Sun Java™ System

Directory Proxy Server 5
管理指南

2004Q2

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

文件号码：817-7016

目录

图

表

过程

前言

《*Directory Proxy Server 管理指南*》包含管理 Sun Java System Directory Proxy Server 所需的信息。

该前言中包含以下几部分：

在执行本指南中描述的任何任务之前，请先阅读 《*Directory Proxy Server 发行说明*》。

本指南的适用读者

本指南是专门为将配置和操作一台或多台服务器的系统管理员编写的。

本指南的作者假设您熟悉以下知识：

- Sun Java System Directory Proxy Server 5 及其管理
- LDAP 及相关协议的规范
- 互联网和万维网技术

本指南的组织结构

本指南分为以下几个部分：

使用文档

Directory Proxy Server 手册可用作 Portable Document Format （PDF，便携式文档格式）和 Hypertext Markup Language （HTML，超文本标记语言）格式的联机文件。残障人士可采用辅助技术读取这两种格式的文档。可从以下位置访问 Sun™ 文档 Web 站点：

http://docs.sun.com

可从以下位置访问 Directory Proxy Server 文档集：

http://docs.sun.com/db/coll/DirectoryProxyServer_04q2 和
http://docs.sun.com/db/coll/DirectoryProxyServer_04q2_zh

表 1 简单描述文档集中的各个文档。左列提供各文档的名称和 Web 站点。右列描述文档的一般内容。

表 1 Directory Proxy Server 文档

文档	内容
Directory Proxy Server 发行说明 http://docs.sun.com/doc/817-7023	包含有关 Directory Proxy Server 的最新信息，包括已知问题。
Directory Proxy Server 管理指南 http://docs.sun.com/doc/817-7016	介绍管理目录内容和配置 Directory Proxy Server 的各种功能的过程。
Java Enterprise System 2004Q2 发行说明 http://docs.sun.com/doc/817-7049	包含有关更新、升级和数据迁移过程的最新信息，以便迁移至 Directory Proxy Server 的最新版本。
Java Enterprise System 2004Q2 安装指南 http://docs.sun.com/doc/817-7056	涵盖更新、升级和数据迁移过程，以便迁移至 Directory Proxy Server 的最新版本。

约定

表 2 描述本指南中使用的字样约定。

表 2 字样约定

字样	含义	示例
AaBbCc123 （等宽）	API 和语言元素、HTML 标记、Web 站点 URL、命令名称、文件名、目录路径名称、计算机屏幕输出、代码样例。	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `% You have mail.`
AaBbCc123 （等宽粗体）	键入的内容 （相对于计算机屏幕输出信息）。	`% su` `Password:`
AaBbCc123 （斜体）	书名。 新词或术语。 要强调的词。 要用实际的名称或值替换的命令行变量。	请阅读 《*开发者指南*》 中的第 6 章。 这些被称为*类*选项。 您*必须*是超级用户才能执行此操作。 该文件位于 *ServerRoot* 目录中。

表 3 描述本指南中使用的占位符约定。

表 3 占位符约定

项	含义	示例
install-dir	安装后软件二进制文件驻留于其下的目录前缀的占位符。	Solaris 系统上缺省的 *install-dir* 前缀是 `/`。 Red Hat 系统上缺省的 *install-dir* 前缀是 `/opt/sun`。
ServerRoot	服务器实例和数据所驻留的目录的占位符。 您可以通过客户端服务器控制台远程管理 *ServerRoot* 下的各个服务器。服务器控制台使用服务器端管理服务器来执行必须直接在服务器端系统上执行的任务。	缺省的 *ServerRoot* 目录为 `/var/opt/mps/serverroot`。
slapd-*serverID*	缺省情况下，驻留在 *ServerRoot* 下的特定服务器实例及其相关数据所在的目录的占位符。	缺省的 *serverID* 是主机名。

表 4 描述本书中使用的符号约定。

表 4 符号约定

符号	含义	表示法	示例
[ ]	包含可选的命令选项。	O[*n*]	-O4, -O
{ }	包含所需命令选项的一组选项。	d{y|n}	-dy
|	分离命令选项的选项。		
+	连接图形用户界面中使用的键盘快捷键中的同时按键。		Ctrl+A
-	连接图形用户界面中使用的键盘快捷键中的连续按键。		Esc-S
>	指示图形用户界面中的菜单选择。		“文件” > “新建” “文件” > “新建” > “模板”

表 5 描述本书中使用的 shell 提示符约定。

表 5 Shell 提示符

Shell	指示符
C shell	*machine-name*%
C shell 超级用户	*machine-name*#
Bourne shell 和 Korn shell	$
Bourne shell 和 Korn shell 超级用户	#

通常用 LDAP 数据交换格式 (LDIF) [RFC 2849] 表示 Directory Proxy Server 命令的输入和输出。为了方便读取，可以换行。

Web 上的资源和工具

以下位置包含有关 Java Enterprise System 及其组件产品 （如 Directory Proxy Server）的信息：

http://wwws.sun.com/software/learnabout/enterprisesystem/index.html

本文档中包含的第三方 URL 可提供附加的相关信息。

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

如何报告问题

如果您在使用 Directory Proxy Server 期间遇到问题，请通过以下方式与 Sun 客户支持部门联系：

- Sun 软件支持的在线服务，网址为：

  http://www.sun.com/service/sunone/software

  此站点上有一些链接，通过这些链接可以访问在线支持中心、 ProductTracker，还可了解维护方案以及用于联系支持部门的电话号码。

- SunSolve 支持 Web 站点的网址为：

  http://sunsolve.sun.com

  此站点提供有修补程序、支持文档、安全性信息和 Sun System 手册。

- 随维护合同一起分发的电话号码

因此在解决问题方面，我们可以提供最好的帮助，请您在与支持部门取得联系之前，提供以下信息：

- 描述问题，包括问题是在何种情况下发生的，以及问题对操作的影响
- 机型、操作系统的版本和产品版本，包括可能影响问题的任何修补程序和其他软件
- 采用某些方法使问题再现的详细步骤
- 任何错误日志或核心转储

Sun 欢迎您提出意见和建议

Sun 愿意对其文档进行改进，并欢迎您提出意见和建议。请使用基于 Web 的形式向 Sun 提供反馈：

http://www.sun.com/hwdocs/feedback/

请在相应的字段内提供完整的文档标题和文件号码。文件号码由 7 位或 9 位数字构成，您可以在书的标题页面或文档的顶部找到。例如，《管理指南》的文件号码为 817-7016。

当您提供意见和建议时，可能需要在表单中提供文档英文版本的标题和文件号码。本文档英文版本的文件号码和标题是：817-6255， Directory Proxy Server 5 Administration Guide。

第 I 部分

Directory Proxy Server 简介

第 1 章

Directory Proxy Server 概述

本章向您介绍 Directory Proxy Server。本章由以下几部分组成：

简介

Directory Proxy Server 是用于电子商务解决方案中任何关键任务的目录服务的基本组件。Directory Proxy Server 是 LDAP 应用层协议网关，它使用应用层负载平衡和故障转移来提供增强的目录访问控制、架构兼容性和高可用性。

就其功能来说， Directory Proxy Server 是位于 LDAP 客户机和 LDAP 目录服务器之间的 “LDAP 访问路由器”。可以基于在 Directory Proxy Server 配置中定义的规则，对来自 LDAP 客户机的请求进行过滤，并将其路由到 LDAP 目录服务器。同样基于在 Directory Proxy Server 配置中定义的规则，对目录服务器所产生的结果进行过滤并将其传递回客户机。此过程对于 LDAP 客户机是完全透明的，客户机连接到 Directory Proxy Server 就像连接到任何 LDAP 目录服务器一样。

Directory Proxy Server 是为 Extranet 和 Intranet 目录基础结构提供高可用性、安全性和客户机兼容性功能的独特产品，这些功能包括：

