管理指南

Sun™ ONE Directory Server

版本 5.2

816-6852-10
2003 年 6 月

目录

关于本指南

Sun™ ONE Directory Server 5.2 是功能强大且具伸缩性的分布式目录服务器，它基于符合工业标准的轻型目录访问协议 (LDAP)。 Sun ONE Directory Server 软件是 Sun Open Net Environment (Sun ONE) 的组成部分，后者是 Sun 推出的基于标准的软件界面、体系结构、平台和专门技术，用于构建和部署按需服务。

Sun ONE Directory Server 是构建集中化与分布式数据库的基础，这样建立的数据库可用于内部网，也可跨越外联网从而实现与商业合作伙伴共享数据资源，或者可跨越公用 Internet 做到与客户进行交流。

本指南的用途

本管理指南介绍了配置和维护基于 Sun ONE Directory Server 的目录服务所需的全部步骤。其中包括从控制台或命令行配置所有 Directory Server 功能的步骤 （如果适用）。

前提条件

本指南介绍如何管理目录服务器及其内容。但是，本手册并没有介绍许多基本的目录和体系结构概念，上述概念是成功设计和部署目录服务所必需的。因此您应该熟悉这些概念。相关具体介绍见于 *Sun ONE Directory Server 部署指南*。

完成目录部署的初步计划后，就可以配置系统并安装 Sun ONE Directory Server。各种 Directory Server 组件的安装说明包含在 *Sun ONE Directory Server 安装和调整指南* 中。

最后，本指南假定读者熟悉 Directory Server 控制台和 *Sun ONE Directory Server 入门指南* 中介绍的基本命令。举例来说，命令行步骤取决于 `ldapmodify` 命令，因此您应该了解此工具所使用的 LDIF （LDAP 数据交换格式）输入。同时， *Sun ONE Server Console 服务器管理指南* 中提供了有关如何使用 Sun ONE 服务器的常规背景信息。

印刷约定

本节讲述本书中使用的印刷约定。

等宽字体 - 该字体用来表示文字类型的文本，例如在文本中显示的属性和对象类的名称。还用来表示 URL、文件名和示例。

斜体字体 - 该字体用于强调、表示新术语，以及表示必须替代为实际值的文本，如路径名中的占位符。

在提及菜单或子菜单中的项时，将大于符号 (>) 作为分隔符。例如，“对象” >“新建” >“用户”是指应选择 “对象”菜单的 “新建”子菜单中的 “用户”项。

注意 “注意”、“警告”以及 “提示”用于突出重要的条件或限制。请务必阅读此类信息，然后再继续。

默认的路径和文件名

Sun ONE Directory Server 产品文档中的所有路径和文件名示例均采用下列两种形式之一：

- *ServerRoot*/...- *ServerRoot* 是 Sun ONE Directory Server 产品的位置。本路径包含目录服务器、管理服务器和 LDAP 命令的共享二进制文件。

  实际的 *ServerRoot* 路径取决于平台、安装和配置。默认路径取决于产品平台和封装，如表 1 （第 15 页）中所示。

- *ServerRoot*/slapd-*serverID*/...- *serverID* 是在安装或配置期间定义的 Directory Server 实例的名称。此路径包含指定实例专用的数据库和配置文件。

注意 本手册中指定的路径使用 Unix 的正斜杠格式，且指定命令时不带文件扩展名。如果使用 Sun ONE Directory Server 的 Windows 版本，则请使用等效的反斜杠格式。 Windows 平台上的可执行文件通常与 `.exe` 或 `.bat` 扩展名具有相同名称。

表 1 默认的 ServerRoot 路径

产品安装	*ServerRoot* 路径
Solaris 软件包[1]	`/var/mps/serverroot` - 配置完成后，此目录包含至以下位置的链接： • `/etc/ds/v5.2`（静态配置文件） • `/usr/admserv/mps/admin`（Sun ONE Administration Server 二进制文件） • `/usr/admserv/mps/console`（Server Console 二进制文件） • `/usr/ds/v5.2`（Directory Server 二进制文件）
在 Solaris 和其他 Unix 系统上的精简安装	`/var/Sun/mps`
在 Windows 系统上的压缩安装	`C:\Program Files\Sun\MPS`

1. 如果使用 Solaris 操作环境且不能确定安装的是 Sun ONE Directory Server 软件的哪一个版本，则请使用 `pkginfo` 命令检查是否存在关键软件包，如 `SUNWdsvu`。例如：`pkginfo | grep SUNWdsvu`。

Directory Server 实例位于 *ServerRoot*`/slapd-`*serverID*`/` 下，其中 *serverID* 表示创建时为实例提供的服务器标识符。例如，如果将 Directory Server 命名为 `dirserv`，则实际路径将如表 2 中所示。如果在其他位置创建了 Directory Server 实例，则请相应地修改该路径。

表 2 示例 `dirserv` 实例位置

产品安装	实例位置
Solaris 软件包	`/var/mps/serverroot/slapd-dirserv`
在 Solaris 和其他 Unix 系统上的精简安装	`/usr/Sun/mps/slapd-dirserv`

表 2　　示例 dirserv 实例位置

产品安装	实例位置
在 Windows 系统上的压缩安装	C:\Program Files\Sun\MPS\slapd-dirserv

下载 Directory Server 工具

某些受支持的平台可提供本机工具，用于访问 Directory Server。要获得检测和维护 LDAP 目录服务器的更多工具，请下载 Sun ONE Directory Server Resource Kit (DSRK)。可在以下位置下载此软件：

```
http://wwws.sun.com/software/download/
```

在 *Sun ONE Directory Server Resource Kit 工具参考* 中可以找到 DSRK 工具的安装说明和参考文档。

如果要开发目录客户机应用程序，还可以从同一位置下载 Sun ONE LDAP SDK for C 和 Sun ONE LDAP SDK for Java。

另外， Java 命名和目录接口 (JNDI) 技术支持使用 Java 应用程序中的 LDAP 和 DSML v2 访问 Directory Server。可从以下位置获得 JNDI 的有关信息：

```
http://java.sun.com/products/jndi/
```

JNDI 指南包含有关如何使用 JNDI 的详细说明和示例。可以在以下位置获得：

```
http://java.sun.com/products/jndi/tutorial/
```

建议的读物

Sun ONE Directory Server 产品文档包括以 HTML 和 PDF 格式提供的下列文档：

- *Sun ONE Directory Server 入门指南* - 可以用于快速查看 Directory Server 5.2 的许多关键功能。
- *Sun ONE Directory Server 部署指南* - 讲述如何计划目录拓扑、数据结构、安全和监控，并讨论示例的部署。
- *Sun ONE Directory Server 安装和调整指南* - 概述了安装和升级过程，并提供了优化 Directory Server 性能的有关提示。
- *Sun ONE Directory Server 管理指南* - 提供了使用控制台和命令行管理目录内容和配置 Directory Server 的每一项功能的步骤。

- *Sun ONE Directory Server 参考手册* - 详述了 Directory Server 配置参数、命令、文件、错误消息和模式。
- *Sun ONE Directory Server Plug-In API 编程指南* - 演示了如何开发 Directory Server 插件。
- *Sun ONE Directory Server Plug-In API 参考* - 详述了 Directory Server 插件 API 的数据结构和功能。
- *Sun ONE Server Console 服务器管理指南* - 讨论了如何使用 Sun ONE Administration Server 和基于 Java 的控制台来管理服务器。
- *Sun ONE Directory Server Resource Kit 工具参考* - 概述了 Sun ONE Directory Server Resource Kit （包括许多有用的工具）的安装和功能。

下列网站还提供了其他有用的信息：

- 产品联机文档：`http://docs.sun.com/coll/S1_s1DirectoryServer_52`
- Sun 软件：`http://wwws.sun.com/software/`
- Sun ONE 服务：`http://www.sun.com/service/sunps/sunone/`
- Sun 支持服务：`http://www.sun.com/service/support/`
- 面向开发人员的 Sun ONE：`http://sunonedev.sun.com/`
- 培训：`http://suned.sun.com/`

第 1 章

Sun™ ONE Directory Server 简介

Sun™ ONE Directory Server 产品中包括一个 Directory Server、一个用于管理多个目录的 Administration Server 和通过图形界面管理这两个服务器的 Sun ONE Server Console。本章概括地介绍有关 Directory Server 的信息以及使用控制台管理目录服务时所需的最基本操作。

本章中说明了 Directory Server 5.2 的两个新功能，即插件签名和 DSML-over-HTTP 协议。验证插件签名是一种附加安全功能，它允许服务器检测或防止加载未经授权的插件。目录服务器标记语言 (DSML) 是一种新的基于 XML 的格式，用于将请求发送到目录服务器。

本章包含以下小节：

- Directory Server 管理概述
- 启动和停止 Directory Server
- 在启用 SSL 的情况下启动服务器
- 使用 Directory Server 控制台
- 配置 LDAP 参数
- 验证插件签名
- 配置 DSML

Directory Server 管理概述

Sun ONE Directory Server 是一种强大且具伸缩性的服务器，用于管理企业范围内的用户和资源目录。此服务器基于名为轻型目录访问协议 (LDAP) 的开放系统服务器协议。 Directory Server 在计算机中作为 `ns-slapd` 进程或服务运行。该服务器管理目录内容并对客户机请求作出响应。

Administration Server 是由 Sun ONE 提供的辅助服务器，用于帮助您管理 Directory Server （以及其他所有 Sun ONE 服务器）；通过它您可以执行大多数 Directory Server 管理任务。 Sun ONE Server Console 是 Administration Server 的图形界面。而 Directory Server 控制台是 Sun ONE Server Console 的一部分，专门为 Sun ONE Directory Server 而设计。

通过 Directory Server 控制台可以执行大多数 Directory Server 管理任务。您也可以通过编辑配置文件或使用命令行公用程序来手动执行管理任务。有关 Sun ONE Server Console 的详细信息，请参阅 *Sun ONE Server Console 服务器管理指南*。

启动和停止 Directory Server

如果系统目前没有使用安全套接字层 (SSL)，则可以使用这里列出的方法来启动和停止 Directory Server。如果正在使用 SSL，请参阅 “在启用 SSL 的情况下启动服务器”（第 21 页）。

注意 在 UNIX 系统上，除非从 Solaris 软件包进行安装，否则重新启动系统不会自动启动 `slapd` 服务器进程。这是因为安装过程不会自动创建启动或运行命令 (`rc`) 脚本。有关如何编写这些脚本的详细信息，请参阅您的操作系统文档。

从命令行启动和停止服务器 (Unix)

如果目录服务器已停止，且未运行 Directory Server 控制台，则必须从命令行启动服务器。如果不希望使用 Directory Server 控制台，也可以从命令行停止服务器。请使用 root 特权运行以下命令之一：

Solaris 软件包
```
# /usr/sbin/directoryserver start
```
其他安装
```
# ServerRoot/slapd-serverID/start-slapd
```

或者

Solaris 软件包
```
# /usr/sbin/directoryserver stop
```
其他安装
```
# ServerRoot/slapd-serverID/stop-slapd
```

其中 *serverID* 是安装服务器时为其指定的标识符。

在 UNIX 上，必须使用与 Directory Server 相同的 UID 和 GID 运行这些脚本。例如，如果以 `nobody` 运行 Directory Server，则必须也以 `nobody` 运行 `start-slapd` 和 `stop-slapd` 公用程序。

请注意，引荐模式不再可用。可以使用 Directory Server 控制台设置全局引荐。“设置默认引荐”（第 67 页）中对此过程进行了说明。

从控制面板启动和停止服务器 (Windows)

如果使用 Windows 系统，请从 “服务控制面板”执行以下步骤：

1. 从桌面选择 “开始” > “设置” > “控制面板”。
2. 双击 “服务”图标。
3. 滚动查看服务列表，然后选择 Sun ONE Directory Server。

   服务名为 `Sun ONE Directory Server 5.2 (serverID)`，其中 *serverID* 是服务器安装或配置过程中为其指定的标识符。
4. 单击 “启动”或 “停止”按钮执行所需的操作。

   停止 Directory Server 时，系统将要求您确认是否要停止该服务。

从控制台启动和停止服务器 （所有平台）

当 Directory Server 控制台正在运行时，可以通过其图形界面启动、停止和重新启动目录服务器。有关运行控制台的说明，请参阅 “启动 Directory Server 控制台”（第 23 页）。

1. 在 Directory Server 控制台的顶级 “任务”标签上，单击 “启动 Directory Server”、“停止 Directory Server”或 “重新启动 Directory Server”旁的相应按钮。

通过 Directory Server 控制台成功地启动或停止 Directory Server 后，控制台将显示一个消息对话框，说明已启动或关闭服务器。在出现错误的情况下，控制台将显示与错误相关的所有消息。

在启用 SSL 的情况下启动服务器

启用 SSL 之前，必须在服务器上安装和配置证书。有关管理证书和启用 SSL 的说明，请参阅第 11 章 “实现安全性”。有关证书、证书数据库以及获取服务器证书的信息，请参阅 *Sun ONE Server Console 服务器管理指南* 中的第 10 章“在 Sun ONE Server 中使用 SSL 和 TLS”。

要在启用了 SSL 的情况下启动服务器，必须提供保护服务器证书的口令：

- 在 Windows 上，必须从服务器的主机启动服务器。出于安全考虑，提示您输入口令的对话框仅出现在服务器的主机上。
- 在 UNIX 上，必须从命令行启动服务器。

或者在任一平台上，可以创建口令文件来存储证书口令。将证书数据库的口令存放在一个文件中，就可以通过服务器控制台启动服务器，还可以允许服务器在无人看管状态下运行时，自动进行重新启动。

警告 此口令以明文形式存储在口令文件中，所以使用口令文件有很大的安全隐患。如果服务器在不安全的环境中运行，请勿使用口令文件这种方式。

必须将此口令文件放在以下位置：

ServerRoot/alias/slapd-*serverID*-pin.txt

其中 *serverID* 是安装服务器时为其指定的标识符。

需要在此文件中包括如下的安全令牌名及其口令：

deviceName Token: *口令*

此示例中显示了内部证书数据库的设备名称 （大写和空格必须完全与显示的一致）：

Internal (Software) Token: *口令*

如果将证书存储在备用设备上，请使用 “管理证书对话框”顶部的下拉菜单中显示的设备名称。要创建证书数据库，必须使用 Administration Server 和 “证书安装向导”。有关在 Directory Server 中使用 SSL 的信息，请参阅第 11 章 “实现安全性”。

使用 Directory Server 控制台

Directory Server 控制台是一个界面，可以作为 Sun ONE Server Console 的独立窗口对其进行访问。可以从 Sun ONE Server Console 启动 Directory Server 控制台，其步骤如下。

启动 Directory Server 控制台

1. 检查目录服务器守候进程 `slapd-`*serverID* 是否正在运行。如果没有运行，请以 root 用户或管理用户身份输入以下命令来启动它：

Solaris 软件包
```
# /usr/sbin/directoryserver start
```
其他安装
```
# ServerRoot/slapd-serverID/start-slapd
```

2. 检查 Administration Server 守候进程 `admin-serv` 是否正在运行。如果没有运行，请以 root 用户或管理用户身份输入以下命令来启动它：

Solaris 软件包
```
# /usr/sbin/directoryserver start-admin
```
其他安装
```
# ServerRoot/start-admin
```

3. 请输入以下命令启动 Sun ONE Server Console：

Solaris 软件包
```
# /usr/sbin/directoryserver startconsole
```
其他安装
```
# ServerRoot/startconsole
```

   如果在未安装 Sun ONE Administration Server 的计算机上运行 Sun ONE Server Console，则可能需要在 Administration Server 上配置连接限制，如 *Sun ONE Server Console 服务器管理指南* 中第 7 章中的 “网络设置”中所述。

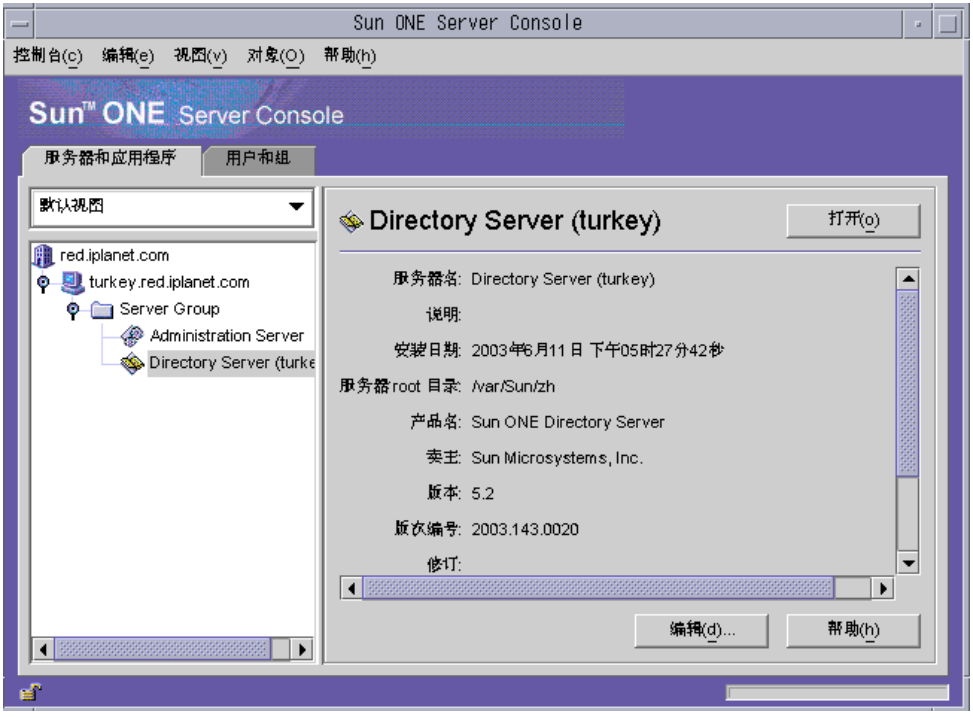
   屏幕上将显示 “控制台”登录窗口。或者，如果您的配置目录 （即包含 `o=NetscapeRoot` 后缀的目录）存储在单独的 Directory Server 实例中，那么屏幕上将显示一个窗口，要求您输入管理员用户 DN 和口令，以及该目录服务器的 Administration Server 的 URL。

4. 使用具有足够访问权限来执行所需操作的用户的绑定 DN 和口令登录。例如，可以使用 `cn=Directory Manager` 和相应的口令。

   屏幕上将显示 Sun ONE Server Console。

5. 浏览左侧面板中的树，找出 Directory Server 所在的主机，然后单击此计算机的名称或图标来显示其常规属性。

图 1-1 Sun ONE Server Console



要编辑目录服务器的名称和说明，请单击 “编辑”按钮。在文本框中输入新的名称和说明。单击 “确定”设置新名称和说明。名称将显示在左侧的树中，如上图所示。

6. 在树中双击 Directory Server 的名称或单击 “打开”按钮以显示用于管理此目录服务器的 Directory Server 控制台。

浏览 Directory Server 控制台

Directory Server 控制台提供了界面，用于浏览 Directory Server 实例以及执行管理操作。它始终显示四个标签，可通过这些标签访问所有 Directory Server 功能：

- “任务”标签 - 其中的按钮可以执行管理任务，如重新启动服务器。
- “配置”标签 - 允许您访问所有服务器管理参数。
- “目录”标签 - 显示和编辑目录中所包含的数据条目。

- “状态”标签 - 显示服务器的统计信息、日志和复制状态。

“任务”标签

打开 Directory Server 控制台时，看到的第一个界面就是 “任务”标签。其中所包含的按钮可用于执行各种主要的管理任务 （如启动或停止 Directory Server），如下图所示。要查看所有任务及其对应按钮，可能需要滚动浏览整个列表。

图 1-2 Directory Server 控制台的 “任务”标签

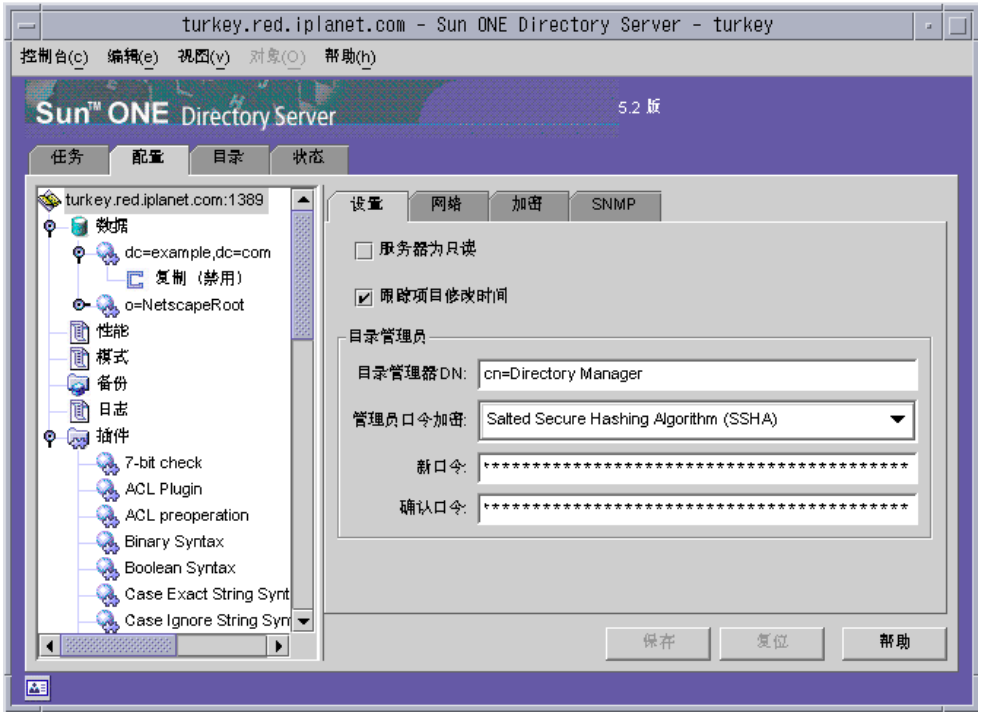
必须以具有管理员权限的用户身份登录，才能执行这些任务。对于没有足够权限的用户，任务按钮将不可见。

“配置”标签

Directory Server 控制台的 “配置”标签提供了界面和对话框，用于查看和修改各种目录设置 （如后缀、复制、模式、日志和插件的目录设置）。只有在以具备管理员权限的用户身份登录时，这些对话框才可用或生效。

此标签左侧包含一个带有所有配置功能的树，右侧则显示专用于管理各个功能的界面。这些界面通常包含其他标签、对话框或弹出窗口。例如，下图显示了整个目录的常规设置。

图 1-3　　Directory Server 控制台的 “配置”标签



当在左侧树中选择某个可配置的项时，该项的当前设置会显示在右侧面板的一个或多个标签中。要了解这些设置的说明和行为，请参阅本指南中具体介绍各项功能的章节。根据设置情况，某些更改会在保存时立即生效，而某些更改则要在重新启动服务器后才会生效。当需要重新启动服务器时，控制台将显示一个对话框通知您。

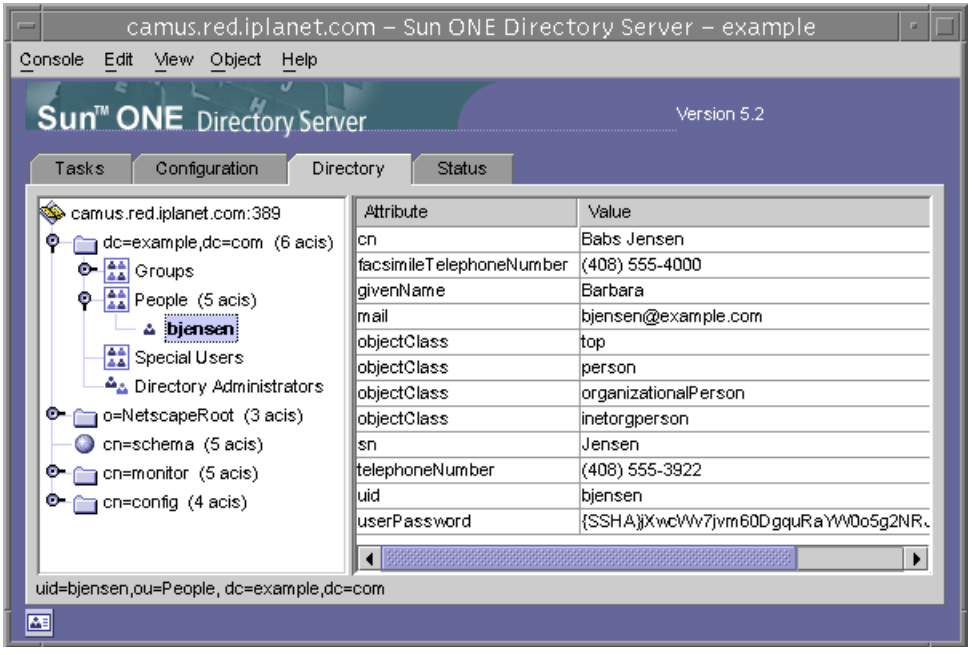
标签名称旁的红色标记表示该标签中的更改尚未保存。即使在配置另一项或查看其他主要标签时，未保存的更改仍会保留在该标签中。“保存”和 “复位”按钮适用于给定配置项的所有标签，但不影响其他项的未保存设置。

大多数文本字段仅允许按该设置的正确语法输入值。默认情况下，如果值的语法不正确，则该设置的标签和您输入的值将会以红色突出显示。在所有设置的语法均有效之前，“保存”按钮将被禁用。可以选择以斜体突出显示不正确的值，如 “可视配置首选项”（第 31 页）中所述。

“目录”标签

控制台的 “目录”标签以树的形式显示目录条目，以方便浏览。在此标签中，可以浏览、显示和编辑所有条目及其包含的属性。

图 1-4 Directory Server 控制台的 “目录”标签



如果登录期间给定的绑定 DN 具有足够的访问权限，那么配置条目将被视为普通条目，可以直接进行修改。不过，若要安全地更改配置设置，则应始终使用 “配置”标签上的可用对话框。

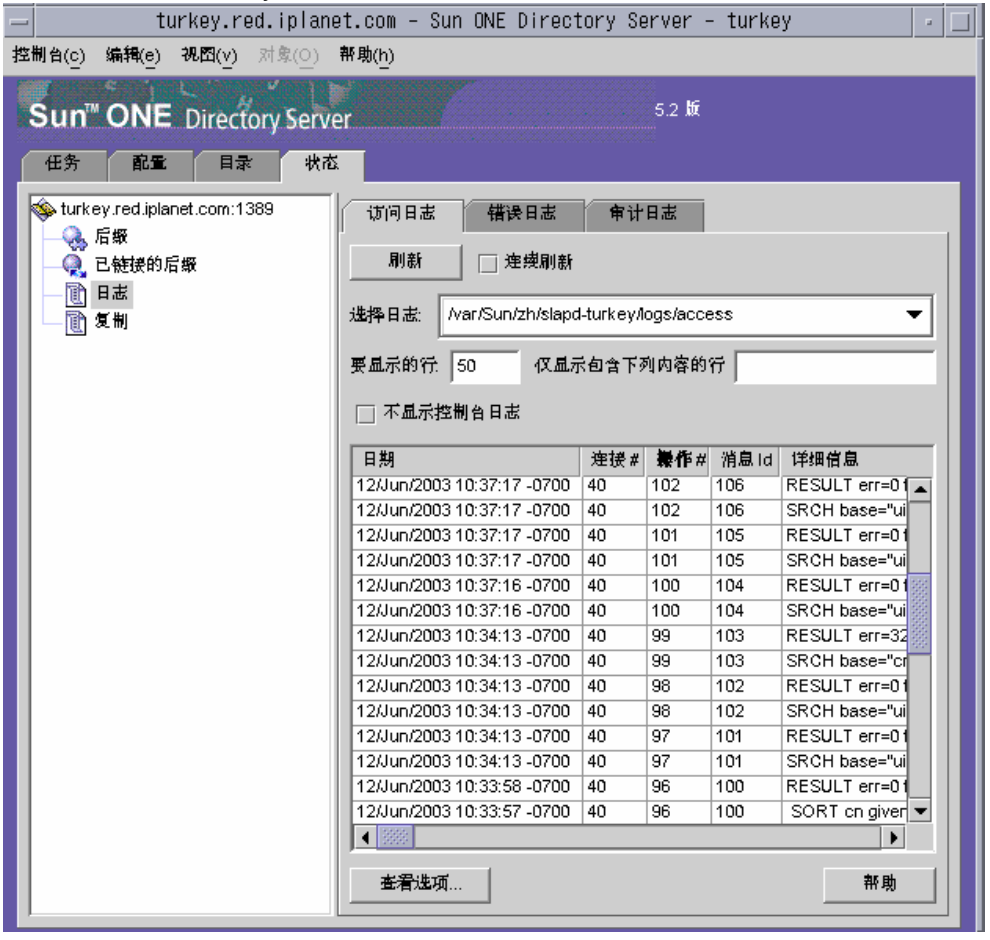
“查看”菜单下的几个可用选项可以用来更改 “目录”标签的布局和内容。新的布局选项包括在单个树中查看所有条目 （包括叶条目），以及在右侧窗格中显示属性。默认设置是在右侧查看叶条目，而不是在左侧的树中查看。

“查看” > “显示”选项为目录树中的所有条目启用 ACI 计数、角色计数和去活状态图标。在上图中， ACI 计数和叶条目显示在左侧树中，而选定条目的属性值显示在右侧窗格中。详细信息，请参阅 “目录树视图选项”（第 31 页）。

“状态”标签

“状态”标签显示服务器统计信息和日志消息。左侧树中列出了全部状态项；选定某项后，该项的内容会显示在右侧窗格中。例如，下图显示了日志条目表。

图 1-5 Directory Server 控制台的 “状态”标签



通过控制台查看当前绑定 DN

单击显示屏左下角的登录图标，可以查看登录至 Directory Server 控制台时使用的绑定 DN。当前绑定 DN 将显示在登录图标旁，如下所示：

更改登录身份

在通过 Directory Server 控制台创建或管理条目时，以及在第一次访问 Sun ONE Server Console 时，可以选择通过提供绑定 DN 和口令来登录。这将识别访问此目录树的用户身份，并确定其用以执行操作的访问权限。

第一次启动 Sun ONE Server Console 时，可以使用目录管理员 DN 登录。可以随时选择以其他用户身份登录，而无需停止并重新启动控制台。

要更改登录到 Sun ONE Server Console 的用户身份，请执行以下操作：

1. 在 Directory Server 控制台上，选择 “任务” 标签，然后单击 “以新用户身份登录到目录服务器” 标签旁的按钮。此外，当位于其他控制台标签中时，可以选择 “控制台” > “以新用户身份登录” 菜单项。

   屏幕上将出现一个登录对话框。

2. 输入新的 DN 和口令，然后单击 “确定”。

   输入要绑定至服务器的条目的完整标识名称。例如，如果要以目录管理员身份执行绑定，请在 “标识名称” 文本框中输入以下 DN：

   ```
   cn=Directory Manager
   ```

目录管理员 DN 和口令将在下一节中详细说明。

使用联机帮助

联机帮助为 Directory Server 控制台中大部分标签和对话框提供上下文相关的信息。“帮助” 按钮通常位于这些界面的右下角。在任何屏幕上，调用上下文相关帮助的键盘快捷键都是 `Alt-P`。

调用联机帮助将在控制台的内置浏览器中显示一个基于 HTML 的页面。在该页面中，可以单击 “在浏览器中启动” 按钮，以在外部浏览器 （如 Netscape Communicator）中打开相同的页面。在联机帮助中，指向更进一步信息的链接也会打开一个外部浏览器窗口。

每个联机帮助页面都对相应的标签或对话框中的字段和按钮进行说明。当通过控制台解释、输入或修改值时，请在该信息的指导下完成。

Sun ONE Directory Server 的帮助系统取决于 Sun ONE Administration Server。如果正在 Administration Server 的远程计算机中运行 Directory Server 控制台，则需要验证以下内容：

- 可能需要配置在 Administration Server 上强制执行的连接限制，以允许从您的计算机进行访问，如 *Sun ONE Server Console 服务器管理指南* 中第 7 章中的 “网络设置” 中所述。
- 如果希望使用外部浏览器查看联机帮助页，且浏览器配置为使用代理，则必须执行以下操作之一：
  - 在浏览器配置中禁用代理。在 Netscape Communicator 中，请选择 “编辑” > “首选项” 菜单项。然后，选择 “高级” > “代理” 类别以访问代理配置。如果使用 Internet Explorer，请在 “工具” 菜单中选择 “Internet 选项”。
  - 配置 Administration Server 中的连接限制，以允许通过代理服务器进行访问。

警告 配置 Administration Server 以允许通过代理服务器进行访问会在系统中造成潜在的安全漏洞。

控制台剪贴板

Directory Server 控制台使用系统剪贴板来复制、剪切和粘贴文本。在 “目录” 标签中浏览时，可以将条目的 DN 或 URL 复制到剪贴板中以减少键入：

在打开对话框或其他标签之前 （您需要在其文本字段中粘贴 DN 或 URL），请执行以下操作：

1. 在 Directory Server 控制台的顶级 “目录” 标签上，浏览树并选择 （左键单击）要复制其 DN 或 URL 的条目。
2. 然后，从菜单中选择 “编辑” > “复制 DN” 或 “编辑” > “复制 URL”。

控制台设置

Directory Server 控制台提供许多设置，用于定制信息在 “配置”和 “目录”标签中的显示方式。

可视配置首选项

当在顶级 “配置”标签上的字段中修改配置参数或输入值时， Directory Server 控制台使用彩色文本表示有效的输入。例如，如果启用了一个功能，该功能要求输入更详细的配置值，则所需字段的标签将显示为红色，在您输入了有效值之后，则变为蓝色。

默认情况下，控制台会使用红色和蓝色，但可以使用以下方法修改此设置：

1. 在 Directory Server 控制台的任意标签上，选择 “编辑” > “首选项”菜单项。在 “控制台首选项”对话框中，选择 “其他”标签。
2. 为希望的可视配置指示符选择相应的单选按钮。可以选择彩色字体或字体外观（或两者）。
3. 有关 “控制台首选项”对话框的其他标签上设置的说明，请参阅 *Sun ONE Server Console 服务器管理指南* 中第 3 章中的 “定制 Sun ONE Server Console”。

   然后单击 “确定”以保存更改。
4. 退出 Sun ONE Server Console 的所有窗口，然后重新启动控制台。

目录树视图选项

在 Directory Server 控制台的顶级 “目录”标签上，“视图”菜单中的各项允许您在目录树中显示其他信息，并选择要在右侧面板中出现的内容。

以下 “视图”选项会影响 “目录”标签的内容：

- 遵循引荐 - 选中此复选框时，目录树将显示条目和引荐目标的所有子级，如同它们在目录中一样。如果未选中该复选框，则引荐显示为引荐条目。详细信息，请参阅 “创建智能引荐”（第 67 页）。
- 对象排序 - 如果未选中此复选框，则按服务器返回条目的顺序显示条目。选中此复选框时，目录树中同一级的条目按下面说明的显示属性排序。有关如何在不影响服务器性能的情况下，对大型子树排序的详细信息，请参阅 “用于控制台的浏览索引”（第 314 页）。

  将对按如下属性显示的条目进行排序：`cn`、`givenname`、`o`、`ou`、`sn`，然后是 `uid`。将不对按其他属性显示的条目进行排序。

- “显示” > “ACI 计数” - 如果条目在 aci 属性中包含一条或多条访问控制指令 (ACI)，目录树将在条目的旁边显示指令的数量。详细信息，请参阅第 6 章 “管理访问控制”。
- “显示” > “角色计数” - 如果条目是一个或多个角色的成员，则目录树将在条目的旁边显示角色的数量。详细信息，请参阅 “分配角色”（第 138 页）。
- “显示” > “去活状态” - 如果已去活用户条目或组条目以阻止其绑定到服务器，则目录树将显示一个红色框和线条穿过条目的图标。详细信息，请参阅 “去活和激活用户和角色”（第 234 页）。
- “布局” > “查看子级” - 选择此布局选项时，左侧面板中的树将不显示目录的叶条目，且选择左侧面板中的父节点将在右侧面板中显示其所有子级 （包括叶条目）。在这两个面板中都可选择条目。
- “布局” > “仅查看树” - 选择此布局选项时，“目录”标签仅具有一个面板，该面板显示一个树 （其中包含目录中的所有条目）。
- “布局” > “查看属性” - 选择此种布局时，左侧面板显示一个树 （其中包含目录中的所有条目），右侧面板则显示该树中所选条目中存储的属性和值。
- “显示属性” - 单击此菜单项，打开 “显示属性”对话框，选择 “目录”标签中显示的条目的标签。默认情况下，标签为条目的第一个 RDN 属性的值 （例如 People）。对于不具有 RDN 的基本条目，标签为整个 DN （例如 dc=example,dc=com）。

  要在目录树中使用不同的属性来显示条目，请选择其他单选按钮并选择一个属性。不具有所选属性的条目仍将使用条目的第一个 RDN 属性。默认情况下，标签中仅使用属性值。如果选中了 “显示属性名称”复选框，则标签将采用类似 ou=People 的形式。
- “刷新” - 进行一些操作后，必须刷新目录树的显示以查看新的值。选择该项将从服务器重新加载整个目录树。

配置 LDAP 参数

LDAP 参数是目录服务器中的基本设置，如目录管理员的标识名称 (DN)、全局只读设置、端口配置以及跟踪所有目录修改时间的功能。

配置目录管理员

目录管理员是具有特权的服务器管理员，与 UNIX 中的 root 用户相似。访问控制不适用于以目录管理员身份定义的条目。此条目的首次定义应该在安装过程中完成。默认值为 cn=Directory Manager。

目录管理员的 DN 存储在 nsslapd-rootDN 属性中，而口令存储在 cn=config 分支的 nsslapd-rootpw 属性中。

使用 Directory Server 控制台更改目录管理员 DN 和口令，以及用于此口令的加密方案：

1. 请以目录管理员身份登录至控制台。

   如果已经登录至控制台，有关如何以其他用户身份登录的说明，请参阅 “更改登录身份”（第 29 页）。

2. 在顶级 “配置”标签上，选择导航树根的服务器节点，然后在右侧面板中选择 “设置”标签。

3. 在 “目录管理员 DN”字段中输入新的标识名称。默认值为安装过程中定义的值。

4. 在 “管理员口令加密”下拉菜单中，选择服务器要使用的目录管理员口令的存储方案。

5. 请使用提供的文本字段输入并确认新口令。

6. 单击 “保存”。

更改 Directory Server 端口号

使用 Directory Server 控制台或在 cn=config 条目下更改 nsslapd-port 属性的值，均可以修改用户目录服务器的端口号或安全端口号。

如果要修改包含 Sun ONE 配置信息 （o=NetscapeRoot 子树）的 Sun ONE Directory Server 的端口或安全端口，则可以通过 Directory Server 控制台完成此操作。

如果要更改配置目录端口、用户目录端口或安全端口号，您需要明确以下可能产生的影响：

- 需要更改为 Administration Server 配置的配置目录端口、用户目录端口或安全端口号。请参阅 *Sun ONE Server Console 服务器管理指南* 中第 7 章中的 “网络设置”。

- 如果安装有指向此配置目录或用户目录的其他 Sun ONE Server，则需要更新这些服务器以使其指向新端口号。

使用以下步骤修改目录服务器监听传入 LDAP 请求时使用的端口或安全端口。要修改用于 DSML 请求的端口，请参阅 “配置 DSML”（第 37 页）。

1. 在 Directory Server 控制台的顶级 “配置”标签上，选择与服务器名称相同的根节点，然后在右侧面板中选择 “网络”标签。

   标签显示用于 LDAP 协议的服务器的当前端口设置。

2. 在 “端口”字段中输入服务器用于非 SSL 通信的端口号。默认值是 389。

3. 如果按第 11 章 “实现安全性”中所述已在该服务器上激活 SSL，则可以在安全端口上允许连接：

   a. 选择该选项以同时使用安全端口和非安全端口。

   b. 在 “安全端口”字段中输入服务器用于 SSL 通信的端口号。默认值是 636。

      指定的加密端口号一定不能与用于标准 LDAP 通信的端口号相同。

4. 单击 “保存”，然后重新启动服务器。

   有关信息，请参阅 “启动和停止 Directory Server”（第 20 页）。

设置全局只读模式

可以将目录中的每个后缀独立地设为只读模式，定义为只读模式后，可能会返回特定引荐。 Directory Server 还提供适用于所有后缀的全局只读模式，定义为此模式后，可能会返回全局引荐。

使用全局只读模式后，在执行如重新索引后缀这样的任务时，管理员可以防止修改目录内容。因此，全局只读模式不适用于以下配置分支：

- `cn=config`
- `cn=monitor`
- `cn=schema`

不论如何设置只读模式，这些分支应该始终由访问控制指令 (ACI) 保护，以防止非管理用户进行修改 （请参阅第 6 章 “管理访问控制”。）全局只读模式将阻止对目录中其他所有后缀的更新操作，包括目录管理员执行的更新操作。

如果启用了只读模式，它还会中断后缀的复制。主副本不再有任何要复制的更改，不过它仍会继续复制启用只读模式前所做的所有更改。禁用只读模式前，使用者副本不会再接收到任何更新。多主复制方案中的主副本既不会有任何要复制的更改，也不能从其他主副本处接收更新。

要启用或禁用全局只读模式，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中，选择配置树中的根节点，然后在右侧面板中选择 “设置”标签。
2. 选中或取消选中 “服务器为只读”复选框。
3. 单击 “保存”。所做的更改将立即生效。

有关将单个后缀设置为只读模式的信息，请参阅 “设置后缀只读模式”（第 117 页）。

跟踪目录条目修改

可以配置服务器，以维护新创建条目或已修改条目的特殊属性：

- `creatorsName` - 最先创建此条目人员的识别名。
- `createTimestamp` - 以 GMT （格林尼治标准时间）格式创建条目时的时间标记。
- `modifiersName` - 上次修改条目人员的识别名。
- `modifyTimestamp` - 上次以 GMT 格式修改的条目的时间标记。

注意 当客户机应用程序要创建或修改链接后缀中的条目时，`creatorsName` 和 `modifiersName` 属性不反映条目的实际创建人或修改人。这些属性包含绑定至远程服务器所需的链接代理名称。有关代理授权的信息，请参阅 “创建代理身份”（第 90 页）。

跟踪复制的后缀的修改时间时，名称和时间标记属性作为常规属性被复制。因此，这些属性反映的是主服务器上对条目所做原始修改的时间，而不是条目复制到使用者服务器上的时间。

要启用 Directory Server 以跟踪此信息，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中，选择配置树中的根节点，然后在右侧面板中选择 “设置”标签。
2. 选中 “跟踪条目修改时间”复选框。

服务器会将 creatorsName、 createTimestamp、 modifiersName 和 modifyTimestamp 属性添加至每个新创建条目或已修改条目。现有条目将不会包含创建属性。

3. 单击 “保存”，然后重新启动服务器。

   详细信息，请参阅 “启动和停止 Directory Server”（第 20 页）。

验证插件签名

验证插件签名是 Directory Server 5.2 的一项新功能。 Directory Server 提供的每个插件都具有一个数字签名，服务器可以在启动时对其进行验证。默认情况下，服务器将验证插件签名，但是不管签名是否存在或有效，它都会加载每个插件。

验证签名具有以下优点：

- 随 Directory Server 提供的插件签名表明该插件已经过严格测试，并且正式得到支持。
- 使用插件二进制自身的校验和，签名验证可以检测出插件是否已被篡改。因此，签名可以保护在服务器本身中运行的敏感代码。
- 可以将服务器配置为仅加载已签名的插件，这可以帮助检测未签名的和不受支持的插件所带来的问题。

配置插件签名的验证

1. 在 Directory Server 控制台的顶级 “配置”标签上，在配置树中选择 “插件”节点。当前的签名验证策略显示在右侧面板中。
2. 选择以下选项之一：
   - 不要验证插件签名 - 将加载在服务器配置中定义的所有插件，而不管其签名如何。将不会显示由于插件签名引起的任何警告或错误。
   - 标记具有无效签名的插件 - 将加载在服务器配置中定义的所有插件，但服务器将验证每个插件的签名。如果插件二进制有任何改变，则签名将不再有效，服务器将在启动时显示一条警告消息并将其记入错误日志中。也将标记没有签名的插件。

     如果有自定义的未签名插件，则此为推荐选项。将加载您的插件，但您仍可以查看所有已签名插件的状态。

- 拒绝签名无效的插件 - 服务器将验证在配置中定义的所有插件的签名，并且仅加载具有有效签名的插件。服务器将在启动时显示一条警告消息并将其记入错误日志，指出哪些插件具有无效签名或没有签名。

  这是最安全的选项，但您将无法加载自定义的未签名插件。

3. 单击 “保存”，然后重新启动目录服务器，如 “启动和停止 Directory Server”（第 20 页）中所述。

查看插件的状态

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开配置树中的 “插件”节点，然后选择要验证的插件。该插件的当前配置显示在右侧面板中。
2. “签名状态”字段显示具有以下某一值的插件的签名验证状态：
   - 未知 - 当服务器配置为不验证插件签名时，所有插件的签名状态都是 “未知”。以下状态仅当验证插件签名时才可见。
   - 有效签名 - 插件配置提供的签名与插件二进制的校验和匹配。该插件已正式得到支持。以下状态仅当标记 （但不拒绝）无效签名时才可见。
   - 无效签名 - 插件配置包含的签名与插件二进制的校验和不匹配。该状态表明插件可能已被篡改。
   - 无签名 - 插件配置未提供签名供服务器验证。

配置 DSML

除了处理轻型目录访问协议 (LDAP) 的请求外， Sun ONE Directory Server 5.2 现在还会响应目录服务标记语言版本 2 (DSMLv2) 发送的请求。 DSML 是客户机对目录操作进行编码的另一种方式，但服务器将使用所有相同的访问控制和安全功能，以处理其他请求的方式来处理 DSML 请求。事实上， DSML 处理允许多种其他类型的客户机访问您的目录内容。

Directory Server 支持通过超文本传输协议 (HTTP/1.1) 使用 DSMLv2，并使用简单对象访问协议 (SOAP) 版本 1.1 作为传送 DSML 内容的编程协议。有关这些协议和 DSML 请求示例的详细信息，请参阅 *Sun ONE Directory Server 部署指南* 中的附录 A “使用 DSMLv2 over HTTP/SOAP 访问数据”。

启用 DSML 请求

由于 LDAP 是用于访问目录的标准协议，因此安装 Directory Server 后，默认情况下不会启用 DSML 请求。如果希望服务器对通过 HTTP/SOAP 发送的 DSML 请求作出响应，必须明确启用此功能。

要通过控制台在服务器上启用 DSML 请求，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，选择配置树中的根节点，然后在右侧面板中选择 “网络”标签。
2. 选中 “启用 DSML”复选框，并选择以下安全选项之一。仅当具有激活的 SSL 时，安全端口选项才可用，如第 11 章 “实现安全性”中所述。
   - 仅非安全端口 - 非安全端口仅接受未加密的 HTTP 上的 DSML 请求。
   - 仅安全端口 - 安全端口仅接受 HTTPS 上的 DSML 请求。
   - 安全端口和非安全端口 - 两种端口都可用，客户机可选择两者之一。
3. 然后编辑以下任意字段：
   - 端口 - 用于接收 DSML 请求的 HTTP 端口。
   - 加密端口 - 使用 SSL 接收加密的 DSML 请求的 HTTPS 端口。
   - 相关 URL - 一个相关的 URL，当附加至主机和端口时，用来确定客户机发送 DSML 请求时必须使用的完整 URL。

   默认情况下，服务器将处理发送至下列 URL 的请求：

   `http://`*主机*`:80/dsml`
4. 单击 “保存”，系统将提示您必须重新启动服务器才能开始响应 DSML 请求。

要通过命令行启用 DSML 请求，请执行以下操作：

1. 执行以下 `ldapmodify` 命令，以启用 DSML 前端插件并修改其设置。修改 `ds-hdsml-port`、 `ds-hdsml-secureport` 和 `ds-hdsml-rooturl` 属性 （可选）：

```
% ldapmodify -h 主机 -p LDAPport -D "cn=Directory Manager" -w 口令
dn:cn=DSMLv2-SOAP-HTTP,cn=frontends,cn=plugins,cn=config
changetype:modify
replace:nsslapd-pluginEnabled
nsslapd-pluginEnabled:on
-
replace:ds-hdsml-port
ds-hdsml-port:DSMLport
-
```

```
add:ds-hdsml-secureport
ds-hdsml-port:secureDSMLport
-
replace:ds-hdsml-rooturl
ds-hdsml-root:relativeURL
-
^D
```

根据已定义的参数和属性值， DSML 客户机可能使用以下 URL 向此服务器发送请求：

`http://host:DSMLport/relativeURL`

`https://host:secureDSMLport/relativeURL`

2. 修改 DSML 前端插件后，必须重新启动服务器更改才能生效。不过，在重新启动服务器前，您可能希望按照后面小节中的说明为 DSML 验证配置安全和标识映射。

配置 DSML 安全性

除上节中介绍的安全端口设置外，还可以配置接受 DSML 请求所必需的安全级别。DSML 前端插件的 `ds-hdsml-clientauthmethod` 属性可以决定客户机所要求的验证方法。该属性可能有下列值：

- `httpBasicOnly` - 服务器将使用 HTTP 授权标头的内容来查找可以被映射至目录中条目的用户名。“DSML 标识映射”（第 40 页）对此过程及其配置进行了详细说明。使用此设置，对安全 HTTPS 端口的 DSML 请求将通过 SSL 进行加密，而不使用客户机证书。
- `clientCertOnly` - 服务器将使用客户机证书的凭证来识别客户机。使用此值，所有 DSML 客户机必须使用安全 HTTPS 端口来发送 DSML 请求，并提供证书。服务器将检查与目录中条目相匹配的客户机证书。有关客户机证书的详细信息，请参阅第 11 章 “实现安全性”。
- `clientCertFirst` - 如果提供了客户机证书，服务器将首先尝试使用客户机证书对客户机进行验证。如果没有提供，服务器将使用授权标头的内容验证客户机。

如果 HTTP 请求中未提供证书和授权标头，则服务器将使用匿名绑定执行 DSML 请求。下列情况也将使用匿名绑定：

- 在指定 `clientCertOnly` 时，客户机提供了有效的授权标头但未提供证书。
- 在指定 `httpBasicOnly` 时，客户机提供了有效的证书但未提供授权标头。

不论 ds-hdsml-clientauthmethod 属性为何值，如果提供了证书但证书却与条目不匹配，或者虽然指定了 HTTP 授权标头但却不能映射至用户条目，则 DSML 请求将会被拒绝，并且返回消息 403：“已禁止”。

要通过控制台设置 DSML 安全要求，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，选择配置树中的根节点，然后在右侧面板中选择 “加密”标签。

   必须已经配置并启用了 SSL，如第 11 章 “实现安全性”中所述。

2. 在 “DSML 客户机验证”字段的下拉菜单中，选择选项之一。

3. 单击 “保存”，然后重新启动服务器以实施此新安全设置。

要通过命令行设置 DSML 安全要求，请执行以下操作：

1. 运行以下 ldapmodify 命令以编辑 DSML 前端插件的属性：

```
% ldapmodify -h 主机 -p LDAP 端口 -D "cn=Directory Manager" -w 口令
dn:cn=DSMLv2-SOAP-HTTP,cn=frontends,cn=plugins,cn=config
changetype:modify
replace:ds-hdsml-clientauthmethod
ds-hdsml-clientauthmethod:httpBasicOnly|
                          clientCertOnly|
                          clientCertFirst
-
^D
```

2. 修改 DSML 前端插件后，需要重新启动服务器以实施新的安全设置。

DSML 标识映射

在没有证书的情况下执行基本验证时， Directory Server 使用名为标识映射的机制来确定接受 DSML 请求时使用的绑定 DN。此机制从 HTTP 请求的授权标头中提取信息，以确定用于绑定的标识。有关该机制的完整说明，请参阅 “标识映射”（第 336 页）。

服务器配置中的下列条目给出了用于 DSML-over-HTTP 的默认标识映射：

```
dn:cn=default,cn=HTTP-BASIC, cn=identity mapping, cn=config
objectclass:top
objectclass:nsContainer
objectclass:dsIdentityMapping
cn:default
dssearchbasedn:ou=People,userRoot
dssearchfilter:(uid=${Authorization})
```

此映射搜索 ou=People,*userRoot* 子树以查找其 uid 属性与授权标头中给定的用户名相匹配的条目。 *userRoot* 是安装目录时定义的后缀，如 dc=example,dc=com。

在这些映射条目属性中，可以使用格式为 ${*header*} 的占位符，其中 *header* 为 HTTP 标头的名称。 DSML 映射中最常用的标头如下：

- ${Authorization} - 将以 HTTP 授权标头中包含的用户名替换此字符串。授权标头既包含用户名也包含口令，但此占位符仅替换用户名。
- ${From} - 将以 HTTP “发件人”标头中包含的电子邮件地址替换此字符串。
- ${host} - 将以 DSML 请求的 URL 中的主机名和端口号替换此字符串，这些主机名和端口号即服务器自身的主机名和端口号。

要使 DSML 请求执行其他的标识映射，请执行以下操作，以便为 HTTP 标头定义新的标识映射：

1. 编辑默认的 DSML-over-HTTP 标识映射或为该协议创建自定义映射。有关标识映射条目中属性的定义，请参阅 “标识映射”（第 336 页）。这些映射条目必须位于以下条目的下方：cn=HTTP-BASIC, cn=identity mapping, cn=config。

   可以用以下两种方式之一创建新的映射条目：

   - 使用 Directory Server 控制台的顶级 “目录”标签创建具有相应对象类的新条目，如 “使用控制台管理条目”（第 45 页）中所述。
   - 使用 ldapmodify 工具从命令行中添加此条目，如 “使用 ldapmodify 添加条目”（第 60 页）中所述。

2. 重新启动 Directory Server 以使新映射生效。

   首先将评估自定义映射，如果没有成功的定制映射，则将评估默认映射。如果所有映射都未能确定 DSML 请求的绑定 DN，则将禁止并拒绝 DSML 请求 （错误 403）。

第 2 章

创建目录条目

本章讨论如何使用 Directory Server 控制台以及 `ldapmodify` 和 `ldapdelete` 命令行公用程序来修改目录的内容，包括结构条目、用户条目和引荐的基本类型。本章还讨论了如何使用可选的属性加密功能存储属性，该功能是 Directory Server 5.2 中的新增功能。

在目录部署的计划阶段中，您应当对目录将要包含的数据类型进行描述。在创建条目与修改默认模式之前，应当首先阅读 *Sun ONE Directory Server 部署指南* 中的第 2 章 “设计与访问目录数据”。

本章假定读者具备 LDAP 模式和对象类及其定义的属性的一些基础知识。有关模式和所有对象类的定义以及 Directory Server 中提供的属性的简介，请参阅 *Sun ONE Directory Server 参考手册* 中的第 4 部分 “Directory Server 模式”。

注意 如果没有定义适当的访问控制指令 (ACI)，则不能修改目录。详细信息，请参阅第 6 章 “管理访问控制”。

本章包含以下小节：

- 配置条目
- 使用控制台管理条目
- 从命令行管理条目
- 设置引荐
- 为属性值加密
- 维护引荐完整性

配置条目

目录服务器在以下文件中存储其所有配置信息：

ServerRoot/slapd-*serverID*/config/dse.ldif

该文件使用 LDAP 数据交换格式 (LDIF) 以文本方式描述 LDAP 条目、属性以及它们的值。该文件中的目录服务器配置由以下部分组成：

- cn=config 条目的属性和值。
- 子树中 cn=config 下的所有条目及其属性和值。通常，条目或属性的存在是有意义的。
- 根条目 ("") 和 cn=monitor 条目的对象类和访问控制指令 (ACI)。这些条目的其他属性由服务器生成。

Directory Server 通过使用 LDAP 使所有配置设置变得可读和可写。默认情况下，只有 Administration Server 中定义的目录系统管理员和目录管理员才能访问目录的 cn=config 分支。这些管理用户可以像查看和修改任何其他目录条目一样查看和修改配置条目。

应该避免在 cn=config 条目下创建条目，因为它们将存储在 dse.ldif 文件中，而不像常规条目一样存储在高伸缩性的数据库中。因此，如果在 cn=config 的下面存储了许多条目 （尤其是那些可能需要经常更新的条目），性能将很可能会受到影响。然而，为了能集中配置信息，将特殊用户条目 （如 “复制管理员”（供应商绑定 DN）条目）存储在 cn=config, 下是十分有用的。

使用控制台修改配置

推荐采用的修改配置方法是使用 Directory Server 控制台的顶级 “配置”标签。该标签的面板和对话框提供基于任务的控件以帮助您快速而有效地设置配置。另外，控制台界面为您管理配置的复杂性和相互依赖性。

该文档中名为 “... 使用控制台”的步骤描述了配置的控制台界面。这些步骤介绍如何使用 “配置”标签的面板和对话框执行特定的管理任务。界面本身指明了如何保存配置和何时需要重新启动服务器以使更改生效。

从命令行修改配置

因为可通过 LDAP 访问 cn=config 子树，所以 ldapsearch、 ldapmodify 和 ldapdelete 命令可用于查看和修改服务器配置。可使用 “从命令行管理条目”（第 57 页）中说明的步骤和 LDIF 格式修改 cn=config 条目和其下的所有条目。

然而，必须了解这些条目的含义、其属性的目的和可以使用的值。这些重要的注意事项在本文档中名为 “从命令行 ...”的步骤中进行了说明。在这些步骤中，将为您展示配置条目及您可能设置的属性的示例。有关所有配置条目及属性的完整说明，包括允许的值的范围，请参阅 *Sun ONE Directory Server 参考手册*。

从命令行修改配置不像使用控制台那样简单。但是，一些很少使用的配置设置无法使用控制台进行修改，而仅能通过命令行步骤进行。也可以通过编写使用命令行工具的脚本来利用命令行步骤自动执行配置任务。

修改 dse.ldif 文件

`dse.ldif` 文件包含服务器启动和重新启动时将读取和使用的配置。该文件的 LDIF 内容为 `cn=config` 条目及其子树。只有安装过程中定义的系统用户能对该文件读取和写入。

通过直接编辑该文件的内容修改配置产生错误的可能性比较大，因此不推荐使用此方法。您应该了解以下行为：

- 启动时仅读取一次 `dse.ldif` 文件。此后，服务器配置即基于配置条目在内存中的 LDAP 映像来运作。因此，启动后对该文件所作的修改将在下一次重新启动后生效。
- 使用控制台或从命令行修改配置会更改配置的 LDAP 映像。某些目录功能在被调用时会读取当前的配置，因此不需要重新启动服务器。
- 每当配置的 LDAP 映像发生改变时，服务器都将写入 `dse.ldif` 文件。某些目录功能仅在服务器启动时读取其配置，因此写入文件能确保更改立即生效。

  现有的 `dse.ldif` 文件将被复制为 `dse.ldif.bak`，原有的 `dse.ldif.bak` 文件将被覆盖。因此，如果服务器重新启动之前通过 LDAP 对配置进行了更改，则对 `dse.ldif` 文件所作的任何手动更改都将丢失。
- 目录每次成功启动后， `dse.ldif` 文件都将被复制到位于同一位置的 `dse.ldif.startOK`。如果由于错误的配置更改而导致服务器无法启动，您将需要从此文件还原 `dse.ldif`。

使用控制台管理条目

您可以使用 Directory Server 控制台上的 “目录”标签和条目编辑器对话框，单独添加、修改或删除条目。如果想同时对多个条目执行操作，请参阅 “使用控制台执行批量操作”（第 56 页）。

有关启动 Directory Server 控制台和浏览用户界面的信息，请参阅 “使用 Directory Server 控制台”（第 22 页）。

创建目录条目

Directory Server 控制台为创建目录条目提供了几个自定义模板。每个模板都是一个用于特定类型对象类的自定义编辑器。表 2-1 列出了用于每个自定义编辑器的对象类。

表 2-1 条目模板与相应的对象类

模板	对象类
用户	inetOrgPerson（用于创建和编辑） organizationalPerson（用于编辑） person（用于编辑）
组	groupOfUniqueNames（可能还有其他的）用于动态组和证书组。
组织单位	organizationalUnit
角色	nsRoleDefinition 及其他取决于托管、过滤或嵌套角色的选择。
服务类	cosSuperDefinition 及其他取决于服务类的类型。
口令策略	passwordPolicy
引荐	referral

这些自定义编辑器所包含的字段表示所有必填属性以及它们各自的对象类的某些常用可选属性。要使用这些模板之一创建条目，请遵循 “使用自定义编辑器创建条目”（第 46 页）中的说明。要创建其他类型的条目，请参阅 “创建其他类型的条目”（第 48 页）。

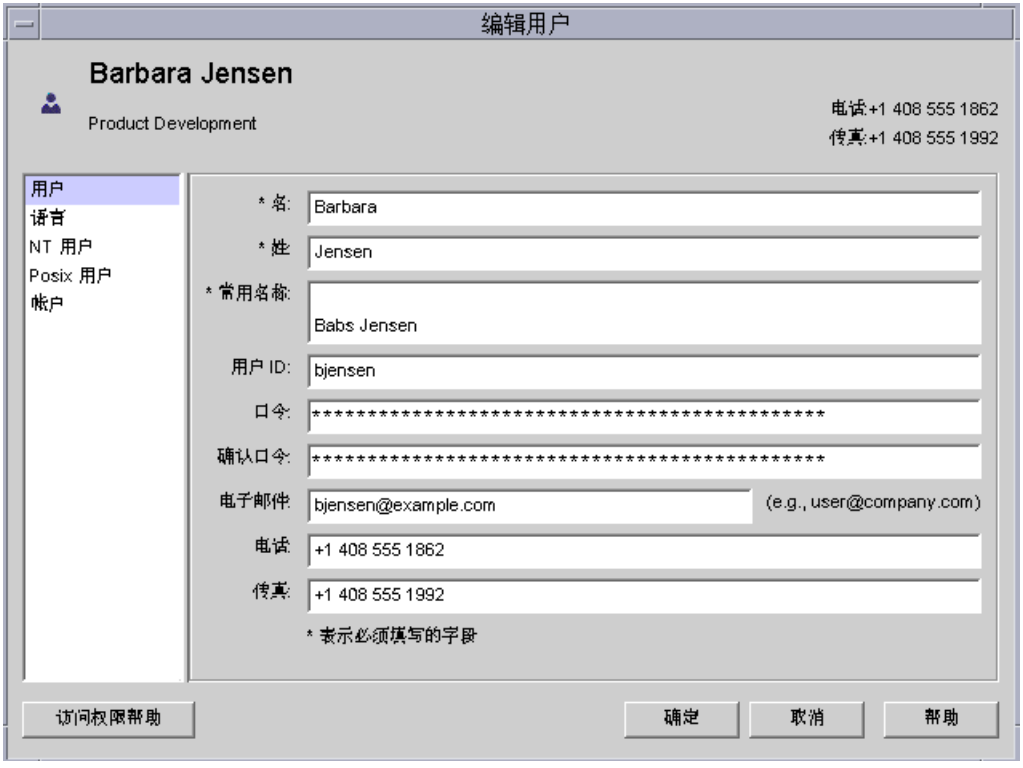
使用自定义编辑器创建条目

1. 在 Directory Server 控制台的顶级 “目录”标签上，展开目录树，显示要成为新条目的父级的条目。
2. 右键单击父条目，选择 “新建”菜单项，然后从子菜单中选择条目的类型：用户、组、组织单位、角色、服务类、口令策略或引荐。或者，可以左键单击父条目将其选中，然后从 “对象 > 新建”菜单中选择条目的类型。将显示选中的条目类型的自定义编辑器对话框。

自定义编辑器在左侧列中显示标签列表，而每个标签的字段则显示在右侧。默认情况下，所有自定义编辑器在打开的时候都会选中顶端的 “用户”或 “常规”标签，其中包含要命名和描述新条目的字段。

例如，下图显示用于用户条目的自定义编辑器：

图 2-1 Directory Server 控制台 - 用户条目的自定义编辑器



3. 在自定义编辑器的字段中，输入要提供的属性的值。必须为所有必填属性输入值，必填属性由字段名旁的星号 (*) 标识。可以将其他任何字段留空。在允许有多个值的字段中，可以键入回车来分隔值。

   单击 “帮助”按钮，获取条目类型的自定义编辑器中特定字段的详细帮助信息。有关 “用户”和 “组织单位”编辑器的 “语言”标签的说明，请参阅 “设置语言支持属性”（第 50 页）。

   有关创建组、角色和服务类条目的进一步说明，请参阅第 5 章 “高级条目管理”。有关创建口令策略的说明，请参阅第 7 章 “用户帐户管理”。有关创建引荐的说明，请参阅 “设置引荐”（第 66 页）。

4. 单击 “确定”创建新条目并关闭自定义编辑器对话框。新条目出现在目录树中。

5. 自定义编辑器对话框并不为其各自对象类的所有可选属性提供字段。如果希望添加未显示在自定义编辑器中的可选属性，请遵循 “使用通用编辑器修改条目”（第 50 页）中的说明。

创建其他类型的条目

遵循这些步骤创建除表 2-1 （第 46 页）中列出的对象类以外的任何对象类条目。也可以使用该步骤创建在目录模式中定义的任何自定义对象类的条目：

1. 在 Directory Server 控制台的顶级 “目录”标签上，展开目录树，显示要成为新条目的父级的条目。

2. 右键单击父条目，并从子菜单中选择 “新建” > “其他”项。或者，可以左键单击父条目将其选中，然后选择 “对象” > “新建” > “其他”菜单项。

   将显示 “新建对象”对话框。

3. 在 “新建对象”对话框的对象类列表中，选择一个定义新条目的对象类，然后单击 “确定”。

   如果选择表 2-1 （第 46 页）中列出的对象类，将显示相应的自定义编辑器（请参阅 “使用自定义编辑器创建条目”（第 46 页））。在所有其他情况下，将显示通用编辑器。

4. 创建新条目时，通用编辑器包含一个字段，该字段用于所选的对象类的每个必需的属性。必须为所有必需属性输入值。某些字段具有通用占位符，如 `New`，应当为您的条目将其替换为有意义的值。

5. 要定义所选对象类上允许的其他属性，必须显式地添加它们。要为可选的属性提供值，请执行以下操作：

   a. 单击 “添加属性”按钮，显示允许的属性的列表。

   b. 从 “添加属性”对话框中选择一个或多个属性，然后单击 “确定”。

   c. 在通用编辑器中的新属性名称旁输入值。

   有关该对话框中其他控件的详细信息，请参阅 “使用通用编辑器修改条目”（第 50 页）。

6. 默认情况下，必需属性之一会被选中作为命名属性，并出现在通用编辑器中显示的条目 DN 中。要更改命名属性，请执行以下操作：

   a. 单击 “更改”按钮，显示 “更改命名属性”对话框。

   b. 在属性表中，选中要在新条目 DN 中使用的一个或多个属性旁的复选框。

c. 在 “更改命名属性”对话框中单击 “确定”。通用编辑器中的 DN 显示使用所选命名属性的新 DN。

7. 在通用编辑器中单击 “确定”，保存新条目。

新条目在目录树中显示为父条目的子级。

使用自定义编辑器修改条目

对于表 2-1 （第 46 页）中列出的对象类，可以选择使用相应的自定义编辑器或通用编辑器编辑条目。使用自定义编辑器时，可以轻松访问最常用的字段，且界面会帮助您定义复杂属性的值，如角色或服务类定义中的值。

通用编辑器可以对条目执行更多的高级操作，如添加对象类、添加允许的属性和处理多值属性。要使用通用编辑器编辑条目，请参阅 “使用通用编辑器修改条目” （第 50 页）。

注意 自定义编辑器仅能用于编辑表 2-1 （第 46 页）中列出的对象类。包含其他结构对象类的条目 （例如从 `inetorgperson` 继承的自定义类）仅能通过通用编辑器进行编辑。

除了列出的对象类之一以外，还包含辅助对象类的条目，可以使用自定义编辑器进行管理。但是，所有由辅助类定义的属性在自定义编辑器中将不可见。有关辅助对象类的定义，请参阅 *Sun ONE Directory Server 参考手册* 第 9 章中的 “对象类”。

调用自定义编辑器

要编辑对象类在表 2-1 （第 46 页）中列出的条目，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “目录”标签上，展开目录树，显示要编辑的条目。
2. 双击该条目。还有其他几种方法也可以调用条目的自定义编辑器：
   - 右键单击该条目，并选择 “用自定义编辑器进行编辑”菜单项。
   - 左键单击该条目将其选中，然后选择 “对象” > “用自定义编辑器进行编辑”菜单项。
   - 左键单击该条目将其选中，然后使用键盘快捷键 Control-P。

   将显示条目对象类的自定义编辑器。例如，图 2-1（第 47 页）中显示了用户条目的自定义编辑器。

3. 默认情况下，所有自定义编辑器在打开的时候都会选中顶端的 “用户”或 “常规”标签，其中包含要命名和描述新条目的字段。在自定义编辑器的字段中，编辑或删除要修改的属性的值。可以修改，但不能删除必填属性的值，必填属性由字段名旁的星号 (*) 标识。可以将其他任何字段留空。在允许有多个值的字段中，可以键入回车来分隔值。

   选择左侧列中的其他标签，修改相应面板上的值。单击 “帮助”按钮，获取条目类型的自定义编辑器中特定字段的详细帮助信息。

   有关 “用户”和 “组织单位”编辑器的 “语言”标签的说明，请参阅 “设置语言支持属性”（第 50 页）。用户和组条目的 “帐户”标签字段在第 7 章 “用户帐户管理”中进行了说明。为 Directory Server 同步服务提供了 “NT 用户”和 “Posix 用户”标签，请与 Sun 代表联系以获取详细信息。

   有关修改组、角色和服务类条目的进一步说明，请参阅第 5 章 “高级条目管理”。有关修改口令策略的说明，请参阅第 7 章 “用户帐户管理”。有关修改引荐的说明，请参阅 “设置引荐”（第 66 页）。

4. 单击 “确定”保存对条目所作的更改并关闭自定义编辑器对话框。如果修改了命名属性，例如用户条目的通用名称，则更改将在目录树中反映出来。

设置语言支持属性

用户条目和组织单位条目的自定义编辑器都提供了用于国际化目录的语言支持。

1. 如 “调用自定义编辑器”（第 49 页）中所述打开条目的自定义编辑器。
2. 在左侧列中单击 “语言”标签。
3. 对于用户条目，可以使用下拉列表设置一种首选语言。
4. 对于用户条目和组织单位条目，您都可以在给定的字段中为列表中显示的任何语言输入本地化的值。选择一种语言，然后以该语言输入一个或多个值。当定义了本地化的值时，语言的名称将在列表中以粗体显示。

   某些语言还具有发音字段，可在其中输入本地化值的语音表示法。

5. 单击 “确定”保存对条目所作的更改并关闭自定义编辑器对话框。

使用通用编辑器修改条目

通用编辑器根据用于登录到控制台的绑定 DN，允许您查看条目的所有可读属性并编辑其可写属性。通用编辑器允许您添加和删除属性、设置多值属性以及管理条目的对象类。添加属性时，可以为二进制属性和语言支持定义子类型。

调用通用编辑器

要调用目录中任何条目的通用编辑器，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “目录” 标签上，展开目录树，以显示要编辑的条目。
2. 右键单击该条目，并选择 “用通用编辑器进行编辑” 菜单项。还有其他几种方法也可以调用通用编辑器：
   - 左键单击该条目将其选中，然后选择 “对象” > “用通用编辑器进行编辑” 菜单项。
   - 如果条目的对象类未在表 2-1 （第 46 页）中列出，请双击该条目。对于不具有自定义编辑器的对象类，默认情况下将使用通用编辑器。

   将显示通用编辑器，如下图中所示。

图 2-2 Directory Server 控制台 - 通用编辑器

在通用编辑器中，条目的属性按字母顺序列出，每个属性具有一个文本框，其中包含每个属性的值。所有属性 （包括只读属性和可操作属性）都会显示出来。右边的控件允许您修改编辑器的显示方式并编辑属性列表。

3. 或者，可以使用 “视图”框中的控件修改通用编辑器的显示方式。

   - 选择 “显示属性名称”选项以查看属性的名称，该名称是最先在模式中定义的名称。将重新安排属性列表，以便按名称的字母顺序排列。
   - 选择 “显示属性说明”选项，按照其属性的备用名称 （如果已在模式中定义）列出属性。备用名称通常是属性更清楚明了的说明。将重新安排属性列表，以便按说明的字母顺序排列。
   - 取消选中 “仅显示具有值的属性”复选框，列出所有由条目对象类的模式明确允许的属性。如果该条目包括 `extensibleObject` 对象类，则所有条目将暗中允许，但不会列出。默认情况下，仅显示具有定义值的属性。
   - 选中或取消选中 “显示 DN”复选框，切换属性列表下条目的标识名称的显示。
   - “刷新”按钮将访问服务器以根据条目当前内容更新所有属性的值。

警告 单击 “刷新”按钮将立即删除在通用编辑器中所做的所有修改，而不进行保存。

以下小节说明用于设置属性值、管理对象类和更改条目的命名属性的控件。

修改属性值

1. 如 “调用通用编辑器”（第 51 页）中所述，打开通用编辑器。
2. 滚动查看属性列表并单击要修改的值。

   选中的属性将突出显示，且编辑光标出现在包含所选值的文本字段中。
3. 使用鼠标和键盘将文本编辑为所需的值。可使用系统的剪贴板在该字段中复制、剪切和粘贴文本。

   如果不能编辑文本字段中的内容，则属性为只读或没有写权限以修改属性。
4. 对该条目编辑其他任何值或执行其他所需修改，然后单击 “确定”，以保存更改并关闭通用编辑器。

编辑多值属性

在目录模式中定义为多值的属性在通用编辑器中可具有多值字段。详细信息，请参阅第 9 章 “扩展目录模式”。

要为多值属性添加一个新值，请执行以下操作：

1. 如 “调用通用编辑器”（第 51 页）中所述，打开通用编辑器。
2. 滚动属性列表，单击属性或属性的一个值。所选属性突出显示，且激活了 “添加值”按钮。如果该按钮未激活，则所选属性未定义为多值属性，或属性为只读，或者您不具有写权限，无法修改属性。
3. 单击 “添加值”按钮。列表中属性名称旁边将显示一个新的空白文本字段。
4. 在新文本字段中输入该属性的新值。可使用系统的剪贴板在该字段中复制、剪切和粘贴文本。
5. 对该条目编辑其他任何值或执行其他所需修改，然后单击 “确定”，保存更改并关闭通用编辑器。

要删除多值属性的一个值，请执行以下操作：

1. 如 “调用通用编辑器”（第 51 页）中所述，打开通用编辑器。
2. 滚动查看属性列表并单击要删除的特定值。所选属性突出显示，且激活了 “删除值”按钮。如果该按钮未激活，则所选属性为只读，或者您不具有写权限，无法修改属性。
3. 单击 “删除值”按钮。包含所选值的文本字段被删除。
4. 对该条目编辑其他任何值或执行其他所需修改，然后单击 “确定”，保存更改并关闭通用编辑器。

添加属性

条目必须包含需要或允许该属性的对象类，您才能向其中添加属性。详细信息，请参阅 “管理对象类”（第 54 页）和第 9 章 “扩展目录模式”。

要向条目中添加属性，请执行以下操作：

1. 如 “调用通用编辑器”（第 51 页）中所述，打开通用编辑器。
2. 确保 “仅显示具有值的属性”选项已选中。
3. 单击 “添加属性”按钮，显示带有属性列表的对话框。该列表仅包含为条目定义的对象类所允许的属性。
4. 在 “添加属性”对话框中，选择要添加的一个或多个属性。
5. 或者，可从对话框顶部的下拉列表中选择以下两种子类型或其中之一：
   - Language 子类型 - 使用该子类型表示属性的值中使用的语言。可使用不同的语言多次添加属性以在目录中存储本地化信息。

或者，在 language 子类型的基础上，还可选择 Pronunciation 子类型表示该属性的值包含与给定语言的值相当的语音。

- Binary 子类型 - 为属性分配 binary 子类型表示该属性值是二进制数据。虽然可以无需 binary 子类型而在属性中存储二进制数据，但它向客户机表示可能存在多种属性类型。

6. 选择属性及其可选的子类型后，请单击 “确定”。属性即按字母顺序添加到通用编辑器中的列表中。
7. 在新属性名称旁的空白文本字段中为该属性输入一个新值。可使用系统的剪贴板在该字段中复制、剪切和粘贴文本。
8. 对该条目编辑其他任何值或执行其他所需修改，然后单击 “确定”，以保存更改并关闭通用编辑器。

删除属性

要从条目中删除属性及其所有值，请执行以下操作：

1. 如 “调用通用编辑器”（第 51 页）中所述，打开通用编辑器。
2. 滚动查看属性列表并单击要删除的属性名称。所选属性突出显示，且 “删除属性”按钮被激活。如果该按钮未激活，则所选属性为只读，或者您不具有写权限，无法修改属性。

注意 通用编辑器允许您删除对象类所需的属性，该对象类可能为此属性定义。如果试图在没有所需对象类的情况下保存条目，则服务器将响应 “对象类违规”。确保条目包括所有定义的对象类的所需属性。

3. 单击 “删除属性”按钮。将删除属性及其所有文本字段值。
4. 对该条目编辑其他任何值或执行其他所需修改，然后单击 “确定”，保存更改并关闭通用编辑器。

管理对象类

条目的对象类由多值 `objectclass` 属性定义。修改该属性时，通用编辑器提供特殊的对话框以帮助管理定义的对象类。

要向条目中添加对象类，请执行以下操作：

1. 如 “调用通用编辑器”（第 51 页）中所述，打开通用编辑器。
2. 滚动查看属性列表，然后选择 `objectclass` 属性。“添加值”按钮被激活。如果该按钮未激活，则说明您没有权限修改该条目的对象类。

3. 单击 “添加值”按钮。

   将显示 “添加对象类”对话框。它会显示可向条目中添加的对象类的列表。

4. 选择要添加到该条目的一个或多个对象类，并单击 “确定”。所选对象类将出现在 `objectclass` 属性值的列表中。

5. 如果新的对象类需要未存在于条目中的属性，则通用编辑器将自动添加这些属性。必须为所有必需属性提供值。

6. 对该条目编辑其他任何值或执行其他所需修改，然后单击 “确定”，保存更改并关闭通用编辑器。

要从条目中删除对象类，请执行以下操作：

1. 如 “调用通用编辑器”（第 51 页）中所述，打开通用编辑器。

2. 滚动查看属性列表并单击要删除的 `objectclass` 属性的特定值。如果模式允许删除所选的对象类，且您具有修改该条目的对象类的权限，则 “删除值”按钮将被激活。

3. 单击 “删除值”按钮。特定的对象类被删除。

   删除对象类时，通用编辑器将自动删除剩下的对象类不允许或不需要的所有属性。如果删除了命名属性之一，将自动选中另一个，且控制台将把此更改告知您。

4. 对该条目编辑其他任何值或执行其他所需修改，然后单击 “确定”，保存更改并关闭通用编辑器。

重命名条目

命名属性是出现在条目的标识名称 (DN) 中的条目属性值对。命名属性从条目的现有属性中进行选择。修改命名属性以重命名条目：

1. 如 “调用通用编辑器”（第 51 页）中所述，打开通用编辑器。

   “更改”按钮旁的文本显示了该条目当前的命名属性。如果选中了 “显示 DN”复选框，则您可以在属性值列表下的 DN 中查看这些属性。

2. 单击 “更改”按钮。如果该按钮未激活，则说明您不具有重命名该条目的权限。

   显示 “更改命名属性”对话框。

3. 滚动查看属性列表，选择希望该条目的 DN 具有的属性。分别选中或取消选中属性旁的复选框以从命名属性中添加或删除该属性。

同一父级下的条目 DN 必须是唯一的。因此，必须选择值或值组合为唯一的命名属性。如果条目的 DN 不唯一，服务器将拒绝保存该条目。按照约定，所有条目 （如那些代表用户的条目）应该使用相同的命名属性。

4. 在 “更改命名属性”对话框中单击 “确定”。通用编辑器中会显示该条目的新 DN。
5. 对该条目编辑其他任何值或执行其他所需修改，然后单击 “确定”，保存更改并关闭通用编辑器。

删除目录条目

要使用 Directory Server 控制台删除条目，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “目录”标签上，展开目录树，显示要删除的条目。

   也可以通过选中子树的根节点来删除目录的整个分支。

2. 右键单击该条目并选择 “删除”菜单项。还有其他几种操作也可以删除条目：

   - 左键单击该条目将其选中，然后选择 “编辑” > “删除”菜单项。如果希望将该条目粘贴到目录中的其他地方，也可以使用 “编辑” > “剪切”菜单项。
   - 左键单击该条目将其选中，然后使用键盘快捷键 Control-D。

   如果您已经选择了 “视图” > “布局”选项以在 Directory Server 控制台的右侧面板中显示子级，则可以按住 Control 键或 Shift 键单击以选择多个条目进行删除。

3. 确认您希望删除条目或子树及其所有内容。

   服务器会立即删除条目。条目删除后不可恢复。如果删除多个条目，控制台将显示一个信息对话框，其中包含删除的条目数目以及删除过程中可能发生的错误。

使用控制台执行批量操作

可以使用 LDIF 文件添加多个条目、执行混合操作或导入整个后缀。要使用 LDIF 文件和 Directory Server 控制台来添加条目，请执行以下操作：

1. 使用前一节中显示的语法在 LDIF 文件中定义条目或操作。如果仅添加条目或初始化后缀，则您不需要 `changetype` 关键字，且 LDIF 文件可能仅包含条目。如果执行混合操作，则每个 DN 后都应跟一个 `changetype` 以及特定的操作或属性值 （如果适用）。
2. 从 Directory Server 控制台导入 LDIF 文件。详细信息，请参阅 “导入 LDIF 文件”（第 118 页）。

   如果执行混合操作，一定要取消选中 “导入 LDIF”对话框上的 “仅添加”，这样服务器才能执行所有的 LDIF 操作。

从命令行管理条目

`ldapmodify` 和 `ldapdelete` 命令行公用程序提供完整的功能性，用于添加、编辑和删除目录内容。可以使用它们管理服务器的配置条目和用户条目中的数据。这些公用程序还可以用于编写脚本，以便对一个或多个目录执行批量管理。

全书中的步骤都用到了 `ldapmodify` 和 `ldapdelete` 命令。以下各节说明了执行这些管理步骤所需的所有基本操作。更多功能、所有的命令行选项以及这些命令的返回值在 *Sun ONE Directory Server Resource Kit 工具参考* 的第 4 章 “ldapmodify”和第 5 章 “ldapdelete”中进行了说明。

对这些命令行公用程序的输入总是采用 LDAP 数据交换格式 (LDIF)，您可以直接从命令行输入或通过输入文件输入。 LDIF 是条目、属性以及它们的值的文本表示。LDIF 是一种标准格式，在 RFC 2849 (`http://www.ietf.org/rfc/rfc2849.txt`) 中对其进行了说明。以下小节提供了有关 LDIF 输入的信息，而后继的小节则说明了每种修改类型的 LDIF。

提供 LDIF 输入

向命令行公用程序提供 LDIF 时，请记住一些关于命令行输入、特殊字符、模式检查以及条目的顺序和大小的特殊注意事项。

在命令行上终止 LDIF 输入

`ldapmodify` 和 `ldapdelete` 公用程序读取您在命令后输入的 LDIF 语句的方式与从文件读取时相同。提供输入完成后，请输入您的 shell 将其识别为文件结束 (EOF) 转义序列的字符。

