志记录，输入以下命令：

```
commadmin debug log -D paul -n sesta.com -w bolton \
-t off
```

关闭日志时无需指定文件名。

commadmin domain create

`commadmin domain create` 命令用于在 Access Manager 上创建单个域。要创建多个域，请使用 `-i` 选项。

语法

`commadmin domain create -D` *login* `-d` *domain name* `-n` *domain* `-w` *password* `[-A [+]` *attributename*`:`*value*`] [-h] [-?] [-i` *inputfile*`] [-o` *organization RDN*`] [-p` *AM port*`] [-s] [-v] [-V] [-X` *AM host*`] [-S mail -H` *preferred mailhost*`] [-S cal [-B` *backend calendar data server*`] [-C` *searchable domains*`] [-g` *access control string*`] [-P` *propertyname*`[:`*value*`]] [-R` *right*`[:`*value*`]] [-T` *calendar time zone string*`]]`

选项

以下选项是强制性选项：

选项	说明
-D *login*	顶级管理员的用户 ID。
-d *domain name*	要创建的域的 DNS 域名。
-n *domain*	顶级管理员所属的域。
-w *password*	顶级管理员的密码。

以下选项是非强制性选项：

选项	说明
-A [+]*attributename*: *value*	要修改的属性。*attributename* 以 LDAP 模式定义；所指定的 *value* 将替换目录中当前存在的此属性的所有值。重复此选项可同时修改多个属性，或者为同一属性指定多个值。 *attributename* 前面的 "+" 表示向当前属性列表中添加值。 如果没有指定操作值 (+)，则默认操作为添加现有的值。
-h, -?	打印命令用法语法。
-i *inputfile*	从文件中而不是命令行中读取命令信息。
-o *organization RDN*	指定该域的组织 RDN。例如，o=varrius.florizel.com。 如果未指定此选项，则使用 o= 域名 o=osiSuffix 在 osi suffix 下创建组织。
-p *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
-s	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

选项	说明
-S *service*	指定要添加到域的服务。 *service* 的值可以为单个服务或多个服务。有效的 *service* 值包括 mail 和 cal。 这些值区分大小写。 如果指定了 -S mail 选项，则必须指定 -H 选项。 可以列为以逗号分隔的列表。 例如： -S mail,cal 将根据 Access Manager 的配置文件中特定服务定义的值所指的服务来创建域。
以下选项仅在指定了 -S mail 选项的情况下才允许使用：	
-H *preferred mailhost*	域的首选邮件主机。该主机必须为全限定主机名，例如，mailhost.sesta.com。 如果指定了 -S mail 选项，则此选项是强制性选项。
以下选项仅在指定了 -S cal 选项的情况下才允许使用：	
-B *backend calendar data server*	指定分配给域中某个用户或资源的默认后端主机。
-C *searchable domains*	指定在查找日历或用户时要搜索的域。
-g *access control string*	为新创建的用户日历指定存取控制表 (Access Control List, ACL)。
-P *propertyname*[: *value*]	为多值属性和位导向属性设置值。有关各个属性及其说明和值的信息，请参阅第 179 页中的 “属性值” 。
-R *right*[:*value*]	设置日历域属性 icsAllowRights。该属性包含位图值。有关各个属性及其值和说明的列表，请参见第 179 页中的 “属性值” 。
-T *calendar time zone string*	指定导入文件时所使用的时区 ID。 有关有效时区字符串的列表，请参见第 181 页中的 “日历时区字符串” 。

示例

要用邮件服务和日历服务创建新的域，请输入：

```
commadmin domain create -D chris -d florizel.com -n sesta.com -w bolton \
-S mail,cal -H mailhost.sesta.com
```

commadmin domain delete

`commadmin domain delete` 命令用于将单个托管域标记为“已从服务器删除”。要将多个托管域标记为“已删除”，请使用 `-i` 选项。

当您将域标记为“已删除”时，该域中的所有用户和组条目都会被标记为“已删除”。

第 121 页中的“commadmin domain purge”命令将永久删除域。

要禁止组织管理员使用服务（例如日历服务或邮件服务），可使用 `-S` 选项。此处 `S` 是大写的。

语法

`commadmin domain delete -D` *login* `-d` *domain name* `-n` *domain* `-w` *password* `[-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-S` *service*`] [-v] [-V] [-X` *AM host*`]`

选项

以下选项是强制性选项：

选项	说明
`-D` *login*	顶级管理员的用户 ID。
`-d` *domain name*	要删除的 DNS 域名。如果没有指定 `-d`，则使用 `-n` 所指定的域。
`-n` *domain*	顶级管理员所属的域。
`-w` *password*	顶级管理员的密码。

以下选项是非强制性选项：

选项	说明
`-h, -?`	打印命令用法语法。
`-i` *inputfile*	从文件中而不是命令行中读取命令信息。
`-p` *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果没有指定，则使用默认的 *AM port*；如果在安装过程中没有配置默认端口，则使用端口 80。
`-s`	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。

选项	说明
-S *service*	将指定服务状态属性值修改为“已删除”。 多个服务以逗号分隔。有效的 *service* 值包括 mail 和 cal。这些值区分大小写。
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

示例

要删除现有的域，可使用以下命令：

```
commadmin domain delete -D chris -w bolton -d florizel.com -n sesta.com
```

要从 florizel.com 域中仅删除邮件服务，则使用：

```
commadmin domain delete -D chris -w bolton -d florizel.com -n sesta.com \
-S mail
```

commadmin domain modify

commadmin domain modify 命令用于修改单个域的目录条目的属性。要修改多个域，请使用 -i 选项。

语法

commadmin domain modify -D *login* -d *domain* -n *domain* -w *password* [-A [+|-]*attributename*:*value*] [-h] [?] [-i *inputfile*] [-p *AM port*] [-s] [-v] [-V] [-X *AM host*] [-S mail -H *preferred mailhost*] [-S cal [-g *access string*] [-C *cross domain search domains*] [-B *backend calendar data server*] [-P [*action*]*propertyname*[:*value*]] [-R *propertyname*[:*value*]] [-T *calendar time zone string*]]

选项

以下选项是强制性选项：

选项	说明
-D *login*	顶级管理员的用户 ID。

选项	说明
-d *domain*	要修改的 DNS 域名。如果没有指定 -d，则使用 -n 所指定的域。
-n *domain*	顶级管理员所属的域。
-w *password*	顶级管理员的密码。

以下选项是非强制性选项：

选项	说明
-A [+ | -]*attributename*: *value*	要修改的属性。*attributename* 以 LDAP 模式定义，value 将替换目录中当前存在的此属性的所有值。重复此选项可同时修改多个属性，或者为同一属性指定多个值。 *attributename* 前面的 "+" 表示向当前属性列表中添加值。"-" 表示删除值。 在使用 "-" 的情况下，如果在命令行指定该命令，则必须在 "-" 前面加两个反斜杠。如果在一个输入文件内提供该选项，则必须在 "-" 符号前面加一个反斜杠。 如果没有指定操作值（+ 或 -），则默认操作为替换现有的值。
-h, -?	打印命令用法语法。
-i *inputfile*	从文件中而不是命令行中读取命令信息。
-p *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
-s	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。
-S *service*	在修改过程中对域添加指定的服务。 有效的 *service* 值包括 mail 和 cal。这些值区分大小写。 通过使用 -S 选项而列出的服务以逗号分隔。 如果指定了 -S mail，则必须指定 -H 选项。

选项	说明
添加服务时，仅在指定了 `-S mail` 选项的情况下才允许使用以下选项：	
`-H` *preferred mailhost*	域的首选邮件主机。 如果指定了 `-S mail` 选项，则此选项是强制性选项。
添加服务时，仅在指定了 `-S cal` 选项的情况下才允许使用以下选项：	
`-B` *backend calendar data server*	分配给域中某个用户或资源的默认后端主机。
`-C` *cross domain search domains*	指定在查找日历或用户时要搜索的域。
`-g` *access string*	为新创建的用户日历指定存取控制表 (Access Control List, ACL)。
`-P` [*action*]*propertyname* [:*value*]	为多值属性和位导向属性设置值。有关 *propertyname* 的说明和值的信息，请参阅第 179 页中的 “属性值” 表格。
`-T` *calendar time zone string*	导入文件时所使用的时区 ID。 有关有效时区字符串的列表，请参见第 181 页中的 “日历时区字符串”。
`-R` *propertyname*[: *value*]	设置日历域属性 `icsAllowRights`。该属性包含位图值。有关各个属性名称及其值和说明的信息，请参见第 179 页中的 “属性值”。

示例

要修改某个现有的域，可使用以下命令：

```
commadmin domain modify -D chris -w bolton -n sesta.com -d varrius.com \
-A preferredmailhost:test.siroe.com
```

commadmin domain purge

`commadmin domain purge` 命令用于永久删除标记为“已删除”的所有条目或条目的服务。这些条目可以是域、用户、组和资源。

执行定期维护操作时，应使用 `commadmin domain purge` 命令清除已被删除且保留时间超过指定宽限期的所有条目。

可以通过手动调用此命令随时进行清除。

调用此命令时，将搜索目录，并创建域列表，其中的条目为标记为“已被删除且保留时间超过指定宽限期”的域。宽限期的默认值设置为 5 天。

如果指定了 -d* 选项，将会在所有域中搜索标记为“已删除”的域和用户。将把标记为“已删除”的用户从他们所属的域中清除，但不会清除该域，除非该域也标记为“已删除”。如果域标记为“已删除”，将会把该域与其中的所有用户一起清除。

将服务标记为“已删除”之后，必须运行一个实用程序来删除诸如邮箱或日历之类的资源才能从目录中清除该服务。对于邮件服务，程序称为 msuserpurge。有关 msuserpurge 实用程序的信息，请参阅 Sun Java System Messaging Server Administration Reference。对于日历服务，该程序是 csclean。有关 csclean 实用程序的信息，请参阅 Sun Java System Calendar Server 管理指南。

注 – commadmin domain purge 命令必须由顶级管理员运行。

▼ 从域中删除用户、组和日历资源

此过程将从域中永久性地删除用户、组和日历资源。域本身在 LDAP 目录中保持不变。仅删除选择为要删除的 LDAP 条目。

1 将用户、组和资源标记为“ 已删除 ”。

例如，要将 florizel.com 域中的选定条目标记为“已删除”，可使用以下命令：

```
commadmin user delete -D chris -w bolton -d florizel.com \
-n sesta.com -i deletedusers

commadmin group delete -D chris -w bolton -d florizel.com \
-n sesta.com -i deletedgroups

commadmin resource delete -D chris -w bolton -d florizel.com \
-n sesta.com -i deletedresources
```

在上例中，deletedusers、deletedgroups 和 deletedresources 是列出标记为要删除的条目的输入文件。

也可以使用 Delegated Administrator 控制台来删除条目：

a. 导航到指定的组织。

b. 单击“ 用户 ”选项卡（ 如果该选项卡未显示 ），选择要删除的用户，然后单击“ 删除 ”。

c. 单击“ 组 ”选项卡，选择要删除的组，然后单击“ 删除 ”。

d. 单击“ 资源 ”选项卡，选择要删除的资源，然后单击“ 删除 ”。

2 从域中选定的用户、组和日历中删除资源。

资源可以是邮箱或日历。

对于邮件服务，运行 msuserpurge 实用程序。

有关 msuserpurge 实用程序的信息，请参阅 Sun Java System Messaging Server Administration Reference。

对于日历服务，运行 csclean 实用程序。

有关 csclean 实用程序的信息，请参阅 Sun Java System Calendar Server 管理指南。

3 **通过调用 第 121 页中的“ commadmin domain purge ”命令，从域中永久性删除选定的条目。**

例如，要从 florizel.com 域中删除选定的用户、组和资源，可使用以下命令：

```
commadmin domain purge -D chris -w bolton -d florizel.com -n sesta.com
```

在上述命令中，florizel.com 域保持不变。仅删除在 deletedusers、deletedgroups 和 deletedresources 输入文件中指定的条目。

▼ 从域中删除服务

此过程将从域和域的每个用户、组和资源中永久性删除邮件和日历服务。域本身（包括其从属 LDAP 条目）在目录中保持不变。

1 **通过运行 commadmin domain delete 命令将域中的服务标记为“ 已删除 ”。**

例如，要将 florizel.com 域中的邮件和日历服务标记为“已删除”，可使用以下命令：

```
commadmin domain delete -D chris -w bolton -d florizel.com -n sesta.com \
-S mail,cal
```

2 **将资源从域中的所有用户、组和资源中删除。**

资源可以是邮箱或日历。

对于邮件服务，运行 msuserpurge 实用程序。

有关 msuserpurge 实用程序的信息，请参阅 Sun Java System Messaging Server Administration Reference。

对于日历服务，运行 csclean 实用程序。

有关 csclean 实用程序的信息，请参阅 Sun Java System Calendar Server 管理指南。

注 – 如果**没有**删除域中任何用户的邮箱或日历，则不能从域中清除该服务。例如，对于邮件服务，要确定宽限期已到且已在域中包括的所有邮件消息存储区上运行 msuserpurge 实用程序。

---

3 **通过调用 第 121 页中的“ commadmin domain purge ”命令可将服务从域中永久性删除。**

例如，要从 `florizel.com` 域中删除邮件和日历服务，可使用以下命令：

```
commadmin domain purge -D chris -w bolton -d florizel.com -n sesta.com \
-S mail,cal
```

▼ 永久性删除整个域

此过程将从目录中永久性删除域。域中的所有用户、组和资源也会从目录中删除。

1 **通过运行 `commadmin domain delete` 命令将此域标记为“ 已删除 ”。**

例如，要将 `florizel.com` 域标记为“已删除”，可使用以下命令：

```
commadmin domain delete -D chris -w bolton -d florizel.com -n sesta.com
```

也可通过使用 Delegated Administrator 控制台在“组织”页面选择组织并单击**删除**，来标记要删除的域。

2 **将资源从域的所有用户、组和资源中删除。**

资源可以是邮箱或日历。

对于邮件服务，运行 `msuserpurge` 实用程序。

有关 `msuserpurge` 实用程序的信息，请参阅 Sun Java System Messaging Server Administration Reference。

对于日历服务，运行 `csclean` 实用程序。

有关 `csclean` 实用程序的信息，请参阅 Sun Java System Calendar Server 管理指南。

注 – 如果**没有**删除域中任何用户的邮箱或日历，则不能删除该域。例如，对于邮件服务，要确定宽限期已到且已在域中包括的所有邮件消息存储区上运行 `msuserpurge` 实用程序。

---

3 **通过调用 第 121 页中的“ commadmin domain purge ”命令永久性删除域。**

例如，要删除 `florizel.com` 域，可使用以下命令：

```
commadmin domain purge -D chris -w bolton -d florizel.com -n sesta.com
```

语法

```
commadmin domain purge -D login -n domain -w password -d domain [-g grace] [-h] [-?]
[-i inputfile] [-p AM port] [-s] [-S service] [-v] [-V] [-X AM host]
```

选项

以下选项是强制性选项：

选项	说明
-D *login*	顶级管理员的用户 ID。
-n *domain*	顶级管理员所属的域。
-w *password*	顶级管理员的密码。
-d *domain*	清除指定的域。可以使用 * 运算符 (-d*) 来搜索模式。

以下选项是非强制性选项：

选项	说明
-g *grace*	清除域之前可以保留的宽限期（以天为单位）。标记为“已删除”但保留时间少于 *grace* 天的域不会被清除。0（零）表示立即清除。默认值为 5 天。不能永久更改默认值。只能通过使用 commadmin domain purge 命令中的 -g *grace* 选项来更改宽限期。
-h, -?	打印命令用法语法。
-i *inputfile*	从文件中而不是命令行中读取命令信息。
-p *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
-S *service*	从域中删除与对象类和属性相关的服务。如果域中包含用户和资源，将会从这些用户和资源的目录中删除服务特定数据。 服务列表以逗号 (,) 分隔符分隔。 有效的 *service* 值包括 mail 和 cal。这些值区分大小写。
-s	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

示例

在以下示例中，将清除 siroe.com 域以及该域中的所有条目：

```
commadmin domain purge -D chris -d siroe.com -n sesta.com -w bolton
```

commadmin domain search

`commadmin domain search` 命令用于获取与单个域相关联的所有目录属性。要获取多个域的所有目录属性，请使用 `-i` 选项。如果在此命令中指定了 `-S`，则仅显示具有活动的指定服务的域。

语法

`commadmin domain search -D` *login* `-n` *domain* `-w` *password* `[-d` *domain*`] [-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-S` *service*`] [-t` *Search Template*`] [-v] [-V] [-X` *AM host*`]`

选项

以下选项是强制性选项：

选项	说明
`-D` *login*	有权执行此命令的用户的用户 ID。
`-n` *domain*	`-D` 选项所指定用户所属的域。
`-w` *password*	`-D` 选项所指定用户的密码。

以下选项是非强制性选项：

选项	说明
`-d` *domain*	搜索此域。如果没有指定 `-d` 或指定了 `-d*`，则显示所有域。
`-h`, `-?`	打印命令用法语法。
`-i` *inputfile*	从文件中而不是命令行中读取命令信息。
`-p` *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
`-s`	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。

选项	说明
-S *service*	指定要在活动域中搜索的服务。 *service* 的值可以为单个服务或多个服务。有效的 *service* 值包括 mail 和 cal。 这些值区分大小写。 服务列表以逗号 (,) 分隔符分隔。 例如 : -S mail,cal
-t *Search template*	指定要代替默认搜索模板来使用的搜索模板的名称。搜索之后将仅显示活动域。
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host* ；如果在安装时没有配置默认主机，则使用本地主机。

commadmin group create

commadmin group create 命令用于在 Access Manager 上添加单个组。要创建多个组，请使用 -i 选项。

如果创建的组不包含任何成员，则默认情况下，此组是静态组。

注 – 组中不能同时包含静态成员和动态成员。

电子邮件分发列表就是一种组。当向此组地址发送消息时， Access Manager 会将此消息发送给组中的所有成员。

语法

commadmin group create -D *login* -G *groupname* -n *domain* -w *password* [-A [+]*attributename*:*value*] [-d *domain*] [-f *ldap-filter*] [-h] [-?] [-i *inputfile*] [-m *internal-member*] [-p *AM port*] [-s] [-v] [-V] [-X *AM host*] [-S *service* [-H *mailhost*] [-E *email*] [-M *external-member*] [-o *owner*] [-r *moderator*]] [-a true|false] [-b true|false] [-c *group id*] [-j *DWPHost*] [-q *secondary owner*] [-t *time zone*]

选项

以下选项是强制性选项 :

选项	说明
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	-D 选项所指定用户所属的域。
-G *groupname*	此组的组名（例如，mktg-list）。
-w *password*	-D 选项所指定用户的密码。

以下选项是非强制性选项：

选项	说明
-A [+]*attributename*: *value*	要修改的属性。*attributename* 以 LDAP 模式定义，*value* 将替换目录中当前存在的此属性的所有值。重复此选项可同时修改多个属性，或者为同一属性指定多个值。 *attributename* 前面的 "+" 表示向当前属性列表中添加值。
-d *domain*	此组的全限定域名（例如，varrius.com ）。默认值为本地域。如果没有指定 -d，则使用 -n 所指定的域。
-f *ldap-filter*	创建动态组。 通过指定属性或属性组合来设置 LDAP 过滤器。 可以指定多个 -f 命令来为组中的各个成员定义多个 LDAP 过滤器。
-h, -?	打印命令用法语法。
-i *inputfile*	从文件中而不是命令行中读取命令信息。
-m *internal -member*	添加到此组的内部成员的用户 ID。要添加多个成员，请使用多个 -m 选项。 此选项应当用于创建静态组。
-p *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。
-s	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。

选项	说明
-S *service*	指定要添加到此组的服务。 *service* 的值可以为单个服务或多个服务。有效的服务值包括 mail 和 cal。这些值区分大小写。 服务列表以逗号 (,) 分隔符分隔。 例如： `-S mail,cal`

如果指定了 `-S mail` 选项，则允许使用以下选项：

选项	说明
-o *owner*	组所有者的电子邮件地址。所有者就是对分发列表负责的个人。 所有者可以添加或删除分发列表成员。 （当指定了 `-S cal` 选项时，允许使用此选项，并且是强制性的。）
-E *email*	此组的电子邮件地址。（当指定了 `-S cal` 选项时，允许使用此选项。）
-H *mailhost*	此组所响应的邮件主机（例如，`mailhost.varrius.com` ）。默认值为本地邮件主机。
-M *external-member*	将外部成员添加到此组。*external-member* 的值是该用户的电子邮件地址。要添加多个成员，请使用 `-M` 选项。
-r *moderator*	仲裁者的电子邮件地址。

如果指定了 `-S cal` 选项，则以下选项是强制性的：

选项	说明
-o *owner*	组所有者的电子邮件地址。所有者就是对日历组的分发列表负责的个人。所有者可以添加或删除分发列表成员。 组所有者必须具有日历服务。 （当指定了 `-S mail` 选项时，允许使用此选项。）

如果指定了 `-S cal` 选项，则允许使用以下非强制性选项：

选项	说明
-a true|false	允许或不允许自动接受日历日程。 true 启用日程的自动接受。 false 禁用日程的自动接受。
-b true|false	允许或不允许日历日程重复预订，同时可批准多个日程。 true 启用日程的重复预订。 false 禁用日程的重复预订。
-c *group id*	指定日历组的组 ID。如果未指定此选项，Delegated Administrator 自动提供一个组 ID。
-E *email*	此组的电子邮件地址。此地址用于向组成员通知日历事件。 （当指定了 -S cal 选项时，允许使用此选项。）
-j *DWPHost*	托管此日历组的日历的后端 Calendar Server 的 DNS 名称。此主机是存储日历及其数据的数据库有线通信协议 (Database Wire Protocol, DWP) 服务器。 如果没有指定后端 Calendar Server 的 DNS 名称，则使用该服务器的 ics.conf 文件中所存储的值作为默认值。
-q *secondary owner*	次要所有者的电子邮件地址。次要所有者可以管理日历组的分发列表。 要添加多个次要所有者，可使用多个 -q *secondary owner* 选项。 所有的次要所有者必须具有日历服务。
-t *time zone*	用于在日历用户界面显示日历组的日历的时区。 有关有效时区字符串的列表，请参见第 181 页中的 “日历时区字符串”。

示例

要在域 sesta.com 中创建组 testgroup，可使用以下命令：

```
commadmin group create -D chris -n sesta.com -w bolton -G testgroup \
-d sesta.com -m lorca@sesta.com -S mail,cal -M achiko@varrius.com \
-o achiko@varrius.com -c calgroup1
```

commadmin group delete

commadmin group delete 命令用于将单个组标记为“已删除”。要将多个组标记为“已删除”，请使用 -i 选项。

要禁止组使用服务（例如 Calendar Server 或 Messaging Server），可使用 -S 选项。此处 S 是大写的。

注 – 要永久删除某个组，必须运行以下命令：第 121 页中的 “commadmin domain purge”.