- 自动负载平衡
- 透明的服务器故障转移和故障回复
- 自动跟随引荐
- Extranet/Intranet 访问控制组
- 安全的客户机和服务器验证

- 动态查询和响应过滤
- 动态架构映射
- 基于目录或基于文件的配置
- 可配置的日志记录

Directory Proxy Server 与新建的以及现有的 LDAP 目录基础结构共存，并对它们进行补充，同时，与已经在企业 Extranet 和 Intranet 中部署的启用目录的应用程序进行无缝集成。当对它进行部署后，便可以利用客户的目录基础结构中的现有投资。Directory Proxy Server 可与任何遵守 LDAP 协议的目录服务器进行互操作。Directory Proxy Server 可与任何支持并遵守 LDAP 协议的目录一起工作，无论它是本机 LDAP 目录、支持 LDAP 的 X.500 目录，还是支持 LDAP 的关系数据库。

Directory Proxy Server 实现了 LDAPv3 Internet 规范，并且还支持旧的和功能较少的 LDAPv2 规范，以确保与已部署的启用目录的客户机应用程序 （使用 LDAPv2）互相兼容。Directory Proxy Server 是作为 UNIX 平台上单独的系统服务器进程来运行的。服务器是多线程的，并且可以处理数以千计的 LDAP 客户机请求，同时将访问控制规则和协议过滤规则应用到每个请求中。

Directory Proxy Server 可以帮助各个组织保护其专用目录信息，以免受到未经授权的访问；同时，让这些组织能够安全地发布其公共信息。 Directory Proxy Server 可用于在 LDAP 目录上精细配置访问控制策略，例如，控制哪些用户能够在目录信息树 (DIT) 的不同部分执行不同类型的操作。也可以配置 Directory Proxy Server 以禁止通常由 Web 拖网者和机器人为了收集信息而执行的某类操作。

与 Web 代理服务器不同， Directory Proxy Server 是以反向代理模式操作的。它不将那些来自防火墙内部的客户机连接转发给 Internet 上的任意服务器，也不缓存搜索结果。这样做的主要原因是由于数据应用访问控制的问题。当前只在维护了访问控制的 LDAP 目录服务器中完成。Directory Proxy Server 不了解目录服务器访问控制。

Directory Proxy Server 功能集

Directory Proxy Server 功能集提供了如下功能：高可用性、负载平衡、故障转移、类似于防火墙的安全性，以及客户机－服务器兼容性。

高可用性

Directory Proxy Server 旨在支持高可用性目录部署，具体方法是：在一组重复的 LDAP 目录服务器中提供自动负载平衡和自动故障转移及故障回复。对于 Extranet 和 Intranet 环境，常常需要确保启用目录且具有关键任务的客户机和应用程序能够全天候地访问目录数据。 Directory Proxy Server 对其了解的所有目录服务器的连接状态信息进行维护，并能够在一组已配置的目录服务器上，对 LDAP 操作动态、按比例地执行负载平衡。当一个或多个目录服务器不可用时，负载就会按比例地在剩余服务器之间进行重新分配。当目录服务器重新联机时，负载会按比例、动态地重新分配。

例如，假设目录服务器 A 被配置为接收 40% 的 LDAP 客户机负载，服务器 B 接收 20% 负载，服务器 C 接收 20% 负载，服务器 D 接收 20% 负载。如果目录服务器 B 发生故障，Directory Proxy Server 将意识到服务器 A 所配置承担的负载是服务器 C 和 D 的两倍，则会重新分配来自服务器 B 的 20% 负载，以使服务器 A 现在接收 50% 的负载，服务器 C 接收 25% 的负载，服务器 D 接收 25% 的负载。当目录服务器 B 恢复时， Directory Proxy Server 会自动检测到这种情况，并回复到原来涉及所有四台服务器而配置的负载百分比。

网络层 IP 负载平衡设备无法访问 LDAP 协议层。然而， Directory Proxy Server 将负载平衡与访问控制、查询过滤和查询路由集成，并可以进行智能的应用层访问控制和 LDAP 路由判定。

负载平衡

必须使用第 111 页上的 “定义和管理属性对象”中描述的负载平衡属性在 Directory Proxy Server 中配置负载平衡。可以与 Directory Proxy Server 进行通信的每一台后端目录服务器被配置为接收总客户机负载的某个百分比。然后 Directory Proxy Server 自动将客户机查询分配给不同的后端服务器，以满足配置中定义的负载条件。如果某台服务器不可用， Directory Proxy Server 会将该服务器的负载百分比按比例地在可用服务器之间分配 （根据它们的负载百分比）。如果所有的后端 LDAP 服务器都不可用， Directory Proxy Server 就会拒绝客户机查询。

Directory Proxy Server 中的负载平衡是基于会话的。这意味着，选择客户机的查询将定向到哪一台特定服务器的决策功能针对每个客户机会话只应用一次；尤其是在客户机会话开始的时候。该会话中的所有后续客户机查询都将被定向到会话开始时选择的服务器。

Directory Proxy Server 可以进行负载平衡的后端 LDAP 服务器的数量取决于多种因素，如运行 Directory Proxy Server 的主机大小、可用的网络带宽、 Directory Proxy Server 接收的查询混合、客户机会话的长度，以及 Directory Proxy Server 的配置。一般而言，如果大多数会话持续时间短暂，并且查询的计算量密集，则 Directory Proxy Server 可以支持较少的服务器。计算量密集的查询是那些需要检查整个消息的查询，例如使用第 112 页上的 “特性重命名属性”中描述的特性重命名功能时的查询。

Directory Proxy Server 使用监视进程在其后端服务器 （包括仅通过 SSL 进行通信的那些服务器）上进行运行状况检查。如果使用了负载平衡，则该功能将自动启用。 Directory Proxy Server 每隔 10 秒钟就会为它的每个后端目录服务器对 Root DSE 执行一次匿名搜索操作。如果其中之一变得不可用或没有响应，则 Directory Proxy Server 就会将其从活动的负载平衡服务器集中移除。当服务器再次可用时，则会再次将它引入到活动的负载平衡服务器集中。

故障转移

当服务器由于以下原因而变得不可用时， Directory Proxy Server 就会进行检测：连接尝试因拒绝连接错误而返回，或者连接尝试出现超时。由于这两种情况均发生在会话初期，并且尚未对该会话进行任何操作，因此 Directory Proxy Server 会将故障转移到另一台服务器 （只要这台服务器确实可用）。在连接尝试超时的情况下，客户机在获取响应时可以感觉到明显的延迟。如果 Directory Proxy Server 和后端服务器之间的连接突然丢失，那么 Directory Proxy Server 就会向受影响的客户机返回所有未完成操作的 LDAP_BUSY 错误。随后， Directory Proxy Server 将该客户机会话的故障转移到另一台目录服务器。

为了避免 Directory Proxy Server 成为目录部署的单一故障点，建议您至少使用两台 Directory Proxy Server，在其前面应用一个 IP。

安全性

Directory Proxy Server 提供了灵活的外部目录访问控制功能，这些功能增强了目录服务器提供的基本访问控制。访问控制机制允许不同的用户和用户群体与特定的访问组关联，这些访问组将应用管理员定义的安全限制和查询过滤。管理员可以基于 LDAP 验证信息、 IP 地址、域名及其他条件来控制对条目的访问。

Directory Proxy Server 提供的一个重要安全功能是保护 LDAP 客户机和 LDAP 目录服务器之间建立的连接。通过配置 Directory Proxy Server 来监视许多特定的标准，可以防止 LDAP 目录服务器遭到连接攻击：客户机同时进行的操作数、客户机可以在每个连接请求的操作数，以及特定客户机组的连接数。它还具有使非活动客户机超时的能力。

可以使用特定阈值限制来配置 Directory Proxy Server 不超出给定标准。 Directory Proxy Server 将监视这些标准并确保不超出阈值。 Directory Proxy Server 保留了多个标准 （例如从特定主机打开的连接数、在特定会话上执行的操作数等）来限制目录拖网和拒绝服务攻击的可能性。第 69 页上的 “创建系统配置实例”中详细描述了这些参数的配置。

Directory Proxy Server 还通过禁止某些类型的通用过滤 （如 (cn=A*) 或 (cn>A)）来限制拖网。第 79 页上的 “创建和管理组”中提供了有关如何配置过滤器的过滤的详细信息。

