Sun Java™ System

Communications Services 6 Delegated Administrator 指南

2005Q1

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

文件号码：819-1103

目录

前言

本指南说明了如何配置和管理 Sun™ Java System Communications Services Delegated Administrator。此外，本指南还介绍了 Delegated Administrator 命令，并提供了语法和示例。

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

本章包括以下主题：

目标读者

本书适用于负责管理、配置和部署站点的 Delegated Administrator 的人员。

阅读本书之前

本书假设您负责管理软件，并大致了解以下内容：

- Internet 和万维网
- Messaging Server 协议
- Sun Java System Administration Server
- Sun Java System Directory Server 和 LDAP
- Sun Java System Console
- 以下平台上的系统管理和联网：
  - 用于 SPARC 和 x86 的 Solaris 8
  - 用于 SPARC 和 x86 的 Solaris 9
  - 用于 SPARC 和 x86 的 Solaris 10
  - HP-UX 11.x
  - Windows 2000
- 一般的部署体系结构

本书的结构

下表对本书内容进行了概括介绍。

表 1 本书的结构

章节	描述
第 1 章 “Delegated Administrator 概述”	介绍了 Delegated Administrator 提供的目录组织、管理员角色和服务等级软件包。
第 2 章 “安装和配置规划”	介绍了安装和配置 Sun Java System Communications Services Delegated Administrator 所需的步骤。
第 3 章 “配置 Delegated Administrator”	介绍并逐步执行了 Delegated Administrator 的配置程序。
第 4 章 “自定义 Delegated Administrator”	介绍了如何自定义 Delegated Administrator，例如更改控制台的外观。
第 5 章 “命令行实用程序”	介绍了 `commadmin` 实用程序，并提供了语法和示例。

表 1 本书的结构 （续）

章节	描述
附录 A “服务提供商管理员和服务提供商组织”	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提供商组织和业务组织。
附录 B “属性值和日历时区”	列出了特定命令行选项的属性值和时区值。
附录 C “调试 Delegated Administrator”	列出了日志文件，可以通过查看这些文件来调试 Delegated Administrator。
附录 D “ACI 合并”	介绍了如何合并 ACI 以及从目录中删除不使用的 ACI。

本书中使用的约定

这一部分中的表格介绍了本书中使用的约定。

印刷约定

下表介绍了本书中使用的印刷约定。

表 2 印刷约定

字体	含义	示例
AaBbCc123 （等宽字体）	在计算机屏幕上显示的任何文本或应键入的文本。可以是 API 和语言元素、 HTML 标记、 Web 站点 URL、命令名、文件名、目录路径名、计算机屏幕输出和样例代码。	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `% You have mail.`
AaBbCc123 （等宽粗体）	在代码示例或其他计算机屏幕输出中显示时应键入的文本。	`% su` `Password:`
AaBbCc123 （斜体）	命令或路径名中的占位符，应使用实际的名称或值来替换它 （例如变量）。	文件位于 *msg_svr_base*`/bin` 目录中。
新词术语强调	新词或术语以及要强调的词。	这些称为 **class** 选项。 **不要**保存文件。
《》	书名。	阅读 《用户指南》的第 6 章。

符号

下表介绍了本书中使用的符号约定。

表 3 符号约定

符号	描述	示例	含义
[ ]	包含可选命令选项。	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。
-	将同时使用的多个键击连接在一起。	Control-A	按下 A 键的同时按下 Ctrl 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”。

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 4 默认的路径和文件名

条目	描述
msg_svr_base	表示 Messaging Server 的基本安装目录。 msg_svr_base 安装的默认值如下： Solaris™ 系统：/opt/SUNWmsgsr Linux 系统：/opt/sun/messaging
da_base	表示 Delegated Administrator 的基本安装目录。 Delegated Administrator 基本目录 (*da_base*) 表示用于安装 Delegated Administrator 的目录路径。 *da_base* 的默认值为 /opt/SUNWcomm。

命令行提示符

示例中没有显示命令行提示符 （例如， % 表示 C-Shell， $ 表示 Korn 或 Bourne shell）。根据所用操作系统的不同，将会显示不同的命令行提示符。但是，除非另有明确说明，否则您应该按照文档所示输入命令。

相关文档

通过 http://docs.sun.com Web 站点，可以联机访问 Sun 技术文档。可以浏览文档集或查找某个特定的书名或主题。

Messaging Server 文档

可以使用以下 URL 查看所有 Messaging Server 文档：

http://docs.sun.com/coll/MessagingServer_05q1 和

http://docs.sun.com/coll/MessagingServer_05q1_zh

可以获取以下文档：

- Sun Java™ System Messaging Server 发行说明
- 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
- Sun Java™ System Messenger Express Customization Guide

Messaging Server 产品套件还包含其他产品，如 Sun Java™ System Directory Server 和 Administration Server。可以在以下 URL 上找到这些产品及其他产品的文档：

http://docs.sun.com/prod/entsys.05q1 和

http://docs.sun.com/db/prod/entsys.05q1?l=zh

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/CalendarServer_05q1 和

http://docs.sun.com/coll/CalendarServer_05q1_zh

可以获取以下文档：

- Sun Java™ System Calendar Server 发行说明
- Sun Java™ System Calendar Server 管理指南
- Sun Java™ System Calendar Server Developer's Guide

Communications Services 文档

可以使用以下任何一个 URL 来查看适用于所有 Communications Services 产品的文档：

http://docs.sun.com/coll/MessagingServer_05q1 和

http://docs.sun.com/coll/MessagingServer_05q1_zh

或

http://docs.sun.com/coll/CalendarServer_05q1 和

http://docs.sun.com/coll/CalendarServer_05q1_zh

可以获取以下文档：

- Sun Java™ System Communications Services Delegated Administrator 指南
- Sun Java System Communications Services Deployment Planning Guide
- Sun Java™ System Communications Services Schema Migration Guide
- Sun Java™ System Communications Services Schema Reference
- Sun Java™ System Communications Services Event Notification Service Guide
- Sun Java™ System Communications Express 管理指南
- Sun Java™ System Communications Express Customization Guide

联机访问 Sun 资源

有关产品下载、专业服务、修补程序和支持以及其他开发者信息，请访问以下站点：

- 下载中心
  http://wwws.sun.com/software/download/

- 专业服务
  http://www.sun.com/service/sunps/sunone/index.html
- Sun Enterprise 服务、 Solaris 修补程序和支持
  http://sunsolve.sun.com/
- 开发者信息
  http://developers.sun.com/prodtech/index.html

联系 Sun 技术支持

如果您遇到通过本文档无法解决的技术问题，请访问以下网址：
http://www.sun.com/service/contacting。

第三方 Web 站点

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。

如果您要提出意见，请转到 http://docs.sun.com，然后单击 “发送意见”。请在联机表单中提供文档标题和文件号码。文件号码包含 7 或 9 个数字，可以在书的标题页或文档顶部找到该号码。例如，本书的标题为 《Sun Java System Communications Services 2005Q1 Delegated Administrator 指南》，文件号码为 819-1103。

当您提供意见和建议时，可能需要在表单中提供文档英文版本的标题和文件号码。本文档英文版本的文件号码和标题为：819-0114，《Sun Java System Communications Services 2005Q1 Delegated Administrator Guide》。

第 1 章

Delegated Administrator 概述

Communications Services Delegated Administrator 实用程序和控制台允许您在 Communications Services 应用程序 （如 Messaging 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：

简介

通过 Delegated Administrator，可以将置备任务分发给级别较低的管理员，这些管理员具有管理 LDAP 目录中指定组织的权限。委托用户管理这一功能具有以下优点：

- 置备大型目录时，在多个管理员之间分发可能非常耗时的任务。可以有数十或数百个管理员来管理目录 （该目录可能包括数千或数百万用户）内的组织。
- 允许您在目录结构中创建组织，这些组织可以作为独特 （或唯一）的单位进行管理和置备。这些组织可以包含属于客户企业、公司部门或其他组的用户。

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

- Delegated Administrator 实用程序
- Delegated Administrator 控制台

以下部分对这两个界面进行了概括介绍。

Delegated Administrator 实用程序

Delegated Administrator 实用程序是一组命令行工具，用于置备 Messaging Server 和 Calendar Server 用户。（在早期版本中， Delegated Administrator 实用程序称为 User Management 实用程序。）

通过 Delegated Administrator 实用程序，可以置备组织、用户、组和日历资源。

注 Delegated Administrator 实用程序提供了命令行功能，这些功能同样存在于早期版本的 Communications Services 产品 （Messaging Server 6 2004Q2 和 Calendar Server 6 2004Q2）中。 Delegated Administrator 实用程序未提供用于创建服务提供商角色和组织 （如本书中所述）的命令。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` 命令调用该实用程序。

有关 `commadmin` 实用程序的语法和选项的信息，请参见第 5 章 “命令行实用程序”。

Delegated Administrator 控制台

Delegated Administrator 控制台是用于置备 Messaging Server 用户和组织的图形用户界面 (Graphical User Interface, GUI)。

要置备组和日历资源，请使用 Delegated Administrator 实用程序。不要使用 Delegated Administrator 控制台。在此版本的 Delegated Administrator 中，不能使用控制台来置备组和日历资源。

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

Delegated Administrator 和 LDAP 目录

Delegated Administrator 允许您通过修改 LDAP 目录来置备用户。您不必直接修改该目录。但是，如果能了解添加到目录中的用户条目和较高层节点的 Delegated Administrator 属性，可能会非常有用。

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

置备用户的方案

根据业务需求，可以创建由单个管理员管理的简单目录结构，也可以创建将置备和管理任务委托给较低级别管理员的多层目录结构。

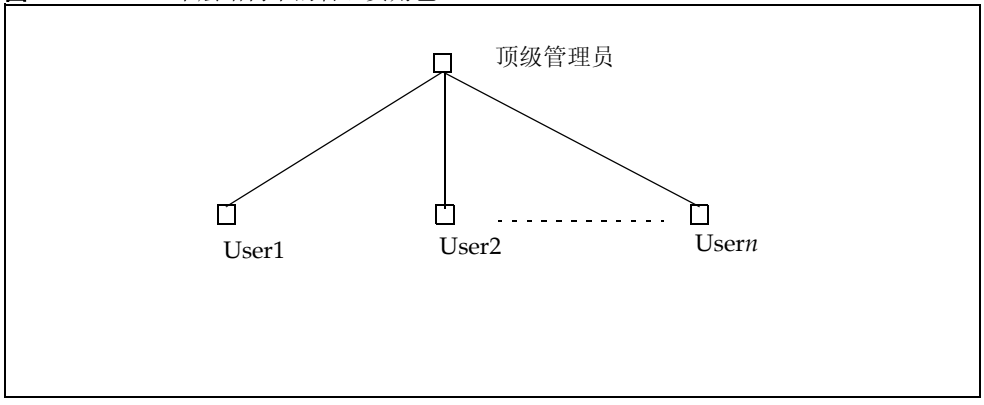
本部分概括介绍了三种复杂程度依次递增的方案。然后介绍了 Delegated Administrator 为支持这些方案的要求而提供的管理员角色和目录结构。

单层结构

在此方案中，公司或组织可能支持数百或数千名员工或用户。所有用户均属于一个组织。单个管理员角色可以查看和管理整个组。不对管理任务进行委托。

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



在此单层结构中，管理员称为顶级管理员 (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，直到 User*n*）。

如果目录中只有一个组织，则 TLA 是唯一需要的管理员。

有关详细信息，请参见以下部分：

- 支持单层结构的目录结构
- 顶级管理员角色

双层结构

在此方案中， Internet 服务提供商 (Internet Service Provider, ISP) 之类的大型公司为企业提供服务。每个企业均拥有属于自身的唯一域，其中可能包含数千或数万个用户。

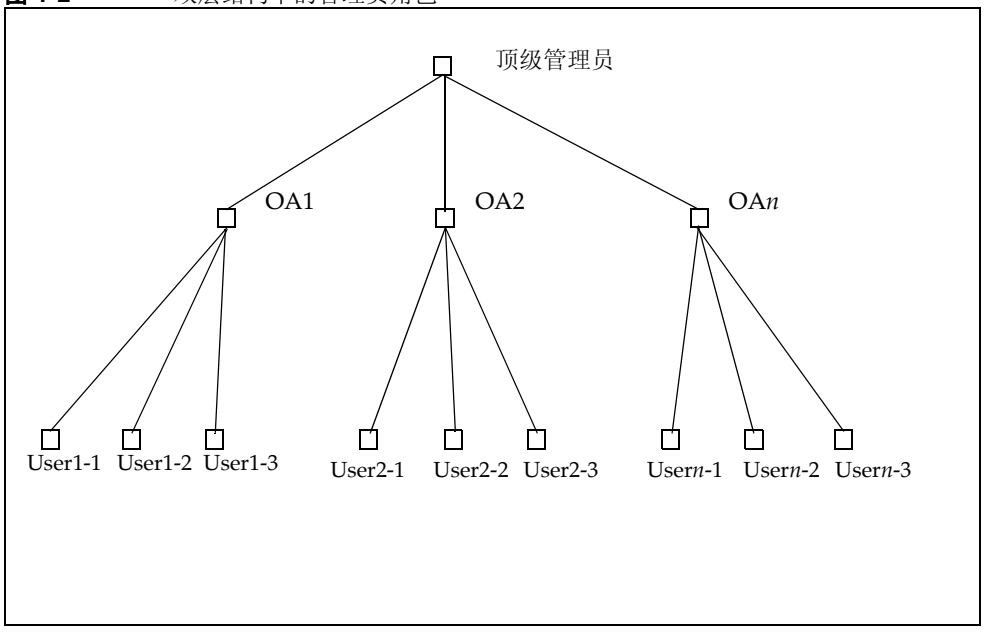
此方案支持将任务委托给级别较低的管理员，而不是依赖单个顶级管理员 (TLA) 来管理和置备所有域。

在双层结构中，目录包含多个组织。将为每个托管域创建单独的组织。

将每个组织分配给组织管理员 (Organization Administrator, OA)。 OA 负责该组织中的用户。 OA 无法查看或修改自己组织之外的目录信息。

图 1-2 显示了双层结构中的管理员角色示例。

图 1-2 双层结构中的管理员角色



在图 1-2 所示的示例中， TLA 创建和管理 OA1、 OA2，直到 OA*n*。每个 OA 都管理一个组织中的用户。

如果您的目录中需要有多个组织，则应创建 TLA 和 OA 来管理这些组织及其用户。

有关详细信息，请参见以下部分：

- 支持双层结构的目录结构
- 顶级管理员角色
- 组织管理员角色

三层结构

在此方案中， ISP 之类的公司要为数百或数千家小型企业提供服务，其中每家企业都要求拥有自身的组织。

ISP 可以支持数百万个需要邮件服务的最终用户。而且， ISP 还可以与管理最终用户业务的第三方转售商合作。

每天都可能会有许多组织添加到该目录中。

在双层结构中， TLA 必须创建所有这些新组织。

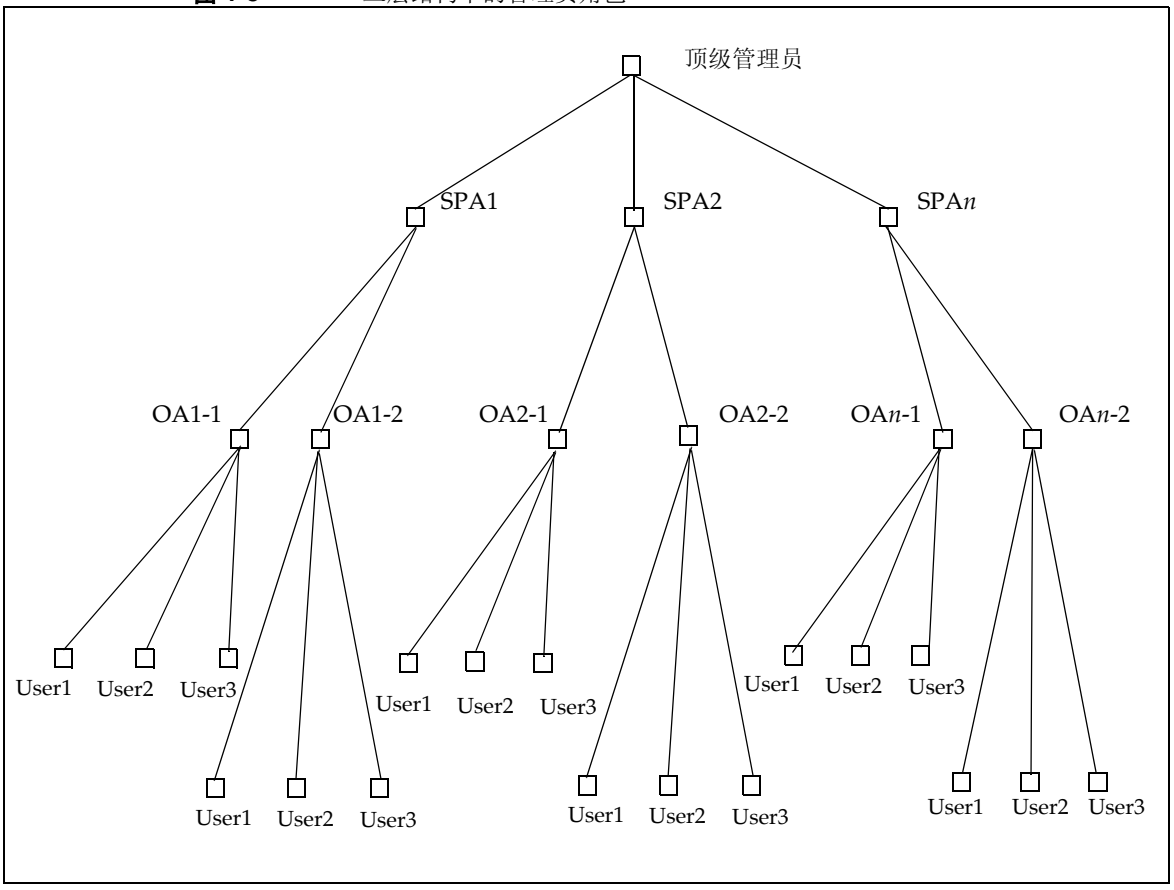
在三层结构中，可以将管理任务委托给第二级管理员。第二级委托可以简化对大型 LDAP 目录所支持的大客户群的管理。

为了支持此分层结构， Delegated Administrator 引入了新的角色，即服务提供商管理员 (Service Provider Administrator, SPA)。

SPA 的权限范围介于顶级管理员 (TLA) 和组织管理员 (OA) 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 可以将管理权限委托给服务提供商管理员 (SPA)。 SPA 可以为新客户创建业务组织，并指定组织管理员 (OA) 来管理这些业务组织中的用户。