语法

`commadmin group delete -D` *login* `-G` *groupname* `-n` *domain* `-w` *password* `[-d` *domain*`] [-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-S` *service*`] [-v] [-V] [-X` *AM host*`]`

选项

以下选项是强制性选项：

选项	说明
`-D` *login*	有权执行此命令的用户的用户 ID。
`-G` *groupname*	要标记为“已删除”的组的名称。例如，`mktg-list` 。
`-n` *domain*	`-D` 选项所指定用户所属的域。
`-w` *password*	`-D` 选项所指定用户的密码。

以下选项是非强制性选项：

选项	说明
`-d` *domain*	此组所属的域。如果没有指定 `-d`，则使用 `-n` 选项所指定的域。
`-h, -?`	打印命令用法语法。
`-i` *inputfile*	从文件中而不是命令行中读取命令信息。
`-p` *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
`-s`	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
`-S` *service*	将指定服务状态属性值修改为“已删除”。 通过使用 `-S` 选项而列出的服务以逗号分隔。有效的 *service* 值包括 `mail` 和 `cal`。这些值区分大小写。
`-v`	启用调试输出。

选项	说明
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

示例

以下示例将把组 testgroup@varrius.com 标记为“已删除”：

```
commadmin group delete -D chris -n sesta.com -w bolton -G testgroup \
-d varrius.com
```

以下示例将把 testgroup@varrius.com 的邮件服务标记为“已删除”：

```
commadmin group delete -D chris -n sesta.com -w bolton -G testgroup \
-d varrius.com -S mail
```

commadmin group modify

commadmin group modify 命令用于更改已经存在于 Access Manager 中的单个组的属性。要更改多个组的属性，请使用 -i 选项。

邮递列表就是一种组。当向此组地址发送消息时，Access Manager 会将此消息发送给组中的所有成员。

语法

commadmin group modify -D *login* -G *groupname* -n *domain* -w *password* [-A [+|-]*attributename*:*value*] [-d *domain*] [-f [*action*]*ldap-filter*] [-h] [-?] [-i *inputfile*] [-m [+|-]*internal-member*] [-p *AM port*] [-s] [-v] [-V] [-X *AM host*] [-S mail [-o *owner*] [-E *email*] [-H *mailhost*] [-M *external-member*] [-r *moderator*] [-a true|false] [-b true|false] [-c *group id*] [-j *DWPHost*] [-q *secondary owner*] [-t *time zone*]

选项

以下选项是强制性选项：

选项	说明
-D *login*	有权执行此命令的用户的用户 ID。
-G *groupname*	要修改的组的名称。例如，mktg-list。

选项	说明
-n *domain*	-D 选项所指定用户所属的域。
-w *password*	-D 选项所指定用户的密码。

以下选项是非强制性选项：

选项	说明
-A [+ | -]*attributename*: *value*	要修改的属性。*attributename* 以 LDAP 模式定义，value 将替换目录中当前存在的此属性的所有值。重复此选项可同时修改多个属性，或者为同一属性指定多个值。 *attributename* 前面的 "+" 表示向当前属性列表中添加值。"-" 表示删除值。在使用 "-" 的情况下，如果在命令行指定该命令，则必须在 "-" 前面加两个反斜杠或者在两边加引号。如果在一个输入文件内提供该选项，则必须在 "-" 符号前面加一个反斜杠。
-d *domain*	此组所属的域。如果没有指定 -d，则使用 -n 选项所指定的域。
- f [*action*] *ldap-filter*	指明是向此组中添加 LDAP 过滤器还是从此组中删除 LDAP 过滤器。 *ldap-filter* 前面的 "+" 表示将其添加到现有的过滤器中。"-" 表示删除现有过滤器。键入 -f-* 可删除所有过滤器。在使用 "-" 的情况下，如果在命令行指定该命令，则必须在 "-" 前面加两个反斜杠或者在两边加引号。 如果没有指定 *action*，则默认情况下将添加该过滤器（假设该过滤器当前不存在）。否则，将显示错误消息。
-h, -?	打印命令用法语法。
-i *inputfile*	从文件中而不是命令行中读取命令信息。
-m [*action*] *internal -member*	指明是添加还是删除内部成员。 内部 *-member* 的值可以是电子邮件地址或用户 ID。 *action* 值： 如果是 +，将把该成员添加到现有内部成员列表中。 如果是 -，则从现有内部成员列表中删除该成员。在使用 "-" 的情况下，如果在命令行指定该命令，则必须在 "-" 前面加两个反斜杠或者在两边加引号。 如果是 -m-*，将会删除所有内部成员。
-p *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。

选项	说明
`-s`	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
`-v`	启用调试输出。
`-V`	打印关于该实用程序及其版本的信息。
`-X` *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。
`-S` *service*	指定修改期间添加到组的服务。在添加服务之前，Delegated Administrator 会验证服务是否已经存在。如果该服务已经存在，将显示错误消息。 *service* 的值可以为单个服务或多个服务。有效的服务值包括 mail 和 cal。这些值区分大小写。 服务列表以逗号 (,) 分隔符分隔。 例如： `-S mail,cal`

如果指定了 `-S mail` 选项，则允许以下选项：

选项	说明
`-o` *owner*	组所有者的电子邮件地址。所有者就是对分发列表负责的个人。 所有者可以添加或删除分发列表成员。 （当指定了 `-S cal` 选项时，允许使用此选项，并且是强制性的。）
`-E` *email*	此组的电子邮件地址。（当指定了 `-S cal` 选项时，允许使用此选项。）
`-H` *mailhost*	此组所响应的邮件主机（例如，`mailhost.varrius.com` ）。默认值为本地邮件主机。
`-M` *external-member*	将外部成员添加到此组。*external-member* 的值是该用户的电子邮件地址。要添加多个成员，请使用 `-M` 选项。
`-r` *moderator*	仲裁者的电子邮件地址。

如果指定了 `-S cal` 选项，则以下选项是强制性的：

选项	说明
-o *owner*	组所有者的电子邮件地址。所有者就是对日历组的分发列表负责的个人。所有者可以添加或删除分发列表成员。 组所有者必须具有日历服务。 （当指定了 -S mail 选项时，允许使用此选项。）

如果指定了 -S cal 选项，则允许使用以下非强制性选项：

选项	说明
-a true|false	允许或不允许自动接受日历日程。 true 启用日程的自动接受。 false 禁用日程的自动接受。
-b true|false	允许或不允许日历日程重复预订，同时可批准多个日程。 true 启用日程的重复预订。 false 禁用日程的重复预订。
-c *group id*	指定日历组的组 ID。如果未指定此选项，Delegated Administrator 自动提供一个组 ID。
-E *email*	此组的电子邮件地址。此地址用于向组成员通知日历事件。 （当指定了 -S cal 选项时，允许使用此选项。）
-j *DWPHost*	托管此日历组的日历的后端 Calendar Server 的 DNS 名称。此主机是存储日历及其数据的数据库有线通信协议 (Database Wire Protocol, DWP) 服务器。 如果没有指定后端 Calendar Server 的 DNS 名称，则使用该服务器的 ics.conf 文件中所存储的值作为默认值。
-q *secondary owner*	次要所有者的电子邮件地址。次要所有者可管理日历组的分发列表。 要添加多个次要所有者，可使用多个 -q *secondary owner* 选项。 所有的次要所有者必须具有日历服务。
-t *time zone*	用于在日历用户界面中显示日历组的日历的时区。 有关有效时区字符串的列表，请参见第 181 页中的 “日历时区字符串”。

示例

要从域 varrius.com 内的组 testgroup 中删除一个内部成员 (jsmith)，可使用以下命令：

```
commadmin group modify -D chris -d varrius.com -G testgroup -n sesta.com \
-w bolton -m \\-jsmith
```

要为域 varrius.com 中的组 testgroup 添加日历服务，可使用以下命令：

```
commadmin group modify -D chris -d varrius.com -G testgroup -n sesta.com \
-w bolton -S cal -o achiko@varrius.com -c calgroup1
```

commadmin group search

commadmin group search 命令用于获取与单个组相关联的所有目录属性。要获得多个组的所有目录属性，请使用 -i 选项。

语法

commadmin group search -D *login* -n *domain* -w *password* [-d *domain*] [-E *string*] [-G *string*] [-h] [-?] [-i *inputfile*] [-p *AM port*] [-s] [-S *service*] [-t *search template*] [-v] [-V] [-X *AM host*]

选项

以下选项是强制性选项：

选项	说明
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	-D 选项所指定用户所属的域。
-w *password*	-D 选项所指定用户的密码。

以下选项是非强制性选项：

选项	说明
-d *domain*	要搜索的组所属的域。如果没有指定 -d，将会搜索所有域。
-E *string*	此组的电子邮件地址。可以在字符串的任意部分使用通配符 (*)。
-G *string*	要搜索的组的名称。例如，mktg-list。如果没有指定 -G，将会显示 -d 所指定的域中的所有组。可以在字符串的任意部分使用通配符 (*)。
-h, -?	打印命令用法语法。

选项	说明
`-i` *inputfile*	从文件中而不是命令行中读取命令信息。
`-p` *AM port*	指定 IS Server 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
`-s`	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
`-S` *service*	指定要搜索的服务。 *service* 的唯一有效值为 `mail` 。此值区分大小写。 例如： `-S mail` 仅显示具有活动服务的组。
`-t` *Search Template*	指定要代替默认搜索模板来使用的搜索模板的名称。这是目录中用来定义搜索过滤器的一个条目。仅搜索活动组。
`-v`	启用调试输出。
`-V`	打印关于该实用程序及其版本的信息。
`-X` *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

示例

要在 `siroe.com` 域中搜索名为 `developers` 的组，可使用以下命令：

```
commadmin group search -D chris -n sesta.com -w password -G developers \
-d siroe.com
```

commadmin resource create

`commadmin resource create` 命令用于为资源创建目录条目。

有关创建资源的说明，请参见第 139 页中的 “创建资源”。

语法

`commadmin resource create -D` *login* `-n` *domain* `-w` *password* `-u` *identifier* `-N` *name* `[-c` *calendar identifier*`] [-A [+]`*attributename*`:`*value*`] [-C` *DWPHost*`] [-d` *domainname* `] [-h] [-?] [-i` *inputfile*`][-p` *AM port*`] [-s] [-T` *time zone*`] [-v] [-V] [-X` *AM host*`]`

选项

以下选项是强制性选项：

选项	说明
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	-D 选项所指定用户所属的域。
-w *password*	-D 选项所指定用户的密码。
-u *identifier*	资源的唯一标识符。 此 *identifier* 值在域命名空间内或在日历模式下日历所管理的用户和资源内应当是唯一的。
-N *name*	用来显示日历 GUI 中的资源的好记的名称。
-c *calendar identifier*	此资源的日历标识符。 此标识符值在 Calendar Server 所管理的所有日历中应当是唯一的。

以下选项是非强制性选项：

选项	说明
-A [+] *attributename*: *value*	要修改的属性。*attributename* 以 LDAP 模式定义，*value* 将替换目录中当前存在的此属性的所有值。重复此选项可同时修改多个属性，或者为同一属性指定多个值。 *attributename* 前面的 "+" 表示向当前属性列表中添加值。
-C *DWPHost*	托管此用户日历的后端 Calendar Server 的 DNS 名称。 如果没有指定后端 Calendar Server 的 DNS 名称，则使用该服务器的 ics.conf 文件中所存储的值作为默认值。
-d *domain name*	此资源所属的域。如果没有指定 -d，则使用 -n 所指定的域。
-h, -?	打印命令用法语法。
-i *inputfile*	从文件中而不是命令行中读取命令信息。
-p *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
-s	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
-T *time zone*	在此资源的日历用户界面中显示日历时所使用的时区。 有关有效时区字符串的列表，请参见第 181 页中的 “日历时区字符串” 。
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。

选项	说明
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

示例

要在域 varrius.com 下的日历 cal.siroe.com 中创建名为 peter 的资源，可使用以下命令：

```
commadmin resource create -D chris -n sesta.com -w bolton \
-d varrius.com -u id -c calid -N peter -C cal.siroe.com
```

创建资源

资源由两项数据说明组成：目录条目和 Calendar Server 数据库中的日历。目录条目具有 icsCalendar 属性，其值是与资源相关联的日历的名称。

可以通过以下任意一种方法，用这两项数据说明来创建资源：

- 使用 commadmin resource create 创建目录条目。

  当资源首次被邀请到某个事件时，会自动创建该资源的日历。ics.conf 参数 resource.invite.autoprovision 确定在邀请资源到事件时，是否自动创建资源的日历。默认情况下，此参数的值设置为“是”。

  要在向资源发送任何邀请前创建资源的日历，可使用 cscal 实用程序。

  示例

  使用 commadmin resource create 创建目录条目：

  ```
  commadmin resource create -D amadmin -w ampassword -n blink.sesta.com \
   -X blink -p 5555 -d varrius.com -u resourceOne \
   -N firstResource -c resourceOneCalendar
  ```

  该目录条目如下所示：

  ```
  dn: uid=resourceONE,ou=People,o=varrius,o=domainroot
  uid: resrouceONE
  objectClass: icsCalendarResource
  objectClass: top
  cn: firstResource
  icsStatus: active
  icsCalendar: resourceOne
  ```

- 请使用 csresource 实用程序本身。csresource 实用程序创建目录条目和日历。

  但是，仅当没有使用 Access Manager 且目录位于 Schema 1 环境下时，才建议使用 csresource 同时创建目录条目和日历。

现在，您可以以任何用户身份登录并邀请资源参加到事件中。

有关 csresource 和 cscal 实用程序的详细说明，请参见《Sun Java System Calendar Server 6.3 Administration Guide》中的附录 D “Calendar Server Command-Line Utilities Reference”。

commadmin resource delete

commadmin resource delete 命令用于将资源标记为“已删除”。

注 – 要永久删除资源，请运行第 121 页中的 “commadmin domain purge” 。

语法

commadmin resource delete -D *login* -u *identifier* -n *domain* -w *password* [-d *domainname*] [-h] [-?] [-i *inputfile*] [-p *AM port*] [-s] [-v] [-V] [-X *AM host*]

选项

以下选项是强制性选项：

选项	说明
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	-D 选项所指定用户所属的域。
-w *password*	-D 选项所指定用户的密码。
-u *identifier*	资源的唯一标识符

以下选项是非强制性选项：

选项	说明
-d *domainname*	此资源所属的域。如果没有指定 -d，则使用 -n 所指定的域。
-h, -?	打印命令用法语法。
-i *inputfile*	从文件中而不是命令行中读取命令信息。
-p *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
-s	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。

选项	说明
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

示例

要将资源标记为“已删除”，可使用以下命令：

```
commadmin resource delete -D chris -n sesta.com -w bolton -u bill023
```

commadmin resource modify

`commadmin resource modify` 命用于令修改资源。

语法

`commadmin resource modify -D` *login* `-n` *domain* `-w` *password* `-u` *identifier* `[-A [+|-]`*attributename*`:` *value*`] [-d` *domainname* `] [-h] [-?] [-i` *inputfile*`] [-N` *name*`] [-p` *AM port*`] [-s] [-T` *time zone*`] [-v] [-V] [-X s`*AM host*`]`

选项

以下选项是强制性选项：

选项	说明
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	-D 选项所指定用户所属的域。
-w *password*	-D 选项所指定用户的密码。
-u *identifier*	资源的唯一标识符。

以下选项是非强制性选项：

选项	说明
-A [+ | -]*attributename*: *value*	要修改的属性。*attributename* 以 LDAP 模式定义，value 将替换目录中当前存在的此属性的所有值。重复此选项可同时修改多个属性，或者为同一属性指定多个值。 *attributename* 前面的 "+" 表示向当前属性列表中添加值。"-" 表示删除值。 在使用 "-" 的情况下，如果在命令行指定该命令，则必须在 "-" 前面加两个反斜杠。如果在一个输入文件内提供该选项，则必须在 "-" 符号前面加一个反斜杠。
-d *domainname*	此资源所属的域。如果没有指定 -d，则使用 -n 所指定的域。
-h, -?	打印命令用法语法。
-i *inputfile*	从文件中而不是命令行中读取命令信息。
-N *name*	在日历用户界面中显示此资源时所使用的通用名。
-p *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
-s	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
-T *time zone*	在日历 GUI 中显示资源日历时所使用的时区。 有关有效时区字符串的列表，请参见第 181 页中的 “日历时区字符串” 。
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

示例

要用唯一标识符 bill023 和新的通用名 bjones 来修改资源，可使用以下命令：

```
commadmin resource modify -D chris -n sesta.com -w bolton -d test.com \
-u bill023 -N bjones
```

commadmin resource search

commadmin resource search 命令用于搜索资源。

语法

`commadmin resource search -D` *login* `-n` *domain* `-w` *password* `[-d` *domain*`] [-h] [-?] [-i` *inputfile*`] [-N` *string*`] [-p` *AM port*`] [-s] [-t` *Search Template*`] [-u` *string*`] [-V] [-v] [-X` *AM host*`]`

选项

以下选项是强制性选项：

选项	说明
`-D` *login*	有权执行此命令的用户的用户 ID。
`-n` *domain*	`-D` 选项所指定用户所属的域。
`-w` *password*	`-D` 选项所指定用户的密码。