Directory Proxy Server 允许经过验证的客户机更改其对目录服务的访问控制。这允许经过验证的客户机即使在安全网络之外，也可以对目录信息具有更大的访问权限。

Directory Proxy Server 通过支持安全套接字层 (SSL) 传输协议来提供数据保护。例如，您可以配置 Directory Proxy Server，以使从受保护的网络外面访问目录服务的所有客户机必须建立 SSL 会话。第 159 页上的 “配置安全性”中提供了有关在 Directory Proxy Server 中配置 SSL 的详细信息。

这些功能可以帮助防止目前在业界极为普遍的 “拒绝服务”攻击和 “满载攻击”。如果 Directory Proxy Server 检测到已经达到阈值，它将开始拒绝与目录服务器的连接，防止目录服务器遭到攻击和控制。

客户机—服务器兼容性

Directory Proxy Server 基于 LDAP 识别名 (DN) 和组访问权限做出查询路由决策，包括基于验证凭据识别移动用户。 Directory Proxy Server 自动跟随可能由目录服务器返回的 LDAP 引荐，支持高度分布和可扩展的目录服务。对于必须在一组目录服务器中物理分布目录信息，但分布式目录对于用户来说好像是一个逻辑目录的大型目录部署来说，自动跟随引荐具有很大的优势。 Directory Proxy Server 通过提供逻辑上统一分布式目录数据以支持可扩展的分布式目录服务的功能，来支持这种类型的部署方案。

Directory Proxy Server 支持任何遵守 LDAPv2 或 LDAPv3 协议的客户机应用程序。为架构重新编写提供了支持，以便向客户机应用程序提供 “不是始终匹配目录服务器的架构”的固定架构。例如， Microsoft Outlook™ 电子邮件客户程序具有一个固定架构，该架构希望目录服务器实现 Microsoft 定义的特性，该特性可能不匹配某个企业的更一般的架构要求。架构重新编写功能允许目录系统管理员实现一个通用的企业架构，然后将该架构的特定元素动态地映射到功能较少的客户机应用程序所需的特性类型集。否则， Directory Proxy Server 不能识别架构，并接受大型标准集定义的任何特性类型和对象类以及*特定*行业架构定义，包括 RFC1274、 X.520、 X.521、 LIPS、 PKIX、 inetOrgPerson 和 DEN。

第 2 章

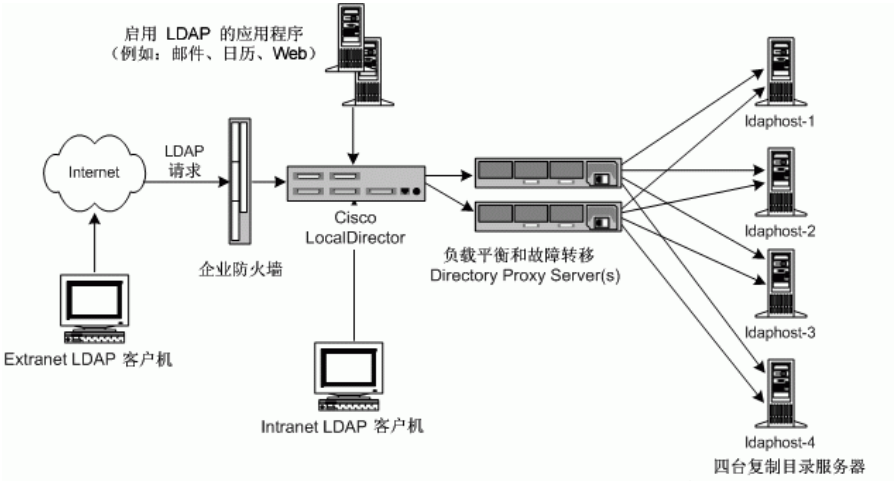
Directory Proxy Server 部署方案

根据具体的计算环境，部署 Directory Proxy Server 的方法可以有多种。本章介绍并说明一些典型的部署方法，包括：

内部高可用性配置

在图 2-1 所示的配置中，客户部署了只用于企业内部的 LDAP 基础结构。对外部网络能否访问到企业的任意 LDAP 服务不作要求。该客户部署的企业防火墙将拒绝防火墙外部对内部 LDAP 服务的所有访问。内部发出的所有客户机 LDAP 请求仍必须经由 Cisco Local Director （以获取高可用性）传送到 Directory Proxy Server，此处所示的 Cisco Local Director 仅作为 IP 数据包交换的一个示例，确保客户机至少能够访问到一个 Directory Proxy Server。客户将阻止所有设备对目录服务器的直接访问 （除运行 Directory Proxy Server 的主机之外）；具体实现方法是使用防火墙来保护运行目录服务器和 Directory Proxy Server 的主机。

图 2-1 内部高可用性配置



分布式 LDAP 目录基础结构

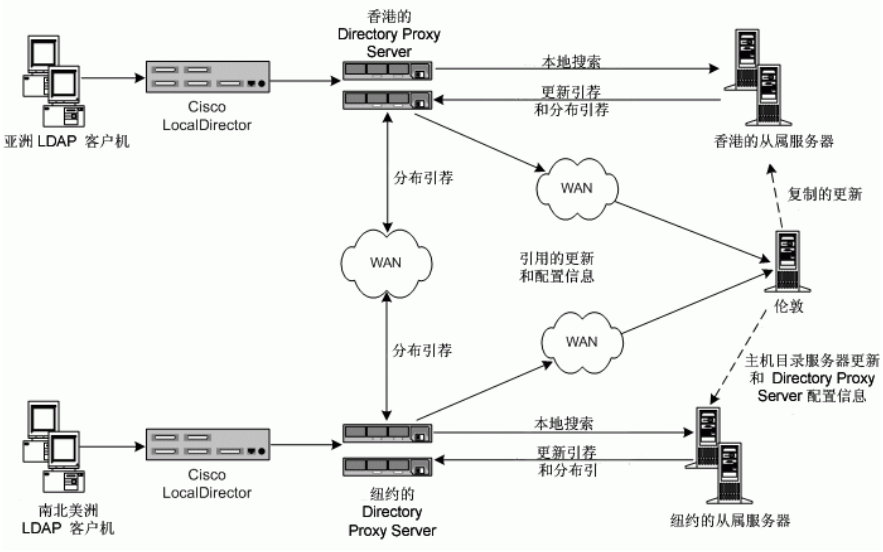
以下部分介绍了分布式 LDAP 目录基础结构中 Directory Proxy Server 的作用：

- 客户方案
- 客户部署
- LDAP 请求流

客户方案

在图 2-2 所示的配置中，一家大型金融机构的总部设在伦敦，其数据中心分别位于伦敦、纽约和香港。目前，雇员可以使用的大部分数据集中驻留在伦敦旧的 RDBMS 信息库中。该金融机构的客户机群对这些数据的所有访问均要通过广域网 (WAN)。由于使用此集中式模式，该金融机构遇到了伸缩性和性能方面的问题，因此决定转为使用分布式数据模式。该金融机构同时也决定部署 LDAP 目录基础结构。这里谈到的数据被认为是 “关键任务”，因此将其部署在具有高可用性的容错基础结构中。对客户机应用程序配置文件的分析显示：在各地区客户机群访问的数据中，有 95% 是该机群特定的数据，这是因为数据是基于客户的。虽然很少有位于亚洲地区的客户机访问北美客户的数据，但偶尔也会出现这种情况。客户机群还需要随时更新客户的信息。

图 2-2 分布式 LDAP 目录基础结构



客户部署

如果配置文件表明 95% 为本地数据访问，金融机构则决定按地域分布其 LDAP 目录基础结构。他在每个地理位置 （即香港、纽约和伦敦；图中未显示伦敦使用者服务器）部署了多个目录使用者服务器。每个使用者服务器被配置为保存当地的客户数据。欧洲和中东客户的数据保存在伦敦使用者服务器中，北美和南美客户的数据保存在纽约使用者服务器中，而亚太地区客户的数据则保存在香港使用者服务器中。利用这种部署，本地客户机群的大部分数据要求都位于该机群中。由于可以在本地处理客户机请求，所以这种模式与集中式模式相比，性能有了显著的提高，同时降低了网络开销；本地目录服务器可以有效地划分目录基础结构，从而增强了目录服务器的性能和伸缩性。每组使用者目录服务器都配置为：如果客户机提交更新请求或提交对位于别处的数据的搜索请求，则返回引荐。