如果您需要将自身划分为子组或组织的多个组织，则可以使用实现 TLA、 SPA 和 OA 角色的三层结构。

有关 SPA 角色的信息，请参见附录 A “服务提供商管理员和服务提供商组织”。

管理员角色和目录分层结构

本部分介绍了实现单层结构和双层结构的目录信息树样例。然后介绍了顶级管理员和组织管理员可以执行的任务。

支持单层结构的目录结构

通过运行配置程序 `config-commda` 配置 Delegated Administrator 时，将会创建顶级管理员 (TLA) 和默认组织。

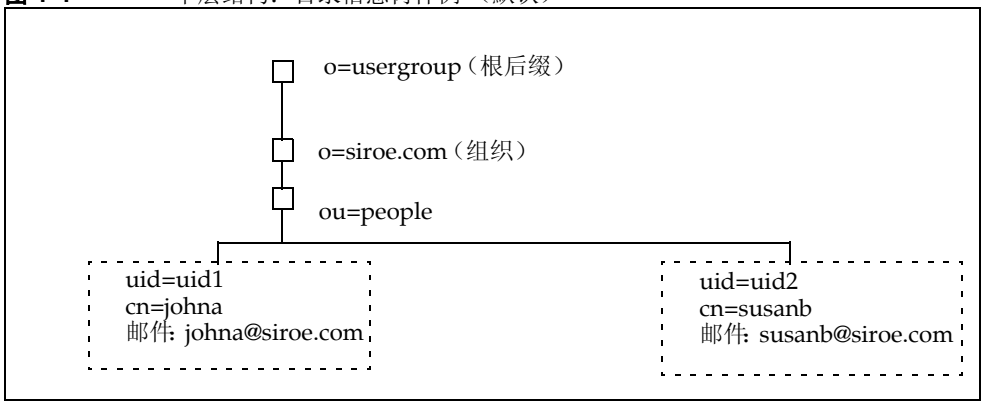
单层结构：默认组织位于根后缀下

默认情况下，配置程序会将默认组织放在根后缀下。

目录信息树类似于图 1-4 所示的示例。

图 1-4 显示了以单层结构组织的目录信息树样例 （默认配置）。

图 1-4 单层结构：目录信息树样例 （默认）



单层结构：默认组织位于根后缀处

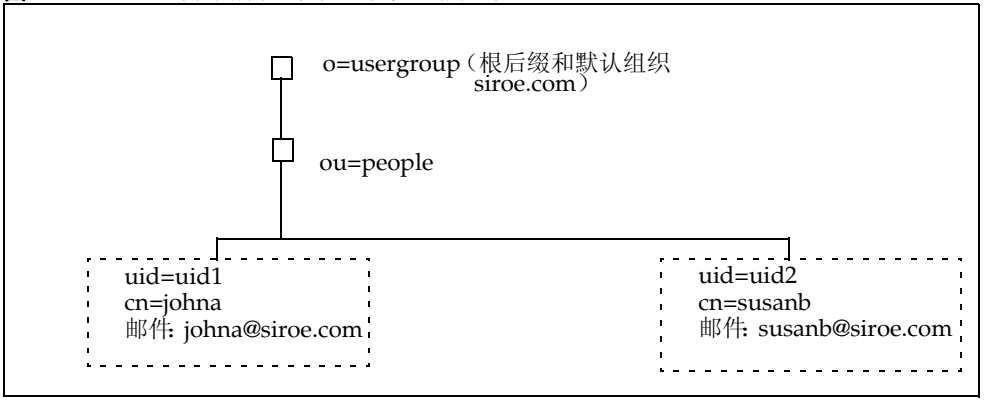
运行配置程序 (`config-commda`) 时，可以选择在根后缀处 （而不是在其下）创建默认组织。有关配置的详细信息，请参见第 3 章 “配置 Delegated Administrator”中的步骤 6，组织标识名 (DN)。

在这种情况下，目录信息树类似于图 1-5 所示的示例。

但是，如果您在根后缀处创建默认组织，此种配置的 LDAP 目录将无法支持多个托管域。要支持多个托管域，默认组织必须位于根后缀下。

图 1-5 显示了在根后缀处创建默认组织的单层结构示例。

图 1-5 单层结构：默认组织位于根后缀处

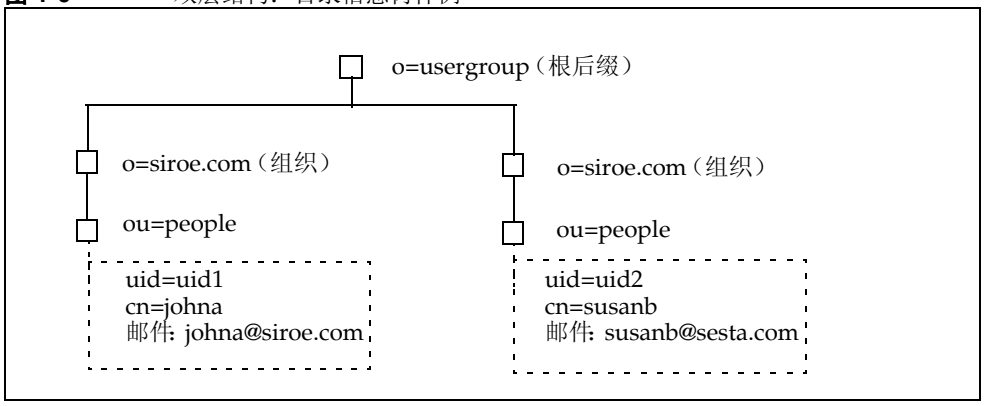


支持双层结构的目录结构

使用 `config-commda` 程序配置了 Delegated Administrator 之后， TLA 可以创建其他组织，如图 1-6 所示。

图 1-6 显示了以双层结构组织的目录信息树样例。

图 1-6 双层结构：目录信息树样例



顶级管理员角色

TLA 具有执行以下任务的权限：

- 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，在此示例中，这两个组织也是唯一的 （托管）域。

- 创建、删除和修改用户。
- 将 OA 角色分配给用户。例如， TLA 可以将 OA 角色分配给 `siroe.com` 组织中的用户 `johna`。

  TLA 还可以删除用户的 OA 角色。

- 将 TLA 角色分配给其他用户。 TLA 还可以删除用户的 TLA 角色。
- 将服务软件包分配给组织。

  有关服务软件包的信息，请参见本概述后面的服务软件包。

  TLA 可以将指定类型的服务软件包分配给组织，并确定可以在该组织中使用的每个软件包的最大数量。

  例如， TLA 可分配以下服务软件包：

  - 在 `siroe.com` 组织中：

    ```
    1,000 个 Gold 软件包
       500 个 Platinum 软件包
    ```

- 在 sesta.com 组织中：

  2,000 个 Silver 软件包
  1,500 个 Gold 软件包
  100 个 Platinum 软件包

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

有关 commadmin 命令的描述，请参见第 5 章 “命令行实用程序”中的表 5-1，Delegated Administrator 命令行界面。

组织管理员角色

OA 具有执行以下任务的权限：

- 创建、删除和修改 OA 组织中的用户。

  在图 1-6 所示的示例中，如果为 siroe.com 组织中的用户 johna 分配了 OA 角色，则 johna 可以管理 siroe.com 中的用户。

- 将 OA 角色分配给 OA 组织中的其他用户。
- 对于 OA 组织之外的用户， OA 无法进行管理或为其分配 OA 角色。

  例如， johna 无法在 sesta.com 中管理用户或分配 OA 角色。

- 为 OA 组织中的用户分配服务软件包，或删除其服务软件包。

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

有关 OA 可以使用的 commadmin 命令的描述，请参见第 5 章 “命令行实用程序”中的表 5-1， Delegated Administrator 命令行界面。

对于以前的 iPlanet Delegated Administrator 用户

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

具有 LDAP Schema 1 目录的 Messaging Server 早期版本用户可能使用过一个过时的工具：iPlanet Delegated Administrator。如果您仍具有 Schema 1 目录，则应使用 iPlanet Delegated Administrator 来置备用户。

iPlanet Delegated Administrator 使用的管理员角色术语与 Communications Service Delegated Administrator 当前使用的术语稍有不同。

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 和 Communications Services Delegated Administrator 中的管理员角色

iPlanet Delegated Administrator	Communications Services Delegated Administrator 实用程序	Communications Services Delegated Administrator 控制台	定义
站点管理员	顶级管理员 (TLA)	顶级管理员 (TLA)	管理 Delegated Administrator 支持的整个目录，包括组织和用户 *。
（无）	（在此版本中未提供）	服务提供商管理员 (SPA)	管理提供商组织、提供商组织下的共享及完整业务组织，以及这些业务组织中的用户。
域管理员	组织管理员 (OA)	组织管理员 (OA)	管理一个组织及该组织中的用户。

* 在此版本的 Delegated Administrator 中， TLA 无法在提供商组织下创建提供商组织或业务组织。

服务软件包

服务软件包由 LDAP 目录中的服务等级机制实现。此机制允许您为预定义属性 （这些属性是在配置 Delegated Administrator 时安装到目录中的）设置值。服务软件包会将服务的特征添加到用户条目中。

在 Delegated Administrator 控制台中，可以执行以下服务软件包任务：

- 为组织分配服务软件包。为组织分配了部分 （或全部）软件包后，组织中的用户即可使用这些软件包。对于每类软件包，可以分配指定数量的软件包。

  例如，对于 ABC 组织，可以分配 5,000 个 Gold 服务软件包和 10,000 个 Silver 服务软件包。

- 将服务软件包分配给用户。

  必须为 LDAP 目录中置备的每个用户至少分配一项服务。可以为一个用户分配多个服务软件包。

在为用户分配服务软件包时，服务软件包中的所有属性和值均会自动分配给该用户。

服务等级定义

此版本为 Messaging Server 用户提供了一个服务等级定义。表 1-2 显示了为邮件用户定义的 LDAP 属性：

表 1-2 可在服务软件包中使用的邮件服务属性

属性	定义
mailMsgMaxBlocks	可向用户或组发送的邮件大小的最大值 （单位为 MTA 块）。
mailAllowedServiceAccess	用于指定哪些客户端可以访问指定服务的过滤器。例如： +imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
mailMsgQuota	允许用户使用的最大邮件数 （包括所有用户文件夹）。
mailQuota	允许用户邮箱使用的磁盘空间 （单位为字节）。

有关这些属性的更多信息，请参见 《Sun Java System Communications Services Schema Reference》中的第 3 章 "Attributes"。

在称为 standardMail 的服务等级定义中定义了这些邮件服务属性。配置 Delegated Administrator 时，将在目录中安装 standardMail 定义。

standardMail 服务等级定义如下：

```
dn: cn=standardMail,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: mailAllowedServiceAccess
cosAttribute: mailMsgMaxBlocks
cosAttribute: mailquota
cosAttribute: mailmsgquota
daServiceType: mail user
```

注：Delegated Administrator 配置程序在目录中安装 standardMail 定义时，上面显示的变量 <ugldapbasedn> 将被根后缀 （如 o=usergroup）替换。

除了邮件属性之外，standardMail 定义还在属性 daServiceType 中将服务类型定义为邮件用户。

查看扩展服务软件包方面的限制

可以通过将任何属性添加到定义条目来扩展 Delegated Administrator 服务软件包定义。

但是，在此版本的 Delegated Administrator 中，使用控制台只能查看配置 Delegated Administrator 时提供的预定义属性。Delegated Administrator 控制台不显示添加到服务软件包定义中的任何属性。

在此版本中，您也不能从 Delegated Administrator 提供的 standardMail 服务等级定义中删除预定义的属性定义。

服务等级模板

根据服务等级定义中的属性，您可以创建自己的服务软件包，以便为不同用户定义不同的服务级别。

默认的服务等级模板

默认情况下， Delegated Administrator 配置程序 (config-commda) 将在目录中安装 ldif 文件 cos.default.ldif。此 ldif 文件提供了称为 defaultmail 的通用服务等级模板。

cos.default.ldif 文件中包括以下服务等级模板：

```
dn: cn=defaultmail,o=cosTemplates,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
mailquota: -2
cn: defaultmail
```

注：Delegated Administrator 配置程序在目录中安装 defaultmail 模板时，上面显示的变量 <ugldapbasedn> 将被根后缀（如 o=usergroup）替换。

在默认服务等级模板 (defaultmail) 中，仅定义了一个邮件服务属性 mailquota。其值为 -2，表示此服务的邮件配额为系统默认值。

服务等级模板样例

运行 Delegated Administrator 配置程序 config-commda 时，可以选择加载其他服务软件包样例。（运行配置程序时，请在**服务软件包和组织样例 (Service Package and Organization Samples)** 面板中选择**加载样例服务软件包 (Load sample service packages)**。）配置程序将 cos.sample.ldif 文件添加到 LDAP 目录树中。

cos.sample.ldif 文件包括以下样例服务等级模板：

Platinum
Gold
Silver
Bronze
Ruby
Topaz
Diamond
Emerald

每个模板均包含服务等级定义中所列的一个或多个属性的特定值。这些模板是服务软件包的原型示例。

例如， cos.sample.ldif 文件中包含 Platinum 服务等级模板：

```
dn: cn=platinum,o=cosTemplates,$rootSuffix
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: platinum
mailMsgMaxBlocks: 800
mailQuota: 4000000000
mailMsgQuota: 6000
mailAllowedServiceAccess: +imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
```

注：Delegated Administrator 配置程序在目录中安装样例服务等级模板时，上面显示的变量 $rootSuffix 将被根后缀（如 o=usergroup）替换。

有关所有样例服务等级模板的邮件服务值的列表，请参见本章末尾的样例服务等级模板中的邮件服务级别。

创建您自己的服务软件包

本章中介绍的服务等级模板只是一些示例。您很可能需要使用特定的属性值 （适用于您的安装中的用户）来创建自己的服务软件包。

要创建您自己的服务软件包，可以使用 `da.cos.skeleton.ldif` 文件中存储的服务等级模板。此文件是专门作为编写服务软件包的模板而创建的。配置 Delegated Administrator 时，未在 LDAP 目录中安装该文件。

可以复制和编辑 `da.cos.skeleton.ldif` 文件，并使用 `ldapmodify` 之类的 LDAP 目录工具在目录中安装服务软件包。

有关使用 `da.cos.skeleton.ldif` 文件配置您自己的服务软件包的说明，请参见第 3 章 “配置 Delegated Administrator”中的创建服务软件包。

分配给 LDAP 用户条目的样例服务软件包

使用 Delegated Administrator 将服务软件包分配给用户时，会将单个属性 (`inetCOS`) 添加到 LDAP 目录中的用户条目。`inetCOS` 属性的值可将整个服务软件包分配给用户。（`inetCOS` 是多值属性。）

例如，假设您将 Platinum 软件包分配给某个用户。以下属性将添加到用户条目中：

```
inetCOS: platinum
```

Platinum 软件包包含邮件服务属性的以下值。因此，分配 Platinum 软件包与将这些属性添加到用户条目具有相同的效果：

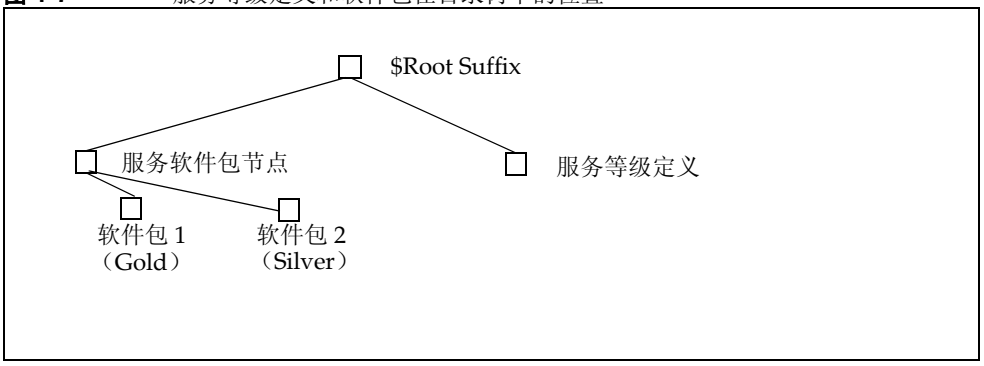
```
mailMsgMaxBlocks: 800
mailQuota: 4000000000
mailMsgQuota: 6000
mailAllowedServiceAccess: +imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
```

服务等级定义和软件包的位置

在 LDAP 目录信息树 (Directory Information Tree, DIT) 中，服务等级定义位于根后缀正下方的节点中。由于它存储在 DIT 的顶部，因此可将服务软件包分配给目录中的所有用户条目。

图 1-7 显示了服务定义和软件包在 DIT 中的位置。此处有两个示例软件包：Gold 软件包和 Silver 软件包。

图 1-7 服务等级定义和软件包在目录树中的位置



Delegated Administrator 使用典型的服务等级定义。

有关服务等级机制的更多信息，请参见 Sun Java System Directory Server 管理指南。特别是第 5 章 “管理标识和角色”中的 “定义服务等级 (CoS)”。

Directory Server 管理指南还介绍了一些相关主题，例如，如果在分配给用户的服务软件包中定义的属性已存在于该单个用户条目中，如何确定哪个服务属性值优先。

样例服务等级模板中的邮件服务级别

本部分列出了样例服务等级模板提供的邮件服务级别。这些模板中的属性值只是一些示例，并非源自于实际的安装。

Platinum

```
mailMsgMaxBlocks: 800
mailquota: 10000000
mailmsgquota: 6000
mailAllowedServiceAccess: +imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
```

Gold

```
mailMsgMaxBlocks: 700
mailquota: 8000000
mailmsgquota: 3000
mailAllowedServiceAccess: +imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
```

Silver

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

Bronze

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

Ruby

```
mailMsgMaxBlocks: 600
mailquota: 1048576
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+smtp:ALL$+http:ALL
```

Emerald

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

Diamond

```
mailMsgMaxBlocks: 5000
mailquota: 3145728
mailmsgquota: 3000
mailAllowedServiceAccess: +imap:ALL$+smtp:ALL$+http:ALL
```

Topaz

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

第 2 章

安装和配置规划

要在 Solaris 系统上安装 Sun Java System Communications Services Delegated Administrator，必须使用 Sun Java Enterprise System 安装程序，该安装程序还会安装其他 Sun 组件产品。

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

1. 收集 Delegated Administrator 配置信息
2. 运行 Java Enterprise System 安装程序
3. 运行 Directory Server 设置脚本
4. 配置 Delegated Administrator
5. 配置 Messaging Server 和 Calendar Server

有关 Delegated Administrator 的最新信息，请参见 Sun Java System Messaging Server 发行说明。

收集 Delegated Administrator 配置信息

Delegated Administrator 组件

Delegated Administrator 包含以下组件：

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

  此组件为必需组件。必须在安装 Delegated Administrator 的所有计算机上配置该实用程序。

- **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。

  此组件为必需组件。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)。

  此组件为可选组件。如果您希望仅使用 Delegated Administrator 实用程序，则不必配置控制台。

Web 容器

此外，还必须将 Delegated Administrator 服务器和控制台部署到 Web 容器。可以在以下组件上配置 Delegated Administrator 控制台和服务器

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

请遵循以下指导：

- 必须将 Delegated Administrator 服务器部署到 Access Manager 使用的 Web 容器中。
- 可以在两个不同的 Web 容器、 Web 容器的两个不同实例或同一个 Web 容器上部署 Delegated Administrator 控制台和服务器。

配置信息

在配置 Delegated Administrator 之前，应收集配置信息。

表 2-1 列出了 Delegated Administrator 所需的配置选项。

表 2-2 列出了用于在 Web Server 上进行部署的配置选项。

表 2-3 列出了用于在 Application Server 7.*x* 上进行部署的配置选项。

表 2-4 列出了用于在 Application Server 8.*x* 上进行部署的配置选项。

.

表 2-1 Delegated Administrator：必需的配置选项

选项	描述
配置目录	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台服务器上。
Access Manager 端口号	Access Manager 的端口号。该端口号应该与 Web Server 的端口号相同。
默认域	顶级管理员的默认域。在执行 `commadmin` 命令行实用程序时，如果未使用 `-n` 选项明确指定某个域，则使用此域。
默认 SSL 端口	Delegated Administrator 客户端使用的 SSL 端口。
Access Manager 基本目录	安装 Access Manager 的目录。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	Access Manager 创建的用户。此为 LDAP 服务的 BindDN 用户。
组织名称	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。
默认组织的顶级管理员用户 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 的计算机的名称。如果选择在目录中安装样例组织，则必须输入首选邮件主机。

.