以下选项是非强制性选项：

选项	说明
`-d` *domain*	此资源所属的域。搜索操作只能在该域中执行。如果没有指定 `-d` 或指定了 `-d*`，将会搜索所有域。
`-h, -?`	打印命令用法语法。
`-i` *inputfile*	从文件中而不是命令行中读取命令信息。
`-N` *string*	输入此资源的通用名。可以在字符串的任意部分使用通配符 (*)。
`-p` *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
`-s`	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
`-t` *Search Template*	指定要代替默认搜索模板来使用的搜索模板的名称。这是目录中用来定义搜索过滤器的一个条目。将只搜索活动资源。
`-u` *string*	对于域命名空间和日历所管理的所有用户和资源，指定的资源标识符必须是唯一的。 可以在字符串的任意部分使用通配符 (*)。 如果没有指定标识符或指定了 `-l*`，则在搜索过程中将显示所有资源。
`-v`	启用调试输出。

选项	说明
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

示例

要在域 sesta.com 中搜索资源 arabella，可使用以下命令：

```
commadmin resource search -D serviceadmin -w serviceadmin -n sesta.com \s
-d sesta.com -u arabella
```

commadmin user create

commadmin user create 命令用于在 Access Manager 系统中创建单个用户。要创建多个用户，请使用 -i 选项。

语法

commadmin user create -D *login* -F *firstname* -n *domain* -L *lastname* -l *userid* -w *password* -W *password* [-A [+] *attributename*:*value*] [-d *domain*] [-I *initial*] [-h] [-?] [-i *inputfile*] [-p *AM port*] [-s] [-v] [-V] [-X *AM host*] [-S mail [-E *email*] [-H *mailhost*]] [-S cal [-B *DWPHost*] [-E *email*] [-k *calid_type*] [-J *First Day of Week*] [-T *time zone*]

选项

以下选项是强制性选项：

选项	说明
-D *login*	有权执行此命令的用户的用户 ID。
-F *firstname*	用户的名字，必须是不带空格的单个词。
-n *domain*	-D 选项所指定用户所属的域。
-l *userid*	用户的登录名称。
-w *password*	-D 选项所指定用户的密码。

选项	说明
-W *password*	要创建的用户的密码。 还可以通过文本文件 *password*.txt 来指定 *password*。 例如，如果指定了 -W mypassword.txt，而 mypassword.txt 文件的内容是 secret，那么 commadmin 实用程序将字符串 secret 作为密码。 注意，如果您指定了 -W mypassword.txt，而 mypassword.txt 文件不存在，那么 commadmin 实用程序将字符串 mypassword.txt 本身作为密码。
-L *lastname*	用户的姓氏。

以下选项是非强制性选项：

选项	说明
-A [+]*attributename*: *value*	要修改的属性。*attributename* 以 LDAP 模式定义，*value* 将替换目录中当前存在的此属性的所有值。重复此选项可同时修改多个属性，或者为同一属性指定多个值。 *attributename* 前面的 "+" 表示向当前属性列表中添加值。
-d *domain*	此用户所属的域。如果没有指定 -d，则使用 -n 所指定的域。
-i *inputfile*	从文件中而不是命令行中读取命令信息。
-I *initial*	用户的中间名缩写。
-h, -?	打印命令用法语法。
-p *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
-s	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

选项	说明
-S *service*	在创建过程中向用户添加指定的服务。*service* 的值可以为单个服务或多个服务。有效的 *service* 值包括 mail 和 cal。这些值区分大小写。 服务列表以逗号 (,) 分隔符分隔。 例如： -S mail,cal
以下选项仅在指定了 -S mail 选项的情况下才允许使用：	
-E *email*	用户的电子邮件地址。
-H *mailhost*	用户的邮件主机。
以下选项仅在指定了 -S cal 选项的情况下才允许使用：	
-B *DWPHost*	托管此用户日历的后端日历的 DNS 名称。
-E *email*	日历用户的电子邮件地址。
-J *First Day of Week*	当日历显示在 Calendar Server 用户界面中时，所显示的那一周的第一天。有效值为 0 - 6（0 表示星期日，1 表示星期一，依此类推）。
-k *calid_type*	指定要创建的日历 ID 的类型。可接受的值包括 legacy 和 hosted。如果指定了 -k legacy，则仅使用日历 ID（例如， jsmith）。如果指定了 -k hosted，则使用日历 ID 和域（例如，jsmith@sesta.com）。 如果没有指定 -k 选项，默认值为使用日历 ID 和域 (hosted)。 如果没有指定 -k 选项，则您可以设置所创建的日历 ID 类型的值。要执行此操作，请将以下参数添加到 resource.properties 文件： switch-caltype=*value* 其中 *value* 是 "hosted" | "legacy"。 resource.properties 文件位于以下目录中： *da-base*/data/WEB-INF/classes/sun/comm/cli/ \ server/servlet/resource.properties
-T *time zone*	显示用户日历的时区。 有关有效时区字符串的列表，请参见第 181 页中的 “日历时区字符串”。

示例

要创建新用户 smith，请输入：

```
commadmin user create -D chris -n sesta.com -w secret -F smith -l john \
-L major -W secret -S mail -H mailhost.siroe.com
```

commadmin user delete

`commadmin user delete` 命令用于将单个用户标记为“已删除”。要将多个用户标记为“已删除”，请使用 `-i` 选项。

不存在用来取消删除的实用程序。但可以在清除宽限期到期并对用户条目运行清除之前，随时使用 `ldapmodify` 命令将该条目的状态属性更改为 `active`。

▼ 删除用户的步骤

1. **通过运行 `commadmin user delete` 命令将此用户标记为“ 已删除 ”。**

2. **删除此用户的资源。**
   资源可以是邮箱或日历。

   对于邮件服务，该程序称为 `msuserpurge`。有关 `msuserpurge` 实用程序的信息，请参阅 Sun Java System Messaging Server Administration Reference。

   对于日历服务，该程序是 `csclean`。有关 `csclean` 实用程序的信息，请参阅 Sun Java System Calendar Server 管理指南。

3. **通过调用以下命令可以永久清除此用户：第 121 页中的“ commadmin domain purge ”.**
   有关删除用户的更多信息，请参见 第 121 页中的 “commadmin domain purge” 。

语法

`commadmin user delete -D` *login* `-n` *domain* `-l` *login name* `-w` *password* `[-d` *domain*`] [-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-S` *service*`] [-v] [-V] [-X` *AM host*`]`

选项

以下选项是强制性选项：

选项	说明
`-D` *login*	有权执行此命令的用户的用户 ID。
`-n` *domain*	`-D` 选项所指定用户所属的域。
`-w` *password*	`-D` 选项所指定用户的密码。

选项	说明
`-l` *userid*	要删除的用户的用户 ID。

以下选项是非强制性选项：

选项	说明
`-d` *domain*	此用户所属的域。如果没有指定 `-d`，则使用 `-n` 所指定的域。
`-h, -?`	打印命令用法语法。
`-i` *inputfile*	从文件中而不是命令行中读取命令信息。
`-p` *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
`-s`	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
`-S` *service*	指定要对此用户删除的服务。用户将保持活动状态，而仅取消激活所指定的服务。如果没有指定 `-S`，则用户将被删除。 *service* 的值可以为单个服务或多个服务。有效的 *service* 值为 `mail` 和 `cal`。这些值区分大小写。 服务列表以逗号 (,) 分隔符分隔。 例如： `-S mail,cal`
`-v`	启用调试输出。
`-V`	打印关于该实用程序及其版本的信息。
`-X` *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

示例

要将某个现有用户标记为“已删除”，可使用以下命令：

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith
```

要仅删除用户 `smith` 的邮件服务，可使用以下命令：

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith -S mail
```

commadmin user modify

`commadmin user modify` 命令用于修改单个用户的目录条目的属性。要修改多个用户，请使用 `-i` 选项。

语法

`commadmin user modify -D` *login* `-n` *domain* `-l` *userid* `-w` *password* `[-A [+|-]`*attributename*`:`*value*`] [-d` *domain*`] [-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-v] [-V] [-X` *AM host*`] [-S mail -H` *mailhost* `[-E` *email*`]] [-S cal [-B` *DWPHost*`] [-E` *email*`] [-k` *calid_type*`] [-J` *First Day of Week*`] [-T` *time zone*`]]`

选项

以下选项是强制性选项：

选项	说明
`-D` *login*	有权执行此命令的用户的用户 ID。
`-n` *domain*	`-D` 选项所指定用户所属的域。
`-w` *password*	`-D` 选项所指定用户的密码。
`-l` *userid*	用户的登录 ID。

以下选项是非强制性选项：

选项	说明
`-A [+ | -]`*attributename*`:` *value*	要修改的属性。*attributename* 以 LDAP 模式定义，value 将替换目录中当前存在的此属性的所有值。您可以重复此选项以同时修改多个属性，或者为同一属性指定多个值。 *attributename* 前面的 "+" 表示向当前属性列表中添加值。 "-" 表示删除值。 在使用 "-" 的情况下，如果在命令行指定该命令，则必须在 "-" 前面加两个反斜杠。如果在一个输入文件内提供该选项，则必须在 "-" 符号前面加一个反斜杠。
`-d` *domain*	用户或组所属的域。如果没有指定 `-d`，则使用 `-n` 所指定的域。
`-h, -?`	打印命令用法语法。
`-i` *inputfile*	从文件中而不是命令行中读取命令信息。

选项	说明
-p *AM port*	指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
-s	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。
-S *service*	先验证用户是否用 -S 选项指定了指定的服务，然后向用户添加该服务。如果用户已经具有该服务，将显示错误消息。 *service* 的值可以为单个服务或多个服务。有效的 *service* 值包括 mail 和 cal。 这些值区分大小写。 服务列表以逗号 (,) 分隔符分隔。 例如： -S mail,cal
以下选项仅在指定了 -S mail 选项的情况下才允许使用：	
-E *email*	指定用户的电子邮件地址。
-H *mailhost*	用户的邮件主机。 如果指定了 -S mail 选项，则此选项是强制性选项。
以下选项仅在指定了 -S cal 选项的情况下才允许使用：	
-B *DWPHost*	指定托管此用户日历的后端 Calendar Server 的 DNS 名称。 注：只能添加此属性；如果它已经存在，将不能进行修改。
-E *email*	为日历用户指定电子邮件地址。
-J *First Day of Week*	当日历显示在 Calendar Server 用户界面中时，所显示的那一周的第一天。有效值为 0 - 6（0 表示星期日，1 表示星期一，依此类推）。

选项	说明
-k *calid_type*	指定在添加日历服务时要创建的日历的类型。可接受的值包括 legacy 和 hosted。如果指定了 -k legacy，则仅使用日历 ID（例如，jsmith）。如果指定了 -k hosted，则使用日历 ID 和域（例如，jsmith@sesta.com）。 如果没有指定 -k 选项，默认值为使用日历 ID 和域 (hosted)。 如果没有指定 -k 选项，则您可以设置所创建的日历 ID 类型的值。要执行此操作，请将以下参数添加到 resource.properties 文件： switch-caltype=*value* 其中 *value* 是 "hosted" | "legacy"。 resource.properties 文件位于以下目录中： *da-base*/data/WEB-INF/classes/sun/comm/cli/ \ server/servlet/resource.properties
-T *time zone*	此时区中会显示用户日历。 有关有效时区字符串的列表，请参见第 181 页中的 “日历时区字符串”。

示例

以下示例将为用户 smith 添加电子邮件服务：

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith \
-A description:"new description" -S mail -H mailhost.siroe.com
```

在此示例中，为用户 smith 添加了邮件转发地址：

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith \
-A +mailforwardingaddress:tsmith@siroe.com
```

commadmin user search

commadmin user search 命令用于获取与单个用户相关联的所有目录属性。要获取多个用户的所有目录属性，请使用 -i 选项。搜索之后将仅显示活动用户。

语法

commadmin user search -D *login* -n *domain* -w *password* [-d *domain*] [-E *string*] [-F *string*] [-h] [-?] [-i *inputfile*] [-L *string*] [-l *string*] [-p *AM port*] [-s] [-S *service*] [-t *Search Template*] [-v] [-V] [-X *AM host*]

选项

以下选项是强制性选项：

选项	说明
`-D` *login*	有权执行此命令的用户的用户 ID。
`-n` *domain*	`-D` 选项所指定用户所属的域。
`-w` *password*	`-D` 选项所指定用户的密码。

以下选项是非强制性选项：

选项	说明
`-d` *domain*	用户所属的域。将只在指定的域中搜索用户。 如果没有指定 `-d`，将会搜索所有的域。
`-E` *string*	搜索用户的邮件地址。可以在字符串的任意部分使用通配符 (*)。
`-F` *string*	搜索用户的名字。可以在字符串的任意部分使用通配符 (*)。
`-h`, `-?`	打印命令用法语法。
`-i` *inputfile*	从文件中而不是命令行中读取命令信息。
`-L` *string*	搜索用户的姓氏。可以在字符串的任意部分使用通配符 (*)。
`-l` *string*	搜索用户的登录名称。可以在字符串的任意部分使用通配符 (*)。
`-p` *AM port*	使用此选项可指定 Access Manager 侦听的备用 TCP 端口。如果未指定，则使用默认的 *AM port*，如果在安装时没有配置默认端口，则使用端口 80。
`-s`	使用 SSL（Secure Socket Layer，安全套接口层）连接到 Access Manager。
`-S` *service*	指定在用户搜索中匹配的服务。 *service* 的值可以为单个服务或多个服务。有效的 *service* 值包括 `mail` 和 `cal`。这些值区分大小写。 服务列表以逗号 (,) 分隔符分隔。 例如： `-S mail,cal`
`-t` *Search template*	指定要代替默认搜索模板来使用的搜索模板的名称。这是目录中用来定义搜索过滤器的一个条目。将只搜索活动用户。

选项	说明
-v	启用调试输出。
-V	打印关于该实用程序及其版本的信息。
-X *AM host*	指定运行 Access Manager 的主机。如果没有指定，则使用默认的 *AM host*；如果在安装时没有配置默认主机，则使用本地主机。

示例

以下示例将在 varrius.com 域中搜索用户：

```
commadmin user search -D chris -w bolton -d varrius.com -n sesta.com
```

◆ ◆ ◆ 附 录 A

服务提供商管理员和服务提供商组织

Delegated Administrator 控制台提供了一种新的管理员角色—服务提供商管理员 (Service Provider Administrator, SPA)，以及可以在目录中创建的新组织类型。

本附录介绍了以下主题：

本附录介绍了服务提供商管理员角色以及新的组织类型，并说明了如何在 Delegated Administrator 中创建这些组织。

服务提供商管理员

Delegated Administrator 控制台允许您将管理任务委托给一种新角色—服务提供商管理员 (Service Provider Administrator, SPA)，SPA 可以创建和管理新的从属组织类型。

SPA 的权限范围介于顶级管理员 (Top-Level Administrator, TLA) 与组织管理员 (Organization Administrator, OA) 的权限范围之间。

具有了 SPA 权限，您就可以创建三层管理结构，如第 1 章的第 22 页中的 “三层结构” 所述。

这种二级委托可以使得对大型 LDAP 目录所支持的大型客户库的管理容易一些。例如，ISP 可以向数百或数千家小公司提供服务，每家小公司都需要具有各自的组织。每天都可能需要向目录中添加许多新组织。

如果您使用了两层结构，那么 TLA 必须创建所有这些新组织。现在，TLA 就可以将这些任务委托给 SPA。

SPA 可以为新客户创建从属组织并指派 OA 来管理这些组织中的用户。

图 A–1 显示了三层组织结构样例的逻辑视图。

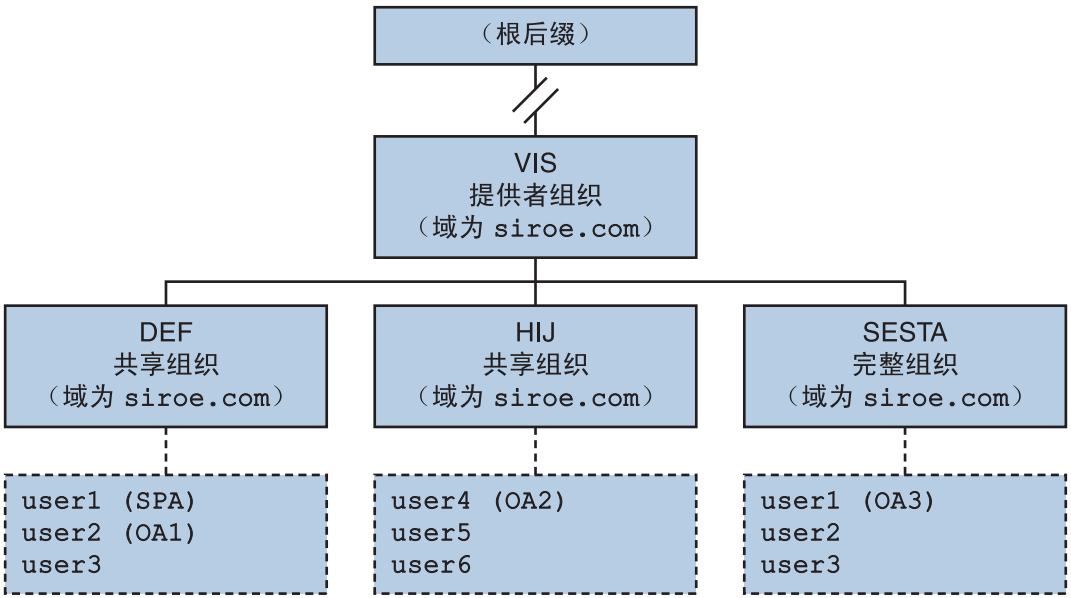

图 A–1 使用服务提供商管理员的目录：逻辑视图

图 A–1 中的示例显示了一个提供商组织。但实际上目录中可以包含多个提供商组织。

在此示例中，管理任务的委托方式如下：

- SPA 有权管理 VIS 提供商组织及其包含的所有组织。SPA 角色被指派给 DEF 组织中的 `user1`。
- 名为 OA1 的组织管理员可管理共享组织 DEF。此 OA 角色被指派给 DEF 组织中的 `user2`。
- OA2 可管理共享组织 HIJ。此 OA 角色被指派给 HIJ 组织中的 `user4`。
- OA3 可管理完整组织 SESTA。此 OA 角色被指派给 SESTA 组织中的 `user1`。

  SESTA 是一个完整的组织，具有其自己的唯一名称空间。SESTA（在 `sesta.com` 域中）中的 `user1` 具有唯一用户 ID。

有关提供商和从属组织的定义，请参见第 158 页中的 “由服务提供商管理员管理的组织”。

服务提供商管理员角色

SPA 可以执行以下任务：

- 在 SPA 有权管理的提供商组织中创建、删除和修改共享组织和完整组织。

  在图 A–1 显示的示例中，VIS 提供商组织的 SPA 可以

  - 修改或删除 DEF、HIJ 和 SESTA 组织
  - 在 VIS 提供商组织下创建其他组织。
- 在提供商组织下的任意组织中创建、删除和修改用户。
- 在提供商组织下的任意组织中创建、删除和修改组。
- 在提供商组织下的任意组织中创建、删除和修改日历资源。
- 将 OA 角色指派给用户。

  例如，在图 A–1 显示的样例组织中，SPA 可以将 OA 角色指派给 SESTA 组织中的 `user2`。这样，`user2` 就可以管理 SESTA 组织中的用户。

  SPA 还可以撤消用户的 OA 角色。
- 将 SPA 角色指派给提供商组织下的其他合法用户（以及撤消 SPA 角色）。
- 将服务包分配给各个组织。

  有关服务包的信息，请参见第 1 章中的第 27 页中的 “服务包”。

  SPA 可以将指定类型的服务包分配给一个组织并确定可以在该组织中使用的每种包的最大数量。

  例如，SPA 可以分配以下服务包：

  - 在 DEF 组织中：

    ```
    1,000 个 gold 包
    500 个 platinum 包
    ```
  - 在 HIJ 组织中：

    ```
    2,500 个 topaz 包
    500 个 platinum 包
    500 个 emerald 包
    1,000 个 ruby 包
    ```
  - 在 SESTA 组织中：

    ```
    2,000 个 silver 包
    1,500 个 gold 包
    100 个 platinum 包
    ```

    SPA 可以使用 Delegated Administrator 控制台来执行这些任务。在此版本中，Delegated Administrator 实用程序不包含执行这些任务的命令选项。