LDAP 请求流

客户机的 LDAP 请求通过 Cisco LocalDirector 发送到 Directory Proxy Server。此处显示的 LocalDirector 产品仅作为 IP 数据包交换的一个示例，确保客户机始终能够至少访问一个 Directory Proxy Server。本地部署的 Directory Proxy Server 首先将所有请求路由到保存本地客户数据的本地目录服务器的阵列。 Directory Proxy Server 的实例配置为在目录服务器阵列中进行负载平衡，因此可提供自动故障转移

和故障回复。客户机对本地客户信息的搜索请求由本地目录满足，并且相应的响应将通过 Directory Proxy Server 返回到客户机。客户机对 “外部”地区客户信息的搜索请求最初由本地目录服务器来满足，方法是将引荐返回到 Directory Proxy Server。

此引荐包含的 LDAP URL 指向分布于各地区的 Directory Proxy Server 的相应实例。本地 Directory Proxy Server 代表本地客户机处理此引荐，并将搜索请求发送到 Directory Proxy Server 分布于各地区的相应实例。该分布式 Directory Proxy Server 将搜索请求转发给分布式目录服务器，并接收相应的响应。然后，此响应将通过 Directory Proxy Server 的分布于各地区的实例和本地实例返回到本地客户机。

本地 Directory Proxy Server 接收的更新请求最初也由本地目录服务器返回的引荐来满足。此外， Directory Proxy Server 代表本地客户机跟随此引荐，但这次将更新请求转发至位于伦敦的供应商目录服务器上。供应商目录服务器将此更新应用于供应商数据库，并通过本地 Directory Proxy Server 将响应发回本地客户机。随后，供应商目录服务器将更新下传到相应的使用者目录服务器。

所有的 Directory Proxy Server 被配置为在供应商目录服务器中启动和查找其配置。这样可以按地域分布 Directory Proxy Server 的多个实例，但将集中管理其配置。

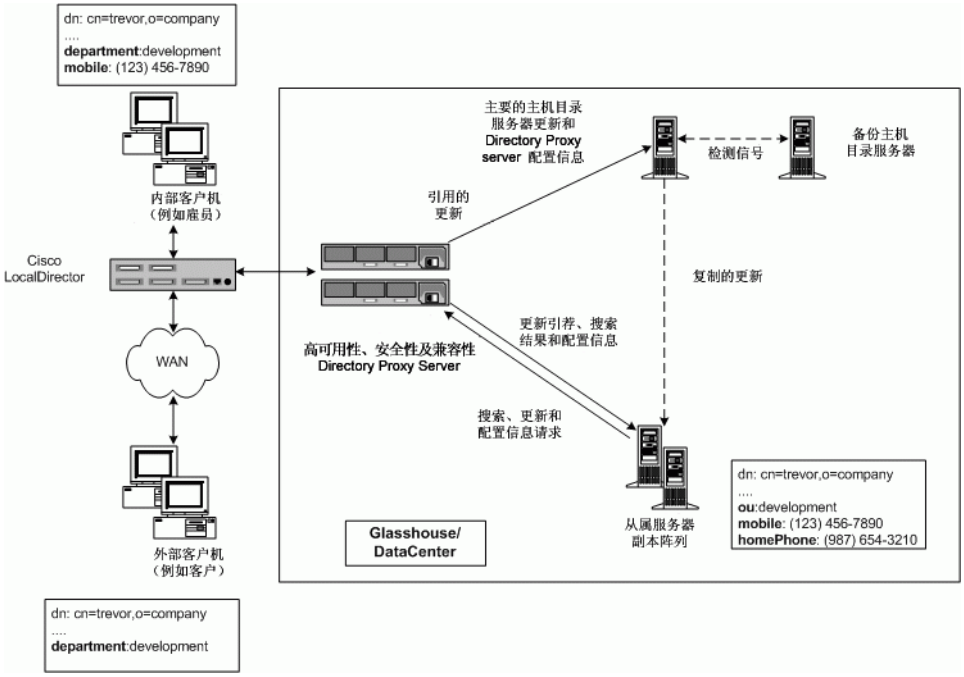
集中式 LDAP 目录基础结构

下列几部分介绍集中式 LDAP 目录基础结构中 Directory Proxy Server 的作用：

客户方案

图 2-3 描述的是一家大型跨国企业，客户和雇员遍布全世界，企业需要部署公司白页和黄页 （电子电话簿）以降低印刷纸质电话簿的成本，提高公司信息的准确性，并减少对环境资源的消耗。必须使用相应的访问控制同时向客户和雇员提供白页和黄页信息。同时由于客户和雇员分布于全世界的各个时区，因此必须全天候地提供这些信息并且将这些信息归类为关键任务。

图 2-3 集中式 LDAP 目录基础结构



客户部署

该跨国企业决定部署集中式 LDAP 目录基础结构，以支持白页和黄页的部署。由于白页和黄页仅用于为公司雇员提供信息，因此本实例中选择了集中式部署。尽管旨在使客户可以访问某些信息，但这不是客户数据库。由于预计伸缩性和性能都不会出现问题，因此确定目录数据库计划的大小（大约 200,000 条）不足以需要更加复杂的分布式部署模式。

由于存在高可用性需求，该企业决定部署由单个供应商目录服务器提供的多个使用者目录服务器副本。为消除单个供应商目录服务器引起的单点故障，企业部署了备份供应商目录服务器。

Directory Proxy Server 的部署基于三个不同的原因。第一，为所有的 LDAP 客户机与目录服务器副本阵列之间提供负载平衡以及自动故障转移和故障回复。第二，为了能够区分外部和内部客户机，并相应地设置相应的访问控制。第三，为使用白页和黄页的 LDAP 客户机与目录服务器自身之间提供兼容性。除了使用定制的白页和黄页应用程序之外， LDAP 客户机还使用了大量现成的支持 LDAP 的应用程序，他

们具有固定的架构需求。这些架构需求并不是始终能够符合企业设计的目录架构，因此需要一些基本的架构属性映射。此外，并非客户机使用的所有支持 LDAP 的应用程序都能够正确地处理从目录服务器接收到的引荐。 Directory Proxy Server 被配置为代表客户机跟随这些引荐。

LDAP 请求流

所有的客户机请求 （无论来自内部还是外部客户机，是搜索请求还是更新请求）均通过 Cisco LocalDirector 发送到 Directory Proxy Server 的实例。此处显示的 LocalDirector 产品仅作为 IP 数据包交换的一个示例，确保客户机始终能够至少访问一个 Directory Proxy Server。部署 Directory Proxy Server 多个实例的目的是确保没有单点故障。 Directory Proxy Server 实例对从阵列中所有使用者目录服务器中的客户机接收的所有请求进行负载平衡。 Directory Proxy Server 还将检测任何使用者服务器的故障并将故障转移到阵列中可用的使用者服务器。

由于使用者服务器是只读副本，因此他们被配置为从客户机接收更新请求时返回 LDAP 引荐。此引荐包含的 LDAP URL 指向供应商目录服务器。当目录服务器返回引荐时， Directory Proxy Server 代表客户机识别并跟随引荐。他绑定到供应商目录服务器并将向其发送更新请求。供应商目录服务器将此更新应用于供应商数据库，并通过 Directory Proxy Server 将响应发回到客户机。随后，供应商目录服务器将更新下传到相应的使用者目录服务器。