表 2-2 Web Server 配置选项

选项	描述
Web Server 根 （实例）目录	Web Server 实例所在的目录。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 实例标识符	Web Server 实例的全限定域名。它可以由 *host.domain* 名称指定，如 `west.sesta.com`。
虚拟服务器标识符	由 `https-`*host.domain* 名称指定，如 `https-west.sesta.com`。

表 2-2 Web Server 配置选项 （续）

选项	描述
HTTP 端口号	Web Server 的 HTTP 端口号。

表 2-3 Application Server 7.*x* 配置选项

选项	描述
Application Server 安装目录	安装 Application Server 7.*x* 的目录。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 实例名称	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 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 管理员用户 ID 和密码。	Administration Server 管理员的用户 ID 和密码。用户 ID 示例：`admin`。
Administration Server 实例的 HTTP 或 HTTPS 访问	您需要指定 Administration Server 实例的 HTTP 访问是否安全。

表 2-4 Application Server 8.*x* 配置选项

选项	描述
Application Server 安装目录	安装 Application Server 8.*x* 的目录。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` 。

表 2-4 Application Server 8.*x* 配置选项 （续）

选项	描述
Application Server 目标名称	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 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 管理员用户 ID 和密码。	Administration Server 管理员的用户 ID 和密码。用户 ID 示例：`admin`。
Administration Server 实例的 HTTP 或 HTTPS 访问	您需要指定 Administration Server 实例的 HTTP 访问是否安全。

运行 Java Enterprise System 安装程序

Java Enterprise System 安装程序可以安装能够交互操作的一系列产品、共享组件和库。此安装程序还将执行检查操作，以确保您已经安装了以下必需的支持组件：Sun Java System Directory Server 5.x 和以下 Web 容器之一：

- Sun Java System Web Server 6.1
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

注 如果要从早期版本的 Sun Java System 升级 Delegated Administrator，请参见 Sun Java Enterprise System 升级和迁移指南中的第 3 章 “从早期版本的 Java Enterprise System 升级”。（在升级和迁移指南的第 3 章中，“升级 Messaging Server”部分包含一个题为 “升级 Delegated Administrator”的部分。）本指南可通过以下 URL 进行访问：`http://docs.sun.com/doc/819-2237`。

要成功安装和配置 Delegated Administrator，需要通过 Java Enterprise System 安装程序安装以下组件：

- Sun Java System Access Manager

  （在早期版本中， Access Manager 称为 Identity Server。）

由于 Delegated Administrator 要求使用 LDAP Schema 2 来置备用户和组，因此需要通过 Java Enterprise System 安装程序来安装 Access Manager。应将 Delegated Administrator 与 Access Manager 一起安装。

Java Enterprise System 安装程序将在称为 *da_base* 的目录中安装 Delegated Administrator （例如，默认值为 `/opt/SUNWcomm`）。

Delegated Administrator 为 Messaging Server 和 Calendar Server 的置备工具。因此，要成功使用 Delegated Administrator，应通过 Java Enterprise System 安装程序安装以下组件：

- Sun Java System Messaging Server 和 Sun Java System Calendar Server，或这两者之一。

注 建议**不要**将 Messaging Server 或 Calendar Server 与 Access Manager 安装在同一系统上。

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。

有关 Java Enterprise System 安装程序的信息，请参阅 Sun Java Enterprise System 安装指南 (http://docs.sun.com/doc/819-0810)。

运行 Directory Server 设置脚本

在配置 Delegated Administrator、 Messaging Server 或 Calendar Server 之前，Directory Server Preparation Tool 脚本 (`comm_dssetup.pl`) 只能运行一次。此脚本可以配置 LDAP Directory Server，以便与 Delegated Administrator、 Messaging Server 或 Calendar Server 配置一起使用。 `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，必须在运行 `comm_dssetup.pl` 脚本时选择 "Schema 2" 模式类型。

合并目录中的 ACI

对于包含 Access Manager、 Messaging Server 和 LDAP Schema 2 目录的大型安装，可能需要合并目录中的访问控制指令 (Access Control Instructions, ACI)。

将 Access Manager 与 Messaging Server 一起安装时，最初会在目录中安装大量的 ACI。有许多默认的 ACI 并不是 Messaging Server 所需要或使用的。通过在目录中合并默认 ACI 以减少其数量，可以提高 Directory Server 的性能，进而提高 Messaging Server 查找的性能。

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 D “ACI 合并”。

配置 Delegated Administrator

在安装 Delegated Administrator 之后，请使用收集 Delegated Administrator 配置信息中提供的信息运行 Delegated Administrator 配置程序。

有关配置程序的信息，请参见第 3 章 “配置 Delegated Administrator”。

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

配置 Delegated Administrator

Delegated Administrator 配置程序 (`config-commda`) 可以根据您的特定要求创建新的配置。此初始运行时配置程序执行最小配置。

运行该程序后，可以按照配置后的任务中介绍的步骤来完成初始配置。

通过执行 “自定义 Delegated Administrator”中介绍的任务，可以进一步自定义 Delegated Administrator 配置。

您可能还需要按 Sun Java System Messaging Server 管理指南中所述进行其他的配置。

本章介绍了以下主题：

软件自身的 DA 配置程序尚未本地化，为了便于理解，本章对涉及的界面词汇使用了双语形式。

选择要配置的组件

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

- **Delegated Administrator 实用程序 （客户端）** — 使用 `commadmin` 调用的命令行界面。
- **Delegated Administrator 服务器** — 运行 Delegated Administrator 实用程序和控制台所需的 Delegated Administrator 服务器组件。

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

配置程序将根据所选组件显示不同的面板。

以下步骤对各配置选项进行了概括介绍。每个摘要步骤 （如下）均链接到本章后面的某个部分，将在那里介绍实际的配置面板。

1. 开始配置

   在这些面板中输入所需信息，以便开始进行配置。

2. 配置 Delegated Administrator 实用程序

   这些面板紧跟在**选择要配置的组件 (Select Components to Configure)** 面板的后面。它们要求提供用于配置 Delegated Administrator 实用程序的信息。

   Delegated Administrator 实用程序是必需的，所有安装了 Delegated Administrator 组件 （服务器或控制台）的计算机上都必须配置该实用程序。

   因此，必须始终在这些面板中输入需要的信息。

3. 配置 Delegated Administrator 控制台

   这些面板跟在用于配置实用程序的面板后面。

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

   - 如果在同一台计算机上部署 Delegated Administrator 控制台和服务器，应在**选择要配置的组件 (Select Components to Configure)** 面板中同时选择控制台和服务器。
   - 此外，还可以在不同的计算机上部署 Delegated Administrator 控制台和服务器。

     在部署控制台的计算机上，只需在**选择要配置的组件 (Select Components to Configure)** 面板中选择控制台。（应始终选择实用程序。）

     在这种情况下，必须在部署服务器的计算机上再次运行配置程序。

     如果在不同的计算机上部署控制台和服务器，则在**两台**计算机上均需配置实用程序。

   配置程序将根据为控制台选择的 Web 容器来显示不同的面板。可以部署到以下 Web 容器之一：

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

- Sun Java System Application Server 8.*x*

如果在一台计算机上配置 Delegated Administrator 服务器和控制台，则需按上述说明操作**两次**（一次针对服务器，一次针对控制台）。

4. 配置 Delegated Administrator 服务器

   这些面板跟在用于配置控制台的面板后面。

   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服务器，配置程序将警告您必须在另一台计算机上配置它。服务器组件对于运行实用程序和控制台是必需的。

   部署服务器的所有其他注意事项均与部署控制台的注意事项相同（在配置 Delegated Administrator 控制台中进行了介绍）。

   另外还要注意的是，服务器使用的 Web 容器与 Access Manager 相同。（配置程序将在要求提供 Access Manager 基本目录后再要求提供 Web 容器信息。）

5. 完成配置

   在这些面板中输入所需信息，以完成配置。

运行配置程序

本部分介绍的步骤将指导您配置 Delegated Administrator。

要运行配置程序，请作为（或成为）超级用户进行登录，并转到 `/opt/SUNWcomm/sbin` 目录。然后输入命令：

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

运行 `config-commda` 命令之后，将会启动配置程序。

以下部分将介绍配置面板：

开始配置

请执行以下步骤：

1. **欢迎使用**

   配置程序中的第一个面板是版权页。可单击“下一步” (Next) 继续或单击“取消” (Cancel) 退出。

2. **选择用于存储配置和数据文件的目录**

   选择用于存储 Delegated Administrator 配置和数据文件的目录。默认的配置目录为 `/var/opt/SUNWcomm`。此目录应与 *da_base* 目录 (`/opt/SUNWcomm`) 分开。

   输入该目录的名称，或保留默认值，然后单击 “下一步” (Next) 继续。

   如果该目录不存在，则会显示一个对话框，询问是否要创建该目录或选择一个新目录。可单击 “创建目录” (Create Directory) 来创建该目录，或单击 “选择新目录” (Choose New) 来输入新的目录。

   此时将显示一个对话框，指示正在加载组件。这可能需要几分钟的时间。

3. **选择要配置的组件**

   在组件面板上选择要配置的一个或多个组件。

   - **Delegated Administrator 实用程序 （客户端）** — 使用 `commadmin` 调用的命令行界面。此组件为必需组件，并且在默认情况下将选择该组件。无法取消选择该组件。
   - **Delegated Administrator 服务器** — 运行 Delegated Administrator 控制台所需的 Delegated Administrator 服务器组件。
   - **Delegated Administrator 控制台** — Delegated Administrator 图形用户界面 (GUI)。

   可单击 “下一步” (Next) 继续、单击 “上一步” (Back) 返回到上一个面板，或单击 “取消” (Cancel) 退出。

   有关如何选择组件的更多信息，请参见选择要配置的组件。

   如果选择不配置 Delegated Administrator 服务器，则会出现一个对话框，警告您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

请执行以下步骤：

1. **Access Manager 主机名和端口号**

   输入 Access Manager （以前称为 Identity Server）的主机名和端口号。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。

   可单击 “下一步” (Next) 继续、单击 “上一步” (Back) 返回到上一个面板，或单击 “取消” (Cancel) 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，如果未使用 `-n` 选项明确指定某个域，则使用此域。它也称为默认组织。如果指定的域在目录中不存在，则将创建该域。

   可单击“下一步” (Next) 继续、单击“上一步” (Back) 返回到上一个面板，或单击“取消” (Cancel) 退出。

3. **客户端的默认 SSL 端口**

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

   可单击“下一步” (Next) 继续、单击“上一步” (Back) 返回到上一个面板，或单击“取消” (Cancel) 退出。

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

   完成配置

   如果选择同时配置 Delegated Administrator 控制台和服务器，或者选择仅配置控制台，请转至

   配置 Delegated Administrator 控制台

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

   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 (Select a Web Container for Delegated Administrator)

选择用于部署 Delegated Administrator 控制台的 Web 容器。可以在以下组件上配置 Delegated Administrator

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

可单击“下一步” (Next) 继续、单击“上一步” (Back) 返回到上一个面板，或单击“取消” (Cancel) 退出。

此面板及其后面的面板用于收集有关 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：

- Web 服务器配置
- Application Server 7.x 配置
- Application Server 8.x 配置

可以在两个不同的 Web 容器、Web 容器的两个不同实例或同一个 Web 容器上部署 Delegated Administrator 控制台和服务器。

如果选择在面板 3 中同时配置 Delegated Administrator 控制台和 Delegated Administrator 服务器，则另一系列的面板将询问服务器的 Web 容器信息。

因此，您将看到 Web 容器配置面板出现两次。请按照部署每个 Delegated Administrator 组件的相应说明执行操作。

在完成 Web 容器配置面板时：

- 如果选择同时配置 Delegated Administrator 控制台和服务器，请转至

  配置 Delegated Administrator 服务器

- 如果选择仅配置 Delegated Administrator 控制台 （以及所需的 Delegated Administrator 实用程序），请转至

  完成配置

Web 服务器配置

如果要在 Web 服务器上部署 Delegated Administrator 服务器或控制台，请执行以下步骤：

1. **Web 服务器配置详细信息**

   此面板中的文本将显示您是否正在为 Delegated Administrator 服务器或控制台提供 Web 服务器配置信息。

   输入 Web 服务器根目录。可以通过浏览来选择该目录。

   输入 Web 服务器实例标识符。这可以由 *host.domain* 名称指定，如 `west.sesta.com`。

   输入虚拟服务器标识符。这可以由 `https-`*host*`.`*domain* 名称指定，如 `https-west.sesta.com`。

   有关 Web 服务器实例标识符和虚拟服务器标识符的更多信息，请参见 Web 服务器文档。

   Web 服务器实例的文件存储在 Web 服务器安装目录下的 `https-`*host*`.`*domain* 目录中，例如 `/opt/SUNWwbsvr/https-west.sesta.com`。

   输入 Web 服务器的 HTTP 端口号。

   可单击“下一步” (Next) 继续、单击“上一步” (Back) 返回到上一个面板，或单击“取消” (Cancel) 退出。

   配置程序将检查您指定的值是否有效。如果目录或标识符无效或不存在，则会显示一个对话框，要求您选择新的值。

   接下来，配置程序将检查 Web 服务器实例连接是否处于活动状态。如果未处于活动状态，则会显示一个对话框，警告您配置程序无法连接到指定实例，并且您的配置可能未完成。您可以接受指定的值，或选择新的 Web 服务器配置值。

2. **默认域分隔符**

   只有在配置 Delegated Administrator 控制台时才会显示此面板。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。可以在配置程序运行之后编辑此属性值。有关更多信息，请参见“自定义 Delegated Administrator”。

3. **如果要配置 Delegated Administrator 控制台：**

   - 如果选择同时配置 Delegated Administrator 控制台和服务器，请转至

     配置 Delegated Administrator 服务器

   - 如果选择仅配置 Delegated Administrator 控制台 （以及所需的 Delegated Administrator 实用程序），请转至

完成配置

如果要配置 Delegated Administrator 服务器：

请转至

步骤 3，配置 Delegated Administrator 服务器中的 Directory (LDAP) Server。

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，请执行以下步骤：

1. **Application Server 7.*x* 配置详细信息**

   此面板中的文本将显示您是否正在为 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目录。

   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。

   可单击“下一步”(Next) 继续、单击“上一步”(Back) 返回到上一个面板，或单击“取消”(Cancel) 退出。

   配置程序将检查您指定的目录是否有效。如果目录无效或不存在，则会显示一个对话框，要求您选择新的目录。

   接下来，配置程序将检查 Application Server 实例连接是否处于活动状态。如果未处于活动状态，则会显示一个对话框，警告您配置程序无法连接到指定实例，并且您的配置可能未完成。您可以接受指定的值，或选择新的 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`

   输入管理员用户密码。

   如果要使用安全的 Administration Server 实例，请选中**安全的 Administration Server 实例 (Secure Administration Server Instance)** 框。如果不使用此实例，请使该框保持未选中状态。

   可单击“下一步” (Next) 继续、单击“上一步” (Back) 返回到上一个面板，或单击“取消” (Cancel) 退出。

3. **默认域分隔符**

   只有在配置 Delegated Administrator 控制台时才会显示此面板。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. **如果要配置 Delegated Administrator 控制台：**

   - 如果选择同时配置 Delegated Administrator 控制台和服务器，请转至

     配置 Delegated Administrator 服务器

   - 如果选择仅配置 Delegated Administrator 控制台 （以及所需的 Delegated Administrator 实用程序），请转至

     完成配置

   如果要配置 Delegated Administrator 服务器：

   请转至

   步骤 3，配置 Delegated Administrator 服务器中的 Directory (LDAP) Server。

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，请执行以下步骤：

1. **Application Server 8.*x* 配置详细信息**

   此面板中的文本将显示您是否正在为 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目录。

   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`。

   输入 Application Server 的目标 HTTP 端口号。

   可单击“下一步”(Next) 继续、单击“上一步”(Back) 返回到上一个面板，或单击“取消”(Cancel) 退出。

   配置程序将检查您指定的目录是否有效。如果目录无效或不存在，则会显示一个对话框，要求您选择新的目录。

   接下来，配置程序将检查 Application Server 目标连接是否处于活动状态。如果未处于活动状态，则会显示一个对话框，警告您配置程序无法连接到指定目标，并且您的配置可能未完成。您可以接受指定的值，或选择新的 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，请选中**安全的 Administration Server 实例 (Secure Administration Server Instance)** 框。如果不使用此实例，请使该框保持未选中状态。

   可单击“下一步”(Next) 继续、单击“上一步”(Back) 返回到上一个面板，或单击“取消”(Cancel) 退出。

3. **默认域分隔符**

   只有在配置 Delegated Administrator 控制台时才会显示此面板。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. **如果要配置 Delegated Administrator 控制台：**

   - 如果选择同时配置 Delegated Administrator 控制台和服务器，请转至

     配置 Delegated Administrator 服务器

   - 如果选择仅配置 Delegated Administrator 控制台 （以及所需的 Delegated Administrator 实用程序），请转至

     完成配置

   如果要配置 Delegated Administrator 服务器：

   请转至

   步骤 3，配置 Delegated Administrator 服务器中的 Directory (LDAP) Server。

配置 Delegated Administrator 服务器

如果选择配置 Delegated Administrator 服务器，配置程序将显示以下面板。请输入所需信息：

1. **Access Manager 基本目录**

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

   可单击 “下一步” (Next) 继续、单击 “上一步” (Back) 返回到上一个面板，或单击 “取消” (Cancel) 退出。

   配置程序将检查是否指定了有效的 Access Manager 基本目录。如果未指定，则会显示一个对话框，指示必须选择现有的 Access Manager 基本目录。

2. 接下来，将显示 Web 容器的**配置详细信息 (Configuration Details)** 面板。

   如果选择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 (Configuration Details)** 面板。

   Delegated Administrator 服务器将被部署到与 Access Manager 相同的 Web 容器中。（不能为 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：

- Web 服务器配置
- Application Server 7.x 配置
- Application Server 8.x 配置

3. **Directory (LDAP) Server**

   此面板要求提供有关连接到用户 / 组后缀的 LDAP Directory Server 的信息。

   在文本框中输入用户和组的 Directory Server LDAP URL (**LdapURL**)、Directory Manager （**绑定为 (Bind As)**）和密码。

   Directory Manager 对 Directory Server 以及使用 Directory Server （例如 Delegated Administrator）的所有 Sun Java System Server 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访问权限。默认和推荐的标识名 (Distinguished Name, DN) 为 `cn=Directory Manager`。

   可单击“下一步”(Next) 继续、单击“上一步”(Back) 返回到上一个面板，或单击“取消”(Cancel) 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 时将创建用户 ID 和密码。默认用户 ID 为 `amadmin`。

   可单击“下一步”(Next) 继续、单击“上一步”(Back) 返回到上一个面板，或单击“取消”(Cancel) 退出。

5. **Access Manager 的内部 LDAP 验证密码**

   输入 Access Manager 内部 LDAP 验证用户的密码。

   验证用户名被固定编码为 `amldapuser`。它由 Access Manager 安装程序创建，是 LDAP 服务的绑定 DN 用户。

   可单击“下一步”(Next) 继续、单击“上一步”(Back) 返回到上一个面板，或单击“取消”(Cancel) 退出。

6. **组织标识名 (DN)**

   输入默认域的组织 DN。例如，如果您的组织 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` 为您的根后缀。

   默认情况下，配置程序将在 LDAP 目录中的根后缀下添加默认域。

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

   例如，如果您的组织 DN 为 `o=siroe.com`，根后缀为 `o=usergroup`，请从文本框中的 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，可能很难迁移到托管域配置。`config-commda` 程序将显示以下警告信息：

   “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，请在用户 / 组后缀的下一级指定 DN。”
   (The Organization DN you chose is the User/Group Suffix. Although this is a valid choice, if you ever decide to use hosted domains, there will be difficult migration issues. If you do wish to use hosted domains, then specify a DN one level below the User/Group suffix.)