通常，根据操作系统的具体情况， EOF 转义序列为以下几种之一：

- UNIX - 几乎始终为 Control-D (^D)。
- Windows - 通常为 Control-Z 后接回车 (^Z<Return>)。

以下示例说明如何在 UNIX 系统上终止对 ldapmodify 命令的输入：

```
prompt> ldapmodify -h 主机 -p 端口 -D bindDN -w 口令
dn:cn=Barry Nixon,ou=People,dc=example,dc=com
changetype:modify
delete:telephonenumber
^D
prompt>
```

出于简化性以及可移植性的考虑，本文档中的示例未显示提示或 EOF 序列。

使用特殊字符

在命令行上输入命令选项时，您可能需要对对于命令行解释器具有特殊意义的字符执行转义操作，如空格 ( )、星号 (*)、反斜杠 (\) 等。例如，很多 DN 包含空格，且对于大多数 UNIX shell，您必须用双引号 ("") 将值括起来。

```
-D "cn=Barbara Jensen,ou=Product Development,dc=example,dc=com"
```

根据命令行解释器的具体情况，应使用单引号或双引号达到此目的。详细信息，请参阅操作系统文档。

另外，如果使用包含逗号的 DN，则必须用反斜杠 (\) 对逗号进行转义。例如：

```
-D "cn=Patricia Fuentes,ou=People,o=example.com Bolivia\,S.A."
```

请注意 ldapmodify 命令后的 LDIF 语句由命令而不是 shell 来解释，所以不需要考虑特殊的注意事项。

模式检查

添加或修改条目时，您使用的属性必须是条目中的对象类必需或允许的，且属性必须包含匹配其定义语法的值。

修改条目时， Directory Server 对整个条目执行模式检查，而不仅仅是对正被修改的属性进行检查。因此，如果条目中任何对象类或属性不符合模式要求，则操作可能会失败。详细信息，请参阅 “模式检查”（第 289 页）。

LDIF 条目排序

在用于添加条目的 LDIF 文本的任何序列中 （不管是在命令行上还是文件中），父条目必须在其子级之前列出。这样，当服务器处理 LDIF 文本时，它将在子条目之前创建父条目。

例如，如果要在不存在于目录中的 “人员”子树中创建条目，然后在子树中的条目前列出代表 “人员”容器的条目，请执行以下操作：

```
dn:dc=example,dc=com
dn:ou=People,dc=example,dc=com
...
People subtree entries
...
dn:ou=Group,dc=example,dc=com
...
Group subtree entries
...
```

可以使用 `ldapmodify` 命令行公用程序在目录中创建任何条目，但是，后缀或子后缀的根条目是一个特殊的条目，它必须与必需的配置条目相关联。要添加新的根后缀或子后缀及其相关配置条目，请参阅 “从命令行创建后缀”（第 83 页）。

管理大型条目

添加或修改具有非常大的属性值的条目之前，可能需要配置服务器以接受它们。为防止服务器超过负载，默认情况下客户机被限制为只能发送不大于 2 MB 的数据。

如果添加大于 2 MB 的条目，或将属性修改为大于 2 MB 的值，服务器将拒绝执行此操作并立即关闭连接。例如，二进制数据 （如条目的一个或多个属性中的多媒体内容）可能会超过此限制。

定义了一个大型静态组的条目也可能包括过多的成员，以致它们的表示会超出此限制。但是，出于性能考虑，不推荐使用这样的组，您应该考虑重新设计目录结构。详细信息，请参阅 “管理组”（第 136 页）。

要修改服务器强制执行的客户机发送数据的大小限制，请执行以下操作：

1. 为 `cn=config` 条目的 `nsslapd-maxbersize` 属性设置新值。

- 要使用控制台执行此操作，请以 “管理员”或 “目录管理员”的身份登录，并按照 “使用通用编辑器修改条目”（第 50 页）中所述的步骤编辑 `cn=config` 条目。将 `nsslapd-maxbersize` 属性设为客户机可以一次发送的最大字节数。
- 要从命令行执行此操作，请使用以下命令：

  ```
  ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
  dn:cn=config
  changetype:modify
  replace:nsslapd-maxbersize
  nsslapd-maxbersize:sizeLimitInBytes
  ```

  详细信息，请参阅 *Sun ONE Directory Server 参考手册* 第 4 章中的 “`nsslapd-maxbersize`”。

2. 如 “启动和停止 Directory Server”（第 20 页）中所述，重新启动服务器。

错误处理

命令行工具按顺序处理 LDIF 输入中的所有条目或修改。默认行为是当第一个错误发生时停止处理。使用 `-c` 选项继续处理所有输入而不管任何错误。在工具的输出中将看到错误状态。

除了以上列出的注意事项，常见错误有：

- 不具有适当的操作访问权限。
- 添加条目的 DN 在目录中已存在。
- 将条目添加到一个不存在的父级下面。

有关错误状态和如何避免这些错误的详细信息，请参阅 *Sun ONE Directory Server Resource Kit 工具参考* 的第 4 章 “ldapmodify”和第 5 章 “ldapdelete”。

使用 ldapmodify 添加条目

可使用 `ldapmodify` 的 `-a` 选项将一个或多个条目添加到目录。以下示例创建一个结构条目以包含用户，然后创建一个用户条目：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:ou=People,dc=example,dc=com
objectclass:top
objectclass:organizationalUnit
ou:People
description:Container for user entries

dn:uid=bjensen,ou=People,dc=example,dc=com
objectclass:top
objectclass:person
objectclass:organizationalPerson
objectclass:inetorgPerson
uid:bjensen
givenName:Barbara
sn:Jensen
cn:Babs Jensen
telephoneNumber: (408) 555-3922
facsimileTelephoneNumber: (408) 555-4000
mail:bjensen@example.com
userPassword:clearPassword
```

-D 和 -w 选项分别给出具有权限创建这些条目的用户的绑定 DN 和口令。 -a 选项表示将添加 LDIF 中的所有条目。然后每个条目由其 DN 和属性值给定，每个条目间有一个空白行。 ldapmodify 公用程序在条目输入和报告所有错误后将创建每个条目。

按照约定，条目的 LDIF 按照以下顺序列出属性：

- 对象类列表。
- 命名属性或属性。这是在 DN 中使用的属性，且不一定是必需的属性。
- 所有对象类的必需属性列表。
- 所有希望包含的允许的属性。

当为 userpassword 属性输入值时，请给出明文形式的口令。服务器会将该值加密并仅存储加密值。一定要限制读取权限以保护 LDIF 文件中的明文口令。

也可使用 LDIF 的另一种形式，该形式在命令行中不需要 -a 选项。该形式的优点是可将条目条件和下一段中显示的条目修改语句合并。

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:ou=People,dc=example,dc=com
changetype:add
objectclass:top
objectclass:organizationalUnit
ou:People
description:Container for user entries

dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:add
objectclass:top
objectclass:person
objectclass:organizationalPerson
objectclass:inetorgPerson
uid:bjensen
givenName:Barbara
sn:Jensen
cn:Barbara Jensen
telephoneNumber: (408) 555-3922
facsimileTelephoneNumber: (408) 555-4000
mail:bjensen@example.com
userPassword:clearPassword
```

changetype:add 关键字表示具有给定 DN 的条目在创建时应带有所有后续的属性。所有其他选项和 LDIF 约定都一样。

两个示例中都可使用 `-f` *filename* 选项从文件读取 LDIF，而非从终端输入。按照 `-a` 选项的用法， LDIF 文件必须包含与终端输入相同的格式。

使用 ldapmodify 修改条目

使用 `changetype:modify` 关键字添加、替换或删除现有条目中的属性及其值。当指定 `changetype:modify` 时，必须也提供一个或多个更改操作以表示条目将如何修改。以下示例中显示了三个可能的 LDIF 更改操作：

```
dn:entryDN
changetype:modify
add:attribute
attribute:value
...
-
replace:attribute
attribute:newValue
...
-
delete:attribute
[attribute:value]
...
```

在一行中使用连字号 (-) 以分开在同一条目上的操作，使用一空白行分开多组在不同条目上的操作。也可为每个操作给出多个 *attribute*：*value* 对以同时添加、替换或删除它们。

添加属性值

以下示例显示如何使用同一 `add` LDIF 语法将值添加到现有多值属性中或尚不存在的属性中：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
add:cn
cn:Babs Jensen
-
add:mobile
mobile: (408) 555-7844
mobile: (408) 555-7845
```

处于以下情况时，这些操作可能失败且服务器将返回一个错误：

- 属性的给定值已存在。

- 值未遵从为属性定义的语法。
- 属性类型不是条目的对象类必需的或允许的。
- 属性类型不是多值的且属性已有一个值。

添加二进制属性值

二进制属性值以 *attribute*;binary 子类型标记。虽然该子类型不是必需的，但可帮助用户和客户机确定属性的内容。可在与 ldapmodify 命令一起使用的任何 LDIF 语句中为属性名称添加适当的子类型。

要输入二进制值，可直接在 LDIF 文本中输入或从另一个文件中读取。以下示例显示了从文件读取二进制值的 LDIF 语法：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
version: 1
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
add:jpegphoto;binary
jpegphoto;binary:< file:///path/filename.jpg
```

< 前后的空格非常重要，必须完全按照显示的形式保留空格。要使用 < 语法来指定文件名，您必须以行 version:1 作为 LDIF 语句的开头。 ldapmodify 处理此语句时，会将该属性设置为可以从给定文件的全部内容中读取的值。

添加具有 Language 子类型的属性

属性的 Language 和 pronunciation 子类型指定本地化的值。当为属性指定 language 子类型时，该子类型将按照以下方式添加到属性名称中：

attribute;lang-*CC*

其中 *attribute* 是现有属性类型， *CC* 是两个字母的国家 （地区）代码以指定语言。可选择为 language 子类型添加 pronunciation 子类型以指定本地化值的等效语音。在这种情况下，属性名称变为：

attribute;lang-*CC*;phonetic

要对具有子类型的属性执行操作，必须明确地匹配其子类型。例如，如果要修改包含 lang-fr language 子类型的属性值，则必须按如下所示在修改操作中包含 lang-fr:

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
replace:homePostalAddress;lang-fr
homePostalAddress;lang-fr:34\, avenue des Champs-Elysées
```

修改属性值

以下示例显示如何使用 LDIF 中的 `replace` 语法修改单值属性和多值属性的所有值：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
replace:sn
sn:Morris
-
replace:cn
cn:Barbara Morris
cn:Babs Morris
```

当使用 `replace` 语法时，将删除指定属性的所有当前值并添加所有给定值。

删除属性值

以下示例显示如何完全删除属性和仅删除多值属性的值：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
delete:facsimileTelephoneNumber
-
delete:cn
cn:Babs Morris
```

当使用 `delete` 语法而未指定 *attribute:value* 对时，将删除属性的所有值。如果指定一对 *attribute:value*，则将仅删除该值。

修改多值属性的值

为了使用 `ldapmodify` 命令修改多值属性的值，必须执行以下示例中显示的两个操作：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
delete:mobile
mobile: (408) 555-7845
-
add:mobile
mobile: (408) 555-5487
```

使用 ldapmodify 重命名条目

当为条目重命名时，将修改条目的相对标识名称 (RDN)，该名称位于条目 DN 中的 *attribute=value* 对的最左边。该属性称为命名属性，且必须以同一值存在于条目的属性中。

当为条目重命名时，不能更改 DN 的其他任何部分 （如将条目移动到不同的子树）。要将条目移至完全不同的分支，必须使用旧条目的属性在其他子树中创建新条目，然后删除旧条目。

也不能重命名具有任何子条目的条目，因为父条目的 RDN 已用在子条目的 DN 中，且 DN 中的所有条目必须存在。要删除整个树，必须在新位置重建树。

使用 `changetype:modrdn` 关键字在 LDIF 语句中重命名条目。以下示例将为 Barbara Morris 重命名 `uid` 命名属性：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modrdn
newrdn:uid=bmorris
deleteoldrdn: 1
```

`newrdn` 行使用 *attribute=value* 语法给出新的命名属性。 `deleteoldrdn` 行表示是否应同时将前命名属性从条目中删除 （`1` 为是， `0` 为否）。在两种情况下，新的命名属性都将被添加到条目。

使用 ldapdelete 删除条目

使用 `ldapdelete` 命令行公用程序从目录中删除条目。此公用程序绑定到目录服务器并删除一个或多个由其 DN 给定的条目。必须提供具有权限以删除指定条目的绑定 DN。

基于同样的原因，不能重命名父条目，不能删除具有子条目的条目。 LDAP 协议禁止出现子条目将不再拥有父条目的情形。例如，不能删除组织单位条目，除非首先删除了属于组织单位的所有条目。

警告 不要删除后缀 `o=NetscapeRoot`。 Sun ONE Administration Server 使用此后缀存储有关已安装的 Sun ONE 服务器的信息。删除此后缀会强制您重新安装所有的 Sun ONE 服务器，包括目录服务器。

以下示例中，组织单位中仅有一个条目，因此可删除它，然后删除父条目：

```
ldapdelete -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
uid=bjensen,ou=People,dc=example,dc=com
ou=People,dc=example,dc=com
```

使用 ldapmodify 删除条目

也可使用 `changetype:delete` 关键字以使用 ldapmodify 公用程序删除条目。当使用以上说明的 `ldapdelete` 时，也同样具有这些限制。使用 LDIF 语法删除条目的优点在于，您可以在单个 LDIF 文件中执行混合操作。

下面的示例将执行与前面的示例相同的删除操作：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:delete

dn:ou=People,dc=example,dc=com
changetype:delete
```

设置引荐

使用引荐告诉客户机应用程序在信息本地不可用时应联系哪个服务器。引荐是指向远程后缀或条目的指针， Directory Server 将其作为结果返回到客户机。然后，客户机必须在引荐中指定的远程服务器上再次执行该操作。在三种情况下，会发生重定向：

- 当客户机应用程序请求一个本地服务器上不存在的条目时，服务器将返回默认引荐。
- 当整个后缀由于安全原因或需要维护而脱机时，服务器将返回该后缀定义的引荐。后缀级的引荐在 “设置访问权限和引荐”（第 87 页）中进行了说明。当客户机请求写入操作时，后缀的只读副本也会将引荐返回到主服务器。
- 可以创建名为智能引荐的条目。当客户机专门访问智能引荐时，服务器将返回其定义的引荐。 Directory Server 控制台自动采用智能引荐，所以它们作为本地条目出现在顶级 “目录”标签上。

在所有情况下，引荐即包含主机名、端口号以及其他服务器上的 DN （可选）的 LDAP URL。详细信息，请参阅 *Sun ONE Directory Server 参考手册* 中的附录 D “LDAP URL”。有关如何在目录部署中使用引荐的概念性信息，请参阅 *Sun ONE Directory Server 部署指南*。

以下小节说明定义目录的默认引荐和智能引荐的过程。

设置默认引荐

当客户机应用程序提交一个 DN 上的操作，而由目录维护的任何后缀都不包含此 DN 时，会将默认引荐返回到客户机应用程序。默认引荐有时称为全局引荐，因为默认引荐应用于目录中的所有后缀。服务器将返回所有定义的引荐，但返回的顺序没有定义。

使用控制台设置默认引荐

1. 在 Directory Server 控制台的顶级 “配置”标签上，选择配置树根的服务器节点，然后在右侧面板中选择 “网络”标签。
2. 选中 “返回引荐”复选框，并在文本字段中输入 LDAP URL。或者，单击 “构造 URL”以指导定义 LDAP URL。到安全端口的 LDAP URL 示例如下：

   ```
   ldaps://east.example.com:636/dc=example,dc=com
   ```

   可输入多个用空格分隔并用引号括起的引荐 URL，如下所示：

   ```
   "ldap://east.example.com:389/" "ldap://backup.example.com:389/"
   ```

3. 单击 “保存”以使更改立即生效。

从命令行设置默认引荐

使用 `ldapmodify` 命令行公用程序将一个或多个默认引荐添加或替换到目录配置文件中的 `cn=config` 条目。例如：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=config
changetype:modify
replace:nsslapd-referral
nsslapd-referral:ldap://east.example.com:389/
nsslapd-referral:ldap://backup.example.com:389/
```

无需重新启动服务器。

创建智能引荐

智能引荐允许将目录条目或目录树映射到特定的 LDAP URL。使用智能引荐，可将客户机应用程序引荐到特定服务器或特定服务器上的特定条目。

通常，智能引荐指向实际的条目，该条目在另一个服务器上有相同的 DN。然而，可定义对相同服务器或不同服务器上的任何条目的智能引荐。例如，可定义具有以下 DN 的条目：

```
uid=bjensen,ou=People,dc=example,dc=com
```

作为指向服务器 `east.example.com` 上的另一个条目的智能引荐。

```
cn=Babs Jensen,ou=Sales,o=east,dc=example,dc=com
```

目录使用智能引荐的方法符合 RFC 2251 (`http://www.ietf.org/rfc/rfc2251.txt`) 4.1.11 小节中指定的标准。

使用控制台创建智能引荐

1. 在 Directory Server 控制台的顶级 “目录”标签上，展开目录树，显示要成为智能引荐的父级的条目。
2. 右键单击父条目，选择 “新建” > “引荐”菜单项。或者，可以左键单击父条目将其选中，然后选择 “对象” > “新建” > “引荐”菜单项。显示引荐条目的自定义编辑器对话框。

   显示引荐的自定义编辑器。
3. 在编辑器的 “常规”标签上，输入引荐的名称并从下拉列表中选择其命名属性。该名称将成为所选的命名属性的值。也可选择输入引荐的说明字符串。
4. 在编辑器的 “URL”标签上，单击 “构造”按钮以定义智能引荐的 URL。在显示的对话框中输入 LDAP URL 的元素。

   URL 的元素包括持有引荐条目的目录服务器的主机名和 LDAP 端口号，以及服务器上目标条目的 DN。默认情况下，目标 DN 就是智能引荐条目的 DN。不过，目标 DN 可为任何后缀、子树或叶条目。
5. 在 LDAP URL 构造对话框中单击 “确定”。 URL 显示在新引荐文本框中。
6. 单击新引荐文本框旁的 “添加”按钮，将引荐添加到列表中。
7. 可定义多个 URL 以作为该条目的引荐返回。使用 “构造”、“添加”、“删除”和 “更改”按钮创建和管理 “引荐列表”。
8. 单击 “引荐验证”按钮显示对话框，其中可设置凭证， Directory Server 控制台将使用此凭证更随引荐以绑定到远程服务器。可定义访问服务器时要使用的绑定 DN 和口令。所有对同一服务器的引荐将使用相同的凭证。
9. 使用 “添加”、“编辑”和 “删除”按钮管理服务器列表和相应的凭证。完成后单击 “确定”。
10. 在引荐的自定义编辑器中，单击 “确定”以保存智能引荐条目。

在控制台的目录树中，应可在智能引荐条目的位置看到目标子树或目标条目。如果智能引荐条目上有黄色警告图标，则 URL 或凭证无效。双击条目，当看到“引荐错误”时单击“继续”，并修改 URL 或“引荐验证”以更正错误。

从命令行创建智能引荐

要创建智能引荐，请使用 `referral` 对象类和 `extensibleObject` 对象类创建条目。引荐对象类允许 `ref` 属性，该属性将包含 LDAP URL。`extensibleObject` 对象类允许您使用任何模式属性作为命名属性，从而匹配目标条目。

例如，定义以下条目以返回智能引荐，而非条目 `uid=bjensen`：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
objectclass:top
objectclass:extensibleObject
objectclass:referral
uid:bjensen
ref:ldap://east.example.com/cn=Babs%20Jensen,ou=Sales,
 o=east,dc=example,dc=com
```

注意 服务器将忽略 LDAP URL 中空格后的所有信息。基于这个原因，必须在要作为引荐使用的 LDAP URL 内使用 `%20` 以代替空格。

定义了智能引荐后，对 `uid=bjensen` 条目的修改将实际在另一个服务器的 `cn=Babs Jensen` 条目上执行。`ldapmodify` 命令将自动更随引荐，例如：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:replace
replace:telephoneNumber
telephoneNumber: (408) 555-1234
```

为了修改智能引荐条目，必须使用 `ldapmodify` 的 `-M` 选项，例如：

```
ldapmodify -M -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:replace
replace:ref
ref:ldap://east.example.com/cn=Babs%20Jensen,ou=Marketing,
 o=east,dc=example,dc=com
```

为属性值加密

属性加密是 Sun ONE Directory Server 5.2 中的新功能，它在敏感数据存储于目录中时对其进行保护。属性加密允许您指定条目的某些属性以加密格式进行存储。这将防止数据存储在数据库文件、备份文件和导出的 LDIF 文件时可读。

使用此功能，属性值会在存储于 Directory Server 中之前被加密，并在返回之前解密。应当使用 ACI 之类的其他机制以防止 LDAP 客户访问受限数据，使用 SSL 加密通讯。有关数据安全性常规信息和属性加密详细信息的结构性概述，请参阅 *Sun ONE Directory Server 部署指南* 中的第 7 章 “设计安全目录”。

仅当服务器上配置并启用了 SSL 时，属性加密才有效。但是，在默认情况下所有属性都是不加密的。属性加密在后缀级别进行配置。这意味着属性加密应用于它在其中显示为某一后缀的所有条目。如果要在整个目录中对属性进行加密，则必须对每个后缀中的该属性启用加密。

警告 属性加密将影响到与后缀相关联的所有数据和索引文件。如果修改了现有后缀的加密配置，您必须首先导出其内容，进行配置更改，然后重新导入内容。控制台将帮助您执行这些步骤。

此外，当启用加密时，必须手动删除数据库缓存文件，该文件可能仍然包含未加密的值。

最好在以新的后缀加载或创建数据之前启用加密属性。

如果选择加密一个属性，且该属性是某些条目的命名属性， DN 中显示的值将不加密，但条目中存储的值将被加密。

可选择 `userPassword` 属性用于加密，不过这不会真正提高安全性，除非口令是以明文方式存储的，如 DIGEST-MD5 SASL 验证。如果口令已具有口令策略中定义的加密机制，则进一步的加密对安全性不会提高太多，反而会影响每个绑定操作的性能。

使用控制台配置属性加密

1. 在 Directory Server 控制台中选择 “配置”标签，展开 “数据”节点，然后选择要加密属性值的后缀。在右侧面板中选择 “属性加密”标签。

   该标签包含一个表格，表格中列出了此后缀的所有当前已加密的属性的名称和加密模式。

2. 要启用属性的加密，请执行以下操作：

a. 单击 “添加属性”按钮，显示属性列表。

b. 从列表中选择要加密的属性并单击 “确定”。该属性将被添加到表格的 “属性名称”列中。

c. 从属性名称旁边的下拉列表中选择此属性的 “加密模式”。

3. 要使属性不再加密，请从表格中选择属性名称，并单击 “删除属性”按钮。

4. 单击 “保存”。系统会提示您在修改配置之前将后缀的内容导出到 LDIF 文件。

5. 单击 “导出后缀”打开 “导出”对话框，或单击 “继续”修改属性加密配置而不进行导出操作。新配置随后将被保存。

   如果还未导出后缀，则必须现在导出以保存其内容。当您计划使用该 LDIF 文件在下一步中重新初始化后缀时，如果后缀包含加密属性，则可在已导出的 LDIF 中继续保持加密。

   系统现在会提示您从 LDIF 文件初始化后缀。

6. 单击 “初始化后缀”打开 “初始化”对话框，然后输入 LDIF 文件的名称以加载到目录中。

   如果在上一步中导出了具有加密属性的后缀，则现在必须使用该文件进行初始化，因为后缀重新初始化后，已加密的值将无法恢复。文件加载完成并创建了索引后，指定属性的所有值就被加密了。

   如果不想立即初始化后缀，请单击 “关闭”。使用 “导入数据”（第 118 页）中所述的步骤，可以稍后导入数据。

7. 如果已更改配置对一个或多个属性进行加密，且这些属性在导入操作前具有值，则那些未加密的值中的一部分可能在数据库缓存中仍然可见。要清除数据库缓存，请执行以下操作：

   a. 如 “启动和停止 Directory Server”（第 20 页）中所述，停止目录服务器。

   b. 作为 root 或具有管理员特权的用户，从文件系统中删除数据库缓存文件：

   ServerRoot`/slapd-`*serverID*`/db/__db.*`

   c. 再次启动目录服务器。服务器将自动创建新的数据库缓存文件。

从命令行配置属性加密

1. 如果要配置属性加密的后缀包含任何条目，则必须先将该后缀的内容导出到 LDIF 文件。详细信息，请参阅 “导出数据”（第 124 页）。

   当您计划使用该 LDIF 文件在 步骤 5 中重新初始化后缀时，如果后缀包含加密属性，则可在已导出的 LDIF 中继续保持加密。

2. 要启用属性的加密，请使用 ldapmodify 命令添加以下配置条目：

```
ldapmodify -a -h 主机 -p 端口 -D cn=Directory Manager -p 口令
dn:cn=attributeName, cn=encrypted attributes, cn=databaseName,
 cn=ldbm database, cn=plugins, cn=config
objectclass:top
objectclass:dsAttributeEncryption
cn:attributeName
dsEncryptionAlgorithm:cipherName
```

其中 *attributeName* 是要加密的属性的类型名称， *databaseName* 是与后缀对应的数据库的符号名称，而 *cipherName* 是以下各项之一：

- ckm_des_cbc - DES 块密码
- ckm_des3_cbc - Triple-DES 块密码
- ckm_rc2_cbc - RC2 块密码
- ckm_rc4 - RC4 流密码

3. 要使属性不再加密，请使用 ldapmodify 命令修改以下配置条目：

```
ldapmodify -h 主机 -p 端口 -D cn=Directory Manager -p 口令
dn:cn=attributeName, cn=encrypted attributes, cn=databaseName,
 cn=ldbm database, cn=plugins, cn=config
changetype:modify
replace:dsEncryptionAlgorithm
dsEncryptionAlgorithm:clearText
```

其中 *attributeName* 是要加密的属性的类型名称， *databaseName* 是与后缀对应的数据库的符号名称。

注意 不要删除属性加密配置条目。下次后缀初始化时，该条目将被自动删除。

4. 如果已更改配置对一个或多个属性进行加密，且这些属性在导入操作前具有值，则那些未加密的值中的一部分可能在数据库缓存中仍然可见。要清除数据库缓存，请执行以下操作：

   a. 如 “启动和停止 Directory Server”（第 20 页）中所述，停止目录服务器。

   b. 作为 root 或具有管理员特权的用户，从文件系统中删除数据库缓存文件：

   ServerRoot/slapd-*serverID*/db/__db.*

   c. 再次启动目录服务器。服务器将自动创建新的数据库缓存文件。该后缀中操作的性能将受到轻微的影响，直到缓存被重新填充。

5. 如 “导入数据”（第 118 页）中所述，使用 LDIF 文件初始化后缀。如果在步骤 1 中导入后缀，请使用该文件确保后缀具有最新的内容。如果在步骤 1 中导出了具有加密属性的后缀，则现在必须使用该文件进行初始化，因为后缀重新初始化后，已加密的值将无法恢复。

   文件加载完成并创建了相应的索引后，指定属性的所有值就被加密了。

维护引荐完整性

引荐完整性是确保相关条目之间的关系得以维持的一种插件机制。几种属性类型（如用于组成员身份的属性）包含另一个条目的 DN。引荐完整性可用于确保当条目被删除时，所有包含其 DN 的属性也将被删除。

例如，如果从目录中删除了某个用户的条目且启用了引荐完整性，则服务器还从包含此用户成员的任何组中删除此用户。如果未启用引荐完整性，则必须由管理员手动从组中删除此用户。如果您要将目录服务器与依赖用于用户和组管理的目录的其他 Sun ONE 产品集成，则这是一个重要功能。

引荐完整性的工作方式

启用引荐完整性插件时，它在执行了删除或重命名操作后，立即对特定属性执行完整性更新。但默认情况下，系统禁用引荐完整性插件。

不论何时删除或重命名目录中的用户条目或组条目，操作都记录到引荐完整性日志文件中：

ServerRoot/slapd-*serverID*/logs/referint

在指定的时间 （即更新时间间隔）后，服务器对已启用引荐完整性的所有属性执行搜索，并将此搜索获得的条目与日志文件中已删除或已修改的条目的 DN 进行匹配。如果日志文件显示已删除条目，则删除对应的属性。如果日志文件显示已更改条目，则相应地修改对应的属性值。

当启用了引荐完整性插件的默认配置时，每次执行删除或重命名操作后，此插件对 member、 uniquemember、 owner、 seeAlso 和 nsroledn 属性执行完整性更新。但是，可以配置引荐完整性插件的行为以适合您的需要：

- 在另一文件中记录引荐完整性更新。
- 修改更新时间间隔。如果要减少引荐完整性更新对系统的影响，则要增加更新之间的时间。

- 选择将引荐完整性应用到的属性。如果使用或定义包含 DN 值的属性，则需要使用引荐完整性插件监视这些属性。

配置引荐完整性

使用以下步骤从 Directory Server 控制台启用或禁用引荐完整性以及配置插件：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “插件”节点，并选择 “referential integrity postoperation”插件。

   该插件的设置显示在右侧面板中。

2. 选中 “启用插件”复选框可启用该插件，取消选中此复选框可禁用该插件。
3. 设置参数 1 的值以修改更新时间间隔 （以秒为单位）。通用值为：
   - 0 - 每次操作后立即更新。请注意，每次删除或修改操作以后立即进行引荐完整性检查可能严重影响服务器的性能。
   - 90 - 每 90 秒钟更新一次
   - 3600 - 每小时更新一次
   - 10,800 - 每 3 小时更新一次
   - 28,800 - 每 8 小时更新一次
   - 86,400 - 每天更新一次
   - 604,800 - 每周更新一次
4. 将参数 2 的值设置为要使用的引荐完整性日志文件的绝对路径。

   参数 3 未使用，但是必须存在。

5. 为引荐完整性而监视的属性从参数 4 开始列出，单击 “添加”和 “删除”按钮管理该列表以及添加自己的属性。

注意 为获得最佳性能，由引荐完整性插件更新的属性也应该被编制索引。有关信息，请参阅第 10 章 “管理索引”。

6. 单击 “保存”保存更改。
7. 为使更改生效，必须重新启动 Directory Server。

将引荐完整性与复制一起使用

当需要在复制环境中使用引荐完整性插件时，存在一定的限制：

- 必须在包含主副本的所有服务器上启用引荐完整性。
- 必须在每个主副本上使用相同的配置启用它。
- 在仅包含集线器副本或使用者副本的服务器上启用引荐完整性是没有意义的。

要在复制拓扑结构中配置引荐完整性插件，请执行以下操作：

1. 确保所有副本已配置且所有复制协议已定义。
2. 确定要为其维护引荐完整性的属性集。也请确定要在主服务器上使用的更新时间间隔。
3. 使用相同的属性集和相同的更新时间间隔，在所有主服务器上启用引荐完整性插件。此过程在 “配置引荐完整性”（第 74 页）中已说明。
4. 确保在全部的使用者服务器上禁用引荐完整性插件。

第 3 章

创建目录树

目录树包含服务器中的所有条目，由其标识名称 (DN) 标识。 DN 的层次属性创建了在树中组织数据的分支和叶子。为了管理目录树，依照后缀、子后缀和链接后缀的组织方式对其进行定义。Directory Server 控制台对创建和管理所有这些元素进行控制，或者可以使用命令行工具。

有关组织目录数据的概念性信息，请参阅 *Sun ONE Directory Server 部署指南* 中的第 4 章 “设计目录树”。

本章包含以下小节：

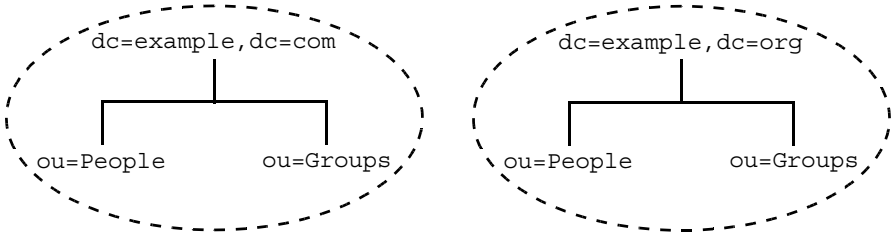
- 简介
- 创建后缀
- 管理后缀
- 创建已链接的后缀
- 管理已链接的后缀
- 配置级联链接

简介

后缀是其全部内容都被视作管理任务单元的分支和子树。例如，为完全后缀定义索引、可以在单个操作中初始化完全后缀、后缀是复制的单位希望采用同一种方式访问和管理的数据应位于同一后缀中。后缀可以位于目录树的根，有时称其为根后缀。

下图显示具有两个根后缀的目录，每个根后缀代表一个单独的公司实体：

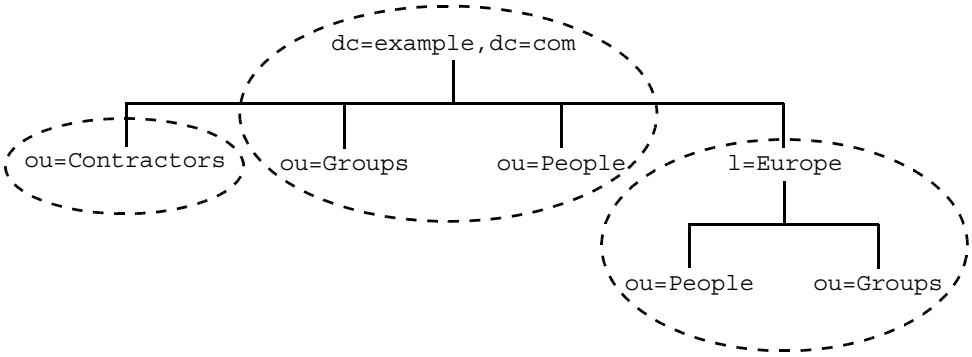
图 3-1 一个 Directory Server 中的两个根后缀



一个后缀也可以是另一个后缀的分支，在此情况下，这个后缀称为子后缀。父后缀不包括用于管理操作的子后缀的内容，因而子后缀的管理独立于其父后缀。但是，LDAP 操作结果不包含有关后缀的信息，目录客户机不知道条目是根后缀还是子后缀的一部分。

下图显示一家大型公司实体中具有单个根后缀和多个子后缀的目录：

图 3-2 具有多个子后缀的一个根后缀



后缀对应于服务器内的单个数据库。但是，数据库及其文件现在由服务器内部管理，并且从 Sun ONE Directory Server 5.2 开始除去了数据库术语。

链接后缀通过引用其他服务器上的后缀来创建虚拟目录树。利用链接后缀，Directory Server 在远程后缀上执行操作并返回结果，就像在本地执行一样。数据的位置是透明的，因为客户机不知道后缀是链接的后缀，也不知道数据是从远程服务器检索得到的。一个服务器上的根后缀可以包含链接到另一个服务器的子后缀，这样，从客户机的角度而言创建的是单个树结构。

在级联链接的特殊情况下，链接后缀可以引荐远程服务器上的另一个链接后缀，依此类推。每个服务器都将转发操作，最后将结果返回到处理客户机请求的服务器。

有关链接的常规信息，请参阅 *Sun ONE Directory Server 部署指南* 的第 5 章 “设计目录拓扑结构”。

创建后缀

可以使用 Directory Server 控制台或命令行创建根后缀和子后缀。

使用控制台创建新的根后缀

1. 在 Directory Server 控制台的顶级 “配置”标签上，右键单击 “数据”节点，并从弹出菜单中选择 “新建后缀”。

   或者，可以选择 “数据”节点，并从 “对象”菜单中选择 “新建后缀”。

   显示 “新建后缀”对话框。

2. 在 “后缀 DN”字段中输入唯一的后缀名称。此名称必须使用由逗号分隔的一个或多个属性 - 值对组成的标识名称格式。

   按照约定，根后缀使用域组件 (dc) 命名属性。例如，可以为新后缀 DN 输入 `dc=example,dc=org`。

注意 虽然后缀名称包含 DN 格式的属性 - 值对，但将其视作单个字符串。因此，所有空格都有意义，都是后缀名称的一部分。

3. 默认情况下，此后缀的数据库文件的位置由服务器自动选择。另外，默认情况下，此后缀只维护系统索引，将不对属性进行加密，也不对复制进行配置。

   要修改任一默认值，请单击 “选项”按钮以显示新后缀选项：

   a. 数据库的名称也是包含数据库文件的目录的名称。默认数据库名称是后缀 DN 中第一个命名属性的值，可能还附加了唯一性数字。要使用其他名称，请选择 “使用自定义”单选按钮，然后输入一个新的、唯一的数据库名称。

      数据库名称只能包含 ASCII （7 位）字母数字字符、连字符 (-) 和下划线 (_)。例如，可以将此新数据库命名为 `example_2`。

   b. 还可以选择包含数据库文件的目录的位置。默认情况下，此位置是下列路径的子目录：

      ServerRoot`/slapd-`*serverID*`/db`

输入新路径，或单击 “浏览”查找数据库目录的新位置。新的路径必须可以在目录服务器主机上访问。

c. 要加速配置新后缀，可以选择复制现有的后缀。选择 “复制后缀配置”，并从下拉菜单中选择要复制的后缀。然后选择下列任一配置进行复制：

- 复制索引配置 - 新后缀将对相同属性维护与已复制后缀相同的索引。
- 复制属性加密配置 - 新后缀将对与已复制后缀中相同的属性列表和加密方案启用加密。
- 克隆复制配置 - 新后缀将与已复制后缀具有相同的副本类型，如果副本是供应商副本，则将复制所有复制协议，而且将启用复制。

d. 配置所有新后缀的选项后，单击 “确定”。“新建后缀”对话框将显示您选择的所有选项。

4. 在 “新建后缀”对话框中单击 “确定”以创建新的根后缀。

   根后缀自动出现在 “数据”分支下。有关进一步配置新后缀的信息，请参阅 “管理后缀”（第 86 页）。

   新的根后缀不包含任何条目，甚至不包含后缀 DN 的条目。因而，新的子后缀在被初始化和授予适当的访问权限前，不仅在目录中是不可访问的，而且在控制台的 “目录”标签中也是不可见的。

   如果从 LDIF 文件初始化此后缀，则可以跳过其余步骤。但是，请确保 LDIF 文件中的根条目都包含部署所需的访问控制指令 (ACI)。

5. 选择控制台的顶级 “目录”标签。新后缀在目录树中仍然不可见。

6. 如果您没有以目录管理员的身份登录，则立即通过选择 “控制台” > “以新用户身份登录”菜单项进行登录。输入目录管理员的 DN 和口令进行登录。默认情况下，目录管理员的 DN 是 `cn=Directory Manager`。

7. 右键单击目录树的根节点，此根节点包含服务器的主机名和端口。从弹出菜单中选择 “新建根对象”项，然后选择新的根后缀的 DN。

   或者，选择目录树的根节点，然后从 “对象”菜单中选择 “新建根对象”项。

8. 在显示的 “新建对象”对话框中，为该根对象选择单个对象类。此对象类将确定可以添加到根条目中的其他属性。

   按照约定，包含 `dc` 命名属性的后缀 DN 的根对象属于 `domain` 对象类。通常情况下，根对象是简单对象，包含很少的数据。

9. 选择了对象类后，在 “新建对象”对话框中单击 “确定”。

控制台立即显示新的根对象的通用编辑器。默认的 ACI 集合被自动添加到该新对象中。有关其他信息，请参阅 “默认 ACI”（第 164 页）。添加并编辑拓扑所需的任何属性值，包括对 ACI 集合所做的任何修改。

如果新后缀将包含用户条目，则应修改标题为 “允许 nsroledn 和 aci 属性之外的条目进行自我修改”的默认 ACI。要获得额外的安全性，请用以下 ACI 将其替换：

```
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";)
```

10. 编辑此条目后，在 “通用编辑器”中单击 “确定”以创建新后缀的根对象。

    新后缀立即出现在目录树中，可以按照 ACI 授予的权限通过控制台进行管理。

使用控制台创建新的子后缀

下列过程描述在已存在的根或子后缀下如何创建新的子后缀：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点和任何后缀节点以显示父后缀。
2. 右键单击父后缀节点，从弹出菜单中选择 “新建子后缀”。

   或者，可以选择父后缀节点，并从 “对象”菜单中选择 “新建子后缀”。

   出现 “新建子后缀”对话框。
3. 在 “子后缀 RDN”字段中输入唯一名称。此名称必须使用相对标识名称格式，它由一个或多个由逗号分隔的属性 - 值对组成，例如 `ou=Contractors`。

   文本框下的一行显示此子后缀的完整 DN，由附加到 RDN 的父后缀 DN 组成。

注意 虽然子后缀名称包含采用 RDN 格式的属性 - 值对，但将其视作单个字符串。因此，所有空格都有意义，都是后缀 DN 的一部分。

4. 默认情况下，此后缀的数据库文件的位置由服务器自动选择。另外，默认情况下，此后缀只维护系统索引，将不对属性进行加密，也不对复制进行配置。

   要修改任一默认值，请单击 “选项”按钮以显示新后缀选项：

   a. 数据库的名称也是包含数据库文件的目录的名称。默认的数据库名称是 RDN 中第一个命名属性的值，可能还附加了唯一性数字。要使用其他名称，请选择 “使用自定义”单选按钮，然后输入一个新的、唯一的数据库名称。

      数据库名称只能包含 ASCII （7 位）字母数字字符、连字符 (-) 和下划线 (_)。例如，可以将此新数据库命名为 `temps-US`。

   b. 还可以选择包含数据库文件的目录的位置。默认情况下，此位置是下列路径的子目录：

      ServerRoot/`slapd-`*serverID*/`db`

      输入新路径，或单击 “浏览”查找数据库目录的新位置。新的路径必须可以通过目录服务器应用程序访问。

   c. 要加速新子后缀的配置，可以选择复制现有的后缀，可以是这个新子后缀的父后缀，也可以是任何其他后缀。选择 “复制后缀配置”，并从下拉菜单中选择要复制的后缀。然后选择下列任一配置进行复制：

      - 复制索引配置 - 新后缀将对相同属性维护与已复制后缀相同的索引。
      - 复制属性加密配置 - 新后缀将对与已复制后缀中相同的属性列表和加密方案启用加密。
      - 复制复制配置 - 新后缀将与已复制后缀具有相同的副本类型，如果副本是供应商副本，则将复制所有复制协议，而且将启用复制。

   d. 配置所有新后缀的选项后，单击 “确定”。“新建子后缀”对话框将显示您选择的所有选项。

5. 在 “新建子后缀”对话框中单击 “确定”以创建子后缀。

   在 “配置”标签中，子后缀自动出现在其父后缀下。有关进一步配置新后缀的信息，请参阅 “管理后缀”（第 86 页）。

   新的子后缀不包含任何条目，甚至不包含 RDN 的条目。因而，新的子后缀在被初始化和授予适当的访问权限前，不仅在目录中是不可访问的，而且在控制台的 “目录”标签中也是不可见的。

   如果从 LDIF 文件初始化此后缀，则可以跳过其余步骤。但是，请确保 LDIF 文件中的父后缀和新条目都包含部署所需的访问控制指令 (ACI)。

6. 在控制台的顶级 “目录”标签中，展开目录树，以显示子后缀的父后缀。新的子后缀仍是不可见的。

7. 如果您没有以目录管理员的身份登录，则立即通过选择 “控制台” > “以新用户身份登录”菜单项进行登录。输入目录管理员的 DN 和口令进行登录。默认情况下，目录管理员的 DN 是 `cn=Directory Manager`。

8. 右键单击子后缀的父后缀，然后从弹出菜单中选择 “新建”项。在新建对象的列表中，选择对应于子后缀的 RDN 的对象类型。例如，如果创建了 `ou=Contractors` 子后缀，则选择 OrganizationalUnit 项。如果未列出子后缀的对象类，则选择 “其他”，然后从显示的 “新建对象”对话框中选择此对象类。

   或者，选择子后缀的父后缀，然后从 “对象”菜单中选择 “新建”项。

9. 控制台立即显示新对象的自定义或通用编辑器。添加并编辑拓扑所需的任何属性值，包括对 ACI 集合所做的任何修改。

10. 编辑此条目后，在 “编辑器”中单击 “确定”以创建新的子后缀的条目。

    新的子后缀立即出现在目录树中，可以按照 ACI 授予的权限通过控制台进行管理。

从命令行创建后缀

还可以使用 `ldapmodify` 命令行公用程序在目录中创建后缀。由于根后缀和子后缀都由服务器采用相同方式在内部进行管理，所以从命令行创建根后缀和子后缀的过程几乎相同。

1. 使用以下命令为根后缀在 `cn=mapping tree,cn=config` 下创建后缀配置条目：

   ```
   ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn="suffixDN",cn=mapping tree,cn=config
   objectclass:top
   objectclass:extensibleObject
   objectclass:nsMappingTree
   cn:suffixDN
   nsslapd-state:backend
   nsslapd-backend:databaseName
   ^D
   ```

   对于子后缀，请使用带另一属性的相同命令：
   `nsslapd-parent-suffix:"`*parentSuffixDN*`"`

   suffixDN 是新后缀的完整 DN。对于根后缀，按约定是使用域组件 (`dc`) 命名属性，例如 `dc=example,dc=org`。对于子后缀， *suffixDN* 包括子后缀的 RDN 和其父后缀的 DN，例如 `ou=Contractors,dc=example,dc=com`。

注意 虽然后缀名称采用 DN 格式，但将其视作单个字符串。因此，所有空格都有意义，都是后缀名称的一部分。要访问此后缀，就需要采用 *suffixDN* 字符串中使用的间隔。

databaseName 是与此后缀相关的内部管理的数据库的名称。此名称在所有后缀的 *databaseNames* 中是唯一的，按照约定，它是 *suffixDN* 的第一个命名组件的值。 *databaseName* 也是包含后缀的数据库文件的目录的名称，因此应仅包含 ASCII（7 位）字母数字字符、连字符 (-) 和下划线 (_)。

对于子后缀， *parentSuffixDN* 即是父后缀的 DN。

2. 使用以下命令创建数据库配置条目：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=databaseName,cn=ldbm database,cn=plugins,cn=config
objectclass:top
objectclass:extensibleObject
objectclass:nsBackendInstance
cn:databaseName
nsslapd-suffix:suffixDN
^D
```

其中， *databaseName* 和 *suffixDN* 的值必须与上个步骤中使用的值相同。

当将此条目添加到目录中时，服务器的数据库模块将在下列目录中自动创建数据库文件：

ServerRoot/slapd-*serverID*/db/*databaseName*

要使服务器在另一个位置创建数据库文件，请使用下列属性创建数据库配置条目：

```
nsslapd-directory:path/databaseName
```

服务器将自动在给定的位置创建一个名为 *databaseName* 的目录以存放数据库文件。

3. 创建根后缀或子后缀的基本条目。

例如，可以使用以下命令创建 dc=example,dc=org 根后缀的基本条目：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:dc=example,dc=org
objectclass:top
objectclass:domain
dc:example
^D
```

必须包括 DN 的第一个命名属性及其值。还必须包括基本条目的对象类的模式所需的所有属性。根据约定，使用域组件 (dc) 的根后缀 DN 包含 `domain` 对象类，此对象类不需要任何其他属性。

还应向根后缀中添加访问控制指令 (ACI) 属性，以强制执行您的访问策略。下面是一些 `aci` 属性值，可以添加这些属性值以允许匿名读取，确保自我修改和以完全的管理员特权访问：

```
aci:(targetattr != "userPassword") (version 3.0; acl
 "Anonymous access";
 allow (read, search, compare)userdn = "ldap:///anyone";)
aci:(targetattr != "nsroledn || aci || nsLookThroughLimit ||
 nsSizeLimit || nsTimeLimit || nsIdleTimeout ||
 passwordPolicySubentry || passwordExpirationTime ||
 passwordExpWarned || passwordRetryCount || retryCountResetTime
 || accountUnlockTime || passwordHistory ||
 passwordAllowChangeTime")(version 3.0; acl "Allow self entry
 modification except for nsroledn, aci, resource limit
 attributes, passwordPolicySubentry and password policy state
 attributes"; allow (write)userdn ="ldap:///self";)
aci:(targetattr = "*")(version 3.0; acl
 "Configuration Administrator";
 allow (all) userdn = "ldap:///uid=admin,ou=Administrators,
 ou=TopologyManagement, o=NetscapeRoot";)
aci:(targetattr ="*")(version 3.0;acl
 "Configuration Administrators Group";
 allow (all) (groupdn =
 "ldap:///cn=Configuration Administrators, ou=Groups,
 ou=TopologyManagement, o=NetscapeRoot");)
```

作为子后缀的一个示例，可以使用以下命令创建 `ou=Contractors,dc=example,dc=com` 的基本条目：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:ou=Contractors,dc=example,dc=com
objectclass:top
objectclass:organizationalUnit
description:base of separate subsuffix for contractor identities
^D
```

必须包括 DN 的命名属性及其值。还必须包括基本条目的对象类的模式所需的所有属性，可以添加允许的任何其他属性。子后缀将具有其父后缀上的 ACI 定义的访问控制，只要这些 ACI 的范围包括此新的子后缀即可。要在子后缀上定义不同的访问策略，请在创建基本条目时指定 `aci` 属性。

管理后缀

创建后缀允许您管理其全部内容。本节说明如何管理对后缀的访问，包括禁用所有操作、使后缀为只读和创建后缀级别的引荐。

可以在后缀级别配置许多其他目录管理任务，但在本书的不同章节进行说明：

- “导入数据”（第 118 页）。
- “导出数据”（第 124 页）。
- “管理索引”（第 303 页）。
- “为属性值加密”（第 70 页）。
- “管理复制”（第 239 页）。

禁用或启用后缀

某些时候可能因维护而需要使后缀不可用，或出于安全考虑使其内容不可用。禁用后缀使服务器无法因响应尝试访问此后缀的任何客户机操作而读写此后缀的内容。如果定义了默认引荐，则在客户机尝试访问已禁用的后缀时，该返回该默认引荐。

使用控制台禁用或启用后缀

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点，然后选择要禁用的后缀。
2. 在右侧面板中选择 “设置”标签。默认情况下，所有后缀在创建时都将启用。

   如果已启用此后缀的复制操作，则您将看到一条通知，告知此标签的内容可能已自动更新。禁用复制的后缀还将中断对此后缀的复制。只要中断复制的时间不比恢复设置的时间长，复制机制就会在此后缀再次启用时恢复对此副本的更新。复制恢复设置包括此使用者副本的清理延迟及其供应商更改日志的最大大小和存留期 （请参阅 “高级使用者配置”（第 245 页））。
3. 取消选中 “启用对该后缀的访问权限”复选框以禁用此后缀，或选中此复选框以启用此后缀。
4. 单击 “保存”应用更改并立即禁用或启用此后缀。
5. 可选地，禁用此后缀时，也可为对此后缀执行的所有操作设置将返回的全局默认引荐。此设置位于顶级 “配置”标签的根节点的 “网络”标签上。详细信息，请参阅 “使用控制台设置默认引荐”（第 67 页）。

从命令行禁用或启用后缀

1. 使用以下命令在后缀的配置条目中编辑 nsslapd-state 属性：

   ```
   ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn="suffixDN",cn=mapping tree,cn=config
   changetype:modify
   replace:nsslapd-state
   nsslapd-state:disabled or backend
   ^D
   ```

   其中， *suffixDN* 是后缀 DN 定义时的完整字符串，包含所有空格。将 nssladp-state 属性设置为值 disabled 可禁用后缀，设置为值 backend 可实现完全访问。

   成功执行命令后，将立即禁用后缀。

2. 可选地，禁用此后缀时，也可为对此后缀执行的所有操作设置将返回的全局默认引荐。详细信息，请参阅 “从命令行设置默认引荐”（第 67 页）。

设置访问权限和引荐

如果要限制对后缀的访问，而不完全禁用它，则可以修改访问权限以允许只读访问。在此情况下，必须定义对另一个服务器的引荐，以用于写操作。还可以同时拒绝读写访问，为对后缀执行的所有操作定义引荐。

还可以使用引荐将客户机应用程序临时指向其他服务器。例如，可以添加对某个后缀的引荐，以便在备份此后缀的内容时，此后缀指向其他服务器。

复制机制依赖写权限和引荐来配置后缀以进行复制。启用复制、升级副本或降级副本都将修改引荐设置。

警告 如果复制此后缀，则修改引荐可能会影响此后缀的已复制的行为。

使用控制台设置访问权限和引荐

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点，然后选择要设置引荐的后缀。
2. 在右侧面板中选择 “设置”标签。如果启用了已链接的后缀，则将只能设置权限和引荐。如果已启用此后缀的复制操作，则您将看到一条通知，告知此标签的内容可能已自动更新。
3. 选择以下某一单选按钮，以设置对此后缀中条目进行任何写操作时的响应：

- 处理读写请求 - 默认情况下将选择此单选按钮，它代表后缀的正常行为。可以定义引荐，但不会返回它们。
- 处理读请求并返回写请求引荐 - 如果要使后缀为只读并在列表中输入要作为写请求引荐返回的一个或多个 LDAP URL，请选择此单选按钮。
- 为读写请求返回引荐 - 如果要同时拒绝读写访问，请选择此单选按钮。此行为类似于禁用对后缀的访问，不同的是，此行为可以为此后缀专门定义引荐，而不是使用全局默认引荐。

4. 通过 “添加”和 “删除”按钮编辑引荐列表。单击 “添加”按钮将显示一个对话框，用于创建新引荐的 LDAP URL。可以在远程服务器中创建对任何分支的 DN 的引荐。有关 LDAP URL 结构的详细信息，请参阅 *Sun ONE Directory Server 入门指南*。

   可输入多个引荐。该目录将返回此列表中的所有引荐，以响应来自客户机应用程序的请求。

5. 单击 “保存”应用更改并立即开始执行新的权限和引荐设置。

从命令行设置访问权限和引荐

在以下命令中， *suffixDN* 是后缀 DN 定义时的完整字符串，包含所有空格。*LDAPURL* 是有效的 URL，它包含主机名、端口号和目标的 DN，例如：

```
ldap://phonebook.example.com:389/ou=People,dc=example,dc=com
```

1. 使用以下命令编辑后缀的配置条目：

   ```
   ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn="suffixDN",cn=mapping tree,cn=config
   changetype:modify
   replace:nsslapd-state
   nsslapd-state:referral on update or referral
   -
   add:nsslapd-referral
   nsslapd-referral:LDAPURL
   ^D
   ```

   可以重复最后一个更改语句以将 LDAP URL 的任何数字添加到 `nsslapd-referral` 属性中。

   当 nsslapd-state 的值是 `referral on update` 时，此后缀为只读且所有 LDAP URL 都将作为写操作引荐返回。当值是 `referral` 时，系统将拒绝读写操作并为任一请求返回引荐。

2. 此后缀将变为只读或不可访问，并准备在成功执行命令后立即返回引荐。

删除后缀

删除后缀将从目录中删除其整个分支。可以删除父后缀，并将其子后缀作为新的根后缀保存在目录中。

警告 删除后缀时，将从目录中永久删除此后缀的所有条目，并删除此后缀的所有配置 （包括其复制配置）。

使用控制台删除后缀

1. 在 Directory Server 控制台的 “配置”标签上，展开 “数据”节点。
2. 右键单击要删除的后缀，从弹出菜单中选择 “删除”。

   或者，可以选择后缀节点，并从 “对象”菜单中选择 “删除”。
3. 出现确认对话框，告知将从该目录中删除所有后缀条目。

   另外，对于父后缀，可以选择采用递归方式删除其所有子后缀。如果要删除整个分支，请选择 “删除此后缀及其所有子后缀”。否则，如果只想删除此特定后缀并在目录中保存其子后缀，请选择 “只删除此后缀”。
4. 单击 “确定”以删除此后缀。

   显示进程对话框，告知您这些步骤正在由控制台完成。

从命令行删除后缀

要从命令行删除后缀，请使用 `ldapdelete` 命令从目录中删除其配置条目。

如果要删除包含子后缀的整个分支，则必须找到已删除的父后缀的子后缀，并对每个后缀及其可能的子后缀重复此过程。

1. 使用以下命令删除后缀配置条目：

   ```
   ldapdelete -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
              -v 'cn="suffixDN",cn=mapping tree,cn=config'
   ```

   此命令从服务器删除后缀，从 *suffixDN* 处的基本条目开始删除。现在，此后缀在目录中既不可见，也不能访问。
2. 删除位于 `cn=`*databaseName*`,cn=ldbm database,cn=plugins,cn=config` 中的相应数据库配置条目及其下的所有条目。以下命令使用 Sun ONE Directory Server Resource Kit (DSRK) 的 `ilash` 工具。有关下载和使用 DSRK 的信息，请参阅 “下载 Directory Server 工具”（第 16 页）。

```
% ilash -call "http://主机:端口/" -user "cn=Directory Manager"
[...]
Enter password for "cn=Directory Manager": 口令
[...]
[example,com]% dcd cn=config
[config]% ddelete -subtree \
"cn=databaseName,cn=ldbm database,cn=plugins,cn=config"

Removed cn=aci, cn=index, cn=databaseName, cn=ldbm database,
cn=plugins, cn=config

Removed cn=entrydn, cn=index, cn=databaseName, cn=ldbm database,
cn=plugins, cn=config

[...]

Removed cn=encrypted attributes, cn=databaseName, cn=ldbm database,
cn=plugins, cn=config

Removed cn=index, cn=databaseName, cn=ldbm database, cn=plugins,
cn=config

Removed cn=monitor, cn=databaseName, cn=ldbm database, cn=plugins,
cn=config

Removed cn=databaseName,cn=ldbm database,cn=plugins,cn=config
```

此输出显示与数据库相关和需要删除的所有索引配置条目。完全删除数据库配置后，服务器将删除与此后缀相关的所有数据库文件和目录。

创建已链接的后缀

根后缀和子后缀都可以链接到另一台服务器，这两个过程都可以通过控制台或从命令行来执行。

但是，在创建任何已链接的后缀前，应在远程服务器上创建代理身份。本地服务器在通过已链接后缀转发操作时，将使用代理身份绑定到远程服务器上。

如果配置的许多已链接后缀都具有相同参数，则还应为新的已链接后缀的链接参数设置默认值。在创建已链接后缀前后的任何时间，还可以为 LDAP 控件和服务器组件设置链接策略，如 “配置链接策略”（第 101 页）中所述。

创建代理身份

代理身份是本地服务器将用于绑定和转发已链接操作的远程服务器上的用户。出于安全考虑，配置代理时，一定不要使用目录管理员或管理用户 (admin) 的身份。

相反，从给定服务器创建将只用于已链接操作的新身份。在将链接的所有服务器上以及在 “使用控制台创建已链接的后缀”（第 94 页）或 “使用控制台修改链接策略”（第 104 页）中定义的所有故障切换服务器上创建此身份。

使用控制台创建代理身份

此过程适用于已连接到远程服务器 （作为已链接后缀的目标）的 Directory Server 控制台。

1. 在 Directory Server 控制台的顶级 “目录”标签上，展开目录树。
2. 右键单击 cn=config 条目并从弹出菜单中选择 “新建” > “用户”项。或者，选择 cn=config 条目并从 “对象”菜单中选择 “新建” > “用户”项。
3. 在 “创建新用户”对话框的字段中填写值以描述代理身份，例如：

名字：	proxy
姓氏：	*主机 1*
通用名：	*主机 1* chaining proxy
用户 ID：	*主机 1*_proxy
口令：	*口令*
确认口令：	*口令*

   其中，主机 1 是包含已链接后缀的服务器的名称。对已有后缀链接到服务器的各个服务器，应使用不同的代理身份。
4. 单击 “确定”以保存此新的代理身份。

从命令行创建代理身份

此过程使用主机 1 和主机 2 分别指包含已链接后缀的本地服务器，以及作为已链接后缀目标的远程服务器。

1. 使用以下命令在主机 2 上创建代理身份：

```
ldapmodify -a -h 主机2 -p 端口2 -D "cn=Directory Manager" -w 口令2
dn:uid=主机1_proxy,cn=config
objectclass:top
objectclass:person
objectclass:organizationalPerson
objectclass:inetorgperson
uid:主机1_proxy
cn:主机1 chaining proxy
sn:主机1
userpassword:口令
description:proxy entry to be used for chaining from 主机1
^D
```

设置默认链接参数

链接参数确定服务器如何连接到已链接的服务器上，以及如何处理对该已链接后缀执行的操作。在每个已链接后缀上配置这些参数。 Directory Server 提供每次创建已链接后缀时使用的默认值。可以在所有新的已链接后缀上编辑这些默认值以指定链接参数。

修改默认参数后创建的每个新的已链接后缀将具有您指定的值。但是，创建了后缀后，就只能修改 “管理已链接的后缀”（第 101 页）中描述的参数。

链接参数的属性和默认值在下面进行了描述。有关允许值的描述，请参阅 *Sun ONE Directory Server 参考手册* 的第 5 章中的 “已链接的后缀插件属性”：

客户机返回参数

- `nsReferralOnScopedSearch` - 默认情况下设置为 on 时，客户机搜索 （其范围完全在已链接的后缀内）将接收对远程服务器的引荐。这样可避免将搜索结果传输两次。设置为 off 时，应设置大小和时间限制参数，以避免对已链接的后缀进行长时间搜索。

- `nsslapd-sizelimit` - 此参数确定响应已链接的搜索操作而将返回的条目数。默认值大小限制是 2000 个条目。如果要限制对涉及的已链接后缀进行大范围搜索，请将此参数设置为较低的值。在任何情况下，操作将受远程服务器上的任何大小设置所限制。

- `nsslapd-timelimit` - 此参数控制已链接操作的时间长度。默认时间限制是 3600 秒 （1 小时）。如果要限制对已链接后缀执行操作的时间，则将此参数设置为较低的值。在任何情况下，操作将受远程服务器上的任何时间设置所限制。

级联链接参数

- `nsCheckLocalACI` - 在单级别链接中，本地服务器不检查已链接的后缀上绑定用户的访问权限，因为这是远程服务器的职责。因此，默认值为 `off`。但是，为了检查和限制转发已链接操作的服务器所使用的代理 DN 的访问权限，级联链接中的中间服务器必须将此参数设置为 `on`。

- `nsHopLimit` - 循环检测依赖此参数以定义允许的最大跃点数。假设在级联拓扑中存在意外循环，则到达此跃点数的任何已链接操作将不进行转发，而是放弃。

连接管理参数

- `nsOperationConnectionsLimit` - 已链接的后缀通过远程服务器可以建立的最大同时发生的 LDAP 连接数。默认值是 10 个连接。

- `nsBindConnectionsLimit` - 已链接的后缀通过远程服务器可以建立的最大同时发生的 TCP 连接数。默认值是 3 个连接。

- nsConcurrentBindLimit - 每个 LDAP 连接最大的同时绑定操作数。默认值是每个连接有 10 个突出绑定操作。
- nsBindRetryLimit - 出错时，已链接的后缀尝试重新绑定到远程服务器上的次数。值 0 表示已链接的后缀将仅尝试绑定一次。默认值是尝试 3 次。
- nsConcurrentOperationsLimit - 每个 LDAP 连接最大的同时操作数。默认值是每个连接有 10 个操作。
- nsBindTimeout - 链接服务器上绑定尝试超时之前的时间长度 （以秒为单位）。默认值为 15 秒。
- nsAbandonedSearchCheckInterval - 在服务器检查是否已放弃某项操作前的秒数。默认值为 2 秒。
- nsConnectionLife - 已链接的后缀与远程服务器之间的连接保持为打开状态以便可以重新使用的时间长度。将连接保持为打开状态可以加快访问速度，但要使用更多的资源。例如，如果使用拨号连接，则希望限制连接时间。默认情况下，连接不受限制，由值 0 定义。

错误检测参数

- nsmaxresponsedelay - 远程服务器响应已链接操作的初始化 LDAP 请求所花费的最长时间。此期间按秒计算。在此延迟后，本地服务器将测试连接。默认延迟期是 60 秒。
- nsmaxtestresponsedelay - 检查远程服务器是否正在响应的测试的持续时间。此测试是对不存在的条目所执行的简单搜索请求。此期间按秒计算。如果在测试延迟期间未接收响应，则已链接的后缀将假定远程服务器停机。默认的测试响应延迟期是 15 秒。

  如果为此已链接后缀只定义了一个远程服务器，则对远程服务器的所有已链接操作将阻塞 30 秒，以防止超载。如果已定义了故障切换服务器，则已链接的操作将开始使用下一个已定义的备用服务器。

使用控制台设置默认链接参数

1. 在 Directory Server 控制台的顶级 “目录”标签上，展开目录树并选择以下条目：cn=default instance config,cn=chaining database,cn=plugins,cn=config。
2. 双击此条目或选择 “对象” > “用通用编辑器进行编辑”菜单项。从以上列表中根据需要修改属性值。
3. 在 “通用编辑器”对话框中单击 “保存”，所做的更改将立即生效。

从命令行设置默认链接参数

1. 使用 `ldapmodify` 命令编辑条目 `cn=default instance config,cn=chaining database,cn=plugins,cn=config`。此条目的所有属性成为新的已链接后缀中参数的默认值。

   例如，在新的已链接后缀中，以下命令将默认大小限制增加到 5000 个条目，将默认时间限制减少到 10 分钟。

   ```
   ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn=default instance config,cn=chaining database,
    cn=plugins,cn=config
   changetype:modify
   replace:nsslapd-sizelimit
   nsslapd-sizelimit: 5000
   -
   replace:nsslapd-timelimit
   nsslapd-timelimit: 600
   ^D
   ```

   对此条目所做的修改将立即生效。

使用控制台创建已链接的后缀

下列过程与创建已链接的根后缀和已链接的子后缀的过程几乎相同：

1. 在 Directory Server 控制台上选择 “配置”标签。

- 对于已链接的根后缀，右键单击 “数据”节点，然后从弹出菜单中选择 “新建已链接的后缀”。或者，可以选择 “数据”节点，并从 “对象”菜单中选择 “新建已链接的后缀”。
- 对于已链接的子后缀，展开 “数据”节点和任何后缀节点以显示父后缀。右键单击父后缀节点，从弹出菜单中选择 “新建已链接的子后缀”。或者，可以选择父后缀节点，并从 “对象”菜单中选择 “新建已链接的子后缀”。

  显示 “新建已链接的 （子）后缀”对话框。

2. 在要链接到的远程服务器上输入条目的 DN。远程条目不一定是远程后缀的基本条目：

- 对于根后缀，在 “后缀 DN”字段中输入远程条目的完整 DN。可以输入作为远程目录树中一个条目的任一 DN。该条目将是已链接的根后缀的基础，此条目下的所有内容都将通过已链接的后缀获得。
- 对于子后缀，输入将要链接的条目的子后缀 RDN。该条目将是已链接的子后缀的基础。文本字段下出现的完整的子后缀名称必须是存在于远程服务器中的条目。

3. 输入包含后缀数据 （如有必要，也包括域）的远程服务器的主机名。

4. 输入用于访问远程服务器的端口号，如果该端口是安全端口，请选中该复选框。使用安全端口时，将通过 SSL 对链接操作进行加密。详细信息，请参阅 “使用 SSL 链接”（第 100 页）。

   对话框底部的文本将显示远程服务器的完整 URL。

5. 在远程服务器上输入代理身份的绑定 DN 和口令。访问远程服务器上后缀的内容时，本地服务器将此 DN 用作代理。例如，使用在 “创建代理身份”（第 90 页）中定义的 `uid=` *主机 1*`_proxy,cn=config` DN。

   不能使用远程服务器上目录管理员的 DN。通过已链接后缀执行的操作将在 `creatorsName` 和 `modifiersName` 属性中使用此代理身份。可以忽略代理 DN，在此情况下，本地服务器将在访问远程服务器时匿名进行绑定。

6. 单击 “确定”以创建已链接的后缀。新后缀将出现在配置树中，并带有链接图标。

7. 单击新的已链接后缀以选择它，然后在右侧面板中选择 “远程服务器”标签。

8. 可选地，可为此已链接的后缀定义一个或多个故障切换服务器。如果此服务器无法与远程服务器联系，则它将按定义的顺序尝试每个故障切换服务器，直到有一个服务器响应为止。故障切换服务器必须包含正在链接的相同后缀，并允许使用同一个绑定 DN 执行代理。

   要定义故障切换服务器，请在 “远程服务器 URL”字段中输入多个由空格分隔的主机名和端口号对。此字段采用下列格式：

   ```
   ldap[s]://hostname[:port][ hostname[:port]].../
   ```

9. 在 “远程服务器”标签底部，文本框显示允许通过链接执行代理操作所需的 ACI。必须将此 ACI 添加到其 *suffixDN* 位于远程服务器上的条目中。如果定义了任何故障切换服务器，则应将此 ACI 添加到所有这些服务器中。使用 “复制 ACI”按钮将 ACI 文本复制到系统的剪贴板上进行粘贴。

   将此 ACI 添加到远程服务器上的基本条目后，已链接的后缀在本地服务器的目录树中将是可见的。

警告 可能需要在同一个条目上定义其他 ACI 以限制对目前通过链接而公开的远程服务器进行访问。请参阅 “通过已链接的后缀进行的访问控制”（第 99 页）。

10. 如果已为服务器组件配置了链接策略，则还必须添加将允许这些组件访问远程服务器的 ACI。例如，如果允许对引荐完整性插件进行链接，则必须将下列 ACI 添加到已在步骤 2 中给出其 DN 的基本条目中：

```
aci:(targetattr "*")
 (target="ldap:///suffixDN")
 (version 3.0; acl "RefInt Access for chaining"; allow
 (read,write,search,compare) userdn = "ldap:///cn=referential
 integrity postoperation,cn=plugins,cn=config";)
```

从命令行创建已链接的后缀

还可以使用 `ldapmodify` 命令行公用程序在目录中创建已链接的后缀。由于已链接的根后缀和已链接的子后缀都由服务器以相同方式在内部进行管理，所以从命令行创建已链接的根后缀和已链接的子后缀的过程几乎相同。

1. 使用以下命令为已链接的根后缀在 `cn=mapping tree,cn=config` 下创建已链接的后缀条目：

   ```
   ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn=suffixDN,cn=mapping tree,cn=config
   objectclass:top
   objectclass:extensibleObject
   objectclass:nsMappingTree
   cn:suffixDN
   nsslapd-state:backend
   nsslapd-backend:databaseName
   ^D
   ```

   对于已链接的子后缀，请使用带另一属性的相同命令：
   `nsslapd-parent-suffix:`*parentSuffixDN*

   对于已链接的子后缀， *suffixDN* 是子后缀的 RDN 和其父后缀的 DN，例如 `l=Europe,dc=example,dc=com`。 *suffixDN* 必须是通过远程服务器可用的条目的 DN，但它不一定是远程后缀的基本条目。

注意 虽然后缀名称采用 DN 格式，但将其视作单个字符串。因此，所有空格都有意义，都是后缀名称的一部分。为了使服务器访问远程条目，*suffixDN* 字符串必须采用远程后缀中使用的间隔。

   databaseName 是链接插件组件用于标识这个已链接后缀的昵称。此名称在所有后缀的 *databaseNames* 中是唯一的，按照约定，它是 *suffixDN* 的第一个命名组件的值。与本地后缀不同，已链接的后缀在本地服务器上没有任何数据库文件。

   对于子后缀， *parentSuffixDN* 即是父后缀的 DN。父后缀可以是本地后缀，也可以是已链接的后缀。

2. 使用以下命令创建链接配置条目：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=databaseName,cn=chaining database,cn=plugins,cn=config
objectclass:top
objectclass:extensibleObject
objectclass:nsBackendInstance
cn:databaseName
nsslapd-suffix:suffixDN
nsfarmserverurl:LDAPURL
nsmultiplexorbinddn:proxyDN
nsmultiplexorcredentials:ProxyPassword
^D
```

其中， *databaseName* 和 *suffixDN* 的值必须与上个步骤中使用的值相同。 *LDAPURL* 是远程服务器的 URL，但它不包含任何后缀信息。 URL 可以包含采用下列格式列出的故障切换服务器：

```
ldap[s]://主机名[:端口][ 主机名[:端口]].../
```

在 LDAP URL 中列出的所有远程服务器都必须包含 *suffixDN*。有关指定安全端口的信息，请参阅 “使用 SSL 链接”（第 100 页）。

proxyDN 是远程服务器上代理身份的 DN。访问远程服务器上后缀的内容时，本地服务器将此 DN 用作代理。通过已链接后缀执行的操作将在 `creatorsName` 和 `modifiersName` 属性中使用此代理身份。如果未指定代理 DN，本地服务器在访问远程服务器时将匿名进行绑定。

ProxyPassword 是代理 DN 的未加密的口令值。如果口令存储在配置文件中，则将对口令进行加密。例如：

```
nsmultiplexorbinddn:uid=host1_proxy,cn=config
nsmultiplexorcredentials:secret
```

警告 应通过加密端口执行 `ldapmodify` 命令以避免发送明文口令。

新条目将自动包括所有链接参数，默认值已在 `cn=default instance config,cn=chaining database,cn=plugins,cn=config` 中定义。创建链接配置条目时，可以通过设置具有不同值的属性覆盖其中的任何值。有关可定义其值的属性列表，请参阅 “设置默认链接参数”（第 92 页）。

3. 使用以下命令在远程条目上创建 ACI。需要此 ACI 以允许通过链接执行代理操作。有关 ACI 的详细信息，请参阅第 6 章 “管理访问控制”。

```
ldapmodify -h 主机2 -p 端口2 -D "cn=Directory Manager" -w 口令2
dn:suffixDN
changetype:modify
add:aci
aci:(targetattr=*)(target = "ldap:///suffixDN")(version 3.0;acl
 "Allows use of admin for chaining"; allow (proxy)
 (userdn="ldap:///proxyDN");)
^D
```

警告 可能需要在同一个条目上定义其他 ACI 以限制对目前通过此服务器而公开的远程服务器进行访问。请参阅 “通过已链接的后缀进行的访问控制”（第 99 页）。

4. 如果已为服务器组件配置了链接策略，则还必须添加将允许这些组件访问远程服务器的 ACI。例如，如果允许对引荐完整性插件进行链接，则必须将下列 ACI 添加到基本条目中 , 该条目的 *suffixDN* 为：

```
aci:(targetattr "*")
 (target="ldap:///suffixDN")
 (version 3.0; acl "RefInt Access for chaining"; allow
 (read,write,search,compare) userdn = "ldap:///cn=referential
 integrity postoperation,cn=plugins,cn=config";)
```

下列命令给出创建已链接的子后缀的示例。注意，只有当逗号出现在 DN 的命名属性中时， suffixDN 中的逗号才必须用反斜杠进行转义 (\)。

代码示例 3-1 使用命令行创建已链接的子后缀

```
ldapmodify -a -h 主机1 -p 端口1 -D "cn=Directory Manager" -w 口令1
dn:cn=l=Europe\,dc=example\,dc=com,cn=mapping tree,cn=config
objectclass:top
objectclass:extensibleObject
objectclass:nsMappingTree
cn:l=Europe,dc=example,dc=com
nsslapd-state:backend
nsslapd-backend:Europe
nsslapd-parent-suffix:dc=example,dc=com

dn:cn=Europe,cn=chaining database,cn=plugins,cn=config
objectclass:top
objectclass:extensibleObject
objectclass:nsBackendInstance
cn:Europe
nsslapd-suffix:l=Europe,dc=example,dc=com
nsfarmserverurl:ldap:// 主机2: 端口2/
nsmultiplexorbinddn:uid= 主机1_proxy,cn=config
nsmultiplexorcredentials:proxyPassword
```

代码示例 3-1　　使用命令行创建已链接的子后缀 （续）

```
^D

ldapmodify -h 主机2 -p 端口2 -D "cn=Directory Manager" -w 口令2
dn:l=Europe,dc=example,dc=com
changetype:modify
add:aci
aci:(targetattr=*)(target =
 "ldap:///l=Europe,dc=example,dc=com")(version 3.0;acl
 "Allows use of admin for chaining"; allow (proxy)
 (userdn="ldap:///uid=host1_proxy,cn=config");)
^D
```

通过已链接的后缀进行的访问控制

当已验证的用户访问已链接后缀时，服务器会将此用户的身份发送到远程服务器。访问控制始终在远程服务器上进行评估。在远程服务器上评估的每个 LDAP 操作使用客户机应用程序 （通过已代理的授权控件进行传递）的原始身份。只有当用户对远程服务器上包含的子树具有正确的访问控制时，操作才能在远程服务器上获得成功。这表示需要向远程服务器添加仅有少许限制的常规访问控制：

- 不能使用所有类型的访问控制。

  例如，基于角色或基于过滤器的 ACI 需要访问用户条目。因为您正通过已链接的后缀访问数据，所以只能验证代理控件中的数据。请考虑以某种方式设计目录，使用户条目与用户数据位于同一个后缀中。

- 所有基于客户机的 IP 地址或 DNS 域的访问控制可能行不通，因为客户机的原始域在链接过程中已丢失。

  远程服务器将客户机应用程序视为与已链接后缀具有相同 IP 地址并在同一个 DNS 域中。

以下限制适用于所创建的与已链接后缀一起使用的 ACI：

- ACI 必须与其使用的组位于同一服务器上。如果组为动态，则组中的所有用户必须与 ACI 和组位于同一位置。如果组为静态，则它指远程用户。
- ACI 必须与其使用的任何角色定义以及任何想拥有这些角色的用户位于同一服务器。
- 如果是远程用户，则引荐用户的条目值 （如 `userattr` 主题规则）的 ACI 将有效。

虽然通常在远程服务器上评估访问控制，但仍可选择在包含已链接后缀的服务器和远程服务器上都进行评估。这会有一些限制：

- 在访问控制评估过程中，用户条目的内容并不一定可用 （例如，如果访问控制是在包含已链接后缀的服务器上评估，且条目位于远程服务器上）。

  出于性能原因，客户机不可进行远程查询和评估访问控制。

- 已链接的后缀不一定对正由客户机应用程序修改的条目具有访问权。

  当执行修改操作时，已链接的后缀不具有对存储在远程服务器上的全部条目的访问权。如果执行删除操作，已链接的后缀只知道条目的 DN。如果访问控制指定了特定属性，则当通过已链接后缀执行删除操作时，删除操作将失败。

默认情况下，包含已链接后缀的服务器上设置的访问控制将不被评估。要覆盖此默认设置，请使用 `cn=`*databaseName*`,cn=chaining database,cn=plugins,cn=config` 条目中的 `nsCheckLocalACI` 属性。但是，除非使用级联链接，否则不推荐在包含已链接后缀的服务器上评估访问控制。详细信息，请参阅 “配置级联链接”（第 112 页）。

使用 SSL 链接

当对已链接的后缀执行操作时，可配置服务器以使用 SSL 与远程服务器进行通讯。使用 SSL 进行链接包括以下步骤：

1. 在远程服务器上启用 SSL。
2. 在包含已链接后缀的服务器上启用 SSL。

   有关启用 SSL 的详细信息，请参阅第 11 章 “实现安全性”。

3. 在创建或修改已链接后缀的过程中指定 SSL 和远程服务器的安全端口。

   当使用控制台时，请在已链接后缀的创建或配置过程中选中安全端口复选框。请参阅 “使用控制台创建已链接的后缀”（第 94 页）或 “使用控制台修改链接策略”（第 104 页）。

   当使用命令行过程时，请指定 LDAPS URL 和远程服务器的安全端口，例如：`ldaps://example.com:636/`。请参阅 “从命令行创建已链接的后缀”（第 96 页）或 “从命令行修改链接策略”（第 104 页）。

当配置已链接的后缀和远程服务器以使用 SSL 进行通讯时，并不表示进行操作请求的客户机应用程序也必须使用 SSL 进行通讯。客户机可使用 LDAP 协议或 DSML 协议的两个端口之一。

管理已链接的后缀

本节说明如何更新和删除现有已链接的后缀以及如何控制链接机制。

配置链接策略

服务器的链接策略确定哪些 LDAP 控件将拓展到链接的服务器，以及允许哪些服务器组件访问链接的后缀。应了解这些设置及其对涉及已链接后缀的操作的影响。链接策略将用于服务器上的所有已链接后缀。

默认设置用于允许透明完成一般操作。但是，如果操作涉及 LDAP 控件，或者使用引荐完整性插件之类的服务器组件，则应确保按需要配置链接策略。

最好在创建任何已链接后缀之前先配置链接策略，以便一启用已链接后缀就可应用策略。不过，也可在以后任何时间修改策略。

LDAP 控件的链接策略

LDAP 控件由客户机作为请求的一部分发送，以便以某种方式对操作或其结果进行修改。服务器链接策略确定服务器将哪些控件随操作转发给已链接的后缀。默认情况下，以下控件将被转发给已链接后缀的远程服务器：

表 3-1　　默认情况下允许链接的 LDAP 控件

控件的 OID	控件的名称和说明
1.2.840.113556.1.4.473	服务器端排序 - 与搜索关联以根据其属性值对结果条目进行排序。*
1.3.6.1.4.1.1466.29539.12	链接循环检测 - 跟踪服务器与另一服务器链接的次数。当链接计数达到配置的数字时，将放弃操作并通知客户机应用程序。详细信息，请参阅 “传输用于级联的 LDAP 控件”（第 114 页）。
2.16.840.1.113730.3.4.2	智能引荐的受管 DSA - 以条目返回智能引荐，而非遵循引荐。这将允许更改或删除智能引荐本身。
2.16.840.1.113730.3.4.9	虚拟列表视图 (VLV) - 提供搜索的部分结果，而非一次返回所有结果条目。*

(*) 服务器端排序和 VLV 控件仅当搜索范围为单一后缀时才可通过链接受支持。当客户机应用程序对多个后缀发出请求时，已链接的后缀无法支持 VLV 控件。

下表列出了通过配置链接策略可允许链接的其他 LDAP 控件：

表 3-2 可链接的 LDAP 控件

控件的 OID	控件的名称和说明
1.3.6.1.4.1.42.2.27.9.5.2	获得有效的权限请求 - 要求服务器在结果中返回有关条目和属性的访问权限和 ACI 的信息。
2.16.840.1.113730.3.4.3	持续的搜索 - 表明服务器应使操作保持活动状态，而且无论何时添加、删除或修改与搜索过滤器匹配的条目，都将结果发送到客户机。
2.16.840.1.113730.3.4.4	口令过期通知 - 通知客户机应用程序其口令已过期。
2.16.840.1.113730.3.4.5	口令到期通知 - 通知客户机应用程序其口令将在给定时间内到期。
2.16.840.1.113730.3.4.12	已代理的授权 （旧规范）- 允许客户机在请求期间内采用另一个身份。 *
2.16.840.1.113730.3.4.13	复制更新信息 - 包含通用唯一标识符 (UUID) 和复制操作的更改序列号 (CSN)。
2.16.840.1.113730.3.4.14	特定的数据库搜索 - 用于搜索操作以指定搜索必须在控件中命名的数据库上执行。
2.16.840.1.113730.3.4.15	验证响应 - 与绑定响应一起返回到客户机应用程序以提供 DN 和使用的验证方法 （采用 SASL 或证书时有用）。
2.16.840.1.113730.3.4.16	验证请求 - 提供绑定请求以要求服务器在绑定响应中提供其证书。
2.16.840.1.113730.3.4.17	仅真实属性请求 - 表明服务器应仅返回真实包含在返回条目中的属性，并不需要解决虚拟属性。
2.16.840.1.113730.3.4.18	已代理的授权 （新规范）- 允许客户机在请求期间内采用另一个身份。 *
2.16.840.1.113730.3.4.19	仅虚拟属性请求 - 表明服务器应仅返回由角色和服务类功能生成的属性。

(*) 应用程序可以使用任何一种已代理的授权控件。对于两种控件的 OID 而言，应该具有相同的链接策略。详细信息，请参阅 “传输用于级联的 LDAP 控件”（第 114 页）。

服务器组件的链接策略

组件是服务器中使用内部操作的任何属性或功能单元。例如，插件就被视为组件。对于大多数组件而言，要执行其任务，必须访问目录内容，包括配置数据或存储在目录中的用户数据。

默认情况下，不允许链接任何服务器组件。如果要让组件访问已链接的后缀，则必须明确允许链接。可访问已链接数据的组件按其 DN 列出如下。

如 “使用控制台创建已链接的后缀”（第 94 页）中所述，必须在远程服务器上的 ACI 中授予一定的权限以允许链接。当链接服务器组件时，必须在此 ACI 中允许搜索、读取和比较，以便服务器组件可以执行这些操作。此外，某些组件要求在远程服务器上的写入权限，如列表中所述：

- `cn=ACL Plugin,cn=plugins,cn=config` - ACL 插件实现访问控制功能。不能链接用于检索和更新 ACI 属性的操作，因为混合本地和远程 ACI 属性不安全。不过，可以链接用于访问用户条目的请求。有关围绕 ACI 和链接的限制的进一步信息，请参阅第 164 页的 “ACI 限制”。
- `cn=old plugin,cn=plugins,cn=config` - 此插件代表所有 Directory Server 4.x 插件，以及是否允许它们链接。 4.x 插件共享同一链接策略。可能需要在远程服务器上根据 4.x 插件执行的操作设置 ACI。
- `cn=resource limits,cn=components,cn=config` - 此组件根据用户绑定 DN 设置资源使用限制。允许链接此组件时，可对其身份存储在已链接后缀中的用户强制执行资源限制。
- `cn=certificate-based authentication,cn=components,cn=config` - 当使用 SASL 外部绑定方法时使用此组件。它从远程服务器检索用户证书。

警告 从已链接的后缀允许基于证书的验证可能造成安全漏洞。如果其他后缀链接到不受信任的远程服务器，则不受信任服务器上的证书可用于验证。

- `cn=referential integrity postoperation,cn=plugins,cn=config` - 该插件确保条目的删除会拓展到可能已引用了其 DN 的其他条目，如组成员列表。当组成员位于已链接的后缀中时，链接使用此插件有助于简化静态组的管理。当此插件访问已链接的后缀时，它要求远程服务器上的写权限。
- `cn=uid uniqueness,cn=plugins,cn=config` - UID 唯一性插件确保指定属性的所有新值在服务器上都是唯一的。允许此插件链接将确保其在整个目录树中的唯一性。

注意 以下组件不能被链接：

- 角色插件
- 口令策略组件
- 复制插件

使用控制台修改链接策略

1. 在 Directory Server 控制台的 “配置”标签上，选择 “数据”节点，并在右侧面板中选择 “链接”标签。
2. 从右侧列表中选择一个或多个 LDAP 控件，然后单击 “添加”以允许它们链接。使用 “添加”和 “删除”按钮创建允许链接的控件列表。

   按其 OID 列出 LDAP 控件。请参阅 “LDAP 控件的链接策略”（第 101 页），以获取每个控件的名称和说明。
3. 允许链接的服务器组件列在同一标签的底端。从右侧列表中选择一个或多个组件名称，然后单击 “添加”以允许它们链接。使用 “添加”和 “删除”按钮创建允许链接的组件列表。

   请参阅 “服务器组件的链接策略”（第 102 页），以获取每个组件的说明。
4. 单击 “保存”以保存链接策略。
5. 重新启动服务器以使更改生效。

从命令行修改链接策略

`cn=config,cn=chaining database,cn=plugins,cn=config` 条目包含链接策略配置的属性。使用 `ldapmodify` 命令编辑此条目：

1. 修改 `nsTransmittedControls` 多值属性，以使其包含所有允许链接的 LDAP 控件的 OID。请参阅 “LDAP 控件的链接策略”（第 101 页），以获取所有可被链接的控件的 OID。

   例如，以下命令将有效的权限控件添加到已链接控件的列表中：

   ```
   ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn=config,cn=chaining database,cn=plugins,cn=config
   changetype:modify
   add:nsTransmittedControls
   nsTransmittedControls: 1.3.6.1.4.1.42.2.27.9.5.2
   ^D
   ```

   如果客户机应用程序使用自定义控件，而且您希望允许它们链接，则也可将其 OID 添加到 `nsTransmittedControls` 属性。
2. 修改 `nsActiveChainingComponents` 多值属性，以使其包含所有允许链接的服务器组件的 DN。请参阅 “服务器组件的链接策略”（第 102 页），以获取每个组件的说明。

   例如，以下命令将引荐完整性组件添加到已链接组件的列表中：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=config,cn=chaining database,cn=plugins,cn=config
changetype:modify
add:nsActiveChainingComponents
nsActiveChainingComponents:cn=referential integrity
 postoperation,cn=components,cn=config
^D
```