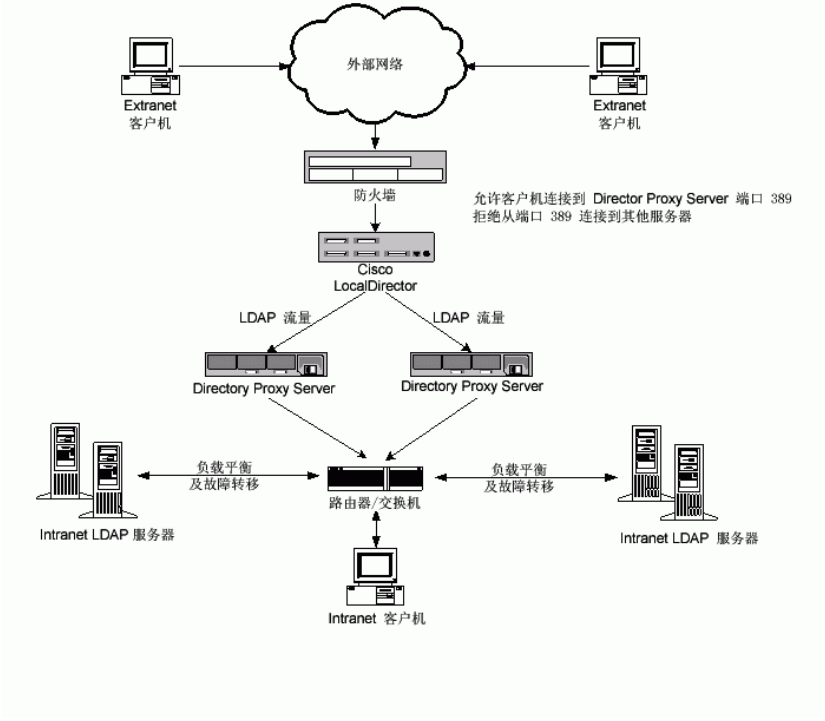
客户机发送的搜索请求通过 Directory Proxy Server 路由到使用者目录服务器副本的阵列。可将 Directory Proxy Server 配置为：“检查”这些搜索请求，然后将其发送到目录服务器，过滤出任何不符合为特定客户机组配置的访问控制和安全规则的请求，并执行任何必需的映射。还可将 Directory Proxy Server 配置为：“检查”目录服务器返回的搜索结果，然后再次执行相应的过滤和映射。在图 2-3 所示的示例中，内部和外部客户机均已请求搜索属于“Trevor”的条目。 Directory Proxy Server 同等对待这些传入的请求，无论客户机的类型如何。目录服务器成功执行请求并将“Trevor”的条目返回到 Directory Proxy Server。 Directory Proxy Server 已经配置为：根据原始请求是来自内部还是外部客户机，以不同方式来处理搜索结果。如果是外部客户机，则条目中的移动电话和家庭电话号码字段都会被过滤掉，因为他们被视为不适宜客户使用的数据。还要注意 ou: development 特性 / 值对已经映射到 department: development。这是必需的，因为客户机要使用其访问目录的某一应用程序 （如 Outlook、 Outlook Express）已有固定的架构元素，他们与企业目录服务器中部署的架构元素不匹配。如果是内部客户机，则可确定移动电话号码属于雇员共享的重要数据元素，而家庭电话号码则不是。因此，对于内部客户机， Directory Proxy Server 配置为：只过滤出家庭电话号码，并允许客户机查看移动电话号码。请注意还要执行 ou 特性到 department 特性的相同映射。

所有的 Directory Proxy Server 被配置为在供应商目录服务器中启动和查找其配置。这样允许从一个目录集中管理多个 Directory Proxy Server 配置。

使用单防火墙部署 Directory Proxy Server

您的组织的防火墙必须按图 2-4 中所示进行配置，以便只允许 LDAP 客户机访问运行 Directory Proxy Server 的计算机和端口。通常， LDAP 客户机将连接到 TCP 端口 389。这将保护运行 Directory Proxy Server 的主机免遭未经授权的客户机可能试图对其进行的访问。同时，通过使用路由器交换机将运行代理服务器的主机置于他自己的 LAN 中，将保护内部网络免遭拒绝服务的攻击，如多余的流量堵塞您的网络。防火墙也应该禁止 LDAP 访问 LDAP 目录服务器在其上处于 “隐藏”状态的计算机和端口，从而保护 LDAP 目录数据库。

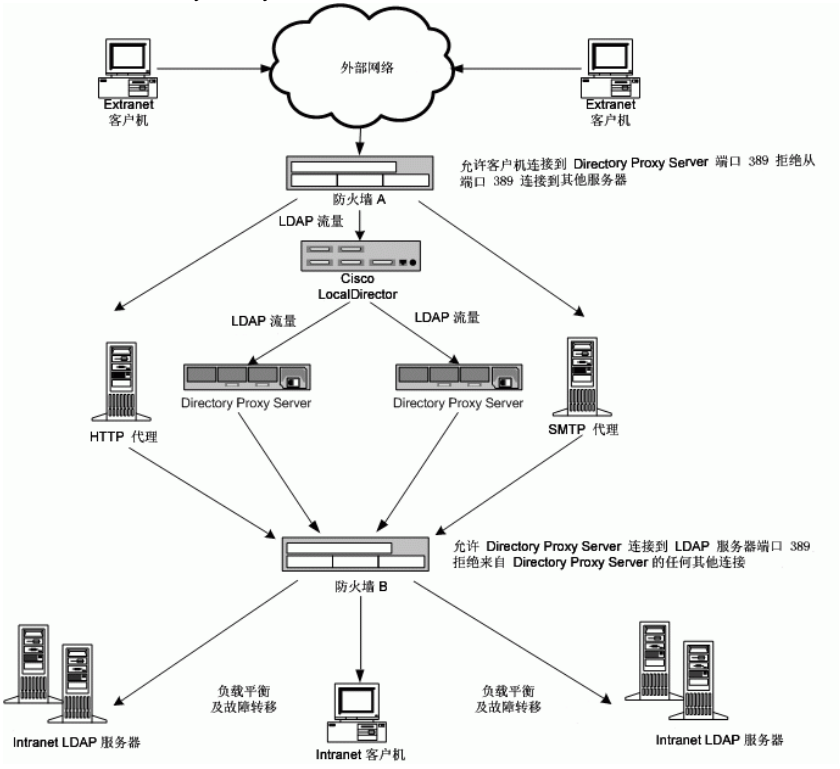
图 2-4 Directory Proxy Server 使用单防火墙的设置



使用双防火墙部署 Directory Proxy Server

图 2-5 中所示的配置具有图 2-4 中显示的配置的所有优势，同时增加了某些安全性。安装双防火墙会在 “代理服务器” 周围形成一个控制区，使站点管理员能够限制外部网络的流量。同时确保无法直接利用其中一个 “代理” 服务器的安全隐患攻击内部网络中的其他计算机。防火墙 A 将配置为：如果目标 IP 地址为处理 TCP 或 UDP 协议的代理服务器的 IP 地址，则仅允许传入的数据包。防火墙 B 将配置为：只允许来自代理计算机的数据包，这些代理计算机适用于代理服务器需要访问的服务器。

图 2-5 Directory Proxy Server 使用双防火墙的设置



第 II 部分

系统调优

第 41 页上的 “系统调优”

第 3 章

系统调优

要优化基于 Directory Proxy Server 的服务的性能，需要对系统进行调优。有关如何优化系统的信息，请参阅以下部分：

验证系统调优

`idsktune` 程序分析 Solaris 内核的优化。该程序发现错误并建议对系统的优化进行改进。在用于安装的解压缩软件包目录中提供了 `idsktune` 程序。

有关优化的详细信息，请参阅下列文档

- 有关 Solaris 基本优化的信息，请参阅 *Sun Performance and Tuning:Java and the Internet* (ISBN 0-13-095249-4)。
- 有关 Solaris 高级优化的信息，请参阅 *Solaris Tunable Parameters Reference Manual*。