   有关更多信息，请参见第 1 章 “Delegated Administrator 概述”中的支持单层结构的目录结构。

   可单击 “下一步” (Next) 继续、单击 “上一步” (Back) 返回到上一个面板，或单击 “取消” (Cancel) 退出。

7. **默认组织的顶级管理员**

   输入要在默认域 （组织）中创建的顶级管理员的用户 ID 和密码。

   可单击 “下一步” (Next) 继续、单击 “上一步” (Back) 返回到上一个面板，或单击 “取消” (Cancel) 退出。

8. **服务软件包和组织样例**

   可以选择将样例服务软件包和样例组织添加到您的 LDAP 目录中。

   加载样例服务软件包。如果您要使用或修改样例服务软件包模板来创建您自己的服务等级软件包，请选择此选项。（在 Delegated Administrator 中，必须至少将一个服务等级软件包分配给 LDAP 目录中的每个用户。）

   加载样例组织。如果要在 LDAP 目录树中包含样例服务提供商组织节点和业务组织节点，请选择此选项。

   您可以

   - 同时选择样例服务软件包和样例组织
   - 仅选择这些选项中的一项
   - 不选择任何选项

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

   例如 `mymachine.siroe.com`

   如果选择将样例组织加载到您的 LDAP 目录中，则必须为这些样例输入首选邮件主机名。

   有关服务软件包和组织的信息，请参见第 1 章 “Delegated Administrator 概述”。

   运行配置程序后，必须修改服务软件包模板，以创建您自己的服务等级软件包。有关此配置后任务的信息，请参见创建服务软件包。

完成配置

要完成配置，请执行以下步骤：

1. **准备配置**

   验证面板会显示将要配置的项目。

   可单击“立即配置”(Configure Now) 开始配置、单击“上一步”(Back) 返回到前面的任何一个面板以更改信息，或单击 “取消” (Cancel) 退出。

2. **任务顺序**

   “任务顺序” (Task Sequence) 面板上显示了任务的执行顺序。这是实际配置发生的时间。

   当面板显示 “所有任务已通过” (All Tasks Passed) 时，可单击 “下一步” (Next) 继续，或单击 “取消” (Cancel) 停止执行这些任务并退出。

   此时将显示一个对话框，提醒您重新启动 Web 容器，以使配置更改生效。

3. **安装摘要**

   “安装摘要” (Installation Summary) 面板显示了所安装的产品，以及用于显示有关此配置的更多信息的 “详细信息 ...” (Details...) 按钮。

   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。

   单击 “关闭” (Close) 以完成配置。

重新启动 Web 容器

完成 Delegated Administrator 配置后，必须重新启动部署 Delegated Administrator 的 Web 容器 （以下组件之一）：

- Web Server
- Application Server 7.*x*
- Application Server 8.*x*

`config-commda` 程序创建的配置和日志文件

配置文件

使用面板中提供的信息，`config-commda` 程序将为三个 Delegated Administrator 组件创建以下配置文件：

- Delegated Administrator 实用程序：

  配置文件名：`cli-usrprefs.properties`
  默认位置：`/var/opt/SUNWcomm/config`

- Delegated Administrator 服务器：

  配置文件名：resource.properties
  默认位置：
  /opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet
  或
  /var/opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet

- Delegated Administrator 控制台：

  配置文件名：daconfig.properties
  默认位置：
  /opt/SUNWcomm/WEB-INF/classes/com/sun/comm/da/resources
  或
  /var/opt/SUNWcomm/WEB-INF/classes/com/sun/comm/da/resources

有关这些文件、它们所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 “自定义 Delegated Administrator”。

日志文件

Delegated Administrator 控制台可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 日志文件的更多信息，请参见附录 C “调试 Delegated Administrator”。

执行无提示安装

Delegated Administrator 实用程序初始运行时配置程序将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，可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。

例如，运行了一次 config-commda 程序之后，即可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

要启动 Delegated Administrator 控制台，请执行以下步骤：

1. 转至以下 URL：

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

   其中

   host 为 Web 容器主机

   port 为 Web 容器端口

   例如：

   http://siroe.com:8080/da/DA/Login

   此时将显示 Delegated Administrator 控制台登录窗口。

2. 登录到 Delegated Administrator 控制台。

   可以使用 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。在以下面板中要求提供此信息：

   默认组织的顶级管理员 (Top-Level Administrator for the default organization)

运行命令行实用程序

要运行 Delegated Administrator 实用程序 (commadmin)，请执行以下步骤：

1. 转至 *da_base*/bin/ 目录。例如，转至 /opt/SUNWcomm/bin/。
2. 输入 commadmin 命令。

   例如：

   commadmin -D *userid* -w *password*

   其中 *userid* 和 *password* 是 Delegated Administrator 配置程序中指定的顶级管理员 (TLA) 的用户 ID 和密码。在以下面板中要求提供此信息：

   默认组织的顶级管理员 (Top-Level Administrator for the default organization)

配置后的任务

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

- 将邮件和日历服务添加到默认域
- 创建服务软件包

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

- 为 Schema 2 兼容模式添加 ACI

将邮件和日历服务添加到默认域

config-commda 程序将创建默认域。

如果要在默认域中创建具有邮件服务或日历服务的用户，首先必须将邮件服务和日历服务添加到该域中。

要执行此任务，请将 commadmin domain modify 命令与 -S mail 和 -S cal 选项一起使用。

下面的示例显示了如何使用 commadmin domain modify 将邮件和日历服务添加到默认域中：

```
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 “命令行实用程序”。

创建服务软件包

在 LDAP 目录中使用 Delegated Administrator 置备的每个用户都应具有服务软件包。一个用户可拥有多个服务软件包。

预定义的服务等级模板

在运行 Delegated Administrator 配置程序 (`config-commda`) 时，将在 LDAP 目录中安装默认的服务等级模板 (`defaultmail`)。还可以选择让 `config-commda` 程序在该目录中安装由 8 个样例服务等级模板组成的模板集。

有关样例服务等级模板以及服务软件包中的可用邮件属性的信息，请参见第 1 章 “Delegated Administrator 概述”中的服务软件包。

可以将样例服务等级模板用作服务软件包。但是，这些模板只是一些示例。

创建自己的服务软件包

您很可能需要使用特定的属性值 （适用于您的安装中的用户）来创建自己的服务软件包。

要创建您自己的服务软件包，请使用 `da.cos.skeleton.ldif` 文件中存储的服务等级模板。

此文件是专门作为编写服务软件包的模板而创建的。配置 Delegated Administrator 时，未在 LDAP 目录中安装该文件。

da.cos.skeleton.ldif 文件中的服务等级模板如下：

```
# Template for creating a COS template for a service package.
#
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
# - mailQuota
# - mailMsgQuota
# - mailAllowedServiceAccess
#
# 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>
#
dn:cn=<service package name>,o=cosTemplates,<rootSuffix>
changetype:add
objectclass:top
objectclass:LDAPsubentry
objectclass:extensibleobject
objectclass:cosTemplate
cn:<service package name>
mailMsgMaxBlocks:<mailMsgMaxBlocksValue>
mailQuota:<mailQuotaValue>
mailMsgQuota:<mailMsgQuotaValue>
mailAllowedServiceAccess:<mailAllowedServiceAccessValue>
```

要创建您自己的服务软件包，请执行以下步骤：

1. 复制并重命名 da.cos.skeleton.ldif 文件。

   安装 Delegated Administrator 时，将在以下目录中安装 da.cos.skeleton.ldif 文件：

   da_base/lib/config-templates

2. 在 da.cos.skeleton.ldif 文件的副本中编辑以下条目：

   - <rootSuffix>

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

<rootSuffix> 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软件包名称。

  <service package name> 参数显示在 DN 和 cn 中。

- 邮件属性值：

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

  按照您的规范编辑这些值。

  例如，您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
  ```

  有关这些属性的定义和描述，请参见 《Sun Java System Communications Services Schema Reference》中的第 3 章 "Attributes"。

  不必在服务软件包中使用所有这四个邮件属性。可以从服务软件包中删除一个或多个属性。

3. 使用 LDAP 目录工具 ldapmodify 将服务软件包安装在目录中。

   例如，您可以运行以下命令：

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

   其中

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

   <password> 为 Directory Service 管理员的密码。

   <cos.finished.template.ldif> 为编辑过的 ldif 文件的名称，该文件要作为服务软件包安装在目录中。

为 Schema 2 兼容模式添加 ACI

如果要在 Schema 2 兼容模式下使用 LDAP 目录，则必须将 ACI 手动添加到该目录中，以便 Delegated Administrator 在您的目录中执行置备任务。请执行以下步骤：

1. 将下面两个 ACI 添加到 OSI 根。可以在位于 /opt/SUNWcomm/config 目录的 usergroup.ldif 文件中找到下面两个 ACI。

   请确保使用您的 usergroup 后缀来替换 *ugldapbasedn*。将编辑过的 usergroup.ldif 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. 将下面两个 ACI 添加到 DC 树根后缀中。可以在位于 /opt/SUNWcomm/config 目录的 dctree.ldif 文件中找到下面两个 ACI。

   请确保使用您的 DC 树根后缀来替换 *dctreebasedn*，并使用您的 usergroup 后缀来替换 *ugldapbasedn*。将编辑过的 dctree.ldif 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. 将下面的附加 ACI 添加到 DC 树根后缀中。（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，请修改 <*IS_base_directory*>/lib/AMConfig.properties 文件中的以下行：

   将
   com.iplanet.am.domaincomponent=o=isp
   修改为
   com.iplanet.am.domaincomponent=o=internet

5. 启用 Access Manager（以前称为 Identity Server）以使用兼容模式。在 Access Manager Console 的 “管理控制台服务”页中，选中 （启用）**启用域组件树**复选框。

6. 将 inetdomain 对象类添加到所有 DC 树节点 （如 dc=com,o=internet）中，如下例所示：

```
/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。

第 4 章

自定义 Delegated Administrator

在使用配置程序 (config-commda) 安装和配置了 Delegated Administrator 之后，您可以通过自定义配置来满足您的特定需求。本章提供了有关如何自定义某些 Delegated Administrator 功能的示例。

本章介绍了以下主题：

- 使用服务范围的默认值配置首选邮件主机
- 为 Delegated Administrator 添加插件
- 自定义用户登录

使用服务范围的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，则可以执行在本部分中介绍的任务。

如果需要从控制台中 （具体地说，是从 “新建组织向导” 和 “组织属性” 屏幕中）删除 “首选邮件主机” 字段，则可以执行以下步骤：

- 编辑 Security.properties 文件。本部分介绍了这一步骤。
- 启用 MailHostStorePlugin。在下面的部分为 Delegated Administrator 添加插件中介绍了这一步骤。

使用 Security.properties 文件可以为所有角色或单个角色自定义 Delegated Administrator 控制台。

Security.properties 文件位于以下目录中：
da_base/da/WEB-INF/classes/com/sun/comm/da/resources

要从控制台中删除首选邮件主机，请将下面所示的行添加到 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
```

警告：您可以将这些行添加到此文件中，以便进行自定义配置，但不要编辑已存在的行。编辑现有行可能会导致控制台抛出异常。

此文件中的属性格式如下：*Security Element Name=Permission*

安全元素名称的格式如下：
Role Name.Container View Name.Console Element Name

安全元素指定了为其定义权限的控制台元素和角色。如果您不知道元素名称，请查看页面源代码，查找您所需的控制台元素在页面上的名称。

页面上的名称为全限定名称。您只需选取该名称的最后两个元素，即构成 *Container View Name.Console Element Name* 的元素。

Delegated Administrator 的有效角色名称如下：

"ProviderAdminRole" (SPA)。有关此角色的信息，请参见附录 A “服务提供商管理员和服务提供商组织”。

"OrganizationAdminRole" (OUA)

"Top-levelAdminRole" (TLA)

"*" （将权限应用于所有角色，除非该权限被特定角色的权限覆盖）

权限必须为以下字符串之一：

- EDITABLE — 指明安全元素是可编辑的。
- NONEDITABLE — 指明安全元素是只读的。
- VISIBLE — 指明安全元素可见且是只读的。
- INVISIBLE — 指明安全元素不可见。

为 Delegated Administrator 添加插件

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

- `MailHostStorePlugin`

默认情况下，此插件是禁用的。如果在创建业务组织时未提供 preferredmailhost，则会出现异常。如果启用了该插件，则仅在缺少相应属性时，才会使用平面文件 （将在本部分的后面进行介绍）中的值。

- MailDomainReportAddressPlugin

  使用域值返回所需的 DSN 地址。默认实现是返回字符串 MAILER-DAEMON@<*domain*>。

- UidPlugin

  生成唯一的 ID 字符串。默认实现是生成 GUID 以返回给调用者。

- VolInternalLoginPlugin

  通过使用 "volmaillogin" 属性值 （由 Delegated Administrator 控制台传入）以及在 volinternalloginpluginfile 中找到的值来设置属性 "volinternallogin"。 volinternallogin 属性的格式为 <*volmaillogin value*>@<*value found in file*>。有关 volinternalloginpluginfile 的详细信息，请参见本部分后面的两个插件所需的其他平面文件。

  在 resource.properties 文件中，必须将 attr-loginid 设置为 volmaillogin。

- ObjectclassPlugin

  将 "volperson" 对象类添加到创建的每个用户。

启用插件

要启用这些插件，请编辑位于以下目录中的 commcli servlet resource.properties 文件：

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 文件中具有以下标题的部分：

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

每个插件都以 "plugin" 作为后缀。当前列表看起来如下所示：

```
jdapi-mailhoststoreplugin=disabled
```

```
jdapi-mailhoststorepluginclass=sun.comm.cli.server.util.MailHostStorePlugin
jdapi-mailhoststorepluginfile=/tmp/mailhostmailstore
jdapi-volinternalloginplugin=disabled
jdapi-volinternalloginpluginclass=sun.comm.cli.server.util.
  VolInternalLoginPlugin
jdapi-volinternalloginpluginfile=/tmp/volinternalloginplugin
jdapi-objectclassplugin=disabled
jdapi-objectclasspluginclass=sun.comm.cli.server.util.ObjectClassPlugin
jdapi-maildomainreportaddressplugin=enabled
jdapi-maildomainreportaddresspluginclass=sun.comm.cli.server.
  util.MailDomainReportAddressPlugin
jdapi-uidautogenerationplugin=disabled
jdapi-uidautogenerationpluginclass=sun.comm.cli.server.util.UidPlugin
```

插件格式

每个插件至少有两行，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"` 更改为 `"enabled"`。

对于本部分中列出的所有插件都提供了插件类。这些类位于以下目录中：

da_base`/data/WEB-INF/classes/sun/comm/cli/server/util`

您不必对这些类执行任何操作。

两个插件所需的其他平面文件

`MailHostStorePlugin` 和 `VolInternalLoginPlugin` 这两个插件需要一个平面文件，该文件包含在插件的第三行中。插件可读取平面文件中的值，并使用该值来设置属性值。如果启用了插件，则该文件必须存在，否则将出现错误。

- `jdapi-mailhoststoreplugin`
  - `jdapi-mailhoststorepluginin`f=<*full file name*>
  - `file has one line`
    - `value is that for :`
      - `preferredmailhost attribute`
      - `preferredmailmessagestore attribute`
    - `form`
      - <*mailhost*>:<*mailpartion*>

- jdapi-volinternalloginplugin
  - jdapi-volinternalloginpluginfile=<*full file name*>
  - file has one line
  - value is that for
    - right hand side of volinternallogin attribute

自定义用户登录

在运行 Delegated Administrator 配置程序 (config-commda) 时，会将您用于登录 Delegated Administrator 的值设置为 uid。

例如，如果要作为 TLA 登录，并且 TLA 的 uid 为 john.doe，则需使用 john.doe 登录 Delegated Administrator。

您可以自定义 Delegated Administrator，以便您能够使用其他用户登录值。例如，您可以添加邮件地址 (mail)。

如何设置用户登录值

config-commda 程序使用 resource.properties 文件中的 loginAuth-idAttr 属性将此值设置为 uid，如下例所示：

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

其中 <*$rootSuffix*> 为目录中的根后缀。

resource.properties 文件位于 /var/opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties 中。

添加用户登录值

可以通过编辑 resource.properties 文件来设置其他用户登录值。

例如，要使用邮件地址 （如 john.doe@sesta.com）进行登录，可以将以下行添加到 resource.properties 文件中：

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

其中 *<$rootSuffix>* 为目录中的根后缀。

请注意，对于每个新值，必须向 `loginAuth-idAttr` 属性中添加一个增量。在此示例中，需要添加第二个值，因此将 `-2` 添加到 `loginAuth-idAttr` 中。

可以向 `loginAuth-idAttr` 属性中添加多个实例：

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

第 5 章

命令行实用程序

Delegated Administrator 命令行实用程序允许管理员为用户、组、域和组织管理不同的通信服务。本章介绍了一个命令行工具集，可用于对用户、组、域和组织执行诸如创建、修改、删除和搜索等批量操作。

表 5-1 中列出了这些命令。此表由三列组成；第一列列出了命令、第二列列出了命令描述，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	描述	执行权限 *
commadmin admin add	将组织管理员权限授予用户	顶级管理员
commadmin admin remove	吊销用户的组织管理员权限	顶级管理员
commadmin admin search	搜索和显示具有组织管理员权限的用户	顶级管理员、组织管理员
commadmin domain create	创建域	顶级管理员
commadmin domain delete	删除域	顶级管理员
commadmin domain modify	修改域	顶级管理员
commadmin domain purge	清除域	顶级管理员
commadmin domain search	搜索域	顶级管理员
commadmin group create	创建组	顶级管理员、组织管理员和邮件列表拥有者
commadmin group delete	删除组	顶级管理员、组织管理员和邮件列表拥有者
commadmin group modify	修改组	顶级管理员、组织管理员和邮件列表拥有者

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

命令	描述	执行权限 *
commadmin group search	搜索组	任何人
commadmin resource create	创建资源	顶级管理员、组织管理员
commadmin resource modify	修改资源	顶级管理员、组织管理员
commadmin resource delete	删除资源	顶级管理员、组织管理员
commadmin resource search	搜索资源	任何人
commadmin user create	创建用户	顶级管理员、组织管理员
commadmin user delete	删除用户	顶级管理员、组织管理员
commadmin user search	搜索用户	任何人
commadmin user modify	修改用户	顶级管理员、组织管理员

* 此版本的 Delegated Administrator 不支持服务提供商管理员使用 commadmin 实用程序。

执行模式

有三种可能的命令行执行模式：

- 使用文件中指定的选项执行

  commadmin *object task* -i *inputfile*

  分析 *inputfile* 并执行它。

- 交互式

  commadmin *object task*

  向管理员询问其余的选项和属性。

- 立即执行或 shell 执行

  commadmin *object task* [*options*]

命令文件格式

可以使用 -i 选项在文件内指定选项。

在文件内，选项名称和选项值之间使用空格分隔。选项值以第一个非空格的字符开头，并可扩展到行尾字符。选项集之间使用空行分隔。

一般语法为：

```
<option name><white space>[option value, if any]
<option name><white space>[option value, if any]
...
<option name><white space>[option value, if any]
<blank line>
<option name><white space>[option value, if any]
<option name><white space>[option value, if any]
...
<option name><white space>[option value, if any]
```

命令行中给定的选项值将成为每个选项集的默认值。或者，也可以为每个选项集指定这些选项。该值随后将覆盖命令行上指定的任何默认值。

下面是文件的格式和语法 （使用 commadmin user add 命令的 -i 选项指定）示例。

```
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 ...>
```

命令描述

本部分提供了命令行工具的描述、语法和示例。

强制性 commadmin 选项

下面列出了可用于验证管理员或用户的强制性选项。

选项	描述
-D *userid*	用于绑定到目录的用户 ID。
-w *password*	用于验证访问目录的 userID 的密码。 也可以通过文本文件 *password*.txt 来指定 *password*。
-n *domain*	管理员所属的域。

Access Manager 主机 (-x)、 Access Manager 端口 (-p) 以及默认域 (-n) 的值均在安装过程中指定，并存储在 cli-userprefs.properties 文件中。

注 如果在执行 commadmin 命令时未指定 -X、 -p 和 -n 选项，将从 cli-userprefs.properties 文件中获取其值。

commadmin admin add

commadmin admin add 命令将组织管理员权限授予特定域的用户。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 IS Port] [-X IS Host] [-?] [-s] [-v] [-V]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	顶级管理员的用户 ID。
-l *login*	要授予组织管理权限的用户的用户 ID。该用户应存在于目录中，并作为 -d 选项所指定的域的一部分。

选项	描述
-n *domain*	顶级管理员的域。如果未指定此选项，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。如果未指定此选项，则使用 -n 选项指定的域。