注 – TLA 可以修改或删除任何现有的共享组织或完整组织，还可以管理这些组织中的用户。

TLA 可以撤消用户的 SPA 角色，但不能通过控制台指派 SPA 角色。有关此版本的 Delegated Administrator 中的约束列表，请参见第 158 页中的 “此版本的注意事项”。

有关由 TLA 执行的管理任务的完整说明，请参见第 1 章中的第 23 页中的 “管理员角色与目录分层结构”。

将 SPA 角色指派给用户

要将 SPA 角色指派给某个组织中的用户，该组织必须是为 SPA 指定的并且从属于 SPA 将管理的提供商组织。

在图 A–1 显示的示例中，假设需要为名为 VIS 的提供商组织创建 SPA。可以将 SPA 角色指派给组织 DEF 中的 `user1`。

SPA 必须位于从属组织中，因为提供商组织节点不包含任何用户。

因此，必须至少在提供商组织下创建一个组织，SPA 才能管理该提供商组织。应指定此组织来包含被指派为 SPA 角色的用户。有关详细信息，请参见第 160 页中的 “创建提供商组织和服务提供商管理员”。

此版本的注意事项

在此版本的 Delegated Administrator 中，无法使用 Delegated Administrator 控制台或实用程序来创建 SPA 或提供商组织。

要创建 SPA 或提供商组织，必须手动修改自定义服务提供商模板 `da.provider.skeleton.ldif`。

有关使用自定义服务提供商模板来执行这些任务的说明，请参见本附录后面的第 160 页中的 “创建提供商组织和服务提供商管理员”。

由服务提供商管理员管理的组织

SPA 可以创建、修改和删除从属于该 SPA 的提供商组织的以下组织类型：

- 第 159 页中的 “完整组织”
- 第 159 页中的 “共享组织”

以下几节介绍了提供商组织、完整组织和共享组织。

提供商组织

提供商组织是 LDAP 目录中的一个节点，在逻辑上包含完整组织和共享组织。 提供商组织节点具有一些属性，这些属性使得 SPA 可以管理从属组织。

在 LDAP 目录中，提供商组织必须位于邮件域下。有关示例，请参见本附录后面的第 174 页中的 “样例服务提供商组织数据”。

提供商组织不能包含用户条目，而应在提供商组织下所创建的组织中置备用户。

提供商组织可存储有关在其下创建的组织的目录信息。 例如：

- 此提供商组织是否可以包含共享组织、完整组织或两者都包含
- 在此提供商组织下创建的共享组织可以使用的域名
- 可供在此提供商组织下创建的组织使用的服务类包类型和数量
- 被指定为此提供商组织的 SPA 所在位置的组织

完整组织

完整组织具有以下特征：

- 它从属于提供商组织并由 SPA 创建。
- 可以在完整组织中置备用户。

  在图 A–1 显示的示例中，`user2` 属于 `sesta.com` 域，其邮件地址为 `user2@sesta.com`。
- 完整组织拥有其自己的域（其他组织不能共享该域），并且拥有自己的唯一名称空间。

  在图 A–1 显示的示例中，完整组织 SESTA 具有域名 `sesta.com`。

共享组织

共享组织具有以下特征：

- 它从属于提供商组织并由 SPA 创建。
- 可以在共享组织中置备用户。

  在图 A–1 显示的示例中，`user5` 属于 `siroe.com` 域，其邮件地址为 `user5@siroe.com`。
- 它使用提供商组织所提供的列表中的一个或多个共享域名。

  在图 A–1 显示的示例中，共享组织 DEF 使用域名 `siroe.com`。
- 其他共享组织可以共享此组织所使用的域名。

  在图 A–1 显示的示例中，DEF 和 HIJ 组织都属于 `siroe.com` 域。

- 共享组织不具有唯一名称空间。

创建提供商组织和服务提供商管理员

在此版本的 Delegated Administrator 中，必须使用 Delegated Administrator 所提供的自定义服务提供商模板 (`da.provider.skeleton.ldif`) 来创建您自己的提供商组织和 SPA。

注 – 运行 Delegated Administrator 配置程序后，还可以在目录中安装样例提供商组织（带有从属组织）和样例 SPA。可通过在配置程序中选择**装入样例组织**来执行此操作。

但样例组织模板 (`da.sample.data.ldif`) 只是一个示例，并不是用来创建您自己的提供商组织的模板。有关此示例的详细信息，请参见本附录后面的第 174 页中的 “样例服务提供商组织数据”。

创建了提供商组织和 SPA 之后，SPA 就可以登录到 Delegated Administrator 控制台，创建和管理从属组织，并将 SPA 角色指派给该 SPA 的组织中的其他用户。但是，这些 SPA 只能管理同一个提供商组织。

要创建另一个提供商组织和管理该组织的 SPA，应再次使用自定义服务提供商模板。

本节包含以下主题：

- 第 160 页中的 “模板创建的条目”显示了在目录中安装经过编辑的模板副本后所创建的组织示例。
- 第 161 页中的 “创建提供商组织、从属组织和 SPA 所需的信息”定义了在模板中创建提供商组织、从属共享组织和 SPA 所需的参数。
- 第 166 页中的 “创建提供商组织和服务提供商管理员的步骤”说明了如何编辑模板以及如何在目录中安装信息。
- 第 168 页中的 “自定义服务提供商模板”是模板列表。

模板创建的条目

在目录中安装经过编辑的自定义服务提供商模板副本后，就创建了以下条目：

- 提供商组织
- 指定来包含 SPA 用户的从属共享组织
- 从属组织中被指派为 SPA 角色的一个用户
- 可以在其下创建完整组织的占位符节点。这些完整组织将由此提供商组织的 SPA 来管理。

图 A–2 显示了通过安装模板创建的条目示例。它是各个组织的目录信息树 (Directory Information Tree, DIT) 视图。

图 A–2 只是一个示例。组织名称、SPA 用户名以及 DIT 结构应该特定于您自己的安装。

```
o=usergroup
  o=varrius.com
  o=siroe.com
    o=MyProviderOrg
      o=MySPAUserOrg
        ou=People
           uid=user1
  o=MyProviderOrgDomainsRoot
```

图 A–2 自定义服务提供商模板：目录信息树视图

作为样例安装的自定义服务提供商模板中的节点

图 A–2 显示的示例中的节点如下：

- `o=usergroup`—用户/组数据的根后缀。
- `o=varrius.com` - 默认邮件域。
- `o=siroe.com`—提供商组织所使用的邮件域。
- `o=MyProviderOrg`—提供商组织节点。
- `o=MySPAUserOrg`—指定来包含提供商组织用户（包括被指派为 SPA 角色的用户）的从属共享组织。
- `ou=people`—必需的标准 LDAP 组织单元，用于包含用户。
- `uid=user1`—MySPAUserOrg 组织中被指派为 SPA 的用户的 uid。
- `o=MyProviderOrgDomainsRoot`—占位符节点，用于包含从属于 MyProviderOrg 提供者组织的完整组织。

创建提供商组织、从属组织和 SPA 所需的信息

要创建提供商组织、一个从属组织和 SPA，需要将自定义服务提供商模板中的参数替换为特定于您的安装的信息。

当您读取这些参数时，可以看到第 168 页中的 “自定义服务提供商模板”中显示的 `da.provider.skeleton.ldif` 列表。或者打开位于以下目录的实际 ldif 文件：

da-base`/lib/config-templates`

有关与这些参数相关联的属性的定义，请参见 *Sun Java Communications Suite Schema Reference* 中的第 5 章 "Communications Suite Delegated Administrator Classes and Attributes (Schema 2)" 和第 3 章 "Messaging Server and Calendar Server Attributes"。

定义提供商组织和从属组织的参数

要创建提供商组织和从属组织，请编辑以下参数：

- *ugldapbasedn*

  目录中的用户/组数据的根后缀。

  示例：

  ```
  o=usergroup
  ```

  ```
  dc=red,dc=iplanet,dc=com
  ```

- *maildomain_dn*

  将在其下创建提供商组织的邮件域的完整 DN。

  示例：

  ```
  o=siroe.com, o=usergroup
  ```

  ```
  o=sesta.com,o=SharedDomainsRoot,o=Business,dc=red, \
  dc=iplanet,dc=com
  ```

- *maildomain_dn_str*

  将所有逗号 (,) 均替换为下划线 (_) 的邮件域 DN。

  例如，如果邮件域 DN 为

  ```
  o=siroe.com,o=SharedDomainsRoot,o=Business,dc=red, \
  dc=iplanet,dc=com
  ```

  则邮件域 DN 字符串将为

  ```
  o=siroe.com_o=SharedDomainsRoot_o=Business_dc=red_ \
  dc=iplanet_dc=com
  ```

- *providerorg*

  提供商组织的名称。将为提供商组织所位于的目录节点给定此名称。

  此参数在 `da.provider.skeleton.ldif` 模板中会多次用到。

  示例：

  ```
  sunProviderOrgDN: o=MyProviderOrg,o=siroe.com,o=usergroup
  ```

  ```
  o=MyProviderOrg
  ```

  ```
  sunBusinessOrgBase: o=MyProviderOrgdomainsroot, o=usergroup
  ```

- *servicepackage*

  服务包名称，服务包可以被指派给从属于提供商组织的各个组织中的用户。这是一个多值参数。

  在 `da.provider.skeleton.ldif` 文件中的 "Provider Organization" 部分，您将看到以下属性：

```
sunIncludeServices: <servicepackage>
```

针对要包括在提供商组织中的每个服务包，均应添加一个 `sunIncludeServices` 属性实例和一个 *servicepackage* 参数实例。只有在此列出的这些服务包才可以被指派给从属组织中的用户。

示例：

```
sunIncludeServices: gold
sunIncludeServices: platinum
sunIncludeServices: ruby
sunIncludeServices: silver
```

如果不使用 `sunIncludeServices` 属性（即，如果删除包含 *servicepackage* 参数的行），则可以指派目录中的所有服务包。

- *domain_name*

  可以指派给提供商组织中的从属组织的域名。这是一个多值参数。

  在 `da.provider.skeleton.ldif` 文件中的“提供商组织”部分，您将看到以下属性：

  ```
  sunAssignableDomains: <domain_name>
  ```

  `sunAssignableDomains` 属性中的域名是邮件域组织的 `sunPreferredDomain` 和 `associatedDomain` 属性中的名称列表的子集（部分或全部）。（邮件域就是在其下创建了此提供商组织的组织。）

  针对要包括在提供商组织中的每个域名，均应添加一个 `sunAssignableDomains` 属性实例和一个 *domain_name* 参数实例。只有在此列出的域名才可以被指派给从属组织。

  示例：

  ```
  sunAssignableDomains: siroe.com
  sunAssignableDomains: siroe.net
  sunAssignableDomains: varrius.com
  sunAssignableDomains: sesta.com
  sunAssignableDomains: sesta.net
  ```

- *provider_sub_org*

  SPA 用户所位于的共享组织的名称。在目录中安装经过编辑的 ldif 信息后，就创建了此组织来作为共享组织，它从属于提供商组织。它被指定为包含 SPA 用户的组织。其他被指派为此提供商组织的 SPA 角色的用户都必须位于此从属共享组织。

  在 `da.provider.skeleton.ldif` 文件中的“提供商组织”部分，您将看到以下属性：

  ```
  sunProviderOrgDN:
  o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
  ```

  `sunProviderOrgDN` 属性标识了为提供商组织用户（尤其是 SPA 用户）指定的组织。

  示例：

```
sunProviderOrgDN:
o=MySPAUserOrg,o=MyProviderOrg,o=siroe.com,o=usergroup
```

- *preferredmailhost*

  作为提供商组织从属组织（SPA 用户位于其中）的首选邮件主机的计算机名。必须使用全限定域名 (Fully Qualified Fomain Name, FQDN)。

  在 `da.provider.skeleton.ldif` 文件中的“共享从属组织”部分，您将看到以下属性：

  ```
  preferredMailHost: <preferredmailhost>
  ```

  示例：

  ```
  preferredMailHost: mail.siroe.com
  ```

- *available_domain_name*

  可以指派给特定从属组织中的用户的域名。这是一个多值参数。

  available_domain_name 的值是为 `sunAssignableDomains: <domain_name>` 属性和参数给定的值的相应部分。其中 *domain_name* 适用于整个提供商组织，*available_domain_name* 适用于单个从属组织。

  在 `da.provider.skeleton.ldif` 文件中的“共享从属组织”部分，您将看到以下属性：

  ```
  sunAvailableDomainNames: <available_domain_name>
  ```

  针对您希望此从属组织从提供商组织的 `sunAssignableDomains` 属性中的域名列表中继承的每个域名，均应添加一个 `sunAvailableDomains` 属性实例和一个 *available_domain_name* 参数实例。只有在此列出的域名才可以被指派给此从属组织。

  示例：

  ```
  sunAvailableDomainNames: siroe.com
  sunAvailableDomainNames: siroe.net
  sunAvailableDomainNames: varrius.com
  ```

- *available_services*

  可供特定从属组织使用的服务包。这是一个多值参数。

  指派给从属组织的服务包是使用 `sunIncludeServices` 属性指派给整个提供商组织的服务包的子集。

  在 `da.provider.skeleton.ldif` 文件中的“共享从属组织”部分，您将看到以下属性：

  ```
  sunAvailableServices: <available_services>
  ```

  available_services 参数的格式是

  service package name: count

  其中 *count* 是一个整数。如果未指定数量，则默认值为无限数。

针对您希望此从属组织从提供商组织的 sunIncludeServices 属性中可用的服务包继承的每个服务包，均应添加一个 sunAvailableServices 属性实例和一个 *available_services* 参数实例。

示例：

```
sunAvailableServices: gold:1500
sunAvailableServices: platinum:2000
sunAvailableServices: silver:5000
```

用于定义 SPA 的参数

要创建 SPA，请编辑以下参数：

- *spa_uid*

  SPA 用户的用户 ID。

  示例：

  ```
  uid: user1
  ```

- *spa_password*

  SPA 用户的密码。

  示例：

  ```
  userPassword: x12P3&qrS
  ```

- *spa_firstname*

  SPA 用户的名字。

  示例：

  ```
  givenname: John
  ```

- *spa_lastname*

  SPA 用户的姓。

  示例：

  ```
  sn: Smith
  ```

- *spa_servicepackage*

  指派给 SPA 用户的服务包。有关服务包的信息，请参见第 1 章中的第 27 页中的 “服务包”。

  示例：

  ```
  inetCos: platinum
  ```

- *spa_mailaddress*

  SPA 用户的邮件地址。邮件地址的域部分必须是替换 *available_domain_name* 参数的域值中的一个。即，它必须是可以在 SPA 用户所位于的从属组织中使用的域。有关详细信息，请参见第 162 页中的 “定义提供商组织和从属组织的参数”。

示例：

```
mail: user1@siroe.com
```

有关如何编辑自定义服务提供商模板以及如何在目录中安装信息的说明，请参见第 166 页中的 “创建提供商组织和服务提供商管理员的步骤”。

创建提供商组织和服务提供商管理员的步骤

使用 ldif 文件 `da.provider.skeleton.ldif` 来执行以下过程。

▼ 创建提供商组织和服务提供商管理员

此过程假设您已经在目录中安装了根后缀和默认邮件域，如以下示例所示：

```
o=usergroup
   o=varrius.com
```

1 在目录中创建一个邮件域。

如果您尚未创建邮件域，请在目录中创建一个。提供商组织及其从属共享组织将使用此邮件域。

示例：

在以下示例中，`siroe.com` 是新的邮件域，`da.provider.skeleton.ldif` 文件将要在其下安装提供商组织和服务提供商管理员。

```
o=usergroup
   o=varrius.com
   o=siroe.com
```

2 复制并重命名 `da.provider.skeleton.ldif` 文件。

当您安装 Delegated Administrator 后，`da.provider.skeleton.ldif` 文件会安装在以下目录中：

da-base`/lib/config-templates`

3 编辑 `da.provider.skeleton.ldif` 文件副本中的以下参数。将这些参数替换为针对您的安装的相应值。

有关这些参数的定义，请参见第 161 页中的 “创建提供商组织、从属组织和 SPA 所需的信息”。

某些参数在 ldif 文件中多次用到。您必须搜索并替换每个参数的所有实例。

少数参数代表多值属性的值。可以复制并编辑这些参数及其相关联的属性名称，以便允许这些属性在 ldif 文件中出现多次。以下标出了多值参数。

- `<ugldapbasedn>`

- <maildomain_dn>
- <maildomain_dn_str>
- <providerorg>
- <servicepackage>（多值）
- <domain_name>（多值）
- <provider_sub_org>
- <preferredmailhost>
- <available_domain_name>（多值）
- <available_services>（多值）
- <spa_uid>
- <spa_password>
- <spa_firstname>
- <spa_lastname>
- <spa_servicepackage>
- <spa_mailaddress>

  有关与这些参数相关联的属性的定义，请参见 *Sun Java Communications Suite Schema Reference* 中的第 5 章 "Communications Suite Delegated Administrator Classes and Attributes (Schema 2)" 和第 3 章 "Messaging Server and Calendar Server Attributes" 。

4 使用 LDAP 目录工具 ldapmodify 在目录中安装提供商组织和 SPA。

例如，可以运行以下命令：

```
ldapmodify -D <directory manager> -w <password> \
-f <da.provider.finished.ldif>
```

其中

<directory manager> 是 Directory Server 管理员的用户名。

<password> 是 Directory Server 管理员的密码。

<da.provider.finished.ldif> 是要在目录中作为新提供商组织和 SPA 安装的、经过编辑的 ldif 文件的名称。

示例：

以下示例显示了安装在 siroe.com 邮件域下的组织节点和服务提供商管理员用户：

```
o=usergroup
   o=varrius.com
   o=siroe.com
     o=MyProviderOrg
       o=MySPAUserOrg
```

```
        ou=People
           uid=user1
   o=MyProviderOrgDomainsRoot
```

注意，MyProviderOrgDomainsRoot 组织位于根后缀 usergroup 之下。MyProviderOrgDomainsRoot 是由 ldif 创建的占位符节点，它保持整个组织从属于 MyProviderOrg 组织。