➤ 验证系统调优

1. 从安装目录，运行以下命令：

   ```
   # ./idsktune -q > idsktune.out
   ```

   `idsktune` 程序发现错误并建议您做一些可以改善系统性能的更改。

2. 修复所有指明的 ERROR 状况。

   如果不修复 ERROR 状况，安装则会失败。

   发行时推荐的修补程序如果未安装在系统上，则会报告为丢失。甚至未安装在系统上的软件包的修补程序也会被报告为丢失。

3. 按照建议改善系统性能。

警告 如果要更改参数，那么需要知道所做的更改对正在系统上运行的其他应用程序有何影响。

设置最大同时连接数

与 Directory Proxy Server 的最大同时连接数是由文件 /etc/system 中的文件描述符参数 rlim_fd_max 来设置。

如果 /etc/system 文件中不存在 rlim_fd_max 参数，则与 Directory Proxy Server 的最大同时连接数为 1024。

rlim_fd_max 参数的最大值是 4096。将 rlim_fd_max 参数的值增大到 4096 以上可能会影响系统的稳定性。

➤ 设置与 Directory Proxy Server 的最大同时连接数

1. 将下面一行添加到 /etc/system 文件：

   ```
   set rlim_fd_max=4096
   ```

2. 重新启动系统。

优化 TCP

缺省情况下， Solaris 内核中的 TCP/IP 实现并没有针对 Internet 或 Intranet 服务进行正确的调优。优化下列参数以适应安装环境的网络拓扑。

表 3-1 TCP 优化参数

参数	说明
tcp_time_wait_interval	指定 TCP 连接在关闭后还保留在内核表中的毫秒数。 如果该值大于 30000 （30 秒），而且该目录正在某个 LAN、 MAN 中或单一网络管理下使用，则应减少该参数的值。要减少该参数的值，请将如下一行添加到 /etc/init.d/inetinit 文件中： `ndd -set /dev/tcp tcp_close_wait_interval 30000` 该参数仅针对 Solaris 8。

tcp_conn_req_max_q0, tcp_conn_req_max_q	控制内核作为 Directory Proxy Server 过程时可接受的最大待办事项连接数。
	如果预计有大量客户机同时使用该目录，则应将这些参数的值至少增大到 1024。要增大这些参数值，请将如下行添加到 /etc/init.d/inetinit 文件中：
	`ndd -set /dev/tcp tcp_conn_req_max_q0 1024`
	`ndd -set /dev/tcp tcp_conn_req_max_q 1024`

tcp_keepalive_interval	对于每个打开的 TCP 连接而言，指定由 Solaris 发送的保持连接数据包之间的间隔（秒数）。 此参数用于移除那些已经从网络中断开的客户机的连接。 此外，还可以使用 Directory Proxy Server 控制台配置屏幕上的 Specify timeout 选项移除闲置的连接。
tcp_rexmit_interval_initial	在 LAN 或高速 MAN 或 WAN 上执行服务器性能测试时，需要对该值进行检查。对于在广域 Internet 上的操作，请不要更改该参数的值。
tcp_smallest_anon_port	控制可同时连接到服务器的连接数。 如果 rlim_fd_max 参数的值设置为大于 4096，则应减小该参数的值。要减少该参数的值，请将如下一行添加到 /etc/init.d/inetinit 文件中： `ndd -set /dev/tcp tcp_smallest_anon_port 8192`
tcp_slow_start_initial	如果客户机主要使用 Windows TCP/IP 堆栈，则应对该参数进行检查。
tcp_ip_abort_cinterval	控制在建立新连接时 Directory Proxy Server 等待 LDAP 服务器作出响应的毫秒数。 要减少该参数的值，请将如下一行添加到 /etc/init.d/inetinit 文件中： `ndd -set /dev/tcp tcp_ip_abort_cinterval 10000` 在某些情况下，也可能有必要更改 tcp_ip_abort_interval 和 tcp_strong_iss 优化参数。

第 III 部分

基于控制台管理

第 4 章

Directory Proxy Server 控制台简介

安装 Directory Proxy Server 后，首先将其配置为根据目录部署进行工作，然后密切监视其活动。在管理 Directory Proxy Server 的过程中，您将执行服务器特定的任务：如启动、停止和重新启动服务器；创建组；设置服务器以标识某些事件并执行适当操作；更改配置；执行任意常规服务器维护任务；以及监视日志等。

为了让您既快速又方便地完成这些服务器特定任务， Directory Proxy Server 提供了基于 GUI 的管理工具，称为 *Directory Proxy Server 控制台*和 *Directory Proxy Server 配置编辑器控制台*，它们均可从控制台内部进行访问。本章提供了 Sun Java System 和 Directory Proxy Server 控制台的概述。

本章包含以下几个部分：

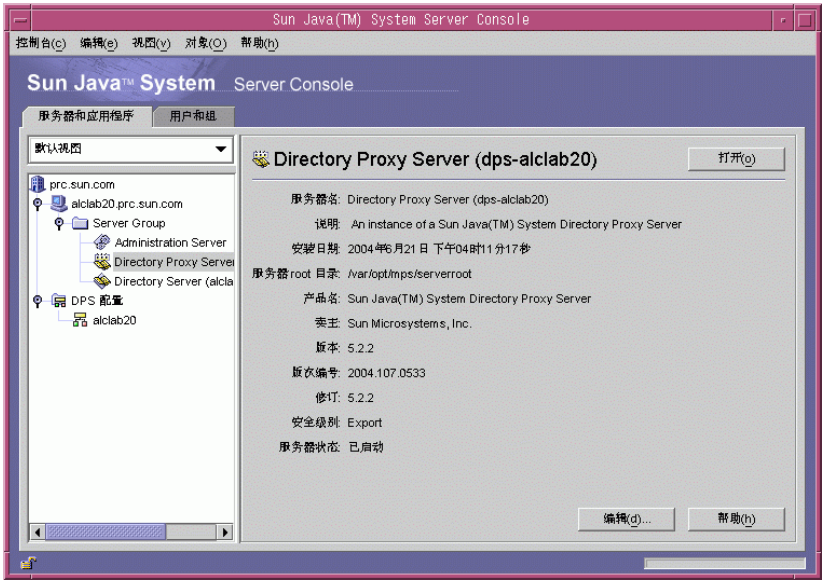
注 您可以使用 Sun Java System 服务器控制台来管理各种网络资源。然而，本章只侧重于介绍如何使用 Sun Java System 服务器控制台进行 Directory Proxy Server 管理。有关 Sun Java System 服务器控制台的完整信息，请参阅 《*使用 Sun Java System 服务器控制台管理服务器*》，它包含在 Directory Proxy Server 文档中。也可以通过以下站点获取该书的副本：http://docs.sun.com/

Sun Java System 服务器控制台入门

Sun Java System 服务器控制台是独立的 Java 应用程序，为在企业*配置目录*中注册的所有网络资源提供基于 GUI 的前端。这个统一的管理界面通过向网络上安装的所有 Sun Java System 5.x 版服务器实例提供访问点简化了网络管理。同样，它通过向用户目录提供统一的管理界面也简化了基本用户和组管理。

图 4-1 显示了选择 Directory Proxy Server 实例时 Sun Java System 服务器控制台的“服务器和应用程序”选项卡。

图 4-1 Sun Java System Server Console：“服务器和应用程序”选项卡



“服务器和应用程序”选项卡

对于 Sun Java System 服务器控制台的任意给定实例，它可以管理的网络范围由其配置信息存储在同一配置目录中的资源集定义，即可以从 Sun Java System 服务器控制台监视的主机和服务器最大集。*超级管理员*（管理配置目录的人员）可以设置在配置目录中注册的所有网络资源的访问权限。因此，对于使用 Sun Java System 服务器控制台的给定管理员，可见主机和服务器的实际数目可能会少些，具体取决于超级管理员所设置的访问权限。

“服务器和应用程序”选项卡显示了在特定配置目录中注册的所有服务器，您可以统一查看所控制的所有服务器软件和资源。您控制哪些软件和资源取决于超级管理员为您设置的访问权限。

利用该视图，只需一步操作，您就可以跨任意服务器组或群集执行任务。换句话说，您可以使用 “服务器和应用程序”选项卡管理在一台计算机的不同端口上安装的单台服务器或多台服务器。另外，也可以通过双击相应服务器实例条目 (SIE) 的图标来访问单台服务器控制台 （或管理界面）。