以下选项是非强制性的：

选项	描述
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS Port*	使用此选项指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*。
-h, -?	打印命令使用语法。
-V	打印有关实用程序及其版本的信息。
-s	使用安全套接字层 (Secure Socket Layer, SSL) 连接到 Access Manager。
-v	启用调试输出。

示例

以下命令将组织管理员权限授予用户 ID 为 admin1 的用户。

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

以下命令将组织管理员权限授予域 florizel.com 中用户 ID 为 admin2 的用户。

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

commadmin admin remove

commadmin admin remove 命令删除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。

要删除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 IS port] [-X IS host] [-s] [-v] [-V]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	顶级管理员的用户 ID。
-l *login*	需要吊销管理员权限的用户的用户 ID。
-n *domain*	顶级管理员的域。
-w *password*	顶级管理员的密码。
-d *domain name*	要吊销管理员权限的域。如果未指定 -d，则使用 -n 指定的域。

以下选项是非强制性的：

选项	描述
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS Port*	使用此选项指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。

示例

以下命令删除用户 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 命令搜索并显示域的特定或所有组织管理员。

语法

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

选项

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	使用 -D 选项指定的用户的域。
-w *password*	使用 -D 选项指定的用户的密码。

以下选项是非强制性的：

选项	描述
-l *login*	搜索的组织管理员的用户 ID。如果未指定 -l，或使用通配符 (-l* 或 -l '*') 指定了 -l，则会显示域的所有组织管理员。
-d *domain*	搜索对指定域具有组织管理员权限的用户。如果未指定 -d，则使用 -n 指定的域。

示例

搜索 test.com 域的所有组织管理员：

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

commadmin domain create

`commadmin domain create` 命令在 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 IS Port] [-s] [-v] [-V] [-X IS 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

以下选项是强制性的：

选项	描述
`-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*	顶级管理员的域。
`-w` *password*	顶级管理员的密码。

以下选项是非强制性的：

选项	描述
`-A [+ ]`*attributename*:*value*	要修改的属性。 *attributename* 在 LDAP Schema 中定义，指定的 *value* 将替换目录中此属性的所有当前值。要同时修改多个属性或为同一属性指定多个值，请重复使用此选项。 *attributename* 之前的 "+" 表示将值添加到属性的当前列表。 如果未指定操作值 (+)，则默认操作是添加现有值。
`-h, -?`	打印命令使用语法。
`-i` *inputfile*	从文件 （而不是命令行）中读取命令信息。

选项	描述
-o *organization RDN*	为域指定组织 RDN。例如 o=varrius.florizel.com。 如果未指定此选项，则在 osi 后缀下创建该组织，并使用 o= 域名，即 o=osiSuffix。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。
-S *service*	指定要添加到域中的一项或多项服务。 *service* 可具有单项服务或多项服务的值。有效的 *service* 值为 mail 和 cal。这些值不区分大小写。 如果指定了 -S mail 选项，则必须指定 -H 选项。 可以通过以逗号分隔的列表形式列出。 例如： -S mail,cal 在创建域时，将根据 Identity Sever 配置文件中存在的特定服务定义的值，向该域中添加相应的服务。
仅在指定了 -S mail 选项时，才允许使用以下选项：	
-H *preferred mailhost*	域的首选邮件主机。主机必须是全限定主机名，例如 mailhost.sesta.com。 如果指定了 -S mail 选项，则此选项是强制性的。
仅在指定了 -S cal 选项时，才允许使用以下选项：	
-B *backend calendar data server*	指定分配给域中的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访问控制列表 (Access Control List, ACL)。
-P *propertyname*[:*value*]	为多值属性和面向位的属性设置值。要了解属性、属性描述及属性值，请参阅表 B-1 （在第 133 页）。
-R *right*[:*value*]	设置日历域属性 icsAllowRights。该属性由一组位图值组成。要了解属性、属性值及属性描述的列表，请参见表 B-2 （在第 134 页）。

选项	描述
-T *calendar time zone string*	指定在导入文件时所用的时区 ID。 要了解有效时区字符串的列表，请参见“日历时区字符串”（在第 135 页）。

示例

要创建具有邮件和日历服务的新域，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删除，请使用 `-i` 选项。

`commadmin domain purge` 命令将永久删除该域。

要禁止组织管理员使用日历服务或邮件服务之类的服务，请使用 `-S` 选项。此处的 `S` 为大写。

语法

```
commadmin domain delete -D login -d domain name -n domain -w password [-h] [-?]
  [-i inputfile] [-p IS Port] [-s] [-S service] [-v] [-V] [-X IS Host]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	顶级管理员的用户 ID。
-d *domain name*	要删除的 DNS 域名。如果未指定 `-d`，则使用 `-n` 指定的域。
-n *domain*	顶级管理员的域。
-w *password*	顶级管理员的密码。

以下选项是非强制性的：

选项	描述
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装过程中未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-S *service*	将指定服务的状态属性值修改成 "deleted"。 使用逗号来分隔多项服务。有效的 *service* 值为 mail 和 cal。这些值不区分大小写。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。

示例

删除现有域：

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

从 florizel.com 域中仅删除邮件服务：

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

commadmin domain modify

commadmin domain modify 命令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 IS Port] [-s] [-v] [-V]
  [-X IS Host]
  [-S mail -H preferred maillhost]
  [-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

以下选项是强制性的：

选项	描述
-D *login*	顶级管理员的用户 ID。
-d *domain*	要修改的 DNS 域名。如果未指定 -d，则使用 -n 指定的域。
-n *domain*	顶级管理员的域。
-w *password*	顶级管理员的密码。

以下选项是非强制性的：

选项	描述
-A [+ | -]*attributename*:*value*	要修改的属性。*attributename* 在 LDAP Schema 中定义，value 将替换目录中此属性的所有当前值。要同时修改多个属性或为同一属性指定多个值，请重复此选项。 *attributename* 之前的 "+" 表示将值添加到属性的当前列表。 "-" 表示删除该值。 如果使用 "-"，则在命令行上指定命令时，必须在 "-" 前面加上两个反斜杠。如果在输入文件内提供该选项，则必须在 "-" 符号前面加上一个反斜杠。 如果未指定操作值 （+ 或 -），则默认操作是替换现有值。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-v	启用调试输出。

选项	描述
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。
-S *service*	在修改过程中将指定的一项或多项服务添加到域中。 有效的 *service* 值为 mail 和 cal。这些值不区分大小写。 使用 -S 选项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。
在添加服务时，仅在指定了 -S mail 选项时，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，则此选项是强制性的。
在添加服务时，仅在指定了 -S cal 选项时，才允许使用以下选项：	
-B *backend calendar data server*	分配给域中的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访问控制列表 (ACL)。
-P [*action*]*propertyname*[:*value*]	为多值属性和面向位的属性设置值。要了解 *propertyname* 的描述和值，请参见表 B-1 （在第 133 页）。
-T *calendar time zone string*	导入文件时使用的时区 ID。 要了解有效时区字符串的列表，请参见 “日历时区字符串”（在第 135 页）。
-R *propertyname*[:*value*]	设置日历域属性 icsAllowRights。该属性包含位图值。要了解属性名称、属性值及属性描述的列表，请参见表 B-2 （在第 134 页）。

示例

修改现有域：

```
commadmin domain modify -D chris -w bolton -n sesta.com -d varrius.com \
-A preferredmailhost:test.siroe.com
```

commadmin domain purge

commadmin domain purge 命令永久删除标记为删除的所有条目或服务。这可以包括域、用户、组和资源。如果将域标记为删除，则会删除该域内的所有条目和服务，无论它们是否标记为删除。

作为定期维护操作的一部分，应使用 commadmin domain purge 命令删除所有标记为删除的时间超过指定宽限期的条目。

通过手动调用该命令，可以随时执行清除操作。

调用该命令时，将搜索目录并创建域列表，该列表中的条目包括标记为删除的时间超过指定宽限期的域。在安装时，宽限期的默认值最初设置为 10 天。

如果指定了 -d* 选项，则在所有域中搜索标记为删除的用户和域。标记为删除的用户将从域中清除，但不会清除该域，除非它也被标记为删除。如果将域标记为删除，将清除该域以及其中的所有用户。

将服务标记为删除后，必须先运行用于删除资源 （如邮箱或日历）的实用程序，然后才能从目录中清除服务。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，该程序为 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。

语法

```
commadmin domain purge -D login -n domain -w password -d domain [-g grace] [-h]
  [-?] [-i inputfile] [-p IS Port] [-s] [-S service] [-v] [-V] [-X IS Host]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	顶级管理员的用户 ID。
-n *domain*	顶级管理员的域。
-w *password*	顶级管理员的密码。
-d *domain*	清除指定域。可以使用 * 操作符 (-d*) 来搜索模式。

以下选项是非强制性的：

选项	描述
-g *grace*	在清除域之前的宽限期 （单位为天）。不会清除标记为删除的时间少于 *grace* 天的域。 0 表示立即清除。从服务器上的配置文件中读取默认值。在安装时，默认值设置为 10 天。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 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，它会从这些用户和资源的目录中删除特定于服务的数据。 服务列表使用逗号 (,) 分隔符分隔。 有效的 *service* 值为 mail 和 cal。这些值不区分大小写。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。

示例

在下面的示例中，将清除 siroe.com 域，同时删除该域中的所有条目：

```
commadmin domain purge -D chris -d siroe.com -n sesta.com -w bolton
```

commadmin domain search

commadmin domain search 命令获取与单个域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。在此命令中指定 -S 时，仅显示正在使用指定服务的域。

语法

```
commadmin domain search -D login -n domain -w password [-d domain] [-h] [-?]
  [-i inputfile] [-p IS Port] [-s] [-S service] [-t Search Template] [-v] [-V]
  [-X IS Host]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	使用 -D 选项指定的用户的域。
-w *password*	使用 -D 选项指定的用户的密码。

以下选项是非强制性的：

选项	描述
-d *domain*	搜索此域。如果未指定 -d 或指定了 -d*，则显示所有域。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-S *service*	指定要在活动域中搜索的服务。 *service* 可具有单项服务或多项服务的值。有效的 *service* 值为 mail 和 cal。这些值不区分大小写。 服务列表使用逗号 (,) 分隔符分隔。 例如： -S mail,cal
-t *Search template*	指定要使用的搜索模板的名称，而不是默认的搜索模板。在搜索后仅显示活动域。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。

选项	描述
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。

commadmin group create

`commadmin group create` 命令将单个组添加到 Access Manager。要创建多个组，请使用 `-i` 选项。

如果创建了不包含任何成员的组，则默认情况下，该组为静态组。

注 组不能同时包含静态成员和动态成员。

电子邮件群发列表是一种类型的组。在将邮件发送到组地址时， Access Manager 会将邮件发送到该组中的所有成员。

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 IS Port] [-s] [-v] [-V] [-X IS Host]
  [-S service [-H mailhost] [-E email] [-M external-member] [-o owner] [-r moderator]]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	-D 选项指定的用户的域。
-G *groupname*	组的名称 （例如 mktg-list）。
-w *password*	-D 选项指定的用户的密码。

以下选项是非强制性的：

选项	描述
-A [+]*attributename*:*value*	要修改的属性。*attributename* 在 LDAP Schema 中定义，*value* 将替换目录中此属性的所有当前值。要同时修改多个属性或为同一属性指定多个值，请重复此选项。 *attributename* 之前的 "+" 表示将值添加到属性的当前列表。
-d *domain*	组的全限定域名（例如 varrius.com）。默认值为本地域。如果未指定 -d，则使用 -n 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。 可指定多个 -f 命令，以便为组的成员定义多个 LDAP 过滤器。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件（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。 应使用此选项来创建静态组。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-S *service*	指定要添加到组中的服务。 *service* 可具有单项服务或多项服务的值。有效的 service 值为 mail 和 cal。这些值不区分大小写。 服务列表使用逗号 (,) 分隔符分隔。 例如： -S mail,cal
仅在指定了 -S mail 选项时，才允许使用以下选项：	
-H *mailhost*	此组响应的邮件主机（例如 mailhost.varrius.com）。默认值为本地邮件主机。
-E *email*	组的电子邮件地址。

选项	描述
-M *external-member*	添加到此组的外部成员的用户 ID。要添加多个成员，请使用多个 -M 选项。
-o *owner*	组拥有者的电子邮件地址。拥有者是负责群发列表的个人。 拥有者可以添加或删除群发列表成员。
-r *moderator*	仲裁者的电子邮件地址。

示例

在域 sesta.com 中创建组 testgroup：

```
commadmin group create -D chris -n sesta.com -w bolton -G testgroup \
-d sesta.com -m lorca@sesta.com -S mail -M achiko@varrius.com
```

commadmin group delete

commadmin group delete 命令将单个组标记为删除。要将多个组标记为删除，请使用 -i 选项。

要禁止组使用 Calendar Server 或 Messaging Server 等服务，请使用 -S 选项。此处的 S 为大写。

注 要永久删除组，必须运行 commadmin domain purge 命令。

语法

```
commadmin group delete -D login -G groupname -n domain -w password [-d domain]
  [-h] [-?] [-i inputfile] [-p IS Port] [-s] [-S service] [-v] [-V] [-X IS Host]
```

选项

下面是一些强制性选项：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-G *groupname*	要标记为删除的组的名称。例如 mktg-list。

选项	描述
-n *domain*	-D 选项指定的用户的域。
-w *password*	-D 选项指定的用户的密码。

下面是一些非强制性选项：

选项	描述
-d *domain*	组的域。如果未指定 -d，则使用 -n 选项指定的域。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-S *service*	将指定服务的状态属性值修改成 "deleted"。 使用 -S 选项列出的服务以逗号分隔。有效的 *service* 值为 mail 和 cal。这些值不区分大小写。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。

示例

将组 testgroup@varrius.com 标记为删除：

```
commadmin group delete -D chris -n sesta.com -w bolton -G testgroup \
-d varrius.com
```

下面的示例将 testgroup@varrius.com 的邮件服务标记为删除：

```
commadmin group delete -D chris -n sesta.com -w bolton -G testgroup \
-d varrius.com -S mail
```

commadmin group modify

`commadmin group modify` 命令更改 Access Manager 中已存在的单个组的属性。要更改多个组的属性，请使用 `-i` 选项。

邮递列表是一种类型的组。在将邮件发送到组地址时， Access Manager 会将邮件发送到该组中的所有成员。

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 IS Port] [-s] [-v] [-V] [-X IS Host]
  [-S mail [-o owner] [-E email] [-H mailhost] [-M external-member] [-r moderator]]
```

选项

下面是一些强制性选项：

选项	描述
-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`。
-n *domain*	`-D` 选项指定的用户的域。
-w *password*	`-D` 选项指定的用户的密码。

下面是一些非强制性选项：

选项	描述
-A [+ | -]*attributename:value*	要修改的属性。*attributename* 在 LDAP Schema 中定义，value 将替换目录中此属性的所有当前值。要同时修改多个属性或为同一属性指定多个值，请重复此选项。 *attributename* 之前的 "+" 表示将值添加到属性的当前列表。 "-" 表示删除该值。如果使用 "-"，则在命令行上指定命令时，必须在 "-" 前面加上两个反斜杠，或使用引号将其引起来。如果在输入文件内提供该选项，则必须在 "-" 符号前面加上一个反斜杠。
-d *domain*	组的域。如果未指定 `-d`，则使用 `-n` 选项指定的域。

选项	描述
-f [*action*] *ldap-filter*	指明是将 ldap 过滤器添加到组中，还是从组中删除该过滤器。 *ldap-filter* 前面的 "+" 表示将其添加到现有过滤器中。 "-" 表示删除现有过滤器。键入 -f-* 将删除所有过滤器。如果使用 "-"，则在命令行上指定命令时，必须在 "-" 前面加上两个反斜杠，或使用引号将其引起来。 如果未指定 *action*，则默认情况下将添加过滤器 （如果该过滤器不存在）。否则将显示一条错误消息。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （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。 *internal-member* 的值是邮件地址或用户 ID。 *action* 值： + 将成员添加到内部成员的现有列表中。 - 从内部成员的现有列表中删除成员。如果使用 "-"，则在命令行上指定命令时，必须在 "-" 前面加上两个反斜杠，或使用引号将其引起来。 -m-* 删除所有内部成员。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。
-S mail	验证邮件服务是否已存在后，在修改过程中将邮件服务添加到组中。如果该服务存在，将显示一条错误消息。 -S 的唯一有效值为 mail。
仅在指定了 -S mail 选项时，才允许使用以下选项：	
-o *owner*	组拥有者的电子邮件地址。拥有者是负责群发列表的个人。 拥有者可以添加或删除群发列表成员。
-E *email*	组的电子邮件地址。
-H *mailhost*	组的邮件主机。默认值为本地邮件主机。
-M *external -member*	添加外部成员。 *external-member* 的值是用户邮件地址。

选项	描述
-r *moderator*	仲裁者的用户 ID。如果仲裁者位于其他域中，则键入电子邮件地址。 必须使用此选项指定 -S mail 选项。

示例

从域 varrius.com 内的组 testgroup 中删除内部成员 (jsmith)：

```
commadmin group modify -D chris -d varrius.com -G testgroup -n sesta.com \
-w bolton -m \\-jsmith
```

commadmin group search

commadmin group search 命令获取与单个组关联的所有目录属性。要获取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 IS Port] [-s] [-S service] [-t search template]
  [-v] [-V] [-X IS Host]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	-D 选项指定的用户的域。
-w *password*	-D 选项指定的用户的密码。

以下选项是非强制性的：

选项	描述
-d *domain*	要搜索的组的域。如果未指定 -d，则搜索所有域。
-E *string*	组的电子邮件地址。可以在字符串的任何部分使用通配符 (*)。
-G *string*	要搜索的组的名称。例如 mktg-list。如果未指定 -G，则显示 -d 指定的域中的所有组。可以在字符串的任何部分使用通配符 (*)。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-S *service*	指定要搜索的服务。 *service* 的唯一有效值为 mail。此值不区分大小写。 例如： -S mail 仅显示正在使用服务的组。
-t *Search Template*	指定要使用的搜索模板的名称，而不是默认的搜索模板。这是目录中定义搜索过滤器的条目。仅搜索活动组。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。

示例

在 siroe.com 域下搜索名为 developers 的组：

```
commadmin group search -D chris -n sesta.com -w password -G developers \
-d siroe.com
```

commadmin resource create

`commadmin resource create` 命令为资源创建目录条目。

有关创建资源的说明，请参见创建资源。

语法

```
commadmin resource create -D login -n domain -w password -u identifier -N name
  -o owner [-A [+]attributename:value] [-c calendar identifier] [-C DWPHost]
  [-d domainname ] [-h] [-?] [-i inputfile][-p IS Port] [-s] [-T time zone] [-v]
  [-V] [-X IS Host]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	使用 -D 选项指定的用户的域。
-w *password*	使用 -D 选项指定的用户的密码。
-u *identifier*	资源的唯一标识符。 在域名称空间或在日历模式下日历所管理的所有用户和资源中，该 *identifier* 值应该是唯一的。 如果未指定 -c 选项，则将 -u 选项指定的标识符用作日历标识符。
-N *name*	用于在日历 GUI 中显示资源的友好名称。
-o *owner*	资源的拥有者。此用户 ID 必须位于创建资源所在的域之下。

以下选项是非强制性的：

选项	描述
-A [+] *attributename:value*	要修改的属性。*attributename* 在 LDAP Schema 中定义，*value* 将替换目录中此属性的所有当前值。要同时修改多个属性或为同一属性指定多个值，请重复此选项。 *attributename* 之前的 "+" 表示将值添加到属性的当前列表。
-c *calendar identifier*	此资源的日历标识符。 该标识符值在 Calendar Server 管理的所有日历中应该是唯一的。

选项	描述
-C *DWPHost*	存放此用户日历的后端日历服务器的 DNS 名称。 如果未指定后端日历服务器的 DNS 名称，则将该服务器的 ics.conf 文件中存储的值用作默认值。
-d *domain name*	资源的域。如果未指定 -d，则使用 -n 指定的域。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-T *time zone*	用于在日历的用户界面中显示资源日历的时区。 要了解有效时区字符串的列表，请参见 “日历时区字符串”（在第 135 页）。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。

示例

在域 varrius.com 下的日历 cal.siroe.com 中创建名为 peter 的资源：