自定义服务提供商模板

模板 (da.provider.skeleton.ldif) 包含一些参数，您必须修改这些参数才能创建新的提供商组织和 SPA。

以下列表显示了 ldif 文件中具有参数的部分。此列表没有包含整个文件。此处不包含支持 Access Manager 所需的条目和 ACI。

您只能在 ldif 文件中修改这些参数。请勿修改文件中与 Access Manager 相关的部分。

da.provider.skeleton.ldif 文件（相关部分）

```
#
# The following parameterized values must be replaced.
#
# <ugldapbasedn>          :: Root suffix for user/group data
# <maildomain_dn>         :: Complete dn of the mail domain underneath
#                            which the provider organization will be
#                            created.
# <maildomain_dn_str>     :: The maildomain dn with all ',' replaced
#                                       by '_'. E.g.
#                            dn --\> o=siroe.com,o=SharedDomainsRoot,
#                            o=Business,dc=red,dc=iplanet,dc=com
#                            dn_str --> o=siroe.com_o=SharedDomainsRoot_
#                            o=Business_dc=red_dc=iplanet_dc=com
# <providerorg>            : Organization value for provider node.
# <servicepackage>        :: One for each service package to include.
#                            All service packages in the system
#                            may be assigned by leaving this value empty.
# <domain_name>           :: One for each DNS name which may be assigned
#                            to a subordinate organization.
#                            These names form a proper subset (some or
#                            all) of the names listed in the <maildomain>
#                            organization's sunpreferreddomain
#                            and associateddomain attributes.
# <provider_sub_org>      :: Organization value for the shared subordinate
#                            organization in which the Provider
#                            Administrator resides.
# <preferredmailhost>     :: Name of the preferred mail host for the
```

```
#                            provider's subordinate organization.
# <available_domain_name> :: one for each DNS name that an organization
#                            allows an organization admin to use when
#                            creating a user's mail address.  This is
#                            a proper subset of the values given for
#                            <domain_name> (sunAssignableDomains attribute).
# <available_services>    :: One for each service packags available to an
#                            organization (sunAvailableServices attribute).
#                            These service packages form a proper subset
#                            of the ones assigned to a provider organization
#                            - <servicepackage> (sunIncludeServices
#                            attribute).  Form is
#                            <service package name>:<count>
#                            where count is an integer.  If count is absent
#                            then default is unlimited.
# <spa_uid>               :: The uid for the service provider administrator.
# <spa_password>          :: The password for the service provider
#                            administrator.
# <spa_firstname>         :: First name of the service provider
#                            administrator.
# <spa_lastname>          :: Last name of the service provider
#                            administrator.
# <spa_servicepackage>    :: Service package assigned to the service
#                            provider administrator.
# <spa_mailaddress>       :: The spa's mail address. The domain part of the
#                            mail address must be one of the values used for
#                            <available_domain_name>.
#


#
# Provider Organization
#
dn: o=<providerorg>,<maildomain_dn>
changetype: add
o: <providerorg>
objectClass: top
objectClass: sunismanagedorganization
objectClass: sunmanagedorganization
objectClass: organization
objectClass: sunManagedProvider
sunAllowBusinessOrgType: full
sunAllowBusinessOrgType: shared
sunBusinessOrgBase: o=<providerorg>domainsroot,<ugldapbasedn>
sunIncludeServices: <servicepackage>
sunAssignableDomains: <domain_name>
sunAllowMultipleDomains: true
sunAllowOutsideAdmins: false
```

```
sunProviderOrgDN: o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# Full Organizations node
#
dn: o=<providerorg>DomainsRoot,<ugldapbasedn>
changetype: add
o: <providerorg>DomainsRoot
objectClass: top
objectClass: organization
objectClass: sunmanagedorganization
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# Provider Admin Role shared organizations
#
dn: cn=Provider Admin Role,o=<providerorg>,<maildomain_dn>
changetype: add
cn: Provider Admin Role
objectClass: ldapsubentry
objectClass: nssimpleroledefinition
objectClass: nsroledefinition
objectClass: nsmanagedroledefinition
objectClass: iplanet-am-managed-role
objectClass: top
iplanet-am-role-description: Provider Admin

#
# Provider Admin Role full organizations
#
dn: cn=Provider Admin Role,o=<providerorg>DomainsRoot,<ugldapbasedn>
changetype: add
cn: Provider Admin Role
objectClass: ldapsubentry
objectClass: nssimpleroledefinition
objectClass: nsroledefinition
objectClass: nsmanagedroledefinition
objectClass: iplanet-am-managed-role
objectClass: top
```

```
iplanet-am-role-description: Provider Admin

#
# Shared Subordinate Organization. Includes 1 user who is
# the Provider Administrator.
#
dn: o=<provider_sub_org>,=<providerorg>,<maildomain_dn>
changetype: add
preferredMailHost: <preferredmailhost>
sunNameSpaceUniqueAttrs: uid
o: <provider_sub_org>
objectClass: inetdomainauthinfo
objectClass: top
objectClass: sunismanagedorganization
objectClass: sunnamespace
objectClass: sunmanagedorganization
objectClass: organization
objectClass: sunDelegatedOrganization
objectClass: sunMailOrganization
sunAvailableDomainNames: <available_domain_name>
sunAvailableServices: <available_services>
sunOrgType: shared
sunMaxUsers: -1
sunNumUsers: 1
sunMaxGroups: -1
sunNumGroups: 0
sunEnableGAB: true
sunAllowMultipleServices: true
inetDomainStatus: active
sunRegisteredServiceName: GroupMailService
sunRegisteredServiceName: DomainMailService
sunRegisteredServiceName: UserMailService
sunRegisteredServiceName: iPlanetAMAuthService
sunRegisteredServiceName: UserCalendarService
sunRegisteredServiceName: iPlanetAMAuthLDAPService
sunRegisteredServiceName: DomainCalendarService
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

dn: ou=People,o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
ou: People
objectClass: iplanet-am-managed-people-container
objectClass: organizationalUnit
objectClass: top
```

```
dn: ou=Groups,o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
ou: Groups
objectClass: iplanet-am-managed-group-container
objectClass: organizationalUnit
objectClass: top
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# User - provider administrator
#
dn: uid=<spa_uid>,ou=People,o=<provider_sub_org>,o=<providerorg>, \
        <maildomain_dn>
changetype: add
sn: <spa_lastname>
givenname: <spa_firstname>
cn:  <spa_firstname> <spa_lastname>
uid: <spa_uid>
iplanet-am-modifiable-by: cn=Top-level Admin Role,<ugldapbasedn>
objectClass: inetAdmin
objectClass: top
objectClass: iplanet-am-managed-person
objectClass: iplanet-am-user-service
objectClass: iPlanetPreferences
objectClass: person
objectClass: organizationalPerson
objectClass: inetuser
objectClass: inetOrgPerson
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: inetSubscriber
objectClass: userPresenceProfile
objectClass: icsCalendarUser
mailhost: <preferredmailhost>
mail: <spa_mailaddress>
maildeliveryoption: mailbox
mailuserstatus: active
inetCos: <spa_servicepackage>
inetUserStatus: Active
nsroledn: cn=Provider Admin Role,o=<providerorg>,<maildomain_dn>
userPassword: <spa_password>
```

创建共享从属组织和完整从属组织

当您创建了提供商组织和 SPA 之后，SPA 就可以创建并管理从属于该提供商组织的共享组织和完整组织。SPA 使用 Delegated Administrator 控制台来完成这些任务。

以下任务概述了创建共享组织或完整组织的关键步骤。此任务没有说明如何输入使用“创建新组织”向导创建组织时所显示的全部信息。有关“创建新组织”向导的详细说明，请参见 Delegated Administrator 控制台联机帮助。

▼ 创建共享从属组织或完整从属组织的步骤

1 **启动 Delegated Administrator 控制台。**

转至以下 url：

`http://`*host* `:`*port*`/da`

其中

host 是 Web 容器主机

port 是 Web 容器端口

例如：

```
http://siroe.com:8080/da
```

Delegated Administrator 控制台登录窗口将会出现。

2 **使用 SPA 登录 ID 和密码登录到 Delegated Administrator 控制台。**

前面一节第 160 页中的 “创建提供商组织和服务提供商管理员”介绍了如何创建 SPA。

“服务提供商管理员”页将会出现。默认选中的是“组织”选项卡。此页显示了从属于该 SPA 的提供商组织的组织。

3 **单击新建组织。**

“创建新组织”向导将会出现。有关在“创建新组织”向导中输入和选择信息的详细信息，请参见 Delegated Administrator 控制台联机帮助。

4 **在“组织信息”面板中输入信息，然后单击下一步。**

“联系信息”面板将会出现。

5 **在“联系信息”面板中输入信息，然后单击下一步。**

“帐户信息”面板将会出现。

6 **选择要创建共享组织还是完整组织。**

在“帐户信息”面板中，确定新组织将是共享组织还是完整组织。

共享组织将使用与其他组织共享的现有域。

完整组织将拥有自己的唯一域。

- 要创建共享组织，请单击**从可用域中进行选择**单选按钮。

  从下拉式列表中选择一个域。

  注 – 创建共享组织时，会从现有父域继承日历服务的详细信息。因此，不用为新组织输入日历服务信息。“日历服务详细信息”面板不会出现在“创建新组织”向导中。此外，创建了共享组织后，“日历服务详细信息”面板也不会出现在该组织的“属性”页中。

- 要创建完整组织，请单击**新建域**单选按钮。

  在文本框中输入一个新的邮件域名。例如：`siroe.com`。

  您可以根据需要在**新域的别名**文本框中为新域输入别名。

7 **在“创建新组织”向导的其余面板中输入信息。**

有关这些面板的详细信息，请参见 Delegated Administrator 控制台联机帮助。

样例服务提供商组织数据

运行 Delegated Administrator 配置程序 `config-commda` 时，您可以选择在目录中安装样例组织数据（在 ldif 文件中定义）。（运行配置程序时，在**服务软件包和组织样例**面板中选择**加载样例组织**。）配置程序会将 `da.sample.data.ldif` 文件添加到 LDAP 目录树。

此 ldif 文件只是一个示例，并不是用来创建您自己的提供商组织的模板。要创建新的提供商组织，请参见第 161 页中的 “创建提供商组织、从属组织和 SPA 所需的信息”。

由样例数据提供的组织

图 A–1 显示了由样例 ldif 文件提供的组织结构的逻辑视图。（图 A–1 中增加了该文件中不存在的共享组织 HIJ。）

样例 ldif 文件在根后缀节点下包含以下组织：

- VIS 提供商组织。以下组织由 VIS 提供商组织的 SPA 来管理：
  - SESTA，一个完整组织。SESTA 组织拥有自己的域 `sesta.com`。

  - DEF，一个共享组织。DEF 组织使用共享域 `siroe.com`。
- ESG 提供商组织。没有为此提供商组织定义任何从属组织。

ldif 文件为这些组织定义了以下管理员角色：

- VIS 提供商组织的 SPA (`user2@abc.com`)
- ESG 提供商组织的 SPA (`user2_def`)
- SESTA 组织的 OA (`user1@abc.com`)
- DEF 组织的 OA (`user1_def`)

逻辑分层结构和目录信息树

在三层目录结构中，目录信息树 (Directory Information Tree, DIT) 与图 A–1 中显示的逻辑视图不完全一样。该 DIT 中所实现的组织的分层结构有些不同。

例如，在 DIT 中，完整域必须直接位于根后缀下。因此，应在根后缀下添加域节点来存储有关共享域（由共享组织使用）和完整组织（拥有自己的域）的 LDAP 信息。

样例组织数据：目录信息树视图

图 A–3 显示了样例组织数据的目录信息树 (Directory Information Tree, DIT) 视图。

图 A–3 中显示的示例（与图 A–1 中显示的逻辑视图相似）包含以下组织：

- VIS 和 ESG（提供商组织）
- DEF，一个从属于 VIS 提供商组织的共享组织
- SESTA，一个从属于 VIS 提供商组织的完整组织

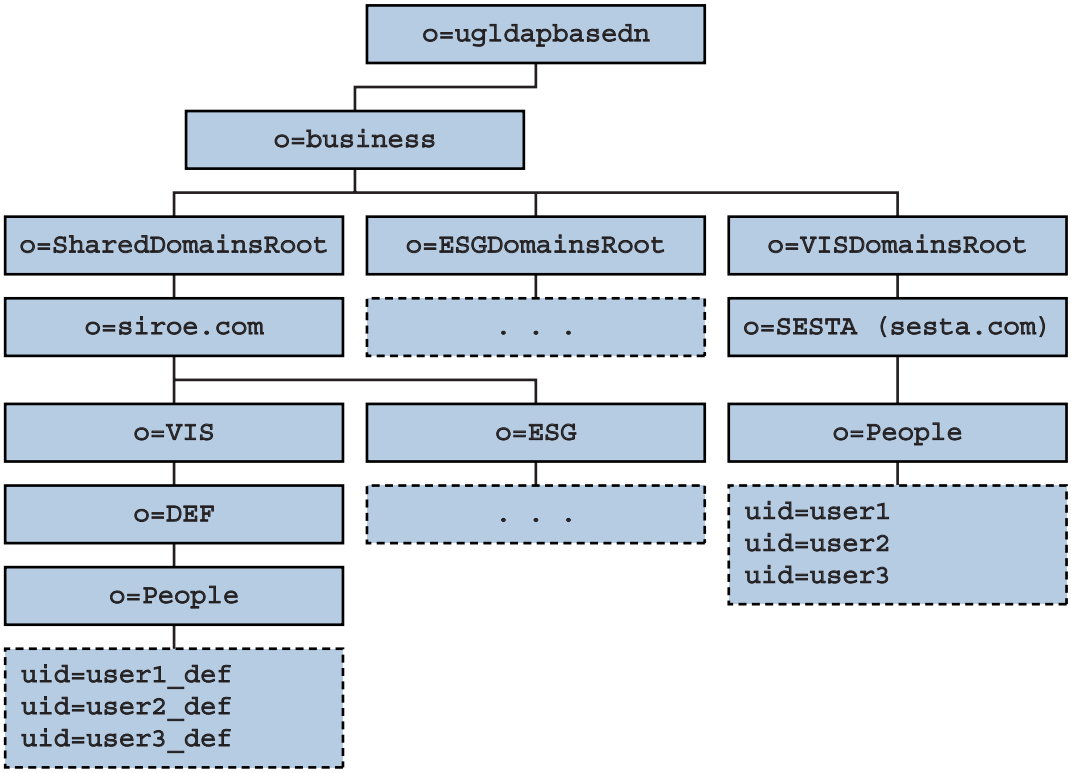

图 A–3 样例组织数据：目录信息树视图

样例目录信息树中的节点

样例组织文件 (`da.sample.data.ldif`) 中的节点如下：

- *ugldapbasedn*—此参数表示根后缀。
- `o=business`—包含目录中所有业务的节点。
- `o=SharedDomainsRoot`—包含共享组织使用的域所需的节点。

  在此目录信息树中，从属于不同服务提供商组织的共享组织可以使用同一个共享域。这是因为这两个提供商组织都具有 `SharedDomainsRoot` 节点下的节点。
- `o=ESGDomainsRoot` 和 `o=VISDomainsRoot`—这些节点包含从属于 ESG 和 VIS 提供商组织的所有完整组织。

  每个管理完整组织的提供商组织都必须具有此级（在根后缀下）节点。

  `ESGDomainsRoot` 或 `VISDomainsRoot` 下可以存在多个完整组织（每个都具有自己的域）。
- `o=siroe.com`—共享域。它由共享组织 DEF 使用。

- o=VIS 和 o=ESG—这些提供商组织节点包含从属于 VIS 和 ESG 提供商组织的所有共享组织。

  例如，共享组织 DEF 从属于 VIS 提供商组织。
- o=SESTA—完整组织。它拥有自己的域，sesta.com。
- o=DEF—共享组织。它使用域 siroe.com。
- ou=people—必需的标准 LDAP 组织单元，用于包含用户。

样例目录信息树中的用户 DN

图 A–3 中显示的样例组织文件中的某些用户 DN 如下：

- 对于名为 user1_def 的用户（该用户属于 DEF 组织）：

  ```
  dn: uid=user1_def,ou=People,o=DEF,o=VIS,o=siroe.com, \
  o=SharedDomainsRoot,o=Business,ugldapbasedn
  ```
- 对于名为 user1 的用户（该用户属于 SESTA 组织）：

  ```
  dn: uid=user1,ou=People,o=SESTA,o=VISDomainsRoot, \
  o=Business,ugldapbasedn
  ```

◆ ◆ ◆ 附 录 B

属性值和日历时区

属性值

表 B–1 中列出的属性可以在以下命令中与 -P 选项结合使用：第 115 页中的 “commadmin domain create” 和 第 119 页中的 “commadmin domain modify” 。这些属性要么是位导向属性，要么是多值属性。

表 B–1 -P 选项的属性

属性	值	说明
createLowerCase	yes/no	指定是否为新用户创建小写日历。另外，指定在查找日历时是否查找小写日历。
filterPrivateEvents	yes/no	指定在查询服务器时是否过滤专用或保密事件。
fbIncludeDefCal	yes/no	指定是否在用户的 freebusy-calendar-list 中包含用户的默认日历。
subIncludeDefCal	yes/no	指定是否在用户的 subscribed-calendar-list 中包含用户的默认日历。
resourceDefaultAcl	yes/no	指定是否对资源日历使用默认的 ACL。
calmasterCred	字符串	被指定为 Calendar Server 管理员的用户的证书。
calmasterUid	字符串	service.admin.calmaster.userid
calmasterAccessOverride	yes/no	指定 Calendar Server 管理员是否可以覆盖访问控制。

表 B–1 -P 选项的属性 （续）

属性	值	说明
setPublicRead	yes/no	将默认的用户日历设置为公共读或专用写。如果选择了 no，就将用户日历设置为了专用读或专用写。
uiBaseUrl	字符串	基服务器地址，例如 "https://proxyserver/"
uiConfigFile	字符串	用户界面配置文件。
uiProxyUrl	字符串	要附加在 HTML 用户界面的 JavaScript 文件中的 Proxy Server 地址。例如 https://web_portal.iplanet.com/
domainAccess	字符串	域访问控制字符串。用于进行跨域搜索。由一个或多个 ACI 段（以分号分隔）组成的访问控制信息 (Access Control Information, ACI) 字符串。 ACI 用于在跨域搜索中批准外部域对本域进行搜索。注意，ACI 字符串可能包括指定的外部域名。 有关 Calendar Server ACI 的更多信息，请参见 Sun Java System Calendar Server WCAP Developer's Guide 中的第 2 章 "Calendar Server WCAP Common Topics" 中的 "Access Control Information"。
uiAllowAnyone	yes/no	指定是否允许 HTML 用户界面显示和使用 "Everybody" ACL。
allowProxyLogin	yes/no	指定是否允许代理登录。

表 B–2 中列出的属性可以在以下命令中与 -R 选项结合使用：第 115 页中的 “commadmin domain create” 和 第 119 页中的 “commadmin domain modify”。这些属性具有位导向值。

有关 WCAP 和 WCAP set-userprefs 命令的信息，请参见 *Sun Java System Calendar Server Developer's Guide*。

表 B–2 -R 选项的属性

属性	值	说明
allowUserDoubleBook	bit 8	允许在同一时段内多次安排此日历。
allowResourceDoubleBook	bit 9	允许在同一时段内多次安排此资源日历。

表 B–2 -R 选项的属性 （续）

属性	值	说明
allowModifyUserPreferences	bit 4	允许 Calendar Server 管理员为用户修改用户首选项。
allowModifyPassword	bit 5	允许用户通过此服务器更改他们的密码。
allowCalendarCreation	bit 0	允许创建日历。
allowCalendarDeletion	bit 1	允许删除日历。
allowPublicWritableCalendars	bit 2	允许用户拥有公共可写日历。
allowSetCn	bit 10	允许 set-userprefs.wcap 修改 cn 用户首选项。
allowSetGivenName	bit 11	允许 set_userprefs.wcap 修改 givenname 用户首选项。
allowSetGivenMail	bit 12	允许 set_userprefs.wcap 修改 mail 用户首选项。
allowSetPrefLang	bit 13	允许 set_userprefs.wcap 修改 preferredlanguage 用户首选项。
allowSetSn	bit 14	允许 set-userprefs.wcap 修改 sn 用户首选项。

日历时区字符串

以下时区字符串可以在 第 115 页中的 “commadmin domain create” 、第 119 页中的 “commadmin domain modify” 、第 137 页中的 “commadmin resource create” 、第 141 页中的 “commadmin resource modify” 、第 144 页中的 “commadmin user create” 和 第 149 页中的 “commadmin user modify” 命令中与 -T 时区选项结合使用：

您也可以添加新的时区并将其设置为默认时区。有关详细信息，请参见第 100 页中的 “添加新的日历时区” 。

- Africa/Cairo
- Africa/Casablanca
- Africa/Johannesburg
- Africa/Lagos
- Africa/Tripoli
- Africa/Windhoek
- America/Adak
- America/Anchorage
- America/Buenos_Aires
- America/Caracas
- America/Chicago

- America/Costa_Rica
- America/Cuiaba
- America/Denver
- America/Godthab
- America/Grand_Turk
- America/Halifax
- America/Havana
- America/Indianapolis
- America/Los_Angeles
- America/Miquelon
- America/New_York
- America/Phoenix
- America/Port-au-Prince
- America/Santiago
- America/Sao_Paulo
- America/St_Johns
- Asia/Alma-Ata
- Asia/Amman
- Asia/Anadyr
- Asia/Aqtau
- Asia/Aqtobe
- Asia/Baku
- Asia/Bangkok
- Asia/Beirut
- Asia/Bishkek
- Asia/Calcutta
- Asia/Dacca
- Asia/Irkutsk
- Asia/Jerusalem
- Asia/Kabul
- Asia/Kamchatka
- Asia/Karachi
- Asia/Katmandu
- Asia/Krasnoyarsk
- Asia/Magadan
- Asia/Novosibirsk
- Asia/Rangoon
- Asia/Riyadh
- Asia/Shanghai
- Asia/Tokyo
- Asia/Ulan_Bator
- Asia/Vladivostok
- Asia/Yakutsk
- Asia/Yekaterinburg