3. 修改了链接策略配置条目后，就必须重新启动服务器以使更改生效。

禁用或启用已链接的后缀

某些时候可能由于维护或安全原因需要使已链接的后缀不可用。禁用后缀可防止服务器与远程服务器联络以响应任何试图访问后缀的客户机操作。如果有已定义的默认引荐，则在客户机尝试访问已禁用的后缀时，该引荐将被返回。

使用控制台禁用或启用已链接的后缀

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点，然后选择要禁用的已链接后缀。
2. 在右侧面板中选择 “设置”标签。默认情况下，所有已链接的后缀在创建时已启用。
3. 取消选中 “启用对该后缀的访问权限”复选框以禁用此后缀，或选中此复选框以启用此后缀。
4. 单击 “保存”应用更改并立即禁用或启用此后缀。
5. 可选地，禁用此后缀时，也可为对此后缀执行的所有操作设置将返回的全局默认引荐。此设置位于顶级 “配置”标签的根节点的 “网络”标签上。详细信息，请参阅 “使用控制台设置默认引荐”（第 67 页）。

从命令行禁用或启用后缀

1. 请用以下命令编辑已链接的后缀条目中的 `nsslapd-state` 属性：

   ```
   ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn=suffixDN,cn=mapping tree,cn=config
   changetype:modify
   replace:nsslapd-state
   nsslapd-state:disabled or backend
   ^D
   ```

   其中， *suffixDN* 为后缀 DN 定义时的完整字符串，包括空格或反斜杠 (\) 以避免在值中使用逗号。将 `nssladp-state` 属性设置为值 `disabled` 可禁用后缀，设置为值 `backend` 可实现完全访问。

成功执行命令后，将立即禁用后缀。

2. 可选地，禁用此后缀时，也可为对此后缀执行的所有操作设置将返回的全局默认引荐。详细信息，请参阅 “从命令行设置默认引荐”（第 67 页）。

设置访问权限和引荐

如果要限制对已连接后缀的访问而不完全禁用它，则可以修改访问权限以允许只读访问。在此情况下，必须定义对另一个服务器的引荐，以用于写操作。还可以同时拒绝读写访问，为对后缀执行的所有操作定义引荐。

有关一般引荐的详细信息，请参阅 *Sun ONE Directory Server 部署指南*。

使用控制台设置访问权限和引荐

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点，然后选择要设置引荐的已链接后缀。
2. 在右侧面板中选择 “设置”标签。如果启用了已链接的后缀，则将只能设置权限和引荐。
3. 选择以下某一单选按钮，以设置对此后缀中条目进行任何写操作时的响应：
   - 处理读写请求 - 默认情况下将选择此单选按钮，它代表正常行为。读取和写入操作都将转发到远程服务器，并将结果返回客户机。可以定义引荐，但不会将它们返回到客户机。
   - 处理读请求并返回写请求引荐 - 服务器将仅转发读请求并将其结果返回客户机。请在列表中输入将作为写请求引荐返回的一个或多个 LDAP URL。
   - 为读写请求返回引荐 - 在列表中输入将作为所有操作引荐返回的一个或多个 LDAP URL。此行为类似于禁用对后缀的访问，不同的是，此行为可以为此后缀专门定义引荐，而不是使用全局默认引荐。
4. 通过 “添加”和 “删除”按钮编辑引荐列表。单击 “添加”按钮将显示一个对话框，用于创建新引荐的 LDAP URL。可以在远程服务器中创建对任何分支的 DN 的引荐。有关 LDAP URL 结构的详细信息，请参阅 *Sun ONE Directory Server 入门指南*。

   可输入多个引荐。该目录将返回此列表中的所有引荐，以响应来自客户机应用程序的请求。
5. 单击 “保存”应用更改并立即开始执行新的权限和引荐设置。

使用控制台设置访问权限和引荐

在以下命令中， *suffixDN* 是已链接后缀定义时的完整字符串，包括所有空格。*LDAPURL* 是有效的 URL，它包含主机名、端口号和目标的 DN，例如：

```
ldap://alternate.example.com:389/ou=People,dc=example,dc=com
```

1. 使用以下命令编辑已链接的后缀条目：

   ```
   ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn=suffixDN,cn=mapping tree,cn=config
   changetype:modify
   replace:nsslapd-state
   nsslapd-state:referral on update or referral
   -
   add:nsslapd-referral
   nsslapd-referral:LDAPURL
   ^D
   ```

   可以重复最后一个更改语句以将 LDAP URL 的任何数字添加到 `nsslapd-referral` 属性中。

   当 nsslapd-state 的值是 `referral on update` 时，此后缀为只读且所有 LDAP URL 都将作为写操作引荐返回。当值是 `referral` 时，系统将拒绝读写操作并为任一请求返回引荐。

2. 此后缀将变为只读或不可访问，并准备在成功执行命令后立即返回引荐。

修改链接参数

定义了已链接的后缀后，就可修改控制链接的参数。可以指定如何访问远程服务器、如何更改用于代理的 DN，甚至如何更改远程服务器。还可修改性能参数，这些参数控制服务器如何建立和维护与已链接服务器的连接。

使用控制台修改链接参数

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点，然后选择要修改的已链接后缀。
2. 在右侧面板中选择 “远程服务器”标签。
3. 要更改远程服务器的名称或端口，请修改 “远程服务器 URL”字段。该 URL 包含以下格式的一个或多个远程服务器的主机名和可选端口号：

   ```
   ldap[s]:// 主机名 [: 端口 ][ 主机名 [: 端口 ]].../
   ```

此 URL 不包括任何后缀信息。有关指定安全端口的信息，请参阅 “使用 SSL 链接”（第 100 页）。当 URL 中的第一个服务器响应链接请求失败时，将按列出的顺序与 URL 中的其他服务器联系。所有在 LDAP URL 中列出的远程服务器必须包含 *suffixDN*，它是已链接后缀的基本条目。

4. 要更改代理用户的 DN，请在 “绑定 DN”字段中输入一个新值。在 “口令”字段中输入并确认此 DN 的相应口令。

   proxyDN 是远程服务器上的用户的 DN。访问远程服务器上后缀的内容时，本地服务器将此 DN 用作代理。通过已链接后缀执行的操作将在 `creatorsName` 和 `modifiersName` 属性中使用此代理身份。如果未指定代理 DN，本地服务器在访问远程服务器时将匿名进行绑定。

5. 标签底部的文本框显示允许链接此后缀所需要的 ACI。如果更改了远程服务器 URL，则必须将该 ACI 添加到其 *suffixDN* 位于新的一台或多台远程服务器上的条目中。如果修改了代理 DN, 则应更新所有已链接服务器上的 ACI。使用 “复制 ACI”按钮将 ACI 文本复制到系统的剪贴板上进行粘贴。

6. 选择 “限制和控制”标签以配置用于链接请求的参数。在 “配置级联链接”（第 112 页）中描述了级联链接参数。

7. 设置 “控制客户机返回”参数以限制已链接操作的大小和时间：

   - 返回范围搜索的引荐 - 范围完全在已链接后缀中的搜索是效率低的搜索，因为结果被传输了两次。默认情况下，服务器将返回对已链接服务器的引荐，强制客户机直接在已链接服务器上执行搜索。如果取消选择此选项，则应设置以下参数以限制将被链接的结果的大小。

   - 大小限制或无大小限制 - 此参数确定为响应已链接的搜索操作而将返回的条目数量。默认值大小限制是 2000 个条目。如果要限制对涉及的已链接后缀进行大范围搜索，请将此参数设置为较低的值。在任何情况下，操作将受远程服务器上的任何大小设置所限制。

   - 时间限制或无时间限制 - 此参数控制已链接操作的时间长度。默认时间限制是 3600 秒 （1 小时）。如果要限制对已链接后缀执行操作的时间，则将此参数设置为较低的值。在任何情况下，操作将受远程服务器上的任何时间设置所限制。

8. 设置 “连接管理”参数以控制服务器如何管理网络连接以及与远程服务器的绑定：

   - 最大的 LDAP 连接数。已链接的后缀通过远程服务器可以建立的最大同时发生的 LDAP 连接数。默认值是 10 个连接。

   - 最大的 TCP 连接数。已链接的后缀通过远程服务器可以建立的最大同时发生的 TCP 连接数。默认值是 3 个连接。

- 每个连接最大的绑定数。每个 LDAP 连接最大的同时绑定操作数。默认值是每个连接有 10 个突出绑定操作。
- 最大的绑定重试次数。出错时，已链接的后缀尝试重新绑定到远程服务器上的次数。值 0 表示已链接的后缀将仅尝试绑定一次。默认值为尝试 3 次。
- 每个连接最大的操作数。每个 LDAP 连接最大的同时操作数。默认值是每个连接有 10 个操作。
- 绑定超时或无绑定超时。链接服务器上绑定尝试超时之前的时间长度 （以秒为单位）。默认值为 15 秒。
- 放弃前的超时或无超时。服务器检查是否已放弃某个操作之前的秒数。默认值为 2 秒。
- 连接生命周期或无限制。已链接的后缀与远程服务器之间的连接保持打开状态以便可以重新使用的时间长度。将连接保持为打开状态可以加快访问速度，但要使用更多的资源。例如，如果使用拨号连接，则希望限制连接时间。默认情况下，连接不受限制。

错误检测参数无法通过控制台获取。请参阅 “从命令行修改链接参数”（第 109 页）。

9. 完成链接参数的设置后请单击 “保存”。

从命令行修改链接参数

从命令行，可设置使用控制台时设置的所有相同参数，并且也可配置 “错误检测参数”（第 93 页）中描述的其他参数：

1. 使用以下命令编辑对应于要修改的后缀的链接配置条目：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=databaseName,cn=chaining database,cn=plugins,cn=config
changetype:modify
replace:attributeName
attributeName:attributeValue
-
changetype:modify
replace:attributeName
attributeName:attributeValue
...
^D
```

以下步骤说明了可能的属性名和值。可在命令中包括多个更改语句，以便一次更改任意多个参数。

2. 修改 `nsfarmserverURL` 属性以更改远程服务器的名称或端口。该属性值为包含以下格式的一个或多个远程服务器的主机名和可选端口号的 URL：

```
ldap[s]:// 主机名 [: 端口 ][ 主机名 [: 端口 ]].../
```

此 URL 不包括任何后缀信息。有关指定安全端口的信息，请参阅 “使用 SSL 链接”（第 100 页）。当 URL 中的第一个服务器响应链接请求失败时，将按列出的顺序与 URL 中的其他服务器联系。所有在 LDAP URL 中列出的远程服务器必须包含 *suffixDN*，它是已链接后缀的基本条目。

3. 修改 `nsmultiplexorBindDN` 和 `nsmultiplexorCredentials` 属性以更改用于代理访问远程服务器的 DN。

   访问远程服务器上后缀的内容时，本地服务器将此 DN 用作代理。通过已链接后缀执行的操作将在 `creatorsName` 和 `modifiersName` 属性中使用此代理身份。如果未指定代理 DN，本地服务器在访问远程服务器时将匿名进行绑定。

4. 如果修改代理 DN 或其凭证，则必须在远程服务器上创建相应的 ACI。需要此 ACI 以允许通过链接执行代理操作：

   ```
   ldapmodify -h 主机2 -p 端口2 -D "cn=Directory Manager" -w 口令2
   dn:suffixDN
   changetype:modify
   add:aci
   aci:(targetattr=*)(target = "ldap:///suffixDN")(version 3.0;acl
    "Allows use of admin for chaining"; allow (proxy)
    (userdn="ldap:///proxyDN");)
   ^D
   ```

5. 设置 “设置默认链接参数”（第 92 页）中描述的任何属性，以控制远程服务器上的连接和操作处理。在 “配置级联链接”（第 112 页）中进一步说明了级联参数。

优化线程使用

也可设置服务器全局使用的线程数以考虑用于链接的线程资源。已链接的操作可能会占用很长时间，因为必须将它们转发到远程服务器，但当远程服务器处理操作时它们的线程为空闲状态。如果已链接的服务器严重延迟，则应增加线程数，以便有更多的资源可用于同时处理本地操作。

默认情况下，服务器使用的线程数为 30 个。但是，当使用已链接的后缀时，可通过增加可用于处理操作的线程数来提高性能。根据已链接后缀的数量、在其执行的操作数和操作类型，以及在远程服务器上处理操作需要的平均时间来确定需要的线程数。

通常，应将每个已链接后缀的线程数增加 5 到 10 个 （假定已链接的后缀是与本地后缀相同数量的操作的目标）。

使用控制台设置线程资源

1. 在 Directory Server 控制台的顶级 “配置”标签上，单击 “性能”节点，然后在右侧面板中选择 “杂项”标签。
2. 在 “最大线程数”字段中输入新值。
3. 单击 “确定”以保存更改，并确认需要重新启动服务器以使更改生效的消息。
4. 重新启动 Directory Server 以使用新的线程数。

从命令行设置线程资源

1. 使用以下命令编辑全局配置条目以修改线程数：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=config
changetype:modify
replace:nsslapd-threadnumber
nsslapd-threadnumber:newThreadNumber
^D
```

2. 重新启动 Directory Server 以使用新的线程数。

删除已链接的后缀

删除一个已链接的后缀将使其不可通过本地目录树访问，但不会删除已链接服务器上的条目或后缀。可以删除父后缀，并将其子后缀作为新的根后缀保存在目录中。

使用控制台删除已链接的后缀

1. 在 Directory Server 控制台的 “配置”标签上，展开 “数据”节点。
2. 右键单击要删除的后缀，从弹出菜单中选择 “删除”。

   或者，可以选择后缀节点，并从 “对象”菜单中选择 “删除”。
3. 出现确认对话框，告知可通过此已链接后缀访问的条目将*不会*从远程目录中删除。

   另外，对于父后缀，可以选择采用递归方式删除其所有子后缀。如果要删除整个分支，请选择 “删除此后缀及其所有子后缀”。否则，如果只想删除此特定后缀并在目录中保存其子后缀，请选择 “只删除此后缀”。
4. 单击 “确定”以删除此后缀。

   显示进程对话框，告知您这些步骤正在由控制台完成。

从命令行删除后缀

要从命令行删除后缀，请使用 ldapdelete 命令从目录中删除其配置条目。

如果要删除包含子后缀的整个分支，则必须找到已删除的父后缀的子后缀，并对每个后缀及其可能的子后缀重复此过程。

1. 使用以下命令删除后缀配置条目：

   ```
   ldapdelete -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   cn=suffixDN,cn=mapping tree,cn=config
   ```

   此命令使此已链接后缀及其远程条目在目录中再也不可见。

2. 删除位于 cn=*databaseName*,cn=chaining database,cn=plugins,cn=config 中的相应数据库配置条目及其下面的监视器条目：

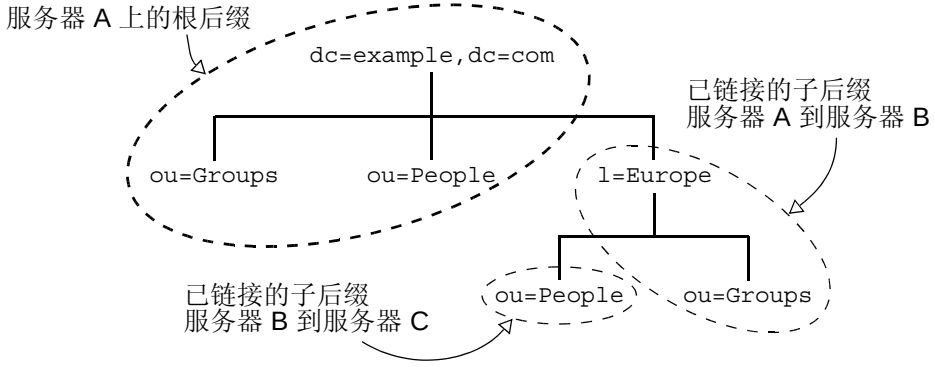
   ```
   ldapdelete -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   cn=monitor,cn=dbName,cn=chaining database,cn=plugins,cn=config
   cn=dbName,cn=chaining database,cn=plugins,cn=config
   ```

配置级联链接

在级联链接中，从一个服务器链接的子树可能自身也是一个已链接后缀或包含已链接的子后缀。当操作包含一个服务器中的已链接后缀时，它将被转发到中间服务器，该中间服务器将与第三个服务器联系，以此类推。无论何时发生的多于一个跃点的服务器间的级联链接都必须访问目录树中的所有数据。

例如，下面的图表显示对条目 ou=People,l=Europe,dc=example,dc=com 的访问是如何从服务器 A 链接到服务器 B，最后到达服务器 C。服务器 A 包含根后缀 dc=example,dc=com，以及分支 l=Europe,dc=example,dc=com 的到服务器 B 的已链接子后缀。服务器 B 包含条目 l=Europe,dc=example,dc=com，但分支 ou=People,l=Europe,dc=example,dc=com 是到服务器 C 的已链接子后缀。服务器 C 实际包含条目 ou=People,l=Europe,dc=example,dc=com

图 3-3 通过三个服务器进行级联链接



设置级联参数

可配置两个链接参数用于级联：

- 所有服务器应配置循环检测，以便检测到链接拓扑中的任何意外循环。如果未启用循环检测，循环中的服务器将不停地循环转发操作直到超过负载。
- 应将所有中间的已链接后缀配置成评估本地 ACI，通常在已链接后缀的第一级未进行此操作。

使用控制台设置级联参数

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点，然后选择要修改的已链接后缀。
2. 在右侧面板中，选择 “限制和控制”标签，可在此处修改级联链接参数。
3. 在级联链接中的所有中间服务器上，选中检查本地 ACI 的复选框。

   在单级链接中，未选中此复选框是因为用户的访问权限不在第一个服务器上评估，而是在第二个服务器上通过代理进行评估。但是，在级联链接的中间服务器上，必须启用 ACI 检查以允许在再次转发操作之前执行访问控制。
4. 在级联链接中的所有服务器上，设置允许拓扑中所有链接操作的最大跃点数。每次将同一个操作转发到另一个已链接后缀计为一个跃点，当达到最大跃点数限制时，已链接后缀将不再转发操作。

   应设置一个比最长级联链接中跃点数更大的数字。所有达到此限制的操作都将被放弃，因为服务器将假定它为拓扑中的一个意外循环。

   还必须设置链接配置以允许循环检测控制，如 “传输用于级联的 LDAP 控件”（第 114 页）中所述。

5. 完成级联参数的设置后请单击 “保存”。

从命令行设置级联参数

1. 在所有中间服务器上，使用以下命令编辑用于级联后缀的链接配置条目：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=databaseName,cn=chaining database,cn=plugins,cn=config
changetype:modify
replace:nsCheckLocalACI
nsCheckLocalACI:on
-
changetype:modify
replace:nsHopLimit
nsHopLimit:maximumHops
^D
```

   应将 *maximumHops* 设置为大于最长级联链接中的跃点数。所有达到此限制的操作都将被放弃，因为服务器将假定它为拓扑中的一个意外循环。还必须设置链接配置以允许循环检测控制，如 “传输用于级联的 LDAP 控件”（第 114 页）中所述。

2. 在级联链接中的所有其他服务器上，使用以下命令编辑用于级联后缀的链接配置条目：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=databaseName,cn=chaining database,cn=plugins,cn=config
changetype:modify
replace:nsHopLimit
nsHopLimit:maximumHops
^D
```

   其中， *maximumHops* 具有与上一步中相同的定义。

传输用于级联的 LDAP 控件

默认情况下，已链接的后缀不传输 “代理授权”控件。但是，当一个已链接后缀与另一个后缀联系时，则需要用此控件来传输远程服务器上的访问控制所需的用户标识。中间的已链接后缀必须允许链接此控件。

最近，已为 “代理授权”控件定义第二个协议。因为不同服务器版本可能使用两种控件之一，所以应配置所有级联服务器允许链接新旧两种 “代理授权”控件。

“循环检测”控件也是级联链接中防止循环所需的控件。默认情况下，允许此控件随已链接的操作转发，但应对该配置进行验证。如果服务器不允许此控件链接，则将不检测任何涉及该服务器的循环。

按照 “配置链接策略”（第 101 页）中的步骤执行操作，以确保允许链接以下三个控件：

- 2.16.840.1.113730.3.4.12 - “代理授权”控件 （旧规范）
- 2.16.840.1.113730.3.4.18 - “代理授权”控件 （新规范）
- 1.3.6.1.4.1.1466.29539.12 - “循环检测”控件

第 4 章

填充目录内容

目录服务器管理的数据经常进行批量导入。Directory Server 提供导入和导出全部后缀的工具。它还提供用于一次备份所有后缀和从备份恢复所有数据的工具。

本章介绍填充目录的以下过程：

- 设置后缀只读模式
- 导入数据
- 导出数据
- 备份数据
- 从备份还原数据

设置后缀只读模式

在 Directory Server 上执行特定的导出或备份操作前，可在任何给定后缀上启用只读模式，以确保在给定时间拥有其内容状态的可靠图像。另外，在执行导入或还原操作前，必须确保受操作影响的后缀并非处于只读模式。

在执行导出或备份操作前，Directory Server 控制台和命令行公用程序不会自动将目录置于只读模式，因为这样会使目录无法更新。但是，如果拥有多主配置，则可在服务器上启用只读模式，并且数据将在其他主副本上保持可写状态。

要将后缀设为只读，请执行 “设置访问权限和引荐”（第 87 页）中所述的步骤。换句话说，可使整个 Directory Server 不可写入，如 “设置全局只读模式”（第 34 页）中所述。

导入数据

Sun ONE Directory Server 提供了两种导入数据的方法：

- 导入 LDIF 文件允许批量添加、修改和删除任何目录后缀中的条目。
- 初始化 LDIF 文件中的后缀，会删除该后缀中的当前数据，并替换成 LDIF 文件的内容。

这两种方法都可以通过 Directory Server 控制台和使用命令行公用程序实施。

注意 导入的所有 LDIF 文件必须使用 UTF-8 字符集编码。

导入 LDIF 时，父条目必须存在于目录中或首先从文件添加。初始化后缀时， LDIF 文件必须包含根条目和相应后缀的所有目录树节点。

下表显示了导入和初始化之间的差异：

表 4-1 导入数据与初始化后缀的比较

比较的域	导入数据	初始化后缀
覆盖内容	否	是
LDAP 操作	添加、修改、删除	只添加
性能	较慢	快速
响应于服务器故障	最佳努力 （保留该故障点的所有更改）	全部毁坏 （发生故障后，丢失所有更改）
LDIF 文件位置	在控制台计算机上。	本地到控制台或本地到服务器
导入配置信息 (`cn=config`)	是	否

导入 LDIF 文件

执行导入操作时， Directory Server 控制台执行 `ldapmodify` 操作以向目录中添加新条目。条目在 LDIF 文件中指定，可能也包含更新语句以修改或删除现有条目，作为导入操作的一部分。

导入条目的目标，可以是 Directory Server 管理的任何后缀以及在配置中定义的任何已链接的后缀或已链接的子后缀。如同添加条目的任何其他操作一样，服务器将在导入条目时对所有新的条目编制索引。

使用控制台导入 LDIF

必须以目录管理员或管理员的身份登录执行导入操作：

1. 在 Directory Server 控制台的顶级 “任务” 标签上，滚动到标签的底部，然后单击 “从 LDIF 导入” 旁边的按钮。

   显示 “导入 LDIF” 对话框。

2. 在 “导入 LDIF” 对话框的 “LDIF 文件” 字段中，输入要导入的 LDIF 文件的完整路径，或单击 “浏览” 以选择本地文件系统中的文件。

   如果正在访问远程计算机上的目录，该字段名会显示为 “LDIF 文件 （在控制台计算机上）”。此标签提示您正在浏览的是本地文件系统，而不是远程目录服务器计算机上的文件系统。

3. 按照要求设置下列选项：

   a. “仅添加” - LDIF 文件除了包含默认的添加指令外，还可能包含修改和删除指令。如果希望控制台仅执行添加指令而忽略 LDIF 文件中的所有其他指令，请选中此复选框。

   b. “出错时继续” - 如果希望控制台即使在出现错误时也能继续导出，请选中此复选框。例如，如果正在导入的 LDIF 文件包含后缀中已有的条目，则可使用此选项。控制台会记录此类错误，如执行导入操作时拒绝文件中现有的条目。

      如果未选中此复选框，则在遇到第一个错误后导入操作将停止。 LDIF 文件中之前的所有条目都已经成功导入，并将保留在目录中。

4. 在 “拒绝的文件” 字段中，输入要控制台记录所有无法导入条目的文件的完整路径，或单击 “浏览” 以选择本地文件系统中的文件。

   例如，服务器无法导入目录中已经存在的条目或者没有父对象的条目。控制台将在拒绝文件中写入服务器发送的错误消息。

   如果保留该字段为空，则服务器将不记录被拒绝的条目。

5. 单击 “确定” 开始执行导入操作。

   Directory Server 控制台显示一个对话框，对话框中包含操作的状态和所有发生的错误的文本。如果 “拒绝的文件” 不为空，则所有错误消息也将写入到已命名的文件中。

从命令行导入 LDIF

`ldif2ldap` 命令 （Solaris 软件包中为 `directoryserver ldif2ldap`）将通过 LDAP 导入 LDIF 文件并执行其包含的所有操作。使用此脚本将数据同时导入所有目录后缀。为了使用 `ldif2ldap` 导入，服务器必须正在运行。

该命令的完整路径为：

Solaris 软件包其他安装

```
# /usr/sbin/directoryserver ldif2ldap
# ServerRoot/slapd-serverID/ldif2ldap
```

以下示例使用 `ldif2ldap` 命令执行导入。不需要 root 特权运行命令，但必须在命令行赋予目录管理员凭证。最后一个参数是一个或多个要导入的 LDIF 文件的名称。

UNIX shell 脚本：

```
# use directoryserver ldif2ldap on Solaris Packages installations
/var/Sun/mps/slapd-example/ldif2ldap \
  "cn=Directory Manager" 口令 \
  /var/Sun/mps/slapd-example//ldif/demo.ldif
```

Windows 批处理文件：

```
C:\Program Files\Sun\MPS\slapd-example\ldif2ldap.bat
  "cn=Directory Manager" 口令
  C:\Program Files\Sun\MPS\slapd-example\ldif\demo.ldif
```

有关使用此脚本的详细信息，请参阅 *Sun ONE Directory Server 参考手册* 第 2 章中的 “`ldif2ldap`”。

初始化后缀

初始化后缀用 LDIF 文件的内容覆盖后缀中的现有数据，该 LDIF 文件仅包含用于添加的条目。

警告 从 LDIF 文件初始化后缀时，注意不要覆盖 `o=NetscapeRoot` 后缀，除非正在还原数据。否则，将删除要求重新安装所有 Sun ONE 服务器的信息。

为初始化后缀，必须被验证为目录管理员或管理员。出于安全考虑，只有目录管理员和管理员具有访问后缀根条目的权限，例如 `dc=example,dc=com`。所以，只有这些身份可以导入包含根条目的 LDIF 文件。

从控制台初始化后缀

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点，显示要初始化的后缀。

2. 右键单击后缀节点，从弹出菜单中选择 “初始化”。或者，可以选择后缀节点，然后从 “对象”菜单中选择 “初始化”。

   显示 “初始化后缀”对话框。

3. 在 “LDIF 文件”字段中，输入要用于初始化的 LDIF 文件的完整路径，或单击 “浏览”在计算机上找到该文件。

4. 如果操作的是导入文件的本地计算机的控制台，则可跳到第 6 步。如果操作的是包含 LDIF 文件服务器的远程计算机的控制台，则选择下列选项之一：

   从本地计算机。表明 LDIF 文件位于本地计算机上。

   从服务器计算机。表明 LDIF 文件位于远程服务器上。默认情况下，控制台在以下目录中查找该文件：

   ServerRoot/slapd-*serverID*/ldif

5. 单击 “确定”。

警告 该脚本会覆盖后缀中的数据。

6. 确定您要覆盖后缀中的数据。

   将继续进行后缀初始化，同时在对话框中报告所有错误。

使用 ldif2db 命令初始化后缀

ldif2db 命令 （Solaris 软件包中为 directoryserver ldif2db）初始化后缀并覆盖现有的数据。脚本要求您在继续进行导入操作前关闭服务器。

默认情况下，先保存该脚本，然后将任何现有的 o=NetscapeRoot 配置信息和所导入文件中的 o=NetscapeRoot 配置信息合并。

警告 该脚本覆盖后缀中的数据。

要在导入 LDIF 的同时停止服务器，请执行以下操作：

1. 从命令行以 root 身份使用以下命令停止服务器：

Solaris 软件包
```
# /usr/sbin/directoryserver stop
```
其他安装
```
# ServerRoot/slapd-serverID/stop-slapd
```

2. 运行位于以下位置的命令：

Solaris 软件包
```
# /usr/sbin/directoryserver ldif2db
```
其他安装
```
# ServerRoot/slapd-serverID/ldif2db
```

3. 使用适当的命令启动服务器：

Solaris 软件包
```
# /usr/sbin/directoryserver start
```
其他安装
```
# ServerRoot/slapd-serverID/start-slapd
```

以下示例使用 `ldif2db` 命令将两个 LDIF 文件导入到一个后缀中。

UNIX shell 脚本：

```
# use directoryserver ldif2db on Solaris Packages installations
/var/Sun/mps/slapd-example/ldif2db -n Database1 \
 -i /var/Sun/mps/slapd-example/ldif/demo.ldif \
 -i /var/Sun/mps/slapd-example/ldif/demo2.ldif
```

Windows 批处理文件：

```
C:\Program Files\Sun\MPS\slapd-example\ldif2db.bat -n Database1
  -i C:\Program Files\Sun\MPS\slapd-example\ldif\demo.ldif
  -i C:\Program Files\Sun\MPS\slapd-example\ldif\demo2.ldif
```

表 4-2　示例中使用的 ldif2db 选项的说明

选项	说明
`-n`	指定导入数据的数据库名称。 警告：如果在 -n 选项中指定数据库不与 LDIF 文件中包含的后缀相对应，则该数据库中包含的所有数据都将被删除，并且导入失败。确保数据库的名称没有拼错。
`-i`	指定要导入的 LDIF 文件的完整路径名称。该选项是必需的。可以使用多个 `-i` 参数一次导入多个 LDIF 文件。导入多个文件时，服务器按从命令行指定的顺序导入 LDIF 文件。

有关使用该命令的详细信息，请参阅 *Sun ONE Directory Server 参考手册* 第 2 章中的 “ldif2db”。

使用 ldif2db.pl Perl 脚本初始化后缀

与 `ldif2db` 命令一样， `ldif2db.pl` 脚本（Solaris 软件包中为 `directoryserver ldif2db-task`）覆盖指定后缀中的数据。该脚本要求服务器正在运行，以执行导入。

警告 该脚本覆盖后缀中的数据。

此脚本的命令依平台而定：

Solaris 软件包
```
# /usr/sbin/directoryserver ldif2db-task
```
Windows 平台
```
cd ServerRoot
bin\slapd\admin\bin\perl slapd-serverID\ldif2db.pl
```
其他安装
```
# ServerRoot/slapd-serverID/ldif2db.pl
```

以下示例使用 `ldif2db.pl` 脚本导入 LDIF 文件。运行该脚本无需 root 特权，但必须进行目录管理员身份的验证。

UNIX shell 脚本：

```
# use directoryserver ldif2db-task on Solaris Packages installations
/var/Sun/mps/slapd-example/ldif2db.pl \
  -D "cn=Directory Manager" -w 口令 -n Database1 \
  -i /var/Sun/mps/slapd-example/ldif/demo.ldif
```

Windows 批处理文件：

```
C:\Program Files\Sun\MPS\bin\slapd\admin\bin\perl.exe
  C:\Program Files\Sun\MPS\slapd-example\ldif2db.pl
    -D "cn=Directory Manager" -w 口令 -n Database1
    -i C:\Program Files\Sun\MPS\slapd-example\ldif\demo.ldif
```

下表说明本示例中使用的 `ldif2db.pl` 选项：

表 4-3 示例中使用的 ldif2db.pl 选项的说明

选项	说明
`-D`	指定目录管理员的 DN。
`-w`	指定目录管理员的口令。
`-n`	指定导入数据的数据库名称。
`-i`	指定要导入的 LDIF 文件的完整路径名称。该选项是必需的。可以使用多个 `-i` 参数一次导入多个 LDIF 文件。导入多个文件时，服务器按从命令行指定的顺序导入 LDIF 文件。

有关使用该 perl 脚本的详细信息，请参阅 *Sun ONE Directory Server 参考手册* 第 2 章中的 “ldif2db.pl”。

导出数据

可以使用纯文本 LDAP 数据交换格式 (LDIF) 导出目录的内容。 LDIF 是条目、属性以及其值的文本表示。 LDIF 是一种标准格式，在 RFC 2849 (`http://www.ietf.org/rfc/rfc2849.txt`) 中对其进行了说明。

导出数据可以有下列用途：

- 备份服务器中的数据。
- 将数据复制到另一个目录服务器。
- 将数据导出到另一个应用程序。
- 更改目录拓扑结构后，重新填充后缀。

导出操作不会导出配置信息 (`cn=config`)。

警告 在执行导出操作期间，请不要停止服务器。

使用控制台将整个目录导出到 LDIF

可以将部分或所有目录数据导出到 LDIF，具体情况要视最终导出的文件位置而定。如果 LDIF 文件在服务器上，则可以仅导出服务器上本地后缀中包含的数据。如果 LDIF 文件不在服务器上，则可以导出所有的后缀和链接的后缀。

要在服务器运行的情况下从 Directory Server 控制台导出目录数据，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “任务”标签上，滚动到标签的底部，然后单击 “导出到 LDIF”旁边的按钮。

   显示 “导出”对话框。

2. 在 “LDIF 文件”字段中输入 LDIF 文件的完整路径和文件名，或单击 “浏览”查找该文件。

   如果在远程服务器上使用控制台，则不能使用 “浏览”。未启用 “浏览”按钮时，默认情况下，该文件存储在下列目录中：

   ServerRoot`/slapd-`*serverID*`/ldif`

3. 如果在服务器的远程计算机上运行控制台，则在 LDIF 文件字段下显示两个单选按钮。选择 “到本地计算机”，表明您正在导出到运行控制台的计算机上的 LDIF 文件中。选择 “到服务器计算机”，表明您正在导出到位于服务器计算机上的 LDIF 文件。

4. 如果要导出整个目录，请选择 “所有后缀”单选按钮。

   如果只想导出目录的一个子树，请选择 “子树”单选按钮，然后在文本框中输入子树基准上的 DN。

   还可以单击 “浏览”选择子树。

5. 单击 “确定”将目录内容导出到文件。

使用控制台将单一后缀导出到 LDIF

要在服务器运行的情况下将一个后缀从 Directory Server 控制台导出到 LDIF，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点，显示要导出的后缀。
2. 右键单击后缀节点，从弹出菜单中选择 “导出”。或者，可以选择后缀节点，然后从 “对象”菜单中选择 “导出”。

   显示 “导出后缀”对话框。

3. 在 “LDIF 文件”字段中，输入该 LDIF 文件的完整路径，或单击 “浏览”以在计算机上找到它。

   未启用 “浏览”按钮时，默认情况下，该文件存储在下列目录中：

   ServerRoot/slapd-*serverID*/ldif

4. 如果复制了后缀，您可以选中复选框以 “导出复制信息”。仅当使用导出的 LDIF 初始化该后缀的其他副本时，才需要使用该功能。
5. 如果对此后缀启用了属性加密，则可以选中该复选框对属性进行 “解密”。为此，必须提供保护服务器证书数据库的口令。选择该选项，输入口令或输入包含口令的文件名称。如果无法提供口令对属性值进行解密，则 LDIF 输出中将显示加密的值。
6. 单击 “确定”将后缀的内容导出到文件。

从命令行导出到 LDIF

可以使用 db2ldif 命令 （Solaris 软件包中为 directoryserver db2ldif）将任意后缀或目录的子树导出到 LDIF。当服务器运行或停止时，该脚本将所有的后缀内容或部分内容导出到 LDIF 文件。

要将数据库的内容导出到 LDIF 文件中，请使用下列命令：

Solaris 软件包
其他安装

```
# /usr/sbin/directoryserver db2ldif
# ServerRoot/slapd-serverID/db2ldif
```

以下示例将两个后缀导出到一个 LDIF 文件中：

```
db2ldif -a output.ldif \
        -s "dc=example,dc=com" -s "o=NetscapeRoot"
```

下表介绍本示例中使用的 `db2ldif` 选项：

表 4-4　本示例中使用的 db2ldif 选项的说明

选项	说明
`-a`	定义输出文件的名称，服务器将导出的 LDIF 保存到该文件中。默认情况下，该文件存储在 *ServerRoot*`/slapd-`*serverID* 目录下。
`-s`	指定要包括在导出中的后缀或子树。可以使用多个 `-s` 参数指定多个后缀或子树。

`db2ldif` 命令可同时与 `-r` 选项一起使用，以将复制的后缀导出到 LDIF 文件中。结果 LDIF 将包含复制机制使用的属性子类型。然后可以将该 LDIF 文件导入到使用者服务器中，以初始化使用者副本，如 “初始化副本”（第 255 页）中所述。

`db2ldif` 命令与 `-r` 选项一起使用时，不可运行服务器。必须先停止服务器，然后再启动它，或者将 `db2ldif.pl` 脚本与 `-r` 选项一起使用，该选项不需要停止服务器。

有关使用该脚本的详细信息，请参阅 *Sun ONE Directory Server 参考手册* 第 2 章中的 “db2lidf”。

备份数据

备份数据会保存内容或目录的快照，以备将来数据库文件损坏或被删除时使用。可以使用 Directory Server 控制台或命令行脚本备份后缀。

警告　在执行备份操作期间，切勿停止服务器。

默认情况下，此处说明的所有备份步骤都将把服务器文件的副本存储在同一主机上。然后，您应该将备份复制并存储到其他计算机或文件系统上，以保证更好的安全性。

注意 无法使用这些备份方法备份远程服务器上的链接后缀。必须独立地备份单独的服务器。

使用控制台备份服务器

从 Directory Server 控制台备份服务器时，服务器将所有的数据库内容及相关的索引文件复制到备份位置。可以在运行服务器的同时执行备份操作。

要从 Server Console 备份服务器，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “任务”标签上，单击 “备份 Directory Server”旁边的按钮。

   显示 “备份目录”对话框。

2. 在 “目录”文本框中，输入要存储备份的目录的完整路径。如果在目录所在的计算机上运行控制台，请单击 “浏览”查找本地目录。

   或单击 “使用默认目录”在以下目录中存储备份：

   ServerRoot/slapd-*serverID*/bak/*YYYY_MM_DD_hh_mm_ss*

   其中， *serverID* 是目录服务器的名称，同时还将生成目录名称以包含备份的创建日期和时间。

3. 单击 “确定”，创建该备份。

从命令行备份服务器

可以使用 db2bak 命令 （Solaris 软件包中为 directoryserver db2bak）从命令行备份服务器。不管服务器是否正在运行，该脚本都可以起作用。

不能使用该备份方法备份配置信息。有关备份配置信息的详细信息，请参阅 “备份 dse.ldif 配置文件”（第 128 页）。

要备份目录，请使用以下命令：

Solaris 软件包
```
# /usr/sbin/directoryserver db2bak backupDir
```
其他安装
```
# ServerRoot/slapd-serverID/db2bak backupDir
```

backupDir 参数指定应在其中存储备份的目录。默认备份目录名称从当前日期生成：`YYYY_MM_DD_hh_mm_ss`。有关使用该脚本的详细信息，请参阅 *Sun ONE Directory Server 参考手册* 第 2 章中的 “db2bak”。

备份 dse.ldif 配置文件

Directory Server 自动备份 `dse.ldif` 配置文件。启动 Directory Server 时，它会自动在以下目录中名为 `dse.ldif.startOK` 的文件中，创建 `dse.ldif` 文件的备份：

ServerRoot`/slapd-`*serverID*`/config`

如果您对 `cn=config` 分支进行修改，则服务器在将修改写入到 `dse.ldif` 文件之前，会首先将文件备份到 `config` 目录中的名为 `dse.ldif.bak` 的文件中。如果需要保存配置，请创建这些文件之一的副本。

从备份还原数据

以下步骤说明如何使用 Directory Server 控制台或命令行还原目录中的后缀。服务器必须已经使用 “备份数据”（第 126 页）中所述的步骤进行了备份。在还原复制参数中涉及的后缀之前，请阅读 “还原已复制的后缀”（第 128 页）。

警告 在执行备份或还原操作期间，不要停止服务器。

还原服务器会覆盖任何现有的数据库文件，并会丢失备份后对数据所做的任何修改。

还原已复制的后缀

还原在供应商服务器和使用者服务器之间复制的后缀之前，需要特殊的考虑。如果可能，您应该通过复制机制更新后缀，而不是从备份进行还原。该小节说明如何和何时还原副本，以及在操作后如何确保其与其他副本同步。有关使用备份和还原初始化副本的进一步信息，请参阅 “初始化副本”（第 255 页）。

在单个主方案中还原供应商

后缀，即单主供应商，包含整个复制拓扑的授权数据。因此，还原该后缀等于重新初始化整个拓扑中的所有数据。只有要重新初始化要还原的备份内容的所有数据时，才需要还原单主副本。

如果单主数据由于错误而无法恢复，则可以考虑使用使用者副本之一上的数据，因为它可能包含比备份更新的更新内容。在这种情况下，则需要将数据从使用者副本导出到 LDIF 文件，并从 LDIF 文件重新初始化主副本。

无论是在主副本上还原备份还是导入 LDIF 文件，接下来都必须重新初始化从该副本接收更新的所有集线器副本和使用者副本。供应商服务器的日志会记录一条消息，提示您需要对使用者副本重新初始化。

在多主方案中还原供应商

在多主复制中，其他主副本每个都包含复制数据的授权副本。不能用当前的副本内容还原可能已过时的旧备份。如有可能，应允许复制机制从其他主副本的内容更新该主副本。

如果不可能，则只应当以下列方式中的一种还原多主副本：

- 最简单的方式不是还原备份，而是从其他主副本中的一个重新初始化计划的主副本。这样可以确保将最新的数据发送到计划主副本中，并准备好供复制的数据。请参阅 “使用控制台初始化副本”（第 259 页）或 “从命令行初始化副本”（第 260 页）。
- 对于具有数百万个条目的副本，更快的方法是使用新的二进制复制功能还原较近的、从其他主副本中获取的备份。请参阅 “使用二进制复制初始化副本”（第 262 页）。
- 如果主副本的备份不比任何其他主副本上的更改日志内容的最早日期更早，则该备份可用来还原此主副本。有关更改日志存留期的说明，请参阅 “高级多主复制配置”（第 249 页）。还原旧备份时，其他主副本将使用其更改日志更新该主副本，更新内容包括备份保存以来已经处理的所有修改。

不管采用何种方式还原或重新初始化，主副本初始化后都将保持只读模式。该行为允许该副本与其他主副本同步，此后，可允许执行写操作，如 “多主副本初始化后会聚”（第 256 页）中所述。

允许在还原或重新初始化主副本上执行写操作之前，允许会聚所有副本的优点是，不需要重新初始化集线器或使用者服务器。

还原集线器副本

本节只适用于复制机制不能自动更新集线器副本的情况。例如，如果数据库文件毁坏或复制中断的时间很长。在这样的情况下，将需要以以下方式之一还原或重新初始化集线器副本：

- 最简单的方式不是还原备份，而是从主副本中的一个重新初始化集线器。这样可以确保将最新的数据发送到集线器，并准备好供复制的数据。请参阅 “使用控制台初始化副本”（第 259 页）或 “从命令行初始化副本”（第 260 页）。

- 对于具有数百万个条目的副本，更快的方法是使用新的二进制复制功能还原较近的、从另一个集线器副本中获取的备份。请参阅 “使用二进制复制初始化副本”（第 262 页）。如果没有要复制的其他集线器副本，则必须如前一段落中所述的那样重新初始化集线器，或者按下一段落中所述的那样进行还原 （如果可能）。
- 如果集线器的备份不比任何供应商副本 （集线器副本或主副本）上的更改日志内容的最早日期早，则该备份可用来还原此集线器。有关更改日志存留期的说明，请参阅 “高级多主复制配置”（第 249 页）。还原旧备份时，它的供应商副本将使用其更改日志更新该集线器，更新内容包括备份保存以来已经处理的所有修改。

注意 不管还原或重新初始化集线器副本的方式如何，随后都必须重新初始化该集线器的所有使用者，包括任何其他级别的集线器。

还原专门的客户

本节只适用于复制机制不能自动更新专门的使用者副本的情况。例如，数据库文件毁坏或复制中断的时间很长的情况。在这样的情况下，将需要以以下方式之一还原或重新初始化使用者副本：

- 最简单的方式不是还原备份，而是从其供应商副本 （主副本或集线器副本）中的一个重新初始化使用者。这样可以确保将最新的数据发送到使用者，并准备好供复制的数据。请参阅 “使用控制台初始化副本”（第 259 页）或 “从命令行初始化副本”（第 260 页）。
- 对于具有数百万个条目的副本，更快的方法是使用新的二进制复制功能还原较近的、从另一个使用者副本中获取的备份。请参阅 “使用二进制复制初始化副本”（第 262 页）。如果没有要复制的其他使用者，则必须如前一段落所述的那样重新初始化副本，或按下一段落所述的那样进行还原 （如果可能）。
- 如果使用者的备份不比任何供应商副本 （集线器副本或主副本）上的更改日志内容的最早日期更早，则该备份可用来还原使用者。有关更改日志存留期的说明，请参阅 “高级多主复制配置”（第 249 页）。还原旧备份时，它的供应商副本将使用其更改日志更新该集线器，更新内容包括备份保存以来已经处理的所有修改。

使用控制台还原服务器

如果目录数据已毁坏，则可使用 Directory Server 控制台从先前生成的备份还原数据。为了使用控制台还原服务器，必须运行目录服务器。然而，在还原期间不能使用相应的后缀处理操作。

要从先前创建的备份还原服务器，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “任务”标签上，单击 “还原 Directory Server”旁边的按钮。

   显示 “还原目录”对话框。

2. 从 “可用的备份”列表中选择备份，或在 “目录”文本框中输入有效备份的完整路径。

   “可用的备份”列表会显示默认目录中的全部备份：

   ServerRoot/slapd-*serverID*/bak

3. 单击 “确定”还原服务器。

从命令行还原服务器

可使用以下脚本从命令行还原服务器：

- 使用 bak2db 命令 （Solaris 软件包中为 directoryserver bak2db）。该脚本需要关闭服务器。
- 使用 bak2db.pl perl 脚本 （Solaris 软件包中为 directoryserver bak2db-task）。该脚本需要运行服务器。

使用 bak2db 命令行脚本。

要在关闭服务器的情况下从命令行还原目录，请执行以下操作：

1. 从命令行以 root 身份使用以下命令停止服务器：

Solaris 软件包
```
# /usr/sbin/directoryserver stop
```
其他安装
```
# ServerRoot/slapd-serverID/stop-slapd
```

2. bak2db 命令与备份目录的完整路径一起使用：

Solaris 软件包
```
# /usr/sbin/directoryserver bak2db backupDir
```
其他安装
```
# ServerRoot/slapd-serverID/bak2db backupDir
```

3. 使用适当的命令启动服务器：

Solaris 软件包
```
# /usr/sbin/directoryserver start
```
其他安装
```
# ServerRoot/slapd-serverID/start-slapd
```

以下示例从默认的备份目录中还原备份：

```
# bak2db /var/Sun/mps/slapd-example/bak/2001_07_01_11_34_00
```

详细信息，请参阅 *Sun ONE Directory Server 参考手册* 第 2 章中的 “bak2db”。

使用 bak2db.pl Perl 脚本

要在服务器运行的情况下从命令行还原目录，请使用以下 perl 脚本：

Solaris 软件包
```
# /usr/sbin/directoryserver bak2db-task
```
Windows 平台
```
cd ServerRoot
bin\slapd\admin\bin\perl slapd-serverID\bak2db.pl
```
其他安装
```
# ServerRoot/slapd-serverID/bak2db.pl
```

以下示例使用 `ldif2db.pl` 脚本导入 LDIF 文件。-a 选项给出备份目录的完整路径。

UNIX shell 脚本：

```
# use directoryserver bak2db-task on Solaris Packages installations
/var/Sun/mps/slapd-example/bak2db.pl \
  -D "cn=Directory Manager" -w 口令 \
  -a /var/Sun/mps/slapd-example/bak/checkpoint
```

Windows 批处理文件：

```
C:\Program Files\Sun\MPS\bin\slapd\admin\bin\perl.exe
 C:\Program Files\Sun\MPS\slapd-example\bak2db.pl
  -D "cn=Directory Manager" -w 口令
  -a C:\Program Files\Sun\MPS\slapd-example\bak\2001_07_01_11_34_00
```

详细信息，请参阅 *Sun ONE Directory Server 参考手册* 第 2 章中的“bak2db.pl”。

还原 dse.ldif 配置文件

该目录在以下目录中创建 `dse.ldif` 文件的两个备份副本：

ServerRoot/slapd-*serverID*/config

`dse.ldif.startOK` 文件在服务器启动时，记录 `dse.ldif` 文件的副本。`dse.ldif.bak` 文件包含 `dse.ldif` 文件最近所做更改的备份。将包含最近更改的文件复制到目录中。

要还原 `dse.ldif` 配置文件，请执行以下操作：

1. 从命令行以 root 身份使用以下命令停止服务器：

Solaris 软件包
```
# /usr/sbin/directoryserver stop
```
其他安装
```
# ServerRoot/slapd-serverID/stop-slapd
```

2. 改为包含配置文件的目录。
3. 使用已知为完好的备份配置文件覆盖 `dse.ldif` 文件。例如，可键入以下内容：

```
cp dse.ldif.startOK dse.ldif
```

4. 使用适当的命令启动服务器：

Solaris 软件包

```
# /usr/sbin/directoryserver start
```

其他安装

```
# ServerRoot/slapd-serverID/start-slapd
```

第 5 章

高级条目管理

除了目录中数据的分层结构以外，管理代表用户的条目通常需要创建组和共享公共属性值。 Sun ONE Directory Server 通过组、角色和服务类 (CoS) 提供此高级条目管理功能。

组是命名其他条目的条目，可作为成员列表或成员过滤器。角色通过在角色的每个成员上生成 `nsrole` 属性的机制提供与组相同的功能，以及其他更多功能。 CoS 同样生成虚拟属性，允许条目共享公共属性值，而无须将其存储在各个条目中。

注意 Sun ONE Directory Server 5.2 引入了基于角色和 CoS 虚拟属性的值执行搜索的功能。用于任何操作中的过滤器字符串现在都可以包括 `nsRole` 属性或 CoS 定义生成的任何属性，并对该属性的值执行任何比较操作。但是，无法编制虚拟 CoS 属性的索引，因此任何有关 CoS 生成的属性的搜索都不会编入索引。

要充分利用角色和服务类所提供的功能，最好在目录部署的计划阶段确定目录拓扑结构。有关这些机制的说明以及它们如何简化您的拓扑结构，请参阅 *Sun ONE Directory Server 部署指南* 的第 4 章 “设计目录树”。

本章包含以下小节：

- 管理组
- 分配角色
- 定义服务类 (CoS)

管理组

组是一种关联条目的机制以方便管理，如定义 ACI 的机制。组定义是特殊条目，可以为静态列表中的成员命名，或提供过滤器以定义一组动态条目。有关创建等效角色定义的过程，请参阅 “分配角色”（第 138 页）。

可能的组成员范围是整个目录，而不管组定义条目位于何处。为简化管理，所有组定义条目通常存储在一个位置，通常在根后缀下的 `ou=Groups`。

定义静态组的条目是从 `groupOfUniqueNames` 对象类继承。组成员作为 `uniqueMember` 属性的多个值按其 DN 列出。

定义动态组的条目从 `groupOfUniqueNames` 和 `groupOfURLs` 对象类继承。组成员身份由多值 `memberURL` 属性中给出的一个或多个过滤器定义。动态组中的成员是评估过滤器时与任一过滤器匹配的条目。

以下各节介绍如何使用控制台创建和修改静态组和动态组。

添加新静态组

1. 在 Directory Server 控制台的顶级 “目录”标签上，右键单击目录树中希望添加新组的条目，然后选择 “新建” > “组”项目。

   或者，从 “对象”菜单中选择条目，并选择 “新建” > “组”项目。

2. 在 “创建新组”对话框中，必须在 “组名称”字段中为新组键入一个名称，可以在 “说明”字段中添加组的说明 （可选）。组名称将成为新组条目的 `cn`（通用名）属性的值，并显示在其 DN 中。

3. 在对话框左侧列表中单击 “成员”。在右侧面板中，默认情况下选择 “静态组”标签。

4. 单击 “添加”将新成员添加到组中。显示标准 “搜索用户和组”对话框。

5. 在 “搜索”下拉列表中，选择 “用户”并输入要搜索的字符串，然后单击 “搜索”。单击 “高级”按钮以搜索特定属性或特定的属性值。

   在结果中选择一个或多个条目并单击 “确定”。重复此步骤，将所有希望添加的成员添加至静态组。

注意 由于链接，静态组成员可能是远程的。可以使用引荐完整性插件确保删除的成员条目从静态组条目中自动删除。有关使用具有链接的引荐完整性的详细信息，请参阅 “配置链接策略”（第 101 页）。

6. 单击左侧列表中的 “语言”，使用其他语言为您的组命名和添加说明字符串。当控制台使用相应区域时，将显示上述内容。

7. 单击 “确定”创建新组。它显示为创建时所在条目的子级。

添加新的动态组

1. 在 Directory Server 控制台 的顶级 “目录”标签上，右键单击目录树中希望添加新组的条目，然后选择 “新建” > “组”项目。

   或者，从 “对象”菜单中选择条目，并选择 “新建” > “组”项目。

2. 在 “创建新组”对话框中，必须在 “组名称”字段中为新组键入一个名称，可以在 “说明”字段中添加组的说明 （可选）。组名称将成为新组条目的 cn （通用名）属性的值，并显示在其 DN 中。

3. 在对话框左侧的列表中单击 “成员”，然后在右侧面板中选择 “动态组”标签。

4. 单击 “添加”创建 LDAP URL，包含将定义组成员的过滤器字符串。显示标准 “构造及测试 LDAP URL”对话框。

5. 在文本字段中输入 LDAP URL，或选择 “构造”以按照指导构造包含用于组的过滤器的 LDAP URL。单击 “测试”查看该过滤器返回的条目列表。

   完成构造 URL 后单击 “确定”。重复此步骤，添加包含将定义动态组的过滤器的所有 URL。

6. 单击左侧列表中的 “语言”，使用其他语言为您的组命名和添加说明字符串。当控制台使用相应区域时，将显示上述内容。

7. 单击 “确定”创建新组。它显示为创建时所在条目的子级。

修改组定义

1. 在 Directory Server 控制台的顶级 “目录”标签上，双击代表要修改的组的条目。

   或者，从 “对象”菜单中选择条目并选择 “打开”。

2. 在 “编辑项目”对话框中，对 “常规”、“成员”或 “语言”类别中的组信息作出更改。可以添加或删除静态组的成员，或者添加、编辑或删除包含用于动态组的过滤器的 URL。

3. 修改完组定义后单击 “确定”。

   要在控制台中查看更改，请从 “查看”菜单中选择 “刷新”。

删除组定义

要删除组的两种类型之一，只需删除定义它的条目。

分配角色

角色是一种备用分组机制，旨在更高效和轻松的用于应用程序。角色如同组一样定义和管理，但是除此之外，成员条目还拥有一个生成的属性，该属性指明它们参与的角色。例如，应用程序可以只是读取条目的角色，而不是选择组并浏览成员列表。

默认情况下，角色的范围限制为定义该角色的子树。Sun ONE Directory Server 5.2 引入嵌套角色的扩展范围，允许嵌套位于其他子树中的角色，并可在目录任何位置都具有成员。

关于角色

每个角色都具有拥有该角色的*成员*或条目。由于条目是从目录检索，角色机制自动在每个条目 （任何角色的成员）中生成 `nsRole` 属性。该多值属性包含所有角色定义 （条目是其中成员）的 DN。 `nsRole` 属性是一个计算属性。它不随条目本身存储，而是作为操作结果中的普通属性返回客户机应用程序。

Sun ONE Directory Server 支持三种类型的角色：

- 受管理的角色 - 管理员通过将 `nsRoleDN` 属性添加到所需的成员条目来分配受管理的角色。该属性的值是角色定义条目的 DN。受管理的角色类似于静态组，其不同之处在于成员身份在每个条目中定义，而不是在角色定义条目中定义。
- 已筛选的角色 - 相当于动态组：它们在其 `nsRoleFilter` 属性中定义过滤器字符串。已筛选的角色的范围是其所在的子树，位于其定义条目的父路径。当服务器返回一个已筛选的角色范围内的条目，且该条目匹配其过滤器时，该条目将包含生成的标识角色的 `nsRole` 属性。
- 嵌套角色 - 命名其他角色定义的角色，包括其他嵌套角色。嵌套角色的成员集是该角色包含的所有成员的联合。嵌套角色也可以定义扩展范围，以包括其他子树中的角色成员。

角色允许客户机应用程序直接读取某个条目的 nsRole 属性，从而知道该条目的所有角色成员身份。这样就简化了客户机优化目录使用的过程。角色可以与 CoS 机制结合在一起使用以为角色成员生成其他属性 （请参阅 “创建基于角色的属性”（第 157 页））。角色可用于定义访问控制 （请参阅 “定义角色访问 - roledn 关键字”（第 181 页））。角色还支持其他功能，如立即激活或去活其所有成员 （请参阅 “去活和激活用户和角色”（第 234 页））。

搜索 nsRole 属性

Sun ONE Directory Server 5.2 现在允许在所有搜索过滤器中使用 nsRole 属性。可以使用任何比较操作符为该属性搜索特定值。但是，请注意以下事项：

- 涉及 nsRole 属性的搜索可能会花很长时间，因为所有角色必须在筛选条目之前进行评估。
- 优化目录服务器用于等式搜索成员身份，特别是受管理的角色中。例如，下列搜索的速度近乎于搜索真实属性：

  ```
  (&(objectclass=person)
    (nsRole=cn=managersRole,ou=People,dc=example,dc=com)
  ```

- 默认情况下，用于定义受管理的角色成员身份的 nsRoleDN 属性在所有后缀中编制了索引。如果禁用对该属性的索引，则将失去对于搜索受管理的角色成员身份的优化。
- 搜索包含已筛选角色的条目涉及到使用角色过滤器进行内部搜索。如果出现在角色过滤器中的所有属性都在角色范围内的所有后缀中编制了索引，则该内部操作将会最快。

nsRole 属性的权限

nsRole 属性仅能由角色机制进行分配，而不能由任何目录用户写入或修改。但是，应注意以下事项：

- nsRole 属性对于任何目录用户都可能是可读的，不过您可以定义访问控制以防止对它进行读取。
- nsRoleDN 属性定义受管理的角色成员身份，您应该决定用户是否可以从角色添加或删除其自身。有关阻止用户修改其自身角色的 ACI，请参阅 “受管理的角色定义示例”（第 144 页）。
- 已筛选的角色通过过滤器确定成员身份，这些过滤器基于用户条目中属性的存在或值。应仔细定义这些属性的用户权限，从而控制可以定义已筛选角色中成员身份的用户。

有关如何使用目录中的角色的详细信息，请参阅 *Sun ONE Directory Server 部署指南* 中的第 4 章 “设计目录树”。

使用控制台分配角色

本节介绍创建和修改角色的过程。

创建受管理的角色

受管理的角色拥有角色定义条目，并且通过将 nsRoleDN 属性添加到每个成员条目来指派成员。要使用控制台创建并将成员添加到受管理的角色，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “目录”标签上，右键单击目录树中希望添加新角色定义的条目，然后选择 “新建” > “角色”项目。

   或者，从 “对象”菜单中选择条目，并选择 “新建” > “角色”项目。

2. 在 “创建新角色”对话框中，必须在 “角色名称”字段中为新角色键入一个名称，可以在 “说明”字段中添加角色的说明 （可选）。组名称将成为新角色条目的 cn （通用名）属性的值，并显示在其 DN 中。

3. 在对话框左侧列表中单击 “成员”。默认情况下，在右侧窗格中已选择 “受管理的角色”单选按钮。

4. 单击成员列表下的 “添加”，将新成员添加到角色中。显示标准 “搜索用户和组”对话框。

5. 在 “搜索”下拉列表中，选择 “用户”并输入要搜索的字符串，然后单击 “搜索”。单击 “高级”按钮以搜索特定属性或特定的属性值。

   在结果中选择一个或多个条目并单击 “确定”。重复此步骤，将所有希望添加的成员添加至静态组。

6. 完成将条目添加到角色后，单击 “确定”。新角色显示在目录树中并带有受管理角色的图标，所有成员条目会获得属性 nsRoleDN，其值为该新角色条目的 DN。

7. 创建角色后，还可以将该角色分配到任何条目，方法是将 nsRoleDN 属性添加到条目，其值为角色条目的 DN。

创建已筛选的角色

如果条目具有角色定义中 LDAP 过滤器选定的属性或属性值，则条目为已筛选角色的成员。

注意 已筛选的角色的过滤器字符串可能基于任何属性，不包括由 CoS 机制生成的其他虚拟属性 （请参阅 “关于 CoS”（第 147 页））。

要使用控制台创建并将成员添加到已筛选的角色，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “目录”标签上，右键单击目录树中希望添加新角色定义的条目，然后选择 “新建” > “角色”项目。

   或者，从 “对象”菜单中选择条目，并选择 “新建” > “角色”项目。

2. 在 “创建新角色”对话框中，必须在 “角色名称”字段中为新角色键入一个名称，可以在 “说明”字段中添加角色的说明 （可选）。组名称将成为新角色条目的 `cn` （通用名）属性的值，并显示在其 DN 中。

3. 在对话框左侧列表中单击 “成员”，并且在右侧面板中选择 “已筛选的角色”单选按钮。

4. 在文本字段中输入 LDAP 过滤器，以定义将确定角色成员的过滤器。或者单击 “构造”以按照指导构造一个 LDAP 过滤器。

5. 如果单击 “构造”，则将显示 “构造 LDAP 过滤器”对话框。放弃 LDAP 服务器主机、端口、基准 DN 和搜索范围字段，因为您无法在已筛选的角色定义中指定这些。

   a. 在已筛选的角色中仅搜索用户。这样会将 `(objectclass=person)` 组件添加到过滤器。如果不需要此组件，则必须在 “创建新角色”对话框的文本字段中编辑 LDAP 过滤器。

   b. 通过从 “位置”下拉列表中选择属性并设置匹配条件来调整过滤器。要添加其他过滤器，请单击 “多于”。要删除不必要的过滤器，请单击 “少于”。

   c. 单击 “确定”在已筛选的角色定义中使用您的过滤器。然后可以在文本字段中编辑过滤器以修改任何组件。

6. 单击 “测试”试用您的过滤器。“过滤器测试结果”对话框将显示当前匹配过滤器的条目。

7. 单击 “确定”创建新的角色条目。新角色显示在目录树中，且具有已筛选角色的图标。

创建嵌套角色

嵌套角色允许您创建包含其他角色的角色，并扩展现有角色的范围。创建嵌套角色之前，必须存在另一个角色。创建嵌套角色时，控制台显示一个可用于嵌套的角色列表。嵌套角色可能包含另一个嵌套角色，最多嵌套 30 层。超出此固定限制之后，对该角色进行评估时，服务器将记录一条错误消息。

要使用控制台创建并将成员添加到嵌套角色，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “目录”标签上，右键单击目录树中希望添加新角色定义的条目，然后选择 “新建” > “角色”项目。

   或者，从 “对象”菜单中选择条目，并选择 “新建” > “角色”项目。

2. 在 “创建新角色”对话框中，必须在 “角色名称”字段中为新角色键入一个名称，可以在 “说明”字段中添加角色的说明 （可选）。组名称将成为新角色条目的 cn （通用名）属性的值，并显示在其 DN 中。

3. 在对话框左侧列表中单击 “成员”，并且在右侧面板中选择 “嵌套角色”单选按钮。

4. 单击 “添加”将现有角色添加到嵌套角色列表中。在显示的 “角色选择器”对话框中，从可用角色列表中选择一个或多个角色，然后单击 “确定”。

5. 单击 “确定”创建嵌套角色条目。新角色显示在目录中，且具有嵌套角色的图标。

6. 要修改嵌套角色的范围，请使用 “嵌套角色定义示例”（第 146 页）中显示的命令行过程。

查看并编辑条目角色

1. 在 Directory Server 控制台的顶级 “目录”标签上，浏览目录树以显示要为其查看或编辑角色的条目。

2. 右键单击条目并从弹出菜单中选择 “设置角色”。或者，可以左键单击条目以选定条目，并从 “对象”菜单中选择 “设置角色”。

   显示 “设置角色”对话框。

3. 选择 “受管理的角色”标签，显示该条目所属的受管理角色。您可以执行以下操作：

- 要添加新的受管理角色，请单击 “添加”，并从 “角色选择器”窗口选择可用的角色。在 “角色选择器”窗口中单击 “确定”。
- 要删除受管理的角色，请选择该角色并单击 “删除”。
- 要编辑与条目相关的受管理的角色，请在表格中选定它，然后单击 “编辑”。该角色显示在角色的自定义编辑器中。对该角色进行任意更改，然后单击 “确定”，保存新角色定义。

4. 选择 “其他角色”标签，查看该条目所属的已筛选或嵌套角色。要改变已筛选或嵌套角色中的角色成员关系，必须编辑角色定义：

- 选择角色，然后单击 “编辑”以显示角色的自定义编辑器。对该角色进行更改，然后单击 “确定”，保存新角色定义。

5. 完成对角色的修改后，单击 “确定”保存更改。

修改角色条目

1. 在 Directory Server 控制台上，选择 “目录”标签。
2. 浏览导航树以找到现有角色的定义条目。角色是创建时所在条目的子级。双击该角色。

   显示 “编辑项目”对话框。
3. 单击左侧窗格中的 “常规”以更改角色名称和说明。
4. 单击左侧窗格中的 “成员”以更改受管理角色和嵌套角色的成员或者更改已筛选角色的过滤器。
5. 单击 “确定”以保存更改。

删除角色

删除角色只会删除角色定义的条目，而不会删除其成员。

要删除角色，请执行以下操作：

1. 在 Directory Server 控制台中，选择 “目录”标签。
2. 浏览导航树以找到角色的定义条目。角色是创建时所在条目的子级。
3. 右键单击角色并选择 “删除”。

   显示对话框，要求您确认删除操作。单击 “是”。
4. 显示 “删除的条目”对话框，通知您已成功删除该角色。单击 “确定”。

注意 删除角色会删除角色条目，但不会删除每个角色成员的 `nsRoleDN` 属性。要删除该属性，请启用引荐完整性插件并对其进行配置以管理 `nsRoleDN` 属性。详细信息，请参阅 “维护引荐完整性”（第 73 页）。

从命令行管理角色

在目录系统管理员可通过命令行公用程序访问的条目中定义角色。创建角色后，即可向其分配成员，如下所示：

- 受管理角色的成员在其条目中具有 `nsRoleDN` 属性。
- 已筛选角色的成员是与 `nsRoleFilter` 属性中指定的过滤器匹配的条目。
- 嵌套角色的成员是嵌套角色定义条目的 `nsRoleDN` 属性中指定的角色的成员。

所有角色定义都继承 LDAPsubentry 和 nsRoleDefinition 对象类。下表列出每种类型的角色所特定的其他对象类和相关属性。

表 5-1 用于定义角色的对象类和属性

角色类型	对象类	属性
受管理的角色	nsSimpleRoleDefinition nsManagedRoleDefinition	Description（可选）
已筛选的角色	nsComplexRoleDefinition nsFilteredRoleDefinition	nsRoleFilter Description（可选）
嵌套角色	nsComplexRoleDefinition nsNestedRoleDefinition	nsRoleDN Description（可选）

受管理的角色定义示例

要创建将分配给所有 marketing（市场部）成员的角色，请运行下面的 ldapmodify 命令：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=Marketing,ou=marketing,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:nsRoleDefinition
objectclass:nsSimpleRoleDefinition
objectclass:nsManagedRoleDefinition
cn:Marketing
description:managed role for marketing staff
```

请注意， nsManagedRoleDefinition 对象类继承 LDAPsubentry、nsRoleDefinition 和 nsSimpleRoleDefinition 对象类。

通过使用下面的 ldapmodify 命令更新其条目，将该角色分配给名为 Bob 的 marketing 成员：

```
ldapmodify -D "cn=Directory Manager" -w secret -h host -p 389
dn:cn=Bob Arnold,ou=marketing,ou=People,dc=example,dc=com
changetype:modify
add:nsRoleDN
nsRoleDN:cn=Marketing,ou=marketing,ou=People,dc=example,dc=com
```

条目中存在的 nsRoleDN 属性表示该条目是受管理角色的成员，而该角色由其角色定义的 DN 标识。要通过修改 nsRoleDN 属性来阻止用户在受管理的角色中添加或删除自身，请添加下面的访问控制指令 (ACI)：

```
aci:(targetattr="nsRoleDN")
     (targattrfilters="
add=nsRoleDN:(!(nsRoleDN=cn=AdministratorRole,dc=example,dc=com)),
del=nsRoleDN:(!(nsRoleDN=cn=nsManagedDisabledRole,dc=example,dc=com
)
     ")
     (version3.0;aci "allow mod of nsRoleDN by self
        except for critical values";
        allow(write)
         userdn="ldap:///self";)
```

已筛选的角色定义示例

要为 sales managers （销售部经理）（假设他们都有 `isManager` 属性）设置已筛选的角色，请运行下面的 `ldapmodify` 命令：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=ManagerFilter,ou=sales,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:nsRoleDefinition
objectclass:nsComplexRoleDefinition
objectclass:nsFilteredRoleDefinition
cn:ManagerFilter
nsRoleFilter:(isManager=True)
Description:filtered role for sales managers
```

请注意， `nsFilteredRoleDefinition` 对象类继承 `LDAPsubentry`、`nsRoleDefinition` 和 `nsComplexRoleDefinition` 对象类。 `nsRoleFilter` 属性指定将查找 `ou=sales` 组织 （有从属组织）中的所有员工的过滤器，例如：

```
ldapsearch -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
-b "ou=People,dc=example,dc=com" -s sub "(cn=*Fuentes)"
```

```
dn:cn=Carla Fuentes,ou=sales,ou=People,dc=example,dc=com
cn:Carla Fuentes
isManager:TRUE
...
nsRole:cn=ManagerFilter,ou=sales,ou=People,dc=example,dc=com
```

注意 已筛选的角色的过滤器字符串可能基于任何属性，不包括由 CoS 机制生成的其他虚拟属性 （请参阅 “关于 CoS”（第 147 页））。

已筛选的角色成员是用户条目时，您可以选择将其能力限制为在角色中添加或删除其自身，方法为使用访问控制指令 (ACI) 保护已筛选的属性。

嵌套角色定义示例

使用 nsRoleDN 属性指定嵌套在嵌套角色中的角色。要创建一个包含前面示例所创建角色的 marketing （市场部）人员和 sales manager （销售部经理）成员的角色，请使用下面的命令：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=MarketingSales,ou=marketing,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:nsRoleDefinition
objectclass:nsComplexRoleDefinition
objectclass:nsNestedRoleDefinition
cn:MarketingSales
nsRoleDN:cn=ManagerFilter,ou=sales,ou=People,dc=example,dc=com
nsRoleDN:cn=Marketing,ou=marketing,ou=People,dc=example,dc=com
nsRoleScopeDN:ou=sales,ou=People,dc=example,dc=com
```

请注意， nsNestedRoleDefinition 对象类继承 LDAPsubentry、nsRoleDefinition 和 nsComplexRoleDefinition 对象类。 nsRoleDN 属性包含 marketing （市场部）受管理角色和 sales manager （销售部经理）已筛选角色的 DN。前面示例中的两个用户 Bob 和 Carla 将成为此新嵌套角色的成员。

此过滤器的作用域包含默认作用域 （即此过滤器所在的子树）和 nsRoleScopeDN 属性的任意值下的子树。在这种情况下， ManagerFilter 位于 ou=sales,ou=People,dc=example,dc=com 子树中，因此此子树必须添加到作用域中。

定义服务类 (CoS)

服务类 (CoS) 机制生成虚拟属性，如同为客户机应用程序检索条目。 CoS 简化了条目的管理并减少了对存储的要求。

与组和角色一样， CoS 依赖于目录中的帮助程序条目，并可以通过控制台或命令行进行配置。下面各节说明 CoS 并提供以两种方式管理 CoS 的过程。

注意 作为 Directory Server 5.2 中的一项新属性，任何搜索操作都可测试 CoS 生成的属性是否存在或比较其值。虚拟属性的名称可以用于任何过滤器字符串中，而无论过滤器是来自客户机搜索操作还是用在已筛选角色中的内部过滤器。 Directory Server 5.2 还支持 VLV （虚拟列表视图）操作和服务器端排序控制中的虚拟属性，就如同任何实际属性。

关于 CoS

CoS 为 CoS 作用域中的任何条目 （称为目标条目）定义虚拟属性及其值。每个 CoS 由目录中的以下条目组成：

- CoS 定义条目 - 标识正在使用的 CoS 的类型和将生成的 CoS 属性的名称。类似于角色定义条目，从 `LDAPsubentry` 对象类继承。 CoS 的作用域是 CoS 定义条目的父级下的整个子树。同一 CoS 属性可以有多个定义，因此 CoS 属性可以是多值的。
- 模板条目 - 包含一个或多个虚拟属性的值。 CoS 作用域中的所有条目将使用此处定义的值。也可以有多个模板条目，此时生成的属性可以是多值的。

有三种类型的 CoS，每种对应 CoS 定义和模板条目之间的一种不同交互：

- 指针 CoS - CoS 定义条目直接按其 DN 标识模板条目。所有目标条目中的 CoS 属性值将与模板中给出的值相同。
- 间接 CoS - CoS 定义标识一个属性，称为间接指示符，在目标条目中的值必须包含模板的 DN。由于具有间接 CoS，每个目标条目可以使用不同模板，从而具有 CoS 属性的不同值。
- 典型 CoS - CoS 定义标识模板的基准 DN 和指示符，是目标条目中属性的名称。指示符属性必须包含 RDN （相对域名）， RDN 与模板基准 DN 结合时，确定包含 CoS 值的模板。

CoS 定义条目是 `cosSuperDefinition` 对象类的实例，还可以从下面的一个对象类中继承以指定 CoS 的类型：

- `cosPointerDefinition`
- `cosIndirectDefinition`
- `cosClassicDefinition`

CoS 定义条目包含特定于 CoS 每种类型的属性，这些 CoS 用于命名虚拟 CoS 属性、模板 DN 和目标条目中的指示符属性 （如果需要）。默认情况下， CoS 机制将不会使用与 CoS 属性相同的名称覆盖现有属性的值。但是， CoS 定义条目的语法允许控制此行为。

CoS 模板条目是 `cosTemplate` 对象类的实例。 CoS 模板条目包含 CoS 机制所生成的属性的值。在目录树中，给定 CoS 的模板条目与 CoS 定义存储在同一级上。

如果可能，定义和模板条目应位于同一位置以利于管理。另外，它们的命名方式应体现它们所提供的功能。例如，`cn=ClCosGenerateEmployeeType,ou=People,dc=example,dc=com` 这样的定义条目 DN 比 `cn=ClassicCos1,ou=People,dc=example,dc=com` 更具有说明性。

Sun ONE Directory Server 部署指南 第 4 章中的 “管理服务类的属性”比较详细地描述了 CoS 类型，并提供了示例及有关部署的注意事项。有关与每种类型 CoS 相关的对象类和属性的详细信息，请参阅 “从命令行管理 CoS”（第 151 页）。

CoS 限制

CoS 定义和模板条目的创建和管理必须遵守以下限制。*Sun ONE Directory Server 部署指南* 第 4 章中的 “CoS 限制”中给出了有关部署 CoS 虚拟属性的进一步限制。

涉及 CoS 所生成属性的搜索是没有索引的。任何搜索过滤器都可测试虚拟属性的值是否存在或比较该值。但是，无法对虚拟属性编制索引，并且涉及 CoS 所生成属性的任何过滤器组件将导致没有索引的搜索，从而对性能产生明显影响。

受限的子树。您不能在 `cn=config` 和 `cn=schema` 子树中创建 CoS 定义。因此，这些条目不能包含虚拟属性。

受限的属性类型。一定不能使用 CoS 机制生成下列属性类型，因为它们不会与同名的实际属性具有相同的行为：

- `userPassword` - CoS 生成的口令值不能用于绑定到目录服务器。
- `aci` - 目录服务器不会根据 CoS 所定义的虚拟 ACI 值的内容应用任何访问控制。
- `objectclass` - 目录服务器不会对 CoS 所定义的虚拟对象类的值执行模式检查。
- `nsRoleDN` - 目录服务器不会使用 CoS 生成的 `nsRoleDN` 值来生成角色。

属性子类型不受支持。CoS 机制将不生成带有子类型的属性，如语言或 `;binary`。

实际属性值和虚拟属性值。 CoS 机制不会生成包含 “实际”值 （在条目中定义）和 “虚拟”值 （在 CoS 模板中定义）的多值属性。属性值可能是存储在条目中的值，也可能是 CoS 机制生成的值，如 “覆盖实际属性值”和 “多值 CoS 属性”（第 153 页）中所述。

所有模板都必须是本地模板。模板条目的 DN （位于 CoS 定义中，或者位于目标条目的指示符中）必须引用目录服务器中的本地条目。无法通过目录链接或引荐检索模板和所包含的值。

使用控制台管理 CoS

本节说明如何通过 Directory Server 控制台创建和编辑 CoS 定义。

另外，如果需要保护 CoS 值，则应为 CoS 定义和模板条目以及目标条目中的指示符属性定义访问控制指令 (ACI)。有关 CoS 安全性注意事项，请参阅 *Sun ONE Directory Server 部署指南*；有关使用控制台创建 ACI 的过程，请参阅第 6 章 “管理访问控制”。

创建新的 CoS

如果是指针 CoS 和典型 CoS，则必须在定义条目之前创建模板条目：

1. 在 Directory Server 控制台的顶级 “目录”标签上，右键单击目录树中希望添加的新模板条目，然后从弹出菜单中选择 “新建” > “其他”项目。

   或者，从 “对象”菜单中选择父条目，并选择 “新建” > “其他”项目。

2. 在 “新建对象”对话框中，从对象类列表中选择 `costemplate`。将打开 “通用编辑器”对话框，其中有新模板中某些属性的默认值。

3. 以下面的方式编辑新模板对象：

   a. 将 `LDAPsubentry` 和 `extensibleobject` 值添加到 `objectclass` 属性。

   b. 添加 `cn` 属性并给它赋予标识该模板的值，如 `cosTemplateForHeadquartersFax`。

   c. 将命名属性更改为新的 `cn` 属性。

      可以添加任何其他属性并将其作为命名属性代替使用，但通常使用 `cn`。

   d. 通过将 `cosPriority` 属性设置为整数值以便修改，或者在不需要时将其完全删除。详细信息，请参阅 “Cos 属性优先级”（第 154 页）。

   e. 使用 CoS 机制将希望生成的属性及其值添加到目标条目上。

4. 在 “通用编辑器”对话框中单击 “确定”以创建模板条目。

5. 如果希望为此模板定义指针 CoS，请在目录树中选择新的模板条目并从菜单中选择 “编辑” > “复制 DN”。

创建定义条目的过程对于所有类型的 CoS 都是相同的：

1. 在 Directory Server 控制台的顶级 “目录”标签上，右键单击目录树中希望添加新 CoS 定义的条目，然后从弹出菜单中选择 “新建” > “服务类”项目。

   或者，从 “对象”菜单中选择父条目，并选择 “新建” > “服务类”项目。

   显示 “服务类”条目的自定义编辑器。

2. 输入新 “服务类”的名称和可选的说明。该名称将显示在 CoS 定义条目的 cn 命名属性中。
3. 单击左侧列表中的 “属性”标签。对话框显示 CoS 机制将在目标条目上生成的属性的列表。

   单击 “添加”浏览可能属性的列表并将这些属性添加到列表中。
4. 将属性添加到了列表后，“服务行为类”列将立即包含一个下拉列表。单击此单元选择备用行为：
   - **不覆盖目标条目属性** - 只有当目标条目的相同属性中没有存储相应的属性值时才会生成 CoS 属性值。
   - **覆盖目标条目属性** - CoS 所生成的属性值将覆盖目标条目中该属性的任何值。
   - **覆盖目标条目属性并且是可操作的** - 该属性将覆盖任何目标值并且是可操作的属性，以便客户机应用程序看不到它 （除非明确请求）。

注意	仅当某属性在该模式中定义为可操作时，才可以使之可操作。

5. 单击左侧列表中的 “模板”标签。选择如何标识模板条目，然后填写相应字段。这样可以确定希望定义的 CoS 的类型。
   - **按照其 DN** - 此选项将定义指针 CoS：在 “模板 DN”字段中输入模板条目的 DN。单击 “浏览”从目录中选择模板 DN，或者按 Ctrl-V 粘贴在创建模板条目后复制的 DN。
   - **使用其中一个目标条目的属性值** - 此选项将定义一个间接的 CoS：在 “属性名”字段中输入指示符属性的名称。确保选择包含 DN 值的属性。单击 “更改”从列表中选择属性。
   - **使用一个 DN 以及其中一个目标条目的属性值** - 此选项将定义一个典型的 CoS：输入模板的基准 DN 和属性名。单击 “浏览”选择可能目标条目的父条目，单击 “更改”从列表中选择属性。
6. 单击 “确定”创建 CoS 定义条目。

编辑现有的 CoS

1. 在 Directory Server 控制台的顶级 “目录”标签上，双击 CoS 定义条目，或右键单击此条目，并从弹出菜单中选择 “用通用编辑器进行编辑”。

   显示 “服务类”条目的自定义编辑器。
2. 根据需要编辑名称和说明字段。

3. 单击左侧列表中的 “属性”标签添加或删除将由 CoS 机制生成的虚拟属性。
4. 单击左侧列表中的 “模板”标签重新定义模板指示符属性的名称或模板条目 DN。此对话框还允许您重新定义 CoS 定义的类型。
5. 单击 “确定”以保存更改。

删除 CoS

1. 在 Directory Server 控制台的顶级 “目录”标签上，浏览目录树以显示 CoS 定义条目。
2. 右键单击 CoS 条目并从弹出菜单中选择 “删除”。显示对话框，要求您确认删除操作。单击 “是”。

从命令行管理 CoS

因为所有配置信息和模板数据都作为条目存储在目录中，因此可以使用 LDAP 命令行工具配置和管理 CoS 定义。本节说明如何从命令行创建 CoS 定义和模板条目。

另外，如果需要保护 CoS 值，则应为 CoS 定义和模板条目以及目标条目中的指示符属性定义访问控制指令 (ACI)。有关从命令行创建 ACI 的步骤，请参阅第 6 章 “管理访问控制”。

从命令行创建 CoS 定义条目

所有 CoS 定义条目都有 `LDAPsubentry` 对象类，而且都继承 `cosSuperDefinition` 对象类。另外，每种类型的 CoS 都继承自特定的对象类并包含相应属性。下表列出了与每种类型的 CoS 定义条目相关联的对象类和属性：

表 5-2 CoS 定义条目中的对象类和属性

CoS 类型	CoS 定义条目

指针 CoS	`objectclass:top`
	`objectclass:LDAPsubentry`
	`objectclass:cosSuperDefinition`
	`objectclass:cosPointerDefinition`
	`cosTemplateDN:`*DN*
	`cosAttribute:`*attributeName override merge*

表 5-2 CoS 定义条目中的对象类和属性 （续）

CoS 类型	CoS 定义条目
间接 CoS	objectclass:top objectclass:LDAPsubentry objectclass:cosSuperDefinition objectclass:cosIndirectDefinition cosIndirectSpecifier: *attributeName* cosAttribute:*attributeName override merge*
典型 CoS	objectclass:top bbjectclass:LDAPsubentry objectclass:cosSuperDefinition objectclass:cosClassicDefinition cosTemplateDN: *DN* cosSpecifier: *attributeName* cosAttribute: *attributeName override merge*

在所有情况下， cosAttribute 都是多值的，而且每个定义属性的值都将由 CoS 机制生成。

可以在 CoS 定义条目中使用下列属性 （有关这些属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册*。）：

表 5-3 CoS 定义条目属性

属性	CoS 定义条目中的用途
cosAttribute: *attributeName override merge*	定义要生成值的虚拟属性的名称。此属性具有多个值，每个值给出将从模板生成其值的属性的名称。 *override* 和 *merge* 限定符指定如何在此表下面描述的特殊情况中计算 CoS 属性值。 *attributeName* 可能不包含任何子类型。带有子类型的属性名称将被忽略，但 cosAttribute 的其他值将被处理。
cosIndirectSpecifier: *attributeName*	定义目标条目中属性的名称，间接 CoS 使用该值来标识模板条目。此命名属性称为指示符，并且必须在每个目标条目中包含完整的 DN 字符串。此属性只有一个值，但指示符属性可以有多个值以指定多个模板。
cosSpecifier: *attributeName*	定义目标条目中属性的名称，典型 CoS 使用该属性的值来标识模板条目。此命名属性称为指示符，并且必须包含在目标条目的 RDN 中可以找到的字符串。此属性只有一个值，但指示符属性可以有多个值以指定多个模板。
cosTemplateDN: *DN*	提供模板条目的完整 DN （对于指针 CoS 定义）或模板条目的基准 DN （对于典型 CoS）。

cosAttribute 属性允许在 CoS 属性名称后面带有两个限定符。 *override* 限定符具有下面的一个值：

- default （或没有限定符）- 表示当该属性与虚拟属性类型相同时，服务器不覆盖存储在条目中的实际属性值。
- override - 表示即使在条目中有存储的值时，服务器也总是返回 CoS 生成的值。
- operational - 表示仅当在搜索操作中明确请求该属性时才返回它。Operational 属性不需要传递模式检查以返回。它还与 override 限定符具有相同的行为。

  仅当某属性在该模式中定义为可操作时，才可以使之可操作。例如，如果 CoS 生成 description 属性的值，则无法使用 operational 限定符，原因是此属性没有在该模式中标记为可操作。

merge 限定符不存在或给出下列值：

- merge-schemes - 允许虚拟 CoS 属性具有来自多个模板或多个 CoS 定义的多个值。详细信息，请参阅 “多值 CoS 属性”（第 153 页）。

覆盖实际属性值

可以创建带有 override 限定符的指针 CoS 定义条目，如下所示：