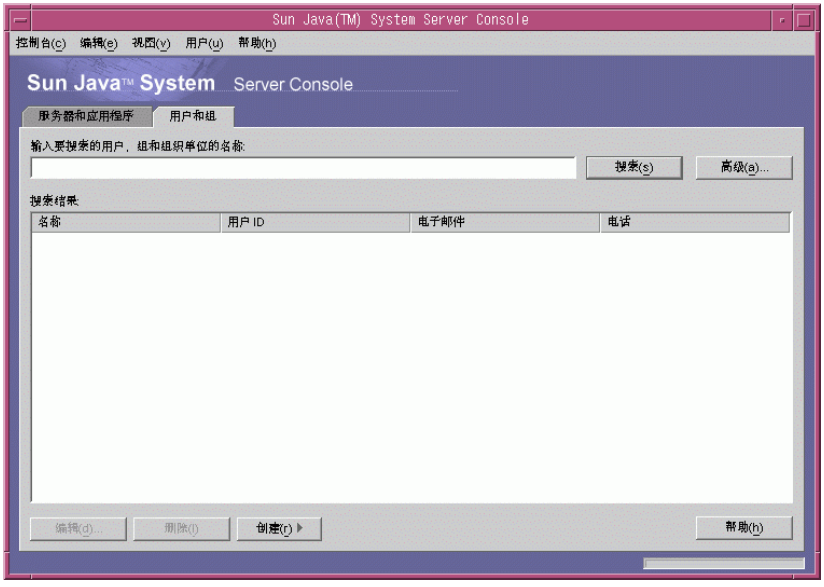
您可以通过 “服务器和应用程序”选项卡完成各项 Directory Proxy Server 特定的任务：

- 启动 Directory Proxy Server 控制台。
- 启动 Directory Proxy Server 配置编辑器控制台 （以便您可以配置 Directory Proxy Server 组）。
- 设置 Directory Proxy Server 的访问权限。
- 启动管理服务器控制台 （以便您可以配置管理 Directory Proxy Server 的管理服务器实例）。

“用户和组”选项卡

“用户和组”选项卡 （如图 4-2 中所示）管理用户帐户、组列表和单个用户和组的访问控制信息。在 Sun Java System 服务器控制台框架中注册的所有应用程序都共享用户目录中的核心用户和组信息，该目录通常是公司范围用户数据的全局目录。

图 4-2 Sun Java System Server Console：“用户和组”选项卡



通过该选项卡，您可以执行以下用户特定的任务以及组特定的任务：

- 添加、修改和删除用户目录中的用户和组信息。

- 搜索用户目录中的特定用户和组条目。

Sun Java System 管理服务器

Sun Java System 管理服务器是基于 Web (HTTP) 的服务器，使您可以通过 Sun Java System 服务器控制台配置所有 Sun Java System 服务器，其中包括 Directory Proxy Server。您必须在管理服务器 （和配置目录）运行之后才能配置任意的这些服务器。管理服务器与所有 Sun Java System 服务器一起提供，并在安装*服务器组*中的首台服务器时进行安装。服务器组指的是安装在服务器根目录中并由管理服务器的单一实例管理的服务器。

访问管理服务器的方法是：在 Sun Java System 服务器控制台的登录屏幕中输入它的 URL，如第 51 页上的 “登录到 Sun Java System 服务器控制台”中所述。该 URL 基于主机名和安装 Directory Proxy Server 时所选的端口号。 URL 的格式类似于：`http://<machine_name>.<your_domain>.<domain>:<port>`

每当尝试访问管理服务器时，将提示您通过输入用户 ID 和口令到配置目录验证自己的身份。这些是在您的计算机上安装 Directory Proxy Server （或服务器组的首台服务器）和管理服务器时指定的*管理员*用户名和口令。运行管理服务器后，您就可以使用 Sun Java System 服务器控制台管理该组中的所有服务器，包括 Directory Proxy Server。

有关管理服务器的全部详细信息，请参阅 《*使用 Sun Java System 服务器控制台管理服务器*》。要在 Directory Proxy Server 安装中查找该书的联机版本，请打开以下文件：`<server-root>/manual/en/admin/ag/contents.htm`

启动管理服务器

Directory Proxy Server 安装程序自动启动在安装期间所标识的管理服务器实例以监视 Directory Proxy Server。如果在 Directory Proxy Server 安装后停止管理服务器，则必须启动它后才能从 Directory Proxy Server 控制台管理 Directory Proxy Server。

可以从命令行启动管理服务器。

- 要从命令行启动管理服务器，请执行以下操作：

  在提示符下，输入以下行：`<server-root>/start-admin`

所有上述提及的方法都在安装期间指定的端口号处启动管理服务器。服务器运行后，就可以使用 Sun Java System 服务器控制台访问 Directory Proxy Server。

停止管理服务器

在不使用管理服务器时将其关闭是一个安全的好做法。这样会降低其他人员更改您的配置的机会。可以通过 Sun Java System 服务器控制台或命令行关闭服务器。

- 要从 Sun Java System 服务器控制台关闭管理服务器，请执行以下操作：
  - **a.** 登录到 Sun Java System 服务器控制台。
  - **b.** 在 “服务器和应用程序”选项卡中，找到要关闭的管理服务器实例，并双击相应的条目。

    管理服务器控制台随即出现。
  - **c.** 在 “任务”选项卡中，单击 “停止服务器”。
- 要从命令行关闭管理服务器，请执行以下操作：

  在提示符下，输入以下行：`<server-root>/stop-admin`

访问 Directory Proxy Server 控制台

要从 Directory Proxy Server 控制台执行任意 Directory Proxy Server 管理任务，需要首先将其打开。

- 登录到 Sun Java System 服务器控制台
- 打开相应的 Directory Proxy Server 控制台

登录到 Sun Java System 服务器控制台

只有在相应配置目录和管理服务器运行时才可以启动和使用 Sun Java System 服务器控制台。如果服务器尚未运行，请转至命令行并启动它们。有关从命令行启动管理服务器的信息，请参阅第 50 页上的 “启动管理服务器”。有关启动配置目录的信息，请查看 Sun Java System 目录服务器文档。

在启动 Sun Java System 服务器控制台后，将显示一个登录窗口。要求您通过输入管理员 ID、口令和表示您所访问的服务器组的管理服务器的 URL （包括端口号），向配置目录进行验证。如果您不具备网络上至少一个服务器组的访问特权，则无法使用 Sun Java System 服务器控制台。

➤ 登录到 Sun Java System 服务器控制台

1. 使用相应的选项打开 Sun Java System 服务器控制台应用程序：

   要在 UNIX 计算机上进行本地访问，请在命令行提示符下输入以下行：
   `<server-root>/start-console`

   Sun Java System 服务器控制台的 “登录”窗口随即出现。

2. 向配置目录验证您自己的身份。

   用户 ID。键入在计算机上安装管理服务器时指定的*管理员 ID*。在安装首台 Sun Java System 服务器时或作为 Directory Proxy Server 安装的一部分时安装了管理服务器。

   口令。键入在 Directory Proxy Server 安装期间在计算机上安装管理服务器时指定的*管理员*口令。

   管理 URL。该字段应显示指向管理服务器的 URL。如果没有 URL 或没有您想要的管理服务器的 URL，请在此字段中键入 URL。该 URL 基于主机名和安装 Directory Proxy Server 时所选的管理服务器端口号。请使用以下格式：

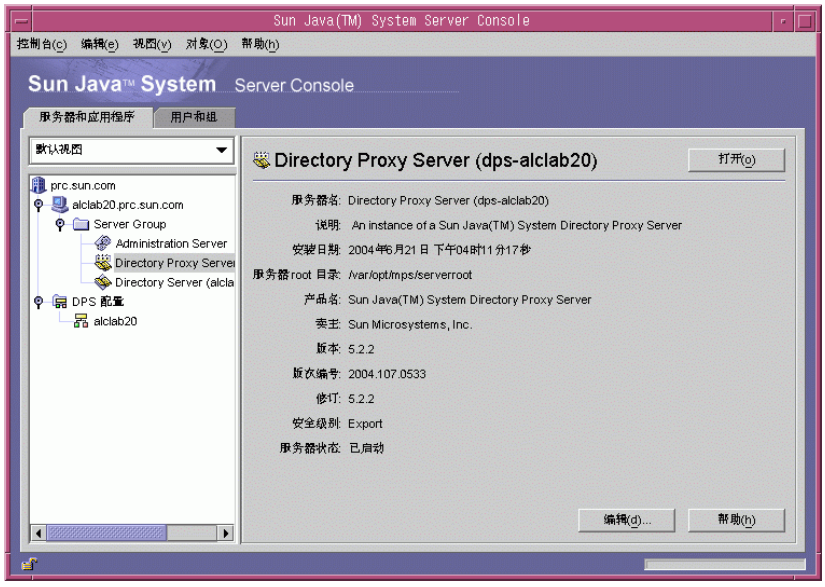
   `http://<machine_name>.<your_domain>.<domain>:<port_number>`