- Asia/Yerevan
- Atlantic/Azores
- Atlantic/Cape_Verde
- Atlantic/South_Georgia
- Atlantic/Stanley
- Australia/Adelaide
- Australia/Brisbane
- Australia/Darwin
- Australia/Hobart
- Australia/Lord_Howe
- Australia/Sydney
- Europe/Bucharest
- Europe/Istanbul
- Europe/London
- Europe/Minsk
- Europe/Moscow
- Europe/Paris
- Europe/Riga
- Europe/Samara
- Europe/Simferopol
- Europe/Warsaw
- Pacific/Apia
- Pacific/Auckland
- Pacific/Chatham
- Pacific/Easter
- Pacific/Fiji
- Pacific/Gambier
- Pacific/Guadalcanal
- Pacific/Honolulu
- Pacific/Kiritimati
- Pacific/Marquesas
- Pacific/Norfolk
- Pacific/Noumea
- Pacific/Pitcairn
- Pacific/Rarotonga
- Pacific/Tongatapu

◆ ◆ ◆ 附 录 C

调试 Delegated Administrator

通过检查由 Delegated Administrator 组件、Delegated Administrator 被部署到的 Web 容器以及由 Directory Server 和 Access Manager 生成的日志文件，可以获得有关 Delegated Administrator 的日志信息。

本附录包含以下主题：

调试命令行实用程序

要调试 Delegated Administrator 实用程序 (`commadmin`)，可以通过在 `commadmin` 命令中使用 `-v` 选项来打印客户机中的调试消息。

Delegated Administrator 控制台日志

Delegated Administrator 控制台会创建运行时日志文件：

- 默认日志文件名：`da.log`
- 默认位置：`/opt/SUNWcomm/log`

通过编辑名为 `logger.properties` 的日志属性文件，可以指定自己的日志文件。

▼ 指定自己的 Delegated Administrator 控制台日志文件

1 **在文本编辑器中打开 `logger.properties` 文件。**

`logger.properties` 文件默认情况下位于以下目录：

da-base`/data/da/WEB-INF/classes/com/sun/comm/da/resources`

2 **您可以更改 logger.properties 文件中的以下属性：**

- `da.logging.enable=yes` 或 `no`

  其中 `yes` 表示启用日志记录，`no` 表示禁用日志记录。

  默认情况下禁用日志记录。要启用日志记录，必须将此值设置为 `yes`。

- `da.log.file=`*full pathname*

  指定日志记录语句写入的目录和文件。此属性用于将 `da.log` 更改为您指定的文件名和位置。

3 **将编辑的 `logger.properties` 文件重新部署到 Delegated Administrator 控制台所使用的 Web 容器。**

必须运行脚本将自定义 `logger.properties` 文件部署到您的 Web 容器，更改才会生效。

有关如何将自定义的属性文件部署到特定 Web 容器的说明，请参见第 92 页中的 “部署自定义配置文件”。

Delegated Administrator 服务器日志

您可以创建 Delegated Administrator 服务器日志，其中包含由安装在 Web 容器中的 Delegated Administrator servlet 生成的调试语句。

要执行此操作，可启用调试 servlet 以记录 Delegated Administrator servlet 执行过程中的调试消息。

您可以使用 `commadmin debug log` 命令将 Delegated Administrator 服务器消息写入到调试日志中。

`-f` 选项指定日志的完整路径名和文件名。

`-t` 选项允许您在将调试消息写入日志和关闭调试日志记录之间进行切换。

例如，输入以下命令：

```
commadmin debug log -D paul -n sesta.com -w bolton \
-t on -f /tmp/debug.log
```

上述命令会将 Debug servlet 的消息记录到以下路径和文件中：

`/tmp/debug.log`

仅能在 `/tmp/` 或 `/var/tmp/` 目录中创建日志。

只要您重新启动 Web 容器，则必须再次运行 `commadmin debug log` 命令。

Web 容器服务器日志

通过检查由 Web 容器生成的服务器日志，可以进一步调试 Delegated Administrator。

Web Server 6.*x*

Web Server 6.*x* 可维护位于以下路径的访问日志和错误日志：

web_server6_base`/https-`*host.domain*`/logs`

其中

- *web_server_base* 是 Web Server 6.*x* 软件的安装路径。例如：`/opt/SUNWwbsvr`。
- *host.domain* 是运行 Web Server 6.*x* 的计算机的主机名和域名。

Web Server 7.*x*

Web Server 7.*x* 可维护位于以下路径的访问日志和错误日志：

web_server7_config_base`/https-` *host.domain*`/logs`

其中

- *web_server7_config_base* 是安装 Web Server 7.*x* 配置和日志文件的路径位置。例如：`/var/opt/SUNWwbsvr7`。
- *host.domain* 是运行 Web Server 7.*x* 的计算机的主机名和域名。

Application Server 7.*x*

Application Server 7.*x* 可维护位于以下路径的访问日志和错误日志：

/application_server7_base`/domains/domain1/server1/logs`

其中

- *application_server7_base* 是 Application Server 7.*x* 软件的安装路径。

Application Server 8.*x*

Application Server 8.*x* 可维护位于以下路径的访问日志和错误日志。

服务器日志 :

/application_server8_base/domains/domain1/logs

访问日志 :

/application_server8_base/domains/domain1/logs/access/server_access_log

其中

- *application_server8_base* 是 Application Server 8.*x* 软件的安装路径。

Directory Server 日志和 Access Manager 日志

通过检查由 Directory Server 和 Access Manager 生成的日志，可以进一步调试 Delegated Administrator。

Directory Server

Directory Server 可维护位于以下路径的访问日志和错误日志 :

/var/opt/mps/serverroot/slapd-*hostname* /logs

其中

- *hostname* 是运行 Directory Server 的计算机名。

Access Manager

Access Manager 可维护位于以下路径的日志文件 :

/var/opt/SUNWam/debug

上述路径包含 amProfile 日志和 amAuth 日志。

/var/opt/SUNWam/logs

上述路径包含 amAdmin.access 日志和 amAdmin.error 日志。

◆ ◆ ◆ 附 录 D

Delegated Administrator 性能调节

以下主题介绍了如何调节 Delegated Administrator 和相关软件以提高 Delegated Administrator 的性能：

- 第 189 页中的 “更快显示用户、组和组织”
- 第 191 页中的 “增加 JVM （Java 虚拟机）堆大小”
- 第 193 页中的 “提高 Directory Server 索引阈值”

除了遵循本附录中所述的原则外，您还可以通过合并和减少目录中的默认 ACI 数量来提高 Directory Server 的性能。有关信息，请参见附录 E。

更快显示用户、组和组织

如果组织中包含多个用户，则 Delegated Administrator 控制台显示“用户”列表页所用的时间可能会较长。如果您试图在该页装入现有用户的过程中创建或编辑用户，将会发生错误。在该页准备就绪之前，不要单击任何按钮或链接。

同样，如果目录中包含多个组织或组，则打开“组织”页或“组”页所用的时间也会较长。

如果装入这些页所用的时间太长，您可以将通配符搜索属性设置为足够低的值，以便使这些页快速装入。

这些属性为

jdapi-wildusersearchmaxresults	用于用户的搜索属性。
jdapi-groupsmaxsearchresults	用于组的搜索属性。
jdapi-wildorgsearchmaxresults	用于组织的搜索属性。

通配符搜索属性的限制如下：

`-1`	返回所有结果。（显示所有用户、组或组织。） `-1` 为默认值。
`0`	不进行搜索。（不显示用户、组或组织。）

n (>0)　返回 *n* 个（指定的结果数）。

▼ 更快显示“用户”页的步骤

1. **打开 resource.properties 文件。**

   resource.properties 文件位于以下目录中：

   da-base/data/WEB-INF/classes/sun/comm/cli/server/servlet

2. **将 jdapi-wildusersearchmaxresults 的值设置为一个较低的值。例如：**

   ```
   jdapi-wildusersearchmaxresults=50
   ```

   或者也可以将该值设置为 0 以不显示用户。在 Delegated Administrator 控制台中，使用**搜索**下拉式列表来搜索指定的用户。

3. **将编辑的 resource.properties 文件重新部署到 Delegated Administrator 服务器使用的 Web 容器。**

   必须运行脚本将自定义的 resource.properties 文件部署到您的 Web 容器，更改才会生效。

   有关如何将自定义的属性文件部署到特定 Web 容器的说明，请参见第 92 页中的 “部署自定义配置文件”。

▼ 更快显示“组”页的步骤

1. **打开 resource.properties 文件。**

   resource.properties 文件位于以下目录中：

   da-base/data/WEB-INF/classes/sun/comm/cli/server/servlet

2. **将 jdapi-groupsmaxsearchresults 的值设置为一个较低的值。例如：**

   ```
   jdapi-groupsmaxsearchresults=50
   ```

   或者也可以将该值设置为 0 以不显示组。在 Delegated Administrator 控制台中，使用**搜索**下拉式列表来搜索指定的组。

3. **将编辑的 resource.properties 文件重新部署到 Delegated Administrator 服务器使用的 Web 容器。**

   必须运行脚本将自定义的 resource.properties 文件部署到您的 Web 容器，更改才会生效。

有关如何将自定义的属性文件部署到特定 Web 容器的说明，请参见第 92 页中的 “部署自定义配置文件” 。

▼ 更快显示“组织”页的步骤

1 **打开 `resource.properties` 文件。**

`resource.properties` 文件位于以下目录中：

da-base`/data/WEB-INF/classes/sun/comm/cli/server/servlet`

2 **将 `jdapi-wildorgsearchmaxresults` 的值设置为一个较低的值。例如：**

```
jdapi-wildorgsearchmaxresults=10
```

或者也可以将该值设置为 `0`，不显示任何组织。在 Delegated Administrator 控制台中，使用**搜索**下拉式列表来搜索指定的组织。

3 **将编辑的 `resource.properties` 文件重新部署到 Delegated Administrator 服务器使用的 Web 容器。**

必须运行脚本将自定义的 `resource.properties` 文件部署到您的 Web 容器，更改才会生效。

有关如何将自定义的属性文件部署到特定 Web 容器的说明，请参见第 92 页中的 “部署自定义配置文件” 。

增加 JVM（ Java 虚拟机 ）堆大小

要提高常用 Delegated Administrator 功能（例如显示页面和执行搜索）的性能，可以增加 Delegated Administrator 被部署到的 Web 容器所使用的 Java 虚拟机 (Java Virtual Machine, JVM) 堆大小。如果该 Web 容器的 JVM 堆大小过小，就可能会影响性能。

JVM 堆大小由以下 JVM 选项设置：

```
-Xmx<n>m
```

其中 <*n*> 是指堆大小（单位是 MB）。

通常， <*n*> 被设置为 `256m`。

以下任务概述了如何为 Web Server 和 Application Server 设置较大的 JVM 堆大小。

▼ 增加 Web Server 6.*x* JVM 堆大小的步骤

1. **登录到 Web Server Administration Server。**
2. **在 Java 选项卡下，选择“JVM 选项”。**
3. **编辑“**`-Xmx256m`**”选项。**
   此选项用于设置 JVM 堆大小。
4. **将“**`-Xmx256m`**”选项设置为一个较高的值，例如** `Xmx1024m`**。**
5. **保存该新设置。**

更多信息 Web Server 文档

有关使用 Web Server Administration Server 和设置 JVM 的详细信息，请参见 Sun Java System Web Server 管理员指南和 Web Server Performance Tuning, Sizing, and Scaling Guide。

▼ 增加 Web Server 7.*x* JVM 堆大小

1. **登录到 Web Server Administration Server。**
2. **在“ 配置任务 ”部分，选择“ 编辑 Java 设置 ”。**
3. **单击“ JVM 设置 ”选项卡以显示 JVM 选项。**
4. **编辑“**`-Xmx256m`**”选项。**
   此选项用于设置 JVM 堆大小。
5. **将“**`-Xmx256m`**”选项设置为一个较高的值，例如** `Xmx1024m`**。**
6. **保存该新设置。**

更多信息 Web Server 文档

有关使用 Web Server Administration Server 和设置 JVM 的详细信息，请参见 Sun Java System Web Server 管理员指南和 Web Server Performance Tuning, Sizing, and Scaling Guide。

▼ 增加 Application Server JVM 堆大小的步骤

1. **登录到 Application Server Administration Server。**
2. **导航至 JVM 选项。**
3. **编辑“-Xmx256m”选项。**
   此选项用于设置 JVM 堆大小。
4. **将“-Xmx256m”选项设置为一个较高的值，例如 Xmx1024m。**
5. **保存该新设置。**

更多信息 Application Server 文档

有关使用 Application Server Administration Server 和设置 JVM 选项的详细信息，请转至 Sun Java System Application Server Documentation Center 并选择 "JVM Advanced Settings"。或者，请参见《Sun Java System Application Server Enterprise Edition 8.1 2005Q4 Performance Tuning Guide》中的 "Tuning the Java Runtime System"。

提高 Directory Server 索引阈值

要提高 Delegated Administrator 功能（例如进行搜索和显示用户）的性能，可以增加 Directory Server 搜索目录所使用的索引阈值。

当 Directory Server 搜索大量 LDAP 对象时，如果阈值被设置为较低的值，则该索引可能会在搜索完成之前就占用完所有空间。剩余的搜索操作将在不进行索引的情况下执行，这会降低搜索操作的速度。

注意 – 仅当您是一名有经验的 Directory Server 管理员时才能执行此操作。

要将索引阈值设置为较高的值，请更改 `dse.ldif` 文件中的 `nssldap-allidsthreshold` 选项的值。

此选项可能被设置为如以下所示的值：

```
nssldap-allidsthreshold: 4000
```

将 `nssldap-allidsthreshold` 设置为一个较高的值。例如：

```
nssldap-allidsthreshold: 200000
```

有关 All IDs 阈值的详细信息，请参见 Sun Java System Directory Server 管理指南的“编制目录数据索引”中的“管理索引”。 有关 `nssldap-allidsthreshold` 选项的定义，请参见 Sun Java System Directory Server Administration Reference 的 "Server Configuration Reference" 中的 "Database Configuration Attributes"。

◆ ◆ ◆ 附 录 E

合并 ACI 以提高 Directory Server 的性能

本附录介绍了以下主题：

简介

将 Access Manager 与 Messaging Server 一起安装并使用 LDAP Schema 2 目录时，一开始会在该目录中安装大量访问控制指令 (Access Control Instruction, ACI)。很多默认的 ACI 对 Messaging Server 来说是不需要的或用不到。

由于在运行时需要检查这些 ACI，因此会影响 Directory Server 的性能，从而影响 Messaging Server 的查找操作和其他目录操作的性能。

可以通过合并和精简目录中的默认 ACI 数量来提高 Directory Server 的性能。合并 ACI 还会使它们更易于管理。

精简 ACI 的方法如下：

- 合并、优化和削减冗余的 ACI
- 修改 ACI 以使用更简单、更有效的语法
- 将多个不同的 ACI 合并（在根后缀处）
- 清除未使用的 ACI
- 对于具有多个组织的目录，允许分别删除各个组织节点上的组织 ACI。

本附录首先介绍了如何使用 ldif 文件 (`replacment.acis.ldif`) 来合并根后缀处的 ACI 并从目录中删除未使用的 ACI。有关详细信息，请参见下面的第 196 页中的 “合并和删除 ACI”。

接下来，本附录将分析每个 ACI 并建议一种对其进行处理的方法：通过删除和修改使该 ACI 更有效，或者重写该 ACI。

请注意，这些建议存在以下约束：

- 最终用户无法访问 Directory 控制台
- 最终用户无法访问 Access Manager 控制台。

考虑到这些约束，您必须自行确定（根据您的安装要求）是否可以使用 ldif 文件来合并和删除 ACI，或者是否需要保留目录中现有的某些 ACI。

有关详细信息，请参见本附录后面的第 201 页中的 “对现有 ACI 的分析”。

然后，本附录将介绍通过 `replacement.acis.ldif` 文件合并的 ACI。本附录列出了在合并之前现有的 ACI 以及在合并之后经过修改的 ACI。有关详细信息，请参见本附录后面的第 218 页中的 “ACI 合并方式分析”。

最后，本附录将列出 `replacement.acis.ldif` 所放弃的 ACI。有关详细信息，请参见本附录后面的第 226 页中的 “要放弃的未使用的 ACI 列表”。

合并和删除 ACI

本节列出的 ldif 文件 `replacement.acis.ldif` 会把合并后的 ACI 安装在根后缀处并从目录中删除未使用的 ACI。此 ldif 文件是由 Delegated Administrator 提供的，位于以下目录中：

da-base`/lib/config-templates`

使用 `ldapmodify` 命令将 `replacement.acis.ldif` 文件应用于目录后，`ldapmodify` 命令会删除根后缀处的全部 `aci` 属性实例，并用 `replacement.acis.ldif` 文件中的 ACI 来替换这些 ACI。

因此，此过程首先会从根后缀处删除**全部** ACI，然后用下面列出的一组 ACI 来替换它们。如果目录中包含由其他应用程序（例如 Portal Server）生成的 ACI，则应该将这些 ACI 保存到一个文件中，然后在应用 `replacement.acis.ldif` 文件之后将这些 ACI 重新应用于目录。

有关使用此 ldif 文件来清理 ACI 的说明，请参见第 199 页中的 “替换 ACI 的步骤”。

replacement.acis.ldif 文件

```
dn: $rootSuffix
changetype: modify
replace: aci
aci: (targetattr = "*")(version 3.0; acl "Configuration Administrator";
```

```
   allow (all)
   userdn= ” ldap:///uid=admin,ou=Administrators,ou=TopologyManagement,
o=NetscapeRoot ” ;)
aci: (target= ” “ ldap:///$rootSuffix ” )
  (targetfilter=(!(objectclass=sunServiceComponent)))
  (targetattr != “ userPassword||passwordHistory
   ||passwordExpirationTime||passwordExpWarned||passwordRetryCount
  ||retryCountResetTime||accountUnlockTime||passwordAllowChangeTime ” )
  (version 3.0; acl “ anonymous access rights ” ;
   allow (read,search,compare)
   userdn = “ ldap:///anyone ” ; )
aci: (targetattr != “ nsroledn||aci||nsLookThroughLimit||nsSizeLimit
  ||nsTimeLimit||nsIdleTimeout||passwordPolicySubentry||passwordExpiration
    Time
  ||passwordExpWarned||passwordRetryCount||retryCountResetTime
  ||accountUnlockTime||passwordHistory||passwordAllowChangeTime||uid||mem
    berOf
  ||objectclass||inetuserstatus||ou||owner||mail||mailuserstatus
  ||memberOfManagedGroup||mailQuota||mailMsgQuota||mailhost
  ||mailAllowedServiceAccess||inetCOS||mailSMTPSubmitChannel ” )
  (version 3.0; acl “ Allow self entry modification ” ;
  allow (write)
  userdn = ” ldap:///self ” ;)
aci: (targetattr != “  aci || nsLookThroughLimit || nsSizeLimit
  || nsTimeLimit|| nsIdleTimeout ” )
  (version 3.0; acl “ Allow self entry read search ” ;
  allow(write)
  userdn = ” ldap:///self ” ;)
aci: (target= ” ldap:///$rootSuffix ” )
  (targetattr= ” * ” )
  (version 3.0; acl “ S1IS Proxy user rights ” ;
  allow (proxy)
  userdn = “ ldap:///cn=puser,ou=DSAME Users,
  $rootSuffix ” ; )
aci: (target= ” ldap:///$rootSuffix ” )
  (targetattr= ” * ” )
  (version 3.0; acl “ S1IS special dsame user rights for all under the root
   suffix ” ;
  allow (all)
  userdn = “ ldap:///cn=dsameuser,ou=DSAME Users,
  $rootSuffix ” ; )
aci: (target= ” ldap:///$rootSuffix ” )
  (targetattr= ” * ” )
  (version 3.0; acl “ S1IS special ldap auth user rights ” ;
  allow (read,search)
  userdn = “ ldap:///cn=amldapuser,ou=DSAME Users,
  $rootSuffix ” ; )
aci: (target= ” ldap:///$rootSuffix ” )
```

```
  (targetattr="*")
  (version 3.0; acl "S1IS Top-level admin rights";
  allow (all)
  roledn = "ldap:///cn=Top-level Admin Role,
  $rootSuffix"; )
aci: (targetattr="*")
  (version 3.0; acl "Messaging Server End User Administrator Read Only
   Access";
  allow (read,search)
  groupdn="ldap:///cn=Messaging End User Administrators Group,ou=Groups,
  $rootSuffix";)
aci: (targetattr="objectclass || mailalternateaddress || Mailautoreplymode
   || mailprogramdeliveryinfo || preferredlanguage || maildeliveryoption
   || mailforwardingaddress || mailAutoReplyTimeout
   || mailautoreplytextinternal
   || mailautoreplytext || vacationEndDate || vacationStartDate
   || mailautoreplysubject || maxPabEntries || mailMessageStore
   || mailSieveRuleSource || sunUCDateFormat || sunUCDateDeLimiter
   || sunUCTimeFormat || mailuserstatus || maildomainstatus
   || nswmextendeduserprefs || pabURI")
  (version 3.0; acl "Messaging Server End User Administrator All Access";
  allow (all)
  groupdn = "ldap:///cn=Messaging End User Administrators Group,ou=Groups,
  $rootSuffix";)
aci: (targetattr = "*")
  (version 3.0;acl "Allow Read-Only Access";
  allow (read,search,compare)
  groupdn = "ldap:///cn=Read-Only,ou=Groups,
  $rootSuffix";)
aci: (target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS Organization Admin Role access deny";
  deny (write,add,delete,compare,proxy)
  roledn = "ldap:///cn=Organization Admin Role,($dn),
  $rootSuffix";)
aci: (target="ldap:///($dn),$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "Organization Admin Role access allow read";
  allow(read,search)
  roledn = "ldap:///cn=Organization Admin Role,[$dn],
  $rootSuffix" ;)
aci: (target="ldap:///($dn),$rootSuffix")
  (targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
  (entrydn=($dn),$rootSuffix))))
  ( targetattr = "*")
  (version 3.0; acl "S1IS Organization Admin Role access allow";
  allow (all)
  roledn = "ldap:///cn=Organization Admin Role,[$dn],
  $rootSuffix";)
```