```
dn:cn=pointerCoS,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
objectclass:cosPointerDefinition
cosTemplateDn:cn=exampleUS,cn=data
cosAttribute:postalCode override
```

该指针 CoS 定义条目表示它与生成 postalCode 属性值的模板条目 cn=exampleUS,cn=data 相关联。 override 限定符表示当目录条目中存在 postalCode 属性值时，该值将优于它。

注意 如果 CoS 属性定义有 operational 或 override 限定符，则无法对 CoS 作用域中任何条目内该属性的 “实际”值执行写操作。

多值 CoS 属性

指定 merge-schemes 限定符时，生成的 CoS 属性可能是多值的。有两种方式可以使 CoS 属性为多值的：

- 对于间接或典型 CoS，目标条目中的指示符属性可以具有多个值。在这种情况下，每个值确定一个模板，并且每个模板的值是生成的值的一部分。
- 可以有任何类型的多个 CoS 定义条目在其 cosAttribute 中包含相同的属性名。在这种情况下，如果所有定义都包含 merge-schemes 限定符，则生成的属性将包含每个定义计算的所有值。

这两种情况可能同时出现并定义甚至更多的值。但是，在所有情况下，在生成的属性中重复值将只返回一次。

在缺少 merge-schemes 限定符的情况下，将使用模板条目的 cosPriority 属性在所有模板中为生成的属性确定一个值，如下一节中所述。

merge-schemes 限定符不会将目标中定义的 “实际”值与从模板生成的值进行合并。 *merge* 限定符独立于 *override* 限定符，所有成对情况都有可能，并且每个限定符所暗示的行为都表达出来。同时，这些限定符可以在属性名后以任何顺序指定。

注意 同一属性具有多个 CoS 定义时，它们必须全部具有相同的 *override* 和 *merge* 限定符。当不同对的限定符出现在 CoS 定义中时，在所有定义中随机选择一种组合。

Cos 属性优先级

如果有多个 CoS 定义或多值指示符，但没有 merge-schemes 限定符，则 Directory Server 使用优先属性来选择定义虚拟属性的单值的一个模板。

cosPriority 属性表示在考虑的所有模板中，特定模板具有全局优先级。零优先级是最高优先级。不包含 cosPriority 属性的模板被认为是最低优先级。当两个或多个模板提供的属性值具有相同 （或没有）优先级时，将随机选择一个值。

使用 merge-schemes 限定符时不考虑模板优先级。合并时，考虑的所有模板定义一个值，而无论它们定义的优先级如何。 cosPriority 属性在 CoS 模板条目中定义，如下一节中所述。

注意 cosPriority 属性不能有负值。另外，由间接 CoS 生成的属性不支持优先级。不要在间接 CoS 定义的模板条目中使用 cosPriority。

从命令行创建 CoS 模板条目

使用指针 CoS 或典型 CoS 时，模板条目包含 LDAPsubentry 和 cosTemplate 对象类。必须为 CoS 定义专门创建此条目。使 CoS 模板条目成为 LDAPsubentry 对象类的实例允许由配置条目不受限制地执行一般搜索。

间接 CoS 机制的模板是指目录中现有的任意条目。不需要提前对目标进行标识，也不需要给出 LDAPsubentry 对象类，但它必须有辅助的 cosTemplate 对象类。只有当 CoS 评估为生成虚拟属性及其值时才访问间接 CoS 模板。

在所有情况下， CoS 模板条目都必须在目标条目中包含 CoS 生成的属性和值。属性名在 CoS 定义条目的 cosAttribute 属性中指定。

下面的示例说明一个指针 CoS 具有最高优先级的模板条目，而该指针 CoS 生成 postalCode 属性：

```
dn:cn=ZipTemplate,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:extensibleobject
objectclass:cosTemplate
postalCode: 95054
cosPriority: 0
```

以下各节提供了模板条目示例以及每种类型 CoS 定义条目的示例。

指针 CoS 示例

以下命令创建 pointer CoS 定义条目，该条目具有 cosPointerDefinition 对象类。该定义条目使用上面给出的 CoS 模板条目在 ou=People,dc=example,dc=com 树的所有条目之间共享一个普通的邮政编码。

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令

dn:cn=pointerCoS,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
objectclass:cosPointerDefinition
cosTemplateDn:cn=ZipTemplate,ou=People,dc=example,dc=com
cosAttribute:postalCode
```

CoS 模板条目 (cn=ZipTemplate,ou=People,dc=example,dc=com) 将存储在其 postalCode 属性中的值提供给位于 ou=People,dc=example,dc=com 后缀下的所有条目。如果在同一子树中搜索不带有邮政编码的任何条目，则将看到生成的属性的值：

```
ldapsearch -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
-b "ou=People,dc=example,dc=com" -s sub "(cn=*Jensen)"

dn:cn=Babs Jensen,ou=People,dc=example,dc=com
cn:Babs Jensen
...
postalCode: 95054
```

间接 CoS 示例

间接 CoS 对 cosIndirectSpecifier 属性中的属性进行命名以查找特定于每个目标的模板。此间接 CoS 使用目标条目的 manager 属性标识 CoS 模板条目。模板条目是 manager 的用户条目，它必须包含要生成的属性的值。

以下命令创建间接 CoS 定义条目，该条目包含 cosIndirectDefinition 对象类：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
```

```
dn:cn=generateDeptNum,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
objectclass:cosIndirectDefinition
cosIndirectSpecifier:manager
cosAttribute:departmentNumber
```

接下来，将 cosTemplate 对象类添加到模板条目，并确保它们定义了要生成的属性。在此示例中，所有的 manager 条目都将成为模板：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
```

```
dn:cn=Carla Fuentes,ou=People,dc=example,dc=com
changetype:modify
add:objectclass
objectclass:cosTemplate
-
add:departmentNumber
departmentNumber: 318842
```

使用此 CoS，包含 manager 属性的目标条目 （ou=People,dc=example,dc=com 下的条目）将自动拥有其经理的部门编号。 departmentNumber 属性在目标条目上是虚拟的，因为它并不存在于服务器中，但是它会作为目标条目的一部分返回。例如，如果 Babs Jensen 的经理要定义为 Carla Fuentes，那么她的部门编号将为：

```
ldapsearch -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
-b "ou=People,dc=example,dc=com" -s sub "(cn=*Jensen)"
```

```
dn:cn=Babs Jensen,ou=People,dc=example,dc=com
cn:Babs Jensen
...
manager:cn=Carla Fuentes,ou=People,dc=example,dc=com
departmentNumber: 318842
```

典型 CoS 示例

此示例说明如何利用典型 CoS 生成邮政地址。生成的值在一个模板条目中给出，该条目是由 CoS 定义中的 cosTemplateDN 和目标条目中的 cosSpecifier 属性的值一起找到的。以下命令使用 cosClassicDefinition 对象类创建定义条目：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
```

```
dn:cn=classicCoS,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
objectclass:cosClassicDefinition
cosTemplateDn:ou=People,dc=example,dc=com
cosSpecifier:building
cosAttribute:postalAddress
```

利用相同命令，创建为每个大楼给出邮政地址的模板条目：

```
dn:cn=B07,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:extensibleobject
objectclass:cosTemplate
postalAddres:7 Old Oak Street$Anytown, CA 95054
```

使用此 CoS，包含 building 属性的目标条目 （ou=People,dc=example,dc=com 下的条目）将自动具有相应的邮政地址。 CoS 机制在其 RDN 中搜索具有指定符属性值的模板条目。在此示例中，如果 Babs Jensen 被分配到大楼 B07，则其邮政地址将生成如下：

```
ldapsearch -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
-b "ou=People,dc=example,dc=com" -s sub "(cn=*Jensen)"
```

```
dn:cn=Babs Jensen,ou=People,dc=example,dc=com
cn:Babs Jensen
...
building:B07
postalAddres:7 Old Oak Street$Anytown, CA 95054
```

创建基于角色的属性

可以创建典型 CoS 模式，根据条目所具有的角色为条目生成属性值。例如，可以使用基于角色的属性将服务器设置为逐条目地查看限制。

要创建基于角色的属性，请将 nsRole 属性用作典型 CoS 的 CoS 定义条目中的 cosSpecifier。因为 nsRole 属性可以具有多个值，因此可以定义具有多个可能的模板条目的 CoS 模式。要解析使用哪个模板条目的多义性，可以在 CoS 模板条目中包含 cosPriority 属性。

例如，可以创建一个 CoS，允许经理角色的成员超过标准邮箱配额。经理角色如下所示：

```
dn:cn=ManagerRole,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:nsRoleDefinition
objectclass:nsComplexRoleDefinition
objectclass:nsFilteredRoleDefinition
cn:ManagerRole
nsRoleFilter:(isManager=True)
Description:filtered role for managers
```

将创建的典型 CoS 定义条目如下所示：

```
dn:cn=generateManagerQuota,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
objectlass:cosClassicDefinition
cosTemplateDn:cn=managerCOS,dc=example,dc=com
cosSpecifier:nsRole
cosAttribute:mailboxquota override
```

CoS 模板名称必须是 cosTemplateDn 和 nsRole 的值的组合，它是角色的 DN。例如：

```
dn:cn="cn=ManagerRole,ou=People,dc=example,dc=com",ou=People,
 dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:extensibleobject
objectlass:cosTemplate
mailboxquota: 1000000
```

CoS 模板条目提供 mailboxquota 属性的值。 override 的另一个限定符使得 CoS 覆盖目标条目中任何现有的 mailboxquota 属性值。是角色成员的目标条目将具有角色和 CoS 生成的虚拟属性，例如：

```
ldapsearch -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
-b "ou=People,dc=example,dc=com" -s sub "(cn=*Fuentes)"

dn:cn=Carla Fuentes,ou=People,dc=example,dc=com
cn:Carla Fuentes
isManager:TRUE
...
nsRole:cn=ManagerRole,ou=People,dc=example,dc=com
mailboxquota: 1000000
```

注意 role 条目和 CoS 定义条目应位于目录树中的同一位置，以便它们在其作用域中具有相同的目标条目。 CoS 目标条目也应位于同一位置，以便易于查找和维护。

第 6 章

管理访问控制

对目录内容的访问控制是创建安全目录的一个不可或缺的组成部分。本章介绍了访问控制指令 (ACI)，这些指令用于确定向访问目录的用户授予哪些权限。 Sun ONE Directory Server 5.2 引入了查看给定用户对给定条目拥有的有效权限的功能。该功能简化了复杂而功能强大的访问控制机制的管理。

在目录部署的规划阶段中，您应当定义一种访问控制策略，用来服务于整体安全策略。有关规划访问控制策略的提示，请参阅 *Sun ONE Directory Server 部署指南* 中的第 7 章 “设计访问控制”。

本章包括以下主题：

- 访问控制的原理
- 默认 ACI
- ACI 语法
- 绑定规则
- 从命令行创建 ACI
- 使用控制台创建 ACI
- 访问控制用法示例
- 查看有效权限
- 高级访问控制：使用宏 ACI
- 访问控制和复制
- 记录访问控制信息
- 与早期版本的兼容性

访问控制的原理

用于定义访问的机制叫做访问控制。当服务器接收到一个请求时，它使用用户在绑定操作中提供的验证信息，以及服务器中定义的访问控制指令 (ACI) 来确定是否允许其访问目录信息。服务器可以允许或拒绝诸如读取、写入、搜索或比较之类的权限。授予用户的权限级别可能取决于所提供的验证信息。

通过使用访问控制，可以控制对整个目录、目录的子树、目录中的特定条目 （包括定义配置任务的条目）或特定的条目属性集的访问。可以为特定用户、属于特定组或角色的所有用户或者目录的所有用户设置权限。最后，可以为由其 IP 地址或 DNS 名称标识的特定客户机定义访问。

ACI 结构

访问控制指令作为条目的属性存储在目录中。 `aci` 属性是操作属性；它可用于目录中的每一个条目，而不管它是否是针对条目的对象类定义的。当目录服务器接收到来自客户机的 LDAP 请求时，它使用该属性来判断应授予或拒绝哪些权限。如果有明确的要求， `aci` 属性将在 `ldapsearch` 操作中被返回。

ACI 语句的三个主要部分是：

- 目标 - 确定要应用权限的条目或属性。
- 权限 - 定义被允许或被拒绝的操作。
- 绑定规则 - 根据用户的绑定 DN 确定服从 ACI 的用户。

ACI 的权限和绑定规则部分被设置为一对，也被称为 “访问控制规则 (ACR)”。对用于访问目标的指定权限是授予还是拒绝，这取决于相应的规则评估是否为 true。详细信息，请参阅 “ACI 语法”（第 165 页）。

ACI 位置

如果包含 ACI 的条目没有任何子条目，那么 ACI 将只应用于该条目。如果该条目具有子条目，那么 ACI 将应用于该条目本身以及它下面的所有条目。因此，当服务器评估任何给定条目的访问权限时，它会验证被请求条目和该条目根后缀基础之间的每一个条目的 ACI。

`aci` 属性是多值的，这意味着可以为同一条目或子树定义多个 ACI。

您可以在条目上创建 ACI，使之不直接应用于该条目，而是应用于其子树中的部分或全部条目。这样做的优点是，您可以在目录树中的较高级别上放置一个通用 ACI，以便有效地应用于可能位于树中下层位置上的条目。例如，在 `organizationalUnit` 条目或 `locality` 条目的级别上，可以为包括 `inetorgperson` 对象类的条目创建 ACI。

通过使用此功能在高级别分支点上放置通用规则，可以减少目录树中的 ACI 数量。对于更为具体的规则，应该尽可能将它们放置在靠近叶条目的位置上，以便限定其作用域。

注意 放置在根 DSE 条目 （其 DN 为 `""`）中的 ACI 只应用于该条目。

ACI 评估

要评估对特定条目的访问权限，服务器会根据条目本身的 ACI、其父条目的 ACI，直至该条目根后缀的基础编译出一个列表。在评估期间，服务器按此顺序处理 ACI。ACI 评估是在条目及其根后缀基础之间的所有后缀和子后缀中进行的，而不是在其他服务器的链接后缀中进行。

注意 “目录管理员”是唯一不适用于访问控制的特许用户。当某个客户机以 “目录管理员”身份绑定至目录时，执行操作之前服务器不会评估任何 ACI。

因此，“目录管理员”的 LDAP 操作的性能无法与其他用户的预期性能相比。您应该始终以典型用户身份检测目录性能。

默认情况下，如果没有 ACI 应用到条目，则此条目将拒绝所有用户的访问 （目录管理员除外）。 ACI 必须为用户明确地授予访问权限，以便访问服务器中的任意条目。默认 ACI 定义匿名的读取访问权限并允许用户修改自己的条目 （安全所需属性除外）。详细信息，请参阅 “默认 ACI”（第 164 页）。

虽然服务器会首先处理距目标条目最近的 ACI，但应用于条目的所有 ACI 的效果是累加的。任意 ACI 授予的访问权都是允许的，除非有 ACI 拒绝此权限。不论出现在列表中的哪个位置，拒绝访问的 ACI 都优先于允许访问相同资源的 ACI。

例如，如果在目录的根级别拒绝写入权限，那么没有一个用户可以写入到该目录，而不管授予他们的特定权限是什么。要授予特定用户对目录的写入权限，则必须限制写入权限原始拒绝的范围，以使它不包括该用户。

ACI 限制

为目录服务创建访问控制策略时，必须注意下列限制：

- 如果目录树使用链接功能分布在多个服务器上，则某些限制应用于可以在访问控制语句中使用的关键字：
  - 依赖于组条目 （groupdn 关键字）的 ACI 必须位于与组条目相同的服务器上。如果该组是动态的，那么该组的所有成员也必须在服务器上具有一个条目。如果该组是静态的，那么成员的条目可以位于远程服务器上。
  - 依赖于角色定义 （roledn 关键字）的 ACI 必须位于与角色定义条目相同的服务器上。计划拥有角色的每个条目也必须位于相同的服务器上。

  然而，可以将存储在目标条目中的值与存储在绑定用户 （例如，使用 userattr 关键字）的条目中的值进行值匹配。即使绑定用户在服务器上不具有持有该 ACI 的条目，也可以正常地对访问进行评估。

  有关如何链接访问控制评估的详细信息，请参阅 “通过已链接的后缀进行的访问控制”（第 99 页）。
- CoS 生成的属性并不能在所有 ACI 关键字中使用。具体来说，不应该将 CoS 生成的属性与 userattr 和 userdnattr 关键字一起使用，因为访问控制规则将不起作用。详细信息，请参阅 “使用 userattr 关键字”（第 182 页）。有关 CoS 的详细信息，请参阅第 5 章 “高级条目管理”。
- 访问控制规则始终是在本地服务器上进行评估的。一定不要在 ACI 关键字中使用的 LDAP URL 中指定服务器的主机名或端口号。如果这样做， LDAP URL 将根本不会被予以考虑。详细信息，请参阅 *Sun ONE Directory Server 参考手册* 中的附录 D “LDAP URL”。
- 授予代理权限时，不能授予用户作为目录管理员进行代理的权限，也不能向目录管理员授予代理权限。

默认 ACI

安装目录服务器时，下列默认 ACI 是在配置期间指定的根后缀中定义的：

- 所有用户具有对目录的搜索、比较和读取操作的匿名访问权。
- 绑定用户可以修改目录中他们自己的条目，但不能删除。他们不能修改 aci、nsroledn 和 passwordPolicySubentry 属性，也不能修改任何资源限制属性、口令策略状态属性或者帐户锁定状态属性。

- 配置管理员 （默认情况下， `uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot`）具有除代理权限之外的所有权限。
- “配置管理员”组的所有成员都具有除代理权限之外的所有权限。
- “目录系统管理员”组的所有成员都具有除代理权限之外的所有权限。
- SIE 组的所有成员都具有除代理权限之外的所有权限。 SIE 组是“管理服务器”中此目录的服务器组的管理员。

不论何时在目录中创建新的根后缀，其基本条目都具有上面列出的默认 ACI （自我修改 ACI 除外）。为了获得额外的安全性，您应该按照 “使用控制台创建新的根后缀”（第 79 页）中的说明添加此 ACI。

“管理服务器”的 NetscapeRoot 子树具有自己的默认 ACI 集：

- “配置管理员”组的所有成员都具有对 NetscapeRoot 子树的除代理权限之外的所有权限。这样，他们可以将新成员添加到 “配置管理员”组中。
- 所有用户具有对 NetscapeRoot 子树的进行搜索和读取操作的匿名访问权。
- 组扩展 ACI 允许管理组的成员访问组定义。

下面几节讲述了如何修改这些默认设置以符合您单位的需要。

ACI 语法

ACI 是具有许多可能变量的复杂结构。不论使用控制台或从命令行创建和修改 ACI，都应该了解 LDIF 中的 ACI 语法。以下小节详细介绍 ACI 语法。

提示 因为 ACI 语法比较复杂，所以 Directory Server 控制台不支持所有 ACI 的可视编辑。另外，使用命令行为大量的目录条目设置访问控制则快得多。因此，了解 ACI 语法是创建具有有效访问控制的安全目录的关键。

`aci` 属性具有下列语法：

```
aci:(target)(version 3.0;acl "name";permission  bindRules;)
```

其中：

- *target* 指定要控制其访问的条目、属性或条目和属性集。目标可以是可分辨的名称、一个或多个属性，或单个 LDAP 过滤器。目标是可选的。没有指定目标时， ACI 应用于定义 ACI 的整个条目及其所有子条目。
- `version 3.0` 是标识 ACI 版本所必需的字符串。
- `"`*name*`"` 是 ACI 的名称。名称可以是标识 ACI 的任何字符串。 ACI 名称是必需的，并应该描述 ACI 的效果。
- *permission* 具体规定了允许或拒绝哪些权限 （例如，读取或搜索权限）。
- *bindRules* 指定用户要被授予访问权必须提供的凭证和绑定参数。绑定规则还可以基于用户身份或组成员身份或客户机的连接属性。

可以具有多个目标和权限 - 绑定规则对。这样，您可以调整条目和作为目标的属性，并针对给定目标有效地设置多个访问控制。例如：

`aci:(`*target*`)...(`*target*`)(version 3.0;acl "`*name*`";` *permission bindRule*`;`
permission bindRule`; ...;` *permission bindRule*`;)`

下面是完整的 LDIF ACI 的示例：

```
aci:(target="ldap:///uid=bjensen,dc=example,dc=com")(targetattr=*)
 (version 3.0; acl "aci1"; allow (write) userdn="ldap:///self";)
```

在本示例中， ACI 声明，用户 bjensen 具有修改其自己的目录条目中所有属性的权限。

下面几节比较详细地介绍了 ACI 每部分的语法。

定义目标

目标标识 ACI 应用的对象。当客户机要求对条目中的属性执行操作时，服务器将评估目标，从而确定是否必须评估 ACI 以允许或拒绝此操作。如果未指定目标，则 ACI 应用于包含 `aci` 属性的条目中的所有属性以及它下面的条目。

目标的通用语法是以下语法之一：

(*keyword* `=` `"`*expression*`"`)

(*keyword* `!=` `"`*expression*`"`)

其中：

- *keyword* 表示目标的类型。目标的下列类型是由表 6-1 （第 167 页）中的关键字定义的：
  - 目录条目或其子树。

- 条目的属性。
- 匹配 LDAP 过滤器的一组条目或属性。
- 匹配 LDAP 过滤器的属性值或值组合。

- 等号 (=) 表示目标是 *expression* 中指定的对象，而不等号 (!=) 表示目标是 *expression* 中未指定的任何对象。
- *expression* 取决于关键字，并标识目标。 *expression* 周围的引号 ("") 是必需的。

下表列出每个关键字以及关联的表达式：

表 6-1 LDIF 目标关键字

关键字	有效表达式	是否允许使用通配符？
`target`	ldap:///*distinguished_name*	是
`targetattr`	*attribute*	是
`targetfilter`	*LDAP_filter*	是
`targattrfilters`	*LDAP_operation:LDAP_filter*	是

将目录条目作为目标

使用目标关键字以及 LDAP URL 中的 DN 可以将特定目录条目以及它下面的所有条目作为目标。目标 DN 必须位于定义 ACI 的条目下的子树中。目标表达式具有下列语法：

```
(target = "ldap:///distinguished_name")
(target != "ldap:///distinguished_name")
```

可分辨的名称必须位于以定义 ACI 的条目作为根的子树中。例如，可以在 `ou=People,dc=example,dc=com` 上的 ACI 中使用下列目标：

```
(target = "ldap:///uid=bjensen,ou=People,dc=example,dc=com")
```

注意 如果访问控制规则应用的条目的 DN 包含逗号，则必须使用单反斜杠 (\) 转义逗号。例如：

```
(target="ldap:///uid=cfuentes,o=Example Bolivia\, S.A.")
```

还可以在 DN 中使用通配符，以便将与 LDAP URL 匹配的任意数量的条目作为目标。下面是合法的通配符用法示例：

- `(target="ldap:///uid=*,dc=example,dc=com")`

  匹配整个 example.com 树中的在条目的 RDN 中具有 `uid` 属性的每一个条目。此目标将与树中任意深度的条目相匹配，例如：

  ```
  uid=tmorris,ou=sales,dc=example,dc=com
  uid=yyorgens,ou=marketing,dc=example,dc=com
  uid=bjensen,ou=eng,ou=east,dc=example,dc=com
  ```

- `(target="ldap:///uid=*Anderson,ou=People,dc=example,dc=com")`

  匹配 `uid` 以 Anderson 结尾的 `ou=People` 分支中的每个条目。

- `(target="ldap:///*Anderson,ou=People,dc=example,dc=com")`

  匹配 RDN 以 Anderson 结尾的 `ou=People` 分支中的每个条目，不考虑其命名属性。

允许使用多个通配符，如 `uid=*,ou=*,dc=example,dc=com`。此示例匹配 example.com 树中的其可分辨名称仅包含 `uid` 和 `ou` 属性的每个条目。

注意 不能在可分辨名称的后缀部分使用通配符。即，如果目录使用后缀 `c=US` 和 `c=GB`，则不能使用下列目标来引用两个后缀：

`(target="ldap:///dc=example,c=*").`

也不能使用诸如 `uid=bjensen,o=*.com` 之类的目标。

将属性作为目标

除了将目录条目作为目标之外，还可以将目标条目中出现的一个或多个属性 （或除上述属性之外的所有属性）作为目标。这一特点在需要拒绝或允许访问有关条目的部分信息时十分有用。例如，可以只允许访问给定条目的通用名、姓，以及电话号码属性。也可以拒绝对诸如个人数据之类的敏感信息的访问。

作为目标的属性不需要存在于目标条目或其子树中，但无论何时这些属性存在于条目或其子树中， ACI 都将应用于此条目。不需要在模式中定义作为目标的属性。缺少模式检查使得在导入数据及其模式之前实现访问控制策略成为可能。

要将属性作为目标，可以使用 `targetattr` 关键字并给出属性名称。 `targetattr` 关键字使用下列语法：

```
(targetattr = "attribute")
(targetattr != "attribute")
```

可以通过使用 `targetattr` 关键字，并使用下列语法，将多个属性作为目标：

```
(targetattr = "attribute1 || attribute2 ...|| attributen")
(targetattr != "attribute1 || attribute2 ...|| attributen")
```

例如，要将条目的通用名、姓和 uid 属性作为目标，可以使用下列语法：

```
(targetattr = "cn || sn || uid")
```

被作为目标的属性包括指定属性的所有子类型。例如，`(targetattr = "locality")` 还将 `locality;fr` 作为目标。还可以专门将子类型作为目标，例如 `(targetattr = "locality;fr;quebec")`。

将条目和属性作为目标

默认情况下，包含 `targetattr` 关键字的 ACI 所针对的条目是在上面放置 ACI 的条目。即，如果将 ACI

```
aci:(targetattr = "uid")(accessControlRules;)
```

放置于 `ou=Marketing, dc=example,dc=com` 条目上，那么该 ACI 应用于整个 Marketing 子树。然而，还可以使用 `target` 关键字显式指定目标，如下所示：

```
aci:(target="ldap:///uid=*,ou=Marketing,dc=example,dc=com")
 (targetattr="uid") (accessControlRules;)
```

指定 `target` 和 `targetattr` 关键字的顺序并不重要。

使用 LDAP 过滤器将条目或属性作为目标

可以使用 LDAP 过滤器将匹配某些条件的一组条目作为目标。要做到这一点，可将 `targetfilter` 关键字与 LDAP 过滤器一起使用。 ACI 将应用于与特定过滤器相匹配的所有条目，这些特定过滤器是位于包含此 ACI 的条目下的子树中。

`targetfilter` 关键字的语法是：

```
(targetfilter = "LDAPfilter")
```

其中， *LDAPfilter* 是标准 LDAP 搜索过滤器。有关过滤器语法的详细信息，请参阅 *Sun ONE Directory Server 入门指南* 中的第 4 章 “LDAP 搜索过滤器”。

例如，假定代表雇员的所有条目都具有薪水或合同工状态 , 和代表作为全职职位的百分比的工作小时数的属性。要将代表合同工或兼职雇员的所有条目作为目标，可以使用下列过滤器：

```
(targetfilter = "(|(status=contractor)(fulltime<=79))")
```

注意 ACI 中不支持描述国际化值的匹配规则的过滤器语法。例如，下列目标过滤器无效：

```
(targetfilter = "(locality:fr:=<= Quebec)")
```

目标过滤器选择整个条目作为 ACI 的目标。可以关联 `targetfilter` 和 `targetattr` 关键字以创建 ACI，以便应用于目标条目中的属性子集。

下列 LDIF 示例允许 Engineering Admins 组的成员修改 Engineering 业务类别中所有条目的 `departmentNumber` 和 `manager` 属性。此示例使用 LDAP 过滤器选择其 `businessCategory` 属性被设置为 `Engineering` 的所有条目：

```
dn:dc=example,dc=com
objectClass:top
objectClass:organization
aci:(targetattr="departmentNumber || manager")
 (targetfilter="(businessCategory=Engineering)")
 (version 3.0; acl "eng-admins-write"; allow (write)
 groupdn ="ldap:///cn=Engineering Admins, dc=example,dc=com";)
```

提示 虽然在将分散在目录中的条目和属性作为目标时，使用 LDAP 过滤器比较有用，但是结果有时难以预料，因为过滤器不直接指定要管理其访问的对象。随着属性的添加或修改，被已过滤的 ACI 作为目标的条目集可能会发生变化。因此，如果在 ACI 中使用 LDAP 过滤器，则应该在 `ldapsearch` 操作中使用同一过滤器验证它们针对的条目和属性正确。

使用 LDAP 过滤器将属性值作为目标

可以使用访问控制以便将特定的属性值作为目标。这表明，如果一个属性的值满足 ACI 中定义的条件，则可以在该属性上授予或拒绝权限。基于属性的值授予或拒绝访问权限的 ACI 叫做基于值的 ACI。

例如，可以给您单位的所有用户授予权限，以便他们能够修改自己的条目中的 `nsRoleDN` 属性。然而，还需要确保他们不给他们自己授予诸如 “顶级管理员”之类的某些关键角色。可以使用 LDAP 过滤器检查属性值上的条件是否满足。

要创建基于值的 ACI，必须使用 `targattrfilters` 关键字，并使用下列语法：

```
(targattrfilters="add=attr1:F1 && attr2:F2...&& attrn:Fn,
                  del=attr1:F1 && attr2:F2 ...&& attrn:Fn")
```

其中：

- `add` 代表创建属性的操作。
- `del` 代表删除属性的操作。
- *attrn* 代表目标属性。
- *Fn* 代表只应用于关联属性的过滤器。

在创建条目时，如果过滤器应用于新条目中的属性，那么该属性的每个实例都必须满足该过滤器。在删除条目时，如果过滤器应用于该条目中的属性，那么该属性的每个实例也都必须满足该过滤器。

在修改条目时，如果操作是添加属性，那么必须满足应用于该属性的添加过滤器；如果操作是删除属性，那么必须满足应用于该属性的删除过滤器。如果替换条目中已经出现了属性的单个值，那么必须满足添加和删除过滤器。

例如，请考虑下列属性过滤器：

```
(targattrfilters="add=nsroleDN:(!(nsRoleDN=cn=superAdmin)) &&
telephoneNumber:(telephoneNumber=123*)")
```

此过滤器可用于允许用户向他们自己的条目添加除 `superAdmin` 角色之外的任何角色 （`nsRoleDN` 属性）。它还允许用户添加前缀为 123 的电话号码。

注意 不能从 Server Console 创建基于值的 ACI。

将单个目录条目作为目标

没有可以将单个条目作为目标的直接方法。然而，这是可以办到的：

- 通过创建绑定规则，以匹配绑定请求中的用户输入与目标条目中存储的属性值。详细信息，请参阅 “基于值匹配来定义访问”（第 181 页）。
- 通过使用 `targetfilter` 关键字。

使用 `targetfilter` 关键字可以指定仅出现在所需条目中的属性值。例如，在安装目录服务器期间，创建下列 ACI：

```
aci:(targetattr="*")(targetfilter=(o=NetscapeRoot))(version 3.0;
 acl "Default anonymous access"; allow (read, search)
 userdn="ldap:///anyone";)
```

此 ACI 仅能应用于 `o=NetscapeRoot` 条目，因为此条目是具有 `o` 属性且该属性的值为 `NetscapeRoot` 的唯一条目。

与这些方法关联的风险是，目录树将来可能会发生变化，必须记住修改此 ACI。

设定权限

权限指定允许或拒绝的访问类型。可以允许或拒绝在目录中执行特定操作的权限。可以指派的各种操作也被称作权限。

设置权限有两部分：

- 允许或拒绝访问
- 指派权限

允许或拒绝访问

可以显式允许或拒绝对目录树的访问权限。有关何时允许访问以及何时拒绝访问的详细指导说明，请参阅 *Sun ONE Directory Server 部署指南* 中的第 7 章 “设计访问控制”。

注意	不能从 Server Console 显式拒绝访问，而只能授予权限。

指派权限

权限详述了用户可以对目录数据执行的特定操作。可以允许或拒绝所有权限，也可以指派下列一个或多个权限：

读取。表示用户是否可以读取目录数据。此权限只应用于搜索操作。

写入。表示用户是否可以通过添加、修改或删除属性来修改条目。此权限应用于修改和 modrdn 操作。

添加。表示用户是否可以创建条目。此权限只应用于添加操作。

删除。表示用户是否可以删除条目。此权限只能应用于删除操作。

搜索。表示用户是否可以搜索目录数据。用户必须具有搜索和读取权限，以便查看作为搜索结果的一部分返回的数据。此权限只应用于搜索操作。

比较。表示用户是否可以将他们提供的数据与存储在目录中的数据进行比较。通过比较权限，目录返回响应查询的成功或失败消息，但用户不能查看条目或属性的值。此权限只应用于比较操作。

自身写入。表示用户是否可以在目标条目的属性中添加或删除自己的 DN。此权限只能用于进行组管理。自身写入与代理授权一起使用：它授予向组条目添加 （或从组条目删除）代理 DN 的权限 （不是绑定用户的 DN）。

代理。表示指定的 DN 是否可以用另一个条目的权限访问目标。可以使用目录中任何用户的 DN 授予代理访问权限，但目录管理员 DN 除外。此外，也不能将代理权限授予目录管理员。“代理授权 ACI 示例”（第 212 页）中提供了一个示例。有关代理访问的概述，请参阅 *Sun ONE Directory Server 部署指南*。

所有。表示指定的 DN 具有针对目标条目的所有权限 （读取、写入、搜索、删除、比较和自身写入），代理权限除外。

权限是彼此独立授予的。这表明，例如，被授予添加权限的用户可以创建条目，但是如果没有特别授予删除权限，那么该用户就不能删除条目。因此，在规划目录的访问控制策略时，必须确保以对用户有意义的方式授予权限。例如，若没有授予读取和搜索权限，则授予写入权限通常没有意义。

LDAP 操作所需的权限

本节介绍了需要授予用户的权限，这主要取决于授权用户执行 LDAP 操作的类型。

添加条目：

- 授予针对被添加的条目的添加权限。
- 授予针对该条目中的每个属性值的写入权限。默认情况下授予此权限，但可以使用 `targattrfilters` 关键字进行限制。

删除条目：

- 授予针对要删除的条目的删除权限。
- 授予针对该条目中的每个属性值的写入权限。默认情况下授予此权限，但可以使用 `targattrfilters` 关键字进行限制。

修改条目中的属性：

- 授予针对属性类型的写入权限。
- 授予针对每个属性类型值的写入权限。默认情况下授予此权限，但可以使用 `targattrfilters` 关键字进行限制。

修改条目的 RDN：

- 授予针对该条目的写入权限。
- 授予针对新 RDN 中使用的属性类型的写入权限。
- 如果需要授予删除旧 RDN 的权限，则授予针对旧 RDN 中使用的属性类型的写入权限。
- 授予针对新 RDN 中使用的属性类型值的写入权限。默认情况下授予此权限，但可以使用 `targattrfilters` 关键字进行限制。

比较属性的值：

- 授予针对属性类型的比较权限。

搜索条目：

- 授予针对搜索过滤器中使用的每个属性类型的搜索权限。
- 授予针对该条目中使用的属性类型的读取权限。

您需要设置权限以便用户能够搜索目录，以下示例可使您更容易地理解这一点。请看下面的 `ldapsearch` 操作：

```
% ldapsearch -h 主机 -s 后缀 -b "uid=bjensen,dc=example,dc=com" \
              objectclass=* mail
```

下列 ACI 用于确定是否可以为用户 `bkolics` 授予访问权：

```
aci:(targetattr = "mail")(version 3.0; acl "self access to mail";
 allow (read, search) userdn = "ldap:///self";)
```

搜索结果列表是空的，因为此 ACI 没有授予对 objectclass 属性的访问权。如果希望上文描述的搜索操作成功，则必须按如下方式修改 ACI：

```
aci:(targetattr = "mail || objectclass")(version 3.0; acl "self
 access to mail"; allow (read, search) userdn = "ldap:///self";)
```

权限语法

在 ACI 语句中，权限的语法是：

`allow|deny` (*rights*)

其中， *rights* 是用括号括起来的关键字列表，其中包括 1 到 8 个以逗号分隔的关键字。有效的关键字有：**`read`**、**`write`**、**`add`**、**`delete`**、**`search`**、**`compare`**、**`selfwrite`**、**`proxy`** 或 **`all`**。

在下列示例中，如果绑定规则被评估为 true，则允许读取、搜索和比较访问：

```
aci:(target="ldap:///dc=example,dc=com") (version 3.0;acl "example";
 allow (read, search, compare) bindRule;)
```

绑定规则

对于某些操作，必须绑定到目录，这取决于为目录定义的 ACI。绑定意味着，必须提供绑定 DN 和口令 （如果使用 SSL，则提供一个证书），才能登录到目录或针对目录对自己进行验证。绑定操作中提供的凭证，以及绑定的情况将决定允许还是拒绝对目录进行访问。

ACI 中设置的每个权限都具有对应的绑定规则，以便详细描述所需的凭证和绑定参数。

绑定规则可以非常简单。例如，绑定规则可以简单地声明，访问目录的人必须属于特定组。绑定规则也可以比较复杂。例如，绑定规则可以声明，一个人必须属于特定组，并必须从使用特定 IP 地址的计算机在上午 8 点和下午 5 点之间进行登录。

绑定规则定义了何人、何时，以及从何处可以访问目录。更具体地讲，绑定规则可以指定：

- 被授予访问权限的用户、组以及角色
- 实体必须从中绑定的位置
- 绑定必须发生的时间或日期
- 绑定期间必须使用的验证类型

此外，绑定规则可以是复杂结构，以便通过使用布尔运算符来合并这些条件。详细信息，请参阅 “使用布尔绑定规则”（第 190 页）。

如 RFC 2251 *轻型目录访问协议 (v3)* 中所描述的，服务器根据一个三值逻辑评估 ACI 中使用的逻辑表达式，该三值逻辑类似于用于评估 LDAP 过滤器的逻辑。总之，这表明，如果表达式中的任意组件评估为 “未定义”（例如，如果表达式的评估由于资源限制而中止），则服务器可以正确处理此情况：它并不错误地授予访问权限，因为在复杂的布尔表达式中发生了未定义的值。

绑定规则的语法

是允许还是拒绝访问，这取决于一个 ACI 的绑定规则是否被评估为 true。绑定规则使用下面两个模式之一：

keyword = "*expression*";

keyword != "*expression*";

其中，等号 (=) 表示 *keyword* 和 *expression* 必须匹配才能保证绑定规则为 true，而不等号 (!=) 表示 *keyword* 和 *expression* 必须不匹配才能保证绑定规则为 true。

注意 timeofday 关键字也支持不等式（<、<=、>、>=）。这是支持这些表达式的唯一关键字。

expression 两边必须有引号 ("") 和界定分号 (;)。可以使用的表达式取决于关联的 *keyword*。

下表列出了每个关键字以及关联的表达式。它还指出了在表达式中是否允许使用通配符。

表 6-2 LDIF 绑定规则关键字

关键字	有效表达式	是否允许通配符？
userdn	ldap:///*distinguished_name* ldap:///all ldap:///anyone ldap:///self ldap:///parent ldap:///*suffix*??sub?(*filter*)	是，只能在 DN 中
groupdn	ldap:///*DN* || *DN*	否
roledn	ldap:///*DN* || *DN*	否
userattr	*attribute#bindType* 或 *attribute#value*	否
ip	*IP_address*	是
dns	*DNS_host_name*	是
dayofweek	sun mon tue wed thu fri sat	否
timeofday	0 - 2359	否
authmethod	无 simple ssl sasl *authentication_method*	否

下面几节进一步详述了每个关键字的绑定规则语法。

定义用户访问 - userdn 关键字

使用 userdn 关键字定义用户访问。 userdn 关键字需要一个或多个有效可分辨的名称，并采用以下格式：

```
userdn = "ldap:///dn [|| ldap:///dn]...[||ldap:///dn]"
```

其中， *dn* 可以是 DN 或 anyone、 all、 self 或 parent 表达式中的某一个。这些表达式适用于以下用户：

- `userdn = "ldap:///anyone"` - 同时适用于匿名用户和经过验证的用户。
- `userdn = "ldap:///all"` - 仅适用于经过验证的用户。
- `userdn = "ldap:///self"` - 仅适用于与 ACI 目标条目相同的用户。
- `userdn = "ldap:///parent"` - 仅适用于 ACI 目标的父条目。

userdn 关键字还可以表示成下列形式的 LDAP 过滤器：

ldap:///*suffix*??sub?(*filter*)

注意 如果 DN 包含逗号，则逗号前面必须要用反斜杠 (\) 转义符。

匿名访问 （anyone 关键字）

授予对目录的匿名访问意味着，任何人无需提供绑定 DN 或口令就可以访问它，并且不管绑定的情况如何。匿名访问可以限于特定的访问类型 （例如，读取访问或搜索访问）、目录中的特定子树或单个条目。使用 anyone 关键字的匿名访问也允许所有经过验证的用户访问。

一般访问 （all 关键字）

可以使用绑定规则指出应用于已经成功地绑定到目录的任何人的权限。因此， all 关键字允许所有经过验证的用户访问。这将允许一般访问，同时又可防止匿名访问。

自访问 （self 关键字）

指定用户被允许或拒绝对他们自己的条目的访问。在这种情况下，如果绑定 DN 匹配目标条目的 DN，则允许或拒绝访问。

父访问 （parent 关键字）

指定只有在用户的绑定 DN 是目标条目的父级的情况下用户才被允许或拒绝对该条目的访问。请注意，必须在 Server Console 中手动编辑 ACI 以使用 `parent` 关键字。

LDAP URL

可以使用具有过滤器的 URL 动态地将 ACI 中的用户作为目标，如下所示：

```
userdn = "ldap:///<suffix>??sub?(filter)"
```

例如，将基于下列 URL 允许或拒绝 example.com 树的 accounting 和 engineering 分支中的所有用户对目标资源进行访问：

```
userdn = "ldap:///dc=example,dc=com??sub?(|(ou=engineering)(ou=accounting))"
```

注意 不要在 LDAP URL 内指定主机名或端口号。 LDAP URL 始终应用于本地服务器。

有关 LDAP URL 的详细信息，请参阅 *Sun ONE Directory Server 入门指南* 中的相应章节。

通配符

还可以通过使用通配符 (*) 指定一组用户。例如，指定 `uid=u*,dc=example,dc=com` 的用户 DN 表示基于您设置的权限只有具有以字母 `u` 开头的绑定 DN 的用户才被允许或拒绝访问。

可以从 Server Console，在 “访问控制编辑器”中设置用户访问。详细信息，请参阅 “使用控制台创建 ACI”（第 192 页）。

示例

本节包含 `userdn` 语法的示例。

包含 LDAP URL 的关键字 Userdn：

```
userdn = "ldap:///uid=*,dc=example,dc=com";
```

如果用户使用指定模式的任何可分辨的名称绑定到目录，则绑定规则被评估为 true。例如，下列两个绑定 DN 将被评估为 true：

```
uid=ssarette,dc=example,dc=com
uid=tjaz,ou=Accounting,dc=example,dc=com
```

而下列绑定 DN 将被评估为 false：

```
cn=Babs Jensen,dc=example,dc=com
```

包含 LDAP URL 的逻辑 OR 的关键字 Userdn：

```
userdn="ldap:///uid=bj,c=example.com ||
ldap:///uid=kc,dc=example,dc=com";
```

如果客户机作为提供的两个可分辨名称中的任何一个绑定，则绑定规则被评估为 true。

排除特定 LDAP URL 的关键字 Userdn：

```
userdn != "ldap:///uid=*,ou=Accounting,dc=example,dc=com";
```

如果客户机不绑定为 accounting 子树中的基于 UID 的可分辨名称，则绑定规则被评估为 true。此绑定规则只有在目标条目不在目录树的 accounting 分支下的情况下才有意义。

包含关键字 self 的 Userdn 关键字：

```
userdn = "ldap:///self";
```

如果用户正在访问由 DN （通过该 DN 用户绑定到目录）代表的条目，则绑定规则被评估为 true。即，如果用户已经绑定为 `uid=ssarette， dc=example,dc=com`，并且用户正在尝试对 `uid=ssarette,dc=example,dc=com` 条目执行操作，那么绑定规则为 true。

例如，如果需要授予 example.com 树中的所有用户对他们的 `userPassword` 属性的写入访问，则可以在 `dc=example,dc=com` 节点上创建下列 ACI。

```
aci:(targetattr = "userPassword") (version 3.0;
 acl "write-self"; allow (write) userdn = "ldap:///self";)
```

包含 all 关键字的 Userdn 关键字：

```
userdn = "ldap:///all";
```

对于任何有效的绑定 DN，绑定规则被评估为 true。要为 true，在绑定操作期间，用户必须提供有效的可分辨名称和口令。

例如，如果需要向所有经过验证的用户授予对整个树的读取访问，可以在 `dc=example,dc=com` 节点创建下列 ACI：

```
aci:(version 3.0; acl "all-read"; allow (read)
 userdn="ldap:///all";)
```

包含 anyone 关键字的 Userdn 关键字：

```
userdn = "ldap:///anyone";
```

绑定规则对于任何人被评估为 true ；可以使用此关键字提供对目录的匿名访问。

例如，如果需要允许对整个 example.com 树进行匿名读取和搜索访问，可以在 dc=example,dc=com 节点创建下列 ACI：

```
aci:(version 3.0; acl "anonymous-read-search";
 allow (read, search) userdn = "ldap:///anyone";)
```

包含 parent 关键字的 Userdn 关键字：

```
userdn = "ldap:///parent";
```

如果绑定 DN 是目标条目的父级，则绑定规则被评估为 true。

例如，如果需要授予对每个用户的子条目的写入访问，则可以在 dc=example,dc=com 节点创建下列 ACI：

```
aci:(version 3.0; acl "parent access";
 allow (write) userdn="ldap:///parent";)
```

如果用户属于 engineering 或 sales 子树，则绑定规则被评估为 true。

定义组访问 - groupdn 关键字

特定组的成员可以访问目标资源。这被称作组访问。组访问是使用 groupdn 关键字定义的，以指定在用户使用属于特定组的 DN 绑定的情况下对目标条目的访问将被允许还是被拒绝。

groupdn 关键字需要一个或多个有效的可分辨名称，并采用以下格式：

```
groupdn="ldap:///dn [|| ldap:///dn]...[|| ldap:///dn]"
```

如果绑定 DN 属于指定的组，则绑定规则被评估为 true。

注意 如果 DN 包含逗号，则逗号必须要用反斜杠 (\) 进行转义。

可以从 Server Console，在 “访问控制编辑器”上定义特定组。详细信息，请参阅 “使用控制台创建 ACI”（第 192 页）。

示例

本节包含 groupdn 语法的示例。

包含 LDAP URL 的 Groupdn 关键字：

```
groupdn = "ldap:///cn=Administrators,dc=example,dc=com";
```

如果绑定 DN 属于 Administrators 组，则绑定规则被评估为 true。如果需要授予 Administrators 组对整个目录树写入的权限，则可以在 dc=example,dc=com 节点创建下列 ACI：

```
aci:(version 3.0; acl "Administrators-write"; allow (write)
 groupdn="ldap:///cn=Administrators,dc=example,dc=com";)
```

包含 LDAP URL 的逻辑 OR 的 Groupdn 关键字：

```
groupdn = "ldap:///cn=Administrators,dc=example,dc=com ||
ldap:///cn=Mail Administrators,dc=example,dc=com";
```

如果绑定 DN 属于 Administrators 组或 Mail Administrators 组，则绑定规则被评估为 true。

定义角色访问 - roledn 关键字

特定角色的成员可以访问目标资源。这被称作角色访问。角色访问是使用 Roledn 关键字定义的，以指定在用户使用属于特定角色的 DN 绑定的情况下对目标条目的访问将被允许还是拒绝。

roledn 关键字需要一个或多个有效的可分辨名称，并采用以下格式：

```
roledn = "ldap:///dn [|| ldap:///dn]...[|| ldap:///dn]"
```

如果绑定 DN 属于指定角色，则绑定规则被评估为 true。

注意	如果 DN 包含逗号，则逗号必须要用反斜杠 (\) 进行转义。

roledn 关键字与 groupdn 关键字具有相同语法，使用方式也相同。

基于值匹配来定义访问

可以设置绑定规则以指定用于绑定到目录的条目的属性值必须匹配目标条目的属性值。

例如，可以指定绑定 DN 必须匹配用户条目的 manager 属性中的 DN 才能使 ACI 应用。在这种情况下，只有用户的管理员才可以访问该条目。

此示例基于 DN 匹配。然而，可以将绑定中使用的条目的任何属性与目标条目进行匹配。例如，可以创建 ACI，以允许其 favoriteDrink 属性是 “beer” 的任何用户读取具有相同 favoriteDrink 值的其他用户的所有条目。

使用 userattr 关键字

userattr 关键字可用于指定哪些属性值必须在用于绑定的条目和目标条目之间进行匹配。

可以指定：

- 用户 DN
- 组 DN
- 角色 DN
- LDAP 过滤器，在 LDAP URL 中
- 任何属性类型

userattr 关键字的 LDIF 语法如下所示：

```
userattr = "attrName#bindType"
```

或者，如果使用需要除用户 DN、组 DN、角色 DN 或 LDAP 过滤器之外的值的属性类型：

```
userattr = "attrName#attrValue"
```

其中：

- *attrName* 是用于进行值匹配的属性的名称
- *bindType* 是 USERDN、 GROUPDN、 LDAPURL 中的某一个
- *attrValue* 是代表属性值的任何字符串

注意 决不能将服务类 (CoS) 定义生成的属性与 userattr 关键字一起使用。包含取决于 CoS 生成的属性值的绑定规则的 ACI 将不工作。

下面几节提供具有各种可能的绑定类型的 userattr 关键字的示例。

具有 USERDN 绑定类型的示例

下面是与基于用户 DN 的绑定相关联的 userattr 关键字的示例：

```
userattr = "manager#USERDN"
```

如果绑定 DN 匹配目标条目中的 manager 属性的值，则绑定规则被评估为 true。可以使用它允许用户的管理员修改员工的属性。此机制只有在目标条目中的 manager 属性表示成完整 DN 的情况下才起作用。

下列示例授予管理员对其员工的条目的完全访问权：

```
aci:(target="ldap:///dc=example,dc=com")(targetattr=*)(version 3.0;
 acl "manager-write"; allow (all) userattr = "manager#USERDN";)
```

具有 GROUPDN 绑定类型的示例

下面是与基于组 DN 的绑定相关联的 userattr 关键字的示例：

```
userattr = "owner#GROUPDN"
```

如果绑定 DN 是目标条目的 owner 属性中指定的组成员，则绑定规则被评估为 true。例如，可以使用此机制允许组管理员工的状态信息。可以使用除 owner 之外的属性，只要您使用的属性包含组条目的 DN。

指向的组可以是动态组，该组的 DN 可以在目录中的任何后缀下。然而，服务器对这种类型的 ACI 的评估很消耗资源。

如果使用在与目标条目相同的后缀下的静态组，则可以使用以下表达式：

```
userattr = "ldap:///dc=example,dc=com?owner#GROUPDN"
```

在此示例中，组条目是在 dc=example,dc=com 后缀下。服务器可以比前面示例更快地处理这种类型的语法。

具有 ROLEDN 绑定类型的示例

下面是与基于角色 DN 的绑定相关联的 userattr 关键字的示例：

```
userattr = "exampleEmployeeReportsTo#ROLEDN"
```

如果绑定 DN 属于目标条目的 exampleEmployeeReportsTo 属性中指定的角色，则绑定规则被评估为 true。例如，如果为贵公司的所有经理创建嵌套角色，则可以使用此机制授予权限，使所有级别的经理访问等级比他们自己低的员工的信息。

角色的 DN 可以在目录中的任何后缀下。此外，如果使用过滤的角色，对这种类型的 ACI 的评估会占用服务器上的许多资源。

具有 LDAPURL 绑定类型的示例

下面是与基于 LDAP 过滤器的绑定相关联的 `userattr` 关键字的示例：

```
userattr = "myfilter#LDAPURL"
```

如果绑定 DN 匹配目标条目的 *myfilter* 属性中指定的过滤器，则绑定规则被评估为 true。 *myfilter* 属性可以替换为包含 LDAP 过滤器的任何属性。

具有任何属性值的示例

下面是与基于任何属性值的绑定相关联的 `userattr` 关键字的示例：

```
userattr = "favoriteDrink#Beer"
```

如果绑定 DN 和目标 DN 包括具有 **`Beer`** 值的 `favoriteDrink` 属性，则绑定规则被评估为 true。

使用具有继承性的 userattr 关键字

在使用 `userattr` 关键字将用于绑定的条目与目标条目关联时， ACI 只应用于指定的目标，而不应用于其下面的条目。在某些情况下，可以将 ACI 应用于目标条目下面的多个级别。通过使用 parent 关键字，并指定应该继承 ACI 的目标下面的级别数，就可以做到这一点。

在将 `userattr` 关键字与 `parent` 关键字联合使用时，语法如下所示：

```
userattr = "parent[inheritance_level].attribute#bindType"
```

其中 ：

- *inheritance_level* 是逗号分隔的列表，表示目标下面多少级别将继承 ACI。可以包括目标条目下面五个级别 `[0,1,2,3,4]` ； 零 (0) 表示目标条目。
- *attribute* 是 `userattr` 或 `groupattr` 关键字针对的属性。
- *bindType* 可以为 `USERDN` 或 `GROUPDN`。`LDAPURL` 和 `ROLEDN` 绑定类型不支持继承性。

例如：

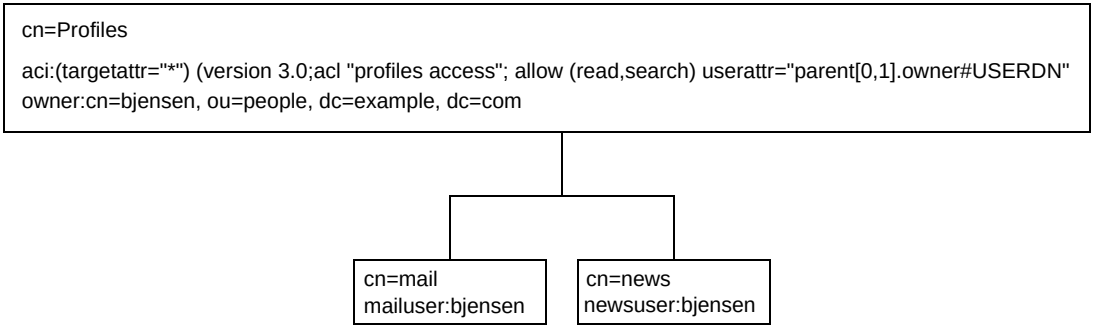
```
userattr = "parent[0,1].manager#USERDN"
```

如果绑定 DN 匹配目标条目的 manager 属性，则此绑定规则被评估为 true。当绑定规则被评估为 true 时授予的权限应用于目标条目以及紧随其下的所有条目。

具有 userattr 继承性的示例

下图中的示例表示用户 bjensen 被允许读取和搜索 cn=Profiles 条目以及包括 cn=mail 和 cn=news 的第一个级别的子条目，从而允许她搜索她自己的邮件和新闻 ID。

图 6-1 使用具有 userattr 关键字的继承



在此示例中，如果没有使用继承性，则必须执行下列操作之一以获得相同结果：

- 为用户 bjensen 显式设置针对目录中 cn=Profiles、 cn=mail 以及 cn=news 条目的读取和搜索访问。
- 向 cn=mail 和 cn=news 条目添加值为 bjensen 的 owner 属性，然后将下列 ACI 添加到 cn=mail 和 cn=news。

```
aci:(targetattr="*") (version 3.0; acl "profiles access"; allow
 (read,search) userattr="owner#USERDN";)
```

使用 userattr 关键字授予添加权限

如果将 userattr 关键字与 **all** 或 **add** 权限一起使用，则会发现服务器的行为不像您预期的那样。通常，当在目录中创建新条目时， Directory Server 评估正在创建的条目上的访问权限，而不是评估父条目上的访问权限。然而，在 ACI 使用 userattr 关键字的情况下，此行为可能会造成安全漏洞，可以修改服务器的正常行为以避免这种情况。

请看下列示例：

```
aci:(target="ldap:///dc=example,dc=com")(targetattr=*) (version 3.0;
 acl "manager-write"; allow (all) userattr = "manager#USERDN";)
```

此 ACI 授予管理员对向他们报告的员工的条目的所有权限。然而，由于访问权限是在正在创建的条目上评估的，这种类型的 ACI 还将允许任何员工创建其 manager 属性被设置为他们自己的 DN 的条目。例如，不满意的员工 Joe (cn=Joe,ou=eng,dc=example,dc=com) 可能想要在树的 Human Resources 分支中创建条目，以使用 （或滥用）授予 Human Resources 员工的权限。

他可以通过创建下列条目做到这一点：

```
dn:cn= Trojan Horse,ou=Human Resources,dc=example,dc=com
objectclass:top
...
cn:Trojan Horse
manager:cn=Joe,ou=eng,dc=example,dc=com
```

为避免这种类型的安全威胁， ACI 评估过程不在级别 0 （即，该条目本身）授予添加权限。然而，可以使用 parent 关键字在现有的条目下授予添加权限。必须为添加权限指定父级别下面的级别数。例如，下列 ACI 允许向其 manager 属性匹配绑定 DN 的 dc=example,dc=com 中的任何条目添加子条目：

```
aci:(target="ldap:///dc=example,dc=com")(targetattr=*)
 (version 3.0; acl "parent-access"; allow (add)
 userattr = "parent[0,1].manager#USERDN";)
```

此 ACI 确保只向其绑定 DN 匹配父条目的 manager 属性的用户授予添加权限。

定义来自特定 IP 地址的访问

使用绑定规则，可以指出绑定操作必须发自特定 IP 地址。这通常用于强制从给定计算机或网络域对所有目录进行更新。

设置基于 IP 地址的绑定规则的 LDIF 语法如下所示：

```
ip = "IPaddressList" 或  ip != "IPaddressList"
```

IPaddressList 是一个或多个以逗号分隔的元素列表，可能为以下任意值：

- 特定 IPv4 地址：123.45.6.7
- 带有通配符的 IPv4 地址用来指定子网络：12.3.45.*
- 带有子网掩码的 IPv4 地址或子网络：123.45.6.*+255.255.255.115
- 以任意合法形式出现的 IPv6 地址，如 RFC 2373 (http://www.ietf.org/rfc/rfc2373.txt) 中定义。以下地址是等效的：
  - 12AB:0000:0000:CD30:0000:0000:0000:0000
  - 12AB::CD30:0:0:0:0

- 12AB:0:0:CD30::

- 带有子网前缀长度的 IPv6 地址：12AB::CD30:0:0:0:0/60

如果访问目录的客户机位于指定的 IP 地址，则绑定规则被评估为 true。对于只允许从特定子网或计算机进行的某些类型的目录访问非常有用。

可以从 Server Console，通过 “访问控制编辑器”定义对其应用 ACI 的特定计算机。详细信息，请参阅 “使用控制台创建 ACI”（第 192 页）。

定义来自特定域的访问

绑定规则可以指定绑定操作必须源于特定域或主机。这通常用于强制从给定计算机或网络域对所有目录进行更新。

设置基于 DNS 主机名的绑定规则的 LDIF 语法如下所示：

```
dns = "DNS_Hostname" 或 dns != "DNS_Hostname"
```

警告 dns 关键字要求在您的计算机上使用的命名服务是 DNS。如果命名服务不是 DNS，则应该使用 ip 关键字代替。

dns 关键字需要完全限定的 DNS 域名。授予对主机的访问而不指定域会带来潜在的安全威胁。例如，允许使用下列表达式，但不建议使用：

```
dns = "legend.eng";
```

应该使用完全限定的名称，如：

```
dns = "legend.eng.example.com";
```

dns 关键字允许使用通配符。例如：

```
dns = "*.example.com";
```

如果访问目录的客户机位于指定的域，则绑定规则被评估为 true。这对于允许只从特定域进行访问非常有用。注意，如果系统使用 DNS 之外的命名服务，则通配符将不起作用。在这种情况下，如果需要限制对特定域的访问，则请使用 ip 关键字，如 “定义来自特定 IP 地址的访问”（第 186 页）中所述。

定义特定时间或星期的访问

可以使用绑定规则指定绑定只能在某些时间或在一个星期中的某些天发生。例如，可以设置规则，以便只允许在星期一到星期五上午 8 点和下午 5 点之间进行访问。用于评估访问权限的时间是目录服务器上的时间，而不是客户机上的时间。

设置基于时间的绑定规则的 LDIF 语法如下所示：

```
timeofday operator "time"
```

其中 *operator* 可以是下列符号之一：等号 (=)、不等号 (!=)、大于号 (>)、大于等于号 (>=)、小于号 (<) 或小于等于号 (<=)。

`timeofday` 关键字要求以 24 小时时钟格式的小时和分钟表示的时间 （0 到 2359）。

注意 使用服务器上的时间进行评估，而不是客户机上的时间。

设置基于星期内的绑定规则的 LDIF 语法如下所示：

```
dayofweek = "day1, day2 ..."
```

dayofweek 关键字的可能值是星期几的三个英语字母缩写：`sun`、 `mon`、 `tue`、 `wed`、 `thu`、 `fri`、 `sat`。

示例

下面是 `timeofday` 和 `dayofweek` 语法的示例：

```
timeofday = "1200";
```

如果客户机正好在中午访问目录，则绑定规则是 true。

```
timeofday != "0100";
```

如果客户机在上午 1 点之外的任何时间访问目录，则绑定规则被评估为 true。

```
timeofday > "0800";
```

如果客户机在上午 8 点以后的任何时间访问目录，则绑定规则被评估为 true。

```
timeofday < "1800";
```

如果客户机在下午 6 点之前的任何时间访问目录，则绑定规则被评估为 true。

```
timeofday >= "0800";
```

如果客户机在上午 8 点或之后访问目录，则绑定规则被评估为 true。

```
timeofday <= "1800";
```

如果客户机在下午 6 点或之前访问目录，则绑定规则被评估为 true。

```
dayofweek = "Sun, Mon, Tue";
```

如果客户机在星期日、星期一或星期二访问目录，则绑定规则被评估为 true。

定义基于验证方法的访问

可以设置绑定规则，以声明客户机必须使用特定验证方法绑定到目录。可用的验证方法有：

- **None** - 不需要验证。这是默认值。它代表匿名访问。
- **Simple** - 客户机必须提供用户名和口令才能绑定到目录。
- **SSL** - 客户机必须通过安全套接字层 (SSL) 或传输层安全性 (TLS) 连接绑定到目录。

  在 SSL 的情况下，建立到 LDAPS 第二个端口的连接；在 TLS 的情况下，通过开始 TLS 操作建立连接。在这两种情况下，都必须提供证书。有关设置 SSL 的信息，请参阅第 11 章 “实现安全性”。
- **SASL** - 客户机必须通过简单验证和安全层 (SASL) 连接绑定到目录。注意，Sun ONE Directory Server 不提供 SASL 模块。

不能通过 “访问控制编辑器”设置基于验证的绑定规则。

设置基于验证方法的绑定规则的 LDIF 语法如下所示：

```
authmethod = "authentication_method"
```

其中 *authentication_method* 是 **`none`**、 **`simple`**、 **`ssl`** 或 **`"sasl`** *sasl_mechanism*`"`。

示例

下面是 `authmethod` 关键字的示例：

```
authmethod = "none";
```

在绑定规则评估期间不检查验证。

```
authmethod = "simple";
```

如果客户机使用用户名和口令访问目录，则绑定规则被评估为 true。

```
authmethod = "ssl";
```

如果客户机通过 LDAPS 使用证书向目录进行验证，则绑定规则被评估为 true。如果客户机通过 LDAPS 使用简单验证 （绑定 DN 和口令）进行验证，则不会为 true。

```
authmethod = "sasl DIGEST-MD5";
```

如果客户机使用 SASL DIGEST-MD5 机制访问目录，则绑定规则被评估为 true。其他受支持的 SASL 机制有 EXTERNAL 和 GSSAPI （仅限 Solaris 系统）。

使用布尔绑定规则

绑定规则可以是使用布尔表达式 AND、 OR，以及 NOT 的复杂表达式，以表达非常精确的访问规则。不能使用 Server Console 创建布尔绑定规则。必须创建 LDIF 语句。

布尔绑定规则的 LDIF 语法如下所示：

bindRule [*boolean*] [*bindRule*] [*boolean*] [*bindRule*] . . . ;)

例如，如果绑定 DN 是管理员组或者邮件管理员组的成员，并且客户机运行于 example.com 域内，那么下面的绑定规则将被评估为 true：

```
(groupdn = "ldap:///cn=administrators,dc=example,dc=com" or
groupdn = "ldap:///cn=mail administrators,dc=example,dc=com" and
dns = "*.example.com";)
```

句末分号 (;) 是必需的分隔符，应出现在最后一个绑定规则之后。

对布尔表达式的评估遵循如下顺序：

- 首先从内到外对括号表达式进行评估
- 从左向右对所有表达式进行评估
- NOT 先于 AND 或 OR 运算符

布尔 OR 和布尔 AND 运算符没有优先级顺序。

请考虑下面的布尔绑定规则：

（*bindRule_A*） OR （*bindRule_B*）

（*bindRule_B*） OR （*bindRule_A*）

由于布尔表达式是从左向右进行评估的，所以在第一种情况下，绑定规则 A 在绑定规则 B 之前进行评估，而在第二种情况下，绑定规则 B 在绑定规则 A 之前进行评估。

但是，布尔 NOT 在布尔 OR 和布尔 AND *之前*进行评估。因此，在下面的示例中：

（*bindRule_A*） AND NOT （*bindRule_B*）

尽管存在从左向右的规则，但绑定规则 B 还是在绑定规则 A 之前进行评估。

从命令行创建 ACI

可以使用 LDIF 语句手动创建访问控制指令，以及使用 `ldapmodify` 命令将它们添加到目录树。因为 ACI 值可能非常复杂，所以查看现有值并对其进行复制以协助创建新的 ACI，这一点会非常有用。

查看 aci 属性值

ACI 作为 `aci` 属性的一个或多个值存储在条目上。 `aci` 属性是多值操作属性，可以由目录用户读取和修改，本身应该由 ACI 保护。管理用户通常被授予对 `aci` 属性的完全访问权，并可以通过以下某种方式查看其值。

可以在 “通用编辑器”中如查看任何其他值一样查看 `aci` 属性值。在 Directory Server 控制台的顶级 “目录”标签中，右键单击带有 ACI 的条目，并选择 “用通用编辑器进行编辑”菜单项。然而， `aci` 值通常是难以在此对话框中查看和编辑的长字符串。

相反，可以通过右击目录树中的条目并选择 “设置访问权限”菜单项，以便调用 “访问控制编辑器”。选择一个 ACI 并单击 “编辑”，然后单击 “手动编辑”以查看对应的 `aci` 值。通过在 ACI 的手动和可视编辑器之间切换，可以将 `aci` 值的语法与其配置进行比较。

如果操作系统允许，则可以从 “通用编辑器”或 “手动访问控制编辑器”复制 `aci` 值以将它粘贴到 LDIF 文件中。管理用户还可以通过运行以下 `ldapsearch` 命令来查看条目的 aci 属性：

```
% ldapsearch -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
              -b entryDN -s base aci
```

结果为 LDIF 文本，可以将其复制到新的 LDIF ACI 定义中以便用于编辑。

注意 要查看以授予或拒绝的权限来表示的 aci 值的效果，请参阅 “查看有效权限”（第 213 页）。

使用控制台创建 ACI

可以配置 Directory Server 控制台来显示目录中的哪些条目具有 aci 属性。通过选择或取消选择 “查看” > “显示” > “ACI 计数”菜单项，可切换此显示。顶层 “目录”标签上列出的条目将显示出它们的 aci 属性中定义的 ACI 的数量。然后，可以使用 Directory Server 控制台查看、创建、编辑和删除目录的访问控制指令。

请参阅 “访问控制用法示例”（第 197 页），以了解 Directory Server 安全策略中通常使用的一组访问控制规则，以及有关使用 Directory Server 控制台创建这些规则的分步指导。

“访问控制编辑器”不允许在可视编辑模式下构建某些比较复杂的 ACI。具体将，不能通过 “访问控制编辑器”执行下列操作：

- 拒绝访问 （请参阅 “权限语法”（第 174 页））
- 创建基于值的 ACI （请参阅 “使用 LDAP 过滤器将属性值作为目标”（第 170 页））
- 定义父访问 （请参阅 “父访问 （parent 关键字）”（第 178 页））
- 创建包含布尔绑定规则的 ACI （请参阅 “使用布尔绑定规则”（第 190 页））
- 在通常情况下，创建使用下列关键字的 ACI：roledn、userattr、authmethod

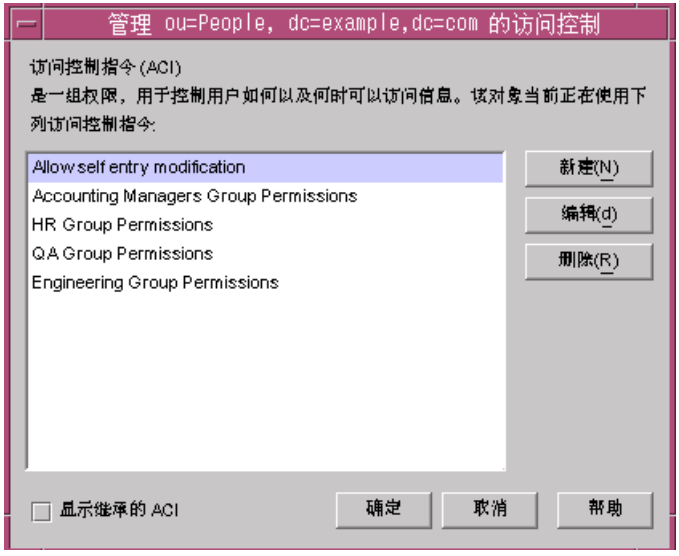
提示 在 “访问控制编辑器”中，可以随时单击 “手动编辑”按钮来检查通过图形界面所作更改的 LDIF 表示。

查看条目的 ACI

1. 在 Directory Server 控制台的顶级 “目录”标签中，浏览目录树以显示要为其设置访问控制的条目。您必须具有目录系统管理员或目录管理员的权限才能编辑 ACI。
2. 右键单击该条目并从弹出菜单中选择 “设置访问权限”。或者，可以用左键单击此条目以选中它，并从 “对象”菜单中选择 “设置访问权限”。

显示 “访问控制管理”对话框，如下图所示。其中列出了对所选条目上定义的所有 ACI 的描述，并允许您编辑或删除它们，以及创建新的 ACI。

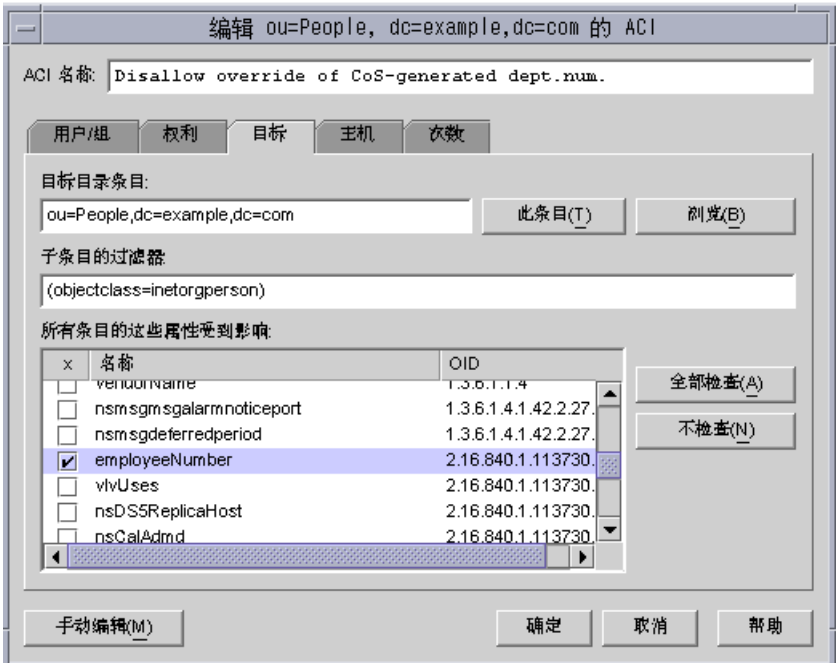
图 6-2 “访问控制管理”对话框



如果选中 “显示继承的 ACI”复选框，那么还将列出由所选条目父级定义的应用于该条目的所有 ACI。不过，继承的 ACI 不能编辑或删除；您必须在定义这些 ACI 的条目上对其进行管理。

3. 单击 “新建”，在选定对象及其整个子树上定义新的访问权限。显示 “ACI 编辑器”，如下图所示。

图 6-3 “ACI 编辑器”对话框



对话框顶部的 ACI 名称是对将出现在“访问控制管理”对话框中的 ACI 的描述。提供描述性的 ACI 名称将使得对整个目录中的 ACI 进行管理变得更容易，特别是在查看叶条目上继承的 ACI 时更是如此。

“访问控制编辑器”的标签可用于指定被允许或拒绝访问的用户，被访问或限制的目标，以及诸如被允许的主机名和操作次数之类的高级参数。有关“访问控制”标签中的单个字段的详细信息，请参阅联机帮助。

ACI 编辑器的标签以图形方式显示了 ACI 值的内容。单击“手动编辑”按钮以查看 ACI 值，并在文本状态下对其进行编辑。在文本编辑器中，可以定义不能通过标签定义的高级 ACI。不过，即使您不使用高级功能，编辑了 ACI 值后，就不能再在可视状态下编辑 ACI。

创建新的 ACI

1. 显示 “访问控制编辑器”。

   此任务在 “查看条目的 ACI”（第 192 页）中讲述。

   如果显示的视图不同于图 6-3 （第 194 页），则请单击 “可视编辑”。

2. 在 “ACI 名称”文本框中键入名称来对 ACI 进行命名。

   名称可以是任何字符串，用于唯一地标识该 ACI。如果没有输入名称，服务器将使用 **`unnamed ACI`**。

3. 在 “用户 / 组”标签中，突出显示 “所有用户”或单击 “添加”按钮来在目录中搜索要授予其访问权的用户。

   在 “添加用户和组”窗口中：

   a. 从下拉列表中选择一个搜索区域，在 “搜索”字段中输入一个搜索字符串，并单击 “搜索”按钮。

      搜索结果会在下面的列表中显示出来。

   b. 在搜索结果列表中突出显示所需的条目，并单击 “添加”按钮将其添加到具有访问权限的条目列表中。

   c. 单击 “确定”关闭 “添加用户和组”窗口。

      您所选的条目将在 ACI 编辑器中的 “用户 / 组”标签上列出。

4. 在 “访问控制编辑器”中，单击 “权限”标签，并使用复选框来选择要授予的权限。

5. 单击 “目标”标签，然后单击 “此条目”来显示此 ACI 所针对的节点。

   可以更改目标 DN 的值，但新 DN 必须是选定条目的直接或间接子条目。

   如果不希望此节点下的子树中的每一个条目都适用该 ACI，那么必须在 “子条目”字段的 “过滤器”中输入一个过滤器。

   此外，还可以通过在属性列表中选择所需的属性来将 ACI 的作用域限制在个别属性上。

6. 单击 “主机”标签，然后单击 “添加”按钮来显示 “添加主机过滤器”对话框。

   可以指定主机名或 IP 地址。如果指定 IP 地址，还可以使用通配符 (*)。

7. 单击 “时间”标签以显示一个上面显示了在哪些时间允许访问的表。

   默认情况下，在任何时候都允许访问。可以通过单击并在表中拖移光标来更改访问时间。不能选择不连续的时间块。

8. 编辑完 ACI 之后，单击 “确定”。

   “ACI 编辑器”关闭，新的 ACI 在 “ACI 管理器”窗口列出。

注意 在创建 ACI 过程中随时都可以单击 “手动编辑”按钮以显示对应于您的输入的 LDIF 语句。可以修改此语句，但您的更改不一定在图形界面中可见。

编辑 ACI

要编辑 ACI，请执行以下操作：

1. 在 “目录”标签上，右键单击子树中的顶部条目，并从弹出菜单中选择 “设置访问权限”。

   “访问控制管理器”窗口将显示出来。它包含属于该条目的 ACI 列表。

2. 在 “访问控制管理器”窗口，突出显示需要编辑的 ACI，并单击 “编辑”。

   将显示 “访问控制编辑器”。有关可以使用此对话框编辑的信息的详细信息，请参阅联机帮助。

3. 在 “访问控制编辑器”的各种标签下进行所需的更改。

4. 编辑完 ACI 之后，单击 “确定”。

   “ACI 编辑器”关闭，修改的 ACI 在 “ACI 管理器”中列出。

删除 ACI

要删除 ACI，请执行以下操作：

1. 在 “目录”标签上，右键单击子树中的顶部条目，并从弹出菜单中选择 “设置访问权限”。

   将显示 “访问控制管理器”窗口。它包含属于该条目的 ACI 列表。

2. 在 “访问控制管理器”窗口，选择需要删除的 ACI。

3. 单击 “删除”。

   该 ACI 不再在 “访问控制管理器”中列出。

访问控制用法示例

本节中提供的示例说明了一个虚构的 ISP 公司 example.com 如何实现其访问控制策略。所有示例讲述了如何从控制台并使用 LDIF 文件执行给定任务。

Example.com 的业务是提供 Web 托管服务和 Internet 访问。Example.com 的 Web 托管服务的一部分是托管客户公司的目录。 Example.com 实际托管并部分管理两个中等规模的公司 Company333 和 Company999 的目录。它还向许多单个用户提供 Internet 访问。

下面是 example.com 需要实施的访问控制规则：

- 为 example.com 的员工授予对整个 example.com 树的读取、搜索和比较的匿名访问 （请参阅 “授予匿名访问”（第 198 页））。
- 授予 example.com 员工诸如 `homeTelephoneNumber`、`homeAddress` 的个人信息的写入访问 （请参阅 “授予对个人条目的写权限”（第 200 页））。
- 授予 example.com 员工向他们的条目添加除某些关键角色之外的任何角色的权限 （请参阅 “限制对关键角色的访问权限”（第 202 页））。
- 授予 example.com Human Resources 组对 People 分支中的条目的所有权限（请参阅 “授予组对后缀的完全访问权限”（第 204 页））。
- 授予所有 example.com 员工在目录的 Social Committee 分支下创建组条目的权限，以及删除他们拥有的条目的权限 （请参阅 “授予添加和删除组条目的权限”（第 205 页））。
- 授予所有 example.com 员工将他们自己添加到目录的 Social Committee 分支下的组条目的权限 （请参阅 “允许用户从组中添加或删除其自身”（第 211 页））。
- 授予 Company333 和 Company999 的目录系统管理员 （角色）对目录树的他们各自的分支的访问权，并带有诸如 SSL 验证、时间和日期限制，以及指定的位置之类的某些条件 （请参阅 “授予对组或角色的条件访问权”（第 207 页））。
- 授予单个用户对他们自己的条目的访问权 （请参阅 “授予对个人条目的写权限”（第 200 页））。
- 拒绝单个用户对他们自己的条目中的记账信息的访问权 （请参阅 “拒绝访问”（第 208 页））。

- 向外界授予对单个用户子树的匿名访问权，特别请求不列出的用户除外。（此部分的目录可以是防火墙外部的从属服务器，并可以一天更新一次。）请参阅“授予匿名访问”（第 198 页）和 “使用过滤器设置目标”（第 211 页）。

授予匿名访问

大多数目录是这样运行的，可以至少匿名地访问一个后缀以便读取、搜索或比较。例如，如果正在运行一个需要员工能够搜索的企业人员目录 （诸如电话簿），则可能需要设置这些权限。在 example.com 内部便是这种情况，并在 ACI “匿名 example.com”示例中进行说明。

作为一个 ISP， example.com 还希望通过创建一本外界可访问的公用电话簿来向其所有用户通知联系信息。这部分在 ACI “匿名世界”示例中进行说明。

ACI “匿名 example.com”

在 LDIF 中，要向 example.com 员工授予对整个 example.com 树的读取、搜索和比较权限，可以写入下列语句：