```
commadmin resource create -D chris -n sesta.com -w bolton -o ownerid \
-d varrius.com -u id -N peter -C cal.siroe.com
```

创建资源

资源由两种数据描述组成：Calendar Server 数据库中的目录条目和日历。该目录条目具有属性 icsCalendar，其值为与资源关联的日历的名称。

可以使用下面任一种方法创建具有两种数据描述的资源：

- 使用可创建目录条目和日历的 csresource 实用程序。

  请注意以下事项：

- 必须在 csresource 中指定与 commadmin resource create 中相同的拥有者。在两个命令中均使用 -o 选项指定拥有者。
- 资源名称的值 （在 csresource 中的 create 命令之后）必须与 commadmin resource create 中 -u 选项所用的值相同。

- 使用 commadmin resource create 创建目录条目，并使用 cscal 实用程序创建日历。例如：

  a. 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 -o test1 -u resourceOne -N firstResource
  ```

  该目录条目如下：

```
dn:uid=resourceONE,ou=People,o=varrius,o=domainroot
uid:resrouceONE
objectClass:icsCalendarResource
objectClass:top
cn:firstResource
icsStatus:active
icsCalendar:test1@varrius.com:resourceOne
```

  b. 使用 cscal 创建日历：

  ```
  cscal -D varrius.com -o test1 -n firstResource create resourceOne
  ```

  cscal 列表中的日历描述为：

  ```
  test1@varrius.com:resourceOne:owner=test1@varrius.com status=enabled
  ```

现在，您可以作为任何用户进行登录，并邀请资源加入事件。

有关 csresource 和 cscal 实用程序的详细描述，请参见 Sun Java System Calendar Server 管理指南中的 “Calendar Server 命令行实用程序”。

commadmin resource delete

commadmin resource delete 命令将资源标记为删除。

注 要永久删除资源，请运行 commadmin domain purge 命令。

语法

```
commadmin resource delete -D login -u identifier -n domain -w password [-d domainname]
  [-h] [-?] [-i inputfile] [-p IS Port] [-s] [-v] [-V] [-X IS Host]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	使用 -D 选项指定的用户的域。
-w *password*	使用 -D 选项指定的用户的密码。
-u *identifier*	资源的唯一标识符

以下选项是非强制性的：

选项	描述
-d *domainname*	资源的域。如果未指定 -d，则使用 -n 指定的域。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。

示例

将资源标记为删除：

```
commadmin resource delete -D chris -n sesta.com -w bolton -u bill023
```

commadmin resource modify

`commadmin resource modify` 命令可用于修改资源。

语法

```
commadmin resource modify -D login -n domain -w password -u identifier
  [-A [+|-]attributename:value] [-d domainname ] [-h] [-?] [-i inputfile]
  [-N name] [-p IS Port] [-s] [-T time zone] [-v] [-V] [-X IS Host]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	使用 -D 选项指定的用户的域。
-w *password*	使用 -D 选项指定的用户的密码。
-u *identifier*	资源的唯一标识符。

以下选项是非强制性的：

选项	描述
-A [+ | -]*attributename*:*value*	要修改的属性。*attributename* 在 LDAP Schema 中定义，value 将替换目录中此属性的所有当前值。要同时修改多个属性或为同一属性指定多个值，请重复此选项。 *attributename* 之前的 "+" 表示将值添加到属性的当前列表。 "-" 表示删除该值。 如果使用 "-"，则在命令行上指定命令时，必须在 "-" 前面加上两个反斜杠。如果在输入文件内提供该选项，则必须在 "-" 符号前面加上一个反斜杠。

选项	描述
-d *domainname*	资源的域。如果未指定 -d，则使用 -n 指定的域。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-N *name*	用于在日历用户界面中显示资源的通用名称。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-T *time zone*	用于在日历 GUI 中显示资源日历的时区。 要了解有效时区字符串的列表，请参见 “日历时区字符串”（在第 135 页）。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。

示例

使用新的通用名称 bjones 修改具有唯一标识符 bill023 的资源：

```
commadmin resource modify -D chris -n sesta.com -w bolton -d test.com \
-u bill023 -N bjones
```

commadmin resource search

commadmin resource search 命令可用于搜索资源。

语法

```
commadmin resource search -D login -n domain -w password [-d domain] [-h] [-?]
  [-i inputfile] [-N string] [-p IS Port] [-s] [-t Search Template] [-u string] [-V] [-v]
  [-X IS Host]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	使用 -D 选项指定的用户的域。
-w *password*	使用 -D 选项指定的用户的密码。

以下选项是非强制性的：

选项	描述
-d *domain*	资源的域。仅在该域中执行搜索。如果未指定 -d 或指定了 -d*，则搜索所有域。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-N *string*	输入资源的通用名称。可以在字符串的任何部分使用通配符 (*)。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-t *Search Template*	指定要使用的搜索模板的名称，而不是默认的搜索模板。这是目录中定义搜索过滤器的条目。仅搜索活动资源。
-u *string*	指定的资源标识符对于域名称空间或日历管理的所有用户和资源来说必须是唯一的。 可以在字符串的任何部分使用通配符 (*)。 如果未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。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。

示例

在域 sesta.com 中搜索资源 arabella：

```
commadmin resource search -D serviceadmin -w serviceadmin -n sesta.com \
-d sesta.com -u arabella
```

commadmin user create

commadmin user create 命令在 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 IS Port] [-s] [-v] [-V] [-X IS Host]
  [-S mail [-E email] [-H mailhost]]
  [-S cal [-B DWPHost] [-E email] [-k calid_type] [-J First Daylof Week] [-T time zone]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-F *firstname*	用户的名字；必须是不包含空格的单个词。
-n *domain*	使用 -D 选项指定的用户的域。
-l *userid*	用户的登录名。
-w *password*	使用 -D 选项指定的用户的密码。
-W *password*	所创建的用户的密码。 也可以通过文本文件 *password*.txt 来指定 *password*。
-L *lastname*	用户的姓氏。

以下选项是非强制性的：

选项	描述
-A [+]*attributename*:*value*	要修改的属性。*attributename* 在 LDAP Schema 中定义，*value* 将替换目录中此属性的所有当前值。要同时修改多个属性或为同一属性指定多个值，请重复此选项。 *attributename* 之前的 "+" 表示将值添加到属性的当前列表。
-d *domain*	用户的域。如果未指定 -d，则使用 -n 指定的域。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-I *initial*	用户中间名的首字母。
-h, -?	打印命令使用语法。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。
-S *service*	在创建期间将指定服务添加到用户。*service* 可以具有单项服务或多项服务的值。有效的 *service* 值为 mail 和 cal。这些值不区分大小写。 服务列表使用逗号 (,) 分隔符分隔。 例如： -S mail,cal
仅在指定了 -S mail 选项时，才允许使用以下选项：	
-E *email*	用户的电子邮件地址。
-H *mailhost*	用户的邮件主机。
仅在指定了 -S cal 选项时，才允许使用以下选项：	
-B *DWPHost*	存放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*	在日历服务器用户界面中显示日历时，将显示该周的第一天。有效值为 0-6 （0 为星期日、 1 为星期一，以此类推）。

选项	描述
-k *calid_type*	指定所创建的日历 ID 的类型。可接受的值为 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 加上域 （例如 jsmith@sesta.com）。 如果未指定 -k 选项，则默认设置是使用日历 ID 加上域 (hosted)。 如果未指定 -k 选项，则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 文件中： 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。 要了解有效时区字符串的列表，请参见 “日历时区字符串”（在第 135 页）。

示例

要创建新的用户 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 命令将单个用户标记为删除。要将多个用户标记为删除，请使用 -i 选项。

不存在取消删除实用程序。但是，可以在到达清除宽限期并将清除设置为针对条目运行之前，使用 ldapmodify 命令随时将用户条目的状态属性更改为 active。

删除用户的过程包括三个步骤：

1. 通过运行 commadmin user delete 命令将用户标记为删除。

2. 从用户删除资源。

   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，该程序为 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 commadmin domain purge 命令，可以永久删除用户。

语法

```
commadmin user delete -D login -n domain -l login name -w password [-d domain]
  [-h] [-?] [-i inputfile] [-p IS Port] [-s] [-S service] [-v] [-V] [-X IS Host]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	使用 -D 选项指定的用户的域。
-w *password*	使用 -D 选项指定的用户的密码。
-l *userid*	要删除的用户的用户 ID。

以下选项是非强制性的：

选项	描述
-d *domain*	用户的域。如果未指定 -d，则使用 -n 指定的域。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。

选项	描述
-S *service*	指定要从用户删除的服务。该用户将保持活动状态，但仅取消激活指定的服务。如果未指定 -S，则删除该用户。 *service* 可具有单项服务或多项服务的值。有效的 *service* 值为 mail 和 cal。这些值不区分大小写。 服务列表使用逗号 (,) 分隔符分隔。 例如： -S mail,cal
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。

示例

将现有用户标记为删除：

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith
```

仅从用户 smith 删除邮件服务：

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith -S mail
```

commadmin user modify

commadmin user modify 命令修改单个用户目录条目的属性。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 IS Port] [-s]
  [-v] [-V] [-X IS 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

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	使用 -D 选项指定的用户的域。
-w *password*	使用 -D 选项指定的用户的密码。
-l *userid*	用户的登录 ID。

以下选项是非强制性的：

选项	描述
-A [+ | -]*attributename*:*value*	要修改的属性。*attributename* 在 LDAP Schema 中定义，value 将替换目录中此属性的所有当前值。可以重复此选项，以便同时修改多个属性或为同一属性指定多个值。 *attributename* 之前的 "+" 表示将值添加到属性的当前列表。 "-" 表示删除该值。 如果使用 "-"，则在命令行上指定命令时，必须在 "-" 前面加上两个反斜杠。如果在输入文件内提供该选项，则必须在 "-" 符号前面加上一个反斜杠。
-d *domain*	用户或组的域。如果未指定 -d，则使用 -n 指定的域。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-p *IS Port*	指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-v	启用调试输出。

选项	描述
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。
-S *service*	验证用户是否拥有 -S 选项指定的服务后，将指定服务添加到用户。如果用户已拥有该服务，将会显示一条错误消息。 *services* 可以具有单项服务或多项服务的值。有效的 *service* 值为 mail 和 cal。这些值不区分大小写。 服务列表使用逗号 (,) 分隔符分隔。 例如： -S mail,cal
仅在指定了 -S mail 选项时，才允许使用以下选项：	
-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，则此选项是强制性的。
仅在指定了 -S cal 选项时，才允许使用以下选项：	
-B *DWPHost*	指定存放此用户日历的后端日历服务器的 DNS 名称。 注：此属性只能添加，而不能修改 （如果它已经存在）。
-E *email*	指定日历用户的电子邮件地址。
-J *First Day of Week*	在日历服务器用户界面中显示日历时，将显示该周的第一天。有效值为 0-6 （0 为星期日、 1 为星期一，以此类推）。
-k *calid_type*	指定所创建 （在添加日历服务时）的日历 ID 的类型。可接受的值为 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 加上域 （例如 jsmith@sesta.com）。 如果未指定 -k 选项，则默认设置是使用日历 ID 加上域 (hosted)。 如果未指定 -k 选项，则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 文件中： switch-caltype=*value* 其中 *value* 为 "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*	将在此时区中显示用户的日历。 要了解有效时区字符串的列表，请参见 “日历时区字符串”（在第 135 页）。

示例

下面的示例将为用户 smith 添加邮件服务：

```
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，将为用户 smith 添加邮件转发地址：

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith \
-A +mailforwardingaddress:tsmith@siroe.com
```

commadmin user search

commadmin user search 命令获取与单个用户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。搜索后仅显示活动用户。

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 IS Port] [-s]
  [-S service] [-t Search Template] [-v] [-V] [-X IS Host]
```

选项

以下选项是强制性的：

选项	描述
-D *login*	有权执行此命令的用户的用户 ID。
-n *domain*	使用 -D 选项指定的用户的域。
-w *password*	使用 -D 选项指定的用户的密码。

以下选项是非强制性的：

选项	描述
-d *domain*	用户的域。仅在指定域中搜索用户。 如果未指定 -d，则考虑搜索所有域。
-E *string*	搜索用户的邮件地址。可以在字符串的任何部分使用通配符 (*)。
-F *string*	搜索用户的名字。可以在字符串的任何部分使用通配符 (*)。
-h, -?	打印命令使用语法。
-i *inputfile*	从文件 （而不是命令行）中读取命令信息。
-L *string*	搜索用户的姓氏。可以在字符串的任何部分使用通配符 (*)。
-l *string*	搜索用户的登录名。可以在字符串的任何部分使用通配符 (*)。
-p *IS Port*	使用此选项指定 Access Manager 正在侦听的备用 TCP 端口。如果未指定此选项，则使用默认的 *IS Port*，或者，如果在安装时未配置默认值，则使用 Port 80。
-s	使用安全套接字层 (SSL) 连接到 Access Manager。
-S *service*	指定在用户搜索中要匹配的服务。 *services* 可以具有单项服务或多项服务的值。有效的 *service* 值为 mail 和 cal。这些值不区分大小写。 服务列表使用逗号 (,) 分隔符分隔。 例如： -S mail,cal
-t *Search template*	指定要使用的搜索模板的名称，而不是默认的搜索模板。这是目录中定义搜索过滤器的条目。仅搜索活动用户。
-v	启用调试输出。
-V	打印有关实用程序及其版本的信息。
-X *IS Host*	指定运行 Access Manager 的主机。如果未指定此选项，则使用默认的 *IS Host*，或者，如果在安装时未配置默认值，则使用 localhost。

示例

下面的示例将在 varrius.com 域中搜索用户：

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

服务提供商管理员和服务提供商组织

Delegated Administrator 控制台提供了新的管理员角色 （服务提供商管理员 (Service Provider Administrator, SPA)）以及可以在目录中创建的新的组织类型。

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和新的组织类型，并说明了如何在 Delegated Administrator 中创建它们。

服务提供商管理员

Delegated Administrator 控制台允许您将管理任务委托给新的角色，即服务提供商管理员 (SPA)，该角色可以创建和管理新类型的从属组织。

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

通过 SPA，可以创建三层管理结构，如第 1 章 “Delegated Administrator 概述” 的三层结构中所述。

第二级委托可以简化对大型 LDAP 目录所支持的大客户群的管理。例如， ISP 可以为数百或数千家小型企业提供服务，其中每家企业都要求拥有自身的组织。每天都可能会有许多组织添加到该目录中。

如果您使用的是双层结构，则 TLA 必须创建所有这些新组织。现在， TLA 便可以将这些任务委托给 SPA。

SPA 可以为新客户创建从属组织，并指定 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

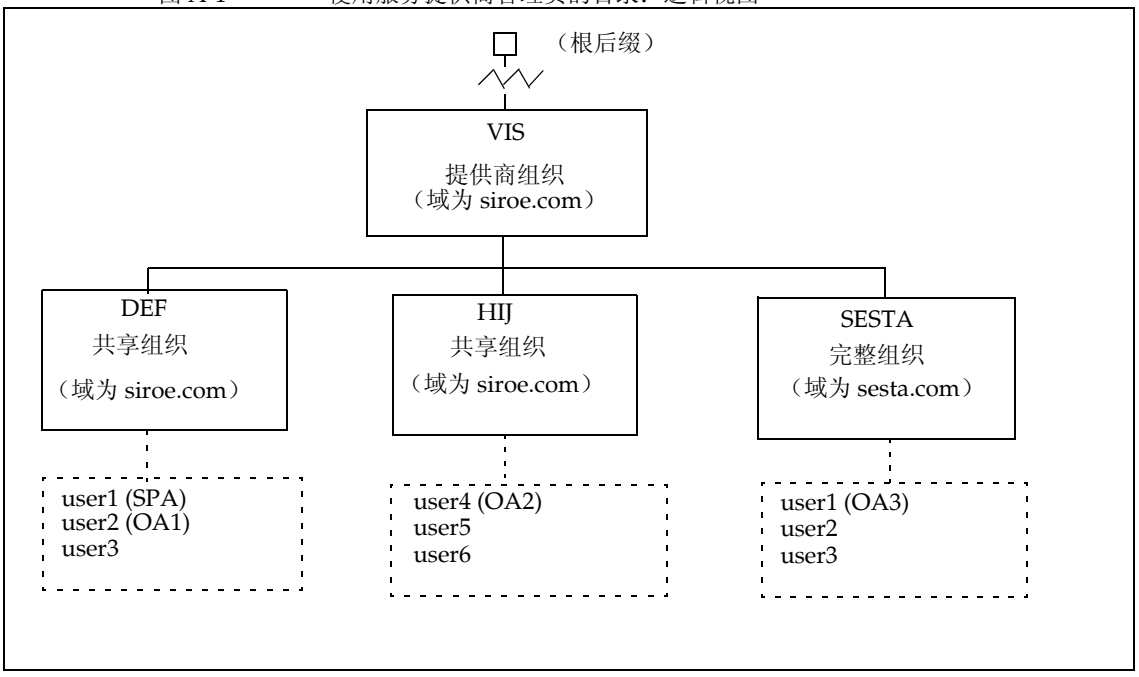


图 A-1 中的示例显示了一个提供商组织。但是，一个目录可以包含多个提供商组织。

在此示例中，管理任务的委托情况如下：

- SPA 具有管理 VIS 提供商组织及其下面所有组织的权限。将 SPA 角色分配给 DEF 组织中的 `user1`。
- 名为 OA1 的组织管理员可以管理共享组织 DEF。将此 OA 角色分配给 DEF 组织中的 `user2`。
- OA2 可以管理共享组织 HIJ。将此 OA 角色分配给 HIJ 组织中的 `user4`。
- OA3 可以管理完整组织 SESTA。将此 OA 角色分配给 SESTA 组织中的 `user1`。

SESTA 是一个完整组织，并具有自身的唯一名称空间。SESTA （在 sesta.com 域中）中的 user1 具有唯一的用户 ID。

有关提供商和从属组织的定义，请参见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 具有管理权限的提供商组织中创建、删除和修改共享组织及完整组织。

  在图 A-1 所示的示例中， 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何组织中创建、删除和修改用户。
- 将 OA 角色分配给用户。

  例如，在图 A-1 所示的样例组织中，SPA 可以将 OA 角色分配给 SESTA 组织中的 user2。然后， user2 便可以管理 SESTA 组织中的用户。

  SPA 还可以删除用户的 OA 角色。
- 将 SPA 角色分配给提供商组织下的其他合法用户 （以及删除 SPA 角色）。
- 将服务等级软件包分配给组织。

  有关服务等级软件包的信息，请参见第 1 章 “Delegated Administrator 概述” 中的服务软件包。

  SPA 可以将指定类型的服务等级软件包分配给组织，并确定可以在该组织中使用的每个软件包的最大数量。

  例如， SPA 可以分配以下服务等级软件包：

  - 在 DEF 组织中：

    ```
    1,000 个 Gold 软件包
       500 个 Platinum 软件包
    ```

  - 在 HIJ 组织中：

    ```
    2,500 个 Topaz 软件包
       500 个 Platinum 软件包
       500 个 Emerald 软件包
    1,000 个 Ruby 软件包
    ```

- 在 SESTA 组织中：