替换 ACI 的步骤

开始之前

在开始此过程之前，建议您先检查目录中现有的 ACI。您应确定是否可能需要保留任何将被此过程删除的 ACI。

此过程首先会从根后缀处删除**全部** ACI，然后用下面列出的一组 ACI 来替换它们。如果目录中包含由 Messaging Server 以外的应用程序生成的 ACI，则应该将这些 ACI 保存到一个文件中，然后在应用 `replacement.acis.ldif` 文件后将这些 ACI 重新应用于目录。

要获得有关对 Access Manager 和 Messaging Server 生成的现有 ACI 进行分析的帮助，请参见本附录后面的以下几节：

- 第 201 页中的 “对现有 ACI 的分析”
- 第 218 页中的 “ACI 合并方式分析”
- 第 226 页中的 “要放弃的未使用的 ACI 列表”

替换 ACI

以下过程描述了如何合并根后缀中的 ACI 并删除未使用的 ACI。

▼ 替换 ACI 的步骤

1. **保存根后缀上现有的 ACI。**

   可以使用 `ldapsearch` 命令，如以下示例所示：

   ```
   ldapsearch -D “cn=Directory Manager” -w <password> -s base -b <$rootSuffix> aci=*
   aci ><filename>
   ```

   其中

   `<password>` 是 Directory Server 管理员的密码。

   `<$rootSuffix>` 是根后缀， 例如 `o=usergroup`。

   `<filename>` 是所保存 ACI 将写入的文件的名称。

2. **复制并重命名 `replacement.acis.ldif` 文件。**

   安装了 Delegated Administrator 后，就会将 `replacement.acis.ldif` 文件安装在以下目录中：

   da-base`/lib/config-templates`

3. **编辑您的 `replacement.acis.ldif` 文件副本中的 `$rootSuffix` 条目。**

   将根后缀参数 $rootSuffix 更改为您的根后缀（例如 `o=usergroup`）。$rootSuffix 参数会在 ldif 文件中出现多次；必须将每个实例都替换掉。

4 **使用 LDAP 目录工具 `ldapmodify` 替换 ACI。**

例如，可以运行以下命令：

```
ldapmodify -D <directory manager> -w <password> -f
<replacement.acis.finished.ldif>
```

其中

`<directory manager>` 是 Directory Server 管理员的用户名。

`<password>` 是 Directory Server 管理员的密码。

`<replacement.acis.finished.ldif>` 是编辑后的 ldif 文件名，该文件用于合并和删除目录中的 ACI。

清除动态组织 ACI

使用 Delegated Administrator 控制台创建了一个组织后，就在该组织节点上创建了一组 ACI。

由于在上述过程中安装了替换 ACI，因此不需要每个组织上的这些 ACI。您可以通过使用 Access Manager 控制台来防止在每个组织节点上创建 ACI。

▼ 清除动态组织 ACI 的步骤

1 **作为 `amadmin` 登录到 AM 控制台。**

AM 控制台位于以下 url：

`http://<` *machine name*`>:<`*port* `>/amconsole`

其中

<*machine name*> 是运行 Access Manager 的计算机

<*port*> 是端口

2 **选择“服务配置”选项卡。**

默认情况下将显示“管理配置”页。

3 **在控制台右侧，向下滚动到“ 动态管理角色 ACI ”。**

4 **选择并删除“动态管理角色 ACI”文本框中的所有 ACI。**

5 **保存编辑后的设置。**

对现有 ACI 的分析

本节中的列表显示了在安装 Access Manager 和 Messaging Server 时安装在目录中的 ACI。还介绍了每个 ACI 的功能，并针对 ACI 是否能够保留、合并或放弃提出了建议。

ACI 分为以下几种类别：

根后缀

```
dn: $rootSuffix
#
# consolidate
#
aci:
(targetattr != “nsroledn || aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry
|| passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime
|| accountUnlockTime || passwordHistory || passwordAllowChangeTime”)
(version 3.0; acl “Allow self entry modification except for nsroledn, aci,
resource limit attributes, passwordPolicySubentry and password policy state
attributes”;
allow (write)
userdn =”ldap:///self”;)
```

操作：合并。

无需自访问此后缀。此 ACI 将被复制；它可以合并到根后缀上的 ACI 自身中。

```
#
# retain
#
aci:
(targetattr = “*”)
(version 3.0; acl “Configuration Administrator”;
allow (all)
userdn = “ldap:///uid=admin, ou=Administrators,
ou=TopologyManagement,o=NetscapeRoot”;)
```

操作：保留。

此后缀是 "admin" 用户，该用户将通过“通道验证”来验证 `slapd-config` 实例。如果所有配置是以 Directory Manager 身份使用命令行实用程序执行的，则无需此 ACI。如果某个用户需要以此用户身份验证控制台，则可以将此 ACI 保留在此处。可以删除类似的 ACI。

```
#
# discard
#
aci:
(targetattr =”*”)
(version 3.0;acl “Configuration Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Configuration Administrators, ou=Groups,
ou=TopologyManagement, o=NetscapeRoot”);)
```

操作：在所有 DB 后端上执行放弃。

此后缀是“配置管理员”组，当使用控制台来委托服务器管理权限时，该组将具有此权限。

```
#
# discard
#
aci:
(targetattr =”*”)
(version 3.0;acl “Directory Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Directory Administrators, $rootSuffix”);)
```

操作：在所有 DB 后端上执行放弃。

此后缀是常见“目录管理员”组权限定义。

```
#
# discard
#
aci:
(targetattr = “*”)
(version 3.0; acl “SIE Group”;
allow (all)
groupdn = “ldap:///cn=slapd-whater, cn=Sun ONE Directory Server,
cn=Server Group, cn=whater.red.iplanet.com, ou=red.iplanet.com,
o=NetscapeRoot”;)
```

操作：在所有 DB 后端上执行放弃。

此后缀是控制台/管理服务器相关组权限定义。

Access Manager

```
# retain
#
aci:
(target=”ldap:///$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “S1IS Proxy user rights”;
allow (proxy)
userdn = “ldap:///cn=puser,ou=DSAME Users,$rootSuffix”; )
```

操作：保留。

此 ACI 可授予系统用户访问 Access Manager 的权限。

```
#
# retain
#
aci:
 (target=”ldap:///$rootSuffix”)
```

```
(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the
root suffix";
allow (all)
userdn = "ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix"; )
```

操作：保留。

此 ACI 可授予系统用户访问 Access Manager 的权限。

```
#
# retain
#
aci:
(target="ldap:///$rootSuffix")(targetattr="*")|
(version 3.0;acl "S1IS special ldap auth user rights";
allow (read,search)
userdn = "ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix"; )
```

操作：保留。

此 ACI 可授予系统用户访问 Access Manager 的权限。

```
#
# discard
#
aci:
(target="ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix")
(targetattr = "*")
(version 3.0;
acl "S1IS special ldap auth user modify right";
deny (write)
roledn != "ldap:///cn=Top-level Admin Role,$rootSuffix";)
```

操作：放弃。

此 ACI 可阻止顶级管理员 (Top-Level Administrator, TLA) 修改 `amldapuser` 帐户。

```
#
# retain
#
aci:
(target=”ldap:///$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “S1IS Top-level admin rights”;
allow (all)
roledn = “ldap:///cn=Top-level Admin Role,$rootSuffix”; )
```

操作：保留。

此 ACI 可向顶级管理员角色授予访问权限。

```
#
# discard
#
aci:
(targetattr=”iplanet-am-saml-user || iplanet-am-saml-password”)
(targetfilter=”(objectclass=iplanet-am-saml-service)”)
(version 3.0; acl “S1IS Right to modify saml user and password”;
deny (all)
(roledn != “ldap:///cn=Top-level Admin Role,$rootSuffix”)
AND (userdn != “ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix”)
AND (userdn != “ldap:///cn=puser,ou=DSAME Users,$rootSuffix”); )
```

操作：放弃。

此 ACI 可保护 SAML 相关属性。

顶级帮助桌面管理角色

```
#
# discard
#
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = “*”)
(version 3.0; acl “S1IS Top-level Help Desk Admin Role access allow”;
allow (read,search)
roledn = “ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix”;)
```

操作：放弃。

```
#
# discard
#
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = “userPassword”)
(version 3.0; acl “S1IS Top-level Help Desk Admin Role access allow”;
allow (write)
roledn = “ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix”;)
```

操作：放弃。

顶级策略管理角色

```
#
# discard
#
aci:
target=”ldap:///$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix))))
(targetattr = “*”)
(version 3.0; acl “S1IS Top-level Policy Admin Role access allow”;
allow (read,search)
roledn = “ldap:///cn=Top-level Policy Admin Role,$rootSuffix”;)
```

操作：放弃。

此 ACI 属于顶级策略管理角色。

```
#
# discard
#
aci:
(target=”ldap:///ou=iPlanetAMAuthService,ou=services,*$rootSuffix”)
```

```
(targetattr = “*”)
(version 3.0; acl “S1IS Top-level Policy Admin Role access Auth Service
deny”;
deny (add,write,delete)
roledn = “ldap:///cn=Top-level Policy Admin Role,$rootSuffix”;)
```

操作：放弃。

此 ACI 属于顶级策略管理角色。

```
#
# discard
#
aci:
(target=”ldap:///ou=services,*$rootSuffix”)
(targetattr = “*”)
(version 3.0; acl “S1IS Top-level Policy Admin Role access allow”;
allow (all)
roledn = “ldap:///cn=Top-level Policy Admin Role,$rootSuffix”;)
```

操作：放弃。

此 ACI 属于顶级策略管理角色。

```
#
# discard
#
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=”(objectclass=sunismanagedorganization)”)
(targetattr = “sunRegisteredServiceName”)
(version 3.0; acl “S1IS Top-level Policy Admin Role access allow”;
allow (read,write,search)
roledn = “ldap:///cn=Top-level Policy Admin Role,$rootSuffix”;)
```

操作：放弃。

此 ACI 属于顶级策略管理角色。

AM 自身

```
#
# consolidate
#
aci:
(targetattr = “*”)
(version 3.0;
acl “S1IS Deny deleting self”;
deny (delete)
userdn =”ldap:///self”;)
```

操作：合并为单个自写 ACI。由于最终用户不具有删除任何条目（包括其自身）的权限，因此无需显式拒绝。

这是若干用于设置自身权限的 ACI 之一。显式拒绝可阻止任何条目删除其自身。

```
#
# consolidate
#
aci:
(targetattr = “objectclass || inetuserstatus
|| iplanet-am-user-login-status
|| iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || iplanet-am-user-account-life
|| iplanet-am-session-max-session-time || iplanet-am-session-max-idle-time
|| iplanet-am-session-get-valid-sessions
|| iplanet-am-session-destroy-sessions
|| iplanet-am-session-add-session-listener-on-all-sessions
|| iplanet-am-user-admin-start-dn
|| iplanet-am-auth-post-login-process-class”)
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(version 3.0; acl “S1IS User status self modification denied”;
deny (write)
userdn =”ldap:///self”;)
```

操作：合并为单个自写 ACI。

这是若干用于设置自写权限的 ACI 之一。

```
#
# consolidate
#
aci:
(targetattr != “iplanet-am-static-group-dn || uid || nsroledn || aci
|| nsLookThroughLimit || nsSizeLimit || nsTimeLimit || nsIdleTimeout
|| memberOf || iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list”)
(version 3.0; acl “S1IS Allow self entry modification except for nsroledn,
aci, and resource limit attributes”;
allow (write)
userdn =”ldap:///self”;)
```

操作：合并为单个自写 ACI。

这是若干用于设置权限的 ACI 之一。

```
#
# consolidate
#
aci:
(targetattr != “aci || nsLookThroughLimit || nsSizeLimit || nsTimeLimit
|| nsIdleTimeout || iplanet-am-domain-url-access-allow”)
(version 3.0; acl “S1IS Allow self entry read search except for nsroledn,
aci, resource limit and web agent policy attributes”;
allow (read,search)
userdn =”ldap:///self”;)
```

操作：合并为单个自写 ACI。

这是若干用于设置自写权限的 ACI 之一。

AM 匿名

```
#
# consolidate
#
aci:
(target=”ldap:///ou=services,$rootSuffix”)
(targetfilter=(!(objectclass=sunServiceComponent)))
```

```
(targetattr = “*”)
(version 3.0; acl “S1IS Services anonymous access”;
allow (read, search, compare)
userdn = “ldap:///anyone”;)
```

操作：合并为单个匿名 ACI。

这是若干用于授予匿名权限的 ACI 之一。

```
#
# consolidate
#
aci:
(target=”ldap:///ou=iPlanetAMAdminConsoleService,*,$rootSuffix”)
(targetattr = “*”)
(version 3.0; acl “S1IS iPlanetAMAdminConsoleService anonymous access”;
allow (read, search, compare)
userdn = “ldap:///anyone”;)
```

操作：合并为单个匿名 ACI。

这是若干用于授予匿名权限的 ACI 之一。

```
#
# discard
#
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=(entrydn=$rootSuffix))
(targetattr=”*”)
(version 3.0; acl “S1IS Default Organization delete right denied”;
deny (delete)
userdn = “ldap:///anyone”; )
```

操作：放弃。

此 ACI 可阻止任何用户（`rootdn` 除外）删除默认组织。

```
#
# discard
#
aci:
(target=”ldap:///cn=Top-level Admin Role,$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “S1IS Top-level admin delete right denied”;
deny(delete)
userdn = “ldap:///anyone”; )
```

操作：放弃。

此 ACI 可阻止任何用户（`rootdn` 除外）删除顶级管理员角色。

AM 拒绝写访问

```
#
# discard
#
aci: (targetattr = “*”)
(version 3.0; acl “S1IS Deny write to anonymous user”;
deny (add,write,delete)
roledn =”ldap:///cn=Deny Write Access,$rootSuffix”;)
```

操作：放弃。

此 ACI 属于拒绝写访问角色。

AM 容器管理角色

```
#
# discard
#
aci:
(target=”ldap:///($dn),$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != “nsroledn”)
(version 3.0; acl “S1IS Container Admin Role access allow”;
```

```
allow (all)
roledn = “ldap:///cn=Container Admin Role,[$dn],$rootSuffix”;)
```

操作：放弃。

此 ACI 属于容器管理角色。

```
#
# discard
#
aci:
(target=”ldap:///cn=Container Admin Role,($dn),$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “S1IS Container Admin Role access deny”;
deny (write,add,delete,compare,proxy)
roledn = “ldap:///cn=Container Admin Role,($dn),$rootSuffix”;)
```

操作：放弃。

此 ACI 属于容器管理角色。

```
#
# discard
#
aci:
 (target=”ldap:///ou=People,$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix)
(nsroledn=cn=Container Admin Role,$rootSuffix))))
(targetattr != “iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || nsroledn”)
(version 3.0; acl “S1IS Group and people container admin role”;
allow (all)
roledn = “ldap:///cn=ou=People_dc=red_dc=iplanet_dc=com,$rootSuffix”;)
```

操作：放弃。

此 ACI 属于组和人员容器管理角色。

组织帮助台

```
#
# discard
#
aci: (extra verses dreambig)
(target=”ldap:///$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = “*”)
(version 3.0; acl “S1IS Organization Help Desk Admin Role access allow”;
allow (read,search)
roledn = “ldap:///cn=Organization Help Desk Admin Role,$rootSuffix”;)
```

操作：放弃。

此 ACI 属于组织帮助台管理角色。

```
#
# discard
#
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = “userPassword”)
(version 3.0; acl “S1IS Organization Help Desk Admin Role access allow”;
allow (write)
roledn = “ldap:///cn=Organization Help Desk Admin Role,$rootSuffix”;)
```

操作：放弃。

此 ACI 属于组织帮助台管理角色。

AM 组织管理角色

```
#
# consolidate
#
aci: (different name - “allow all” instead of “allow”)
(target=”ldap:///($dn),$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != “nsroledn”)
(version 3.0; acl “S1IS Organization Admin Role access allow all”;
allow (all)
roledn =”ldap:///cn=Organization Admin Role,[$dn],$rootSuffix”;)
```

操作：合并。

```
#
# consolidate
#
aci:
(target=”ldap:///cn=Organization Admin Role,($dn),$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “S1IS Organization Admin Role access deny”;
deny (write,add,delete,compare,proxy)
roledn = “ldap:///cn=Organization Admin Role,($dn),$rootSuffix”;)
```

操作：合并。

此 ACI 属于组织管理角色。

```
#
# consolidate
#
aci: (missing)
(target=”ldap:///($dn),$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “Organization Admin Role access allow read to org node”;
allow (read,search)
roledn = “ldap:///cn=Organization Admin Role,($dn),$rootSuffix” ;)
```

操作：合并。

此 ACI 属于组织管理角色。

```
#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

操作：合并。

此 ACI 属于组织管理角色。

```
#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetattr!="businessCategory || description || facsimileTelephoneNumber
|| postalAddress || preferredLanguage || searchGuide || postOfficeBox ||
postalCode
|| registeredaddress || street || l || st || telephonenumber
||maildomainreportaddress
|| maildomainwelcomemessage || preferredlanguage || sunenablegab")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)
```

操作：合并。

此 ACI 属于组织管理角色。

```
#
# consolidate
#
aci:
(target=”ldap:///($dn),$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != “nsroledn”)
(version 3.0; acl “S1IS Organization Admin Role access allow all”;
allow (all)
roledn = “ldap:///cn=Organization Admin Role,[$dn],$rootSuffix”;)
```

操作：合并。

AM 杂项

```
#
#
# discard
#
aci:
(target=”ldap:///$rootSuffix”)
(targetattr!=”nsroledn”)
(version 3.0; acl “S1IS Group admin’s right to the users he creates”;
allow (all)
userattr = “iplanet-am-modifiable-by#ROLEDN”;)
```

操作：放弃。

放弃此 ACI 将会禁用与属性 `iplanet-am-modifiable-by` 关联的权限。

Messaging Server

```
#
# consolidate
#
aci:
(target=”ldap:///$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “Messaging Server End User Administrator Read
```