```
aci:(targetattr !="userPassword")(version 3.0; acl "Anonymous
 example"; allow (read, search, compare) userdn= "ldap:///anyone"
and
 dns="*.example.com";)
```

此示例假设 `aci` 被添加到 `dc=example,dc=com entry`。注意， `userPassword` 属性已从 ACI 的范围中排除。

可以通过执行以下操作从控制台设置此权限：

1. 在 “目录”标签上，右键单击左导航树中的 example.com 节点，并从弹出菜单中选择 “设置访问权限”来显示 “访问控制管理器”。
2. 单击 “新建”，显示 “访问控制编辑器”。
3. 在 “用户 / 组”标签上的 “ACI 名称”字段中，键入 “匿名 example.com”。检查 “所有用户”是否都显示在被授予访问权限的用户列表中。
4. 在 “权限”标签上，选中读取、比较和搜索权限的复选框。确保其他复选框都被清除。
5. 在 “目标”标签上，单击 “此条目”，在目标目录条目字段中显示 `dc=example,dc=com` 后缀。在属性表中，定位 `userPassword` 属性并清除对应的复选框。

   所有其他复选框都应该被选中。如果单击 “名称”标题以按字母顺序组织属性列表，此任务会变得比较容易。
6. 在 “主机”标签上单击 “添加”，并在 DNS 主机过滤器字段，键入 `*.example.com`。单击 “确定”以关闭对话框。

7. 单击 “访问控制编辑器”窗口中的 “确定”。

   新 ACI 被添加到 “访问控制管理器”窗口中列出的 ACI 中。

ACI “匿名世界”

在 LDIF 中，要向外界授予对单个用户子树的读取和搜索访问，而拒绝对未列出的用户的信息访问，可以写入下列语句：

```
aci:(targetfilter= "(!(unlistedSubscriber=yes))")
 (targetattr="homePostalAddress || homePhone || mail") (version 3.0;
 acl "Anonymous World"; allow (read, search) userdn=
 "ldap:///anyone";)
```

此示例假设 ACI 被添加到 `ou=subscribers,dc=example, dc=com` 条目。还假设每一个用户条目都具有可以设置为 yes 或 no 的 `unlistedSubscriber` 属性。目标定义筛选出基于此属性值的未列出的用户。有关过滤器定义的详细信息，请参阅 “使用过滤器设置目标”（第 211 页）。

可以通过执行以下操作从控制台设置此权限：

1. 在 “目录”标签上，右键单击左导航树中 example.com 节点下的 “用户”条目，并从弹出菜单中选择 “设置访问权限”来显示 “访问控制管理器”。
2. 单击 “新建”，显示 “访问控制编辑器”。
3. 在 “用户 / 组”标签上的 “ACI 名称”字段中，键入 “匿名世界”。检查 “所有用户”是否都显示在被授予访问权限的用户列表中。
4. 在 “权限”标签上，选中读取、搜索权限的复选框。确保其他复选框都被清除。
5. 在 “目标”标签上，单击 “此条目”，在目标目录条目字段中显示 `dc=subscribers, dc=example,dc=com` 后缀。

   a. 在子条目字段的过滤器中，键入下列过滤器：

      (!(unlistedSubscriber=yes))

   b. 在属性表中，选中 `homePhone`、 `homePostalAddress` 和 `mail` 属性的复选框。

      所有其他复选框都应该被清除。如果单击 “全部不选”按钮，清除表中所有属性的复选框，然后单击 “名称”标题按字母顺序组织它们，并且选择适当的属性，此任务会变得比较轻松。

6. 单击 “确定”。

   新 ACI 被添加到 “访问控制管理器”窗口中列出的 ACI 中。

授予对个人条目的写权限

许多目录系统管理员希望允许内部用户更改其自己的条目中的某些属性而不是所有属性。 example.com 的目录系统管理员希望允许用户更改其自己的口令、家庭电话号码，以及家庭地址，但不允许更改其他任何信息。这部分在 ACI “写入 example.com”示例中进行说明。

example.com 的策略还允许他们的用户更新 example.com 树中自己的个人信息，前提是他们与目录建立 SSL 连接。这部分在 ACI “写入用户”示例中进行说明。

ACI “写入 example.com”

注意 通过设置此权限，还授予用户删除属性值的权限。

在 LDIF 中，要授予 example.com 雇员更新口令、家庭电话号码和家庭地址的权限，可以写入下列语句：

```
aci:(targetattr="userPassword || homePhone || homePostalAddress")
 (version 3.0; acl "Write example.com"; allow (write) userdn=
 "ldap:///self" and dns="*.example.com";)
```

此示例假设 ACI 被添加到 `ou=example-people,dc=example, dc=com` 条目。

可以通过执行以下操作从控制台设置此权限：

1. 在 “目录”标签上，右键单击左导航树中的 example.com 节点，并从弹出菜单中选择 “设置访问权限”来显示 “访问控制管理器”。
2. 单击 “新建”，显示 “访问控制编辑器”。
3. 在 “用户 / 组”标签上的 “ACI 名称”字段中，键入 “写入 example.com”。在被授予访问权限的用户列表中，执行以下操作：
   a. 选择并删除 “所有用户”，然后单击 “添加”。

      显示 “添加用户和组”对话框。

   b. 将 “搜索”区域设置为 “特殊权限”，并从搜索结果列表中选择 “自身”。
   c. 单击 “添加”按钮，在被授予访问权限的用户列表中列出 “自身”。
   d. 单击 “确定”，关闭 “添加用户和组”对话框。
4. 在 “权限”标签上，选中写权限的复选框。确保其他复选框都被清除。

5. 在 “目标” 标签上，单击 “此条目”，在目标目录条目字段中显示 dc=example,dc=com 后缀。在属性表中，选中 homePhone、homePostalAddress，以及 userPassword 属性的复选框。

   所有其他复选框都应该被清除。如果单击 “全部不选” 按钮，清除表中所有属性的复选框，然后单击 “名称” 标题按字母顺序组织它们，并且选择适当的属性，此任务会变得比较轻松。

6. 在 “主机” 标签上，单击 “添加” 按钮，显示 “添加主机过滤器” 对话框。在 DNS 主机过滤器字段，键入 *.example.com。单击 “确定” 以关闭对话框。

7. 单击 “访问控制编辑器” 窗口中的 “确定”。

   新 ACI 被添加到 “访问控制管理器” 窗口中列出的 ACI 中。

ACI “写入用户”

注意 通过设置此权限，还授予用户删除属性值的权限。

在 LDIF 中，要授予 example.com 用户更新口令、家庭电话号码的权限，可以写入下列语句：

```
aci:(targetattr="userPassword || homePhone") (version 3.0; acl
 "Write Subscribers"; allow (write) userdn= "ldap://self" and
 authmethod="ssl";)
```

此示例假设 aci 被添加到 ou=subscribers,dc=example, dc=com 条目。

请注意， example.com 用户不具有对其家庭地址的写入访问权限，因为他们可能删除该属性，而 example.com 需要该信息进行记帐。因此，家庭地址是对业务比较关键的信息。

可以通过执行以下操作从控制台设置此权限：

1. 在 “目录” 标签上，右键单击左导航树中 example.com 节点下的 “用户” 条目，并从弹出菜单中选择 “设置访问权限” 来显示 “访问控制管理器”。

2. 单击 “新建”，显示 “访问控制编辑器”。

3. 在 “用户 / 组” 标签上的 “ACI 名称” 字段中，键入 “写入用户”。在被授予访问权限的用户列表中，执行以下操作：

   a. 选择并删除 “所有用户”，然后单击 “添加”。

      显示 “添加用户和组” 对话框。

   b. 将 “搜索” 区域设置为 “特殊权限”，并从搜索结果列表中选择 “自身”。

c. 单击 “添加”按钮，在被授予访问权限的用户列表中列出 “自身”。

d. 单击 “确定”，关闭 “添加用户和组”对话框。

4. 在 “权限”标签上，选中写权限的复选框。确保其他复选框都被清除。

5. 在 “目标”标签上，单击 “此条目”，在目标目录条目字段中显示 `dc=subscribers, dc=example,dc=com` 后缀。

   a. 在子条目字段的过滤器中，键入下列过滤器：

      (!(unlistedSubscriber=yes))

   b. 在属性表中，选中 `homePhone`、 `homePostalAddress` 和 `mail` 属性的复选框。

      所有其他复选框都应该被清除。如果单击 “全部不选”按钮，清除表中所有属性的复选框，然后单击 “名称”标题按字母顺序组织它们，并且选择适当的属性，此任务会变得比较轻松。

6. 如果希望用户使用 SSL 进行验证，则通过单击 “手动编辑”按钮切换到手动编辑，并将 `authmethod=ssl` 添加到 LDIF 语句，以使它的形式如下：

```
(targetattr="homePostalAddress || homePhone || mail") (version
3.0; acl "Write Subscribers"; allow (write) (userdn=
"ldap:///self") and authmethod="ssl";)
```

7. 单击 “确定”。

   新 ACI 被添加到 “访问控制管理器”窗口中列出的 ACI 中。

限制对关键角色的访问权限

可以使用目录中的角色定义以标识对业务、网络和目录的管理，或其他目的关键的功能。

例如，可以通过标识全世界企业站点在特定时间和星期几可用的系统管理员子集来创建 `superAdmin` 角色。或者可以创建 `First Aid` 角色，包括在特定站点进行了急救培训的所有成员。有关创建角色定义的信息，请参阅 “分配角色”（第 138 页）。

当某个角色提供的任何一种特权超出了关键企业或业务功能时，应该考虑限制对该角色的访问。例如，在 example.com，雇员可以将除 `superAdmin` 角色之外的任何角色添加到自己的条目中。这部分在 ACI “角色”示例中进行说明。

ACI “角色”

在 LDIF 中，要授予 example.com 雇员将除 `superAdmin` 角色之外的任何角色添加到他们自己的条目的权限，可以写入下列语句：

```
aci:(targetattr="*") (targattrfilters="add=nsRoleDN:(nsRoleDN !=
 "cn=superAdmin, dc=example, dc=com")") (version 3.0; acl "Roles";
 allow (write) userdn= "ldap:///self" and dns="*.example.com";)
```

此示例假设 ACI 被添加到 `ou=example-people,dc=example, dc=com` 条目。

可以通过执行以下操作从控制台设置此权限：

1. 在“目录”标签上，右键单击左导航树中的 example.com 节点，并从弹出菜单中选择“设置访问权限”来显示“访问控制管理器”。
2. 单击“新建”，显示“访问控制编辑器”。
3. 在“用户 / 组”标签上的“ACI 名称”字段中，键入“角色”。在被授予访问权限的用户列表中，执行以下操作：
   a. 选择并删除“所有用户”，然后单击“添加”。

      显示“添加用户和组”对话框。

   b. 在“添加用户和组”对话框中将“搜索”区域设置为“特殊权限”，并从搜索结果列表中选择“自身”。
   c. 单击“添加”按钮，在被授予访问权限的用户列表中列出“自身”。
   d. 单击“确定”以关闭“添加用户和组”对话框。
4. 在“权限”标签上，选中写权限的复选框。确保其他复选框都被清除。
5. 在“主机”标签上，单击“添加”按钮，显示“添加主机过滤器”对话框。在 DNS 主机过滤器字段，键入 `*.example.com`。单击“确定”以关闭对话框。
6. 要为角色创建基于值的过滤器，可通过单击“手动编辑”按钮切换到手动编辑。将下列内容添加到 LDIF 语句的开始：

   ```
   (targattrfilters="add=nsRoleDN:(nsRoleDN != "cn=superAdmin,
   dc=example,dc=com")")
   ```

   LDIF 语句的形式应该如下：

   ```
   (targetattr="*") (targattrfilters="add=nsRoleDN:(nsRoleDN !=
   "cn=superAdmin, dc=example,dc=com")") (target =
   "ldap:///dc=example,dc=com") (version 3.0; acl "Roles"; allow
   (write) (userdn = "ldap:///self") and (dns="*.example.com");)
   ```

7. 单击“确定”。

   新 ACI 被添加到“访问控制管理器”窗口中列出的 ACI 中。

授予组对后缀的完全访问权限

大多数目录具有用于标识某些企业功能的组。可以给这些组授予对整个目录或部分目录的完全访问权限。通过向该组应用访问权限，可以避免分别地为每个成员设置访问权限。相反，可以只通过将用户添加到该组来向他们授予这些访问权限。

例如，在使用 “典型安装” 过程安装 Directory Server 时，默认创建了对目录具有完全访问权限的 Administrators 组。

在 example.com，Human Resources 组被授予对目录的 `ou=example-people` 分支的完全访问权，以使他们可以更新雇员目录。这部分在 ACI “HR” 示例中进行说明。

ACI “HR”

在 LDIF 中，要授予 HR 组对目录的雇员分支的所有权限，可以使用下列语句：

```
aci:(targetattr="*") (version 3.0; acl "HR"; allow (all)
 userdn= "ldap:///cn=HRgroup,ou=example-people,dc=example,dc=com";)
```

此示例假设 ACI 被添加到 `ou=example-people,dc=example, dc=com` 条目。

可以通过执行以下操作从控制台设置此权限：

1. 在 “目录” 标签上，右键单击左导航树中 example.com 节点下的 example.com-people 条目，并从弹出菜单中选择 “设置访问权限” 来显示 “访问控制管理器”。
2. 单击 “新建”，显示 “访问控制编辑器”。
3. 在 “用户 / 组” 标签上的 “ACI 名称” 字段中，键入 “HR”。在被授予访问权限的用户列表中，执行以下操作：
   a. 选择并删除 “所有用户”，然后单击 “添加”。

      显示 “添加用户和组” 对话框。

   b. 将 “搜索” 区域设置为 “用户和组”，并在 “搜索” 字段中键入 “HRgroup”。

      此示例假设已经创建了 HR 组或角色。有关组和角色的详细信息，请参阅第 5 章 “高级条目管理”。

   c. 单击 “添加” 按钮，在被授予访问权限的用户列表中列出 HR 组。

   d. 单击 “确定”，关闭 “添加用户和组” 对话框。
4. 在 “权限” 标签上，单击 “全部选中” 按钮。

   除代理权限以外的所有复选框都被选中。

5. 单击 “确定”。

   新 ACI 被添加到 “访问控制管理器”窗口中列出的 ACI 中。

授予添加和删除组条目的权限

某些组织希望允许雇员在树中创建条目，如果这样做可以提高他们的效率，或者如果可以有助于企业的活力。

例如，在 example.com 有一个活跃的社会委员会，由各种俱乐部组成：网球、游泳、滑雪、角色扮演等。任何 example.com 雇员都可以创建一个代表新俱乐部的组条目。这部分在 ACI “创建组”示例中进行了说明。任何 example.com 雇员都可以成为这些组中的某一个组的成员。这部分在 “允许用户从组中添加或删除其自身”（第 211 页）下的 ACI “组成员”中进行说明。只有组的所有者才能修改或删除组条目。这部分在 ACI “删除组”示例中进行说明。

ACI “创建组”

在 LDIF 中，要授予 example.com 雇员在 `ou=Social Committee` 分支下创建组条目的权限，可以写入下列语句：

```
aci:(target="ldap:///ou=social committee,dc=example,dc=com)
 (targetattr="*")(targattrfilters="add=objectClass:
 (objectClass=groupOfNames)") (version 3.0; acl "Create Group";
 allow (read,search,add) (userdn= "ldap:///uid=*,ou=example-people,
 dc=example,dc=com") and dns="*.example.com";)
```

注意 此 ACI 不授予写权限，这意味着条目创建者无法修改条目。

此示例假设 ACI 被添加到 `ou=social committee, dc=example,dc=com` 条目。

可以通过执行以下操作从控制台设置此权限：

1. 在 “目录”标签上，右键单击左导航树中 example.com 节点下的 Social Committee 条目，并从弹出菜单中选择 “设置访问权限”来显示 “访问控制管理器”。
2. 单击 “新建”，显示 “访问控制编辑器”。
3. 在 “用户 / 组”标签上的 “ACI 名称”字段中，键入 “创建组”。在被授予访问权限的用户列表中，执行以下操作：
   a. 选择并删除 “所有用户”，然后单击 “添加”。

      显示 “添加用户和组”对话框。

b. 将 “搜索”区域设置为 “特殊权限”，并从搜索结果列表中选择 “所有经过验证的用户”。

c. 单击 “添加”按钮，列出被授予访问权限的用户列表中的 “所有经过验证的用户”。

d. 单击 “确定”，关闭 “添加用户和组”对话框。

4. 在 “权限”标签上，选中读取、搜索和添加的复选框。确保其他复选框都被清除。

5. 在 “目标”标签上，单击 “此条目”，在目标目录条目字段中显示 `ou=social committee, dc=example,dc=com` 后缀。

6. 在 “主机”标签上，单击 “添加”按钮以显示 “添加主机过滤器”对话框。在 DNS 主机过滤器字段，键入 `*.example.com`。单击 “确定”以关闭对话框。

7. 要创建将允许雇员只向此子树添加组条目的基于值的过滤器，请通过单击 “手动编辑”按钮切换到手动编辑。将下列内容添加到 LDIF 语句的开始：

```
(targattrfilters="add=objectClass:(objectClass=groupOfNames)")
```

LDIF 语句的形式应该如下：

```
(targetattr = "*")
(targattrfilters="add=objectClass:(objectClass=groupOfNames)")
(target="ldap:///ou=social committee,dc=example,dc=com) (version
3.0; acl "Create Group"; allow (read,search,add) (userdn=
"ldap:///all") and (dns="*.example.com"); )
```

8. 单击 “确定”。

新 ACI 被添加到 “访问控制管理器”窗口中列出的 ACI 中。

ACI “删除组”

在 LDIF 中，要授予 example.com 雇员在 `ou=Social Comittee` 分支下修改或删除他们所拥有的组条目的权限，可以写入下列语句：

```
aci:(target="ou=social committee,dc=example,dc=com)(targetattr =
"*")
 (targattrfilters="del=objectClass:(objectClass=groupOfNames)")
 (version 3.0; acl "Delete Group"; allow (write,delete) userattr=
 "owner#GROUPDN";)
```

此示例假设 `aci` 被添加到 `ou=social committee, dc=example,dc=com` 条目。

使用控制台不是创建此 ACI 的有效方式，因为必须使用手动编辑模式创建目标过滤器，以及检查组的所有权。

授予对组或角色的条件访问权

在许多情况下，授予组或角色对目录的特权访问时，您希望确保防止这些特权被试图假冒有特权用户的入侵者盗用。因此，在许多情况下，授予组或角色关键访问权的访问控制规则通常与许多条件关联。

例如， example.com 已经为其托管的每个公司 （Company333 和 Company999）创建目录系统管理员角色。它希望这些公司能够管理其自己的数据，并实现自己的访问控制规则，同时防止入侵者。因此， Company333 和 Company999 具有对目录树中他们各自的分支的完全访问权限，前提是满足下列条件：

- 通过 SSL 使用证书验证连接
- 在上午 8 点和下午 6 点之间，星期一到星期四请求访问，以及
- 每个公司从指定 IP 地址请求访问。

这些条件在每个公司的单个 ACI （ACI “Company333” 和 ACI “Company999”）中显示。由于这些 ACI 的内容相同，下面的示例只说明了 “Company333”。

ACI “Company333”

在 LDIF 中，要在上述条件下授予 Company333 对目录中他们各自的分支的完全访问权，可以写入下列语句：

```
aci:(target="ou=Company333,ou=corporate-clients,dc=example,dc=com")
 (targetattr = "*") (version 3.0; acl "Company333"; allow (all)
 (roledn="ldap:///cn=DirectoryAdmin,ou=Company333,
 ou=corporate-clients,dc=example,dc=com") and (authmethod="ssl") and
 (dayofweek="Mon,Tues,Wed,Thu") and (timeofday >= "0800" and
 timeofday <= "1800") and (ip="255.255.123.234"); )
```

此示例假设 ACI 被添加到 `ou=Company333, ou=corporate-clients,dc=example,dc=com` 条目。

可以通过执行以下操作从控制台设置此权限：

1. 在 “目录” 标签上，右键单击左导航树中 example.com 节点下的 Company333 条目，并从弹出菜单中选择 “设置访问权限” 来显示 “访问控制管理器”。
2. 单击 “新建”，显示 “访问控制编辑器”。
3. 在 “用户 / 组” 标签上的 “ACI 名称” 字段中，键入 “Company333”。在被授予访问权限的用户列表中，执行以下操作：
   a. 选择并删除 “所有用户”，然后单击 “添加”。

      显示 “添加用户和组” 对话框。

b. 将 “搜索”区域设置为 “用户和组”，并在 “搜索”字段中键入 “DirectoryAdmin”。

此示例假设已经用 DirectoryAdmin 的 cn 创建了管理员角色。

c. 单击 “添加”按钮，在被授予访问权限的用户列表中列出管理员角色。

d. 单击 “确定”，关闭 “添加用户和组”对话框。

4. 在 “权限”标签上，单击 “全部选中”按钮。

5. 在 “目标”标签上，单击 “此条目”，在目标目录条目字段中显示 ou=Company333,ou=corporate-clients,dc=example,dc=com 后缀。

6. 在 “主机”标签上，单击 “添加”按钮，显示 “添加主机过滤器”对话框。在 IP 地址主机过滤器字段，键入 255.255.123.234。单击 “确定”以关闭对话框。

IP 地址必须是主机的有效 IP 地址， Company333 管理员将使用它以连接到 example.com 目录。

7. 在 “时间”标签上，选择对应于星期一到星期四，以及上午 8 点到下午 6 点 的时间块。

表下方将显示一则消息，指定您选择的时间块。

8. 要强制从 Company333 管理员进行 SSL 验证，请通过单击 “手动编辑”按钮来切换到手动编辑。将下列内容添加到 LDIF 语句的末尾：

and (authmethod="ssl")

LDIF 语句应类似于：

```
aci:(targetattr = "*")(target="ou=Company333,
 ou=corporate-clients,dc=example,dc=com") (version 3.0; acl
 "Company333"; allow (all) (roledn="ldap:///cn=DirectoryAdmin,
 ou=Company333,ou=corporate-clients, dc=example,dc=com") and
 (dayofweek="Mon,Tues,Wed,Thu") and (timeofday >= "0800" and
 timeofday <= "1800") and (ip="255.255.123.234") and
 (authmethod="ssl"); )
```

9. 单击 “确定”。

新 ACI 被添加到 “访问控制管理器”窗口中列出的 ACI 中。

拒绝访问

如果目录保存了对业务关键的信息，则可能特别希望拒绝对它的访问。

例如， example.com 希望所有用户都能够读取他们自己的条目下的诸如连接时间或帐户余额之类的记帐信息，但明确希望拒绝对该信息的写入访问。这部分分别在 ACI “记帐信息读取”和 ACI “记帐信息拒绝”中进行说明。

ACI “记帐信息读取”

在 LDIF 中，要授予用户读取他们自己的条目中记帐信息的权限，可以写入下列语句：

```
aci:(targetattr="connectionTime || accountBalance") (version 3.0;
 acl "Billing Info Read"; allow (search,read)
 userdn="ldap:///self";)
```

此示例假设已经在模式中创建相关的属性，并且 ACI 被添加到 `ou=subscribers,dc=example,dc=com` 条目。

可以通过执行以下操作从控制台设置此权限：

1. 在 “目录”标签上，右键单击左导航树中 example.com 节点下的 “用户”条目，并从弹出菜单中选择 “设置访问权限”来显示 “访问控制管理器”。
2. 单击 “新建”，显示 “访问控制编辑器”。
3. 在 “用户 / 组”标签上的 “ACI 名称”字段中，键入 “记帐信息读取”。在被授予访问权限的用户列表中，执行以下操作：
   a. 选择并删除 “所有用户”，然后单击 “添加”。

      显示 “添加用户和组”对话框。

   b. 在 “添加用户和组”对话框中将 “搜索”区域设置为 “特殊权限”，并从搜索结果列表中选择 “自己”。
   c. 单击 “添加”按钮，在被授予访问权限的用户列表中列出 “自身”。
   d. 单击 “确定”以关闭 “添加用户和组”对话框。
4. 在 “权限”标签上，选中搜索和读取权限的复选框。确保其他复选框都被清除。
5. 在 “目标”标签上，单击 “此条目”，在目标目录条目字段中显示 `ou=subscribers, dc=example,dc=com` 后缀。在属性表中，选中 `connectionTime` 和 `accountBalance` 属性的复选框。

   所有其他复选框都应该被清除。如果单击 “全部不选”按钮，清除表中所有属性的复选框，然后单击 “名称”标题按字母顺序组织它们，并且选择适当的属性，此任务会变得比较轻松。

   此示例假设您已经将 `connectionTime` 和 `accountBalance` 属性添加到模式。

6. 单击 “确定”。

   新 ACI 被添加到 “访问控制管理器”窗口中列出的 ACI 中。

ACI “记帐信息拒绝”

在 LDIF 中，要拒绝用户修改他们自己的条目中记帐信息的权限，可以写入下列语句：

```
aci:(targetattr="connectionTime || accountBalance") (version 3.0;
 acl "Billing Info Deny"; deny (write) userdn= "ldap:///self";)
```

此示例假设已经在模式中创建相关的属性，并且 ACI 被添加到 `ou=subscribers,dc=example,dc=com` 条目。

可以通过执行以下操作从控制台设置此权限：

1. 在 “目录”标签上，右键单击左导航树中 example.com 节点下的 “用户”条目，并从弹出菜单中选择 “设置访问权限”来显示 “访问控制管理器”。
2. 单击 “新建”以显示 “访问控制编辑器”。
3. 在 “用户 / 组”标签上的 “ACI 名称”字段中，键入 “记帐信息拒绝”。在被授予访问权限的用户列表中，执行以下操作：

   a. 选择并删除 “所有用户”，然后单击 “添加”。

      显示 “添加用户和组”对话框。

   b. 在 “添加用户和组”对话框中将 “搜索”区域设置为 “特殊权限”，并从搜索结果列表中选择 “自身”。

   c. 单击 “添加”按钮，在被授予访问权限的用户列表中列出 “自身”。

   d. 单击 “确定”以关闭 “添加用户和组”对话框。

4. 在 “权限”标签上，选中写权限的复选框。确保其他复选框都被清除。
5. 单击 “手动编辑”按钮，在显示的 LDIF 语句中，将 **`allow`** 更改为 **`deny`**。
6. 在 “目标”标签上，单击 “此条目”，在目标目录条目字段中显示 `ou=subscribers, dc=example,dc=com` 后缀。在属性表中，选中 `connectionTime` 和 `accountBalance` 属性的复选框。

   所有其他复选框都应该被清除。如果单击 “全部不选”按钮，清除表中所有属性的复选框，然后单击 “名称”标题按字母顺序组织它们，并且选择适当的属性，此任务会变得比较轻松。

   此示例假设您已经将 `connectionTime` 和 `accountBalance` 属性添加到模式。

7. 单击 “确定”。

   新 ACI 被添加到 “访问控制管理器”窗口中列出的 ACI 中。

使用过滤器设置目标

如果希望设置访问控制，允许对分散在目录中的许多条目进行访问，则可能希望使用过滤器设置目标。请记住，由于搜索过滤器不直接指出要管理其访问的对象，因此容易无意中允许或拒绝对错误对象的访问，特别是在目录变得比较复杂时。此外，过滤器可能会使解决目录内的访问控制问题变得比较困难。

允许用户从组中添加或删除其自身

许多目录设置 ACI，允许用户从组中添加或删除他们自身。例如，这对于允许用户从邮件列表添加和删除他们自身是有用的。

在 example.com，雇员可以将他们自己添加到 `ou=social committee` 子树下的任何组条目。这部分在 ACI “组成员”示例中进行说明。

ACI “组成员”

在 LDIF 中，要授予 example.com 雇员从一个组中添加或删除他们自己的权限，可以写入下列语句：

```
aci:(targettattr="member")(version 3.0; acl "Group Members";
 allow (selfwrite)
 (userdn= "ldap:///uid=*,ou=example-people,dc=example,dc=com") ;)
```

此示例假设 ACI 被添加到 `ou=social committee, dc=example,dc=com` 条目。

可以通过执行以下操作从控制台设置此权限：

1. 在 “目录”标签上，右键单击左导航树中 `example.com` 节点下的 `example-people` 条目，并从弹出菜单中选择 “设置访问权限”来显示 “访问控制管理器”。
2. 单击 “新建”，显示 “访问控制编辑器”。
3. 在 “用户 / 组”标签上的 “ACI 名称”字段中，键入 “组成员”。在被授予访问权限的用户列表中，执行以下操作：
   a. 选择并删除 “所有用户”，然后单击 “添加”。

      显示 “添加用户和组”对话框。

   b. 在 “添加用户和组”对话框中将 “搜索”区域设置为 “特殊权限”，并从搜索结果列表中选择 “所有经过验证的用户”。

c. 单击 “添加”按钮，列出被授予访问权限的用户列表中的 “所有经过验证的用户”。

d. 单击 “确定”，关闭 “添加用户和组”对话框。

4. 在 “权限”标签上，选中自身写入的复选框。确保其他复选框都被清除。

5. 在 “目标”标签上，在目标目录条目字段中键入 dc=example,dc=com 后缀。在属性表中，选中 member 属性的复选框。

   所有其他复选框都应该被清除。如果单击 “全部不选”按钮，清除表中所有属性的复选框，然后单击 “名称”标题按字母顺序组织它们，并且选择适当的属性，此任务会变得比较轻松。

6. 单击 “确定”。

   新 ACI 被添加到 “访问控制管理器”窗口中列出的 ACI 中。

为包含逗号的 DN 定义权限

包含逗号的 DN 需要在 LDIF ACI 语句中进行特殊处理。在 ACI 语句的目标和绑定规则部分，逗号必须要用单个反斜杠 (\) 进行转义。下面的示例说明了此语法：

```
dn:dc=example.com Bolivia\, S.A.,dc=com
objectClass:top
objectClass:organization
aci:(target="ldap:///dc=example.com Bolivia\,
 S.A.,dc=com")(targetattr="*") (version 3.0; acl "aci 2"; allow
 (all) groupdn = "ldap:///cn=Directory Administrators,dc=example.com
 Bolivia\, S.A.,dc=com";)
```

代理授权 ACI 示例

代理授权方法是验证的一种特殊形式：使用其自己的身份绑定到目录的用户通过代理授权被授予另一个用户的权限。

对于此示例，假设：

- 客户机应用程序的绑定 DN 是 "uid=MoneyWizAcctSoftware, ou=Applications,dc=example,dc=com"。
- 客户机应用程序请求对其进行访问的目标子树是 ou=Accounting,dc=example,dc=com。
- 目录中已经存在具有对 ou=Accounting,dc=example,dc=com 子树访问权限的 Accounting Administrator。

为了使客户机应用程序获得对 Accounting 子树的访问权 （使用与 Accounting Administrator 相同的访问权限）：

- Accounting Administrator 必须具有对 `ou=Accounting,dc=example,dc=com` 子树的访问权限。例如，下面的 ACI 将所有权限授予 Accounting Administrator 条目：

```
aci:(target="ldap:///ou=Accounting,dc=example,dc=com")
 (targetattr="*") (version 3.0; acl "allowAll-AcctAdmin"; allow
 (all) userdn="uid=AcctAdministrator,ou=Administrators,
 dc=example,dc=com")
```

- 目录中必须存在下列 ACI 向客户机应用程序授予代理权限：

```
aci:(target="ldap:///ou=Accounting,dc=example,dc=com")
 (targetattr="*") (version 3.0; acl "allowproxy-
 accountingsoftware"; allow (proxy) userdn=
 "uid=MoneyWizAcctSoftware,ou=Applications,dc=example,dc=com")
```

有了此 ACI， MoneyWizAcctSoftware 客户机应用程序可以绑定到目录并发送需要代理 DN 访问权限的 LDAP 命令，例如 `ldapsearch` 或 `ldapmodify`。

在上述示例中，如果客户机希望执行 `ldapsearch` 命令，该命令将包括下列控制：

```
# ldapsearch -w 口令 \
-D "uid=MoneyWizAcctSoftware,ou=Applications,dc=example,dc=com" \
-y "uid=AcctAdministrator,ou=Administrators,dc=example,dc=com" ...
```

请注意，客户机作为其自身绑定，但被授予代理条目的权限。客户机不需要代理条目的口令。

注意 不能使用目录管理员的 DN 作为代理 DN。也不能将代理权限授予目录管理员。此外，如果 Directory Server 在同一绑定操作中接收多个代理验证控制，则会向客户机应用程序返回一个错误，绑定尝试失败。

查看有效权限

在目录的条目上维护访问策略时，知道对您定义的 ACI 安全性产生的影响非常有帮助。 Sun ONE Directory Server 5.2 引入了一种新机制，用于评估现有的 ACI，并报告它们为给定用户授予的针对给定条目的有效权限。

Directory Server 将响应可能包括在搜索操作中的新的 “获得有效权限”控制。对此控制的响应是在搜索结果中返回有关条目和属性的有效权限信息。此额外信息包括每个条目以及每个条目中的每个属性的读取和写入权限。用于搜索的绑定 DN 或任意 DN，可能要求这些权限，允许管理员测试目录用户的权限。

警告 查看有效权限本身应该是受保护和受相应限制的目录操作。为 `aclRights` 和 `aclRightsInfo` 属性创建进一步的 ACI 以限制目录用户对此信息的访问。

有效的权限功能依赖于 LDAP 控制。要查看链接后缀上的有效权限，必须在链接策略中启用此控制，如 “配置链接策略”（第 101 页）中所述。还必须确保用于绑定到远程服务器的代理身份也允许访问有效权限属性。

使用 “获得有效权限”控制

通过使用带有 `-J "1.3.6.1.4.1.42.2.27.9.5.2"` 选项的 `ldapsearch` 命令来指定 “获得有效权限”控制。默认情况下，该控制将在搜索结果中返回条目和属性上绑定 DN 条目的有效权限。使用下面的选项更改默认行为：

- `-c "dn:`*DN*`"` - 搜索结果将显示与给定 *DN* 绑定的用户的有效权限。此选项允许管理员检查另一个用户的有效权限。选项 `-c "dn:"` 将显示匿名验证的有效权限。
- `-X "`*attributeName ...*`"` - 搜索结果还将包括指定属性的有效权限。使用此选项指定将不出现在搜索结果中的属性。例如，使用此选项确定用户是否具有权限，添加条目中当前不存在的属性。

使用 `-c` 和 `-X` 属性中的某一个或两者时，隐含了具有 “获得有效权限”控制 OID 的 `-J` 选项，因此不必指定。

然后必须选择希望查看的信息类型：简单权限，或是讲述如何授予或拒绝这些权限的比较详细的记录信息。信息的类型是通过分别添加 `aclRights` 或 `aclRightsInfo;logs` 来确定的，作为要在搜索结果中返回的属性。可以请求两个属性接收全部的有效权限信息，尽管简单权限带有详细日志记录信息中的信息是多余的。

注意 aclRights 和 aclRightsInfo;logs 属性具有虚拟操作属性的行为。它们不存储在目录中，因此除非明确请求，它们将不返回。这些属性是由 Directory Server 响应 “获得有效权限”控制生成的。

因此，这些属性中没有属性可用于任何类型的过滤器或搜索操作中。

下面的示例显示了用户如何可以查看她在目录中的权限。在结果中， 1 表示授予了权限， 0 表示拒绝了权限：

```
% ldapsearch -J "1.3.6.1.4.1.42.2.27.9.5.2" \
             -h rousseau.example.com -p 389 \
             -D "uid=cfuente,ou=People,dc=example,dc=com" \
             -w 口令 -b "dc=example,dc=com" \
             "(objectclass=*)" aclRights

dn:dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:ou=Groups, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:cn=Accounting Managers,ou=groups,dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:cn=HR Managers,ou=groups,dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:uid=bjensen,ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:uid=cfuente, ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:1,proxy:0
```

此结果向 Carla Fuente 显示了目录中的条目，在此，她至少具有读取权限，并且可以修改她自己的条目。有效权限控制不能避开正常的访问权限，因此用户将无法看到他们没有读取权限的条目。在下面的示例中，目录管理员可以看到 Carla Fuente 没有读取权限的条目：

```
% ldapsearch -h rousseau.example.com -p 389 \
             -D "cn=Directory Manager" -w 口令\
             -c "dn:uid=cfuente,ou=People,dc=example,dc=com" \
             -b "dc=example,dc=com" \
             "(objectclass=*)" aclRights
```

```
dn:dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:ou=Groups, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:cn=Directory Administrators, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:0,write:0,proxy:0

dn:ou=Special Users,dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:0,write:0,proxy:0

dn:ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:cn=Accounting Managers,ou=groups,dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:cn=HR Managers,ou=groups,dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:uid=bjensen,ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:uid=cfuente, ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:1,proxy:0
```

在上面的输出中，目录管理员可以看到 Carla Fuente 甚至都不能查看的目录树中“特殊用户”和“目录系统管理员”分支。在下面的示例中，目录管理员可以看到 Carla Fuente 不能修改其自身条目中的 `mail` 和 `manager` 属性：

```
% ldapsearch -h rousseau.example.com -p 389 \
             -D "cn=Directory Manager" -w 口令\
             -c "dn:uid=cfuente,ou=People,dc=example,dc=com" \
             -b "dc=example,dc=com" \
             "(uid=cfuente)" aclRights "*"

version: 1
dn:uid=cfuente, ou=People, dc=example,dc=com

aclRights;attributeLevel;mail:search:1,read:1,compare:1,
 write:0,selfwrite_add:0,selfwrite_delete:0,proxy:0
mail:cfuente@example.com

aclRights;attributeLevel;uid:search:1,read:1,compare:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
uid:cfuente

aclRights;attributeLevel;givenName:search:1,read:1,compare:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
givenName:Carla
```

```
aclRights;attributeLevel;sn:search:1,read:1,compare:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
sn:Fuente

aclRights;attributeLevel;cn:search:1,read:1,compare:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
cn:Carla Fuente

aclRights;attributeLevel;userPassword:search:0,read:0,
 compare:0,write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
userPassword:{SSHA}wnbWHIq2HPiY/5ECwe6MWBGx2KMiZ8JmjF80Ow==

aclRights;attributeLevel;manager:search:1,read:1,compare:1,
 write:0,selfwrite_add:0,selfwrite_delete:0,proxy:0
manager:uid=bjensen,ou=People,dc=example,dc=com

aclRights;attributeLevel;telephoneNumber:search:1,read:1,compare
:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
telephoneNumber: (234) 555-7898

aclRights;attributeLevel;objectClass:search:1,read:1,compare:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
objectClass:top
objectClass:person
objectClass:organizationalPerson
objectClass:inetorgperson

aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0
```

`aclRights` 和 `aclRightsInfo;logs` 属性的格式在 *Sun ONE Directory Server 部署指南* 第 7 章中的 “了解有效权限结果”进行详细描述。

高级访问控制：使用宏 ACI

在使用重复目录树结构的组织中，可以通过使用宏来优化目录中使用的 ACI 的数量。减少目录树中 ACI 的数量使得管理访问控制策略更轻松，并且可以提高 ACI 内存使用的效率。

宏是用于表示 ACI 中的 DN 或 DN 的一部分的占位符。可以使用宏来代表 ACI 目标部分、绑定规则部分或两者中的 DN。实际上，当 Directory Server 获取一个传入 LDAP 操作时， ACI 宏与 LDAP 操作作为目标的资源进行匹配，以确定匹配的子字符串 （如果有）。如果匹配，则将使用匹配的子字符串扩展绑定规则端的宏，并通过评估已扩展的绑定规则来确定对资源的访问权限。

宏 ACI 示例

使用示例可以更好地说明宏 ACI 的优点及其工作方式。图 6-4（第 219 页）显示了一个目录树，其中使用宏 ACI 是减少 ACI 总数的有效方式。

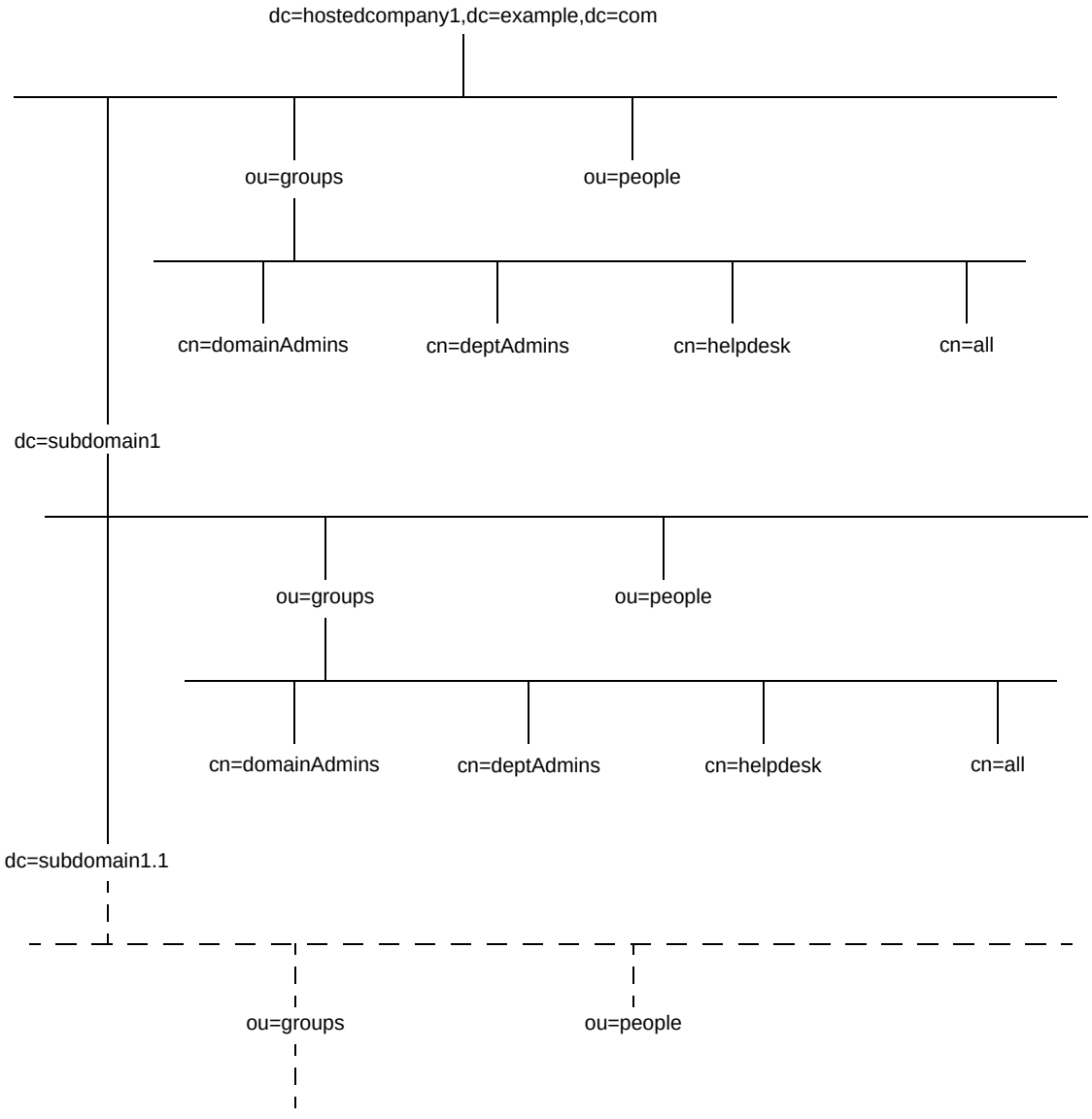
在此插图中，请注意，具有相同树结构 (ou=groups，ou=people) 的子域的重复模式。此模式还跨整个树重复，因为 example.com 目录树存储了下列后缀 dc=hostedCompany2,dc=example,dc=com 和 dc=hostedCompany3,dc=example,dc=com。

在目录树中应用的 ACI 也具有重复模式。例如，下面的 ACI 位于 dc=hostedCompany1,dc=example,dc=com 节点：

```
aci:(targetattr="*")(targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search) groupdn=
 "ldap:///cn=DomainAdmins,ou=Groups,dc=hostedCompany1,dc=example,
 dc=com";)
```

此 ACI 向 DomainAdmins 组授予对 dc=hostedCompany1,dc=example,dc=com 树中的任何条目的读取和搜索权限。

图 6-4 宏 ACI 的示例目录树



下面的 ACI 位于 `dc=hostedCompany1,dc=example,dc=com` 节点：

```
aci:(targetattr="*")(targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search)
 groupdn="ldap:///cn=DomainAdmins,ou=Groups,dc=hostedCompany1,
 dc=example,dc=com";)
```

下面的 ACI 位于 dc=subdomain1,dc=hostedCompany1, dc=example,dc=com 节点：

```
aci:(targetattr="*")(targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search)
 groupdn="ldap:///cn=DomainAdmins,ou=Groups,dc=subdomain1,
 dc=hostedCompany1,dc=example,dc=com";)
```

下面的 ACI 位于 dc=hostedCompany2,dc=example,dc=com 节点：

```
aci:(targetattr="*")(targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search)
 groupdn="ldap:///cn=DomainAdmins,ou=Groups,dc=hostedCompany2,
 dc=example,dc=com";)
```

下面的 ACI 位于 dc=subdomain1,dc=hostedCompany2, dc=example,dc=com 节点：

```
aci:(targetattr="*")(targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search)
 groupdn="ldap:///cn=DomainAdmins,ou=Groups, dc=subdomain1,
 dc=hostedCompany2,dc=example,dc=com";)
```

在上面显示的四个 ACI 中，唯一区别是 groupdn 关键字中指定的 DN。通过为 DN 使用宏，可以在树根部的 dc=example,dc=com 节点上用单个 ACI 替换这些 ACI。此 ACI 的形式如下：

```
aci:(target="ldap:///ou=Groups,($dn),dc=example,dc=com")
 (targetattr="*")(targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search) groupdn=
 "ldap:///cn=DomainAdmins,ou=Groups,[$dn],dc=example,dc=com";)
```

请注意，需要引入以前没有使用的 target 关键字。

在上面的示例中， ACI 的数量从四个减到一个。然而，真正的优点是沿着目录树具有多少重复模式的因素。

宏 ACI 语法

为了简化本节中的讨论，用于提供诸如 userdn、 roledn、 groupdn 和 userattr 绑定凭证的 ACI 关键字统称为 ACI 的*主题*。主题确定 ACI 应用的对象。

宏 ACI 包括下列类型的表达式以替换 DN 或 DN 的一部分：

- (`$dn`) - 用于与目标匹配及在主题中直接替换。
- [`$dn`] - 用于替换主题子树中的多个 RDN。
- (`$attr.`*attributeName*) - 用于将 *attributeName* 属性的值从目标条目替换至主题。

表 6-3 显示了在 ACI 的哪些部分可以使用 DN 宏：

表 6-3 ACI 关键字中的宏

宏	ACI 关键字
(`$dn`)	target、 targetfilter、 userdn、 roledn、 groupdn、 userattr
[`$dn`]	targetfilter、 userdn、 roledn、 groupdn、 userattr
(`$attr.`*attrName*)	userdn、 roledn、 groupdn、 userattr

下面的限制适用：

- 使用主题中的 (`$dn`) 和 [`$dn`] 宏时，必须定义包含 (`$dn`) 宏的目标。
- 可以将主题中的 (`$dn`) 宏 （但不是 [`$dn`]）与 (`$attr.`*attrName*) 宏合并。

匹配目标中的 ($dn)

ACI 的目标中的 (`$dn`) 宏通过与 LDAP 请求的目标条目相比较来确定替换值。例如，如果有目标为 `cn=all,ou=groups,dc=subdomain1, dc=hostedCompany1,dc=example,dc=com` 条目的 LDAP 请求，定义目标的 ACI 如下所示：

```
(target="ldap:///ou=Groups,($dn),dc=example,dc=com")
```

(`$dn`) 宏与 `"dc=subdomain1, dc=hostedCompany1"` 匹配。然后可以使用此子字符串用作 ACI 主题的替换值。

替换主题中的 ($dn)

在 ACI 主题中， (`$dn`) 宏被目标中匹配的全部子字符串所替换。例如：

```
groupdn="ldap:///cn=DomainAdmins,ou=Groups,($dn),dc=example,dc=com"
```

变为：

```
groupdn="ldap:///cn=DomainAdmins,ou=Groups,dc=subdomain1,
 dc=hostedCompany1,dc=example,dc=com"
```

宏扩展后， Directory Server 遵循正常的过程评估 ACI 以确定是否授予访问权。

注意 与标准 ACI 不同，使用宏替换的 ACI 不一定会授予对目标条目的子条目的访问权。原因是当子条目的 DN 是目标时，替换可能不会在主题字符串中创建一个有效 DN。

替换主题中的 [$dn]

`[$dn]` 的替换机制与 `($dn)` 的替换机制稍微有些不同。多次检查目标资源的 DN，每次都丢弃最左边的 RDN 组件，直到找到匹配为止。

例如，有目标为 `cn=all,ou=groups,dc=subdomain1,dc=hostedCompany1,dc=example,dc=com` 子树的 LDAP 请求，以及下列 ACI：

```
aci:(targetattr="*") (target="ldap:///ou=Groups,($dn),dc=example,
 dc=com") (version 3.0; acl "Domain access"; allow (read,search)
 groupdn="ldap:///cn=DomainAdmins,ou=Groups,[$dn],dc=example,dc=com
";)
```

服务器将按照以下步骤进行操作以扩展此 ACI：

1. 目标中的 `($dn)` 匹配 `dc=subdomain1,dc=hostedCompany1`。
2. 将主题中的 `[$dn]` 替换为 `dc=subdomain1,dc=hostedCompany1`。

   结果主题是 `groupdn="ldap:///cn=DomainAdmins,ou=Groups,dc=subdomain1,dc=hostedCompany1,dc=example,dc=com"`。如果由于绑定 DN 是该组的成员而被授予访问权，则宏扩展停止，并评估 ACI。如果不是成员，则该过程继续。
3. 将主题中的 `[$dn]` 替换为 `dc=hostedCompany1`。

   结果主题是 `groupdn="ldap:///cn=DomainAdmins,ou=Groups,dc=hostedCompany1,dc=example,dc=com"`。还要检测绑定 DN 是否为小组成员，如果是， ACI 将被完全评估。如果不是成员，宏扩展将在匹配值的最后一个 RDN 处停止并且此 ACI 的评估也将终止。

`[$dn]` 宏的优点在于它提供了一种灵活方式，可以向域级别的管理员授予对目录树中所有子域的访问权限。因此，对于表达域之间的层次型关系十分有用。

例如，请考虑下列 ACI：

```
aci:(target="ldap:///ou=*,($dn),dc=example,dc=com")
 (targetattr="*")(targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search) groupdn=
 "ldap:///cn=DomainAdmins,ou=Groups,[$dn],dc=example,dc=com";)
```

它授予 `cn=DomainAdmins,ou=Groups,dc=hostedCompany1,dc=example,dc=com` 的成员对 `dc=hostedCompany1` 下所有子域的访问权，因此属于该组的管理员可以访问子树 `ou=people,dc=subdomain1.1,dc=subdomain1`。

但同时， `cn=DomainAdmins,ou=Groups, dc=subdomain1.1` 的成员将被拒绝访问 `ou=people,dc=subdomain1, dc=hostedCompany1` 和 `ou=people,dc=hostedCompany1` 节点。

($attr.*attrName*) 的宏匹配

(`$attr.attrname`) 宏始终用在 DN 的主题部分。例如，可以定义下列 `roledn`：

```
roledn = "ldap:///cn=DomainAdmins,($attr.ou),dc=HostedCompany1,
dc=example,dc=com"
```

现在，假设服务器接收以下列条目为目标的 LDAP 操作：

```
dn:cn=Babs Jensen,ou=People,dc=HostedCompany1, dc=example,dc=com
cn:Babs Jensen
sn:Jensen
ou:Sales
...
```

为了评估 ACI 的 `roledn` 部分，服务器将读取存储在目标条目中的 `ou` 属性的值，并在主题中替换此值以扩展宏。在该示例中， `roledn` 按如下方式扩展：

```
roledn = "ldap:///cn=DomainAdmins,ou=Sales,dc=HostedCompany1,
dc=example,dc=com"
```

然后 Directory Server 根据正常的 ACI 评估算法对 ACI 进行评估。

当在宏中命名的属性是多值时，每个值都用于扩展宏，并使用提供成功匹配的第一个值。

访问控制和复制

ACI 是作为条目的属性存储的，因此，如果包含 ACI 的条目是已复制后缀的组成部分，则 ACI 会像任何其他属性那样被复制。

ACI 始终是在为传入 LDAP 请求提供服务的 Directory Server 上进行评估的。这意味着，当使用者服务器接收到更新请求时，它在评估之前返回的结果是引荐主服务器，而不管主服务器是否可以处理该请求。

记录访问控制信息

要获得错误日志中有关访问控制的信息，必须设置适当的日志等级。

要从控制台设置错误日志等级，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “目录”标签中，右键单击 `cn=config` 节点，然后从弹出菜单中选择 “用通用编辑器进行编辑”。

   显示的 “通用编辑器”中具有 `cn=config` 条目的内容。

2. 向下滚动属性值对的列表，找到 `nsslapd-errorlog-level` 属性。

3. 给 `nsslapd-errorlog-level` 字段中已显示的值加上 128。

   例如，如果显示的值是 8192 （复制调试），则应该将其更改为 8320。有关错误日志等级的完整信息，请参阅 *Sun ONE Directory Server 参考手册*。

4. 单击 “确定”保存更改，并关闭 “通用编辑器”。

与早期版本的兼容性

Directory Server 早期版本中使用的某些 ACI 关键字在 Sun ONE Directory Server 5.2 中已不再使用。但是，为了实现向后兼容性，这些关键字仍受支持。这些关键字包括：

- `userdnattr`
- `groupdnattr`

因此，如果在旧版供应商服务器和使用者 Directory Server 5.2 之间设置了复制协议，应该不会在复制 ACI 时遇到任何问题。

不过，我们建议您使用 `userattr` 关键字的功能替换这些关键字，如 “基于值匹配来定义访问”（第 181 页）中所述。

第 7 章

用户帐户管理

当用户连接到 Directory Server 时验证用户，同时目录可以根据验证过程中确定的身份授予用户访问权限和资源限制。

本章介绍用户帐户管理的任务，包括为目录配置口令和帐户锁定策略、去活帐户或用户组使其不能访问目录和根据用户的绑定 DN 限制用户可用的系统资源。

Directory Server 5.2 引入了单个口令策略。可以定义任意数量的不同口令策略，并将其中之一应用到给定用户或用户组。这样，可以很容易地控制不同类型的用户访问目录的方式。

本章包含以下小节：

- 口令策略概述
- 配置全局口令策略
- 管理单个口令策略
- 复位用户口令
- 去活和激活用户和角色
- 设置单个资源限制

口令策略概述

安全的口令策略通过强制执行以下策略将因容易猜测的口令引起的风险降到最低：

- 用户必须根据计划更改其口令。
- 用户必须提供有价值的口令。
- 因口令错误导致多次绑定后，帐户可能被锁定。

对于 Directory Server 5.2，可以同时具有单个口令策略和全局口令策略。单个口令策略是由目录树中的子条目定义的，具有该策略的用户条目即可引用此策略。如果用户条目不引用单个策略，则 `cn=PasswordPolicy,cn=config` 中的全局口令策略将应用到用户条目。

以下部分介绍如何执行口令策略并将其分配给用户和组。详细信息，请参阅 *Sun ONE Directory Server 部署指南* 中第 7 章中的 “设计口令策略”。

防止词典方式的攻击

在词典方式的攻击中，入侵者企图通过重复尝试猜测直到获得权限的方式来破解口令。此服务器提供三种工具来对抗这样的攻击：

- 口令语法检查将验证与用户条目的 `uid`、 `cn`、 `sn`、 `givenName`、 `ou` 或 `mail` 属性值不匹配的口令。如果口令与上述值之一相匹配，服务器将不允许用户设置口令。不过，语法检查并不制止实际的词典攻击，例如，入侵者尝试 `/usr/dict/words` 中的每个单词以进行攻击。
- 最小口令长度可以确保用户不能设置长度短的口令。口令的字符越长，猜测口令的难度就会相应呈指数级增加，乃至需要尝试所有的值。在 Directory Server 中，必须同时启用口令语法检查和最小口令长度。
- 帐户锁定机制可以防止一定次数的验证尝试失败后发生绑定。锁定可以是暂时，也可以是永久的，这取决于所指定的口令策略的严格程度。

  这两个策略均可以有效地防止自动猜测口令。例如，如果允许尝试五次，然后锁定用户帐户五分钟，则入侵者只能平均每分钟猜测一次，这样一个输入不熟练的入侵者将立刻感觉到非常困难。如果锁定是永久的，则用户口令必须由目录管理员手动复位。

复制环境中的口令策略

单个口令策略和全局口令策略都将被复制。因此，可以在主机上定义口令策略，并允许复制以将策略拓展到已复制的服务器上。设置的所有属性都是可复制的，作为包含口令历史 （已使用过的旧口令）和口令到期日期的操作属性。

不过，应该考虑复制环境中口令策略的以下影响：

- 口令即将到期的用户在更改其口令前，将收到来自于他们绑定的每个副本的警告消息。
- 当用户更改其口令时，可能需要一定时间以在所有的副本上更新此信息。如果用户更改口令并立即以新口令重新绑定到使用者副本之一，则在副本收到更新口令之前，此绑定可能会失败。
- 每个副本保存单独的、非复制的帐户锁定计数器。作为结果，将在任何单一副本上实施锁定策略，但可能在用户尝试绑定到多个副本时无法使用。例如，如果复制拓扑中有 10 台服务器，三次尝试后将激活锁定，则入侵者可能尝试 30 次口令猜测。

尽管复制确实允许入侵者进行多次猜测，但与数十亿的口令值相比，可猜测的次数是微不足道的。通过打开口令检查并将口令长度设置为六位字符或更多，以强制用户拥有强口令，而这一点更为重要。还应该为用户提供一些指导，介绍如何选择并记住非常见词典单词的口令。最后，应该确保所有目录系统管理员用户拥有非常强的口令。

配置全局口令策略

全局口令策略适用于目录中未定义单个策略的所有用户。不过，全局口令策略不适用于目录管理员。

使用控制台配置口令策略

要设置或修改 Directory Server 的全局口令策略，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中选择 “数据”节点，然后在右侧面板中选择 “口令”标签。
2. 在 “口令”标签上，设置策略的以下方面：

- 通过选中 “复位后用户必须更改口令”复选框，指定用户必须在首次登录时更改口令。

  如果选中此复选框，则只有目录管理员被授权复位用户的口令。常规管理用户不能强制用户更新其口令。

- 要允许用户更改自身的口令，请选中 “用户可更改口令”复选框。
- 要限制用户更改其口令的频率，请在 “允许 X 天内更改”文本框中输入天数。要允许用户可根据意愿对口令更改任意次，请选中 “没有限制”复选框。
- 要防止用户反复使用相同的口令，请选中 “保存口令的历史”复选框，并指定希望服务器为每个用户文本框保存的口令数。用户将不能设置列表中仍存在的口令。为了使此功能生效，还应限制用户更改其口令的频率。
- 如果不希望用户口令到期，请选择 “口令没有到期”单选按钮。
- 否则，请选择 “口令在 X 天后到期”单选按钮，以强制用户定期更改口令，然后输入用户口令的有效天数。
- 如果选择了要到期的口令，则可以在 “口令到期前 X 天发送警告”字段中指定口令到期前多久向用户发送警告。

  用户接到警告后，口令将在初始日期到期。取消选中 “无论警告与否都会到期”复选框，将在发送警告后，延长到期日期以允许一个完整的警告时间段。只能有一次警告和一次延长。如果用户在口令到期后绑定，则没有宽限登录。

- 如果希望服务器检查用户口令的语法，以确保口令满足口令策略设定的最低要求，请选中 “检查口令语法”复选框。然后，在 “口令最小长度”文本框中指定可接受的最小口令长度。
- 默认情况下，目录管理员不能复位违反口令策略的口令，例如重新使用历史中的口令。要允许目录管理员复位此类口令，请选中 “允许目录管理员避开口令策略”复选框。
- 从 “口令加密”下拉菜单中，指定希望服务器在存储口令时使用何种加密方法。

3. 单击 “帐户锁定”标签并选中 “帐户可能被锁定”复选框，以定义帐户锁定策略：

- 输入登录的失败次数以及必须登录以触发锁定的时间段。
- 选择 “永远锁定”单选按钮，以确保在目录管理员复位用户口令前永久性锁定口令。
- 否则，请选择 “锁定持续时间”单选按钮，然后输入用户帐户被暂时锁定的分钟数。

4. 完成对口令策略的更改后，单击 “保存”。将立即强制执行新的全局口令策略。

从命令行配置口令策略

全局口令策略是由 cn=Password Policy, cn=config 条目的属性定义的。使用 ldapmodify 公用程序可以在此条目中更改全局口令策略。

Sun ONE Directory Server 参考手册 中的第 4 章中的 “cn=Password Policy” 给出了口令策略中所有可能的属性的定义。

例如，口令语法检查和口令长度检查默认情况下处于关闭状态，帐户锁定处于禁用状态。使用以下命令可以打开语法检查、将口令最小长度设置为 8，并在 5 次错误口令尝试后启用五分钟临时锁定：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=Password Policy,cn=config
changetype:modify
replace:passwordCheckSyntax
passwordCheckSyntax:on
-
replace:passwordMinLength
passwordMinLength: 8
-
replace:passwordLockout
passwordLockout:on
-
replace:passwordMaxFailure
passwordMaxFailure: 5
-
replace:passwordLockoutDuration
passwordLockoutDuration: 300
-
replace:passwordUnlock
passwordUnlock:on
```

管理单个口令策略

单个口令策略是在具有 passwordPolicy 对象类的子条目中定义的。可以在 DN 形式为 cn=*policy name,subtree* 的目录树中的任意位置定义策略。使用 Directory Server 控制台或命令行公用程序定义口令策略后，可以通过在希望的用户条目中设置 passwordPolicySubentry 属性来分配口令策略。

本节中的示例是在 Example.com （其子树根为 dc=example,dc=com）为临时员工实施口令策略。

使用控制台定义策略

1. 在 Directory Server 控制台的顶级 “目录”标签中，显示要在其中定义单个口令策略子条目的条目。

2. 右键单击该条目并选择 “新建” > “口令策略”。或者，可以用左键单击此条目以选中它，并从 “对象”菜单中选择 “新建” > “口令策略”。

   显示 “口令策略”条目的自定义编辑器。

3. 在 “常规”字段中，输入此策略的名称和可选说明。此名称将成为定义策略的子条目的 cn 命名属性的值。

4. 单击 “口令”标签以设置策略的以下方面：

- 通过选中 “复位后用户必须更改口令”复选框，指定用户必须在首次登录时更改口令。

  如果选中此复选框，则只有 “目录管理员”被授权复位用户的口令。常规管理用户不能强制用户更新其口令。

- 要允许用户更改自身的口令，请选中 “用户可更改口令”复选框。

- 要限制用户的口令更改频率，请在 “允许 X 天内更改”文本框中输入天数。要允许用户可根据意愿对口令更改任意次，请选中 “没有限制”复选框。

- 要防止用户反复使用相同的口令，请选中 “保存口令历史”复选框，并指定希望服务器为每个用户文本框保存的口令数。用户将不能设置仍然在列表中的口令。为了使此功能生效，还应该限制用户的口令更改频率。

- 如果不希望用户口令到期，请选择 “口令没有到期”单选按钮。

- 否则，请选择 “口令在 X 天后到期”单选按钮，以强制用户定期更改口令，然后输入用户口令的有效天数。

- 如果选择了要到期的口令，则可以指定在口令到期前多久向用户发送警告。在 “口令到期前 X 天发送警告”文本框中输入口令到期前发送警告的天数。

  用户接到警告后，口令将在初始日期到期。取消选中 “无论警告与否都会到期”复选框，将在发送警告后，延长到期日期以允许一个完整的警告时间段。只能有一次警告和一次延长。如果用户在口令到期后绑定，则没有宽限登录。

- 如果希望服务器检查用户口令的语法，以确保口令满足口令策略设定的最低要求，请选中 “检查口令语法”复选框。然后，在 “口令最小长度”文本框中指定可接受的最小口令长度。

- 默认情况下，目录管理员不能复位违反口令策略的口令，例如重新使用历史中的口令。要允许目录管理员复位此类口令，请选中 “允许目录管理员避开口令策略”复选框。

- 从 “口令加密”下拉菜单中指定希望服务器在存储口令时使用何种加密方法。

5. 单击 “锁定”标签并选中 “帐户可能被锁定”复选框，以定义帐户锁定策略：

- 输入登录的失败次数以及必须登录以触发锁定的时间段。
- 选择 “永远锁定”单选按钮，以确保在目录管理员复位用户口令前永久性锁定口令。
- 否则，请选择 “锁定持续时间”单选按钮，然后输入用户帐户被暂时锁定的分钟数。

6. 在自定义编辑器中单击 “确定”，以保存策略并创建其子条目。

从命令行定义策略

对于此口令策略，设想您希望临时员工口令在 100 天 （8 640 000 秒）后到期，并在口令到期前 3 天 （259 200 秒）开始对绑定的用户返回到期警告。打开语法检查以强制对口令安全性执行基本检查，并强制执行锁定以阻止入侵者通过词典攻击破解口令。策略的其他方面应用默认值。

通过添加 `dc=example,dc=com` 下的以下子条目，在 Example.com 子树中定义此口令策略：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=TempPolicy,dc=example,dc=com
objectClass:top
objectClass:passwordPolicy
objectClass:LDAPsubentry
cn:TempPolicy
passwordStorageScheme:SSHA
passwordChange:on
passwordMustChange:on
passwordCheckSyntax:on
passwordExp:on
passwordExp:on
passwordMinLength: 6
passwordMaxAge: 8640000
passwordMinAge: 0
passwordWarning: 259200
passwordInHistory: 6
passwordLockout:on
passwordMaxFailure: 3
passwordUnlock:on
passwordLockoutDuration: 3600
passwordResetFailureCount: 600
```

Sun ONE Directory Server 参考手册 中的第 4 章 “cn=Password Policy”给出了口令策略中所有可能的属性的定义。

分配口令策略

分配单个口令策略由指向相应的策略子条目组成。将策略作为 `passwordPolicySubentry` 的值添加到单个条目，或者使用 CoS 和角色管理策略。还必须设置访问控制以防止用户修改应用于他们的口令策略。

使用控制台

Directory Server 控制台提供一个界面，用于管理分配给用户或组的口令策略：

1. 在 Directory Server 控制台的顶级 “目录”标签上，显示要在其中分配或修改单个口令策略的用户条目或组条目。
2. 右键单击该条目并从弹出菜单中选择 “设置口令策略”。或者，可以用左键单击此条目以选中它，并从 “对象”菜单中选择 “设置口令策略”。
3. “口令策略”对话框将告知应用于此条目的口令策略：

- 如果全局口令策略适用，请单击 “分配”以在目录树中的任意位置选择一个口令策略子条目。
- 如果已经定义了单个策略，则可以替换、删除或编辑此单个策略。单击 “编辑策略”将调用已命名的策略子条目的自定义编辑器。

  分配或替换口令策略将调用目录浏览器对话框，在此您可能会看到一个以小密钥图标显示的口令策略子条目。

4. 如果更改了此策略，请在 “口令策略”对话框中单击 “确定”。新策略将立即生效。

从命令行

要为用户条目或组条目分配口令策略，请将口令策略的 DN 作为 `passwordPolicySubentry` 属性的值添加。例如，以下命令将为 Barbara Jensen 分配 `cn=TempPolicy,dc=example,dc=com`：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
add:passwordPolicySubentry
passwordPolicySubentry:cn=TempPolicy,dc=example,dc=com
```

使用角色和 CoS

按角色对用户分组时，可以使用 CoS 指向相应的策略子条目。有关使用角色和 CoS 的详细信息，请参阅第 5 章 “高级条目管理”。

下面的示例中，以下命令将在 Example.com 为临时员工创建一个已筛选角色，并为那些具有此角色的员工分配 cn=TempPolicy,dc=example,dc=com：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=TempFilter,ou=people,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:nsRoleDefinition
objectclass:nsComplexRoleDefinition
objectclass:nsFilteredRoleDefinition
cn:TempFilter
nsRoleFilter:(&(objectclass=person)(status=contractor))
description:filtered role for temporary employees

dn:cn=PolTempl,dc=example,dc=com
objectclass:top
objectclass:nsContainer

dn:cn="cn=TempFilter,ou=people,dc=example,dc=com",
 cn=PolTempl,dc=example,dc=com
objectclass:top
objectclass:extensibleObject
objectclass:LDAPsubentry
objectclass:costemplate
cosPriority: 1
passwordPolicySubentry:cn=TempPolicy,dc=example,dc=com

dn:cn=PolCoS,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
objectclass:cosClassicDefinition
cosTemplateDN:cn=PolTempl,dc=example,dc=com
cosSpecifier:nsRole
cosAttribute:passwordPolicySubentry operational
```

具有合同工状态的用户现在将服从口令策略 cn=TempPolicy,dc=example,dc=com。

保护单个口令策略

要防止用户修改应用于他们的口令策略，还必须向根条目添加 ACI，例如：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:dc=example,dc=com
changetype:modify
add:aci
aci:(targetattr != "passwordPolicySubentry")(version 3.0; acl
 "Allow self entry modification except for passwordPolicySubentry";
 allow (write) (userdn ="ldap:///self");)
```

复位用户口令

目录在用户条目的 userPassword 属性中存储口令值。根据服务器的访问控制设置，用户可以使用诸如 ldapmodify 的标准工具将 userPassword 的值设为与指定的口令策略一致。

万一发生永久帐户锁定 （在口令策略中，用户操作属性 accountUnlockTime 为 0，且 passwordUnlock 为 off），可以目录管理员的身份复位口令以解除用户帐户锁定。例如，假设 Example.com 目录用户 Barbara Jensen 在忘记并猜测其口令后被永久性锁定：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
replace:userPassword
userPassword:ChAnGeMe
```

如果在口令策略中 passwordMustChange 已开启，则 Barbara 必须在下次绑定后更改口令。请记住告诉她您已将其口令更改为 ChAnGeMe，最好通过安全的方式。

去活和激活用户和角色

可暂时去活单个用户帐户或一组帐户。去活后，用户无法绑定到目录。验证操作将失败。

本节中的步骤可用于以相同方式去活用户和角色。但是，去活角色时，去活的是 role 中的成员，而非角色条目本身。有关一般角色，以及角色如何与特定访问控制进行交互作用的详细信息，请参阅第 5 章 “高级条目管理”。

使用控制台设置用户和角色激活

1. 在 Directory Server 控制台的顶级 “目录”标签上，浏览目录树以显示要去活或重新激活的用户条目或角色条目。
2. 双击条目以显示其自定义编辑器，在左侧列中单击 “帐户”标签。

   右侧面板将显示条目的激活状态。
3. 单击该按钮以去活或激活与此条目对应的用户或角色。贯穿编辑器中用户图标或角色图标的红色框和条表明此条目将被去活。
4. 单击 “确定”关闭对话框，并保存该条目新的激活状态。

   还可以选择此条目并从 “对象”菜单中选择 “去活”或 “激活”，这是一种打开自定义编辑器的快捷方式。

通过从 “控制台视图” > “显示”菜单中选择 “去活状态”，可以查看任意目录对象的激活状态。随后，所有去活条目的图标将显示为有一个红条贯穿其中。不论是直接去活条目还是通过角色成员身份去活条目，都将显示用户条目的正确激活状态。

从命令行设置用户和角色激活

要去活用户帐户或角色成员，请使用 `ns-inactivate.pl` 脚本 （Solaris 软件包中为 `directoryserver account-inactivate`）。要激活或重新激活用户或角色，请使用 `ns-activate.pl` 脚本 （Solaris 软件包中为 `directoryserver account-inactivate`）。这些脚本的命令依平台而定：

Solaris 软件包

```
# /usr/sbin/directoryserver account-inactivate
# /usr/sbin/directoryserver account-activate
```

Windows 平台

```
cd ServerRoot
bin\slapd\admin\bin\perl slapd-serverID\ns-inactivate.pl
bin\slapd\admin\bin\perl slapd-serverID\ns-activate.pl
```

其他安装

```
# ServerRoot/slapd-serverID/ns-inactivate.pl
# ServerRoot/slapd-serverID/ns-activate.pl
```

以下命令显示如何使用 perl 脚本来去活和重新激活 Barbara Jensen 的用户帐户：

```
ns-inactivate.pl -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令\
                 -I "uid=bjensen,ou=People,dc=example,dc=com"
ns-activate.pl -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令\
               -I "uid=bjensen,ou=People,dc=example,dc=com"
```

在这两个命令中， -I 选项指定要为其设置激活状态的用户或角色的 DN。

详细信息，请参阅 *Sun ONE Directory Server 参考手册* 的第 2 章中的“ns-inactivate.pl”和“ns-activate.pl”。

设置单个资源限制

可使用绑定到目录的客户机应用程序上特定操作属性值，控制搜索操作的服务器限制。可设置以下搜索操作限制：

- 此浏览限制指定搜索操作将检查的最大条目数。
- 大小限制指定服务器响应搜索操作返回到客户机应用程序的最大条目数。
- 时间限制指定服务器处理搜索操作所花费的最长时间。
- 空闲超时指定在服务器放弃连接之前到服务器的客户机连接可以空闲的时间。

注意 默认情况下，目录管理员可以使用无限的资源。

为特定用户设置的资源限制优先于在全局服务器配置中设置的默认资源限制。应该验证存储单个资源限制的属性是否受到后缀（包含用户条目）上的下列 ACI 的保护，以防止其进行自我修改：

```
(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";)
```

使用控制台设置资源限制

1. 在 Directory Server 控制台的顶级 “目录”标签上，浏览目录树以显示要为其设置资源限制的用户。
2. 双击此条目以显示自定义编辑器，在左侧列中单击 “帐户”标签。右侧面板将显示此条目的当前限制。
3. 在上述资源限制的四个文本字段中输入值。如果输入的值 -1，则表示对该资源没有限制。
4. 完成后单击 “确定”以保存新限制。

从命令行设置资源限制

可以使用 `ldapmodify` 命令在用户条目中设置以下属性，以限制用户的资源使用：

属性	说明
`nsLookThroughLimit`	指定搜索操作检查到的条目数。指定为条目的数量。指定该属性值为 -1 表示无限制。
`nsSizeLimit`	指定服务器响应搜索操作返回到客户机应用程序的最大条目数。指定该属性值为 -1 表示无限制。
`nsTimeLimit`	指定服务器处理搜索操作所花费的最长时间。指定属性值为 `-1` 表示无时间限制。
`nsIdleTimeout`	指定服务器在放弃连接之前，与服务器的连接可以为空闲的时间。以秒为单位给出值。指定该属性值为 -1 表示无限制。

例如，可通过如下所述执行 `ldapmodify` 来设置条目的大小限制：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
add:nsSizeLimit
nsSizeLimit: 500
```

`ldapmodify` 语句将 `nsSizeLimit` 属性添加到 Barbara Jensen 的条目中，并给出其搜索返回大小限制为 500 个条目。

第 8 章

管理复制

复制是一种机制，通过这种机制可以将目录内容自动从一个 Directory Server 复制到另一个或多个服务器。任何类型的写操作 - 条目添加、修改乃至删除 - 都可以自动镜像到其他 Directory Server。有关复制概念、复制方案以及如何在目录部署中计划复制的完整说明，请参阅 *Sun ONE Directory Server 部署指南* 中的第 6 章 “设计复制过程”。

Sun ONE Directory Server 5.2 介绍了许多新的复制功能：

- 通过广域网 (WAN) 进行的多主复制 (MMR) 允许您在两个地理位置相距较远的主副本之间创建复制协议，以便更有效地分配数据。
- 目前 MMR 支持四个同时全部互连的、可以提供额外故障保护的主副本。
- 二进制复制可以使大量复制的初始化更加迅速。
- 分式复制允许您指定要复制的属性集，以便更快地分配数据。
- 新命令行工具可以帮助您监控复制部署。

本章介绍可以在主副本、集线器副本和使用者服务器中执行的用以设置所有复制方案类型的任务。本章包括以下主题：

- 简介
- 配置复制的步骤摘要
- 选择复制管理员
- 配置专门的客户
- 配置集线器
- 配置主副本
- 创建复制协议
- 配置分式复制

- 初始化副本
- 启用引荐完整性插件
- 通过 SSL 复制
- 通过 WAN 复制
- 修改复制拓扑
- 使用早期版本进行复制
- 使用 Retro Change Log 插件
- 监控复制状态
- 解决常见复制冲突

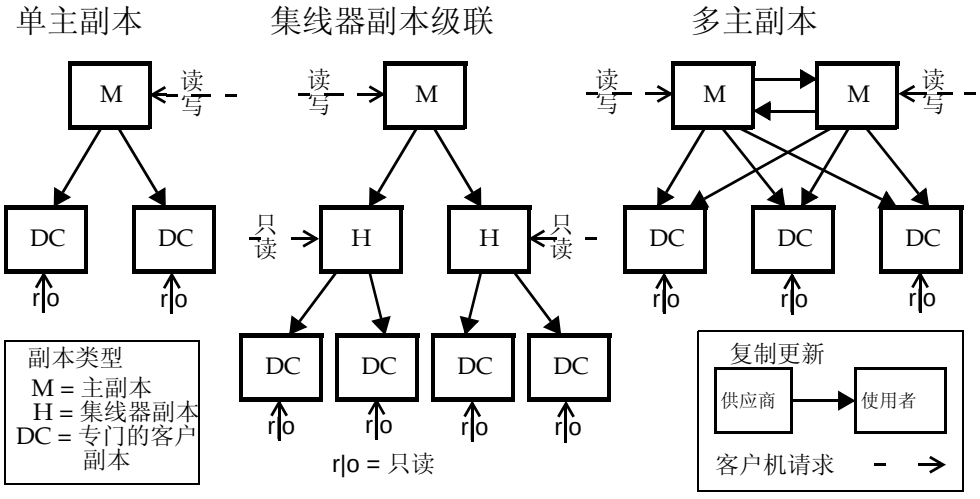
简介

配置复制是比较复杂的任务。开始之前，您应该清楚地了解组织中复制的部署方式，如使用的是单主复制、多主复制还是利用集线器的级联复制。复制单位为后缀或子后缀：将同时复制该后缀的所有条目。在要进行的部署中，必须标识它所包含数据的每个后缀 （主机、集线器或专门的客户）。

服务器中的已复制后缀称为副本。主副本是既能接受客户机读取操作也能接受其写入操作的副本。集线器副本和专门的客户副本是只能通过复制机制接收更新的只读副本。集线器副本可以从主副本或另一集线器副本接收更新，并将其转发给其他集线器或专门的客户。专门的客户只能从主副本或集线器副本接收更新。

下图显示了通用复制方案中副本之间的关系。

图 8-1 通用复制方案



本文档还使用术语供应商和使用者，指的是参与复制协议的两种服务器角色。供应商是发送复制更新的服务器，使用者是接收这些更新的服务器。上图说明了以下关系：

- 单主副本是供应商，不是使用者。
- 多主复制中的主机既是其他主机的供应商也是使用者。
- 集线器始终是供应商和使用者。
- 专门的客户只能是使用者。

许多复制设置都适用于协议的供应商角色或使用者角色中的副本，与复制类型无关。

配置复制的步骤摘要

以下步骤假设您正在复制单个后缀。如果要复制多个后缀，您可以在各个服务器中对其进行并行配置。也就是说，可以重复每一步以配置多个后缀的复制。

要配置任意复制拓扑，应该按以下顺序操作：

1. 在所有服务器中定义复制管理员条目 （单主副本除外）。或者确定在所有服务器中使用默认复制管理员即可。
2. 在包含专门的客户的所有服务器上：

a. 为使用者副本创建一个空后缀。

b. 通过复制向导启用此后缀的使用者副本。

c. 配置高级副本设置 （可选）。

3. 在包含集线器副本的所有服务器上 （如果适用）：

a. 为集线器副本创建一个空后缀。

b. 通过复制向导启用此后缀的集线器副本。

c. 配置高级副本设置 （可选）。

4. 在包含主副本的所有服务器上：

a. 为要成为主副本的副本选择或创建一个后缀。

b. 通过复制向导启用此后缀的主副本。

c. 配置高级副本设置 （可选）。

5. 按照以下顺序配置所有供应商副本上的复制协议：

a. 多主集合中的主副本之间的协议。

b. 主副本及其专门的客户之间的协议。

c. 主副本和集线器副本之间的协议。

在该阶段，可以配置分式复制以及初始化使用者副本和集线器副本 （可选）。如果是多主复制，从包含数据原副本的同一主副本中初始化所有的主副本。

6. 配置所有由主副本直接供给的集线器副本复制协议。这些协议是集线器副本及其使用者副本之间的协议。在该阶段，可以初始化使用者副本 （可选）。在级联复制中为每个级别的集线器副本重复这一步骤。