  ```
  2,000 个 Silver 软件包
  1,500 个 Gold 软件包
     100 个 Platinum 软件包
  ```

SPA 可以使用 Delegated Administrator 控制台来执行这些任务。在此版本中，Delegated Administrator 实用程序不包括用于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。 TLA 还可以管理这些组织中的用户。

TLA 可以删除用户的 SPA 角色，但无法通过控制台来分配 SPA 角色。有关此版本 Delegated Administrator 中的约束列表，请参见此版本的注意事项。

有关 TLA 执行的管理任务的完整描述，请参见第 1 章 “Delegated Administrator 概述”中的管理员角色和目录分层结构。

将 SPA 角色分配给用户

必须将 SPA 角色分配给如下组织中的用户：该组织被指定为包含 SPA，并且从属于 SPA 将要管理的提供商组织。

在图 A-1 所示的示例中，假设您需要为名为 VIS 的提供商组织创建 SPA。您可以将 SPA 角色分配给组织 DEF 中的 `user1`。

SPA 必须在从属组织中，因为提供商组织节点不包含任何用户。

因此，必须在提供商组织下至少创建一个组织后， SPA 才能管理提供商组织。应指定此组织包含分配了 SPA 角色的用户。有关详细信息，请参见本附录后面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上述任务的说明，请参见本附录后面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、修改和删除以下类型的组织，这些组织从属于 SPA 的提供商组织：

- 完整组织
- 共享组织

以下部分将介绍提供商组织、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，在逻辑意义上包含完整组织和共享组织。提供商组织节点具有允许 SPA 管理从属组织的属性。

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样例服务提供商组织数据。

提供商组织不能包含用户条目。但可以在提供商组织下创建的组织中置备用户。

提供商组织存储与在其下创建的组织有关的目录信息。例如：

- 提供商组织能否包含共享组织、完整组织，或同时包含这两者
- 在此提供商组织下创建的共享组织可以使用的域名
- 在此提供商组织下创建的组织可以使用的服务等级软件包的类型和数量
- 被指定为包含提供商组织的 SPA 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 所示的示例中， `user2` 属于 `sesta.com` 域，并具有邮件地址 `user2@sesta.com`。
- 完整组织具有自身的域，任何其他组织都无法共享该域，并且它还具有自身的唯一名称空间。

  在图 A-1 所示的示例中，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 所示的示例中， user5 属于 siroe.com 域，并具有邮件地址 user5@siroe.com。
- 它使用了由提供商组织提供的列表中的一个或多个共享域名。

  在图 A-1 所示的示例中，共享组织 DEF 使用域名 siroe.com。
- 其他共享组织可以共享此组织使用的域名。

  在图 A-1 所示的示例中， DEF 与 HIJ 组织均属于 siroe.com 域。
- 共享组织没有唯一的名称空间。

创建提供商组织和服务提供商管理员

在此版本的 Delegated Administrator 中，您必须使用 Delegated Administrator 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 您还可以在运行 Delegated Administrator 配置程序时，将样例提供商组织 （及其从属组织）和样例 SPA 安装在您的目录中。可以通过在配置程序中选择 “加载样例组织” (Load sample service packages) 来执行此操作。

但是，样例组织模板 (da.sample.data.ldif) 将被用作示例，而不是用作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样例服务提供商组织数据。

创建了提供商组织和 SPA 后， SPA 即可登录到 Delegated Administrator 控制台中，创建和管理从属组织，并将 SPA 角色分配给 SPA 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以及管理该组织的 SPA，应再次使用自定义服务提供商模板。

本部分包含以下主题：

- 模板创建的条目提供了在目录中安装模板的编辑副本时所创建的组织示例。
- 创建提供商组织、从属组织和 SPA 时所需的信息定义了创建提供商组织、从属共享组织和 SPA 时所需的模板中的参数。
- 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将信息安装在您的目录中。
- 自定义服务提供商模板是一个模板列表。

模板创建的条目

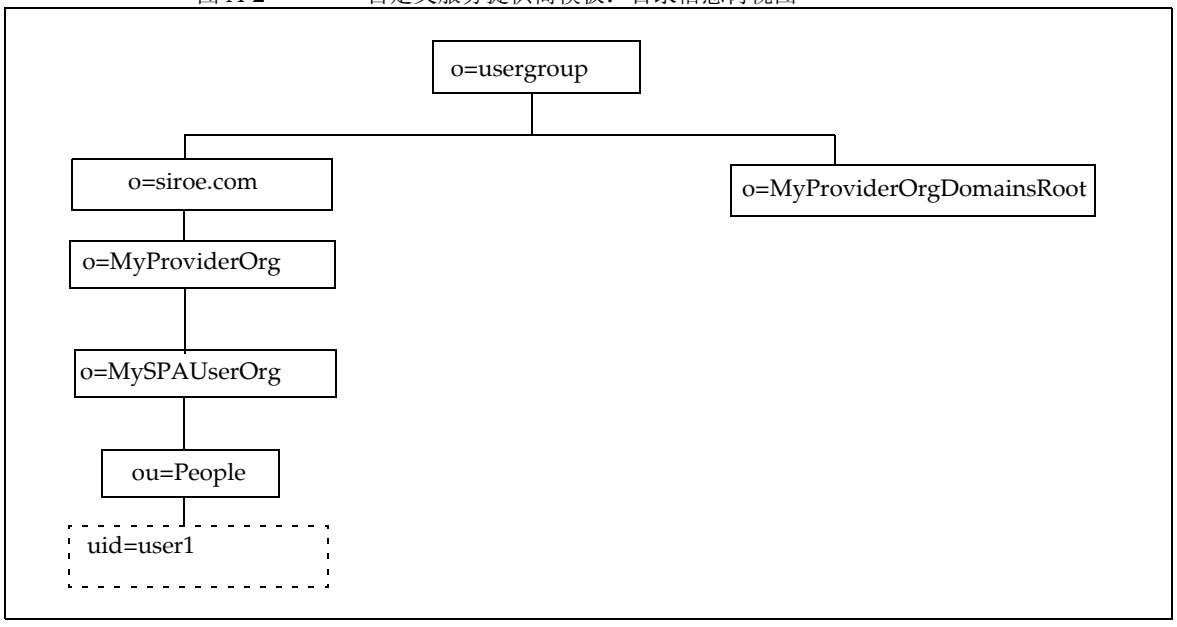
在目录中安装自定义服务提供商模板的编辑副本时，将创建以下条目：

- 提供商组织
- 被指定为包含 SPA 用户的从属共享组织
- 从属组织中分配了 SPA 角色的一个用户
- 可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 进行管理。

图 A-2 显示了安装模板时所创建的条目的示例。它是组织的目录信息树 (Directory Information Tree, DIT) 视图。

图 A-2 只是一个示例。您的组织名称、SPA 用户名和 DIT 结构应特定于您自己的安装。

图 A-2 自定义服务提供商模板：目录信息树视图



安装的自定义服务提供商模板样例中的节点

图 A-2 所示的示例中的节点如下：

- `o=usergroup` — 用户 / 组数据的根后缀。
- `o=siroe.com` — 提供商组织使用的邮件域。
- `o=MyProviderOrg` — 提供商组织节点。
- `o=MySPAUserOrg` — 被指定为包含提供商组织用户 （包括分配了 SPA 角色的用户）的从属共享组织。
- `ou=people` — 用于包含用户的标准 LDAP 组织。
- `uid=user1` — MySPAUserOrg 组织中指定为 SPA 的用户的 UID。
- `o=MyProviderOrgDomainsRoot` — 包含完整组织 （从属于 MyProviderOrg 提供商组织）的占位符节点。

创建提供商组织、从属组织和 SPA 时所需的信息

要创建提供商组织、一个从属组织和 SPA，您需要使用特定于您的安装的信息来替换自定义服务提供商模板中的参数。

在阅读这些参数时，您可以查看自定义服务提供商模板中所示的 `da.provider.skeleton.ldif` 的列表。或者打开位于以下目录中的实际 ldif 文件：

da_base`/lib/config-templates`

有关与这些参数关联的属性的定义，请参见 《Sun Java System Communications Services Schema Reference》中的第 5 章 "Classes and Attributes Used by Communications Services Delegated Administrator (Schema 2)" 和第 3 章 "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*

  用下划线 (_) 替换了所有逗号 (,) 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。将为提供商组织所在的目录节点赋予此名称。

  此参数在 da.provider.skeleton.ldif 模板中使用了多次。

  示例：

  sunProviderOrgDN:o=MyProviderOrg,o=siroe.com,o=usergroup

  o=MyProviderOrg

  sunBusinessOrgBase:o=MyProviderOrgdomainsroot, o=usergroup

- *servicepackage*

  可为用户 （包含在从属于提供商组织的组织中）分配的服务软件包的名称。这是一个多值参数。

  在 da.provider.skeleton.ldif 文件的 "Provider Organization" 部分，您将看到以下属性：

  sunIncludeServices:<servicepackage>

  对于要在提供商组织中包含的每个服务软件包，请添加 sunIncludeServices 属性和 *servicepackage* 参数的一个实例。只有在此处列出的这些服务软件包才能分配给从属组织中的用户。

  示例：

  sunIncludeServices:gold
  sunIncludeServices:platinum
  sunIncludeServices:ruby
  sunIncludeServices:silver

  如果未使用 sunIncludeServices 属性 （删除了包含 *servicepackage* 参数的行），则可以分配目录中的所有服务软件包。

- *domain_name*

  可为提供商组织中的从属组织分配的域名。这是一个多值参数。

  在 da.provider.skeleton.ldif 文件的 "Provider Organization" 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 属性中所列名称的子集 （部分或全部）。（邮件域是在其下创建此提供商组织的组织。）

对于要在提供商组织中包含的每个域名，请添加 sunAssignableDomains 属性和 *domain_name* 参数的一个实例。只有在此处列出的域名才能分配给从属组织。

示例：

```
sunAssignableDomains:siroe.com
sunAssignableDomains:siroe.net
sunAssignableDomains:varrius.com
sunAssignableDomains:sesta.com
sunAssignableDomains:sesta.net
```

- *provider_sub_org*

  SPA 用户所在的共享组织的名称。当您将编辑过的 ldif 信息安装在目录中时，此组织将作为共享组织创建，并从属于提供商组织。它将被指定为包含 SPA 用户的组织。分配了此提供商组织的 SPA 角色的其他用户必须在此从属共享组织中。

  在 da.provider.skeleton.ldif 文件的 "Provider Organization" 部分，您将看到以下属性：

  ```
  sunProviderOrgDN:
  o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
  ```

  sunProviderOrgDN 属性标识被指定为包含提供商组织用户 （特别是 SPA 用户）的组织。

  示例：

  ```
  sunProviderOrgDN:
  o=MySPAUserOrg,o=MyProviderOrg,o=siroe.com,o=usergroup
  ```

- *preferredmailhost*

  提供商组织从属组织 （SPA 用户所在的组织）的首选邮件主机名。必须使用全限定域名 (FQDN)。

  在 da.provider.skeleton.ldif 文件的 "Shared Subordinate Organization" 部分，您将看到以下属性：

  ```
  preferredMailHost:<preferredmailhost>
  ```

  示例：

  ```
  preferredMailHost:mail.siroe.com
  ```

- *available_domain_name*

  可为特定从属组织中的用户分配的域名。这是一个多值参数。

available_domain_name 的值是为 sunAssignableDomains: <domain_name> 属性和参数提供的值的相应子集。但 *domain_name* 应用于整个提供商组织，*available_domain_name* 应用于单个从属组织。

在 da.provider.skeleton.ldif 文件的 "Shared Subordinate Organization" 部分，您将看到以下属性：

```
sunAvailableDomainNames:<available_domain_name>
```

对于希望此从属组织继承 （从提供商组织的 sunAssignableDomains 属性中的域名列表）的每个域名，请添加 sunAvailableDomains 属性和 *available_domain_name* 参数的一个实例。只有在此处列出的域名才能分配给从属组织。

示例：

```
sunAvailableDomainNames:siroe.com
sunAvailableDomainNames:siroe.net
sunAvailableDomainNames:varrius.com
```

- *available_services*

  可用于特定从属组织的服务软件包。这是一个多值参数。

  为从属组织分配的服务软件包是为具有 sunIncludeServices 属性的整个提供商组织分配的服务软件包的子集。

  在 da.provider.skeleton.ldif 文件的 "Shared Subordinate Organization" 部分，您将看到以下属性：

  ```
  sunAvailableServices:<available_services>
  ```

  available_services 参数的格式为

  Service package name:count

  其中 *count* 是一个整数。如果没有该数值，则默认值为无限制的数字。

  对于希望此从属组织继承 （从提供商组织的 sunIncludeServices 属性中的服务软件包）的每个服务软件包，请添加 sunAvailableServices 属性和 *available_services* 参数的一个实例。

  示例：

  ```
  sunAvailableServices:gold:1500
  sunAvailableServices:platinum:2000
  sunAvailableServices:silver:5000
  ```

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 用户的姓氏。

  示例：

  `sn:Smith`

- *spa_servicepackage*

  分配给 SPA 用户的服务软件包。有关服务软件包的信息，请参见第 1 章“Delegated Administrator 概述”中的服务软件包。

  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* 参数的一个域值。也就是说，它必须是可以在 SPA 用户所在的从属组织中使用的域。有关详细信息，请参见 `available_domain_name`。

  示例：

  `mail:user1@siroe.com`

有关如何编辑自定义服务提供商模板以及将信息安装在目录中的说明，请参见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

要创建提供商组织和服务提供商管理员，请执行以下步骤：

1. 在目录中创建邮件域。

   如果您尚未在目录中创建邮件域，请执行此操作。提供商组织及其从属共享组织将使用此邮件域。

2. 复制并重命名 `da.provider.skeleton.ldif` 文件。

   在安装 Delegated Administrator 时，会将 `da.provider.skeleton.ldif` 文件安装在以下目录中：

   da_base`/lib/config-templates`

3. 在 `da.provider.skeleton.ldif` 文件的副本中编辑以下参数。请使用适用于您的安装的正确值替换这些参数。

   有关参数的定义，请参见创建提供商组织、从属组织和 SPA 时所需的信息。

   某些参数在 ldif 文件中使用了多次。您必须搜索和替换每个参数的所有实例。

   有几个参数表示多值属性的值。您可以复制和编辑这些参数及其关联属性名，以便在 ldif 文件中使用这些属性的多个实例。下面对多值参数进行了标注。

   - `<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>

有关与这些参数关联的属性的定义，请参见 《Sun Java System Communications Services Schema Reference》中的第 5 章 "Classes and Attributes Used by Communications Services Delegated Administrator (Schema 2)" 和第 3 章 "Attributes"。

4. 使用 LDAP 目录工具 ldapmodify 将提供商组织和 SPA 安装在目录中。

   例如，您可以运行以下命令：

   ```
   ldapmodify -D <directory manager> -w <password>
   -f <da.provider.finished.ldif>
   ```

   其中

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

   <password> 是 Directory Service 管理员的密码。

   <da.provider.finished.ldif> 是编辑过的 ldif 文件的名称，该文件要作为新的提供商组织和 SPA 安装在目录中。

自定义服务提供商模板

模板 (da.provider.skeleton.ldif) 包含创建新的提供商组织和 SPA 时必须修改的参数。

以下列表显示了 ldif 文件中包含参数的部分。该列表不包括整个文件。此处不包括支持 Access Manager 所需的条目和 ACI。

您只应修改 ldif 文件中的参数。请不要修改与 Access Manager 有关的文件部分。

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 users who is the Provider Administrator.
#
dn:o=<provider_sub_org>,o=<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>
```

样例服务提供商组织数据

运行 Delegated Administrator 配置程序 `config-commda` 时，您可以选择将样例组织数据 （在 ldif 文件中定义）安装在您的目录中。（运行配置程序时，请在**服务软件包和组织样例 (Service Package and Organization Samples)** 面板中选择**加载样例组织 (Load sample service packages)**。）配置程序将 `da.sample.data.ldif` 文件添加到 LDAP 目录树中。

此 ldif 文件将被用作示例，而不是用作创建您自己的提供商组织的模板。要创建新的提供商组织，请参见创建提供商组织、从属组织和 SPA 时所需的信息。

样例数据提供的组织

图 A-1 显示了示例 ldif 文件提供的组织结构的逻辑视图。（图 A-1 添加的共享组织 HIJ 在该文件中不存在。）

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 进行管理：
  - 完整组织 SESTA。 SESTA 组织具有自身的域 `sesta.com`。
  - 共享组织 DEF。 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
- ESG 提供商组织的 SPA
- SESTA 组织的 OA
- DEF 组织的 OA

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 (DIT) 与图 A-1 所示的逻辑视图看上去并非完全一样。组织在 DIT 中实现的分层结构稍有不同。

例如，在 DIT 中，完整域必须直接位于根后缀的下方。因此，应该在根后缀下添加域节点，以存储共享域（供共享组织使用）和完整组织（具有自身的域）的 LDAP 信息。

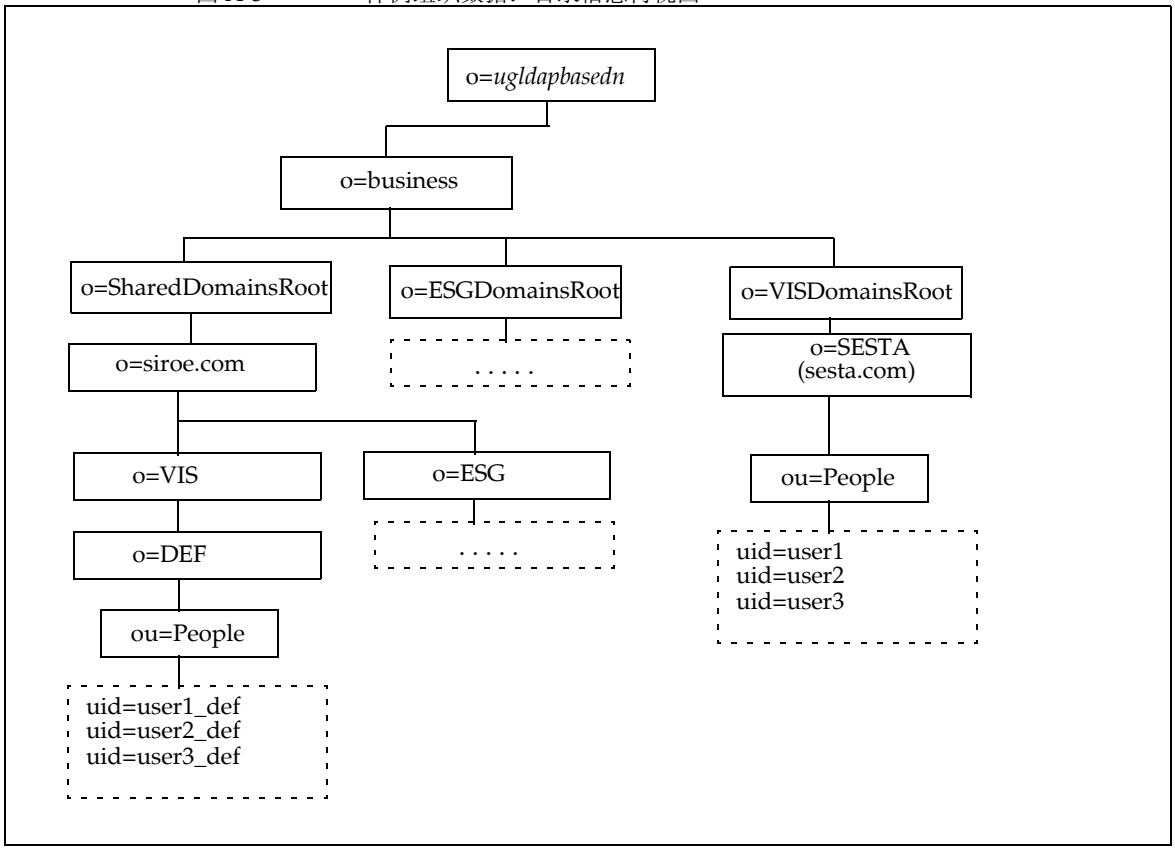
样例组织数据：目录信息树视图

图 A-3 显示了样例组织数据的目录信息树 (DIT) 视图。

与图 A-1 所示的逻辑视图一样，图 A-3 所示的示例包含以下组织：

- VIS 和 ESG（提供商组织）
- 从属于 VIS 提供商组织的共享组织 DEF
- 从属于 VIS 提供商组织的完整组织 SESTA

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 — 包含目录中所有企业的节点。
- o=SharedDomainsRoot — 用于包含共享组织所用域的节点。