```
Access Rights -
product=SOMS,schema 2 support,class=installer,num=1,version=1";
allow (read,search)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
$rootSuffix";)
```

操作：合并。

此 ACI 可向通讯最终用户管理员组授予权限。

```
#
# consolidate
#
aci:
(target="ldap:///$rootSuffix")
(targetattr="objectclass||mailalternateaddress||mailautoreplymode
||mailprogramdeliveryinfo||nswmextendeduserprefs||preferredlanguage
||maildeliveryoption||mailforwardingaddress
||mailAutoReplyTimeout||mailautoreplytextinternal||mailautoreplytext
||vacationEndDate||vacationStartDate||mailautoreplysubject||pabURI
||maxPabEntries||mailMessageStore||mailSieveRuleSource||sunUCDateFormat
||sunUCDateDeLimiter||sunUCTimeFormat")
(version 3.0; acl "Messaging Server End User Adminstrator Write
Access Rights -
product=SOMS,schema 2 support,class=installer,num=2,version=1";
allow (all)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
$rootSuffix";)
```

操作：合并。

此 ACI 可向通讯最终用户管理员组授予权限。

```
#
# consolidate
#
aci:
(targetattr="uid||ou||owner||mail||mailAlternateAddress
||mailEquivalentAddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota
||mailMsgQuota||inetSubscriberAccountId||dataSource||mailhost
```

```
||mailAllowedServiceAcces||pabURI||inetCOS||mailSMTPSubmitChannel
||aci")
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization
Admin Role,*))))
(version 3.0; acl "Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self";)
```

操作：合并。

这是若干用于设置自身权限的 ACI 之一。

ACI 合并方式分析

本节中的列表显示了在替换 ldif 文件 `replacement.acis.ldif`（此文件可用于合并目录中的 ACI）中已被合并的 ACI。有关如何替换 ACI 的说明，请参见第 199 页中的 "替换 ACI 的步骤"。

ACI 分为若干对。对于每种类别，均先列出原始 ACI，再列出合并后的 ACI：

原始匿名访问权限

```
aci:
(targetattr != "userPassword || passwordHistory || passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime ||
accountUnlockTime || passwordAllowChangeTime ")
(version 3.0; acl "Anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)

aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
```

```
version 3.0; acl “S1IS Top-level admin delete right denied”;
deny (delete)
userdn = “ldap:///anyone”; )


aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=(entrydn=$rootSuffix))
(targetattr=”*”)
(version 3.0; acl “S1IS Default Organization delete right denied”;
deny (delete)
userdn = “ldap:///anyone”; )


aci:
(target=”ldap:///ou=services,$rootSuffix”)
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr = “*”)
(version 3.0; acl “S1IS Services anonymous access”;
allow (read, search, compare)
userdn = “ldap:///anyone”;)


aci:
(target=”ldap:///ou=iPlanetAMAdminConsoleService,*,$rootSuffix”)
(targetattr = “*”)
(version 3.0; acl “S1IS iPlanetAMAdminConsoleService anonymous access”;
allow (read, search, compare)
userdn = “ldap:///anyone”;)
```

合并后的匿名访问权限

```
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr != “userPassword||passwordHistory
||passwordExpirationTime||passwordExpWarned||passwordRetryCount
||retryCountResetTime||accountUnlockTime||passwordAllowChangeTime”)
(version 3.0; acl “anonymous access rights”;
allow (read,search,compare)
userdn = “ldap:///anyone”; )
```

分析：此 ACI 位于根上，它可与原始匿名 ACI 集合授予相同的访问权限。它通过列出一组排除的属性来执行此操作。由于此替换 ACI 清除了目标中的 (*)，因此可提高性能。

原始 ACI 自身

```
aci:
(targetattr != “nsroledn || aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime ||
accountUnlockTime || passwordHistory || passwordAllowChangeTime”)
(version 3.0; acl “Allow self entry modification except for nsroledn, aci,
resource limit attributes, passwordPolicySubentry and password policy
state attributes”;
allow (write)
userdn =”ldap:///self”;)


aci:
(targetattr = “*”)
(version 3.0; acl “S1IS Deny deleting self”;
deny (delete)
userdn =”ldap:///self”;)


aci:
(targetattr = “objectclass || inetuserstatus ||
planet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list
|| iplanet-am-user-account-life || iplanet-am-session-max-session-time
|| iplanet-am-session-max-idle-time
|| iplanet-am-session-get-valid-sessions
|| iplanet-am-session-destroy-sessions
|| iplanet-am-session-add-session-listener-on-all-sessions
|| iplanet-am-user-admin-start-dn
|| iplanet-am-auth-post-login-process-class”)
(targetfilter=(!(nsroledn=cn=Top-levelAdmin Role,$rootSuffix)))
(version 3.0; acl “S1IS User status self modification denied”;
deny (write)
userdn =”ldap:///self”;)


aci:
(targetattr != “iplanet-am-static-group-dn || uid || nsroledn || aci
|| LookThroughLimit
|| nsSizeLimit || nsTimeLimit || nsIdleTimeout || memberOf ||
planet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow ||
planet-am-web-agent-access-deny-list”)
(version 3.0; acl “S1IS Allow self entry modification except
for nsroledn, aci, and resource limit attributes”;
```

```
allow (write)
userdn =”ldap:///self”;)


aci:
(targetattr != “aci || nsLookThroughLimit || nsSizeLimit || nsTimeLimit
|| nsIdleTimeout || iplanet-am-domain-url-access-allow”)
(version 3.0; acl “S1IS Allow self entry read search except for
nsroledn, aci, resource limit and web agent policy attributes”;
allow (read,search)
userdn =”ldap:///self”;)


aci:
(targetattr=”uid||ou||owner||mail||mailAlternateAddress
||mailEquivalentaddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota
||mailMsgQuota
||inetSubscriberAccountId||dataSource||mailhost||mailAllowedServiceAccess
||pabURI||inetCOS||mailSMTPSubmitChannel||aci”)
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization Admin
role,*))))
(version 3.0; acl “Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 “;
deny (write)
userdn = “ldap:///self”;)
```

合并后的 ACI 自身

```
aci:
(targetattr != “nsroledn || aci || nsLookThroughLimit || nsSizeLimit
|| nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
asswordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime
|| accountUnlockTime || passwordHistory || passwordAllowChangeTime ||
id || memberOf
|| objectclass || inetuserstatus || ou || owner || mail || mailuserstatus
|| memberOfManagedGroup ||mailQuota || mailMsgQuota || mailhost
|| mailAllowedServiceAccess || inetCOS || mailSMTPSubmitChannel”)
(version 3.0; acl “Allow self entry modification”;
allow (write)
userdn =”ldap:///self”;)


aci:
(targetattr != “ aci || nsLookThroughLimit || nsSizeLimit
|| nsTimeLimit|| nsIdleTimeout”)
```

```
(version 3.0; acl “Allow self entry read search”;
allow(read,search)
userdn =”ldap:///self”;)
```

分析：不具有全部 `iplanet-am-*` 属性。由于在 ACI 不存在的情况下默认值为 `deny`，因此所有 `deny` ACI 都被删除。允许 `write` 的各个 ACI 将被合并为单个 ACI。

原始 Messaging Server ACI

```
aci:
(target=”ldap:///$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “Messaging Server End User Administrator Read
Access Rights -
product=SOMS,schema 2 support,class=installer,num=1,version=1”;
allow (read,search)
groupdn=”ldap:///cn=Messaging End User Administrators Group, ou=Groups,
rootSuffix”;)


aci:
(target=”ldap:///$rootSuffix”)
(targetattr=”objectclass||mailalternateaddress||mailautoreplymode||
mailprogramdeliveryinfo
||nswmextendeduserprefs||preferredlanguage||maildeliveryoption||
mailforwardingaddress
||mailAutoReplyTimeout||mailautoreplytextinternal||mailautoreplytext||
vacationEndDate
||vacationStartDate||mailautoreplysubject||pabURI||maxPabEntries||
mailMessageStore
||mailSieveRuleSource||sunUCDateFormat||sunUCDateDeLimiter||
sunUCTimeFormat”)
(version 3.0; acl “Messaging Server End User Adminstrator Write
Access Rights -
product=SOMS,schema 2 support,class=installer,num=2,version=1”;
allow (all)
groupdn=”ldap:///cn=Messaging End User Administrators Group, ou=Groups,
rootSuffix”;)


aci:
(targetattr=”uid||ou||owner||mail||mailAlternateAddress||
mailEquivalentAddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota||
mailMsgQuota
||inetSubscriberAccountId||dataSource||mailhost||mailAllowedServiceAccess
||pabURI||inetCOS||mailSMTPSubmitChannel||aci”)
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization Admin
```

```
Role,*))))
(version 3.0; acl “Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 “;
deny (write)
userdn = “ldap:///self”;)
```

合并后的 Messaging Server ACI

ACI 自身在多个 ACI 自身中处理。

```
aci:
(targetattr=”*”)
(version 3.0; acl “Messaging Server End User Administrator
Read Only Access”;
allow (read,search)
groupdn = “ldap:///cn=Messaging End User Administrators
group,ou=Groups,$rootSuffix”; )


aci:
(targetattr=”objectclass || mailalternateaddress || Mailautoreplymode
|| mailprogramdeliveryinfo || preferredlanguage || maildeliveryoption
|| mailforwardingaddress || mailAutoReplyTimeout
|| mailautoreplytextinternal
|| mailautoreplytext || vacationEndDate || vacationStartDate
|| mailautoreplysubject || maxPabEntries || mailMessageStore
|| mailSieveRuleSource || sunUCDateFormat || sunUCDateDeLimiter
|| sunUCTimeFormat || mailuserstatus || maildomainstatus
|| nswmextendeduserprefs || pabURI”)
(version 3.0; acl “Messaging Server End User Administrator All Access”;
allow (all)
groupdn = “ldap:///cn=Messaging End User Administrators
group,ou=Groups,$rootSuffix”;)
```

分析：与原始 ACI 相同。

原始组织管理 ACI

```
aci: (different name - “allow all” instead of “allow”)
(target=”ldap:///($dn),$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != “nsroledn”)
(version 3.0; acl “S1IS Organization Admin Role access allow all”;
allow (all)
roledn =”ldap:///cn=Organization Admin Role,[$dn],$rootSuffix”;)
```

```
aci: (missing)
(target=”ldap:///($dn),$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “Organization Admin Role access allow read to org node”;
allow (read,search)
roledn = “ldap:///cn=Organization Admin Role,($dn),$rootSuffix” ;)


aci:
(target=”ldap:///($dn),$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != “nsroledn”)
(version 3.0; acl “Organization Admin Role access allow”;
allow (all)
roledn = “ldap:///cn=Organization Admin Role,[$dn],$rootSuffix”;)


aci:
(target=”ldap:///($dn),$rootSuffix”)
(targetattr!=”businessCategory || description || facsimileTelephoneNumber
|| postalAddress || preferredLanguage || searchGuide || postOfficeBox
|| postalCode
|| registeredaddress || street || l || st || telephonenumber
|| maildomainreportaddress
|| maildomainwelcomemessage || preferredlanguage || sunenablegab”)
(version 3.0; acl “Organization Admin Role access deny to org node”;
deny (write,add,delete)
roledn = “ldap:///cn=Organization Admin Role,($dn),$rootSuffix” ;)


aci: (duplicate of per organization aci)
(target=”ldap:///cn=Organization Admin Role,($dn),$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “S1IS Organization Admin Role access deny”;
deny (write,add,delete,compare,proxy)
roledn = “ldap:///cn=Organization Admin Role,($dn),$rootSuffix”;)


aci:
(target=”ldap:///cn=Organization Admin
Role,($dn),dc=red,dc=iplanet,dc=com”)
(targetattr=”*”)
(version 3.0; acl “S1IS Organization Admin Role access deny”;
deny (write,add,delete,compare,proxy)
roledn = “ldap:///cn=Organization Admin Role,($dn),$rootSuffix”;)
```

```
aci:
(target=”ldap:///o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,
o=Business,rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,dc=red,dc=iplanet,dc=com))))
(targetattr = “nsroledn”)
(targattrfilters=”add=nsroledn:(nsroledn=*,o=fullOrg1,o=VIS,o=siroe.com,
o=SharedDomainsRoot,o=Business,$rootSuffix),
del=nsroledn:(nsroledn=*,o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,
o=Business,$rootSuffix)”)
(version 3.0;
acl “S1IS Organization Admin Role access allow”;
allow (all)
roledn = “ldap:///cn=Organization Admin
Role,o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,o=Business,
$rootSuffix”;)


aci:
(target=”ldap:///($dn),$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != “nsroledn”)
(version 3.0; acl “S1IS Organization Admin Role access allow all”;
allow (all)
roledn = “ldap:///cn=Organization Admin
Role,[$dn],dc=red,dc=iplanet,dc=com”;)
```

合并后的组织管理 ACI

```
aci:
(target=”ldap:///cn=Organization Admin Role,($dn),$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “S1IS Organization Admin Role access deny”;
deny (write,add,delete,compare,proxy)
roledn = “ldap:///cn=Organization Admin Role,($dn),$rootSuffix”;)


aci:
(target=”ldap:///($dn),$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “Organization Admin Role access allow read”;
allow(read,search)
roledn = “ldap:///cn=Organization Admin Role,[$dn],$rootSuffix” ;)
```

```
aci:
(target=”ldap:///($dn),$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(entrydn=($dn),$rootSuffix))))
( targetattr = “*”)
(version 3.0; acl “S1IS Organization Admin Role access allow”;
allow (all)
roledn = “ldap:///cn=Organization Admin Role,[$dn],$rootSuffix”;)
```

要放弃的未使用的 ACI 列表

本节中的列表显示了当您将 `replacement.acis.ldif` 文件应用于目录时将放弃的、目录中未使用的默认 ACI。

要放弃的 ACI 分为以下几种类别：

- 第 226 页中的 “后缀”
- 第 227 页中的 “顶级帮助桌面管理角色”
- 第 228 页中的 “顶级策略管理角色”
- 第 229 页中的 “Access Manager 匿名”
- 第 229 页中的 “Access Manager 拒绝写访问”
- 第 230 页中的 “Access Manager 容器管理角色”
- 第 231 页中的 “组织帮助台”
- 第 231 页中的 “Access Manager 杂项”

后缀

```
# discard
#
aci:
(targetattr =”*”)
(version 3.0;acl “Configuration Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Configuration Administrators, ou=Groups,
ou=TopologyManagement, o=NetscapeRoot”);)


#
# discard
#
aci:
(targetattr =”*”)
(version 3.0;acl “Directory Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Directory Administrators, $rootSuffix”);)
```

```
#
# discard
#
aci:
(targetattr = “*”)
(version 3.0;
acl “SIE Group”;
allow (all)
groupdn = “ldap:///cn=slapd-whater, cn=Sun ONE Directory Server, cn=Server
Group, cn=whater.red.iplanet.com, ou=red.iplanet.com, o=NetscapeRoot”;)


#
# discard - prevents TLA from modifying the amldapuser account.
#
aci:
(target=”ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix”)
(targetattr = “*”)
(version 3.0;
acl “S1IS special ldap auth user modify right”;
deny (write)
roledn != “ldap:///cn=Top-level Admin Role,$rootSuffix”;)


#
# discard - protects SAML related attributes
#
aci:
(targetattr=”iplanet-am-saml-user || iplanet-am-saml-password”)
(targetfilter=”(objectclass=iplanet-am-saml-service)”)
(version 3.0; acl “S1IS Right to modify saml user and password”;
deny (all)
(roledn != “ldap:///cn=Top-level Admin Role,$rootSuffix”)
AND (userdn != “ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix”)
AND (userdn != “ldap:///cn=puser,ou=DSAME Users,$rootSuffix”); )
```

顶级帮助桌面管理角色

```
#
# discard
 #
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = “*”)
(version 3.0; acl “S1IS Top-level Help Desk Admin Role access allow”;
```

```
allow (read,search)
roledn = “ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix”;)


#
# discard
#
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = “userPassword”)
(version 3.0; acl “S1IS Top-level Help Desk Admin Role access allow”;
allow (write)
roledn = “ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix”;)
```

顶级策略管理角色

```
#
# discard
#
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix))))
(targetattr = “*”)
(version 3.0; acl “S1IS Top-level Policy Admin Role access allow”;
allow (read,search)
roledn = “ldap:///cn=Top-level Policy Admin Role,$rootSuffix”;)


#
# discard
#
aci:
(target=”ldap:///ou=iPlanetAMAuthService,ou=services,*$rootSuffix”)
(targetattr = “*”)
(version 3.0; acl “S1IS Top-level Policy Admin Role access
Auth Service deny”;
deny (add,write,delete)
roledn = “ldap:///cn=Top-level Policy Admin Role,$rootSuffix”;)


#
# discard
#
aci:
(target=”ldap:///ou=services,*$rootSuffix”)
(targetattr = “*”)
(version 3.0; acl “S1IS Top-level Policy Admin Role access allow”;
```

```
allow (all)
roledn = “ldap:///cn=Top-level Policy Admin Role,$rootSuffix”;)


#
# discard
#
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=”(objectclass=sunismanagedorganization)”)
(targetattr = “sunRegisteredServiceName”)
(version 3.0; acl “S1IS Top-level Policy Admin Role access allow”;
allow (read,write,search)
roledn = “ldap:///cn=Top-level Policy Admin Role,$rootSuffix”;)
```

Access Manager 匿名

```
#
# discard - prevents anyone other than rootdn from deleting
# default organization.
#
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=(entrydn=$rootSuffix))
(targetattr=”*”)
(version 3.0; acl “S1IS Default Organization delete right denied”;
deny (delete)
userdn = “ldap:///anyone”; )


#
# discard - prevents any user other than rootdn from deleting the
# TLA admin role.
#
aci:
(target=”ldap:///cn=Top-level Admin Role,$rootSuffix”)
(targetattr=”*”)
version 3.0; acl “S1IS Top-level admin delete right denied”;
deny(delete)
userdn = “ldap:///anyone”; )
```

Access Manager 拒绝写访问

```
#
# discard
#
aci:
(targetattr = “*”)
```

```
(version 3.0; acl “S1IS Deny write to anonymous user”;
deny (add,write,delete)
roledn =”ldap:///cn=Deny Write Access,$rootSuffix”;)
```

Access Manager 容器管理角色

```
#
# discard
#
aci:
(target=”ldap:///($dn),$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != “nsroledn”)
(version 3.0; acl “S1IS Container Admin Role access allow”;
allow (all)
roledn = “ldap:///cn=Container Admin Role,[$dn],$rootSuffix”;)


#
# discard
#
aci:
(target=”ldap:///cn=Container Admin Role,($dn),$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “S1IS Container Admin Role access deny”;
deny (write,add,delete,compare,proxy)
roledn = “ldap:///cn=Container Admin Role,($dn),$rootSuffix”;)


#
# discard
#
aci:
(target=”ldap:///ou=People,$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix)
(nsroledn=cn=Container Admin Role,$rootSuffix))))
(targetattr != “iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || nsroledn”)
(version 3.0; acl “S1IS Group and people container admin role”;
allow (all)
roledn = “ldap:///cn=ou=People_dc=red_dc=iplanet_dc=com,$rootSuffix”;)
```

组织帮助台

```
#
# discard
#
aci: (extra verses dreambig)
(target=”ldap:///$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = “*”)
(version 3.0; acl “S1IS Organization Help Desk Admin Role access allow”;
allow (read,search)
roledn = “ldap:///cn=Organization Help Desk Admin Role,$rootSuffix”;)


#
# discard
#
aci:
(target=”ldap:///$rootSuffix”)
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = “userPassword”)
(version 3.0; acl “S1IS Organization Help Desk Admin Role access allow”;
allow (write)
roledn = “ldap:///cn=Organization Help Desk Admin Role,$rootSuffix”;)
```

Access Manager 杂项

```
#
# discard - Removal disables the associated privileges to the attribute
# iplanetam-modifiable-by
#
aci:
(target=”ldap:///$rootSuffix”)
(targetattr!=”nsroledn”)
(version 3.0; acl “S1IS Group admin’s right to the users he creates”;
allow (all)
userattr = “iplanet-am-modifiable-by#ROLEDN”;)
```

索引

资

自

组