注意 在尝试创建复制协议前创建和配置所有副本，这一点非常重要。这样，您还可以在创建复制协议后立即初始化使用者副本。使用者初始化始终是设置复制过程中的最后一个阶段。

选择复制管理员

设置复制的一个关键部分是选择条目，也称为复制管理员，发送复制更新时供应商将使用复制管理员以绑定到使用者服务器。所有包含接收更新后缀 （包括专门的客户、集线器和参与多主复制的主机）的服务器都必须至少有一个复制管理员条目。

Directory Server 有一个可能会在每台服务器中使用的默认复制管理员条目。其 DN 是 cn=Replication Manager,cn=replication,cn=config。

注意 建议您在所有简单复制方案中使用默认复制管理员。复制向导自动使用此条目配置使用者副本，从而简化副本部署。

如果未定义默认复制管理员口令，此复制向导将提示您设置此口令。如果以后要更改默认复制管理员口令，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中选择 “数据”节点，然后在右侧面板中选择 “复制”标签。
2. 在 “复制管理员”标题下的两个文本字段中均输入新的口令。
3. 确认口令后，单击 “保存”。如果口令与确认口令不一致，则 “保存”按钮不活动。

如果已经保存，您就可以创建任意的复制管理员新条目。例如，您可能想让每个已复制后缀都有一个不同的口令，从而有多个复制管理员条目。创建个人复制管理员的另一个原因是为了支持复制的不同验证模式，例如通过 SSL 使用证书。

复制管理员条目必须包含定义复制协议时选择的验证方法所要求的属性。例如，默认复制管理员是 person 对象类，它允许使用 userPassword 属性进行简单验证。有关使用证书以绑定复制管理员的详细信息，请参阅 “通过 SSL 复制”（第 264 页）。

此复制管理员的条目不应该位于使用者服务器的已复制后缀中。定义复制管理员的合适位置是 cn=replication,cn=config。

警告 您一定不要使用复制管理员条目的 DN 和口令在服务器上绑定或执行操作。复制管理员仅供复制机制使用，任何其他使用可能都需要重新初始化副本。

为每个使用者选择了复制管理员后，请执行以下操作：

1. 写下或牢记您所选择或创建的复制管理员 DN。以后如果在供应商中创建与其使用者之间的复制协议时，需要此 DN 和口令。
2. 如果要定义口令过期策略，请注意不要包括复制管理员，否则将导致口令到期后复制失败。要在复制管理员条目上禁用口令到期，请创建一个其口令不会到期的口令策略，然后将此策略分配给复制管理员条目。详细信息，请参阅 “管理单个口令策略”（第 229 页）。

配置专门的客户

专门的客户是已复制后缀的只读副本。它可以接收来自以特殊 “复制管理员”身份绑定的主服务器的更新，以进行更改。配置使用者服务器由两个步骤组成，首先准备用来存放副本的空后缀，然后使用复制向导在该后缀上启用复制。可选的高级配置包括选择其他复制管理员、设置引荐或者设置清理延迟。

以下小节给出了在专门的客户服务器中配置专门的客户的步骤。请在包含给定后缀的专门的客户的每台服务器中重复所有步骤。

创建使用者副本的后缀

如果不存在此后缀，请采用与要使用的主副本相同的 DN 在使用者副本上创建一个空后缀。有关说明，请参阅 “创建后缀”（第 79 页）。

如果存在不为空的后缀，则从主副本中初始化副本时后缀内容将丢失。

启用使用者副本

复制向导可以简化启用专门的客户的过程：

1. 在 Directory Server 控制台的顶级 “配置”标签中，展开 “数据”节点和要作为使用者副本后缀的节点，然后在此后缀下选择 “复制”节点。

   副本状态信息将显示在右侧面板中。

2. 单击 “启用复制”按钮启动复制向导。
3. 默认情况下，“使用者副本”单选按钮处于选中状态。单击 “下一步”以继续。
4. 如果未执行上述步骤，系统将提示您输入并确认默认复制管理员口令。在每个字段中键入同一口令，然后单击 “下一步”以继续。

   如果默认复制管理员已经有一个已定义口令，则向导将跳过这一步。

5. 更新复制配置时，复制向导将显示状态消息。完成后单击 “关闭”。

现在，复制状态会显示副本已准备好接收更新，左侧窗格中的图标会发生变化来反映这种情况。

高级使用者配置

默认情况下，向导将副本配置为使用默认复制管理员。如果已经创建另一个希望使用的复制管理员条目，则需要设置高级配置。还可以使用此对话框设置修改和清理延迟的引荐。

1. 在 Directory Server 控制台的顶级 “配置”标签中，展开 “数据”节点和要配置后缀的节点，然后在此后缀下选择 “复制”节点。
2. 在右侧面板中，单击 “高级”按钮以显示 “高级副本设置”对话框。
3. 在 “绑定 DN”标签中，使用 “添加”和 “删除”按钮来创建一个有效复制管理员的 DN 列表。这样，供应商就可以在与副本间的协议中使用上述任意的 DN。可以通过输入 DN 名称或浏览目录来添加新的 DN。

   要配置通过 SSL 使用证书进行的复制，请以上述其中一个复制管理员身份输入证书条目的 DN。
4. 完成后单击 “确定”，或者选择 “可选”标签进行高级配置。
5. 在 “高级副本设置”对话框的 “可选”标签中， LDAP URL 列表指定了发送至该使用者的修改请求的其他引荐。使用 “添加”或 “删除”按钮创建 LDAP URL 列表。

   此复制机制自动配置使用者，以在复制拓扑中为所有已知主副本返回引荐。这些默认引荐假设客户机通过常规连接使用简单验证。如果要使客户机可以选择使用 SSL 绑定至主副本来实现安全连接，请以 `ldaps://`*servername*`:`*port* 的形式添加引荐 （其中端口号使用的是安全端口号）。

   如果已将一个或多个 LDAP URL 添加为引荐，选中表下面的复选框将会强制使用者仅发送引荐至这些 LDAP URL，而不会发送至主副本。例如，如果希望客户机始终被引荐至主服务器中的安全端口，而不是默认端口，请为这些安全端口创建一个 LDAP URL 列表并选中此复选框。如果希望指定用来处理所有更新的特定主副本或 Directory Server 代理，您也可以使用独占引荐。
6. 还可以在 “可选”标签中更改清理延迟。

   使用者服务器必须存储有关副本内容更新的内部信息，清理延迟参数指定了这些服务器必须保留这些信息多久。这与其供应商服务器上更改日志的 MaxAge 参数有关。这两个参数的较短者决定了这两台服务器间的复制被禁用或关闭多久后，仍可正常恢复复制的时间。大多数情况下， 7 天的默认值已经足够。
7. 单击 “确定”保存此副本的高级复制配置。

配置集线器

集线器副本既可作为使用者副本也可作为主副本，以进一步将已复制数据分配至更多的使用者副本。它们必须既能从供应商接收更新，又能将复制更新发送给其使用者副本。集线器副本不接受修改，但可以将引荐返回到主副本。

配置集线器服务器由两个步骤组成，首先准备用来存放副本的空后缀，然后使用复制向导在该后缀中启用复制。可选的高级配置包括选择其他复制管理员、设置引荐、设置清理延迟以及设置更改日志参数。

以下小节给出了配置集线器服务器的步骤。请在包含给定后缀的集线器副本的每台服务器上重复所有步骤。

创建集线器副本的后缀

如果不存在此后缀，请采用与要使用的主副本相同的 DN 在集线器服务器中创建一个空后缀。有关说明，请参阅 “创建后缀”（第 79 页）。

如果存在不为空的后缀，则从主副本中初始化副本时后缀内容将丢失。

启用集线器副本

复制向导可以简化启用集线器副本的过程：

1. 在 Directory Server 控制台的顶级 “配置”标签中，展开 “数据”节点和要作为集线器副本的后缀的节点，然后在此后缀下选择 “复制”节点。

   副本状态信息将显示在右侧面板中。

2. 单击 “启用复制”按钮启动复制向导。

3. 选择 “集线器副本”单选按钮，然后单击 “下一步”以继续。

4. 如果未执行上述步骤，系统将提示您选择更改日志文件。默认更改日志文件显示在文本字段中。如果不希望使用默认值，请输入更改日志的文件名，或者单击 “浏览”显示一个文件选择器。

   如果已经启用更改日志，则向导将跳过此步骤。

5. 单击 “下一步”。如果未执行上述步骤，系统将提示您输入并确认默认复制管理员口令。在每个字段中键入同一口令，然后单击 “下一步”以继续。

   如果默认复制管理员已经有一个已定义口令，则向导将跳过这一步。

6. 更新复制配置时，复制向导将显示状态消息。完成后单击 “关闭”。

现在，复制状态会显示副本已准备好接收更新，左侧窗格中的图标会发生变化来反映这种情况。

高级集线器配置

作为供应商，集线器服务器需要一个更改日志，向导会将集线器副本配置为使用默认更改日志设置。要修改这些设置，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中选择 “数据”节点，然后在右侧面板中选择 “复制”标签。
2. 您可能需要刷新此标签的内容，方法为选中 “启用更改日志”复选框并单击 “复位”按钮。然后在复制向导中，您将会看到选择的更改日志文件。
3. 可以更改此更改日志文件的名称，以及更新更改日志参数：
   a. 最大的更改日志记录 - 决定了可以存储的总修改量，以向使用者发送更新。默认情况下此值是无限制的。如果对副本进行了大量的改动，则您可能希望限制记录的数目以节省磁盘空间。
   b. 最大的更改日志存留期 - 决定了发送至使用者的更新在集线器中存储的时间。默认情况下此值是无限制的。推荐使用此参数来限制更改日志的大小。

同样，复制向导使用的也是默认复制管理员。如果已经创建另一个希望使用的复制管理员条目，则需要设置高级配置。还可以使用此对话框设置修改和清理延迟的引荐。

1. 在 Directory Server 控制台的顶级 “配置”标签中，展开 “数据”节点和要配置后缀的节点，然后在此后缀下选择 “复制”节点。
2. 在右侧面板中，单击 “高级”按钮以显示 “高级副本设置”对话框。
3. 在 “绑定 DN”标签中，使用 “添加”和 “删除”按钮来创建一个有效复制管理员的 DN 列表。这样，供应商就可以在与副本间的协议中使用上述任意 DN。可以通过输入 DN 名称或浏览目录来添加新的 DN。

   要配置通过 SSL 使用证书进行的复制，请以上述其中一个复制管理员身份输入证书条目的 DN。
4. 完成后单击 “确定”，或者选择 “可选”标签进行高级配置。

5. 在 “高级副本设置”对话框的 “可选”标签中， LDAP URL 列表指定了发送至此集线器的修改请求的其他引荐。使用 “添加”或 “删除”按钮创建 LDAP URL 列表。

   此复制机制自动配置集线器，以在复制拓扑中为所有已知主副本返回引荐。这些默认引荐假设客户机通过常规连接使用简单验证。如果要使客户机可以选择使用 SSL 绑定至主副本来实现安全连接，请以 `ldaps://`*servername*`:`*port* 的形式添加引荐 （其中端口号使用的是安全端口号）。

   如果已将一个或多个 LDAP URL 添加为引荐，选中表下面的复选框将会强制服务器仅发送引荐至这些 LDAP URL，而不会发送至主副本。例如，如果希望客户机始终被引荐至主服务器中的安全端口，而不是默认端口，请为这些安全端口创建一个 LDAP URL 列表并选中此复选框。如果希望指定用来处理所有更新的特定主副本或 Directory Server 代理，您也可以使用独占引荐。

6. 还可以在 “可选”标签中更改清理延迟。

   集线器服务器必须存储副本内容更新的内部信息，清理延迟参数指定了这些服务器必须保存这些信息多久。这与提供更新的服务器中更改日志的 MaxAge 参数有关 （不是其本身更改日志的 MaxAge 参数）。这两个参数的较短者决定了这两台服务器间的复制被禁用或关闭多久后，仍可正常恢复复制的时间。大多数情况下， 7 天的默认值已经足够。

7. 单击 “确定”保存此副本的高级复制配置。

配置主副本

主副本包含数据的主副本，并在向其他所有副本发送更新前集中所有的修改。主副本记录所有的更改、检查其使用者的状态并在必要时向使用者发送更新。在多主复制中，一个主副本还会接收到来自其他主副本的更新。

配置主服务器包括以下步骤：定义包含主副本的后缀、使用复制向导启用主副本以及在必要时配置高级复制。

以下小节给出了配置主服务器的步骤。请在包含给定后缀的主副本的每台服务器中重复所有步骤。

定义主副本的后缀

在包含要复制条目的主副本服务器中选择或创建一个后缀。有关说明，请参阅 “创建后缀”（第 79 页）。

创建复制协议前，此后缀应该包含所有初始数据。这样，您可以立即初始化此数据的使用者副本。要确保正确的主副本配置操作和初始化，只能有一个主副本包含所有的初始数据，其他主副本中的后缀应该为空。

启用主副本

复制向导可以简化启用主副本的过程：

1. 在 Directory Server 控制台的顶级 “配置”标签中，展开 “数据”节点和要作为主副本后缀的节点，然后在此后缀下选择 “复制”节点。

   副本状态信息将显示在右侧面板中。

2. 单击 “启用复制”按钮启动复制向导。

3. 选中 “主副本”单选按钮，然后单击 “下一步”以继续。

4. 输入一个 “副本 ID”：选择 1 到 65534 之间的一个整数 （包括 1 和 65534）。

   对于给定后缀，所有主副本的 “副本 ID”都必须是唯一的。同一服务器中不同后缀的主副本可以使用相同的 “副本 ID”，只要它在每个副本的其他主副本中是唯一的。

5. 单击 “下一步”。如果未执行上述步骤，系统将提示您选择更改日志文件。默认更改日志文件显示在文本字段中。如果不希望使用默认值，请输入更改日志的文件名，或者单击 “浏览”显示一个文件选择器。

   如果已经启用更改日志，则向导将跳过此步骤。

6. 单击 “下一步”。如果未执行上述步骤，系统将提示您输入并确认默认复制管理员口令。如果是单主复制，则无需使用复制管理员，但仍然需要输入一个口令以继续操作。在每个字段中键入同一口令，然后单击 “下一步”以继续。

   如果默认复制管理员已经有一个已定义口令，则向导将跳过这一步。

7. 更新复制配置时，复制向导将显示状态消息。完成后单击 “关闭”。

现在复制状态将显示此主副本的 “副本 ID”，左侧窗格中的图标将发生变化，以此反映此后缀的复制是活动的。

高级多主复制配置

默认情况下，向导将主副本配置为使用默认更改日志设置。要修改更改日志设置，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中选择 “数据”节点，然后在右侧面板中选择 “复制”标签。
2. 您可能需要刷新此标签的内容，方法为选中 “启用更改日志”复选框并单击 “复位”按钮。然后在复制向导中，您将会看到选择的更改日志文件。
3. 可以更改此更改日志文件的名称，以及更新更改日志参数：
   a. 最大的更改日志记录 - 决定了可以存储的总修改量，以向使用者发送更新。默认情况下此值是无限制的。如果对副本进行了大量的改动，则您可能希望限制记录的数目以节省磁盘空间。
   b. 最大的更改日志存留期 - 决定了发送至使用者的更新在集线器中存储的时间。默认情况下此值是无限制的。推荐使用此参数来限制更改日志大小。

同样，复制向导使用的也是默认复制管理员。如果已经创建另一个希望使用的复制管理员条目，则需要设置高级配置。还可以使用此对话框设置修改和清理延迟的引荐。如果配置的是单主副本，您可以跳过此过程。

1. 在 Directory Server 控制台的顶级 “配置”标签中，展开 “数据”节点和要配置后缀的节点，然后在此后缀下选择 “复制”节点。
2. 在右侧面板中，单击 “高级”按钮以显示 “高级副本设置”对话框。
3. 在 “绑定 DN”标签中，使用 “添加”和 “删除”按钮来创建一个有效复制管理员的 DN 列表。这样，供应商就可以在与副本间的协议中使用上述任意 DN。可以通过输入 DN 名称或浏览目录来添加新的 DN。

   要配置通过 SSL 使用证书进行的复制，请以上述其中一个复制管理员身份输入证书条目的 DN。
4. 完成后单击 “确定”，或者选择 “可选”标签进行高级配置。
5. 在 “高级副本设置”对话框的 “可选”标签中， LDAP URL 列表指定了发送至此主副本的修改请求的其他引荐。初始化后，主副本将立即自动返回引荐，如 “多主副本初始化后会聚”（第 256 页）中所述。使用 “添加”或 “删除”按钮创建 LDAP URL 列表。

   此复制机制自动配置集线器，以为复制拓扑中所有已知主副本返回引荐。这些默认引荐假设客户机通过常规连接使用简单验证。如果要使客户机可以选择使用 SSL 绑定至主副本来实现安全连接，请以 `ldaps://`*servername*`:`*port* 的形式添加引荐 （其中端口号使用的是安全端口号）。

   如果已将一个或多个 LDAP URL 添加为引荐，选中表下面的复选框将会强制服务器仅发送引荐至这些 LDAP URL，而不会发送至主副本。例如，如果希望客户机始终被引荐至主服务器中的安全端口，而不是默认端口，请为这些安全端口创建一个 LDAP URL 列表并选中此复选框。

6. 还可以在 “可选”标签中更改清理延迟。

   主副本服务器必须存储副本内容更新的内部信息，清理延迟参数指定了这些服务器必须保存这些信息多长时间。这与提供更新的主副本服务器中更改日志的 MaxAge 参数有关 （不是其本身更改日志的 MaxAge 参数）。这两个参数的较短者决定了这两台服务器间的复制被禁用或关闭多久后，仍可正常恢复复制的时间。大多数情况下， 7 天的默认值已经足够。

7. 单击 “确定”保存此副本的高级复制配置。

创建复制协议

复制协议是与供应商有关的一组参数，它配置和控制发送更新至给定使用者的方式。必须在发送更新至其使用者的供应商副本中创建复制协议。必须为要更新的每个使用者创建复制协议。

按以下顺序创建复制协议：

1. 多主副本集的主副本之间的协议，从包含要复制后缀原副本的主副本开始复制。
2. 主副本和不是通过集线器副本复制的专门的客户之间的协议。
3. 主副本和集线器副本之间的协议。
4. 集线器副本及其客户之间的协议。

例如，图 8-1 （第 241 页）所示的具有 2 个主副本和 3 个专门的客户副本的多主复制拓扑中，应该按以下顺序创建八个复制协议：

- 一个主副本和其他主副本之间的协议。
- 其他主副本和第一个主副本之间的协议。
- 一个主副本和 3 个专门的客户副本中每个副本之间的协议。
- 另一个主副本和 3 个专门的客户副本中每个副本之间的协议。

要创建复制协议，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中，展开 “数据”节点和供应商后缀的节点，然后在此后缀下选择 “复制”节点。

   副本状态信息将显示在右侧面板中。

2. 单击已定义复制协议的列表旁的 “新建”按钮。

3. 在 “复制协议”对话框中，从菜单中选择一个包含使用者副本的现有服务器，或者单击 “其他”按钮定义一个。

   单击 “其他”按钮后，输入完全符合要求的使用者服务器名及其 LDAP 端口号。如果此端口使用 SSL，请选中安全端口复选框，以启用复制更新的连接安全。

4. 输入使用者服务器中复制管理员条目的 DN 和口令。默认情况下，此 DN 即为默认复制管理员的 DN。

   如果选择的是有安全端口的使用者，您可以单击 “选项”按钮以确定 DN 字段的含义。如果使用口令连接，供应商将通过加密 SSL 连接使用简单验证和通讯。如果使用证书连接， DN 字段是包含证书的条目 DN，不需要口令。

5. 键入此协议的说明字符串 （可选）。使用者服务器名和端口号以及说明字符串将显示在此主副本的复制协议列表中。

6. 完成后单击 “确定”。屏幕上将显示一个验证对话框，询问是否要测试刚才输入的连接参数。

7. 如果要使用给定复制管理员和口令测试至给定服务器及端口号的连接，请单击 “是”。如果连接失败，您仍然有可能使用此协议，可能情况为参数正确但服务器脱机。

   测试完成后，协议将显示在此主副本的复制协议列表中。

以后可以编辑复制协议，以更改使用者服务器上的复制管理员 DN 和口令：

1. 从列表中选择复制协议，然后单击 “编辑”按钮。

2. 在 “复制协议”对话框中，选择 “连接”标签。

3. 编辑使用者服务器的复制管理员 DN 或口令。

4. 编辑此协议的说明字符串 （可选）。

5. 单击 “确定”保存新设置，向此使用者发送更新时可以立即开始使用这些新设置。

   其他标签中的配置参数在 “启用分式复制”（第 254 页）和 “通过 WAN 复制”（第 265 页）中进行了说明。

6. 创建了每个复制协议后，可以选择为此后缀配置分式复制，然后立即初始化该副本，如 “初始化副本”（第 255 页）中所述。

配置分式复制

默认情况下，复制会将已复制后缀中的全部条目复制到使用者副本。使用 Sun ONE Directory Server 5.2 中的新分式复制功能，可以指定复制期间要进行复制的属性子集或不对其进行复制的属性子集。分式复制是在复制协议中配置的，允许您为主副本的每个使用者副本定义属性集。这样，您可以更有效地控制要分布的数据，以及使用复制带宽和使用者资源。

例如，如果希望减小复制带宽，可以选择对通常具有较大值的属性不进行复制，如 `photo`、`jpegPhoto` 和 `audio`。这样，在使用者副本中这些属性不可用。再举一例，您可以选择向专门执行验证的使用者服务器仅复制 `uid` 和 `userpassword` 属性。

分式复制注意事项

启用或修改分式属性集要求您重新初始化使用者副本。因此，应该在部署前确定分式复制的需要，并在第一次初始化副本时定义属性集。

鉴于某些属性的复杂功能 （如 ACI、角色和 CoS）存在相关性，复制小型的属性集时应加备小心。此外，不复制 ACI、角色或 CoS 机制的说明符或过滤器中提及的其他属性将会牺牲数据的安全性，或导致搜索返回的属性处于不同的集合中。管理 “不包括的属性”列表相对于管理 “要包括的属性”列表更安全，产生人为错误的可能性也比较小。

如果要复制的属性集合不允许所有要复制条目遵循此模式，则您应该在使用者服务器中关闭模式检查。复制 “不遵循”条目不会导致错误，因为复制机制会避开使用者中的模式检查。不过，这样使用者将包含 “不遵循”条目，应该关闭模式检查以向其客户机公开相关状态。

分式复制是在主副本与集线器副本及专门的客户副本之间的复制协议中配置的。不支持多主复制环境中两个主副本之间的分式复制配置。同时，如果若干主副本与同一副本之间有复制协议，则所有这些协议都必须复制同一属性集。

Sun ONE Directory Server 5.2 中提供的分式复制功能不具有与 Directory Server 以前版本的向后兼容性。配置分式复制协议时，主副本和使用者副本都必须在 Directory Server 5.2 实例中。

定义属性集

属性集是副本中启用分式复制时要复制的属性 （不包括其他所有属性）的列表。可以在主服务器中定义任意数量的属性集，然后将这些属性集之一与复制协议关联。

1. 在 Directory Server 控制台的顶级 “配置”标签中选择 “数据”节点，然后在右侧面板中选择 “复制”标签。
2. 单击 “复制”标签底部的 “管理已复制的属性集”按钮。可能需要向下滑动才能看到此按钮。
3. 单击 “添加”定义新的属性集或者从列表中选择一个现有的属性集，然后单击 “编辑”修改此属性集。在显示的 “属性集”对话框中，选择或取消选择 “复制”列中的复选框以使该集包括或不包括相应的属性。属性名旁边的复选框表明该属性将被复制。

   默认情况下，选择所有属性，建议仅取消选择特别不希望复制的那些属性。如果希望重新选择，“全部选中”按钮将重新选择所有属性。取消选择大量的属性时，目录服务器将复制除取消选择的属性以外的所有属性。如果后来模式中定义了新的属性并将这些新的属性用在了已复制的条目中，则这些新的属性将被复制，除非编辑该属性集以对其进行取消选择。

   单击 “全部不选”按钮将取消选择所有属性，然后可以选择要在集中包括的属性。单击 “全部不选”后，定义精确的属性集时，将仅复制选定的属性。如果后来模式中定义了新的属性并将这些新的属性用在了已复制的条目中，则这些新的属性将不会被复制，除非编辑该属性集以对其进行选择。

注意 属性 `objectClass`、`nsUniqueId` 和 `nsDS50ruv` 以及 RDN 命名属性将始终被复制，不论是否在属性集合中排除这些属性。这是因为 `objectClass` 和命名属性是 LDAP 修改所必需的， `nsUniqueId` 和 `nsDS50ruv` 是正确复制所必需的。

不包括 ACI 属性将会对使用者副本中的访问控制有影响。不包括 `userPassword` 属性将会导致没有用户可以验证使用者副本。

4. 为此属性集输入或修改说明字符串 （可选）。这是在已定义的集列表中显示的文本和编辑将使用该集的复制协议时显示的文本。如果没有提供任何说明，则服务器将根据不包括或包括的属性来生成说明。
5. 完成后单击 “保存”。

启用分式复制

只能在现有复制协议中启用分式复制：

1. 按照 “创建复制协议”（第 251 页）中的说明创建复制协议，或者选择以前定义的协议对其进行修改。
2. 按照 “禁用复制协议”（第 270 页）中的说明禁用复制协议。必须禁用协议才能修改分式复制配置。
3. 选择已禁用协议，然后单击 “编辑”。在显示的 “复制协议”对话框中选择 “复制的属性”标签。
4. 选中 “仅复制一组属性”复选框。
5. 从下拉列表中选择现有属性集，或者单击 “新建”，按照 “定义属性集”（第 253 页）中的说明定义新的属性集。还可以单击 “管理已复制属性集”查看和修改现有属性集定义。

   分式复制仅允许属性集与复制协议关联。该属性集应该包含要复制属性的确切列表。
6. 选择属性集后，单击 “确定”。提示性消息发出警告，说明您已经配置分式复制，需要重新初始化使用者副本。单击 “确定”关掉该消息。
7. 单击 “启用”重新激活复制协议。
8. 根据要复制的属性，您应该考虑在使用者服务器中禁用模式检查。
9. 如果其他主副本与此副本之间也有复制协议，必须在所有这些主副本中重复此步骤，以启用具有相同属性集的分式复制。
10. 现在必须初始化使用者副本，或者如果已复制此副本则对其进行重新初始化。请参阅下面的 “初始化副本”。

初始化副本

创建复制协议后，必须在复制实际开始前初始化使用者副本。初始化期间，将数据从供应商副本物理复制到使用者副本。

某些错误条件或配置更改要求您重新初始化副本。重新初始化时，使用者副本中已复制后缀的内容将被删除，并被主副本中后缀的内容替换。这样可以确保副本保持同步，复制更新可以重新开始。这里说明的所有初始化方法还将自动生成使用者副本的索引，这样使用者就准备好以最佳状态响应客户机的读请求。

何时进行初始化

必须在配置这两个副本后且在可以进行复制前进行副本初始化。后缀中的数据已完全复制到使用者后，供应商可以开始重新对使用者执行更新操作。

在正常操作情况下，绝对不能对使用者副本再次进行初始化。不过，不论何种原因从备份中恢复单主副本中的数据时，您都应该重新初始化所有更新的副本。使用多主复制的情况下，如果使用者已由其他主副本更新，则可能不需要对其进行重新初始化。

可以使用控制台联机初始化副本，也可以使用命令行手动初始化副本。初始化数量较少的使用者，使用控制台进行联机初始化会比较方便。可以从复制协议直接联机初始化副本。不过，由于是按顺序对每个副本进行初始化，所以此方法不适用于初始化大量副本。从一个 LDIF 文件中同时初始化大量使用者副本时，使用命令行手动初始化是更有效的方法。

最后，有经验的管理员还可以使用 Directory Server 5.2 的新二进制复制功能复制主副本或使用者副本。对此功能的某些限制仅能使具有大量数据库文件的副本 （例如包含上百万个条目的副本）具有可操作性并能节省时间。

在多主复制中初始化副本

如果进行多主复制，应该按以下顺序初始化副本：

1. 确保一个主副本中包含要复制数据的完整集合。使用此主副本在其他每个主副本中初始化副本。
2. 从主副本中或者从任一主副本的 LDIF 文件中初始化使用者副本。

在级联复制中初始化副本

如果进行级联复制，请注意应该始终按以下顺序初始化副本：

1. 如果还进行多主复制，请确保一个主副本中包含有要复制数据的完整集合。使用此主副本在其他每个主副本中初始化副本。
2. 在第一级集线器副本的主副本中初始化第一级集线器副本。
3. 如果有几个集线器副本级别，对于每一级要初始化的副本，在它的已初始化的前一级副本中对其进行初始化。
4. 在集线器副本的最后一个级别，初始化专门的客户副本。

多主副本初始化后会聚

如果进行的是多主复制，给定主副本进行初始化时，其他主副本可能会处理更改操作。因此，初始化完成后，新的主副本必须还接收初始化数据中不包括的新更新。由于初始化可能需要很长时间，所以挂起的更新数量可能也会很庞大。

为了允许会聚这些挂起的更新，初始化后，新初始化的主副本会被设置为只能读取客户机操作。这一点对任何类型的初始化都适用，不论是通过命令行 LDIF 文件联机使用控制台进行初始化，或者是使用备份执行二进制复制进行初始化。它是 Sun ONE Directory Server 5.2 中新增的行为。

因此，初始化后，多主配置中的主副本将处理复制更新并允许读操作，但它将从客户机返回所有写操作引荐。可以按“高级多主复制配置”（第 249 页）中的说明定义这些引荐。下列条件下主副本会回复到读 - 写模式：

- 将 `ds5BeginReplicaAcceptUpdates` 配置属性设置为 `start` 以明确允许更新操作。启用更新前，您应该验证此新主副本是否已与其他主副本会聚。可以使用 Directory Server 控制台中的复制配置面板或者通过命令行完成此过程 （见下面的过程）。

  手动干涉是在已初始化副本中启用更新的建议方法，因为这样您可以在允许更新前验证此新主副本是否与其他主副本完全同步。

- 如果先前已经设置了 `ds5referralDelayAfterInit` 属性，则主副本在指定的延迟时间后将自动切换到正常的读 - 写模式。可以为服务器中的每个主副本单独设置此属性。

  如果选择设置此属性，则您应该确定一个时间始终充裕的延迟，以允许主副本在初始化后与其他主副本会聚。此延迟取决于预期初始化的大小和长度，以及在其他主副本中同时发生更改的几率。初始化后，还在复制更改时就接收更新操作的主副本可能会导致异常错误。如果遇到复制错误，请参阅 *Sun ONE Directory Server 参考手册* 中的附录 A “错误代码”。

注意 由于增加了此新行为，使用主副本发送引荐时，希望执行写操作的客户机可能会达到已配置的跳跃限制。可能需要增加客户机的跳跃限制配置，这样它们就可以到达可用的主副本。如果已初始化或重新初始化了所有的主副本，所有的写操作都会失败，这是因为将没有副本接收客户机更新。

任何情况下，您都应该密切监控初始化的主副本，并相应地设置引荐属性以使服务器响应最大化。

通过控制台开始接收更新

执行下列步骤，以明确允许多主副本初始化后可以进行更新操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中，展开 “数据”节点和已复制后缀的节点，然后在此后缀下选择 “复制”节点。

   在右侧面板中，控制台将显示一个消息，指示副本已经初始化，目前正返回更新操作的引荐。如果此消息指示已启用自动引荐延迟，您仍然可以按照此步骤覆盖延迟。

2. 使用 `insync` 工具确保副本已与其他所有主副本会聚。如果所有服务器中修改之间的延迟为零或者副本从未有任何要复制的更改，则副本处于同步状态 （`-1` 延迟）。详细信息，请参阅 *Sun ONE Directory Server 参考手册* 的第 1 章中的 “insync”。

3. 单击消息右侧的按钮立即开始接收更新操作。

通过命令行开始接收更新

通过检查会聚并明确允许更新操作从而自动处理初始化多主副本的脚本中可能会使用到下列命令：

1. 使用 `insync` 工具确保副本已与其他所有主副本会聚。如果所有服务器中修改之间的延迟为零或者副本从未有任何要复制的更改，则副本处于同步状态 （`-1` 延迟）。详细信息，请参阅 *Sun ONE Directory Server 参考手册* 的第 1 章中的 “insync”。

2. 使用下列命令来修改 the `ds5BeginReplicaAcceptUpdates` 配置属性：

   ```
   % ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn=replica, cn=suffixName, cn=mapping tree, cn=config
   changetype:modify
   add:ds5BeginReplicaAcceptUpdates
   ds5BeginReplicaAcceptUpdates:start
   ^D
   ```

初始化副本时，将自动删除 `ds5BeginReplicaAcceptUpdates`，这样初始化后更新操作会被再次拒绝。

设置自动引荐延迟

`ds5referralDelayAfterInit` 配置属性决定了初始化后多长时间 （以秒计）副本将返回引荐。经历此延迟时间后，副本将自动开始处理客户机的更新操作。此属性对于每个副本都是特定的，应该根据 “多主副本初始化后会聚”（第 256 页）中说明的标准对此值进行设置。

如果刚刚对某副本进行了初始化，并且尚不能接收更新，则更改此属性的值将会动态地影响相应的副本。您可以在延迟过程中修改此值以增加或减小延迟。如果此延迟已经到期并且副本正在接收更新，设置此值将没有任何效果。

此属性的默认值是 -1，表示副本将会无限期地拒绝更新操作。在这种情况下，可以定义延迟以在延迟到期时自动允许更新，从初始化后计算此时间。设置已经到期的延迟将会导致副本立即开始接收更新。

1. 使用以下命令设置 ds5referralDelayAfterInit 属性：

```
% ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=replica, cn=suffixName, cn=mapping tree, cn=config
changetype:modify
replace:ds5referralDelayAfterInit
ds5referralDelayAfterInit:seconds
^D
```

使用控制台初始化副本

使用控制台进行联机副本初始化是初始化或重新初始化使用者副本的最简单的方法。不过，如果正在初始化大量条目 （超过 1-2 百万），则此过程可能非常耗时，这种情况下您可能会发现使用命令行手动进行使用者副本初始化是更有效的方法（详细信息，请参阅 “从命令行初始化副本”（第 260 页））。

注意 使用控制台初始化使用者副本时，在初始化过程完成前，此后缀上的所有操作 （包括搜索）都将被引荐回主副本服务器。

使用 Directory Server 控制台时，初始化配置有分式复制的副本将简单明了。初始化期间，仅将选定的属性发送至使用者。

执行联机副本初始化

要使用控制台进行初始化或重新初始化副本，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中，展开 “数据”节点和主副本后缀的节点，然后在此后缀下选择 “复制”节点。

   副本状态信息将显示在右侧面板中。

2. 在已定义协议的列表中，选择要进行初始化的使用者副本的相应复制协议，然后单击 “操作” > “初始化远程副本”。

   将出现一个确认信息，提示使用者副本中存储的所有信息都将被删除。

3. 在验证框中单击 “是”。

   联机使用者副本初始化将立即开始。复制协议的图标将显示一个红色的标记，指示初始化过程的状态。

4. 单击“刷新”>“立即刷新”或“刷新”>“连续刷新”跟踪使用者副本初始化的状态。

   突出显示的协议的所有消息都将显示在此列表下的文本框中。

有关监控复制状态和初始化状态的详细信息，请参阅 “监控复制状态”（第 282 页）。

从命令行初始化副本

对于需复制大量条目的部署，使用命令行手动进行副本初始化是使用者副本初始化的最快方法。出于性能方面的考虑，如果不适合进行联机处理时，我们建议您使用手动处理。不过，手动初始化使用者副本的过程比联机初始化过程要复杂得多。

要手动初始化或重新初始化副本，您首先需要将后缀数据的原副本导出至 LDIF 文件。如果正在初始化分式副本，则您应该过滤此文件以仅保留已复制属性。然后将该文件传送到所有使用者服务器，并导入它。在多主复制部署中，可以使用从原主副本中导出的 LDIF 文件对其他主副本和任意使用者副本进行初始化。在级联复制环境中，可以使用同一个文件来初始化集线器副本及其使用者副本。

不论何种情况，都必须从已配置主副本中导出的 LDIF 文件开始初始化。不能使用任意的 LDIF 来初始化所有副本，因为它不包含复制数据。必须首先将 LDIF 文件导入至主副本，然后按照下列步骤将其导出。

导出副本至 LDIF

可以使用 `db2ldif -r` 或 `db2ldif.pl -r` 命令将副本内容存储在 LDIF 文件中。详细信息，请参阅 “从命令行导出到 LDIF”（第 125 页）。必须使用 `-r` 选项利用这些命令导出副本。

下面的示例会将整个 `dc=example,dc=com` 副本导出至名为 `example_master.ldif` 的文件：

Solaris 软件包

```
# /usr/sbin/directoryserver stop
# /usr/sbin/directoryserver db2ldif -r -s "dc=example,dc=com" \
  -a /var/ds5/slapd-serverID/ldif/example_master.ldif
# /usr/sbin/directoryserver start
```

其他安装

```
# ServerRoot/slapd-serverID/stop-slapd
# ServerRoot/slapd-serverID/db2ldif -r -s "dc=example,dc=com" \
  -a ServerRoot/slapd-serverID/ldif/example_master.ldif
# ServerRoot/slapd-serverID/start-slapd
```

然后，如果必要可以过滤 LDIF 文件，并将其传送到使用者主机，从而对使用者副本进行初始化。

过滤用于分式复制的 LDIF 文件

如果已经配置分式复制，在将导出的 LDIF 文件复制至使用者服务器前，应该过滤出所有不使用的属性。 Directory Server 提供 `fildif` 工具用于完成此过程。此工具过滤指定的 LDIF 文件，以仅保留复制协议中定义的属性集所允许的属性。

此工具将读取服务器配置以确定属性集定义。要读取配置文件， `fildif` 工具必须作为 root 运行。例如，以下命令将过滤在上个示例中从 `dc=example,dc=com` 后缀中导出的文件：

```
# CAMUS=/var/Sun/mps/slapd-camus
# /var/Sun/mps/shared/bin/fildif \
-i $CAMUS/ldif/example_master.ldif \
-o $CAMUS/ldif/filtered.ldif -c $CAMUS/config/dse.ldif \
-b "cn=rousseau.example.com:389, cn=replica, \
cn=dc=example\,dc=com, cn=mapping tree, cn=config"
```

`-i` 和 `-o` 分别为输入和输出文件。 `-c` 选项是包含复制协议和属性集定义的配置文件。 `dse.ldif` 文件是服务器存储 `cn=config` 条目内容 （包括复制协议和属性集）的位置。

`-b` 选项是定义分式复制的复制协议的 DN。通过以目录管理员身份在 Directory Server 控制台中浏览 `cn=config` 后缀，可以找到此条目。在后缀的 `cn=replica` 条目下选择条目，并使用 “编辑” > “复制 DN”菜单项将此 DN 复制到剪贴板，以备输入命令时使用。

Sun ONE Directory Server 参考手册 的第 1 章“LDIF 命令行公用程序”中提供了 `fildif` 工具的完整命令行语法。

然后，您可以使用 `fildif` 生成的 `filtered.ldif` 文件初始化此复制协议中的使用者副本。按照下节中的说明将此文件传送至使用者服务器，并将其导入。

将 LDIF 文件导入至使用者副本

使用 Directory Server 控制台中的导入功能，可以将包含主副本内容的 LDIF 文件导入至使用者副本，或者也可以使用 `ldif2db` 命令或 `ldif2db.pl` 脚本 （在 Solaris 软件包平台中为 `directoryserver ldif2db` 或 `directoryserver ldif2db-task`）导入。进行所有的导入操作时，这些脚本需要目录管理员的绑定 DN 和口令，以执行导入。“从命令行导入 LDIF”（第 119 页）对这两种导入方法进行了说明。

下面的示例显示了如何导入 LDIF 文件来初始化 dc=example,dc=com 使用者副本：

Solaris 软件包

```
# /usr/sbin/directoryserver stop
# /usr/sbin/directoryserver ldif2db -s "dc=example,dc=com" \
  -i example_master.ldif
# /usr/sbin/directoryserver start
```

其他安装

```
# ServerRoot/slapd-serverID/stop-slapd
# ServerRoot/slapd-serverID/ldif2db -s "dc=example,dc=com" \
  -i example_master.ldif
# ServerRoot/slapd-serverID/start-slapd
```

使用 ldif2db.pl 脚本不需要预先停止服务器。详细信息，请参阅 *Sun ONE Directory Server 参考手册* 的第 2 章中的 “ldif2db.pl”。

使用二进制复制初始化副本

Directory Server 5.2 的新二进制复制功能可以复制整个服务器，方法是使用一台服务器中的二进制备份文件在另一台服务器中恢复为相同的目录内容。此高级功能与目录服务器的数据库文件进行交互，且只应该由具有经验的管理员使用。

二进制复制限制

因为二进制复制功能会将数据库文件从一台计算机移动至另一台计算，所以此机制受到以下严格限制：

- 这两台计算机都必须使用相同的硬件和操作系统，包括所有的 Service Pack 或增补程序。
- 这两台计算机安装的 Directory Server 版本必须相同，包括二进制格式 （32 位或 64 位）、 Service Pack 和增补程序级别。
- 这两台服务器必须有包括相同后缀的相同目录树。所有后缀的数据库文件必须一起复制，不能复制单个后缀。
- 每个后缀在两台服务器中都必须有相同的已配置索引，包括 VLV （虚拟列表视图）索引。后缀的数据库必须有相同的名称。
- 要复制的 Directory Server 一定不能保留 o=NetscapeRoot 后缀，这表示它不能是 Sun ONE Administration Server 的配置目录。
- 每台服务器都必须有配置为副本的相同后缀，副本在这两台服务器中必须具有相同的角色 （主副本、集线器副本或使用者副本）。如果配置的是分式复制，则必须在所有的主副本服务器中对其进行相同地配置。
- 两台服务器中都不能使用属性加密。

- 如果启用属性值唯一性插件，则它们在两台服务器中必须具有相同的配置，并且必须在新副本中对其进行重新配置，如下面步骤中所述。

如果符合上述条件，则可以从另一个主服务器的二进制复制初始化或重新初始化主副本，或者从另一个使用者服务器的二进制复制初始化或重新初始化使用者副本。下面两个过程介绍了执行二进制复制的可选方法，一个不需要停止服务器，另一个使用的磁盘空间最小。

在不停止服务器的情况下进行二进制复制

建议使用下面的过程执行二进制复制，因为它使用标准备份功能来创建服务器的数据库文件副本。执行标准备份可以确保所有的数据库文件在无需停止服务器的情况下处于相关状态。

不过，此过程有一定的限制，您需要加以考虑。备份操作和恢复操作在同一台计算机中创建数据库文件的副本，因此每台计算机中这些文件所需磁盘空间将加倍。另外，如果目录包含多至 GB 字节的数据，这些文件的实际复制操作将花费大量的时间。如果您的磁盘空间有限或者数据库文件特别大，请参阅 “使用最小磁盘空间进行二进制复制”（第 263 页）。

1. 在新副本的目标计算机中安装 Directory Server，如果必要请创建服务器的新实例，然后按照 “二进制复制限制”（第 262 页）中的说明对其进行配置。
2. 在涉及此副本的复制拓扑中创建所有复制协议。这包括供应商与此副本之间的协议，如果不是专门的客户副本，还包括此副本与其使用者副本之间的协议。
3. 选择一个与要初始化的副本类型相同并且已完全配置和初始化的后缀 （可能为主副本、集线器副本或使用者副本），并根据 “使用控制台备份服务器”（第 127 页）中的步骤对此后缀执行标准备份。
4. 例如，可以使用 `ftp` 命令，将备份目录中的所有文件复制或传送到目标计算机的目录中。
5. 按照 “从备份还原数据”（第 128 页）中的说明将文件加载至目标服务器。
6. 如果在多主复制方案中已经初始化了一个新的主副本，请按照 “多主副本初始化后会聚”（第 256 页）中的步骤进行操作，以确保新副本可以开始接收客户机的更新操作。

使用最小磁盘空间进行二进制复制

下面的过程使用的磁盘空间以及耗费的时间都较少，因为它不备份数据库文件。不过，它要求您停止被复制的服务器，以确保数据库文件处于相关状态。

警告 千万不要将此过程用于重新初始化已参与多主复制方案的主副本。只能用于重新初始化使用者服务器或者初始化新的主副本服务器。要重新初始化现有主副本，请使用联机初始化、导入 LDIF 文件或者执行“在不停止服务器的情况下进行二进制复制”（第 263 页）中说明的步骤。

1. 在新副本的目标计算机中安装 Directory Server，必要时创建服务器的新实例，然后按照 “二进制复制限制”（第 262 页）中的说明对其进行配置。
2. 在涉及此副本的复制拓扑中创建所有复制协议。包括供应商与此副本之间的协议，如果不是专门的客户副本，还包括此副本与其使用者副本之间的协议。
3. 按照 “启动和停止 Directory Server”（第 20 页）中的说明停止要被初始化或重新初始化的目标服务器。
4. 选择一个与要初始化的副本类型相同并且已完全配置和初始化的副本 （可能为主副本、集线器副本或使用者副本），并停止服务器。如果在多主配置中复制主副本，则您应该确保在停止服务器前，已使用来自其他主副本的最近更改对其进行了完全更新。
5. 从原副本计算机复制或传送所有数据库文件 （包括事务日志）至目标计算机，如使用 `ftp` 命令。除非文件已被重新定位，否则数据库文件和事务日志将位于 *ServerRoot*`/slapd-`*serverID*`/db` 目录下。

   如果初始化主副本或集线器副本，您还必须复制更改日志中的所有文件，默认情况下这些文件位于 *ServerRoot*`/slapd-`*serverID*`/changelog` 下。
6. 重新启动源服务器和目标服务器。

启用引荐完整性插件

如果要使用引荐完整性插件，必须在所有主副本服务器中启用该插件。不需要在集线器服务器或使用者服务器中启用。请参阅 “将引荐完整性与复制一起使用”（第 75 页）。

通过 SSL 复制

可以对复制所涉及到的 Directory Server 进行配置，这样所有复制操作都可以通过 SSL 连接进行。要执行此操作，请完成以下步骤：

1. 将供应商和使用者服务器配置为都可以使用 SSL。

   详细信息，请参阅第 11 章 “实现安全性”。

注意 如果供应商服务器证书为以下的情况，通过 SSL 复制将会失败：

- 自签名的证书。
- SSL 握手期间，只用于服务器而不能充当客户机的 SSL 证书。

2. 如果没有为使用者服务器中的后缀配置复制，请按照 “启用使用者副本”（第 244 页）中的说明启用此复制。
3. 按照 “高级使用者配置”（第 245 页）中说明的步骤，以另一个复制管理员的身份定义使用者服务器中的证书条目 DN。
4. 如果没有为供应商服务器中的后缀配置复制，请按照 “启用集线器副本”（第 246 页）或 “启用主副本”（第 249 页）中的说明启用此复制。
5. 在供应商服务器，创建一个新复制协议，以将更新发送至位于安全 SSL 端口的使用者服务器。详细说明，请按照 “创建复制协议”（第 251 页）中的步骤执行操作。在使用者服务器上指定一个安全端口，选择一个 SSL 选项 （确定使用口令还是证书）。为所选的 SSL 选项输入 DN （复制管理员或证书）。

配置复制协议后，供应商将会通过 SSL 向使用者副本发送所有复制更新消息，如果您选择该项，则将使用证书。如果使用为 SSL 配置的协议通过控制台执行客户初始化，则客户初始化还会使用安全连接。

通过 WAN 复制

Sun ONE Directory Server 5.2 提供执行任意形式复制的能力，包括在通过广域网 (WAN) 连接的计算机之间进行多主复制 (MMR)。复制机制的内部改善允许供应商服务器以较长等待时间和较低带宽通过网络对具有合理延迟的使用者服务器进行初始化和更新。

注意 实际复制延迟和更新性能与多种因素有关，包括但不仅限于下列内容：修改率、条目大小、服务器硬件、平均等待时间和平均带宽。如果您的系统环境中有与复制相关的问题，请与 Sun 专业服务代表联系。

复制机制的内部参数默认情况下处于适用于 WAN 的最佳状态。不过，如果由于上面提及的因素而导致复制速度慢，您可能会根据经验调整窗口大小和组大小这两个参数。您还可以计划复制以避开峰值网络时间，从而改善整个网络的使用情况。最后， Solaris 和 Linux 平台上的 Directory Server 支持复制数据的压缩以优化带宽使用。

配置网络参数

以下两个参数确定了复制机制如何对条目进行分组，以通过网络更有效地发送这些条目。它们影响供应商和使用者交换复制更新消息和确认的方式。

- 窗口大小 （默认值为 10）- 表示不必通过使用者及时确认即可发送的最大更新消息数。在 WAN 环境中，与发送了每条消息后等待确认相比较，一次发送许多消息的方式效率较高。
- 组大小 （默认值为 1）- 表示可捆绑成单个更新消息的最大数据修改数。根据数据的大小和网络的属性，效率可能随发送消息的增多而提高，因此具有更大的组大小。

大多数情况下，默认值可以处于工作最佳状态。不过，如果目录条目过大或过小，或者如果要复制的修改率很大，您可能希望通过 WAN 修改这些参数，以检测其对复制性能的影响。

这两个网络参数在每个复制协议中都是可配置的。这样，您可以根据每个使用者的特定网络状况调整复制性能。

不需要中断复制来修改窗口大小和组大小参数：

1. 在 Directory Server 控制台中选择 “配置”标签，然后展开 “数据”节点和已复制后缀的节点。
2. 在此后缀下选择 “复制”节点，在右侧窗格中选择要配置的复制协议，然后单击 “编辑”。
3. 在 “复制协议”对话框中选择 “网络”标签，输入窗口大小的新值 （范围为 1 到 1000）和组大小的新值 （范围为 1 到 100）。组大小必须小于或等于窗口大小。
4. 单击 “确定”保存新值，然后关闭 “复制协议”对话框。

   新参数值将立即生效，下一个复制更新发送至相应的使用者。

计划复制活动

如果副本之间紧密同步不是非常重要，则通过 WAN 复制数据的一种方法就是在低网络使用率期间计划更新。网络可用性越高，执行更新就越快，如果已经在高使用率下运行，则复制消息将不会进一步加大网络拥塞。

通过使用者复制协议，您可以计划以天或周为周期为每个使用者独立地进行更新：

1. 在 Directory Server 控制台的顶级 “配置”标签中，展开 “数据”节点和已复制后缀的节点。
2. 在此后缀下选择 “复制”节点，在右侧窗格中选择要配置的复制协议，然后单击 “编辑”。
3. 选择 “复制协议”对话框的 “计划”标签，然后选择周调度旁的单选按钮。
4. 定义计划：
   a. 对于每周更新，选中要发生复制日期 （一天或多天）旁的复选框。如果希望在这些天数内进一步限制复制，还可以选择输入时间范围 （使用 24 小时制）。
   b. 对于每日更新，单击 “全部”以每天都进行复制，并输入应该发生复制的时间范围 （使用 24 小时制）。

      请注意时间范围不能跨越午夜。
5. 单击 “确定”保存新值，然后关闭 “复制协议”对话框。

   新计划将立即生效，将导致相应使用者的下一次复制更新被延迟到计划第一次允许其进行更新时。

数据压缩

要减小复制使用的带宽，可以配置复制压缩更新使用者副本时发送的数据。复制机制使用 Zlib 压缩库，该库只可在受支持的 Solaris 和 Linux 平台上使用。供应商和使用者必须运行在 Solaris 或 Linux 平台上才能启用压缩。

只有通过设置主服务器中的复制协议条目上的 `ds5ReplicaTransportCompressionLevel` 属性，复制压缩的配置才可用。该属性的值可能是下列之一：

`0` - 不执行压缩。默认情况下，未指定 `ds5ReplicaTransportCompressionLevel` 属性时会发生该行为。

`1` - 使用 Zlib 库的默认压缩级别。

2 - 使用 Zlib 库的最佳大小压缩级别。

3 - 使用 Zlib 库的最佳速度压缩级别。

您应当根据经验测试和选择压缩级别，以便在 WAN 环境中获得最佳效果，从而实现所期望的复制使用。不应在网络延迟无意义的 LAN （局域网）中设置此参数，因为压缩和解压缩计算将减慢复制速度。

例如，将复制更新发送到 east.example.com 上的使用者时要使用最快的压缩速度，请使用下面的 ldapmodify 命令：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=east.example.com:389,cn=replica,cn="suffixDN",
 cn=mapping tree,cn=config
changetype:modify
add:ds5ReplicaTransportCompressionLevel
ds5ReplicaTransportCompressionLevel: 3
^D
```

修改复制拓扑

本节包含管理现有复制拓扑的步骤，如编辑或删除复制协议，升级、降级或禁用副本，强制对使用者更新，以及管理更改日志。

管理复制协议

在主副本后缀的复制面板中，可以管理复制协议，以更改协议中的验证信息、中断对特定使用者的复制或者从拓扑中删除使用者副本。

更改复制管理员

可以编辑复制协议来更改用于绑定至使用者服务器的复制管理员身份。为避免中断复制，应该在修改复制协议前定义新复制管理员条目或者使用者证书条目。不过，如果由于绑定失败造成复制的中断，在复制还原设置的限制范围内，复制机制会在您更正错误时自动发送所有必要的更新 （请参阅 “高级使用者配置”（第 245 页））。

要更改用于验证使用者的复制管理员，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点和已复制后缀的节点，然后在此后缀下选择 “复制”节点。
2. 在右侧面板中，选择要修改的复制协议，然后单击 “编辑”。

3. 在 “复制协议”对话框中，选择 “连接”标签。

   此状态行会指示使用者服务器的主机名和端口号。

4. 修改 DN 和口令字段，以包含另一个复制管理员条目的 DN 和口令或者使用者服务器中证书条目的 DN。

5. 如果此复制协议通过安全端口使用 SSL，您还可以单击 “选项”按钮来选择安全验证的类型。如果使用口令连接，供应商将通过加密 SSL 连接使用给定 DN 进行简单验证。如果使用证书连接， DN 字段是证书条目的 DN，不需要口令。

   不能将现有复制协议从非安全验证切换到安全验证，反之亦然。要启用具有不同安全设置的复制，必须创建另一个复制协议。

6. 单击 “确定”以保存更改。

对复制协议进行复制

对复制协议进行复制是一种简单方法，用于在大型复制拓扑中配置供应商副本的多个使用者副本：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点和已复制后缀的节点，然后在此后缀下选择 “复制”节点。

2. 在复制协议列表中，选择一个要复制的协议。如果要创建一个具有到使用者的安全连接的新协议，则必须选择一个也使用安全端口的现有协议。如果要创建一个新的非安全协议，则必须选择一个现有的非安全协议。

   单击 “编辑”并浏览 “复制协议”对话框的标签，验证此协议的配置。以下小节将说明这些标签的配置：

   - “更改复制管理员”（第 268 页）对 “连接”标签进行了说明。
   - “通过 WAN 复制”（第 265 页）对 “计划”和 “网络”标签进行了说明。
   - “配置分式复制”（第 253 页）对 “复制属性”标签进行了说明。

3. 保持选中此复制协议，然后单击 “复制”按钮。

4. 从列表中选择新使用者的主机名或端口号，或者单击 “添加主机”按钮使用其他的主机和端口。此列表和 “添加主机”对话框将仅允许您选择与要复制的使用者协议具有相同安全类型的使用者。

5. 确保选中列表中的一个主机名，单击 “确定”为该使用者服务器创建一个新的复制协议。

6. 新协议将复制现有协议的所有配置信息。这就是说您必须具有在两个服务器中定义的完全相同的、并且使用相同口令的复制管理员条目。如果要修改新协议的配置 （如更改复制管理员 DN），请从列表中选择该协议，然后单击 “编辑”。

禁用复制协议

禁用复制协议时，主副本将停止向指定使用者副本发送更新。到该服务器的复制也将停止，但协议中的所有设置都将保留。以后可以通过重新启用协议来恢复复制。有关在中断后恢复复制机制的信息，请参阅下面的 “启用复制协议”。

要禁用复制协议，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点和已复制后缀的节点，然后在此后缀下选择 “复制”节点。
2. 在右侧面板中，选择要禁用的复制协议。
3. 在协议列表下的框中选择 “操作” > “禁用协议”。
4. 单击 “是”确认要禁用复制协议。

列表中此协议的图标会将显示状态更改为已禁用。

启用复制协议

启用复制协议将恢复与指定使用者之间的复制。不过，如果复制的中断时间超过了复制还原设置允许的时间，并且使用者不能由另一供应商更新，则您必须重新初始化使用者。复制还原设置是供应商的更改日志和使用者清理延迟的最大大小和存留期 （请参阅 “高级使用者配置”（第 245 页））。

如果中断时间较短，并且复制可以恢复，则重新启用协议后主副本将自动更新使用者。

要启用复制协议，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点和已复制后缀的节点，然后在此后缀下选择 “复制”节点。
2. 在右侧面板中，选择要启用的复制协议。
3. 在协议列表下的框中选择 “启用”按钮。
4. 必要时重新初始化使用者副本。

删除复制协议

删除复制协议将会停止向相应使用者进行复制，并删除此协议的所有配置信息。如果以后要恢复复制，请禁用协议，如 “禁用复制协议”（第 270 页）中所述。

要删除复制协议，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点和已复制后缀的节点，然后在此后缀下选择 “复制”节点。
2. 在右侧面板中，选择要删除的复制协议。
3. 在协议列表的右侧单击 “删除”按钮。
4. 单击 “是”确认要删除此复制协议。

升级或降级副本

升级或降级副本将会更改其在复制拓扑中的角色。专门的客户副本可以升级为集线器副本，集线器副本可以升级为主副本。主副本可以降级为集线器副本，集线器副本也可以降级为专门的客户副本。不过，主副本不能直接降级为使用者副本，同样使用者副本也不能直接升级为主副本。

多主复制机制中允许的升级和降级使得拓扑非常灵活。先前由某个使用者副本使用的站点可能会增大，并需要一个具有若干副本的集线器副本来处理负载。如果负载包括对副本内容的许多修改，则集线器副本可以成为一个主副本，以更快地进行本地更改，然后可以将这些本地更改复制到其他站点中的其他主副本。

要升级或降级一个副本，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点和已复制后缀的节点，然后在此后缀下选择 “复制”节点。
2. 在右侧面板中，选择 “更改” > “对副本进行升级 - 降级”菜单项。
3. 复制向导仅允许您选择一个许可的新角色，然后按步骤完成配置过程以配置新的副本角色。您应该知道可能会产生以下后果：
   - 当将主副本降级为集线器副本时，副本将变为只读，并被配置为可以向其他主副本发送引荐。新集线器副本将保留它的所有使用者副本，不论是集线器副本还是专门的客户副本。
   - 将单个主副本降级为集线器副本将会创建一个没有主副本的拓扑。如果您要定义新主副本，此向导会允许您完成此操作。不过，最好将新主副本添加为多主副本，并在降级其他副本之前允许对其进行初始化。
   - 当将集线器副本降级为使用者副本时，将删除所有的复制协议。如果其他集线器副本或主副本尚未对集线器的使用者副本进行更新，则它们将不再被更新。您应该在其他集线器副本或主副本中创建新协议，以更新这些使用者副本。

- 将使用者副本升级为集线器副本时，就会启用其更改日志，您可以定义它与使用者副本之间的新协议。
- 将集线器副本升级为主副本时，此副本将接受修改请求，您可以定义此副本与其他主副本、集线器副本或专门的客户副本之间的新协议。

禁用副本

禁用副本将会从复制拓扑中删除此副本。它将不再被更新或发送更新，这取决于它的角色是主副本、集线器副本还是使用者副本。禁用供应商将会删除所有复制协议，如果要再次启用此副本，则必须重新创建这些协议。

要禁用副本，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点和已复制后缀的节点，然后在此后缀下选择 “复制”节点。
2. 在右侧面板中，选择 “更改” > “禁用复制”菜单项。
3. 在验证对话框中单击 “是”。
4. 复位此后缀的写入权限和引荐 （可选）。这些设置将与禁用副本时的设置一样，例如，已禁用的使用者副本仍会向它的前一个主副本发送修改请求。

   要修改写入权限和引荐，请在 “配置”标签中选择此后缀的节点，并在右侧面板的 “设置”选项中进行修改。详细信息，请参阅 “设置访问权限和引荐”（第 106 页）。

移动更改日志

更改日志是对指定供应商副本的全部修改的内部记录，服务器使用更改日志来对其他副本重复进行这些修改。更改日志的内容由服务器自动进行管理，即使重新启动服务器后也会通过多主更新对其进行更新。

在 Directory Server 的早期版本中，可以通过 LDAP 访问更改日志。不过，现在更倾向于在服务器内部使用此日志。如果您有需要读取更改日志的应用程序，请使用 retro change log 插件获取向后兼容性。详细信息，请参阅 “使用 Retro Change Log 插件”（第 279 页）。

只有在需要将更改日志文件移动到另一个位置时，管理员才应该修改更改日志，例如存储此文件的磁盘已满。

警告 禁用更改日志或将其移动至一个新位置时，更改日志将被重新初始化。在上述任一情况下，您都需要重新初始化此服务器中的所有使用者副本。

您必须使用 Directory Server 控制台移动更改日志，千万不要使用操作系统 `rename` 或 `mv` 命令移动：

1. 在 Directory Server 控制台的顶级 “配置”标签上选择 “数据”节点，然后在右侧面板中选择 “复制”标签。
2. 在文本字段中输入一个新位置。从现在起，此内容将是要存储更改日志的新路径和目录名称。例如，将更改日志从默认位置 *ServerRoot*`/slapd-`*serverID*`/changelogdb` 移动至 *ServerRoot*`/slapd-`*serverID*`/newchangelog`。

   现有更改日志将从原位置删除，新的更改日志将保留在新位置中。
3. 在 “复制”标签中单击 “保存”。
4. 重新启动 Directory Server。
5. 按照 “初始化副本”（第 255 页）中的说明重新启动使用者副本。

保持副本同步

停止复制涉及的目录服务器以进行常规维护后，当目录服务器回到联机状态时，您需要确保该服务器已通过复制立即获得更新。如果是多主副本环境中的主副本，则需要多主集合中的另一个主副本对目录信息进行更新。如果是其他情况，集线器副本或专门的客户副本脱机进行维护后，它们回到联机状态时，需要由主副本对这些副本进行更新。

本节介绍复制重试算法，以及如何在无需等待下次重试的情况下强制发生复制更新。

注意 只有已经设置复制并且已经初始化使用者副本时，才能使用本节中说明的步骤。

复制重试算法

供应商尝试向使用者副本中复制不成功时，它将以递增的时间间隔定期重试。重试模式如下所示：20、 40、 80，然后 160 秒。然后供应商将每 160 秒重试一次。

请注意，即使您已将复制协议配置为始终保持供应商副本和使用者副本同步，但要使脱机超过五分钟的副本立即回到最新的状态，仅这样设置还不够。

要确保目录信息在服务器回到联机状态时立即处于同步状态，您可以使用 Directory Server 控制台或可定制的脚本。

通过控制台强制复制更新

要确保在使用者或多主复制配置中的主副本经过一定时间后回到联机状态时，立即发送复制更新，您可以对保留目录数据最新版本的供应商执行这些步骤：

1. 在 Directory Server 控制台顶级 “配置”标签中，展开 “数据”节点和主副本的后缀节点，然后在此后缀下选择 “复制”节点。

   副本状态信息将显示在右侧面板中。

2. 在与要更新的使用者副本相应的列表中选择复制协议，然后单击 “操作” > “现在发送更新”。

   这样，将开始向保留需要被更新信息的副本中进行复制。

通过命令行强制复制更新

在需要更新的使用者副本中，可以运行一个脚本以便提示供应商立即发送复制更新。代码示例 8-1 （第 275 页）中显示了此脚本。

您可以复制此示例，并立即指定一个有意义的名称，如 `replicate_now.sh`。必须为代码示例 8-1 中列出的变量提供实际值。

注意 管理员必须运行此脚本，因为不能将其配置为在脱机服务器回到联机状态后可以自动运行。

代码示例 8-1 Replicate_Now 脚本示例

```
#!/bin/sh
SUP_HOST=supplier_hostname
SUP_PORT=supplier_portnumber
SUP_MGRDN=supplier_directoryManager
SUP_MGRPW=supplier_directoryManager_passwd
MY_HOST=consumer_hostname
MY_PORT=consumer_portnumber

ldapsearch -1 -h ${SUP_HOST} -p ${SUP_PORT} -D "${SUP_MGRDN}" \
-w ${SUP_MGRPW} -b "cn=mapping tree, cn=config" \
"(&(objectclass=nsds5replicationagreement) \
(nsDS5ReplicaHost=${MY_HOST})(nsDS5ReplicaPort=${MY_PORT}))" \
dn nsds5ReplicaUpdateSchedule > /tmp/$$

cat /tmp/$$ |
awk '
BEGIN { s = 0 }
/^dn:/ { print $0;
    print "changetype:modify";
    print "replace:nsds5ReplicaUpdateSchedule";
    print "nsds5ReplicaUpdateSchedule: 0000-2359 0123456";
    print "-";
    print "";
    print $0;
    print "changetype:modify";
    print "replace:nsds5ReplicaUpdateSchedule";
}

/^nsds5ReplicaUpdateSchedule:/ { s = 1; print $0; }

/^$/ {
  if ( $s == 1 )
    { print "-" ; print ""; }
  else
    { print "nsds5ReplicaUpdateSchedule: 0000-2359 0123456";
      print "-" ; print ""; };
  s = 0; }

' > /tmp/ldif.$$

echo "Ldif is in /tmp/ldif.$$"
echo

ldapmodify -c -h ${SUP_HOST} -p ${SUP_PORT} -D "${SUP_MGRDN}" \
-w ${SUP_MGRPW} -f /tmp/ldif.$$
```

如果要使用此脚本，必须在复制环境中将变量替换为实际值。

表 8-1 Replicate_Now 变量

变量	定义
supplier_hostname	供应商服务器的主机名，用于联系以获取与当前使用者之间的复制协议信息。
supplier_portnumber	供应商上使用的 LDAP 端口。
supplier_directoryManager	供应商中特许的目录管理员用户的 DN，或者在 `cn=config` 下具有写入权限的 `admin` 用户。
supplier_directoryManager_passwd	供应商中特许的目录管理员或 `admin` 用户的口令。
consumer_hostname	当前使用者的主机名。
consumer_portnumber	使用者使用的 LDAP 端口。

如果要通过 SSL 连接进行更新操作，您必须使用适当的参数和值修改脚本中的 `ldapmodify` 命令。详细信息，请参阅 “配置 LDAP 客户机以使用安全性”（第 338 页）。

使用早期版本进行复制

本节介绍如何使用 Sun ONE Directory Server 的早期版本配置复制。

Sun ONE Directory Server 5.1 和 5.2 版本几乎与所有复制配置完全兼容，但是以下情况例外：

- 与分式复制配置不兼容，一定不要在 Directory Server 5.2 主副本和 5.1 的使用者副本之间进行配置。
- 配置 5.2 主副本和 5.1 使用者副本之间的协议之前，必须在 `cn=config` 中将 `nsslapd-schema-repl-useronly` 设置为 `on`。否则，在复制到 5.1 时， 5.2 中的模式将发生冲突。进行了此设置之后，将仅复制存储在 `99user.ldif` 文件中的用户定义的那些模式元素。请参阅 “复制模式定义”（第 300 页）。
- 在 Directory Server 5.2 中，模式文件 11rfc2307.ldif 已更改为符合 RFC 2307 的要求。您必须更新 5.1 服务器上的相应文件，如 “更新 Directory Server 5.1 模式”（第 278 页）中所述。

- 已降级为集线器副本的 5.2 主副本仍会显示在 5.1 使用者的引荐列表中。不过，由于降级的内部机制，已降级副本的端口号将为零。此引荐 URL 不可用，大多数客户机在不能遵循这些引荐时会自动将其引荐给其他主副本。不过，您可能需要增加访问这些 5.1 副本的客户机中的引荐的跃点限制。 5.2 使用者副本不显示不可用的引荐 URL，也不会将其返回至已降级的主副本。

Sun ONE Directory Server 5.2 在下列情况下可能会与 Directory Server 4.x 版本的复制方案有关：

- Directory Server 5.2 已配置为主副本，但仅作为使用者副本向 Directory Server 4.x 供应商复制。
- 使用者副本不能同时作为旧版 4.x 供应商和 5.2 供应商的使用者。不过， 5.2 服务器可能有不同的副本，其中有的由旧版 Directory Server 提供，其他的由 5.2 Directory Server 提供。
- 已被配置为旧版 4.x 供应商的使用者的 Directory Server 5.2 副本，在此拓扑中不能作为此后缀的集线器副本。

能够将 Directory Server 5.2 作为旧版 Directory Server 的使用者的主要好处就是可以简化已复制环境的移植。有关移植已复制环境要执行的步骤的详细信息，请参阅 *Sun ONE Directory Server 安装和调整指南* 中的第 2 章 “从以前版本升级”。

将 Directory Server 5.2 配置为 Directory Server 4.x 的使用者

如果要将 Directory Server 5.2 作为 Directory Server 4.x 版本的使用者来使用，必须按照下面的步骤对其进行配置：

1. 按照 “启用主副本”（第 249 页）中的说明将此副本启用为主副本。即使此副本是 4.x 供应商的使用者，也必须将其配置为主副本。
2. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点和已复制后缀的节点，然后在此后缀下选择 “复制”节点。
3. 在右侧面板中，为此副本选择 “更改” > “启用 4.x 兼容性”。此外，还可以从 “对象”菜单中选择 “启用 4.x 兼容性”。
4. 在 “启用 4.x 兼容性”窗口中，指定旧版供应商服务器用来绑定的 “绑定 DN”和口令。还可以使用绑定 DN 的任意管理的条目，包括默认的复制管理员。有关绑定 DN 的详细信息，请参阅 “选择复制管理员”（第 242 页）。

   如果供应商要使用服务器的安全端口进行复制更新，则要输入服务器证书条目的 DN 才能使用安全验证。

5. 单击 “确定”。现在，此使用者副本已准备好接收旧版供应商的更新。
6. 确保 5.2 副本服务器上的模式可以定义将从 4.x 主副本复制的内容所使用的所有属性和对象类。
7. 通过导入在 4.x 主副本上创建的 LDIF 副本文件来初始化 5.2 副本。此文件中的第一个条目包含 4.x 复制机制所需的 `copiedfrom` 属性。

在服务器中启用 4.x 兼容性将配置默认安装的旧版复制插件。此插件将处理旧版供应商的更新，并在已复制后缀的内容中执行更新。

注意 只要启用了 4.x 兼容性，此副本就会为客户机的所有修改请求返回引荐。尽管 Directory Server 5.2 已配置为主副本，但它不会执行此后缀中的修改请求。反之，它会将引荐返回至 4.x 供应商服务器。

要完成旧版复制设置，现在必须配置旧版供应商以向 5.2 Directory Server 进行复制。有关在 4.x Directory Server 中配置复制协议的说明，请参阅随旧版 Directory Server 提供的文档。

更新 Directory Server 5.1 模式

在 Directory Server 5.2 中，模式文件 `11rfc2307.ldif` 已经更改为符合 RFC 2307 要求 (`http://www.ietf.org/rfc/rfc2307.txt`)。在 5.2 和 5.1 服务器之间配置或启用复制之前，必须更新 5.1 服务器上的模式。在服务器的这两个版本上，模式文件都位于 *ServerRoot*`/slapd-`*serverID*`/config/schema/` 下。

1. 将文件 `11rfc2307.ldif` 从 5.2 服务器复制到 5.1 服务器。

- 如果已经在 5.1 服务器上安装了 Solaris 软件包，则还必须删除过时的 `10rfc2307.ldif` 文件。
- 如果基于任何其他平台上在 5.1 服务器上安装了 zip 文件，则将覆盖现有的 `11rfc2307.ldif` 文件。

2. 以下模式文件将受此更改的影响，还必须从 5.2 服务器对其进行复制以覆盖 5.1 服务器上的现有文件：
    - `20subscriber.ldif`
    - `30ns-common.ldif`
    - `50ns-admin.ldif`
    - `50ns-certificate.ldif`

- 50ns-directory.ldif
- 50ns-legacy.ldif
- 50ns-mail.ldif
- 50ns-mlm.ldif
- 50ns-msg.ldif
- 50ns-netshare.ldif

3. 重新启动 5.1 服务器，然后继续配置复制和初始化副本。同步其他模式元素时，可能会复制服务器之间的某些模式属性，不过，对于复制机制而言，这属于正常行为。
4. 您可能需要更新依赖旧版本模式的任意应用程序。新的 11rfc2307.ldif 文件包括以下修改：
   - 删除了 automount 和 automountInformation 属性。
   - ipHost 对象类允许的属性的列表不再包括 o $ ou $ owner $ seeAlso $ serialNumer。
   - ieee802Device 对象类必填属性的列表不再包括 cn。
   - ieee802Device 对象类允许的属性的列表不再包括 description $ l $ o $ ou $ owner $ seeAlso $ serialNumber。
   - bootableDevice 对象类必填属性的列表不再包括 cn。
   - bootableDevice 对象类允许的属性的列表不再包括 description $ l $ o $ ou $ owner $ seeAlso $ serialNumber。
   - nisMap 对象类的 OID 现在是 1.3.6.1.1.1.2.9。

使用 Retro Change Log 插件

希望 Directory Server 5.2 主副本可以维护 4.x 型更改日志时，可以使用 retro change log 插件。有时，这对某些应用程序而言是必要的，如与 Directory Server 4.x 更改日志格式有相关性的 Sun ONE Meta Directory，因为它们从更改日志中读取信息。

Retro change log 插件不允许 Directory Server 5.2 成为旧版 4.x 使用者副本的供应商。仅支持 4.x 供应商的 Directory Server 5.2 使用者，如 “使用早期版本进行复制”（第 276 页）中所述。 Retro change log 插件操作与复制协议无关，对复制拓扑也没有影响。可以在单主部署方案中的任一台服务器中启用 retro change log 插件。在多主环境中插件可能不会正常工作，不应该在这种条件下启用该插件。

除保留在服务器的 5.2 更改日志中外， retro change log 还存储在特殊后缀 `cn=changelog` 下的其他数据库中。Retro change log 由单级条目组成。更改日志中的每个条目都有对象类 `changeLogEntry`，并可以包括下表中列出的属性。

表 8-2 Retro Change Log 条目的属性

属性	定义
`changeNumber`	该单值属性始终存在。它包含一个唯一标识各个更改的整数。此数值与更改发生的顺序相关。数值越大，更改时间越晚。
`targetDN`	此属性包含受 LDAP 操作影响的条目的 DN。如果是 `modrdn` 操作， `targetDN` 属性包含修改或移动操作前条目的 DN。
`changeTime`	此属性指定更改操作发生的时间。
`changeType`	指定 LDAP 操作的类型。该属性的值可能是下列之一：`add`、`delete`、 `modify` 或 `modrdn`。
`changes`	对于添加和修改操作，则包含对条目所作的更改 （LDIF 格式）。
`newRDN`	如果是 `modrdn` 操作，则指定条目的新 RDN。
`deleteOldRdn`	如果是 `modrdn` 操作，则指定是否已删除原 RDN。
`newSuperior`	如果是 `modrdn` 操作，则指定条目的 `newSuperior` 属性。

启用 Retro Change Log 插件

Retro change log 插件配置信息位于 `dse.ldif` 中的 `cn=Retro Changelog Plugin,cn=plugins,cn=config` 条目中。

要从 Directory Server 控制台中启用 retro change log 插件，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “插件”节点，并向下滚动以选择 “Retro Changelog Plugin”。
2. 在右侧面板中，选中 “启用插件”复选框，并单击 “保存”。要禁用该插件，请清除此复选框。

3. 启用或禁用插件后必须重新启动目录服务器。

要从命令行中启用 retro change log 插件，请执行以下操作：

1. 使用以下命令修改 retro change log 插件的配置条目：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=Retro Changelog Plugin,cn=plugins,cn=config
changetype:modify
replace:nsslapd-pluginenabled
nsslapd-pluginenabled:on
```

2. 重新启动服务器。有关重新启动服务器的信息，请参阅 “启动和停止 Directory Server”（第 20 页）。

修整 Retro Change Log

在指定的时间后，可以自动删除更改日志中的条目。要配置条目从更改日志中自动删除前所经历的时间，必须设置 `cn=Retro Changelog Plugin, cn=plugins, cn=config` 条目中的 `nsslapd-changelogmaxage` 配置属性。此属性仅可以从命令行设置，例如：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -p 口令
dn:cn=Retro Changelog Plugin,cn=plugins,cn=config
changetype:modify
replace:nsslapd-changelogmaxage
nsslapd-changelogmaxage:IntegerTimeunit
```

`nsslapd-changelogmaxage` 是具有以下格式的单值属性：

```
nsslapd-changelogmaxage:IntegerTimeunit
```

其中 *Integer* 代表一个数字， *TimeUnit* 可以为下列之一：`s` 表示秒、`m` 表示分钟、`h` 表示小时、`d` 表示天，`w` 表示星期。变量 *Integer* 和 *Timeunit* 之间不应该有空格，例如：

```
nsslapd-changelogmaxage:2d
```

更改日志的下次操作将修整 retro change log 。

访问 Retro Change Log

更改日志支持搜索操作。包括下列形式的过滤器时，搜索处于最佳状态：

```
(&(changeNumber>=X)(changeNumber<=Y))
```

作为一般规则，不应该在 retro change log 条目上执行添加或修改操作，但可以删除条目来减少更改日志的大小。仅在要修改默认访问控制策略时，才需要在 retro change log 中执行修改操作。

创建 retro change log 时，默认情况下将默认应用下列访问控制规则：

- 授予所有经过验证的用户 （`userdn=anyone`，不要与 `userdn=all` 匿名访问相混淆）对 retro change log 顶级条目 `cn=changelog` 的读取、搜索和比较权限。
- 不授予写入和删除权限，但隐式授予目录管理员的除外。

不应向匿名用户授予读取权限，因为更改日志条目中可能包含对敏感信息 （如口令）的修改。如果不允许经过验证的用户查看 retro change log 条目的内容，则您可能希望进一步限制对 retro change log 内容的访问。

要修改适用于 retro change log 的默认访问控制策略，您应该修改 `cn=changelog` 条目的 `aci` 属性。有关设置 `aci` 属性的详细信息，请参阅第 6 章 “管理访问控制”。

监控复制状态

可以使用新命令行工具以及 Directory Server 控制台来监控复制状态。

命令行工具

有三种新命令行工具用于监控复制部署：

- `repldisc` - “发现”并构造复制部署中所有已知服务器的一个列表。
- `insync` - 指示供应商与一个或多个使用者副本之间的同步状态。
- `entrycmp` - 比较两个或多个副本中的相同条目。

这些工具位于以下目录中：

ServerRoot`/shared/bin`

Sun ONE Directory Server 参考手册 第 1 章中的 “复制监控工具”给出了完整的命令行语法以及这些工具的使用示例。

复制状态标签

要查看 Directory Server 控制台中的复制状态摘要，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “状态”标签中选择 “复制”节点。

   右侧面板将显示一个表，包含为此服务器配置的每个复制协议的有关信息。

2. 如果要监控复制状态，请选中 “连续刷新”复选框。例如，您将会看到副本初始化何时结束。

3. 如果要确定尚未复制到使用者副本的上次主副本更改，请单击 “挂起的更改数目”按钮。您将获得一条警告信息，该操作可能需要很长时间并且需要确认。确定挂起更改号需要下载使用者副本的更新记录并和主副本的更改日志相比较。如果这些日志很大，该操作可能需要很长的时间和大量服务器资源。

4. 单击列标题并调整其大小，就可以修改表的布局。单击 “查看选项”按钮，并仅选择那些希望看到的列，还可以修改表的内容。下面的表 8-3 说明了要在表中显示的为服务器的每个协议所选择的复制参数。

表 8-3　Directory Server 控制台 “状态”标签中的复制参数

表标题	说明
后缀	指出被复制的后缀或子后缀。
远程副本	包含使用者服务器的主机名和端口。
说明	包含在该复制协议中提供的说明字符串。
状态	表示协议是否被禁用、初始化使用者或通过增加的更新正常复制。
概述	包含最新的事件 （初始化或更新的开始或结束）以及最新收到的消息。
发送更新	累积自从复制启用或服务器重新启动以来发送到使用者的独立更新的总量。
最后一个启动的更新	表示最近复制更新启动的时间。
最后一个结束的更新	表示最近复制更新结束的时间。
最后一条更新消息	提供最近复制更新的状态。
最后一条初始化消息	提供使用者的最近初始化状态。
最后一个启动的初始化	表示使用者副本开始的最近初始化时间。
最后一个结束的初始化	表示使用者副本结束的最近初始化时间。

解决常见复制冲突

多主复制使用松散一致性复制模式。这就意味着可在不同服务器上同时修改同一条目。当在两个服务器之间发送更新时，需要解决有冲突的更改内容。大多数情况下，根据与每台服务器上的更改相关联的时间标记，系统可以自动解决有冲突的更改。最近发生的更改具有优先权。

但有些情况下则需要人为干预来解决更改冲突问题，以便于解决问题。具有无法由复制过程自动解决的更改冲突的条目中包含作为冲突标记的操作属性 `nsds5ReplConflict`。

定期搜索包含此属性的条目以查找有冲突的条目。例如，可以使用下面的 `ldapsearch` 命令：

```
% ldapsearch -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
-b "dc=example,dc=com" "(nsds5ReplConflict=*)"
```

注意默认情况下会对 `nsds5ReplConflict` 属性编制索引。

解决命名冲突

在不同的服务器中使用相同的 DN 创建两个条目时，复制冲突解决机制将自动重新命名第二个创建的条目。每个目录条目包括操作属性 `nsuniqueid` 指定的唯一标识符，当发生命名冲突时，此唯一性 ID 将附加到非唯一性 DN 的后面。

如果后一个条目的创建时间早于第一台服务器向第二台服务器复制更改的时间，则可能会在两台服务器中创建具有相同 DN 的两个条目。例如，如果在两个主副本中同时创建条目 `uid=bjensen,ou=People,dc=example,dc=com`，则复制后这两个主副本都具有以下两个条目：

- `uid=bjensen,ou=People,dc=example,dc=com`
- `nsuniqueid=66446001-1dd211b2+uid=bjensen,dc=example,dc=com`

应该使用一种使其具有唯一性 DN 的方法对第二个条目进行重命名。可以删除冲突的条目并再次向它添加一个不冲突的名称。不过，最可靠的方法是创建条目时对其重命名。根据命名属性是单值还是多值，重命名过程会有所不同。下面分别说明每个过程。

重命名具有多值命名属性的条目

要重命名具有多值命名属性的冲突条目，请执行以下操作：

1. 使用该命名属性的新值重命名该条目，并保留原 RDN。例如：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令

dn:nsuniqueid=66446001-1dd211b2+uid=bjensen,dc=example,dc=com
changetype:modrdn
newrdn:uid=NewValue
deleteoldrdn: 0
^D
```

2. 删除命名属性和冲突标记属性的旧 RDN 值。例如：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令

dn:uid=NewValue,dc=example,dc=com
changetype:modify
delete:uid
uid:bjensen
-
delete:nsds5ReplConflict
^D
```

注意 修改 RDN 分两步完成，因为您不能删除唯一标识符属性 nsuniqueid。

重命名具有单值命名属性的条目

当命名属性是单值时，不能只将条目重命名为同一属性的另一个值。而必须临时执行以下操作：

1. 使用一个不同的命名属性重命名该条目，并保留旧 RDN。例如：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令

dn:nsuniqueid=66446001-1dd211b2+dc=HR,dc=example,dc=com
changetype:modrdn
newrdn:o=TempName
deleteoldrdn: 0
^D
```