  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相同的共享域。由于这两个提供商组织在 SharedDomainsRoot 节点下都包含节点，因此可以实现这一点。

- o=ESGDomainsRoot 和 o=VISDomainsRoot — 这些节点包含从属于 ESG 和 VIS 提供商组织的任何完整组织。

  管理完整组织的每个提供商组织都必须在此级别上 （在根后缀下）具有一个节点。

  在 ESGDomainsRoot 或 VISDomainsRoot 下可以存在多个完整组织 （每个组织都有自身的域）。

- o=siroe.com — 共享域。供共享组织 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 提供商组织的任何共享组织。

  例如，共享组织 DEF 从属于 VIS 提供商组织。

- o=SESTA — 完整组织。它具有自身的域 sesta.com。
- o=DEF — 共享组织。它使用域 siroe.com。
- ou=people — 用于包含用户的标准 LDAP 组织。

样例目录信息树中的用户 DN

图 A-3 所示的样例组织文件中的某些用户 DN 如下：

- 对于属于 DEF 组织且名为 user1_def 的用户：

  dn:uid=user1_def,ou=People,o=DEF,o=VIS,o=siroe.com,
  o=SharedDomainsRoot,o=Business,*ugldapbasedn*

- 对于属于 SESTA 组织且名为 user1 的用户：

  dn:uid=user1,ou=People,o=SESTA,o=VISDomainsRoot,
  o=Business,*ugldapbasedn*

属性值和日历时区

属性值

表 B-1 中列出的属性可以与以下命令的 -P 选项一起使用：commadmin domain create 和 commadmin domain modify。这些属性是面向位的属性或多值属性。

表 B-1 -P 选项的属性

属性	值	描述
createLowerCase	yes/no	指定是否为新用户创建小写日历，以及在查找日历时，是否查找小写日历。
filterPrivateEvents	yes/no	指定在查询服务器时是否过滤私有或机密事件。
fbIncludeDefCal	yes/no	指定用户的 freebusy-calendar-list 中是否包括用户的默认日历。
subIncludeDefCal	yes/no	指定用户的 subscribed-calendar-list 中是否包括用户的默认日历。
resourceDefaultAcl	yes/no	指定是否对资源日历使用默认 ACL。
calmasterCred	字符串	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 管理员能否覆盖访问控制。
setPublicRead	yes/no	将默认用户日历设置为公共读取或私人写入。如果选择 no，则将用户日历设置为私人读取或私人写入。
uiBaseUrl	字符串	BaseServerAddress，例如 "https://proxyserver/"。
uiConfigFile	字符串	用户界面的配置文件。

表 B-1 -P 选项的属性 （续）

属性	值	描述
uiProxyUrl	字符串	附加在 HTML 用户界面的 JavaScript 文件中的代理服务器地址。例如 https://web_portal.iplanet.com/。
domainAccess	字符串	用于域的访问控制字符串。在跨域搜索时使用。
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 中列出的属性可以与以下命令的 -R 选项一起使用：commadmin domain create 和 commadmin domain modify。这些属性具有面向位的值。

有关 WCAP 和 WCAP set-userprefs 命令的信息，请参见 《Sun Java System Calendar Server Programmer's Manual》。

表 B-2 -R 选项的属性

属性	值	描述
allowUserDoubleBook	bit 8	允许为同一时间段多次安排此日历。
allowResourceDoubleBook	bit 9	允许为同一时间段多次安排此资源日历。
allowModifyUserPreferences	bit 4	允许 Calendar Server 管理员使用 WCAP 的 get/set userprefs 命令来为用户获取或设置用户首选项。
allowModifyPassword	bit 5	允许用户通过此服务器更改其密码。
allowCalendarCreation	bit 0	允许创建日历。
allowCalendarDeletion	bit 1	允许删除日历。
allowPublicWritableCalendars	bit 2	允许用户拥有可公共写入的日历。
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。

表 B-2 -R 选项的属性 （续）

属性	值	描述
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与 commadmin domain create、 commadmin domain modify、commadmin resource create、commadmin resource modify、commadmin user create 和 commadmin user modify 命令的 -T 时区选项一起使用：

- 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/Anandyr
- 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

调试 Delegated Administrator

可以通过检查由 Delegated Administrator 组件、部署 Delegated Administrator 的 Web 容器以及 Directory Server 和 Access Manager 生成的日志文件，来获取 Delegated Administrator 的日志信息。

本附录包括以下主题：

调试命令行实用程序

要调试 Delegated Administrator 实用程序 (`commadmin`)，可以通过结合使用 `-v` 选项和 `commadmin` 命令，在客户端中打印调试消息。

Delegated Administrator 控制台日志

Delegated Administrator 控制台可以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`

可以通过编辑日志属性文件来指定您自己的日志文件：

日志属性文件名：logger.properties
默认位置：/var/opt/SUNWcomm/da/WEB-INF/classes/sun/comm/da/resources

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， no 表示禁用日志。

- da.log.file=*full pathname*

  指定用于写入日志语句的目录和文件。此属性将 da.log 更改为指定的文件名和位置。

Delegated Administrator 服务器日志

可以创建 Delegated Administrator 服务器日志，该日志中包含由 Web 容器上安装的 Delegated Administrator servlet 生成的调试语句。

要执行此操作，应启用调试 servlet，以记录执行 Delegated Administrator servlet 时生成的调试消息。可以转至以下 URL 路径，通过浏览器来打开调试 servlet：

http://*machine name*:*port*/commcli/debug?op=set&state=all&package=all&filename=*full path*

其中

machine name 为运行 Delegated Administrator 服务器的计算机的名称。

full path 为用于写入消息的日志的完整目录路径和名称。

例如：

```
http://abc.red.iplanet.com:8008/commcli/debug?op=set&state=all&package=all&filename=/tmp/debug.log
```

上述 URL 可将调试 servlet 消息记入以下路径和文件中：

```
/tmp/debug.log
```

每当重新启动 Web 容器时，都必须打开调试 servlet。

Web 容器服务器日志

可以通过检查 Web 容器生成的服务器日志，来进一步调试 Delegated Administrator。

Web Server

Web Server 维护位于以下路径中的访问日志和错误日志：

/web_server_base/https-*machine name*/logs

其中

web_server_base 为安装 Web Server 软件的路径。

machine name 为运行 Web Server 的计算机的名称。

Application Server 7.*x*

Application Server 7.*x* 维护位于以下路径中的访问日志和错误日志：

/application_server7_base/domains/domain1/server1/logs

其中

application_server7_base 为安装 Application Server 7.*x* 软件的路径。

Application Server 8.*x*

Application Server 8.*x* 维护位于以下路径中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 为安装 Application Server 8.*x* 软件的路径。

Directory Server 和 Access Manager 日志

可以通过检查 Directory Server 和 Access Manager 生成的日志，来进一步调试 Delegated Administrator。

Directory Server

Directory Server 维护位于以下路径中的访问日志和错误日志：

`/var/opt/mps/serverroot/slapd-`*`hostname`*`/logs`

其中

`hostname` 为运行 Directory Server 的计算机的名称。

Access Manager

Access Manager 维护位于以下路径中的日志文件。

`/var/opt/SUNWam/debug`

上述路径中包含 `amProfile` 和 `amAuth` 日志。

`/var/opt/SUNWam/logs`

上述路径中包含 `amAdmin.access` 和 `amAdmin.error` 日志。

附录 D

ACI 合并

本附录介绍了以下主题：

简介

在同时安装 Access Manager 与 Messaging Server 并使用 LDAP Schema 2 目录时，最初会在该目录中安装大量的访问控制指令 (Access Control Instructions, ACI)。有许多缺省 ACI 并不是 Messaging Server 所需要或使用的。

如果需要在运行时检查这些 ACI，则可能会影响 Directory Server 的性能，反过来，这又会影响 Messaging Server 查找以及其他目录操作的性能。

通过在目录中合并缺省 ACI 以减少其数量，可以提高 Directory Server 的性能。合并 ACI 也可以使其更易于管理。

减少 ACI 的方法如下：

- 组合、优化和简化多余的 ACI
- 修改 ACI 以使用更简单、更有效的语法
- 将 ACI 与其他 ACI 合并 （在根后缀中）
- 删除未使用的 ACI

- 对于具有许多组织的目录，可以删除单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) 在根后缀中合并 ACI，以及如何删除目录中未使用的 ACI。有关详细信息，请参见下面的合并和删除 ACI。

接下来，本附录对每个 ACI 进行了分析，并推荐了处理该 ACI 的方法：删除 ACI、修改 ACI 以使其更有效，或重写 ACI。

请注意，在这些建议中存在以下限制：

- 不存在对 Directory 控制台的最终用户访问
- 不存在对 Access Manager 控制台的最终用户访问。

如果存在这些限制，您必须自行确定 （根据您的安装要求）能否使用 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。

有关更多信息，请参见本附录后面的分析现有 ACI。

接下来，本附录介绍了由 replacement.acis.ldif 文件合并的 ACI。它列出了合并前的现有 ACI，以及合并后修改的 ACI。有关更多信息，请参见本附录后面的分析 ACI 的合并方式。

最后，本附录列出了 replacement.acis.ldif 放弃的 ACI。有关更多信息，请参见本附录后面的要放弃的未使用 ACI 的列表。

合并和删除 ACI

本部分列出的 ldif 文件 replacement.acis.ldif 可将合并的 ACI 安装在根后缀中，并从目录中删除未使用的 ACI。此 ldif 文件由 Delegated Administrator 提供，位于以下目录中：

da_base/lib/config-templates

将 replacement.acis.ldif 文件应用于目录时 （使用 ldapmodify）， ldapmodify 命令将删除根后缀中 aci 属性的所有实例，并使用 replacement.acis.ldif 文件中的 ACI 来替换这些 ACI。

因此，此过程最初将从根后缀中删除**所有** ACI，然后使用下列 ACI 集来替换它们。如果目录中包含由其他应用程序 （如 Portal Server）生成的 ACI，则应将这些 ACI 保存到一个文件，然后在应用 replacement.acis.ldif 文件后重新将它们应用于该目录。

有关使用此 ldif 文件清除 ACI 的说明，请参见本部分后面的替换 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||memb
erOf
  ||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")
  (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

开始之前的准备工作

在开始此过程之前，建议您首先检查目录中的现有 ACI。您应该确定是否需要保留可能会在此过程中删除的任何 ACI。

此过程最初将从根后缀中删除**所有** ACI，然后使用下列 ACI 集来替换它们。如果目录中包含由 Messaging Server 之外的其他应用程序生成的 ACI，则应将这些 ACI 保存到一个文件，然后在应用 `replacement.acis.ldif` 文件后重新将它们应用于该目录。

为了帮助您分析由 Access Manager 和 Messaging Server 生成的现有 ACI，请参见位于本附录后面的以下部分：

- 分析现有 ACI
- 分析 ACI 的合并方式
- 要放弃的未使用 ACI 的列表

替换 ACI

要合并根后缀中的 ACI 并删除未使用的 ACI，请执行以下步骤：

1. 保存根后缀中的现有 ACI。可以使用 ldapsearch 命令，如下例所示：

   ```
   ldapsearch -D "cn=Directory Manager" -w <password>
   -s base -b <$rootSuffix> aci=* aci ><filename>
   ```

   其中

   <password> 为 Directory Server 管理员的密码。

   <$rootSuffix> 为您的根后缀，如 o=usergroup。

   <filename> 为文件名，该文件用于写入保存的 ACI。

2. 复制并重命名 replacement.acis.ldif 文件。

   安装 Delegated Administrator 时，会将 replacement.acis.ldif 文件安装在以下目录中：

   da_base/lib/config-templates

3. 在 replacement.acis.ldif 文件的副本中编辑 $rootSuffix 条目。

   将根后缀参数 $rootSuffix 更改为您的根后缀（如 o=usergroup）。$rootSuffix 参数在 ldif 文件中出现多次；必须替换每个实例。

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> 为 Directory Server 管理员的名称。

   <password> 为 Directory Service 管理员的密码。

   <replacement.acis.finished.ldif> 为编辑过的的 ldif 文件的名称，该文件用于在目录中合并和删除 ACI。

删除动态组织 ACI

使用 Delegated Administrator 控制台创建组织时，将在组织节点上创建一组 ACI。

由于在上述过程中安装了替换 ACI，因此不再需要这些按组织创建的 ACI。可以使用 Access Manager 控制台来阻止按组织创建 ACI。请执行以下步骤：

1. 以 amadmin 的身份登录到 AM 控制台。 AM 控制台位于以下 URL 中：

   http://<*machine name*>:<*port*>/amconsole

   其中

   <*machine name*> 为运行 Access Manager 的计算机

   <*port*> 为端口
2. 选择**服务配置**标签。

   缺省情况下，将显示 “管理”配置页。
3. 在控制台的右侧向下滚动，直到出现**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. 保存编辑过的设置。

分析现有 ACI

本部分中的列表显示了安装 Access Manager 和 Messaging Server 时在目录中安装的 ACI。此外，它还介绍了每个 ACI 的功能，以及对能否保留、合并或放弃 ACI 的建议。

可以将 ACI 划分为以下几类：

- 根后缀
- Access Manager
- 顶级帮助台管理员角色
- 顶级策略管理员角色
- AM 自身
- AM 匿名
- AM 拒绝写入访问权限
- AM 容器管理员角色
- 组织帮助台
- AM 组织管理员角色
- AM 杂项

- Messaging Server

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。

不需要对此后缀的自身访问。此 ACI 是重复的；可以将其合并到根后缀上的自身 ACI 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。

此为 “管理员”用户，该用户将使用 “通过验证”来通过 slapd-config 实例的验证。如果作为 Directory Manager 执行所有配置 （使用命令行实用程序），则不需要此 ACI。如果有人需要作为此用户通过控制台的验证，则可保留此 ACI。可以删除相似的 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：放弃所有数据库后端。

此为 “配置管理员”组，如果使用控制台来委托服务器管理权限，则该组将具有相应权限。

```
#
# discard
#
aci:
(targetattr =”*”)
(version 3.0;acl “Directory Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Directory Administrators, $rootSuffix”);)
```

操作：放弃所有数据库后端。

此为一般的 “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：放弃所有数据库后端。

此为与控制台 / 管理服务器相关的组权限定义。

```
---------------------------------------------------------------------------------------------------
```

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 将访问权限授予 Access Manager 的系统用户。

```
---------------------------------------------------------------------------------------------------
```

```
#
# 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 将访问权限授予 Access Manager 的系统用户。

```
#
# 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 将访问权限授予 Access Manager 的系统用户。

```
#
# 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 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 将访问权限授予顶级管理员角色。

```
#
# discard
#
aci:
(targetattr="iplanet-am-saml-user ||
iplanet-am-saml-password")(targetfilter="(objectclass=iplanet-am-saml-serv
ice)")
(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 保护与 SAML 相关的属性。

顶级帮助台管理员角色

```
#
# 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。

顶级策略管理员角色

```
#
# 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 适用于顶级策略管理员角色。

```
#
# 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 适用于顶级策略管理员角色。

```
#
# 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 适用于顶级策略管理员角色。

```
#
# 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 适用于顶级策略管理员角色。

AM 自身

```
#
# consolidate
#
aci:
(targetattr = "*")
(version 3.0;
acl "S1IS Deny deleting self";
deny (delete)
userdn ="ldap:///self";)
```

操作：合并到单个自写入 ACI 中。不需要显式拒绝，因为最终用户不具备删除任何条目 （包括其自身）的权限。

这是几个设置自身权限的 ACI 中的一个。显式拒绝可阻止任何条目删除自身。

```
#
# 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：合并到单个自写入 ACI 中。

这是几个设置自写入权限的 ACI 中的一个。

```
#
# 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：合并到单个自写入 ACI 中。

这是几个设置权限的 ACI 中的一个。

```
#
# 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：合并到单个自写入 ACI 中。

这是几个设置自写入权限的 ACI 中的一个。

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：合并到单个匿名 ACI 中。

这是几个授予匿名权限的 ACI 中的一个。

```
#
# 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：合并到单个匿名 ACI 中。

这是几个授予匿名权限的 ACI 中的一个。

```
#
# 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 将阻止任何用户 （rootdn 除外）删除缺省组织。

```
#
# 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 将阻止任何用户 （rootdn 除外）删除顶级管理员角色。

AM 拒绝写入访问权限

```
#
# 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 适用于拒绝写入访问角色。

AM 容器管理员角色

```
#
# 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 适用于容器管理员角色。

```
#
# 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 适用于容器管理员角色。

```
#
# 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 适用于组和用户容器管理员角色。

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 适用于组织帮助台管理员角色。

```
#
# 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 适用于组织帮助台管理员角色。

AM 组织管理员角色

```
#
# 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 适用于组织管理员角色。

```
#
# 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 适用于组织管理员角色。

```
#
# 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 适用于组织管理员角色。

```
#
# 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 适用于组织管理员角色。

```
#
# 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 将权限授予邮件最终用户管理员组。

```
#
# 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 将权限授予邮件最终用户管理员组。

```
-------------------------------------------------------------------------------------------------------

#
# 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。

这是几个设置自身权限的 ACI 中的一个。

```
-------------------------------------------------------------------------------------------------------
```

分析 ACI 的合并方式

本部分中的列表显示了已在替换文件 ldif (`replacement.acis.ldif`) 中合并的 ACI，使用 ldif 文件可以合并目录中的 ACI。有关如何替换 ACI 的说明，请参见替换 ACI 的步骤。

可以将 ACI 划分为几对。对于每个类别，首先列出最初的 ACI，然后列出合并的 ACI：

- 最初的匿名访问权限
- 合并的匿名访问权限
- 最初的自身 ACI
- 合并的自身 ACI
- 最初的 Messaging Server ACI

- 合并的 Messaging Server ACI
- 最初的组织管理 ACI
- 合并的组织管理 ACI

最初的匿名访问权限

```
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：可以对根进行匿名访问，这允许存在相同项，并排除了 aci 属性。 Access Manager 的此替换项删除了开销很大的目标中的 (*)，因为它允许对后缀进行匿名访问。

最初的自身 ACI

```
aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
asswordExpirationTime
|| 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 ||
sLookThroughLimit
|| 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||mailEquivalent
address||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota
||mailMsgQuota
||inetSubscriberAccountId||dataSource||mailhost||mailAllowedServiceAccess
||pabURI||inetCOS||mailSMTPSubmitChannel||aci")
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization Admin
ole,*))))
(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";)
```

合并的自身 ACI

```
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：缺少所有的 iplanet-am-* 属性。由于在 ACI 不存在的情况下 deny 为缺省值，因此删除所有的 deny ACI。将允许写入的 ACI 合并到一个 ACI 中。

最初的 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";)
```

合并的 Messaging Server ACI

在自身 ACI 中处理该自身 ACI。

```
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")
(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：与最初的 ACI 相同。

最初的组织管理 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 ACI 的列表

本部分中的列表显示了未使用的缺省 ACI，将 `replacement.acis.ldif` 文件应用于目录时，将从该目录中放弃这些 ACI。

要放弃的 ACI 可划分为以下几类：

- 后缀
- 顶级帮助台管理员角色
- 顶级策略管理员角色
- Access Manager 匿名
- Access Manager 拒绝写入访问权限
- Access Manager 容器管理员角色

- 组织帮助台
- 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"); )
```

顶级帮助台管理员角色

```
#
# 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";)
```

顶级策略管理员角色

```
#
# 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 拒绝写入访问权限

```
#
# 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 容器管理员角色

```
#
# 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”;)
```

词汇表

要获取本文档集中所用术语的完整列表，请参阅 Java Enterprise System 词汇表 (http://docs.sun.com/doc/819-1935)。

索引

D

E

F

G

I

J

L

M

O

P

R

S

T

U

V

W

Y

Z