2. 删除命名属性和冲突标记属性的旧 RDN 值。例如：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令

dn:o=TempName,dc=example,dc=com
changetype:modify
replace:dc
dc:uniqueValue
-
delete:nsds5ReplConflict
^D
```

注意 修改 RDN 分两步完成，因为您不能删除唯一标识符属性 nsuniqueid。

3. 用要使用的命名属性的新的不冲突值对条目进行重命名。例如：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令

dn:o=TempName,dc=example,dc=com
changetype:modrdn
newrdn:dc=uniqueValue
deleteoldrdn: 1
^D
```

通过将 deleteoldrdn 属性的值设置为 1，可以删除临时属性值对 o=*TempName*。如果要保留此属性，可以将 deleteoldrdn 属性的值设置为 0。

解决孤条目冲突

复制删除操作时，如果使用者服务器发现要删除的条目有子条目，冲突解决过程就会创建一个紧附条目，以避免目录中出现孤条目。

同样，复制添加操作时，如果使用者服务器找不到父条目，冲突解决过程就会创建一个代表父条目的紧附条目，以便使新条目不是孤条目。

紧附条目是包含对象类 glue 和 extensibleObject 的临时条目。创建紧附条目的方式有以下几种：

- 如果冲突解决过程发现已删除条目具有匹配的唯一标识符，则紧附条目就是该条目的再生条目，并且还具有 glue 对象类和 nsds5ReplConflict 属性。

  在这种情况下，可以修改紧附条目以删除 glue 对象类和 nsds5ReplConflict 属性，从而将条目保持为常规条目，或者可以删除紧附条目及其子条目。

- 服务器将创建具有 glue 和 extensibleObject 对象类的最小条目。

  在这种情况下，必须修改条目以使其具有一定的意义，或者删除该条目及其所有子条目。

解决潜在的互操作问题

若要与依赖属性唯一性的应用程序（例如邮件服务器）实现互操作性，可能需要对包含 nsds5ReplConflict 属性的条目进行访问限制。如果不限制对这些条目的访问，则仅需要一个属性的应用程序将同时选择原始条目和包含 nsds5ReplConflict 的冲突解决条目，并导致操作失败。

要限制访问，需要使用下列命令修改授予匿名读取访问权限的默认 ACI：

```
ldapmodify -h 主机名 -D "cn=Directory Manager" -w 口令
```

```
dn:dc=example,dc=com
changetype:modify
delete:aci
aci:(target ="ldap:///dc=example,dc=com")
 (targetattr !="userPassword"
 (version 3.0;acl "Anonymous read-search  access";
 allow (read, search, compare)(userdn = "ldap:///anyone");)
-
add:aci
aci:(target="ldap:///dc=example,dc=com")
 (targetattr!="userPassword")
 (targetfilter="(!(nsds5ReplConflict=*))")(version 3.0;acl
 "Anonymous read-search access";allow (read, search, compare)
 (userdn="ldap:///anyone");)
^D
```

新 ACI 从搜索结果中过滤出所有包含 nsds5ReplConflict 属性的条目。

第 9 章

扩展目录模式

Sun ONE Directory Server 具有标准模式，该模式包括数百个对象类和属性。虽然标准对象类和属性应该能够满足您的大多数要求，但可能还需要创建新对象类和属性以扩展模式。

本章在以下小节中介绍如何扩展模式：

- 模式检查
- 扩展模式概述
- 管理属性定义
- 管理对象类定义
- 复制模式定义

模式检查

当模式检查处于打开状态时， Directory Server 可确保所有的导入、添加和修改操作符合当前定义的目录模式：

- 每个条目的对象类和属性都符合模式。
- 条目包含其所有已定义对象类的全部必需的属性。
- 条目仅包含其对象类允许的属性。

注意 修改条目时， Directory Server 对整个条目执行模式检查，而不仅仅是对正被修改的属性进行检查。因此，如果条目中任何对象类或属性不符合模式要求，则操作可能会失败。

Directory Server 中，模式检查默认情况下为打开状态。运行 Directory Server 时，模式检查始终应为打开状态。许多客户机应用程序认为模式检查为打开状态表示所有条目都符合模式。

不过，打开模式检查并不会验证目录中的现有内容。要保证所有目录内容符合模式的唯一办法就是在添加任意条目或重新初始化所有条目之前打开模式检查。

唯一的例外情况是加速已知符合模式的 LDIF 文件的导入操作，此时模式检查可能要关闭。不过，始终存在导入不符合模式的条目的风险，并且检测不到此风险。

当某个条目不符合模式时，将无法搜索到此条目，并且修改此条目的操作也将失败。要使条目符合模式，必须执行以下操作：

1. 如果服务器处于生产环境，您可能希望首先将整个服务器置于只读状态，以防止模式检查为关闭状态时对其进行任何修改。请参阅 “设置全局只读模式”（第 34 页）。
2. 请按照下面的步骤关闭模式检查。
3. 检索条目并手动将此条目与当前定义的模式进行比较，以确定条目不符合模式的原因。请参阅 “查看属性”（第 293 页）和 “查看对象类”（第 297 页）。
4. 修改条目以使其符合模式。

   如果有多个不符合模式的条目，并且这些条目代表了数据的一种模式或新格式，则应改为考虑修改模式。不过，应该在部署前计划模式以尽量减少对模式的更改。详细信息，请参阅 *Sun ONE Directory Server 部署指南* 中第 3 章 “设计模式”。
5. 请按照下面的步骤打开模式检查。
6. 如果已启用全局只读模式，请取消设置。

使用控制台设置模式检查

1. 在 Directory Server 控制台的顶级 “配置”标签中，选择配置树中的模式节点。

   右侧面板包含了模式的定义。
2. 面板顶部的状态消息指示当前模式检查处于启用还是禁用状态。单击右侧的按钮以切换模式检查的关闭或打开状态：

   - 该按钮被标为 “禁用”以关闭模式检查。
   - 当可以打开模式检查时，该按钮将标为 “启用”。

   新的模式检查策略将立即有效。

从命令行设置模式检查

还可以通过设置 cn=config 条目的 nsslapd-schemacheck 属性来打开和关闭模式检查：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=config
changetype:modify
replace:nsslapd-schemacheck
nsslapd-schemacheck:on 或 off
```

服务器将立即实施新模式检查策略。

扩展模式概述

向模式添加新属性时，必须创建新对象类以包含这些属性。虽然仅向现有的对象类（已包含所需的大多数属性）添加所需的属性看起来很方便，但这样操作会损坏与 LDAP 客户机的互用性。

Directory Server 与现有 LDAP 客户机的互用性依赖于标准 LDAP 模式。如果更改标准模式，升级服务器时同样会出现困难。基于同样的理由，不能删除标准模式元素。

有关对象类、属性和目录模式的详细信息，以及扩展模式的指导说明，请参阅 *Sun ONE Directory Server 部署指南* 中的第 3 章“设计模式”。有关标准属性和对象类的信息，请参阅 *Sun ONE Directory Server 参考手册* 中的第 4 部分 “Directory Server 模式”。

Directory Server 模式存储于目录的 cn=schema 条目的属性中。与配置条目相似，这是服务器启动期间从文件读取的模式的 LDAP 视图。模式文件是 LDIF 文件，位于：

ServerRoot/slapd-*serverID*/config/schema

此目录包含 Directory Server 和其他依赖 Directory Server 的 Sun ONE 服务器所使用的标准模式的文件。 *Sun ONE Directory Server 参考手册* 中的第 9 章“Directory Server 5.2 所支持的模式”对这些文件进行了说明。*Sun ONE Directory Server 参考手册* 中第 10 章“对象类参考”和第 11 章“属性参考”对标准模式进行了说明。

修改模式文件

模式文件只能在启动时由服务器读取一次。文件的 LDIF 内容将被添加至 cn=schema 中模式的内存 LDAP 视图。因为模式定义的顺序非常重要，因此模式文件名是以数字作为前缀，并按字母数字顺序加载。只有安装期间定义的系统用户才可以向目录中的模式文件写入。

要修改文件中的模式定义，必须创建或修改希望的文件，然后重新启动服务器。RFC 2252 (http://www.ietf.org/rfc/rfc2252.txt) 对模式文件中的语法定义进行了说明。

在 LDIF 文件中直接定义模式时，一定不要使用 X-ORIGIN 字段的值 'user defined'。此值是为通过 cn=schema 的 LDAP 视图定义且出现在 99user.ldif 中的模式元素所保留。

文件 99user.ldif 包含 cn=schema 条目的附加 ACI，以及从命令行或使用控制台添加的所有模式定义。添加新的模式定义时，文件 99user.ldif 将被改写。如果要修改此文件，必须立即重新启动服务器以确保所做更改具有永久性。

不应该修改在其他模式文件中定义的标准模式。不过，可以添加新文件以定义新的属性和对象类。例如，要在多台服务器中定义新模式元素，应该在一个名为 98mySchema.ldif 的文件中定义这些模式元素，并将此文件复制到所有服务器的模式目录。然后，必须重新启动所有服务器以加载新的模式文件。

从命令行修改模式

因为模式是由 cn=schema 中的 LDAP 视图定义的，所以可以使用 ldapsearch 和 ldapmodify 公用程序联机查看和修改模式。不过，只能修改 X-ORIGIN 字段的值为 'user defined' 的模式元素。服务器将拒绝修改其他定义。

使用 ldapmodify 可以添加和删除 attributeTypes 和 objectClasses 属性的单个值。要修改其中一个值，必须删除该值，然后将其作为新值添加，因为这些属性为多值 （请参阅 “修改多值属性的值”（第 64 页）。）必须使用 RFC 2252 (http://www.ietf.org/rfc/rfc2252.txt) 中说明的语法来定义模式元素。

任何新元素定义及对用户定义元素的更改都将保存在 99user.ldif 文件中。

从命令行修改模式定义很容易出错，因为需要您准确地输入位数多的长值。不过，在需要更新目录模式的脚本中可能会用到此功能。

使用控制台修改模式

定制目录模式的建议方法是使用以下几节中说明的 Directory Server 控制台界面。控制台允许您查看标准模式，并提供一个图形界面，用于定义新的属性和对象类以及编辑已定义的元素。

再重复一遍，任何新元素定义及对用户定义元素的更改都将保存在 `99user.ldif` 文件中。

要扩展目录模式，应该按以下顺序执行操作：

1. 首先如 “创建属性”（第 295 页）中所述创建新属性。
2. 然后创建一个对象类以包含新属性，并将属性添加至对象类。有关信息，请参阅 “创建对象类”（第 297 页）。

管理属性定义

Directory Server 控制台提供一个界面，以查看模式中的所有属性，并可以创建、编辑和删除您自身的属性定义。

查看属性

要查看有关目录模式中当前存在的所有属性的信息，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中，选择配置树中的 “模式”节点，然后在右侧面板中选择 “属性”标签。

   该标签包含各种表格，这些表格列出模式中的所有标准 （只读）属性和用户定义的属性。将鼠标放到表格的某一行，将显示相应属性的说明字符串。

   以下表格说明属性表格的字段。

表 9-1 “属性”标签中的表格列

列标题	说明
名称	属性的名称 （有时称为类型）。
OID	属性的对象标识符。 OID 是一个字符串 （通常由带点的十进制数构成），它唯一标识模式对象。 有关 OID 的详细信息，或者想为企业申请前缀，请向 IANA （Internet 分配号码机构）发邮件，地址是 `iana@iana.org`；也可访问 IANA 网站 `http://www.iana.org/`。

表 9-1 “属性”标签中的表格列 （续）

列标题	说明
语法	语法说明允许的属性值格式，可能的语法已列在表 9-2 （第 294 页）中。
多值	此列中的复选框指定属性是否为多值。多值属性可在条目中出现任意次，但单值属性可能仅出现一次。

表 9-2 属性语法定义

语法名称	定义
二进制 （以前的 bin）	表明该属性的值被视作二进制数据。
布尔型	表明该属性仅拥有两个值中的一个：True 或 False。
国家 （地区）字符串	表明该属性的值限制为两个字母的国家 （地区）代码 （由 ISO 3166 指定），例如 FR。
DN （以前的 dn）	表明该属性的值是 DN （标识名称）。
DirectoryString （以前的 cis）	表明该属性的值可能包含任意 UTF-8 编码字符，并且不区分大小写。
GeneralizedTime	表明该属性的值已被编码为可印刷的字符串。必须指定时区。强烈建议您使用 GMT。
IA5String （以前的 ces）	表明该属性的值可能仅包含 ASCII 字符的子集，并且区分大小写。
整型 （以前的 int）	表明该属性的有效值为数字。
OctetString	和二进制的行为相同。
通讯地址	表明该属性的值被编码为 *dstring*[$ *dstring*]* 其中，每个 *dstring* 组件编码为具有 DirectoryString 语法的值。*dstring* 中的反斜线符号和美元字符必须加上引号，以免被误认为行分隔符。许多服务器通讯地址限制为 6 行，字符限制上限为 30。例如： 1234 Main St.$Anytown, CA 12345$USA
TelephoneNumber （以前的 tel）	表示该属性的值为电话号码形式。建议使用国际形式的电话号码。

表 9-2　属性语法定义 （续）

语法名称	定义
URI	表明该属性的值包含一个 URL （带有一个可选前缀），如 `http://`、`https://`、`ftp://`、`ldap://` 或 `ldaps://`。URI 值的行为与 IA5String 相同 （请参阅 RFC 2396，`http://www.ietf.org/rfc/rfc2396.txt`。）

创建属性

要向模式添加您自身的属性定义，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中，选择配置树中的 “模式”节点，然后在右侧面板中选择 “属性”标签。
2. 单击 “创建”以显示 “创建属性”对话框。
3. 在文本字段中输入以下信息以定义新属性。只有属性名称和语法是必须填写的：
   - 属性名称 - 输入属性的唯一名称，也称为属性类型。属性名称必须以字母开头，并且只能包含 ASCII 字母、数字和连字符。

注意　属性名称可以包含大写字母，但没有 LDAP 客户机会依赖这些字母进行识别。必须按照 RFC 2251 (`http://www.ietf.org/rfc/rfc2251.txt`) 4.1.4 小节的说明，以不区分大小写的方式来处理属性名称。

   - 属性 OID （可选） - 输入属性的对象标识符。在表 9-1 （第 293 页）中对 OID 进行了说明。如果不指定 OID， Directory Server 将自动使用 *attributeName*`-oid`。请注意，为了严格遵从 LDAP v3，必须提供一个有效的数字 OID。
   - 属性别名 （可选） - 在以逗号分隔的列表中输入属性的备用名称。
   - 属性说明 （可选） - 输入简短的说明文字以说明属性的用途。
   - 语法 - 从下拉列表中选择一个说明属性所要包含数据的语法。在表 9-2（第 294 页）中对可供使用的语法进行了说明。
   - 多值 - 默认情况下，属性将为多值。如果属性的每个条目最多只能有一个值，则请取消选中该复选框。

4. 在 “创建属性”对话框中单击 “确定”以定义新属性。该属性将出现在用户定义属性的表格中。

   在目录条目中定义该属性的值之前，必须创建或编辑需要或允许此属性的对象类，如 “管理对象类定义”（第 297 页）中所述。

编辑属性

使用控制台只能编辑用户定义的属性。在修改属性的名称、语法和多值定义之前，必须确保目录中的条目当前未使用此属性，否则客户机将不能访问该条目。

要修改属性的模式定义，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中，选择配置树中的 “模式”节点，然后在右侧面板中选择 “属性”标签。
2. 在 “用户定义的属性”表格中，选择要编辑的属性，然后单击 “编辑”。
3. 修改 “编辑属性”对话框的字段以重新定义属性。

   如果 OID 字符串基于属性名称，则每次更改名称时，都应该更改 OID。在表 9-1（第 293 页）中对 OID 进行了说明。在表 9-2（第 294 页）中对可供使用的语法进行了说明。
4. 完成对属性的编辑后，请单击 “确定”保存更改。

删除属性

使用控制台只能删除用户定义的属性。在删除属性定义之前，必须确保目录中的条目当前未使用此属性，否则客户机将不能访问该条目。

要删除属性的模式定义，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中，选择配置树中的 “模式”节点，然后在右侧面板中选择 “属性”标签。
2. 在 “用户定义的属性”表格中，选择该属性，然后单击 “删除”。
3. 提示您删除时请进行确认。

   服务器将立即删除属性定义。条目删除后不可恢复。

管理对象类定义

Directory Server 控制台还提供一个界面，可以查看模式中的所有对象类，并可以创建、编辑和删除您自身的对象类定义。

查看对象类

要查看有关目录模式中当前定义的所有对象类的信息，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中，选择配置树中的 “模式”节点，然后在右侧面板中选择 “对象类”标签。

   该标签包含的列表列出了模式中的所有标准 （只读）对象类和用户定义的对象类。

2. 选择要在任一列表中查看的对象类。

   此标签中的其他字段显示了有关所选对象类的以下信息：

表 9-3 “对象类”标签的字段

字段	说明
必需的属性	包含必须出现在使用该对象类的条目中的一组属性。该列表包括继承的属性。
允许的属性	包含可能出现于使用该对象类的条目中的一组属性。该列表包括继承的属性。
父对象类	父对象类标识对象类从中继承其属性和结构的对象类。对象类自动从其父对象类继承必需属性和允许属性。
OID	对象类的对象标识符。OID 是一个字符串 （通常由带点的十进制数构成），它唯一标识模式对象。 有关 OID 的详细信息，或者想为企业申请前缀，请向 IANA （Internet 分配号码机构）发邮件，地址是 `iana@iana.org`；也可访问 IANA 网站 `http://www.iana.org/`。

创建对象类

如果要创建互相继承的若干对象类，必须首先创建父对象类。如果新对象类要使用自定义属性，还必须首先定义这些自定义属性。

注意 控制台仅允许创建结构对象类。这些对象类都必须继承父对象类。要定义辅助对象类和抽象对象类，必须使用命令行公用程序。

要向模式添加您自身的对象类定义，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签中，选择配置树中的 “模式”节点，然后在右侧面板中选择 “对象类”标签。
2. 单击 “创建”以显示 “创建对象类”对话框。
3. 在文本字段中输入以下信息，以定义新对象类：
   - 名称 - 输入对象类的唯一名称。
   - 父条目 - 选择要作为父对象类的现有对象类。默认情况下，将选定 `top` 且必须用作父对象类 （如果对象类没有从其他任何对象类继承）。从父对象类继承的必需属性和允许属性及其父对象类将显示在相应的列表中。

     通常，如果要添加用户条目的新属性，则父对象类将是 `inetOrgPerson` 对象类。如果要添加公司条目的新属性，父对象类通常为 `organization` 或 `organizationalUnit`。如果要添加组条目的新属性，父对象类通常为 `groupOfNames` 或 `groupOfUniqueNames`。
   - OID （可选） - 输入属性的对象标识符。在表 9-3 （第 297 页）中对 OID 进行了说明。如果不指定 OID， Directory Server 将自动使用 *objectClassName*`-oid`。请注意，为了严格遵从 LDAP v3，必须提供一个有效的数字 OID。
4. 定义使用新对象类的条目要包含的属性：
   - 要定义必须出现的属性，请在 “可用属性”列表中选择一个或多个属性，然后单击 “必需的属性”框左侧的 “添加”按钮。
   - 要定义可能出现的属性，请在 “可用属性”列表中选择一个或多个属性，然后单击 “允许的属性”框左侧的 “添加”按钮。
   - 要删除先前添加的属性，可在上述任一列表中突出显示该属性，然后单击相应的 “删除”按钮。不能删除从父对象类继承而来的允许属性或必需属性。
5. 在 “创建对象类”对话框中单击 “确定”以定义新对象类。新对象类将出现在用户定义的对象类表格中，现在您可以定义具有此对象类的条目。

编辑对象类

使用控制台只能编辑用户定义的对象类。在修改对象类的定义之前，必须确保目录中当前没有使用此对象类的条目，否则客户机将不能访问该条目。

要修改对象类的模式定义，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置” 标签中，选择配置树中的 “模式” 节点，然后在右侧面板中选择 “对象类” 标签。
2. 从 “用户定义的对象类” 列表中，选择要编辑的对象类，然后单击 “编辑”。
3. 修改 “编辑对象类” 对话框的字段以重新定义对象类。

   不能重命名对象类，也不能更改其 OID。要修改上述内容，请删除此对象类并创建一个新对象类。

   - 父条目 - 选择要作为父对象类的现有对象类。从父对象类中继承的必需属性和允许属性及其父对象类将显示在相应的列表中。
   - 要定义必须出现的属性，请在 “可用属性” 列表中选择一个或多个属性，然后单击 “必需的属性” 框左侧的 “添加” 按钮。
   - 要定义可能出现的属性，请在 “可用属性” 列表中选择一个或多个属性，然后单击 “允许的属性” 框左侧的 “添加” 按钮。
   - 要删除先前添加的属性，可在上述任一列表中突出显示该属性，然后单击相应的 “删除” 按钮。不能删除从父对象类继承而来的允许属性或必需属性。
4. 完成对象类的编辑后，请单击 “确定” 保存更改。

删除对象类

使用控制台只能删除用户定义的对象类。在删除对象类定义之前，必须确保目录中当前没有使用此对象类的条目，否则客户机将不能访问该条目。

要删除对象类的模式定义，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置” 标签中，选择配置树中的 “模式” 节点，然后在右侧面板中选择 “对象类” 标签。
2. 在用户定义的对象类列表中，选择对象类名称，然后单击 “删除”。
3. 提示您删除时请进行确认。

   服务器将立即删除对象类定义。条目删除后不可恢复。

复制模式定义

不论何时配置两个服务器间一个或多个后缀的复制，也将自动复制模式。这将确保所有副本都有一个完整、相同的模式，此模式定义可能复制到使用者的所有对象类和属性。因此，主副本服务器也包含主模式。

要在所有副本上实施模式，必须在所有的主副本上启用模式检查。因为在执行 LDAP 操作的主副本上执行模式检查，所以更新使用者副本时不需要检查模式。为提高性能，复制机制将避开对使用者副本进行模式检查。

注意 不应该在集线器副本和专门的客户副本中关闭模式检查。模式检查对使用者没有性能影响，应该使其保持打开状态，以表示副本内容符合其模式。

使用者初始化期间以及不论何时通过控制台或命令行工具修改模式，主副本服务器会将模式自动复制到其使用者。默认情况下将复制整个模式，并且创建使用者中还不存在的任何其他模式元素，并将其存储在 `99user.ldif` 文件中。

例如，假设启动时主副本服务器在 `98mySchema.ldif` 文件中包含模式定义，然后您定义了与其他服务器（可能为主副本服务器、集线器服务器或专门的客户服务器）之间的复制协议。随后从主副本服务器中初始化副本时，已复制的模式将包含 `98mySchema.ldif` 中的定义，但它们将存储在副本服务器的 `99user.ldif` 中。

使用者初始化期间复制模式后，在主副本的 `cn=schema` 中修改模式也会将整个模式复制到使用者。因此，通过命令行公用程序或控制台对主副本模式所作的任何修改都将被复制到使用者副本。这些修改将被存储在主副本的 `99user.ldif` 中，通过上面所述的相同机制，这些修改也将被存储在使用者副本的 `99user.ldif` 中。

修改已复制的模式文件

复制机制无法检测到对包含模式的 LDIF 文件直接进行的任何更改。因此，如果按照 “修改模式文件”（第 292 页）中的说明更新模式，即使重新启动主副本服务器后，所做的更改也不会复制到使用者副本中。

Directory Server 5.2 提供了以下脚本，用来将模式文件中的更改 “推送”至使用者副本：

Windows 平台

```
cd ServerRoot
bin\slapd\admin\bin\perl slapd-serverID\schema_push.pl
```

其他安装

```
# ServerRoot/slapd-serverID/schema_push.pl
```

请使用以下步骤在主副本服务器上修改模式文件：

1. 在模式目录中添加新模式文件或修改现有模式文件：

   ServerRoot/slapd-*serverID*/config/schema

   只有安装期间定义的系统用户才可以向目录中的模式文件写入。详细信息，请参阅 “修改模式文件”（第 292 页）。

2. 使用上面给出的适当命令运行 schema_push.pl 脚本。该脚本并不是真的向副本“推送”模式，而是将一个特殊属性写入模式文件，这样加载模式文件后，即会对其进行复制。

3. 重新启动服务器。服务器将加载所有模式文件，复制机制会将新模式复制到其使用者副本。

限制模式复制

默认情况下，不论何时复制机制复制模式，都会将整个模式发送至使用者副本。有两种情况不希望出现上述情形：

- 使用控制台或从命令行对 cn=schema 进行修改仅限于用户定义的模式元素，所有标准模式都不会更改。如果经常修改模式，每次发送大量未更改的模式元素将会影响性能。可以通过仅复制用户定义的模式元素来提高复制性能和服务器性能。
- Directory Server 5.2 的主副本服务器向 Directory Server 5.1 的使用者服务器进行复制时，这些版本的配置属性的模式是不同的，并会产生冲突。这种情况下，必须仅复制用户定义的模式元素，如下所述。

使用以下命令来限制模式复制，从而仅复制用户定义的模式：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=config
changetype:modify
replace:nsslapd-schema-repl-useronly
nsslapd-schema-repl-useronly:on
```

如果需要， off 默认值将使整个模式被复制。

第 10 章

管理索引

与书的索引一样，Directory Server 通过将搜索字符串与对目录内容的参考相关联来加速搜索过程。索引是属性值构成的表，它们存储在单独的数据库文件中。目录中的每个后缀都会单独创建索引，并进行管理。在后缀配置中创建索引后，服务器即会自动维护索引。

有关索引及其利弊的简介、`nsslapd-allidsthreshold` 属性的说明以及如何提高 Directory Server 性能的说明，请参阅 *Sun ONE Directory Server 安装和调整指南* 中的第 7 章 “调整索引”。

本章包含以下小节：

- 索引概述
- 管理索引
- 管理浏览索引

索引概述

在相关数据库目录中以文件方式为每个后缀存储索引。每个索引文件包含后缀中为给定属性定义的所有索引。例如，所有为通用名 (`cn`) 属性维护的索引均存储在 *databaseName*`_cn.db3` 文件中。

初始化后缀或使用本章中所述的命令时会创建索引文件。在客户机搜索操作和内部操作过程中，服务器会访问索引以更快地在目录中查找条目。在修改操作过程中，目录必须更新目录内容，并通过更新索引文件来维护索引。

Directory Server 支持下列索引类型：

- 出现索引 (`pres`) - 列出了具有特定属性的条目，与属性的值无关。
- 等式索引 (`eq`) - 使您能够高效地搜索包含特定属性值的条目。

- 近似索引 (approx) - 通过使用 ~= 过滤运算符提供了高效的 “音似”搜索功能。例如，近似索引对于搜索部分名称或拼错的名称很有用。 Directory Server 使用变音位语音算法的一个变体来执行近似索引搜索。

  注意 Directory Server 5.2 中的变音位语音算法仅支持 US-ASCII 字母。因此，近似索引只能用于英语值。

- 子串索引 (sub) - 提供高效的属性值子字符串搜索，如 cn=*john*。这种索引的维护成本很高，因为每个值都有许多可能的子字符串。

  子字符串索引中每个条目的字符数不能少于两个。

- 匹配规则索引 - 通过将本地化的匹配规则 （也称为排序顺序）的 OID 与要索引的属性相关联，以加快在国际目录中的搜索速度。

- 浏览索引 - 缩短在使用虚拟列表视图 (VLV) 控件执行搜索时的响应时间。可以在目录树中任意的分支点上创建浏览索引，以便提高那些密集填充的子树 （例如 ou=People,dc=example,dc=com）的显示性能。

系统索引

系统索引是那些不能被删除或修改的索引。它们是 Directory Server 正常、有效地运作所必需的。下表列出了每个后缀中自动创建的系统索引：

表 10-1 每个后缀中的系统索引

属性	Eq	Pres	目的
aci		X	允许 Directory Server 迅速获取目录中维护的访问控制信息。
entrydn	X		加快基于 DN 搜索的条目检索。
nsUniqueId	X		用于搜索特定条目。
nscpEntryDN	X		Directory Server 内部使用，用于复制。
nsds5ReplConflict	X	X	用于帮助查找复制冲突。
numsubordinates		X	Directory Server 控制台 用来增强 “目录”标签上的显示性能。
objectClass	X		用来帮助加快目录中的子树搜索速度。
parentID	X		增强单级搜索期间的目录性能。

默认索引

在目录中创建新后缀时，服务器在相应的数据库目录中配置一组默认的索引。可以根据索引编制的需要对默认索引进行修改，但在解除索引配置之前，应该确保企业中没有任何服务器插件或者其他服务器依赖于该已编制索引的属性。

要修改创建新后缀时将使用的默认索引集，请参阅 “修改默认索引集”（第 313 页）。

下表列出了 Directory Server 中预配置的默认索引：

表 10-2　每个新后缀中的默认索引

属性	Eq	Pres	Sub	目的
cn	X	X	X	提高最常用的用户目录搜索类型的性能。
givenName	X	X	X	提高最常用的用户目录搜索类型的性能。
mail	X	X	X	提高最常用的用户目录搜索类型的性能。
mailAlternateAddress	X			由 Sun ONE Messaging Server 使用。
mailHost	X			由 Sun ONE Messaging Server 使用。
member	X			提高 Sun ONE 服务器的性能。引荐完整性插件也使用该索引。详细信息，请参阅 “维护引荐完整性”（第 73 页）。
nsCalXItemId	X	X	X	由 Sun ONE Calendar Server 使用。
nsLIProfileName	X			由 Sun ONE Messaging Server 的漫游功能使用。
nsRoleDN	X			提高基于角色的操作的性能。
nswcalCALID	X			由 Sun ONE Calendar Server 使用。
owner	X			提高 Sun ONE 服务器的性能。引荐完整性插件也使用该索引。详细信息，请参阅 *Sun ONE Directory Server 管理指南*。
pipstatus	X			由 Sun ONE Servers 使用。
pipuid		X		由 Sun ONE Servers 使用。
seeAlso	X			提高 Sun ONE 服务器的性能。引荐完整性插件也使用该索引。详细信息，请参阅 “维护引荐完整性”（第 73 页）。
sn	X	X	X	提高最常用的用户目录搜索类型的性能。
telephoneNumber	X	X	X	提高最常用的用户目录搜索类型的性能。

表 10-2 每个新后缀中的默认索引 （续）

属性	Eq	Pres	Sub	目的
uid	X			提高 Sun ONE 服务器的性能。
uniquemember	X			提高 Sun ONE 服务器的性能。引荐完整性插件也使用该索引。详细信息，请参阅 “维护引荐完整性”（第 73 页）。

数据库中的标准索引文件

由于维护默认索引和其他内部索引机制的需要， Directory Server 还维护特定的标准索引文件。默认情况下存在以下标准索引。所以无需再生成它们：

- *databaseName*_id2entry.db3 - 包含目录条目的实际数据库。所有其他的数据库文件都可以由它来重建。
- *databaseName*_id2children.db3 - 限制单级搜索的范围，所谓单级搜索是指检查某个条目的直接子条目的搜索。
- *databaseName*_dn.db3 - 控制子树搜索的范围，所谓子树搜索是指检查某个条目以及它下面的子树中所有条目的搜索。
- *databaseName*_dn2id.db3 - 通过将某个条目的标识名称映射到它的 ID 来有效地开始所有的搜索。

属性名称快速参考表

下表列出了具有主名称或真实名称，以及别名的所有属性。创建索引时，请务必使用主名称。

表 10-3 主属性名称及其别名

主属性名称	属性的别名
authorCn	documentAuthorCommonName
authorSn	documentAuthorSurname
c	countryName
cn	commonName
co	friendlyCountryName
dc	domainComponent

表 10-3　主属性名称及其别名

主属性名称	属性的别名
dn	distinguishedName
drink	favoriteDrink
facsimileTelephoneNumber	fax
l	localityName
labeledUri	labeledUrl
mail	rfc822mailbox
mobile	mobileTelephoneNumber
o	organizationName
ou	organizationalUnitName
pager	pagerTelephoneNumber
sn	surname
st	stateOrProvinceName
street	streetAddress
ttl	timeToLive
uid	userId

管理索引

本节说明如何利用 Directory Server 控制台和命令行来为特定的属性创建和删除出现、等式、近似、子字符串和国际索引。请参阅 “管理浏览索引”（第 314 页）以了解进行虚拟列表视图 (VLV) 操作前所需的单独步骤。

注意　因为索引对每个后缀都是特定的，所以需要记住在每个后缀配置中都创建新索引。

使用控制台创建新后缀时，可以选择复制现有后缀的索引配置。

创建新的索引之前，请权衡由使用索引产生的利与弊。敬请牢记：

- 近似索引不应该用于那些通常包含数字的属性 （如电话号码），因为它们在处理此类属性时的效率不高。

- 子字符串索引不能用于二进制属性。等式索引不应用于很大的值，如计划包含二进制数据的属性，例如 `jpegPhoto`。
- 索引的维护需要很多资源，所以应该只为那些经常搜索的属性编制索引。条目的创建将需要更多的 CPU 时间，因为服务器必须检查所有已编制索引的属性，并为新条目中所包含的每个属性生成新的条目。
- 每个索引文件的大小都与目录的内容成正比。
- 在搜索请求中仍然可以指定未编制索引的属性，但其搜索性能无法与已编制索引的搜索相提并论，这还要取决于搜索的类型。

使用控制台管理索引

如果计划在很多属性上修改或添加索引，则应首先将后缀设为只读，然后将其内容导出到 LDIF。这样通过从 LDIF 文件重新初始化后缀将加快后缀的重新索引。

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点，并选择要索引的后缀。然后在右侧面板中，选择 “索引”标签。

   不能修改 “系统索引”表。在 “附加索引”表中，添加、修改或删除属性的索引。

2. 要在一个仍未索引的属性上添加索引，请单击 “添加属性”按钮。在显示的对话框中，选择一个或多个属性编制索引，并单击 “确定”。

   新属性显示在 “附加索引”表中。

3. 要修改属性的索引，请选中或取消选中想在 “附加索引”表中为该属性维护的每种索引类型的复选框。

4. 如果想要创建一个包含非英语值的属性的索引，请在 “匹配规则”字段中输入想要使用的排序顺序的 OID。

   通过列举多个由逗号分隔的 OID （而不是空格），您可以使用多种语言来为属性编制索引。有关受支持的区域和其相关排序顺序的 OID 的列表，请参阅 *Sun ONE Directory Server 参考手册* 中的附录 C “目录国际化”。

5. 要删除一个属性的所有索引，请在表中选择它所在的行并单击 “删除属性”按钮。

6. 单击 “保存”，保存新索引配置。

   如果删除了一个属性的所有索引，服务器将删除该属性的索引文件并结束配置。如果修改了属性的索引或添加了一个新索引，请继续执行以下步骤。

7. 警告对话框通知您必须更新数据库文件以开始使用新索引。您可重新索引后缀或重新初始化后缀。

- 如果仅添加或修改了一个或两个索引，或后缀必须可用，则应重新索引后缀。单击“重新索引后缀”按钮，显示重新索引对话框。默认情况下，会选定您修改过或添加到索引配置中的属性。单击“确定”，开始重新编制这些属性的索引。重新为带有数百万条条目的目录编制许多属性的索引可能花费数小时的时间，但是重新编制索引期间后缀将始终保持联机。
- 如果添加或修改多个属性的索引，且从此后缀导出了最近的 LDIF 文件，请单击“初始化后缀”按钮。在“初始化后缀”对话框中，输入或浏览到 LDIF 文件的路径和名称，然后单击“确定”。服务器将从 LDIF 文件重新初始化后缀，并根据新的配置创建所有索引。根据目录大小的具体情况，重新初始化后缀通常比重新编制两个或更多属性的索引要快，但是后缀在初始化过程中不可用。
- 如果不重新初始化后缀或重新索引后缀，则所有数据将仍然可用，但是将不会创建新的索引，也不会提高目录访问性能。

如果重新初始化后缀或重新索引后缀，对您添加的所有新数据以及目录中现有的数据，新索引立即生效。不需要重新启动服务器。

从命令行管理索引

从命令行创建或修改索引涉及两个步骤：

- 使用 `ldapmodify` 命令行公用程序添加或修改索引配置条目。索引在每个后缀中单独配置，且索引配置条目与相应的数据库配置一起存储。
- 运行 `db2index.pl` perl 脚本 （Solaris 软件包中为 `directoryserver db2index-task`）以生成由服务器来维护的新索引集。

警告 千万不要删除系统索引，因为这样将会极大地影响 Directory Server 的性能。系统索引位于 `cn=index,cn=`*databaseName*`,cn=ldbm database,cn=plugins,cn=config` 条目和 `cn=default indexes,cn=config,cn=ldbm database,cn=plugins,cn=config` 条目中。

删除默认索引时需要小心，因为这也有可能会影响 Directory Server 的工作方式。

创建索引配置条目

要为还没有编制索引的属性创建索引，则必须在相应的数据库配置中为该属性创建新条目。

索引配置条目具有下列 DN：

```
cn=attributeName,cn=index,cn=databaseName,cn=ldbm database,
 cn=plugins,cn=config
```

其中的 *databaseName* 是与您希望创建索引的后缀相对应的数据库名称。例如，以下命令将为 sn (surname) 属性的值创建法语的出现、等式、子字符串和 “音似”索引：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=sn,cn=index,cn=databaseName,cn=ldbm database,
 cn=plugins,cn=config
objectClass:top
objectClass:nsIndex
cn:sn
nsSystemIndex:false
nsIndexType:pres
nsIndexType:eq
nsIndexType:sub
nsIndexType:approx
nsMatchingRule: 1.3.6.1.4.1.42.2.27.9.4.76.1
```

索引配置条目具有 nsIndex 对象类，且必须具有 nsSystemIndex 属性，其值必须为 false。无法创建新系统索引。将只维护 Directory Server 内部定义的现有系统索引。

nsIndexType 属性的值列出了将为给定属性进行维护的索引。使用上面显示的任意值定义相应的索引。

也可以使用单值 “none”显式地禁用属性的索引，例如为了临时禁用属性的索引。如果索引配置条目中不包括 nsIndexType 属性，则默认情况下将维护所有索引。

可选的 nsMatchingRule 属性包含用于国际化索引的语言排序顺序的 OID。有关受支持的区域和其相关的排序顺序的 OID 的列表，请参阅 *Sun ONE Directory Server 参考手册* 中的附录 C “目录国际化”。

有关索引配置属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册* 第 5 章中的 “默认索引属性”。

注意 创建索引时应该使用属性的主名称，而不是它的别名。属性的主名称是模式中列出的属性的第一个名称，如 userid 属性的主名称为 uid。有关属性主名称和别名的完整列表，请参阅表 10-3 （第 306 页）。

修改索引配置条目

要配置已经在属性上定义的索引，请修改相应的索引条目。例如，在先前定义的 sn 索引配置上执行以下命令将会删除 “音似”索引，并将语言更改为加拿大法语：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=sn,cn=index,cn=databaseName,cn=ldbm database,
 cn=plugins,cn=config
changetype:modify
delete:nsIndexType
nsIndexType:approx
-
replace:nsMatchingRule
nsMatchingRule: 1.3.6.1.4.1.42.2.27.9.4.78.1
^D
```

运行 db2index.pl 脚本

创建索引条目后，将附加索引类型添加到现有的索引条目，或是修改了其排序顺序，请运行 db2index.pl 脚本 （Solaris 软件包中为 directoryserver db2index-task），以生成新的索引。该脚本读取后缀的内容，并根据其配置条目重新编制给定属性的索引。

当此命令运行时，后缀的内容在服务器上保持可用，但是将不会对搜索编制索引，直到脚本完成。重新编制索引是一项相当消耗资源的任务，它可能会影响服务器上其他操作的性能。根据目录大小的具体情况，重新初始化后缀通常比重新编制两个或更多属性的索引要快，但是该后缀在初始化过程中不可用。详细信息，请参阅“重新初始化后缀”（第 313 页）。

此脚本的命令依平台而定：

Solaris 软件包

```
# /usr/sbin/directoryserver db2index-task
```

Windows 平台

```
cd ServerRoot
bin\slapd\admin\bin\perl slapd-serverID\db2index.pl
```

其他安装

```
# ServerRoot/slapd-serverID/db2index.pl
```

下列示例在与 *databaseName* 相对应的后缀中重新生成 *sn* 索引。

UNIX shell 脚本：

```
# use directoryserver db2index-task in the Solaris Packages
Installations
/var/Sun/mps/slapd-example/db2index.pl \
  -D "cn=Directory Manager" -w 口令 -n databaseName -t sn
```

Windows 批处理文件：

```
C:\Program Files\Sun\MPS\bin\slapd\admin\bin\perl.exe
  C:\Program Files\Sun\MPS\slapd-example\db2index.pl
    -D "cn=Directory Manager" -w 口令 -n databaseName -t sn
```

详细信息，请参阅 *Sun ONE Directory Server 参考手册* 第 2 章的 `db2index.pl`。

删除属性的所有索引

如果希望删除为属性配置的所有索引，可以删除其配置条目和数据库文件。例如，下列命令将为名为 *databaseName* 的数据库中的 `sn` 属性解除对所有索引的配置。

```
ldapdelete -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
"cn=sn,cn=index,cn=databaseName,cn=ldbm database,cn=plugins, \
 cn=config"
```

删除该条目后， `sn` 属性的索引将不再在与 *databaseName* 数据库对应的后缀中进行维护。也可以删除相应的索引文件以节约磁盘空间，因为服务器将不再使用它。在此示例中，您可以删除以下文件：

ServerRoot`/slapd-`*serverID*`/db/`*databaseName*`/`*databaseName*`_sn.db3`

重新索引后缀

如果索引文件被损坏，您将需要重新索引后缀以在相应的数据库目录中重新创建索引文件。有两种方法使用 Directory Server 控制台重新索引后缀，即重新编制索引或重新初始化。

重新索引后缀

重新索引后缀时，服务器会检查它包含的所有条目，并重新生成索引文件。重新编制索引过程中，后缀的内容可以用于读取和写入操作。但是，服务器必须为重新编制索引的每个属性扫描整个后缀，对于带有数百万条条目的后缀，这将花费多达数小时的时间，具体情况将取决于您配置的索引。此外，在重新编制索引过程中，索引将不可用，服务器性能也将受影响。

要使用控制台重新编制后缀索引，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，展开 “数据”节点，显示要重新编制索引的后缀。
2. 右键单击后缀配置节点，从弹出菜单中选择 “重新编制索引”。或者，可以左键单击节点将其选中，然后从 “对象”菜单中选择 “重新编制索引”。

   将显示 “重新索引后缀”对话框，该对话框带有在选定后缀中编制索引的所有属性的列表。

3. 选中要重新编制索引的每个属性旁的复选框。使用 “全部选中”和 “全部不选”按钮，帮助您作出选择。因为给定属性的所有索引都存储在同一个数据库文件中，所以必须一起重新编制所有这些索引。
4. 单击 “确定”。控制台将显示确认消息，提醒您可能返回意外的搜索结果，且重新编制索引过程中性能会受影响。
5. 单击 “是”，开始重新编制索引。

   控制台显示有关重新编制索引的所有信息的对话框。完成后关闭该对话框。

要从命令行重新索引后缀，请遵循 “运行 db2index.pl 脚本”（第 311 页）中的说明，并指定要重新生成索引文件的所有属性。

重新初始化后缀

重新初始化后缀时，替换其内容，并创建新的索引文件作为新内容导入。重新初始化后缀通常比重新编制一个以上属性的索引要快，因为加载条目时，所有属性都在一个通道中进行索引。但是，重新初始化后缀时后缀不可用。

可以使用 Directory Server 控制台或从命令行执行以下所有步骤：

1. 如 “设置访问权限和引荐”（第 87 页）中所述，将后缀设为只读。首先必须使后缀变为不可写入，以便在导出内容后不会进行任何修改。
2. 如 “使用控制台将单一后缀导出到 LDIF”（第 125 页）中所述，将整个后缀导出到 LDIF 文件。
3. 如 “初始化后缀”（第 120 页）中所述，将同一 LDIF 文件导入以重新初始化后缀。

   初始化期间，后缀将不可用。当初始化完成后，所有已配置的索引可供使用。
4. 如 “设置访问权限和引荐”（第 87 页）中所述，使后缀再次变为可写。

修改默认索引集

创建新后缀时使用的默认索引集在以下条目中定义：

```
cn=default indexes,cn=config,cn=ldbm database,
 cn=plugins,cn=config
```

无论何时使用控制台或从命令行创建后缀，默认索引定义条目将按原样复制以成为相应数据库的最初索引配置。

默认索引集只能使用命令行公用程序进行配置。默认索引条目具有与 “从命令行管理索引”（第 309 页）中描述的索引配置条目完全相同的语法。例如，使用以下 ldapmodify 命令添加默认索引配置条目：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=drink,cn=default indexes,cn=config,cn=ldbm database,
 cn=plugins,cn=config
objectClass:top
objectClass:nsIndex
cn:drink
nsSystemIndex:false
nsIndexType:eq
nsIndexType:sub
nsMatchingRule: 1.3.6.1.4.1.42.2.27.9.4.76.1
```

添加此条目后，所有新的后缀将具有 drink 属性的值，该属性已编制了法语的等式和子字符串搜索的索引。

要修改或删除默认索引条目，请使用 ldapmodify 或 ldapdelete 命令编辑 cn=default indexes,cn=config,cn=ldbm database,cn=plugins,cn=config 中的索引集。

管理浏览索引

浏览索引是仅用于要求服务器端排序或虚拟列表视图 (VLV) 结果的搜索操作的特殊索引。使用浏览索引可提高需要对大量结果进行服务器端排序的搜索的性能。根据目录配置，服务器可拒绝在没有定义浏览索引的情况下执行要求排序的搜索。这样可防止大量排序操作使服务器资源超过负载。

浏览索引适用于作为搜索基准的条目，且必须为在已排序的请求中使用的每个搜索过滤器创建单独的索引。例如，如果客户机应用程序经常请求所有用户的已排序列表，则应为客户机使用的过滤器字符串创建 ou=People 的浏览索引。

与附加索引一样，在维护浏览索引所需的更新操作期间将损失性能。应仔细计划和测试浏览索引的部署。

用于控制台的浏览索引

Directory Server 控制台经常执行整个目录的搜索以刷新其面板的内容。如果已配置控制台为目录树中的条目排序，如 “目录树视图选项”（第 31 页）中所述，则应为控制台创建浏览索引。

用于控制台的浏览索引专用于由控制台执行的搜索。它们也是使用控制台创建的。要为控制台创建浏览索引，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “目录”标签上，浏览目录树以显示需要排序的大型子树的父级，如包含数千个用户条目的 `ou=People,dc=example,dc=com`。
2. 右键单击父条目并从弹出菜单中选择 “创建浏览索引”。或者，左键单击条目以选定，并从 “对象”菜单中选择 “创建浏览索引”。

   “创建浏览索引”对话框显示索引创建的状态。控制台创建如下所示的浏览索引配置条目，然后生成索引文件的内容。
3. 单击 “关闭”，关闭 “创建浏览索引”对话框。

   任何控制台刷新操作将使新索引立即生效，且将维护添加到目录中的任何新数据。不需要重新启动服务器。

用于控制台的浏览索引配置由以下条目组成。`vlvSearch` 条目定义将被编制索引的搜索的基准、范围和过滤器。`vlvIndex` 条目的 `vlvSort` 属性按照属性排序的顺序显示 “目录”标签中支持排序的属性：

```
dn:cn=MCC entryDN,cn=databaseName,cn=ldbm database,
 cn=plugins,cn=config
objectClass:top
objectClass:vlvSearch
cn:MCC entryDN
vlvBase:"entryDN"
vlvScope: 1
vlvFilter:(|(objectclass=*)(objectclass=ldapsubentry))

dn:cn=by MCC entryDN, cn=MCC entryDN,cn=databaseName,
 cn=ldbm database,cn=plugins,cn=config
objectClass:top
objectClass:vlvIndex
cn:by MCC entryDN
vlvSort:cn givenname o ou sn uid
```

要删除 Directory Server 控制台的浏览索引，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “目录”标签上，浏览目录树，显示已在其中创建浏览索引的条目。
2. 右键单击条目并从弹出菜单中选择 “删除浏览索引”。或者，左键单击条目以选定，并从 “对象”菜单中选择 “删除浏览索引”。此菜单项仅当所选条目具有用于控制台的浏览索引时才可用。
3. 这时将出现 “删除浏览索引”对话框，要求您确认对索引的删除操作。单击 “是”，删除浏览索引。

用于客户机搜索的浏览索引

必须手动定义为排序客户机搜索结果而定制的浏览索引。从命令行创建浏览索引或者虚拟列表视图 (VLV) 索引涉及两个步骤：

- 使用 `ldapmodify` 公用程序或 Directory Server 控制台的 “目录”标签添加新的浏览索引条目或者编辑现有浏览索引条目。
- 运行 `vlvindex`（Solaris 软件包中为 `directoryserver vlvindex`）脚本以生成由服务器维护的新浏览索引集。

指定浏览索引条目

浏览索引是特定于给定基准条目及其子树上的给定的搜索。浏览索引配置是在包含条目的后缀的数据库配置中定义的。

注意	不能在已链接的后缀中创建浏览索引，只能在本地后缀和子后缀中创建。

有两个条目用于配置浏览索引。第一个使用 `vlvSearch` 对象类并指定其结果将被编制索引的搜索操作的基准、范围和过滤器。第二个条目是第一个条目的子级，并使用 `vlvIndex` 对象类指定要排序的属性和以何种顺序排序。

以下示例使用 `ldapmodify` 公用程序创建两个浏览索引配置条目：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=Browsing ou=People, cn=databaseName,
 cn=ldbm database,cn=plugins,cn=config
objectClass:top
objectClass:vlvSearch
cn:Browsing ou=People
vlvbase:ou=People,dc=example,dc=com
vlvscope: 1
vlvfilter:(objectclass=inetOrgPerson)

dn:cn=Sort rev employeenumber, cn=Browsing ou=People,
 cn=databaseName,cn=ldbm database,cn=plugins,cn=config
objectClass:top
objectClass:vlvIndex
cn:Sort rev employeenumber
vlvSort:-employeenumber
^D
```

vlvscope 可为 0 代表基准条目本身，或为 1 代表基准条目的直接子条目，或为 2 代表以基准条目为根的整个子树。 vlvfilter 是将用于客户机搜索操作的同一 LDAP 过滤器。因为所有的浏览索引条目都位于同一位置，所以建议使用描述性的 cn 值命名浏览索引。

每个 vlvSearch 条目必须至少具有一个 vlvIndex 条目。 vlvSort 属性是定义要排序的属性和排序顺序的属性名称的列表。属性名称前面的短横线 (-) 表示反排序。可通过定义多个 vlvIndex 条目为搜索定义多个索引。在前面的示例中，可添加以下条目：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=Sort sn givenname uid, cn=Browsing ou=People,
 cn=databaseName,cn=ldbm database,cn=plugins,cn=config
objectClass:top
objectClass:vlvIndex
cn:Sort sn givenname uid
vlvSort:sn givenname uid
^D
```

要修改浏览索引配置，请编辑相应的 vlvSearch 或 vlvIndex 条目。要删除浏览索引以使其不再由服务器维护，请删除单个的 vlvIndex 条目，或者如果只有一个浏览索引，则删除 vlvSearch 条目和 vlvIndex 条目。当删除 vlvIndex 条目时，也可删除相应的数据库文件，例如

ServerRoot/slapd-*serverID*/db/*dbName*/*dbName*_vlv#Sortsngivennameuid.db3

运行 vlvindex 命令

创建浏览索引条目或修改现有浏览索引条目后，必须运行 vlvindex 命令（Solaris 软件包中为 directoryserver vlvindex）以生成新的浏览索引集。此命令将扫描目录内容并为浏览索引创建数据库文件。

要生成浏览索引，请使用以下命令：

Solaris 软件包

```
# /usr/sbin/directoryserver vlvindex
```

其他安装

```
# installDir/slapd-serverID/vlvindex
```

以下示例生成前面小节中定义的浏览索引：

```
# vlvindex -n databaseName -T "Browsing ou=People"
```

表 10-4　示例中使用的 vlvindex 选项的说明

选项	说明
-n	指定包含需要编制索引的条目的数据库名称。

表 10-4　示例中使用的 vlvindex 选项的说明

选项	说明
-T	指定相应浏览索引的 vlvSearch 条目的命名属性值。将生成所有与给定的 vlvSearch 条目的 vlvIndex 条目相对应的索引。

详细信息，请参阅 *Sun ONE Directory Server 参考手册* 第 2 章中的 “vlvindex”。

第 11 章

实现安全性

Sun ONE Directory Server 支持多种机制以提供安全可信的网络通讯。LDAPS 是运行在安全套接字层 (SSL) 基础上的标准 LDAP 协议，它加密数据并可随意地使用证书进行验证。

Sun ONE Directory Server 还支持 “启动传输层安全性” (Start TLS) 扩展操作，以便在原来未加密的 LDAP 连接上启用 TLS。对于 Directory Server 5.2，StartTLS 在 Windows 平台和 Unix 平台上均受支持。

Directory Server 5.2 现在还支持简单验证和安全层 (SASL) 上的综合安全服务应用程序接口 (GSSAPI)。这样，您就可以在 Solaris 操作环境中使用 Kerberos Version 5 安全协议。然后，标识映射机制会将 Kerberos Principal 与目录中的标识相关联。

本章包含以下小节：

- Directory Server 中的 SSL 简介
- 启用 SSL 的步骤摘要
- 获得并安装服务器证书
- 激活 SSL
- 配置客户机验证
- 标识映射
- 配置 LDAP 客户机以使用安全性

Directory Server 中的 SSL 简介

安全套接字层 (SSL) 提供加密通讯和 Directory Server 及其客户机之间的可选验证服务。可以为 LDAP 和 DSML-over-HTTP 两种协议启用 SSL，从而为所有的服务器连接提供安全性。另外，可以配置复制机制和链接后缀机制，以使用 SSL 保证服务器之间的安全通讯。

利用简单验证 （绑定 DN 和口令）使用 SSL 可以加密所有发送至服务器的数据以及服务器发送的数据，以保证保密性和数据完整性。客户机还可以选择使用证书对 Directory Server 进行验证，或通过简单验证和安全层 (SASL) 对第三方安全机制进行验证。基于证书的验证使用公共密钥加密方法，以防止伪装和假冒客户机或服务器。

Directory Server 可以在不同的端口同时使用 SSL 和非 SSL 通讯。或者，为了安全起见，您也可以将所有通讯都限制在安全端口。客户机验证也是可配置的，它可能是必需的，或者仅使用它来确定要实施的安全级别。

启用 SSL 也将启用支持 Start TLS 扩展操作，Start TLS 扩展操作提供在普通 LDAP 连接上的安全性。客户机可以绑定至非 SSL 端口，然后使用 “传输层安全性 (TLS)”协议启动 SSL 连接。 Start TLS 操作为客户机提供了更大的灵活性，有助于简化端口分配。

SSL 提供的加密机制还可以用于属性加密。启用 SSL 后，可以在后缀中配置属性加密，以便在数据存储在目录中时为其提供保护。详细信息，请参阅 “为属性值加密”（第 70 页）。

要获得额外的安全性，可以根据客户机的 SSL 和证书的使用情况对目录内容的访问控制进行配置。可以定义访问控制指令 (ACI)，它需要特定的验证方法，从而确保数据仅能通过一个安全通道进行传输。详细信息，请参阅 “绑定规则”（第 175 页）。

有关 SSL、因特网安全性和证书的完整说明 （包括如何在 Administration Server 中配置 SSL），请参阅 *Sun ONE Server Console 服务器管理指南* 中的第 10 章“在 Sun ONE Server 中使用 SSL 和 TLS”。

启用 SSL 的步骤摘要

本章的后续小节均包括以下步骤：

1. 为您的 Directory Server 获得和安装证书，并将 Directory Server 配置为信任证书授权机构的证书。此过程包括：

   a. 必要时创建证书数据库。

b. 生成并发送证书请求，将其从服务器发送至将提供服务器证书的证书授权机构。

c. 在服务器中安装新的证书。

d. 信任证书授权机构及其颁发的所有证书。

2. 在目录中激活并配置 SSL，包括 LDAP 和 DSML 操作的安全端口。还可以配置 Directory Server 控制台以使用 SSL 访问服务器。

3. 还可以选择为以下一个或多个客户机验证机制配置服务器：

a. 默认的基于证书的验证。

b. SASL 上的 DIGEST_MD5 验证机制。

c. 允许使用 Kerberos V5 安全机制的 SASL 上的 GSSAPI 验证。

4. 对客户机进行配置以便在与 Directory Server 通讯时使用 SSL，包括要使用的任一可选验证机制。

也可以使用 `certutil` 工具执行上述某些步骤，以便通过命令行来管理证书。 Sun ONE Directory Server Resource Kit 中提供有此工具。详细信息，请参阅 *Sun ONE Directory Server Resource Kit 工具参考* 中第 30 章 “安全工具”。

获得并安装服务器证书

本节介绍如何创建证书数据库、获得并安装用于 Directory Server 的证书，以及如何将 Directory Server 配置为信任证书授权机构 (CA) 的证书。

创建证书数据库

第一次在服务器上配置 SSL 时，必须为安全设备设置口令。如果未使用外部硬件安全设备，则内部安全设备就是存储在下列文件中的证书和密钥数据库：

ServerRoot`/alias/slapd-`*serverID*`-cert7.db`
ServerRoot`/alias/slapd-`*serverID*`-key3.db`

如果 *serverID* 包含大写字母，则必须使用下面的命令行步骤创建证书数据库。

使用控制台

使用控制台时，在第一次调用证书管理器对话框时，服务器将自动创建证书数据库文件：

1. 在 Directory Server 控制台的顶级 “任务”标签上，单击 “管理证书”按钮。或者，显示 “任务”标签后，在 “控制台 > 安全性”菜单中选择 “管理证书”项。
2. 服务器将自动创建证书和密钥数据库，并要求您为安全设备设置口令。此口令将保护服务器中存储的证书的专用密钥。输入两次口令，对其进行确认，然后单击 “确定”。

使用命令行

通过命令行创建证书数据库文件时，必须使用下面步骤中显示的路径和文件名前缀，这样服务器就可以找到它们。

1. 在服务器主机上，请使用以下命令创建证书数据库：

   ```
   certutil -N -d ServerRoot/alias -P slapd-LCserverID-
   ```

   其中 *LCserverID* 为全部使用小写字母的服务器名称。

   此工具将提示您输入口令来保护证书的密钥。

生成证书请求

使用下列步骤之一可以生成 PEM 格式的 PKCS #10 证书请求。PEM 是 RFC 1421 至 1424 (`http://www.ietf.org/rfc/rfc1421.txt`) 指定的 “保密增强邮件”格式，用于表示以 US-ASCII 字符显示的 base64 编码的证书请求。请求的内容将类似于以下示例：

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBrjCCARcCAQAwbjELMAkGA1UBhMCVXMxEzARBgNVBAgTCkNBElGT1JOSUExLD
AqBgVBAoTI25ldHNjYXBlIGNvb11bmljYXRpb25zIGNvcnBvcmF0aWuMRwwGgYDV
QQDExNtZWxsb24umV0c2NhcGUuY29tMIGfMA0GCSqGSIb3DQEBAUAA4GNADCBiQK
BgCwAbskGh6SKYOgHy+UCSLnm3ok3X3u83Us7u0EfgSLR0f+K41eNqqWRftGR83e
mqPLDOf0ZLTLjVGJaHJn4l1gG+JDf/n/zMyahxtV7+T8GOFFigFfuxJaxMjr2j7I
vELlxQ4IfZgwqCm4qQecv3G+N9YdbjveMVXW0v4XwIDAQABAAwDQYJKoZIhvcNAQ
EEBQADgYEAZyZAm8UmP9PQYwNy4Pmypk79t2nvzKbwKVb97G+MT/gw1pLRsuBoKi
nMfLgKp1Q38K5Py2VGW1E47/rhm3yVQrIiwV+Z8Lcc=
-----END NEW CERTIFICATE REQUEST-----
```

使用控制台

1. 在 Directory Server 控制台的顶级 “任务”标签上，单击 “管理证书”按钮。或者，显示 “任务”标签后，在 “控制台 > 安全性”菜单中选择 “管理证书”项。

   显示 “管理证书”对话框。

2. 选择 “服务器证书”标签，并单击 “请求”按钮。

   出现 “证书请求向导”。

3. 如果已经安装了一个允许服务器与 CA 直接进行通讯的插件，则现在可以选择此插件。否则，必须通过电子邮件或网站传输生成的请求，以手动请求证书。单击 “下一步”以继续。

4. 在空白文本字段中输入 “请求方信息”：

   服务器名。输入 Directory Server 的完全限定主机名，该主机名是在 DNS 查找中使用的名称 （例如， `east.example.com`）。

   组织。输入您公司或机构的法定名称。大多数 CA 要求您出示法律凭证 （如企业许可证的副本）以验证此信息。

   组织单元。（可选）。输入您公司内部部门或业务单位的描述性名称。

   地区。（可选）。输入您公司所在的城市的名称。

   州或省。输入您公司所在的州或省的全名 （非缩写）。

   国家 （地区）。选择您国家 （地区）的双字符缩写 （ISO 格式）。美国的国家（地区）代码为 US。 *Sun ONE Directory Server 参考手册* 中的附录 C “目录国际化”包含一个 ISO 国家 （地区）代码列表。

   单击 “下一步”以继续。

5. 输入安全设备的口令，然后单击 “下一步”。此口令是在 “创建证书数据库”（第 321 页）中设置的。

6. 选择 “复制到剪贴板”或 “保存到文件”以保存必须发送到证书授权机构的证书请求信息。

7. 单击 “完成”退出 “证书请求向导”。

使用命令行

1. 请使用以下命令创建服务器证书请求：

   ```
   certutil -R \
   -s "cn=serverName,ou=division,o=company,l=city,st=state,c=country" \
   -a -d ServerRoot/alias -P slapd-serverID-
   ```

   `-s` 选项指定了请求的服务器证书的 DN。通常，证书授权机构会要求此示例中显示的所有属性，以完整地识别此服务器。请参阅上面的步骤 4，以获取每个属性的说明。

2. `certutil` 工具将提示您输入服务器的密钥数据库口令。此口令是在 “创建证书数据库”（第 321 页）中设置的。然后，此工具将生成 PEM 编码文本格式的 PKCS #10 证书请求。

安装服务器证书

服务器会根据请求的步骤将上节中的请求传输至证书授权机构。例如，可能会要求您以电子邮件的形式发送证书请求，或者您也可以通过 CA 的网站输入请求。

发送了请求后，必须等待 CA 对您的证书作出响应。请求响应时间会有所不同。例如，如果 CA 在您公司内部，可能只需要一到两天时间就可响应请求。如果选择了公司外部的 CA，则可能需要几周的时间来响应请求。

当 CA 发送响应时，一定要将信息保存到文本文件中。PEM 格式的 PKCS #11 证书将类似于以下示例。 PEM 是 RFC 1421 至 1424 (`http://www.ietf.org/rfc/rfc1421.txt`) 指定的 “保密增强邮件” 格式，用于表示以 US-ASCII 字符显示的 base64 编码的证书。

```
-----BEGIN CERTIFICATE-----
MIICjCCAZugAwIBAgICCEEwDQYJKoZIhKqvcNAQFBQAwfDELMAkGA1UEBhMCVVMx
IzAhBgNVBAoGlBhbG9a2FWaWxsZGwSBXaWRnZXRzLCBJbmMuMR0wGwYDVQQLExRX
aWRnZXQgTW3FrZXJzICdSJyBVczEpMCcGAx1UEAxgVGVzdCBUXN0IFRlc3QgVGVz
dCBUZXN0IFlc3QgQ0EswHhcNOTgwMzEyMDIzMzUWhcNOTgwMzI2MDIzMpzU3WjBP
MQswCYDDVQQGEwJVUzEoMCYGA1UEChMfTmV0c2NhcGUgRGlyZN0b3J5VIFB1Ymxp
Y2F0aW9uczEWMB4QGA1UEAxMNZHVgh49dq2tLNvbjTBaMA0GCSqGSIb3DQEBAQUA
A0kAMEYkCQCksMR/aLGdfp4m0OiGgijG5KgOsyRNvwGYW7kfW+8mmijDtZaRjYNj
jcgpF3VnlbxbclX9LVjjNLC5737XZdAgEDozYwpNDARBglghkgBhvhCEAQEEBAMC
APAwHkwYDVR0jBBgwFAU67URjwCaGqZHUpSpdLxlzwJKiMwDQYJKoZIhQvcNAQEF
BQADgYEAJ+BfVem3vBOPBveNdLGfjlb9hucgmaMcQa9FA/db8qimKT/ue9UGOJqL
bwbMKBBopsDn56p2yV3PLIsBgrcuSoBCuFFnxBnqSiTS7YiYgCWqWaUA0ExJFmD6
6hBLseqkSWulk+hXHN7L/NrViO+7zNtKcaZLlFPf7d7j2MgX4Bo=
-----END CERTIFICATE-----
```

还应将证书数据备份到一个安全的地方。如果系统曾丢失证书数据，则可使用备份文件重新安装证书。

获得服务器证书后即可将其安装到服务器的证书数据库中。

使用控制台

1. 在 Directory Server 控制台的顶级 “任务” 标签上，单击 “管理证书” 按钮。或者，显示 “任务” 标签后，在 “控制台 > 安全性” 菜单中选择 “管理证书” 项。

   显示 “管理证书” 窗口。

2. 选择 “服务器证书” 标签，并单击 “安装”。

   显示 “证书安装向导”。

3. 从以下证书位置选项中选择一个选项：

在此文件中。在此字段中输入到证书的绝对路径。

在下列编码的文本块中。将来自证书授权机构的文本或您创建的文本文件中的文本复制并粘贴到此字段。例如：

单击 “下一步”以继续。

4. 确认显示的证书信息是否正确，然后单击 “下一步”。
5. 指定证书的名称，然后单击 “下一步”。这就是要在证书表中显示的名称。
6. 提供保护专用密钥的口令以验证证书。此口令与您在 “创建证书数据库”（第 321 页）的步骤 2 中提供的口令一致。完成后单击 “完成”。

   您的新证书将显示在 “服务器证书”标签上的列表中。现在您的服务器已为激活 SSL 准备完毕。

使用命令行

1. 请使用以下命令在证书数据库中安装新的服务器证书：

   ```
   certutil -A -n "certificateName" -t "u,," -a -i certFile \
            -d ServerRoot/alias -P slapd-serverID-
   ```

   其中 *certificateName* 是您给定的用来标识证书的名称， *certFile* 是包含 PEM 格式的 PKCS #11 证书的文本文件。 `-t "u,,"` 选项表示这是一个用于 SSL 通讯的服务器证书。

2. 也可以选择使用以下 `certutil` 命令来验证已安装的证书：

   ```
   certutil -L -d ServerRoot/alias -P slapd-serverID-
   ```

   列出的具有信任属性 `u,,` 的证书是服务器证书。

信任证书授权机构

配置 Directory Server 以信任证书授权机构，配置过程由获得 CA 证书和将其安装到服务器的证书数据库两部分组成。此过程根据您所使用的证书授权机构的不同而有所区别。某些商业 CA 提供允许您自动下载证书的网站，而有些 CA 则根据您的请求以电子邮件的形式将证书发送给您。

使用控制台

获得 CA 证书后，可使用 “证书安装向导”配置 Directory Server 以信任证书授权机构。

1. 在 Directory Server 控制台的顶级 “任务”标签上，单击 “管理证书”按钮。或者，显示 “任务”标签后，在 “控制台 > 安全性”菜单中选择 “管理证书”项。

   显示 “管理证书”窗口。

2. 选择 “CA 证书”标签，并单击 “安装”。

   显示 “证书安装向导”。

3. 如果已将 CA 的证书保存到文件，请在提供的字段中输入路径。如果通过电子邮件收到了 CA 的证书，请将包含标头的证书复制并粘贴到提供的文本字段中。单击 “下一步”。

4. 确认显示的证书信息与证书授权机构提供的信息一致，然后单击 “下一步”。

5. 指定证书的名称，然后单击 “下一步”。

6. 选择信任此 CA 的目的。可以选择二者之一或全选：

   正在接受从客户机的连接 （客户机验证）。如果 LDAP 客户机通过提交此 CA 颁发的证书来执行基于证书的客户机验证，则请选中此复选框。

   正在接受到其他服务器的连接 （服务器验证）。您的服务器通过 SSL 与另一个具有此 CA 所颁发证书的服务器进行通讯的过程中，如果此服务器担当复制供应商或链接多路复用器的角色，请选中此复选框。

7. 单击 “完成”退出该向导。

使用命令行

1. 也可以使用以下命令安装受信任的 CA 证书：

   ```
   certutil -A -n "CAcertificateName" -t "trust,," -a -i certFile \
            -d ServerRoot/alias -P slapd-serverID-
   ```

   其中 *CAcertificateName* 是给定的用来标识受信任 CA 的名称， *certFile* 是包含 PEM 编码文本格式的 PKCS #11 授权机构证书的文本文件， *trust* 是以下代码之一：

   - `T` - 表示此 CA 颁发的客户机证书是受信任的。如果 LDAP 客户机通过提交此 CA 颁发的证书来执行基于证书的客户机验证，则请使用此代码。
   - `C` - 表示此 CA 颁发的服务器证书是受信任的。您的服务器通过 SSL 与另一个具有此 CA 所颁发证书的服务器进行通讯的过程中，如果此服务器担当复制供应商或链接多路复用器的角色，请使用此代码。
   - `CT` - 表示此 CA 颁发的客户机证书和服务器证书都是受信任的。如果上面两种情况均适用于此 CA，请使用此代码。

2. 也可以选择使用以下 `certutil` 命令来验证已安装的证书：

   ```
   certutil -L -d ServerRoot/alias -P slapd-serverID-
   ```

   列出的具有信任属性 `u,,` 的证书是服务器证书，那些具有信任属性 `CT,,` 的证书是受信任的 CA 证书。

激活 SSL

完成服务器证书和受信任 CA 的证书的安装后，即可激活 SSL。大多数时间，您希望服务器在启用 SSL 的情况下运行。如果临时禁用 SSL，请确保在处理要求保密性、验证或数据完整性的操作之前重新启用 SSL。

如 “获得并安装服务器证书”（第 321 页）中所述，必须创建证书数据库、获得并安装服务器证书并信任 CA 的证书，才能激活 SSL。

以下步骤将在 Directory Server 中激活 SSL 通讯并启用加密机制：

1. 在 Directory Server 控制台的顶级 “配置”标签上，选择与服务器名称相同的根节点，然后在右侧面板中选择 “加密”标签。

   此标签显示当前服务器的加密设置。

2. 表明您希望通过选中 “启用该服务器的 SSL”复选框而启用加密功能。

3. 选中 “使用该密码系列”复选框。

4. 从下拉菜单中选择您要使用的证书。

5. 单击 “密码设置”，并在 “密码首选项”对话框中选择要使用的密码。有关特定密码的详细信息，请参阅 “选择加密密码”（第 328 页）。

6. 设置客户机验证的首选项：

   不允许客户机验证。选择此选项，服务器将忽略客户机的证书或 SASL 安全机制，并要求一个绑定 DN 和口令。

   允许客户机验证。这是默认设置。选择此选项，将根据客户机请求执行验证。有关基于证书的验证的详细信息，请参阅 “配置客户机验证”（第 331 页）。

注意	如果正在通过复制方式使用基于证书的验证，则必须将使用者服务器配置为允许或要求客户机验证。

   要求客户机验证。选择此选项，如果客户机不响应服务器的验证请求，则客户机连接将被拒绝。

注意 如果 Sun ONE Server Console 通过 SSL 连接至 Directory Server，选择 “要求客户机验证”将禁用通讯，这是因为 Sun ONE Server Console 没有可以用来进行客户机验证的证书。要通过命令行修改此属性，请参阅 “允许客户机验证”（第 330 页）。

7. 在与 Directory Server 通讯时，如果希望控制台使用 SSL，则还可以在 Sun ONE Server Console 中选择 “使用 SSL”。
8. 完成后单击 “保存”。
9. 还可以选择设置使用 LDAP 和 DSML-over-HTTP 这两种协议进行 SSL 通信时服务器要使用的安全端口。有关信息，请参阅 “更改 Directory Server 端口号”（第 33 页）。

   所有至安全端口的连接都必须使用 SSL。不论是否配置了安全端口，激活 SSL 后，客户机都会通过非安全端口使用 Start TLS 操作来执行 SSL 加密。

10. 重新启动 Directory Server。

    详细信息，请参阅 “在启用 SSL 的情况下启动服务器”（第 21 页）。

选择加密密码

密码 是用于加密和解密数据的算法。通常，加密期间密码使用的位越多，则密码越难破解或者说更安全。使用的消息验证类型也可以标识 SSL 密码。消息验证是另一种计算校验和 （用来保证数据完整性）的算法。有关密码算法及其强弱的更完整的讨论，请参阅 *Sun ONE Server Console 服务器管理指南* 的附录 B “SSL 使用的密码”。

当客户机启动与服务器的 SSL 连接时，客户机和服务器必须使用同一密码以用于加密信息。在任何双向加密过程中，双方都必须使用相同密码 （通常为双方都支持的保护能力最强的密码）。

Sun ONE Directory Server 提供以下 SSL 3.0 和 TLS 密码：

表 11-1 Sun ONE Directory Server 提供的密码

密码名称	说明
None	没有加密，只进行 MD5 消息验证 (rsa_null_md5)。
RC4 （128 位）	带 128 位加密的 RC4 密码并进行 MD5 消息验证 (rsa_rc4_128_md5)。

表 11-1 Sun ONE Directory Server 提供的密码 （续）

密码名称	说明
RC4 （导出）	带 40 位加密的 RC4 密码并进行 MD5 消息验证 (rsa_rc4_40_md5)。
RC2 （导出）	带 40 位加密的 RC2 密码并进行 MD5 消息验证 (rsa_rc2_40_md5)。
DES 或 DES （导出）	带 56 位加密的 DES 并进行 SHA 消息验证 (rsa_des_sha)。
DES (FIPS)	带 56 位加密的 FIPS DES 并进行 SHA 消息验证。此密码满足加密模块实现的 FIPS 140-1 美国政府标准 (rsa_fips_des_sha)。
三元 DES	带 168 位加密的三元 DES 并进行 SHA 消息验证 (rsa_3des_sha)。
三元 DES (FIPS)	带 168 位加密的 FIPS 三元 DES 并进行 SHA 消息验证。此密码满足加密模块实现的 FIPS 140-1 美国政府标准 (rsa_fips_3des_sha)。
Fortezza	带 80 位加密的 Fortezza 密码并进行 SHA 消息验证。
RC4 (Fortezza)	带 128 位加密的 Fortezza RC4 密码并进行 SHA 消息验证。
None (Fortezza)	没有加密，只进行 Fortezza SHA 消息验证。

为了继续使用 Sun ONE Server Console 和 SSL，必须至少选择以下密码中的一种：

- 带 40 位加密的 RC4 密码并进行 MD5 消息验证。
- 没有加密，只进行 MD5 消息验证 （不建议）。
- 带 56 位加密的 DES 并进行 SHA 消息验证。
- 带 128 位加密的 RC4 密码并进行 MD5 消息验证。
- 带 168 位加密的三元 DES 并进行 SHA 消息验证。

使用以下步骤来选择希望服务器使用的密码：

1. 在 Directory Server 控制台的顶级 “配置”标签上，选择与服务器名称相同的根节点，然后在右侧面板中选择 “加密”标签。

   此标签显示当前服务器的加密设置。如 “激活 SSL”（第 327 页）中所述，确保已为服务器启用 SSL。

2. 单击 “密码设置”。

   显示 “密码首选项”对话框。

3. 在 “密码首选项”对话框中，通过选中或取消选中密码名称旁的复选框来指定希望服务器使用的密码。

   除非出于某种安全原因而不能使用特定密码，否则应选择 `none,MD5` 之外的所有密码。

警告 不要选择 “没有加密，只进行 MD5 消息验证”密码，因为如果客户机上没有其他密码可用，服务器就会使用此选项。在这种情况下，连接是不安全的，因为没有使用加密。

4. 在 “密码首选项”对话框中单击 “确定”，然后在 “加密”标签中单击 “保存”。

允许客户机验证

如果已将 Directory Server 配置为要求客户机验证并且使用 SSL 连接至 Sun ONE Server Console，那么就不能再使用 Sun ONE Server Console 管理任何 Sun ONE 服务器。您将只能改为使用相应的命令行公用程序。

然而，如果您希望更改目录配置以便可以使用 Sun ONE Server Console，则必须执行以下步骤以不再*要求*而是允许客户机验证：

1. 使用以下命令修改 `cn=encryption,cn=config` 条目：

   ```
   ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn=encryption,cn=config
   changetype:modify
   replace:nsSSLClientAuth
   nsSSLClientAuth:allowed
   ```

2. 如 “从命令行启动和停止服务器 (Unix)”（第 20 页）中所述，重新启动 Directory Server。

   可立即启动 Sun ONE Server Console。

配置客户机验证

客户机验证是一种服务器验证客户机身份的机制。可以使用客户机提供的证书或者通过基于 SASL 的机制 （如 DIGEST-MD5）执行客户机验证。在 Solaris 操作系统上，目前 Directory Server 通过 SASL 支持 GSSAPI 机制，该机制允许通过 Kerberos V5 进行客户机验证。

基于证书的验证使用通过 SSL 协议获得的客户机证书，来查找用户条目以进行标识。该条目包含的证书必须与要验证的用户的证书相同。此机制也称为 EXTERNAL，因为它处于 SASL 机制的外部。 *Sun ONE Server Console 服务器管理指南* 中的第 10 章 “使用客户机验证”对基于证书的验证进行了完整的说明。

以下小节介绍如何在 Directory Server 上配置两个 SASL 机制。另请参阅 “配置 LDAP 客户机以使用安全性”（第 338 页）。

通过 DIGEST-MD5 进行的 SASL 验证

DIGEST-MD5 机制通过比较具有无序用户口令的客户机发送的无序值对客户机进行验证。然而，因为此机制必须读取用户口令，所以希望通过 DIGEST-MD5 进行验证的所有用户都必须在目录中有一个 {CLEAR} 口令。

配置 DIGEST-MD5 机制

以下过程说明了配置 Directory Server 以使用 DIGEST-MD5 的必要步骤：

1. 使用控制台或 ldapsearch 命令，验证 DIGEST-MD5 是根条目中 supportedSASLMechanisms 属性的值。例如，以下命令将显示启用的 SASL 机制：

   ```
   ldapsearch -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
   -s base -b "" "(objectclass=*)" supportedSASLMechanisms
   ```

   ```
   dn:
   supportedSASLMechanisms:EXTERNAL
   supportedSASLMechanisms:DIGEST-MD5
   supportedSASLMechanisms:GSSAPI
   ```

2. 如果未启用 DIGEST-MD5，请使用下面的 ldapmodify 命令来启用它：

   ```
   ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn=SASL, cn=security, cn=config
   changetype:modify
   add:dsSaslPluginsEnable
   ```

```
dsSaslPluginsEnable:DIGEST-MD5
-
replace:dsSaslPluginsPath
dsSaslPluginsPath:ServerRoot/lib/sasl
```

3. 使用 DIGEST-MD5 的默认标识映射，或者按照 “DIGEST-MD5 标识映射”（第 332 页）中的说明创建新的标识映射。
4. 确保将使用 DIGEST-MD5 通过 SSL 访问服务器的所有用户的口令都存储在 {CLEAR} 中。有关如何配置口令存储方案的说明，请参阅第 7 章 “用户帐户管理”。

警告 在目录中存储 {CLEAR} 口令时，必须确保通过 ACI 对口令值的访问进行适当地限制，如第 6 章 “管理访问控制”中所述。您可能还希望通过在该后缀中配置属性加密对 {CLEAR} 口令实施进一步保护，如 “为属性值加密”（第 70 页）中所述。

5. 如果修改了 SASL 配置条目或者 DIGEST-MD5 标识映射条目之一，请重新启动 Directory Server。

DIGEST-MD5 标识映射

SASL 机制的标识映射尝试将 SASL 标识凭证与目录中的用户条目进行匹配。有关此机制的完整说明，请参阅 “标识映射”（第 336 页）。如果映射未能找到与 SASL 标识相对应的 DN，则验证失败。

SASL 标识是名为 *Principal* 的字符串，它以每个机制的特定格式来表示用户。在 DIGEST-MD5 中，建议客户机创建一个包含 dn: 前缀和 LDAP DN 或 u: 前缀（后面是客户机确定的任意文本）的 Principal。映射期间，客户机发送的 Principal 在 ${Principal} 占位符中可用。

服务器配置中的下列条目给定了 DIGEST-MD5 的默认标识映射：

```
dn:cn=default,cn=DIGEST-MD5,cn=identity mapping,cn=config
objectClass:top
objectClass:nsContainer
objectClass:dsIdentityMapping
objectClass:dsPatternMatching
cn:default
dsMatching-pattern:${Principal}
dsMatching-regexp:dn:(.*)
dsMappedDN: $1
```

此标识映射假设 Principal 的 dn 字段包含目录中现有用户的确切 DN。

要定义您自身的 DIGEST-MD5 标识映射，请执行以下操作：

1. 在 cn=DIGEST-MD5,cn=identity mapping,cn=config 下编辑默认映射条目或创建新的映射条目。有关标识映射条目中属性的定义，请参阅 “标识映射”（第 336 页）。 DIGEST-MD5 的映射示例位于下面的文件中：

   ServerRoot/slapd-*serverID*/ldif/identityMapping_Examples.ldif

   此示例假设 Principal 的不符合要求的文本字段包含具有期望身份的用户名。下面的命令显示了将要如何定义此映射：

```
ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=unqualified-username,cn=DIGEST-MD5,cn=identity mapping,
 cn=config
objectclass:dsIdentityMapping
objectclass:dsPatternMatching
objectclass:nsContainer
objectclass:top
cn:unqualified-username
dsMatching-pattern:${Principal}
dsMatching-regexp:u:(.*)@(.*)\.com
dsSearchBaseDN:dc=$2
dsSearchFilter:(uid=$1)
```

2. 重新启动 Directory Server 以使新映射生效。

通过 GSSAPI 进行 SASL 验证 （仅限 Solaris）

SASL 上的综合安全服务应用程序接口 (GSSAPI) 允许您使用第三方安全系统 （如 Kerberos V5）来验证客户机。GSSAPI 库仅在 Solaris 平台上可用。Sun 建议您在 Sun Enterprise Authentication Mechanism (SEAM) 1.0.1 服务器中安装 Kerberos V5 实现。

服务器将使用此 API 来验证用户的身份。然后， SASL 机制将应用 GSSAPI 映射规则，以获得连接期间所有操作的绑定 DN。

配置 Kerberos 系统

按照制造商的说明配置 Kerberos 软件。如果使用的是 SEAM 1.0.1 服务器，则配置过程包括以下步骤：

1. 配置 /etc/krb5 中的文件。

2. 创建 Kerberos 数据库以存储用户和服务，并在其中创建 LDAP 服务的 principal。 LDAP 服务的 principal 为：

   ldap/*serverFQDN*@*REALM*

   其中 *serverFQDN* 是服务器的完全符合要求的域名。

3. 创建密钥标签以存储服务密钥，其中包括用于 LDAP 服务的一个密钥。

4. 启动 Kerberos 守侯进程。

有关每一步操作的详细说明，请参阅软件文档。

配置 GSSAPI 机制

以下过程说明了配置 Directory Server 以在 Solaris 平台上使用 GSSAPI 的必要步骤：

1. 使用控制台或 ldapsearch 命令，验证 GSSAPI 是根条目中 supportedSASLMechanisms 属性的值。例如，以下命令将显示启用的 SASL 机制：

   ```
   ldapsearch -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
   -s base -b "" "(objectclass=*)" supportedSASLMechanisms

   dn:
   supportedSASLMechanisms:EXTERNAL
   supportedSASLMechanisms:DIGEST-MD5
   ```

2. 默认情况下，未启用 GSSAPI。可使用下面的 ldapmodify 命令来启用它：

   ```
   ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn=SASL, cn=security, cn=config
   changetype:modify
   add:dsSaslPluginsEnable
   dsSaslPluginsEnable:GSSAPI
   -
   replace:dsSaslPluginsPath
   dsSaslPluginsPath:ServerRoot/lib/sasl
   ```

3. 按照 “GSSAPI 标识映射”（第 335 页）中的说明创建 GSSAPI 的默认标识映射和任何自定义映射。

4. 在服务器主机上配置服务器的 Kerberos：

   a. 使用会话密钥在 Kerberos 中创建以下 LDAP 服务 principal：ldap/*serverHostname*@*Realm*，其中：

      - *serverHostname* 是服务器主机的完全符合要求的域名。此值必须与 cn=config 中 nsslapd-localhost 属性的值相同，但它必须全部为小写字母。

- *Realm* 是服务器的 Kerberos 领域。

b. LDAP 服务必须能够读取下面文件中的密钥数据库：
`/etc/krbs/krb5.keytab`。

c. 必须在主机上配置 DNS。

5. 如果修改了 SASL 配置条目或者 GSSAPI 标识映射条目之一，请重新启动 Directory Server。

GSSAPI 标识映射

SASL 机制的标识映射尝试将 SASL 标识凭证与目录中的用户条目进行匹配。有关此机制的完整说明，请参阅 “标识映射”（第 336 页）。如果映射未能找到与 SASL 标识相对应的 DN，则验证失败。

SASL 标识是名为 *Principal* 的字符串，它以每个机制的特定格式来表示用户。在 Kerberos 中使用 GSSAPI 时， Principal 是具有 *uid*`[`/*instance*`]``[`@*realm*`]` 格式的标识，其中 *uid* 可能包含一个可选的 *instance* 标识符 （其后跟着通常为域名的可选 *realm*）。例如，以下全部为有效的用户 Principal：

```
bjensen
bjensen/Sales
bjensen@EXAMPLE.COM
bjensen/Sales@EXAMPLE.COM
```

最初，未在目录中定义 GSSAPI 映射。根据客户机定义其使用的 Principal 的方式，您应该定义默认映射和需要的任何自定义映射。

要定义 GSSAPI 的标识映射，请执行以下操作：

1. 在 `cn=GSSAPI,cn=identity mapping, cn=config` 下创建新的映射条目。有关标识映射条目中属性的定义，请参阅 “标识映射”（第 336 页）。

   GSSAPI 映射示例位于下面的文件中：

   ServerRoot`/slapd-`*serverID*`/ldif/identityMapping_Examples.ldif`

   此文件中建议的默认 GSSAPI 映射假设 Principal 仅包含一个用户 ID，这确定了目录的固定分支中的一个用户：

   ```
   dn:cn=default,cn=GSSAPI,cn=identity mapping,cn=config
   objectclass:dsIdentityMapping
   objectclass:nsContainer
   objectclass:top
   cn:default
   dsMappedDN:uid=${Principal},ou=people,dc=example,dc=com
   ```

此文件中的另一个示例显示了在包括已知 Realm 的 Principal 中包含用户 ID 时如何确定此用户 ID。

```
dn:cn=same_realm,cn=GSSAPI,cn=identity mapping,cn=config
objectclass:dsIdentityMapping
objectclass:dsPatternMatching
objectclass:nsContainer
objectclass:top
cn:same_realm
dsMatching-pattern:${Principal}
dsMatching-regexp:(.*)@example.com
dsMappedDN:uid=$1,ou=people,dc=example,dc=com
```

2. 重新启动 Directory Server 以使新映射生效。

标识映射

Directory Server 中的若干验证机制需要一个从其他协议的凭证至目录中 DN 的映射。目前， DSML-over-HTTP 协议和 DIGEST-MD5 以及 GSSAPI SASL 机制之间就是这种情况。每个验证机制都将使用标识映射来确定由客户机提供的基于协议特定凭证的绑定 DN。

标识映射使用 `cn=identity mapping, cn=config` 配置分支中的条目。此分支为每个必须执行标识映射的协议包括一个容器：

- `cn=HTTP-BASIC, cn=identity mapping, cn=config` - 包含 DSML-over-HTTP 连接的映射。
- `cn=DIGEST-MD5, cn=identity mapping, cn=config` - 包含使用 DIGEST-MD5 SASL 机制进行客户机验证的映射。
- `cn=GSSAPI, cn=identity mapping, cn=config` - 必须创建该容器，以包含使用 GSSAPI SASL 机制进行客户机验证的映射。

映射条目定义了提取协议特定凭证的元素以在搜索目录时使用这些元素的方式。如果该搜索仅返回一个用户条目，则映射已经成功，且连接将使用此条目作为所有操作的绑定 DN。如果搜索没有返回条目或返回多个条目，则映射失败，将应用其他映射。

每个分支应该包含该协议的一个默认映射以及任意数量的自定义映射。默认映射具有 RDN `cn=default`，自定义映射可能具有使用 `cn` 作为命名属性的任何其他 RDN。将首先以不确定的顺序评估所有自定义映射，直至其中一个映射成功。如果所有自定义映射均失败了，则最后将应用默认映射。如果默认映射也失败了，那么客户机验证失败。

映射条目必须包含 top、 Container 和 dsIdentityMapping 对象类。然后，条目还可能包含以下属性：

- dsMappedDN:*DN* - 在目录中定义 DN 的文字串。如果执行映射时此 DN 存在，则它将用于绑定。您还可以定义以下属性，以便在此 DN 不存在的情况下执行搜索。
- dsSearchBaseDN:*DN* - 用于搜索的基准 DN。如果忽略此属性，则映射将在整个目录树中搜索所有根后缀。
- dsSearchScope:base|one|sub - 搜索的范围，它可能是搜索基准本身、基准下的一个子级别，或基准下的整个子树。忽略此属性时，映射搜索的默认范围为整个子树。
- dsSearchFilter:*filterString* - 执行映射搜索的过滤器字符串。 LDAP 搜索过滤器是在 RFC 2254 (http://www.ietf.org/rfc/rfc2254.txt) 中定义的。

另外，映射条目还可能包含允许其使用下列属性的 dsPatternMatching 对象类：

- dsMatching-pattern:*patternString* - 指定要在其上执行模式匹配的字符串。
- dsMatching-regexp:*regularExpression* - 指定应用于模式字符串的正则表达式。

上面所有的属性值 （dsSearchScope 除外）可能包含格式为 ${*keyword*} 的占位符，其中 *keyword* 是协议特定凭证中元素的名称。映射期间，占位符将被替换为客户机提供的元素的实际值。

所有占位符均被替换后，将执行定义的所有模式匹配。将会对模式匹配与正则表达式进行比较。如果正则表达式与模式字符串不匹配，则此映射失败。如果匹配，则括号中正则表达式条件的匹配值将作为可用的已编号占位符，以在其他属性值中使用。例如，可以为 SASL 定义以下映射：

```
dsMatching-pattern:${Principal}
dsMatching-regexp: (.*)@(.*)\.(.*)
dsMappedDN:uid=$1,ou=people,dc=$2,dc=$3
```

如果使用 bjensen@example.com 的 Principal 进行客户机验证，则此映射将定义绑定 DN uid=bjensen,ou=people,dc=example,dc=com。如果目录中存在此 DN，则映射将成功，并对客户机进行验证，此连接期间执行的所有操作都将使用此绑定 DN。

将使用 Posix regexec(3C) 和 regcomp(3C) 函数调用对 dsMatching-pattern 与 dsMatching-regexp 进行比较。 Directory Server 使用扩展的正则表达式，所有的比较项都是不区分大小写的。详细信息，请参阅这些函数的 man 页面。

可能包含占位符的属性值必须对不属于占位符组成部分的任意 $, { 和 } 字符进行编码（即使没有使用占位符）。必须使用以下值对这些字符进行编码：$ 替换为 \24、{ 替换为 \7B， } 替换为 \7D。

使用占位符和替换值将允许您创建映射 （映射将从协议特定凭证中提取用户名或其他任意值），并使用映射值来定义已映射的 DN，或者在目录的任意位置搜索相应的 DN。应该定义提取由目录客户机提供的预期凭证的映射，并将其映射到特定的目录结构。

警告 创建定义不完善的映射将会成为安全漏洞。例如，无模式匹配的到硬编码 DN 的映射总是能成功，因此将验证可能不是目录用户的客户机。

定义若干映射来处理不同的客户机凭证格式，而不是创建一个单一的、过于普通和随意的映射，这样会更安全。应该根据客户机凭证始终尝试将客户机连接映射至特定用户。

配置 LDAP 客户机以使用安全性

以下几节介绍如何在希望与 Directory Server 建立安全连接的 LDAP 客户机中配置和使用 SSL。在 SSL 连接中，服务器会将其证书发送给客户机。客户机首先必须信任其证书以验证服务器。然后，客户机可以通过发送自身的证书或两个 SASL 机制之一 （DIGEST-MD5 或使用 Kerberos V5 的 GSSAPI）的信息来启动某一客户机验证机制。

以下几节使用 `ldapsearch` 工具作为启用 SSL 的 LDAP 客户机的示例。 Directory Server 中提供的 `ldapmodify`、 `ldapdelete` 和 `ldapcompare` 工具的配置方式相同。这些目录访问工具均基于 Sun ONE LDAP SDK for C， *Sun ONE Directory Server Resource Kit 工具参考* 中对其进行了进一步说明。

要在其他 LDAP 客户机上配置 SSL 连接，请参阅应用程序附带的文档。

注意 某些客户机应用程序实施 SSL，但并不验证服务器是否具有受信任的证书。它们使用 SSL 协议以提供数据加密，但既不能保证保密性，也不能防止客户机的假冒。

在客户机中配置服务器验证

当客户机建立与服务器的 SSL 连接时，它必须信任服务器提交的证书。为完成此操作，客户机必须：

- 具有一个证书数据库。
- 信任颁发服务器证书的证书授权机构 (CA)。
- 指定 LDAP 客户机的 SSL 选项。

Netscape Communicator 是使用 SSL 通过 HTTP 协议与 Web 服务器进行通讯的客户机应用程序。可以使用 Communicator 管理 LDAP 客户机也将使用的证书。或者，可以使用 `certutil` 命令行工具管理证书数据库。

通过 Communicator 管理客户机证书

以下过程介绍如何使用 Netscape Communicator 在客户机中管理证书数据库。

1. 启动时， Netscape Communicator 将确保证书数据库存在，否则它将在需要时创建一个证书数据库。证书数据库将与其他 Communicator 首选项一起存储在一个文件中 （例如，在 UNIX 系统上，`/home/`*`username`*`/.netscape/cert7.db`）。

   如果使用此过程，请找到由 Communicator 创建的证书数据库，并记住客户机应用程序使用的路径。

2. 使用 Communicator 浏览为要访问的 Directory Server 颁发证书的证书授权机构的网站。Communicator 将自动检索证书授权机构的证书，并询问您是否信任此证书。

   例如，如果正在使用内部部署的 Sun ONE 证书服务器，请转到具有 `https://`*`hostname`*`:444` 形式的 URL。

3. Communicator 提示您信任证书授权机构的证书时，请遵照执行。应该信任 CA 证书以进行服务器验证。

   根据 CA 的网站规定，此步骤可能无法执行。如果 Communicator 未自动提示您信任 CA 证书，请使用以下步骤手动执行。

通过命令行管理客户机证书

使用 `certutil` 工具通过命令行管理证书。Sun ONE Directory Server Resource Kit 中提供有此工具。详细信息，请参阅 *Sun ONE Directory Server Resource Kit 工具参考* 中的第 30 章 “安全工具”。

1. 在客户机主机上，请使用以下命令创建证书数据库：

   ```
   certutil -N -d 路径 -P 前缀
   ```

   该工具将提示用户输入口令以保护证书。然后，该工具将创建以下文件：*路径* / *前缀* cert7.db 和 *路径* / *前缀* key3.db。

   应该由 LDAP 客户机应用程序的用户在只能由其访问的位置单独创建证书数据库 （例如，其主目录受保护的子目录）。

2. 请与为要访问的 Directory Server 颁发证书的证书授权机构联系，并请求 CA 证书。可以通过发送电子邮件或访问他们的网站，以获得 PKCS #11 证书的 PEM 编码的文本版本。将此证书保存到文件中。

   例如，如果正在使用内部部署的 Sun ONE 证书服务器，请转到具有 https://*hostname*:444 形式的 URL。在顶级 “检索”标签中，选择 “导入 CA 证书链接”并复制那里的已编码证书。

   或者，如果从同一 CA 中获得客户机证书和服务器证书，则可以重复使用通过“信任证书授权机构”（第 325 页）中的过程获得的 CA 证书。

3. 将 CA 证书作为受信任的 CA （用于颁发在 SSL 连接中使用的服务器证书）导入。使用以下命令：

   ```
   certutil -A -n "certificateName" -t "C,," -a -i certFile -d 路径 -P 前缀
   ```

   其中， *certificateName* 是给定的用来标识此证书的名称， *certFile* 是包含 PEM 编码文本格式的 PKCS #11 授权机构证书的文本文件，路径和前缀与步骤 1 中的相同。

   LDAP 客户机应用程序的每个用户都必须将 CA 证书导入至其证书数据库中。所有用户可以导入位于 *certFile* 中的相同证书。

指定 SSL 选项以进行服务器验证

要使用 ldapsearch 工具在 SSL 中执行服务器验证，用户仅需指定其证书数据库的路径即可。通过安全端口建立 SSL 连接时，服务器将发送其证书。然后，ldapsearch 工具将在用户的证书数据库中查找颁发服务器证书的 CA 受信任的 CA 证书。

以下命令显示了用户如何指定其证书数据库 （如果此数据库是由 Netscape Communicator 创建的）：

```
ldapsearch -h 主机 -p securePort \
           -D "uid=bjensen,dc=example,dc=com" -w bindPassword \
           -Z -P /home/bjensen/.netscape/cert7.db \
           -b "dc=example,dc=com" "(givenname=Richard)"
```

在客户机中配置基于证书的验证

客户机验证的默认机制将使用证书来安全地识别 Directory Server 的用户。要执行基于证书的客户机验证，您必须：

- 为每个目录用户获取一个证书，并将其安装在客户机应用程序可以访问到的地方。
- 使用同一证书的二进制副本配置用户的目录条目。验证期间，服务器将客户机应用程序提交的证书与此副本相匹配，以明确地标识该用户。
- 按照 *Sun ONE Server Console 服务器管理指南* 中第 10 章 “使用客户机验证”中的说明，配置服务器以基于证书进行验证。
- 为基于证书的验证指定 LDAP 客户机的 SSL 选项。

这些步骤需要 `certutil` 工具通过命令行管理证书。 Sun ONE Directory Server Resource Kit 中提供有此工具。详细信息，请参阅 *Sun ONE Directory Server Resource Kit 工具参考* 中第 30 章 “安全工具”。

获得并安装用户证书

必须由希望利用基于证书的验证来访问目录的每位用户请求并安装客户机证书。此过程假设用户已经按照 “在客户机中配置服务器验证”（第 339 页）中的说明配置了证书数据库。

1. 请使用以下命令创建用户证书请求：

   ```
   certutil -R \
   -s "cn=Babs Jensen,ou=Sales,o=example.com,l=城市,st=区,c=国家（地区）"\
   -a -d 路径 -P 前缀
   ```

   `-s` 选项指定所请求证书的 DN。通常，证书授权机构会要求此示例中显示的所有属性，以完整地标识证书的拥有者。通过步骤 9 中的证书映射机制，证书 DN 将被映射至用户的目录 DN。

   路径和前缀将查找用户的证书和密钥数据库。 `certutil` 工具将提示用户输入其密钥数据库的口令。然后，此工具将生成 PEM 编码文本格式的 PKCS #10 证书请求。

2. 然后按照规定步骤将编码的证书请求保存到一个文件中，并将其传输至您的证书授权机构。例如，可能会要求您以电子邮件的形式发送证书请求，或者也可以通过 CA 的网站输入请求。

3. 发送了请求后，必须等待 CA 对您的证书作出响应。请求响应时间会有所不同。例如，如果 CA 在您公司内部，可能只需要一到两天时间就可响应请求。如果选择了公司外部的 CA，则可能需要几周的时间来响应请求。

4. CA 发送响应后，请将新证书的 PEM 编码文本下载或复制到一个文本文件。还应将编码的证书备份到一个安全的地方。如果系统曾丢失证书数据，则可使用备份文件重新安装证书。

5. 请使用以下命令在证书数据库中安装新的用户证书：

   ```
   certutil -A -n "certificateName" -t "u,," -a -i certFile -d 路径 -P 前缀
   ```

   其中， *certificateName* 是给定的用来标识证书的名称， *certFile* 是包含 PEM 格式的 PKCS #11 证书的文本文件，路径和前缀与步骤 1 中的相同。

   或者，如果通过 Netscape Communication 管理证书数据库，则在 CA 的网站中可能有一个可以直接安装证书的链接。单击此链接，并按照 Communicator 显示的对话框逐步执行操作。

6. 请使用以下命令创建证书的二进制副本：

   ```
   certutil -L -n "certificateName" -d 路径 -r > userCert.bin
   ```

   其中 *certificateName* 是安装证书时给定的证书名称，路径是证书数据库的位置，*userCert.bin* 是将包含二进制格式证书的输出文件的名称。

7. 在 Directory Server 上，将 `userCertificate` 属性添加至拥有客户机证书的用户的目录条目中。

- 要通过控制台添加证书，请执行以下操作：

  a. 在 Directory Server 控制台的顶级 “目录” 标签中，在目录树中找到用户条目，右键单击此条目并在弹出菜单中选择 “使用通用编辑器编辑”。

  b. 在 “通用编辑器” 中，单击 “添加属性”，并从弹出的对话框中选择 `userCertificate` 属性。

  c. 在 “通用编辑器” 中找到新的 `userCertificate` 字段。单击对应的 “设置值” 按钮为此属性设置二进制值。

  d. 在 “设置值” 对话框中，输入步骤 6 中创建的 *userCert.bin* 文件的名称，或者单击 “浏览” 查找该文件。

  e. 在 “设置值” 对话框中单击 “确定”，然后在 “通用编辑器” 中单击 “保存”。

- 要通过命令行添加证书，请使用下面示例中显示的 `ldapmodify` 命令。此命令使用 SSL 通过安全连接发送证书：

  ```
  ldapmodify -h 主机 -p securePort \
             -D "uid=bjensen,dc=example,dc=com" -w bindPassword \
             -Z -P /home/bjensen/.netscape/cert7.db
  version: 1
  ```

```
dn:uid=bjensen,dc=example,dc=com
changetype:modify
add:userCertificate
userCertificate:< file:///path/userCert.bin
```

< 前后的空格非常重要，必须完全按照显示的形式保留空格。要使用 < 语法来指定文件名，您必须以行 `version:1` 作为 LDIF 语句的开头。`ldapmodify` 处理此语句时，它将该属性设置为可以从给定文件的全部内容中读取的值。

8. 在 Directory Server 上，必要时安装并信任颁发用户证书的 CA 的证书。必须信任此 CA 以接受来自客户机的连接。请参阅 “信任证书授权机构”（第 325 页）。

9. 按照 *Sun ONE Server Console 服务器管理指南* 中第 10 章 “使用客户机验证”中的说明，配置 Directory Server 以基于证书进行验证。在此过程中，可以编辑 `certmap.conf` 文件，这样服务器会将通过 LDAP 客户机提交的用户证书映射至对应的用户 DN。

   确保在 `certmap.conf` 文件中， `verifyCert` 参数已设置为 `on`。然后，服务器将验证包含相同证书的用户条目，从而明确地标识用户。

为基于证书的客户机验证指定 SSL 选项

要使用 `ldapsearch` 工具在 SSL 中执行基于证书的客户机验证，用户需要指定若干命令行选项以使用其证书。通过安全端口建立 SSL 连接时，此工具将验证服务器的证书，然后将用户证书发送至服务器。

以下命令显示了用户如何指定用来访问其证书数据库 （如果此数据库是由 Netscape Communicator 创建的）的选项：

```
ldapsearch -h 主机 -p securePort \
           -Z -P /home/bjensen/.netscape/cert7.db \
           -N "certificateName" \
           -K /home/bjensen/.netscape/key3.db -W keyPassword \
           -b "dc=example,dc=com" "(givenname=Richard)"
```

`-Z` 选项表示基于证书的验证， *certificateName* 指定要发送的证书， `-K` 和 `-W` 选项允许客户机应用程序访问证书，从而可以发送证书。如果未指定 `-D` 和 `-w` 选项，将从证书映射来确定绑定 DN。

在客户机中使用 SASL DIGEST-MD5

在客户机中使用 DIGEST-MD5 机制时，不需要安装用户证书。不过，如果希望使用加密的 SSL 连接，则仍然必须信任服务器证书，如 “在客户机中配置服务器验证”（第 339 页）中所述。

指定领域

领域定义从中选择验证标识的名称空间。在 DIGEST-MD5 验证中，必须验证特定的领域。

Directory Server 使用完全符合要求的主机名作为 DIGEST-MD5 的默认领域。服务器将使用在 `nsslapd-localhost` 配置属性中找到的主机名的小写字母值。

如果未指定领域，则将使用服务器提供的默认领域。

指定环境变量

在 UNIX 环境中，必须设置 `SASL_PATH` 环境变量，这样 LDAP 工具将会找到 DIGEST-MD5 库。 DIGEST-MD5 库是 SASL 插件动态加载的共享库，因此应按如下所示设置 SASL_PATH 变量 （以在 Korn shell 中为例）：

```
export SASL_PATH=ServerRoot/lib/sasl
```

此路径假设 Directory Server 安装在将调用 LDAP 工具的同一主机上。

在 Windows 上，至 SASL 库的路径是在以下注册表密钥中指定的：`[HKEY_LOCAL_MACHINE\SOFTWARE\Carnegie Mellon\Project Cyrus\SASL Library\Available Plugins]`。如果已在相同主机上安装了 Directory Server，则此密钥将自动设置为 *ServerRoot*`/lib/sasl`，且无需对其进行修改。

ldapsearch 命令的示例

无需使用 SSL，即可执行 DIGEST-MD5 客户机验证。下面的示例将使用默认的 DIGEST-MD5 标识映射来确定绑定 DN：

```
ldapsearch -h 主机 -p nonSecurePort -D "" -w bindPassword \
           -o mech=DIGEST-MD5 [-o realm="hostFQDN"] \
           -o authid="dn:uid=bjensen,dc=example,dc=com" \
           -o authzid="dn:uid=bjensen,dc=example,dc=com" \
           -b "dc=example,dc=com" "(givenname=Richard)"
```

上面的示例说明了如何使用 `-o`（o 为小写字母）选项来指定 SASL 选项。Realm 是可选的，但是如果指定了 Realm，则该 Realm 必须为服务器主机的完全符合要求的域名。虽然未使用面向代理操作的 `authzid`，但是 `authid` 和 `authzid` 必须同时出现且相同。

`authid` 的值是标识映射中使用的 Principal。建议 `authid` 应包含 `dn:` 前缀（后面跟目录中的有效用户 DN）或 `u:` 前缀 （后面跟客户机确定的任意字符串）。这样，您就可以使用 “DIGEST-MD5 标识映射”（第 332 页）中所示的映射。

通常，您可能希望有一个 SSL 连接以提供通过安全端口的加密，还希望有 DIGEST-MD5 以便提供客户机验证。下面的示例将通过 SSL 执行相同操作：

```
ldapsearch -h 主机 -p securePort \
           -Z -P /home/bjensen/.netscape/cert7.db \
           -N "certificateName" -W keyPassword \
           -o mech=DIGEST-MD5 [-o realm="hostFQDN"] \
           -o authid="dn:uid=bjensen,dc=example,dc=com" \
           -o authzid="dn:uid=bjensen,dc=example,dc=com" \
           -b "dc=example,dc=com" "(givenname=Richard)"
```

在此示例中， `-N` 和 `-W` 选项是 `ldapsearch` 命令必需的，但它们并不用于客户机验证。相反，服务器将再次执行具有 `authid` 值的 Principal 的 DIGEST-MD5 标识映射。

在客户机中使用 Kerberos SASL GSSAPI

在客户机中使用 GSSAPI 机制时，不需要安装用户证书，但必须配置 Kerberos V5 安全系统。而且，如果希望使用加密的 SSL 连接，则必须信任服务器证书，如“在客户机中配置服务器验证”（第 339 页）中所述。

在客户机主机上配置 Kerberos V5

必须在将运行 LDAP 客户机的主机上配置 Kerberos V5：

1. 请按照其安装说明来安装 Kerberos V5。 Sun 建议安装 Sun 企业验证机制 (SEAM) 1.0.1 客户机软件。
2. 配置 Kerberos 软件。使用 SEAM，配置 `/etc/krb5` 下的文件，以便设置 `kdc` 服务器、定义默认领域以及 Kerberos 系统要求的其他所有配置。
3. 必要时，修改文件 `/etc/gss/mech`，这样列出的第一个值为 `kerberos_v5`。

指定 SASL 选项以进行 Kerberos 验证

1. 使用启用了 GSSAPI 的客户机应用程序前，必须使用下面的命令初始化具有用户 Principal 的 Kerberos 安全系统：

   `kinit` *userPrincipal*

   userPrincipal 是 SASL 标识，例如 `bjensen@example.com`。

2. `ldapsearch` 工具的以下示例说明了如何使用 `-o`（o 为小写字母）选项来指定用于使用 Kerberos 的 SASL 选项：

```
ldapsearch -h 主机 -p securePort \
           -Z -P /home/bjensen/.netscape/cert7.db \
           -N "certificateName" -W keyPassword \
           -o mech=GSSAPI [-o realm="example.com" \
           -o authid="bjensen@example.com" \
           -o authzid="bjensen@example.com"] \
           -b "dc=example,dc=com" "(givenname=Richard)"
```

在此示例中， `-N` 和 `-W` 选项是 `ldapsearch` 命令必需的，但它们并不用于进行客户机验证。可以忽略 `realm`、`authid` 和 `authzid`，这是因为它们将出现在由 `kinit` 命令初始化的 Kerberos 缓存中。如果出现，虽然未使用面向代理操作的 `authzid`，但 `authid` 和 `authzid` 必须相同。`authid` 的值是标识映射中使用的 Principal。详细信息，请参阅 “GSSAPI 标识映射”（第 335 页）。

第 12 章

管理日志文件

本章说明如何通过配置日志记录策略和分析服务器维护的状态信息来监视 Directory Server。

Sun ONE Directory Server 提供三种类型的日志：

- 访问日志 - 列出连接到服务器的客户机。
- 错误日志 - 提供有关服务器错误的信息。
- 审核日志 - 给出对后缀及配置的访问的详细信息。

服务器中的状态信息包括有关连接和缓存活动的统计信息。可以通过 Directory Server 控制台获得该信息，对于监视条目中的信息，可以通过 LDAP 命令行工具查看。有关使用 SNMP 以监视服务器的信息，请参阅第 13 章 “使用 SNMP 监视 Directory Server”。

本章包含以下小节：

- 定义日志文件策略
- 访问日志
- 错误日志
- 审核日志
- 监视服务器的活动

定义日志文件策略

以下各节说明如何定义日志文件创建策略和删除策略。

定义日志文件轮换策略

如果希望目录定期对当前日志进行存档并启动新的日志，则可以在 Directory Server 控制台中定义日志文件轮换策略。可以配置下列参数：

- 希望目录保留的日志总量。当目录达到此日志数量时，它将在创建新的日志之前删除文件夹中最旧的日志文件。默认值为 10 个日志。请不要将此值设置为 1。否则，目录将不轮换日志，并且日志将无限增大。
- 每个日志文件的最大值 （以 MB 计）。如果不想设置最大值，请在此字段中键入 -1。默认值为 100 MB。日志文件达到此最大值 （或在下一步中定义的最大存留期）后，目录将对日志文件进行存档并启动一个新的日志文件。如果将最大的日志数量设置为 1，目录将忽略此属性。
- 目录对当前日志文件进行存档并创建一个新日志文件的周期，可以通过输入分钟数、小时数、天数、周数或月数来进行设置。默认值为每天。如果将最大的日志数量设置为 1，目录将忽略此属性。

定义日志文件删除策略

如果希望目录自动删除旧的存档日志，则可以从 Directory Server 控制台定义日志文件删除策略。

注意 只有在以前定义过日志文件轮换策略的情况下，日志删除策略才有意义。如果只有一个日志文件，日志文件删除将不起作用。

服务器在日志轮换时评估并应用日志文件删除策略。

可以配置下列参数：

- 组合的存档日志的最大值。达到此最大值时，最旧的存档日志将被自动删除。如果不想设置最大值，请在此字段中键入 -1。默认值为 500 MB。如果将日志文件的数量设置为 1，此参数将被忽略。
- 可用磁盘空间的最小值。当可用磁盘空间达到此最小值时，最旧的存档日志将被自动删除。默认值为 5 MB。如果将日志文件的数量设置为 1，此参数将被忽略。

- 日志文件的最大存留期。当日志文件达到此最大存留期时，该日志文件将被自动删除。默认值为 1 个月。如果将日志文件的数量设置为 1，此参数将被忽略。

手动轮换日志文件

如果尚未设置自动的日志文件创建或删除策略，则可以手动轮换日志文件。默认情况下，可在下列目录中找到访问日志文件、错误日志文件和审核日志文件：

ServerRoot/slapd-*serverID*/logs

要手动轮换日志文件，请执行以下操作：

1. 关闭服务器。有关说明，请参阅 “启动和停止 Directory Server”（第 20 页）。
2. 移动或重命名要轮换的日志文件，以防将来参考时需要旧的日志文件。
3. 重新启动服务器。有关说明，请参阅 “启动和停止 Directory Server”（第 20 页）。

   服务器将按照每个日志配置自动创建新的文件。

访问日志

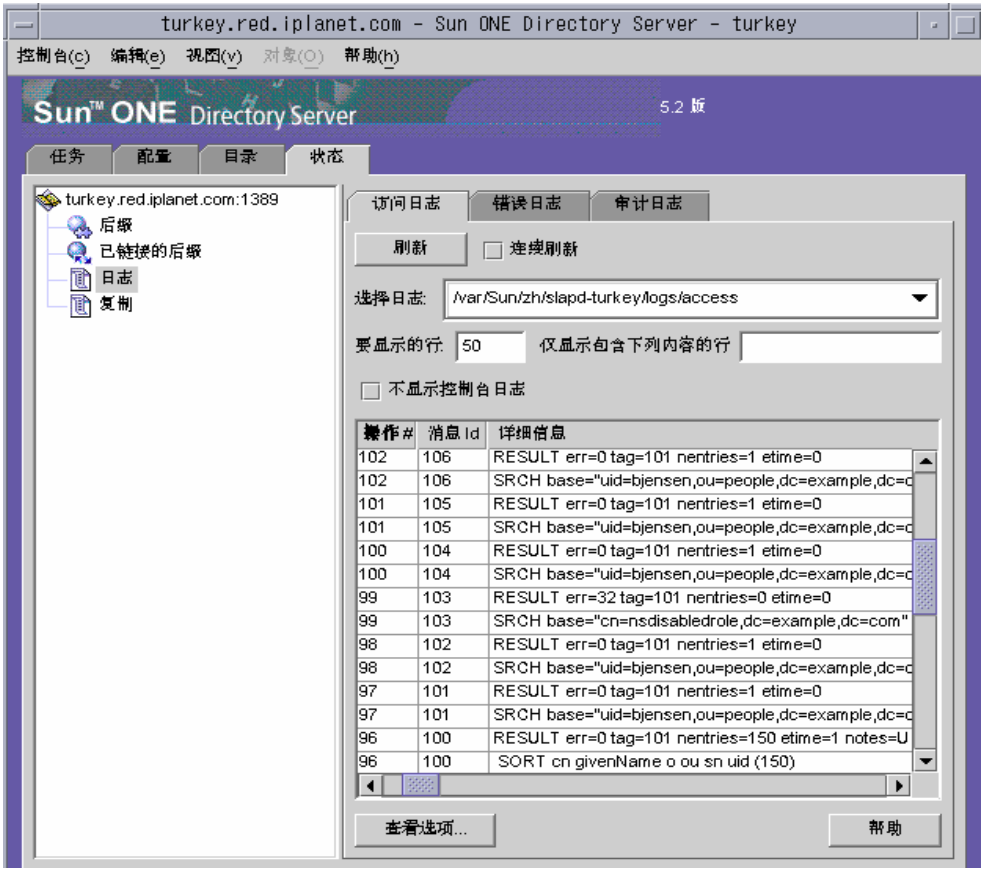
访问日志包含有关目录与客户机之间连接的详细信息。

查看访问日志

1. 在 Directory Server 控制台的顶级 “状态”标签上，选择 “日志”图标，然后在右侧面板中选择 “访问日志”标签。

   该标签显示一个表格，其中包含所选的访问日志中最新的条目，如下图所示。有关访问消息的说明，请参阅 *Sun ONE Directory Server 参考手册* 中的第 8 章 “访问日志和连接代码”。

图 12-1 查看日志内容



2. 要刷新当前显示内容，请单击 “刷新”。如果希望显示内容每 10 秒自动刷新一次，请选中 “连续刷新”复选框。
3. 要查看其他的访问日志文件，请从 “选择日志”下拉菜单中进行选择。
4. 要显示其他数量的消息，请在 “要显示的行”文本框中输入想要查看的数目，然后单击 “刷新”。
5. 要过滤日志消息，可以在 “仅显示包含下列内容的行”文本框中输入字符串，然后单击 “刷新”。此外，还可以选择 “不显示控制台日志”复选框，这样将过滤掉从控制台到服务器的连接所产生的所有消息。
6. 要修改日志条目表的列，请单击 “视图”选项。使用 “视图选项”对话框的控件更改列的顺序、添加或删除列，并选择一列以对表进行排序。

配置访问日志

可以通过对许多设置进行配置来定制访问日志，包括目录存储访问日志的位置以及存储创建和删除策略的位置。

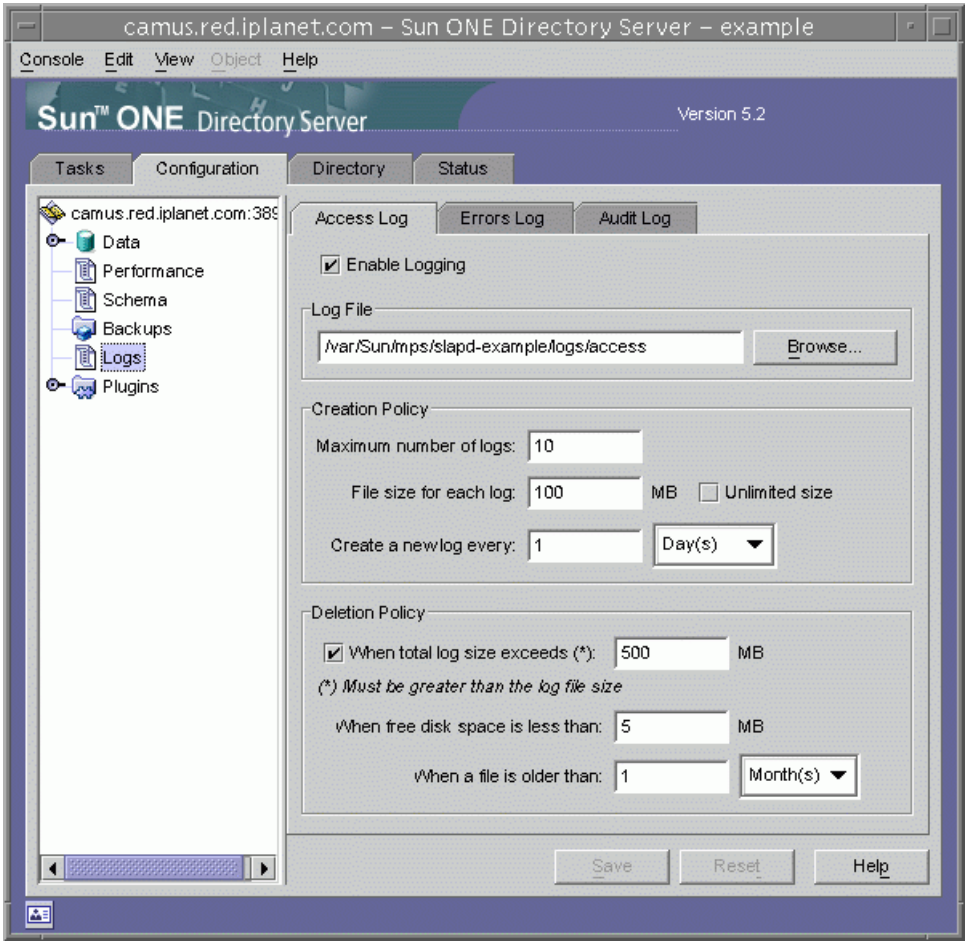
还可以禁用目录的访问日志记录。之所以这样做是因为访问日志的增长速度很快（对目录每访问 2,000 次将导致访问日志大约增加 1 MB）。但是，关闭访问日志记录之前，请仔细查看该访问日志是否提供了有益的疑难解答信息。

要配置目录的访问日志，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，选择 “日志”图标，然后在右侧面板中选择 “访问日志”标签。

   此标签包含访问日志的配置设置，如下图所示：

图 12-2　　日志文件轮换和删除的配置面板



2. 要启用访问日志记录，请选中 “启用日志记录”复选框。

   如果不希望目录维护访问日志，请清除该复选框。

   默认情况下，访问日志记录处于启用状态。

3. 在 “日志文件”字段中，输入希望该目录用于存储访问日志的完整路径和文件名。默认文件为：

   ServerRoot/slapd-*serverID*/logs/access

4. 设置日志的最大数量、日志大小和存档周期。

   有关这些参数的信息，请参阅 “定义日志文件轮换策略”（第 348 页）。

5. 设置组合的存档日志的最大值、可用磁盘空间的最小值以及日志文件的最大存留期。

   有关这些参数的信息，请参阅 “定义日志文件删除策略”（第 348 页）。

6. 完成更改之后，请单击 “保存”。

错误日志

错误日志包含有关日常操作过程中目录遇到的错误和事件的详细信息。

查看错误日志

1. 在 Directory Server 控制台的顶级 “状态”标签上，选择 “日志”图标，然后在右侧面板中选择 “错误日志”标签。

   该标签显示一个表格，其中包含所选的错误日志中最新的条目，如图 12-1（第 350 页）中所示的条目。有关错误消息的说明，请参阅 *Sun ONE Directory Server 参考手册* 中的附录 A “错误代码”。

2. 要刷新当前显示内容，请单击 “刷新”。如果希望显示内容每 10 秒自动刷新一次，请选中 “连续刷新”复选框。

3. 要查看已存档的错误日志，请从 “选择日志”下拉菜单中进行选择。

4. 要指定其他数量的消息，请在 “要显示的行”文本框中输入想要查看的数目，然后单击 “刷新”。

5. 要过滤日志消息，可以在 “仅显示包含下列内容的行”文本框中输入字符串，然后单击 “刷新”。此外，还可以选择 “不显示控制台日志”复选框，这样将过滤掉从控制台到服务器的连接所产生的所有错误消息。

6. 要修改日志条目表的列，请单击 “视图”选项。使用 “视图选项”对话框的控件更改列的顺序、添加或删除列，并选择一列以对表进行排序。

配置错误日志

可以更改错误日志的若干设置，包括目录存储日志的位置以及希望目录在日志中包含的内容。

要配置错误日志，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，选择 “日志”图标，然后在右侧面板中选择 “错误日志”标签。

   此标签包含错误日志的配置设置，如图 12-2 （第 352 页）中所示。

2. 要启用错误日志记录，请选中 “启用日志记录”复选框。

   如果不希望目录维护错误日志，请清除该复选框。

   默认情况下，错误日志记录处于启用状态。

3. 如果要在错误日志中设置详细信息的等级，请单击 “日志等级”按钮以显示 “错误日志等级”对话框。选择要查看其更多错误消息和调试信息的一个或多个内部产品组件。或者，选中 “详细”复选框以返回最大数量的运行时输出，包括无价值的消息。

   更改这些值的默认值可能使错误日志迅速增长，因此必须计划出充足的磁盘空间。为此建议不要更改日志等级，除非 Sun ONE “客户支持”要求您这样做。

4. 在 “日志文件”字段中，输入希望用于存储错误日志的目录的完整路径和文件名。默认文件为：

   ServerRoot/slapd-*serverID*/logs/error

5. 设置日志的最大数量、日志大小和存档周期。

   有关这些参数的信息，请参阅 “定义日志文件轮换策略”（第 348 页）。

6. 设置组合的存档日志的最大值、可用磁盘空间的最小值以及日志文件的最大存留期。

   有关这些参数的信息，请参阅 “定义日志文件删除策略”（第 348 页）。

7. 完成更改之后，请单击 “保存”。

审核日志

审核日志包含有关对每个后缀和服务器配置所做更改的详细信息。不同于访问日志和错误日志，审核日志不是默认启用的。在查看日志前，必须启用审核日志。

配置审核日志

可以使用 Directory Server 控制台启用和禁用审核日志记录，并指定存储审核日志文件的位置。

要配置审核日志，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，选择 “日志”图标，然后在右侧面板中选择 “审核日志”标签。

   此标签包含审核日志的配置设置，如图 12-2 （第 352 页）中所示。

2. 要启用审核日志记录，请选中 “启用日志记录”复选框。

   要禁用审核日志记录，请清除该复选框。默认情况下，审核日志记录处于禁用状态。

3. 在 “日志文件”字段中，输入希望用于存储审核日志的目录的完整路径和文件名。默认文件为：

   ServerRoot/slapd-*serverID*/logs/audit

4. 设置日志的最大数量、日志大小和存档周期。

   有关这些参数的信息，请参阅 “定义日志文件轮换策略”（第 348 页）。

5. 设置组合的存档日志的最大值、可用磁盘空间的最小值以及日志文件的最大存留期。

   有关这些参数的信息，请参阅 “定义日志文件删除策略”（第 348 页）。

6. 完成更改之后，请单击 “保存”。

查看审核日志

1. 在 Directory Server 控制台的顶级 “状态”标签上，选择 “日志”图标，然后在右侧面板中选择 “审核日志”标签。

   该标签显示一个表格，其中包含所选的审核日志中最新的条目，如图 12-1（第 350 页）中所示的条目。

2. 要刷新当前显示内容，请单击 “刷新”。如果希望显示内容每 10 秒自动刷新一次，请选中 “连续刷新”复选框。

3. 要查看已存档的审核日志，请从 “选择日志”下拉菜单中进行选择。

4. 要显示其他数量的消息，请在 “要显示的行”文本框中输入想要查看的数目，然后单击 “刷新”。

5. 要过滤日志消息，可以在 “仅显示包含下列内容的行”文本框中输入字符串，然后单击 “刷新”。

监视服务器的活动

服务器总是维护计数器及其活动的统计信息，例如所有后缀的连接数、操作数和缓存活动。该信息能帮助您对所有错误进行故障排除并观察服务器的性能。可以从 Directory Server Console 或命令行来监视目录服务器的当前活动。

可供监视的许多参数既反映 Directory Server 的性能，又受配置和调整的影响。有关可配置的属性及其调整方式的信息，请参阅 *Sun ONE Directory Server 安装和调整指南*。

使用控制台监视服务器

1. 在 Directory Server 控制台的顶级 “状态”标签上，选择位于状态树根的服务器图标。

   右侧面板显示有关服务器活动的当前信息。如果服务器当前并未运行，此标签将不提供任何性能监视信息。

2. 单击 “刷新”以刷新当前显示内容。如果希望服务器持续更新所显示的信息，请选中 “连续刷新”复选框。

   该服务器状态面板显示：

- 服务器启动时的日期和时间。
- 服务器上的当前日期和时间。启用复制时，应定期检查各个服务器上的日期是否开始出现差异。
- 资源概述表。对于以下每个资源，资源概述表列出了自启动后的总数目和每分钟的平均数。

表 12-1　资源概述表

资源	自启动后的总数目和每分钟平均数目
连接数	建立的客户机连接数。
初始化的操作数	由客户机请求的操作数。
完成的操作数	客户机未放弃的操作数。
发送到客户机的条目数	搜索结果返回的条目数。
发送到客户机的字节数	对所有客户机请求响应的字节数。

- 当前资源使用表。此表格显示面板最后刷新时正在使用的以下资源。

表 12-2 当前资源使用

资源	最新实时使用率
活动线程数	用于处理请求的线程数。其他线程可能是由内部服务器机制创建的，如复制和链接。
打开的连接数	每个连接可以启动多项操作，因此也可以启动多个线程。
其他可用的连接数	服务器可以同时打开的其他连接的总数。这一总数基于当前打开的连接数和允许服务器打开的并发连接总数。在大多数情况下，后者的值由操作系统确定，并用任务可用的文件描述符数来表示。 在 Windows 和 AIX 上，允许的并发连接数是由操作系统生成的，但它并不基于文件描述符。详细信息，请参阅操作系统文档。
等待从客户机读取的线程数	如果服务器开始从客户机接收请求，接着由于某些原因该请求的传输被中止，那么该线程可能正在等待读取。通常，如果有等待读取的线程，则说明网络速度慢或客户机速度慢。
使用的数据库数	该服务器宿主的后缀数。该数目不包括已链接的后缀。

- 连接状态表。此表显示有关当前每个打开的连接的以下信息。

表 12-3 连接状态表

列标头	说明
打开时间	建立连接时服务器上的时间。
初始化的	连接期间请求的操作数。
完成的操作数	连接期间，客户机未中止而由服务器完成的操作数。
绑定为	给出客户机绑定到服务器时使用的标识名称。如果客户机尚未通过服务器的验证，那么该列将显示 `not bound`。
状态	• 未阻塞 - 表示服务器空闲，或正通过连接发送数据或接收数据。 • 阻塞 - 表示服务器正在等待通过连接读取或写入数据。这可能是由于网络速度慢或客户机速度慢。
类型	表明它是 LDAP 连接还是 DSML-over-HTTP 连接。

3. 在左侧状态树中单击 “后缀”节点。该面板显示有关每个后缀的数据库缓存中条目缓存和索引使用率的监视信息，如下图所示。

图 12-3 后缀监视面板

设置刷新模式 （如果需要）。单击面板底部的 “显示后缀”，选择要在表中列出的后缀。

- 第一个表格显示有关每个条目缓存的以下信息。

表 12-4 条目缓存使用率

列标头	说明
后缀	后缀的基准 DN。
命中次数	从缓存 （而非磁盘）读取的条目数。
尝试次数	从缓存请求的条目数。
命中率 (%)	命中次数与尝试次数的比率 （以百分比表示）。
大小 (MB)	来自给定后缀的条目缓存内容的当前大小。
最大大小 (MB)	当前配置中缓存的最大大小。
大小 （条目）	来自给定后缀的缓存中条目的当前数目。
最大大小 （条目）	当前配置中缓存条目的最大数目。

以下表格显示对每个后缀的数据库缓存的访问。

- 第一个表格显示通过配置的索引对数据库缓存的访问。从属性名称列表中，选择要查看其索引统计信息的某一属性。该表将仅显示所选属性已在其中索引的后缀的数据。
- “条目访问”表格显示对检索条目的数据库缓存的访问。
- 最后一个表格中的 “总量”显示对所有数据库缓存的所有组合访问。

所有三个表格都具有以下列：

表 12-5 对数据库缓存的访问

列标头	说明
后缀	后缀的基准 DN。
命中次数	通过索引读取的条目数。
尝试次数	通过索引请求的条目数。
命中率 (%)	命中次数与尝试次数的比率 （以百分比表示）。
读入页	从磁盘读入后缀缓存的页数。
写出页	从缓存写回磁盘的页数。每当一个读写页经过修改后而从缓存中被删除以便为新页面留出空间时，就有一个后缀页被写入磁盘。

- 在表格的下面，以下页退出是所有数据库缓存的累积数。从缓存退出的页必须写入磁盘，这样可能会影响服务器性能。退出的页数越少，则性能越好：
  - 读写页面退出 - 表示为给新页腾出空间而从缓存退出的读写页数。此值不同于写出的页数，因为这些页是未经修改而退出的读写页。
  - 只读页面退出 - 表示为给新页腾出空间而从缓存退出的只读页数。

4. 如果适用，请在左侧状态树中单击“已链接的后缀”节点。该面板显示有关访问在目录中配置的链接后缀的信息。设置刷新模式（如果需要）。

   在列表中选择已链接后缀的 DN 以查看其统计信息。右侧的列表列出了所有在已链接后缀上执行的不同操作的计数。

从命令行监视服务器

通过在以下条目上执行搜索操作，可以从任意 LDAP 客户机监视目录服务器的当前活动：

- `cn=monitor`
- `cn=monitor, cn=ldbm database, cn=plugins, cn=config`
- `cn=monitor,cn=`*`dbName`*`,cn=ldbm database,cn=plugins,cn=config`
- `cn=monitor,cn=`*`dbName`*`,cn=chaining database,cn=plugins,cn=config`

其中 *dbName* 是要监视的后缀的数据库名称。注意，除了有关每个连接的信息以外，默认情况下，`cn=monitor` 条目是任何人都可读的（包括匿名绑定的客户机）。

以下示例显示如何查看常规服务器统计信息：

```
ldapsearch -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令 \
           -s base -b "cn=monitor" "(objectclass=*)"
```

有关这些条目中可用的所有监视属性的说明，请参阅 *Sun ONE Directory Server 参考手册* 中相应的小节：

- 第 4 章中的“监视属性”
- 第 5 章中的“数据库监视属性”
- 第 5 章中的“cn=*dbName* 下的数据库监视属性”
- 第 5 章中的“已链接后缀监视属性”

第 13 章

使用 SNMP 监视 Directory Server

简单网络管理协议 (SNMP) 是标准化管理协议，用于实时监视和管理设备及程序。Directory Server 提供副代理接口，以便可以由 SNMP 管理应用程序对它进行监视。这样，可以使网络应用程序了解目录服务器的状态，并获得有关其活动的标准。

不过， Directory Server SNMP 副代理只包含只读值，而且 SNMP 管理应用程序不能在服务器上执行操作。副代理也不发送 SNMP 陷阱，这些陷阱是报告事件的消息。

通常，第 12 章 “管理日志文件”中描述的活动和错误日志提供有关服务器的详细信息， LDAP 是选择用于安全访问和修改服务器配置的协议。但是， SNMP 副代理不允许 Directory Server 实例参与现有的网络管理系统。

本章包括以下主题：

- Sun ONE Server 中的 SNMP
- Directory Server MIB 概述
- 设置 SNMP
- 在 Directory Server 中配置 SNMP
- 启动和停止 SNMP 副代理

Sun ONE Server 中的 SNMP

SNMP 允许管理应用程序查询运行代理或副代理应用程序的应用程序和设备。SNMP 代理或副代理从应用程序或设备那里收集信息以响应 SNMP 管理器的查询。此信息在代理的管理信息库 (MIB) 定义的表格中被构造为变量。

通常情况下，网络管理员会在副代理中查询 SNMP 变量，然后副代理返回请求的值。 SNMP 还定义一种机制，这种机制允许代理通过将陷阱消息发送给所有网络管理员来报告事件。但是， Directory Server 不实施陷阱，其副代理永远都不会发送陷阱消息。

可以在一台主机上安装多个副代理。例如，如果在同一台主机上安装了 Directory Server、 Enterprise Server 和 Messaging Server，则其中每台服务器的副代理都会与同一个主代理进行通讯。在 Windows 环境中，主代理是由 Windows 操作系统提供的 SNMP 服务。在 UNIX 环境中，主代理是与 Sun ONE Administration Server 一起安装的。

详细信息，请参阅 *Sun ONE Server Console 服务器管理指南* 中的第 11 章“使用 SNMP 监视服务器”。

通过 SNMP 设置要监视的服务器的一般步骤如下：

1. 编译 Directory Server MIB 并将其集成到 SNMP 管理系统。请参阅系统文档。
2. 根据您的平台，在计算机上设置 SNMP，然后通过 Administration Server 控制台来配置和启动 SNMP 主代理。
3. 通过 Directory Server 控制台配置 SNMP 副代理。
4. 通过 Directory Server 控制台启动 SNMP 副代理 （如果适用于您的平台）。
5. 访问由 MIB 定义且通过代理公开的 SNMP 托管对象。此步操作完全依赖于您的 SNMP 管理系统。

Directory Server 配置的特定步骤将在后面的小节中进行说明。

Directory Server MIB 概述

Directory Server 的 MIB 具有以下对象标识符：

```
iso.org.dod.internet.private.enterprises.netscape.nsldap
(nsldapd OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.1450.7 }}
```

而且在下面的文件中对它进行了定义：

ServerRoot/plugins/snmp/netscape-ldap.mib

MIB 定义可通过 SNMP 监视的变量及其所包含值的类型。目录 MIB 分为四个不同的托管对象表：

- 操作表 - 包含有关目录服务器中的绑定、操作、引荐和错误的统计信息。目录的 `cn=snmp,cn=monitor` 条目的属性中也提供有这些变量的值。请参阅 *Sun ONE Directory Server 参考手册* 的第 4 章中的 “监视属性”。
- 条目表 - 包含目录中的条目计数和条目缓存命中率。这些变量的值还与目录的 `cn=snmp,cn=monitor` 条目的属性中的操作变量相混合。请参阅 *Sun ONE Directory Server 参考手册* 的第 4 章中的 “监视属性”。
- 交互表 - 包含有关与此目录服务器通讯的最后 5 个目录服务器的统计信息。*Sun ONE Directory Server 部署指南* 的第 8 章中的 “SNMP 监视”对该表的对象进行了说明。
- 实体表 - 包含描述 Directory Server 的这一实例的变量 （例如，其服务器 ID 和版本）。*Sun ONE Directory Server 部署指南* 的第 8 章中的“SNMP 监视”对该表的对象进行了说明。

必须先编译目录以及将在以下目录中找到的 MIB，然后才可以使用该目录的 MIB：

ServerRoot`/plugins/snmp/mibs`

有关如何编译 MIB 的信息，请参阅 SNMP 产品文档。

设置 SNMP

设置用于监视目录的 SNMP 的步骤取决于您的主机平台是 UNIX、 AIX 还是 Windows：

1. 按照以下小节中的说明，在平台上设置 SNMP：
   - “在 UNIX 平台上”（第 363 页）
   - “在 AIX 平台上”（第 364 页）
   - “在 Windows 平台上”（第 364 页）
2. 按照 “在 Directory Server 中配置 SNMP”（第 365 页）的说明执行操作
3. 按照 “启动和停止 SNMP 副代理”（第 365 页）中的说明重新启动 SNMP。

在 UNIX 平台上

要在 UNIX 计算机 （而非 AIX）上设置支持 Directory Server 的 SNMP，必须使用 Administration Server Console 配置和启动主代理。

如果正在使用默认端口设置 （对 SNMP 为 161），则必须以 root 用户身份运行 Administration Server 和 Directory Server。如果将主代理重新配置为使用值高于 1000 的端口，则无需是 root 用户。

默认情况下，主代理使用端口 161，在大多数平台上，它与 SNMP 本机代理的默认端口冲突。在启动主代理之前必须禁用 SNMP 本机代理，或必须将主代理配置为使用另一个端口。要禁用 SNMP 本机代理，请参阅平台文档。要配置和启动主代理，请按照 *Sun ONE Server Console 服务器管理指南* 的第 11 章中的 “在 UNIX 系统上配置主代理”中的说明执行操作。

在 AIX 平台上

在 AIX 平台上，不需要设置主代理。但是，当 SNMP 守候进程在 AIX 上运行时，它支持替换主代理的 SMUX。不过，需要更改 AIX SNMP 守候进程的配置。

如果正在使用默认的端口设置（对 SMUX 为 199），则必须以 root 用户的身份运行 Administration Server 和 Directory Server。如果将主代理重新配置为使用值高于 1000 的端口，则无需是 root 用户。

AIX 使用多个配置文件过滤自身的通讯。需要对其中的一个配置文件 `snmpd.conf` 进行更改，以便 SNMP 守候进程能够接受来自 SMUX 副代理的传入消息。详细信息，请参阅 `snmpd.conf` 的联机手册页。要定义每个副代理，需要添加一行。

例如，可以将如下行添加到 `snmpd.conf`：

```
smux 1.3.6.1.4.1.1.1450.7 "" IP_address net_mask
```

其中 *IP_address* 是副代理在其上运行的主机的 IP 地址， *net_mask* 是主机的网络掩码。

注意 不要使用环回地址 127.0.0.1。始终都要使用真实的主机 IP 地址。

如果需要详细信息，请参阅 AIX 平台文档。

在 Windows 平台上

值得一提的重点是：Windows 上的主代理是 SNMP 服务，而 *不是* SNMP 代理（SNMP 代理在其他平台上的情形）。使用存储在 Windows 注册表中的信息，SNMP 服务调用 DLL 以访问目录服务器中的监视信息。

要在 Windows 计算机上设置支持 Directory Server 的 SNMP，必须先通过 Windows 控制面板安装和配置 SNMP 服务。有关说明，请参阅 Windows 操作系统文档。

在 Directory Server 中配置 SNMP

在平台上设置了 SNMP 代理或服务后，必须在 Directory Server 实例中配置 SNMP 参数。要从 Directory Server 控制台配置 SNMP 设置，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，选择配置树根部的服务器节点，然后在右侧窗格中选择 SNMP 标签。
2. 选中 “启用统计数据集合”复选框。默认情况下，为了提高资源利用率，并不收集 SNMP 变量的统计信息。如果不使用 SNMP 且不通过 LDAP 监视 `cn=snmp,cn=monitor` 条目的属性，则应取消选中此复选框。
3. 对于 UNIX 服务器，必须在相应的文本字段中输入主代理的主机名和端口号。

   默认值分别为 `localhost` 和端口 `199`。
4. 在 “说明性属性”框的文本字段中输入信息。这些值将反映在此服务器所公开的 SNMP 实体表中：
   - 说明 - 输入目录服务器的说明，类似于 Sun ONE Server Console 拓扑树中此实例的说明字段。
   - 组织 - 输入目录服务器所属的公司或内部组织的名称。
   - 位置 - 输入目录服务器主机的地理位置。
   - 联系 - 输入目录服务器管理员的电子邮件地址或联系信息。
5. 单击 “保存”以存储更改。
6. 按照以下小节中的说明，在 UNIX 平台上启动或重新启动 SNMP 副代理或在 Windows 平台上启动或重新启动 SNMP 服务。

启动和停止 SNMP 副代理

以下过程说明了如何在 UNIX 平台 （包括 AIX）上启动、重新启动或停止 SNMP 副代理，以及如何在 Windows 平台上启动、重新启动或停止 SNMP 服务。

注意 如果在同一主机上添加另一个服务器实例，而且希望该实例成为 SNMP 网络的一部分，则必须重新启动 SNMP 副代理 （UNIX 和 AIX）或 SNMP 服务 (Windows)。

在 UNIX 和 AIX 平台上

要启动、停止和重新启动运行在 UNIX 上的目录的 SNMP 副代理，请执行以下操作：

1. 在 Directory Server 控制台的顶级 “配置”标签上，选择配置树根部的服务器节点，然后在右侧窗格中选择 SNMP 标签。
2. 使用 “说明性属性”框下面的副代理控制按钮启动、停止或重新启动副代理。

   停止目录并不会停止目录的副代理。如果要停止副代理，必须从该标签执行此操作。

在 Windows 平台上

要启动、停止和重新启动运行在 Windows 上的目录的 SNMP 服务，请执行以下操作：

1. 打开 Windows “控制面板”并选择 “服务”。
2. 从 “服务”列表中选择 SNMP。
3. 单击 “启动”启动 SNMP 服务，单击 “停止”停止 SNMP 服务，或单击 “停止，然后启动”重新启动 SNMP 服务。

   停止目录并不会停止 Windows SNMP 服务，必须显式从 “控制面板”执行此操作。

第 14 章

使用传递验证插件

传递验证 (PTA) 是一种机制，Directory Server 通过它查询另一个 Directory Server 以验证绑定请求。 PTA 插件提供了这样的功能：允许 Directory Server 接受未存储在本地后缀中的条目的简单绑定操作 （基于口令）。

Sun ONE Directory Server 5.2 使用 PTA 以便在单独的 Directory Server 实例上管理您的用户目录和配置目录。

注意 如果您的用户目录与配置目录使用的是同一个服务器，则 Directory Server 控制台中将不会列出 PTA 插件，但是可以创建该插件以使用传递验证。

本章在以下几节中介绍了 PTA 插件：

- Directory Server 如何使用 PTA
- 配置 PTA 插件

Directory Server 如何使用 PTA

如果将配置目录和用户目录分别安装在不同的 Directory Server 实例上，则安装程序会自动设置 PTA 以允许 “配置管理员”用户 （通常是 `admin`）来执行管理任务。

由于 `admin` 用户条目存储在配置目录中 `o=NetscapeRoot` 的下面，这时需要 PTA。因此，作为 `admin` 绑定至用户目录的尝试通常都会失败。 PTA 允许用户目录将凭证传送至对它们进行验证的配置目录。这样用户目录就允许 `admin` 用户进行绑定了。

在此示例中，用户目录被用作 PTA 服务器，即将绑定请求传递至另一个 Directory Server 的服务器。配置目录被用作验证服务器，即包含该条目并对请求客户机的绑定凭证进行验证的服务器。

本章中还将使用 *PTA* 子树这个术语。传递子树是指*没有*出现在 PTA 服务器中的子树。如果用户的绑定 DN 包含此子树，系统就会将用户的凭证传递至验证目录。

该步骤顺序显示了传递验证的工作方式：

1. 在主机 `configdir.example.com` 上安装包含传递子树 `o=NetscapeRoot` 的配置目录服务器 （验证目录）。
2. 在主机 `userdir.example.com` 上安装包含 `dc=example,dc=com` 后缀中的数据的用户目录服务器 （PTA 目录）。
3. 在安装用户目录的过程中，系统会提示您提供指向配置目录服务器的 LDAP URL，例如：

   ```
   ldap://configdir.example.com/o=NetscapeRoot
   ```

4. 安装程序使用您提供的 LDAP URL 在用户目录中配置并启用 PTA 插件。

   用户目录现在被配置为 PTA 目录。它将把其 DN 包含 `o=NetscapeRoot` 的条目的所有绑定请求发送到配置目录 `configdir.example.com`。

5. 安装完成后， `admin` 用户会尝试绑定到用户目录以开始创建用户数据。

   `admin` 条目以 `uid=admin, ou=Administrators,ou=TopologyManagement,o=NetscapeRoot` 的形式存储在配置目录中。因此，用户目录将按照 PTA 插件配置中的定义，将绑定请求传递至配置目录。

6. 配置目录验证绑定凭证 （包括口令），并将确认发送回用户目录。
7. 用户目录即允许 `admin` 用户进行绑定。

配置 PTA 插件

PTA 插件配置信息会在 PTA 服务器上的 `cn=Pass Through Authentication,cn=plugins,cn=config` 条目中指定。

如果在不同的服务器实例上安装用户目录和配置目录，则系统会自动将 PTA 插件条目添加至用户目录的配置中。如果将两个目录都安装在同一实例上，且希望对其他目录执行传递验证，则必须首先创建插件配置条目。

创建插件配置条目

1. 运行以下命令，创建插件配置条目：

```
ldapmodify -a -h PTAhost -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=Pass Through Authentication,cn=plugins,cn=config
objectClass:top
objectClass:nsSlapdPlugin
objectClass:extensibleObject
cn:Pass Through Authentication
nsslapd-pluginPath:ServerRoot/lib/passthru-plugin.extension
nsslapd-pluginInitfunc:passthruauth_init
nsslapd-pluginType:preoperation
nsslapd-plugin-depends-on-type:database
nsslapd-pluginId:passthruauth
nsslapd-pluginVersion: 5.2
nsslapd-pluginVendor:Sun Microsystems, Inc.
nsslapd-pluginDescription:pass through authentication plugin
nsslapd-pluginEnabled:on or off
nsslapd-pluginarg0:ldap[s]://authenticatingHost[:port]/PTAsubtree options
```

   其中 *ServerRoot* 要视安装的具体情况而定，而 *extension* 在 HP-UX 上为 `.sl`，在所有其他 UNIX 平台上为 `.so`，在 Windows 上为 `.dll`。

   插件参数指定标识验证目录服务器的主机名、可选的端口以及 PTA 子树的 LDAP URL。如果未指定端口，则 LDAP 的默认端口为 389， LDAPS 的默认端口为 636。也可以设置以下几节中所述的可选连接参数。如果 *PTAhost* 中存在 *PTAsubtree*，则插件不会将绑定请求传递到 *authenticatingHost*，且绑定将在本地处理，而不会进行任何传递。

2. 如 “启动和停止 Directory Server”（第 20 页）中所述，重新启动服务器。

配置 PTA 以使用安全连接

因为 PTA 插件必须将包括口令的绑定凭证发送到验证目录，所以建议使用安全连接。要配置 PTA 目录以使其通过 SSL 与验证目录进行通讯，请执行以下操作：

- 在 PTA 和验证目录中配置并启用 SSL，如第 11 章 “实现安全性”中所述。
- 创建或修改 PTA 插件配置以使用 LDAPS 和 LDAP URL 中的安全端口，例如：

  ```
  ldaps://configdir.example.com:636/o=NetscapeRoot
  ```

设置可选的连接参数

PTA 插件参数可以接受 LDAP URL 后的一组可选的连接参数：

```
ldap[s]://主机[:端口]/子树 [maxconns,maxops,timeout,ldapver,connlife]
```

参数必须以显示的顺序给出。虽然这些参数是可选的，但是如果指定了其中之一，就必须指定所有这些参数。如果不希望定制所有参数，则请指定下面给出的默认值。请确保 *subtree* 参数与可选参数之间以一个空格分隔。

可以为每个 LDAP URL 配置以下可选的参数：

- *maxconns* - PTA 服务器可以同时打开的到验证服务器的最大连接数。该参数限制可以同时传递到验证服务器的绑定数量。默认值为 3。
- *maxops* - 在单个连接中， PTA 目录服务器可以同时对验证目录服务器发送的最大绑定请求数。该参数进一步限制了同时传递的验证的数量。默认值为 5。
- *timeout* - 希望 PTA 服务器等待验证服务器响应的最大延时 （以秒为单位）。默认值为 300 秒 （5 分钟）。
- *ldapver* - 当连接到验证服务器时，希望 PTA 服务器使用的 LDAP 协议的版本。允许的值为 2 (LDAPv2) 和 3 (LDAPv3)。默认值为 3。
- *connlife* - PTA 服务器将重新使用到验证服务器的连接的时间限制 （以秒为单位）。如果已超出该时间后客户机请求 PTA 子树中的绑定，则服务器将关闭该 PTA 连接并打开一个新连接。只有当绑定请求被初始化并且服务器确定已超出时间限制时，服务器才会关闭连接。如果不指定此选项，或者如果 LDAP URL 中仅列出一个验证服务器，则不会强制执行任何时间限制。如果列出了两个或多个主机，默认值为 300 秒 （5 分钟）。

下面的示例中， PTA 插件参数将连接的数量增加到 10，而将超时减少到 1 分钟（60 秒）。为所有其他参数给定默认值：

```
ldaps://configdir.example.com:636/o=NetscapeRoot 10,5,60,3,300
```

指定多个服务器和子树

可以使用多个参数配置 PTA 插件以指定多个验证服务器、多个 PTA 子树，或同时指定两者。每个参数包含一个 LDAP URL，且可以拥有其自身的连接选项集。

当有多个验证服务器用于同一 PTA 子树时，它们会充当故障切换服务器。无论何时 PTA 连接达到超时限制时，插件都将按照列出的顺序建立到这些验证服务器的连接。如果所有连接超时，验证将失败。

如果定义了多个 PTA 子树，插件将根据绑定 DN 将验证请求传递到相应的服务器。以下示例显示了四个 PTA 插件参数，它们定义了两个 PTA 子树，每个子树具有一个用于验证的故障切换服务器和服务器特定的连接参数：

```
nsslapd-pluginarg0:ldaps://configdir.example.com/o=NetscapeRoot
 10,10,60,3,300
nsslapd-pluginarg1:ldaps://configbak.example.com/o=NetscapeRoot
 3,5,300,3,300
nsslapd-pluginarg2:ldaps://east.example.com/ou=East,ou=People,
 dc=example,dc=com 10,10,300,3,300
nsslapd-pluginarg3:ldaps://eastbak.example.com/ou=East,ou=People,
 dc=example,dc=com 3,5,300,3,300
```

修改 PTA 插件配置

可以随时重新配置 PTA 插件，将其启用或禁用，或者更改验证主机或 PTA 子树。

1. 编辑 PTA 插件配置条目 (`cn=Pass Through Authentication,cn=plugins,cn=config`) 以修改 `nsslapd-pluginenabled` 和 `nsslapd-pluginarg`*N* 属性。可以使用控制台或 `ldapmodify` 公用程序编辑配置。

   例如，以下命令将启用具有 SSL 及以上所示连接参数的 PTA 插件。

   ```
   dn:cn=Pass Through Authentication,cn=plugins,cn=config
   changetype:modify
   replace:nsslapd-pluginenabled
   nsslapd-pluginenabled:on
   -
   replace:nsslapd-pluginarg0
   nsslapd-pluginarg0:ldaps://configdir.example.com:636/
    o=NetscapeRoot 10,10,60,3,300
   -
   replace:nsslapd-pluginarg1
   nsslapd-pluginarg1:ldaps://configbak.example.com:636/
    o=NetscapeRoot 3,5,300,3,300
   ^D
   ```

2. 如 “启动和停止 Directory Server”（第 20 页）中所述，重新启动服务器。

第 15 章

使用 UID 唯一性插件

UID 唯一性插件确保给定属性的值在目录或子树的所有条目中都具有唯一性。该插件将停止任何试图添加包含给定属性现有值的条目的操作，或者将属性添加或修改为目录中已有值的任何操作。

默认情况下，该插件确保 `uid` 属性的唯一性，但是在默认情况下不启用该插件。可以创建该插件的新实例，以强制其他属性具有唯一值。 UID 唯一性插件限于保证单个服务器上的属性值具有唯一性。

本章包含以下小节：

- 概述
- 实施 uid 属性的唯一性
- 实施其他属性的唯一性
- 同时使用唯一性插件和复制

概述

UID 唯一性插件是预运行插件。它将在服务器执行目录更新前检查所有 LDAP 操作。该插件确定操作是否将导致两个条目具有相同的属性值，在这种情况下，服务器终止操作并向客户机返回错误 19， `LDAP_CONSTRAINT_VIOLATION`。

可以对该插件进行配置，以便强制要求在目录中的一个或多个子树中具有唯一性，或在特定对象类的条目间具有唯一性。该配置确定将实施唯一属性值的条目集。只有在操作的对象是该集中的条目且属性值在该集的所有条目中不具有唯一性时，操作才能终止。

如果希望强制其他属性具有唯一性，则可定义 UID 唯一性插件的多个实例。为希望其值具有唯一性的每个属性和条目集定义一个插件实例。还可以具有同一属性的多个插件实例，以强制在多个条目集中具有 “单独” 的唯一性。仅允许给定的属性值在每个条目集中出现一次。

在现有目录上启用属性唯一性时，服务器不检查现有条目间的唯一性。只有当添加条目或者添加或修改属性时，才会强制实施唯一性。

默认情况下，将禁用 UID 唯一性插件，因为它影响多主复制操作。使用复制时，可以启用 UID 唯一性插件，但是您应当知道 “同时使用唯一性插件和复制”（第 378 页）中说明的行为。

实施 uid 属性的唯一性

本节介绍如何启用和配置目录中 `uid` 属性的默认唯一性插件。要实施其他属性的唯一性，请参阅 “实施其他属性的唯一性”（第 376 页）。

使用控制台配置插件

使用控制台时，一定不要修改默认的 `uid` 唯一性插件以实施其他属性的唯一性。如果不希望有 `uid` 唯一性插件，请禁用它并创建其他属性的新插件实例，如 “实施其他属性的唯一性”（第 376 页）中所述。

1. 在 Directory Server 控制台的顶级 “配置” 标签上，展开 “插件” 节点，并选择 `uid uniqueness` plugin。
2. 在右侧面板中，选中复选框以启用该插件。

   不要修改初始化函数字段或插件模块路径。
3. 根据对实施唯一性子树的指定方式，修改插件参数：

- 要指定单个子树的基准 DN，请编辑参数 2 的值。要指定多个子树，请单击 “添加” 以添加更多参数，并在每个新的文本字段中输入子树的基准 DN。

- 要通过其基本条目的对象类指定子树，请将参数设置为以下值：

  参数 1：attribute=uid
  参数 2：markerObjectClass=*baseObjectClass*

  该插件将在带有给定 *baseObjectClass* 的每个目录条目下的子树中实施 uid 唯一性。例如，如果在诸如 ou=Employees 和 ou=Contractors 的许多分支中都具有用户条目，则指定 markerObjectClass=organizationalUnit。

  因为标记对象类下的分支范围可能非常广，所以可根据条目的对象类，进一步将属性唯一性的实施限制到某些条目。单击 “添加”，添加第三方插件参数，并将其设置为以下值：

  参数 3：requiredObjectClass=*entryObjectClass*

  在带有 *baseObjectClass* 的条目的子树内部，该插件将仅在带有 *entryObjectClass* 的目标条目的操作中实施唯一性。例如，如果拥有传统用户条目，则指定 requiredObjectClass=inetorgperson。

4. 完成对 uid 唯一性插件的编辑后，单击 “保存”。将会提醒您必须重新启动服务器，更改才能生效。
5. 重新启动服务器，开始实施 uid 属性的唯一值。

从命令行配置插件

以下过程说明如何使用 ldapmodify 命令启用和配置 uid 唯一性插件。该插件配置条目的 DN 是 cn=uid uniqueness,cn=plugins,cn=config。

1. 通过将 nsslapd-pluginEnabled 属性设置分别为 on 或 off，启用或禁用该插件：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=uid uniqueness,cn=plugins,cn=config
changetype:modify
replace:nsslapd-pluginEnabled
nsslapd-pluginEnabled:on 或 off
^D
```

2. 根据对实施唯一性子树的指定方式，修改插件参数：

- 要指定单个子树的基准 DN，请修改 nsslapd-pluginarg1 的值：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=uid uniqueness,cn=plugins,cn=config
changetype:modify
replace:nsslapd-pluginArg1
nsslapd-pluginArg1:subtreeBaseDN
^D
```

要指定多个子树，请添加更多参数，每个参数的值为子树的完整基准 DN：

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=uid uniqueness,cn=plugins,cn=config
changetype:modify
add:nsslapd-pluginArg2
nsslapd-pluginArg2:subtreeBaseDN
-
add:nsslapd-pluginArg3
nsslapd-pluginArg3:subtreeBaseDN
-
...
^D
```

- 要根据其基本条目的对象类指定子树，请将参数设置为以下值。将在每个带有 *baseObjectClass* 的条目下的子树中实施 `uid` 属性唯一性。可选择性地指定第三个参数中的 *entryObjectClass*，以便该插件仅在目标条目带有此对象类的操作中实施唯一性。

```
ldapmodify -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
dn:cn=uid uniqueness,cn=plugins,cn=config
changetype:modify
replace:nsslapd-pluginArg0
nsslapd-pluginArg0:attribute=uid
-
replace:nsslapd-pluginArg1
nsslapd-pluginArg1:markerObjectClass=baseObjectClass
-
replace:nsslapd-pluginArg2
nsslapd-pluginArg2:requiredObjectClass=entryObjectClass
^D
```

3. 重新启动服务器，以使更改生效。

实施其他属性的唯一性

UID 唯一性插件可用于实施任何属性的唯一性。必须在目录中 `cn=plugins,cn=config` 下创建新条目，从而创建该插件的新实例。

1. 使用 ldapmodify 命令添加新插件实例的配置条目。该命令的第一部分显示如下。该命令的其余部分显示在以下步骤中。

   ```
   ldapmodify -a -h 主机 -p 端口 -D "cn=Directory Manager" -w 口令
   dn:cn=plug-in_name,cn=plugins,cn=config
   objectClass:top
   objectClass:nsSlapdPlugin
   objectClass:extensibleObject
   cn:plug-in_name
   nsslapd-pluginDescription:Enforce unique attribute values
   nsslapd-pluginType:preoperation
   nsslapd-plugin-depends-on-type:database
   nsslapd-pluginPath:ServerRoot/lib/uid-plugin.extension
   nsslapd-pluginVersion: 5.2
   nsslapd-pluginVendor:Sun Microsystems, Inc.
   nsslapd-pluginId:NSUniqueAttr
   nsslapd-pluginInitfunc:NSUniqueAttr_Init
   nsslapd-pluginEnabled:state
   ...
   ```

   在该命令的第一部分中， *plug-in_name* 应当是包含属性名的简短描述性名称（例如， cn=mail uniqueness）。 *ServerRoot* 和库 *extension* 取决于平台。最后，在服务器重新启动时，指定新实例的状态为 on 或 off。

2. 如果在服务器中验证插件签名，则新的唯一性插件配置中必须包括该签名。因为您的唯一性插件是 UID 唯一性插件的新实例，所以必须使用相同的签名信息，该签名信息位于以下文件中：

   ServerRoot/plugins/signatures/plugin.signatures

   只有安装服务器时使用的用户身份才可以读取该文件 （例如， root）。在该文件中，在 dn: cn=uid uniqueness,cn=plugins,cn=config 条目下查找信息。使用该文件中给定的相同值将以下属性添加到新的插件实例中。另外，还必须包括 ds-signedPlugin 对象类：

   ```
   objectClass:ds-signedPlugin
   ds-pluginDigest::02Q7yVLYsC8FInPrvbAKYq7Rj0o=
   ds-pluginSignature::MIIBjwYJKoZIhvcNAQcCoIIBgDCCAXwCAQExCzAJBg
    UrDgMCGgUAMAsGCSqGSIb3DQEHATGCAVswggFXAgEBMFYwTTELMAkGA1UEBhMC
    VVMxGTAXBgNVBAoTEFN1biBNaWNyb3N5c3RlbXMxIzAhBgNVBAMTGlBsdWdpbi
    BTaWduaW5nIENlcnRpZmljYXRlAgUA5X1ATjAJBgUrDgMCGgUAoF0wGAYJKoZI
    A2WjAjBgkqhkiG9w0BCQQxFgQU77mUWWJWttkH89eLwTr/fQtz+BswDQYJKoZI
   ```

```
 hvcNAQEBBQAEgYAzZwvgwo+OdKNkXWxlP+pUNpHesL6UQcvXcm37mEQyikRvLs
 hy3X0JutFhEXaCfU4UX76A3Zzedr2Iy0YEGkiPCu3g8jnkFEG/ux0ZMeOPiulF
 f9PUfqpnz6phq19eBZxZ/MBFLxtlzJHG42Ext/un4ZzQIg==
...
```

有关插件签名的详细信息，请参阅 “验证插件签名”（第 36 页）。如果不验证插件签名，则无需这些属性。配置将显示未对新的插件实例进行签名，但插件仍会正常运作。

3. 命令的其余部分指定插件参数，这些参数取决于被实施唯一性的子树的确定方式。

- 要根据其基准 DN 定义一个或多个子树，第一个参数必须是拥有唯一值的属性名称，随后的参数是子树基本条目的完整 DN。

```
nsslapd-pluginarg0:attribute_name
nsslapd-pluginarg1:subtreeBaseDN
nsslapd-pluginarg2:subtreeBaseDN
...
^D
```

- 要根据其基本条目的对象类定义子树，第一个参数必须包含 `attribute=`*attribute_name* 以指定应具有唯一值的属性的名称。第二个参数必须是 *baseObjectClass*，它确定被实施唯一性的子树的基本条目。可选择性地指定第三个参数中的 *entryObjectClass*，以便该插件仅在目标条目带有该对象类的操作中实施唯一性。

```
nsslapd-pluginarg0:attribute=attribute_name
nsslapd-pluginarg1:markerObjectClass=baseObjectClass
nsslapd-pluginarg2:requiredObjectClass=entryObjectClass
^D
```

在所有插件参数中， `=` 号前后一定没有空白区域。

4. 重新启动服务器，将新的唯一性插件实例载入服务器中。

同时使用唯一性插件和复制

将更新作为复制操作的一部分来执行时， UID 唯一性插件不对属性值执行任何检查。这不影响单主复制，但该插件不能自动对多主复制实施属性唯一性。

单主复制方案

因为客户机应用程序所做的所有修改都在主副本上执行，所以应在主服务器上启用 UID 唯一性插件。应将该插件配置为在复制的后缀中实施唯一性。因为主副本可确保期望的属性值具有唯一性，所以不必在使用者服务器上启用该插件。

在单主机的使用者上启用 UID 唯一性插件将不会妨碍复制或正常的服务器操作，但可能会导致性能轻微下降。

多主复制方案

UID 唯一性插件并非设计为用于多主复制方案中。因为多主复制使用不严格的一致性复制模型，所以即使在两个服务器上启用了该插件，也无法检测出在两个服务器上同时添加的同一属性值。

但是，可以在下列条件下使用 UID 唯一性插件：

- 接受唯一性检查的属性是名称属性。
- 在所有主副本上为相同子树中的相同属性启用唯一性插件。

满足这些条件时，唯一性冲突会在复制时报告为命名冲突。命名冲突需要手动解决。有关解决复制冲突的信息，请参阅 “解决常见复制冲突”（第 284 页）。

第三方许可证确认信息

本产品包括以下版权声明所涵盖的软件。这里所提到的所有商标和注册商标都归其各自拥有者所有。

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY HARVARD AND ITS CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HARVARD OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name “Carnegie Mellon University” must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact Office of Technology Transfer Carnegie Mellon University 5000 Forbes Avenue Pittsburgh, PA 15213-3890 (412) 268-4387, fax: (412) 268-7395 tech-transfer@andrew.cmu.edu
4. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).”
CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Kungliga Tekniska Högskolan and its contributors.

4. Neither the name of the Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 1987, 1988 Student Information Processing Board of the Massachusetts Institute of Technology. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of M.I.T. and the M.I.T. S.I.P.B. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. and the M.I.T. S.I.P.B. make no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.

Copyright (c) 1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided “as is” without express or implied warranty.

Copyright 1992 Network Computing Devices, Inc. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Network Computing Devices may not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Network Computing Devices makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.
NETWORK COMPUTING DEVICES DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL NETWORK COMPUTING DEVICES BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 2001-2002 The Apache Software Foundation. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: “This product includes software developed by the Apache Software Foundation (http://www.apache.org/).” Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4.The names “Xerces” and “Apache Software Foundation” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called “Apache”, nor may “Apache” appear in their name, without prior written permission of the Apache Software Foundation.
THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT

LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

COPYRIGHT Copyright (c) 1997-2000 Messaging Direct Ltd. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY MESSAGING DIRECT LTD. “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL MESSAGING DIRECT LTD. OR ITS EMPLOYEES OR AGENTS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. END COPYRIGHT

COPYRIGHT Copyright (c) 2000 Fabian Knittel. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. END COPYRIGHT

The source code to the Standard Version of Perl can be obtained from CPAN sites, including http://www.perl.com/.

This product incorporates compression code by the Info-ZIP group. There are no extra charges or costs due to the use of this code, and the original compression sources are freely available from ftp://ftp.cdrom.com/pub/infozip/ on the Internet.

索引

A

B

C

D

F

G

H

J

K

L

M

N

P

Q

R

S

T

W

X

Y

Z