   例如，如果您的域名是 `sun`，并已在名为 `myHost` 的主机且指定为 `12345` 的端口号上安装了管理服务器，那么 URL 将表示为：`http://myHost.sun.com:12345`

3. 单击 “确定”。

   Sun Java System 服务器控制台将显示您所控制的所有服务器和资源的列表。

图 4-3 Sun Java System Server Console：访问 Directory Proxy Server



打开相应的 Directory Proxy Server 控制台

在 Sun Java System 服务器控制台中，您将注意到有两个 Directory Proxy Server 条目：一个是 Directory Proxy Server 实例节点，另一个是 Directory Proxy Server 配置节点。 Directory Proxy Server 实例节点与 Directory Proxy Server 实例相对应，Directory Proxy Server 配置节点与多个 Directory Proxy Server 实例共享的配置相对应。

每个节点均与基于 GUI 的管理界面相关联：

- Directory Proxy Server 控制台 - 通过此管理界面，您可以创建、配置和管理 Directory Proxy Server 实例；例如，启动实例、停止实例、指定配置和监视日志等。可以使用 Directory Proxy Server 控制台本地或远程访问服务器。使用 Directory Proxy Server 控制台创建和配置的 Directory Proxy Server 实例将影响使用该配置的所有 Directory Proxy Server 实例。
- Directory Proxy Server 配置编辑器控制台 - 逻辑和系统配置可由多个 Directory Proxy Server 实例共享。 Directory Proxy Server 实例共享配置信息的能力简化了管理 Directory Proxy Server 群集的任务。 Directory Proxy Server 配置编辑器控制台是让您可以配置和管理 Directory Proxy Server 群集的管理界面。通过此界面所做的编辑将影响所有使用此编辑配置的 Directory Proxy Server 实例。

打开 Directory Proxy Server 控制台

在登录到 Sun Java System 服务器控制台后，可以打开 Directory Proxy Server 控制台：在 Sun Java System 服务器控制台的导航树中，展开包含 Directory Proxy Server 实例所属服务器组的主机名，展开 "Server Group" 节点，选择与您需要的 Directory Proxy Server 实例相对应的条目，并单击 “打开”。 Directory Proxy Server 控制台随即打开 （图 4-4）。

图 4-4 Directory Proxy Server 控制台：任务

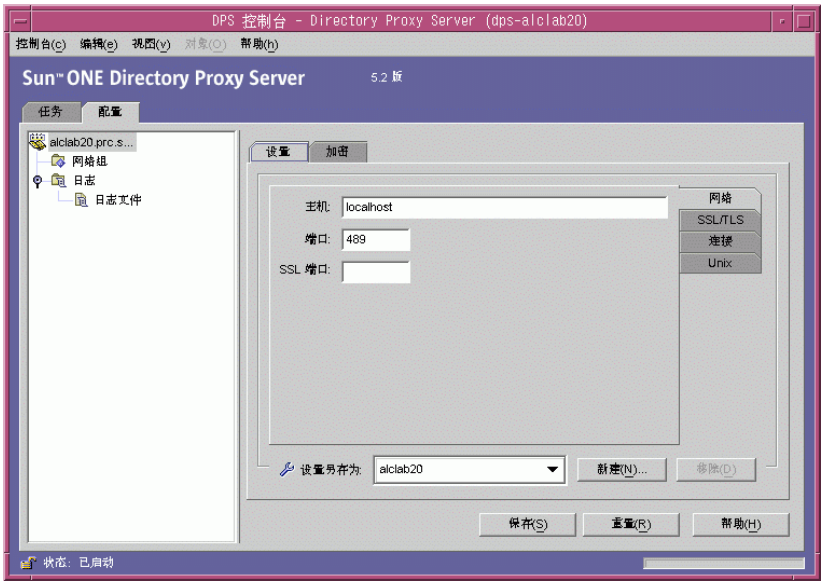
Directory Proxy Server 控制台有两个选项卡，即 “任务”和 “配置”选项卡，每个选项卡访问特定的管理区域。

通过 “任务”选项卡可以执行常规任务，如启动、停止、重新启动和重新加载服务器，分布或平衡不同 LDAP 目录之间的负载并管理证书等。有关更多信息，请参阅以下章节：

- 有关启动、停止和重新启动 Directory Proxy Server 的信息，请参阅第 59 页上的 “启动、重新启动和停止 Directory Proxy Server”。
- 有关负载平衡的信息，请参阅第 111 页上的 “定义和管理属性对象”。
- 有关管理证书的信息，请参阅第 159 页上的 “配置安全性”。

通过 “配置”选项卡 （图 4-5），您可以查看和修改特定实例的配置。

图 4-5 Directory Proxy Server 控制台：配置



“设置”和 “加密”选项卡与如何配置 Directory Proxy Server 的这一特定实例有关。

利用 “设置”选项卡 （图 4-5）可以配置以下参数：

网络。显示 Directory Proxy Server 实例的主机名、端口和 SSL 端口。

SSL/TLS。显示当前选定的配置， Directory Proxy Server 可通过这一配置将消息发送到服务器和客户机，并且从服务器和客户机获取 SSL 证书。它还将识别到 Directory Proxy Server 的客户机 SSL/TLS 版本和到后端通信的 Directory Proxy Server 的 SSL/TLS 版本。

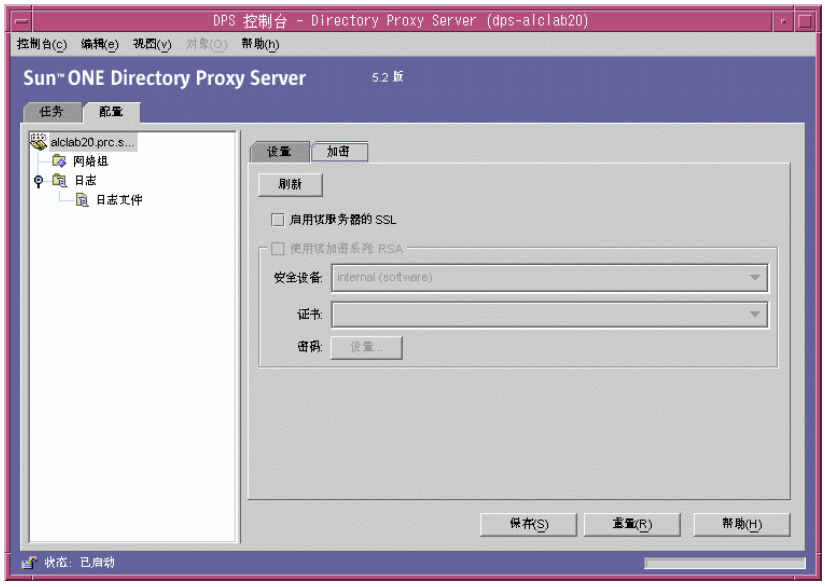
连接。显示 Directory Proxy Server 连接待办事项值，允许指定最大的连接数，并允许设置连接池超时值。

Unix。显示此 Directory Proxy Server 实例的 UNIX 用户 ID 和工作目录。

设置另存为。允许为列表框当前显示的编辑会话指定 Directory Proxy Server 名称值。还可创建新的 Directory Proxy Server 配置或删除旧的配置。

通过 “配置”选项卡的 “加密”选项卡 （图 4-6）可以查看和修改加密设置。

图 4-6 Directory Proxy Server 控制台：加密



通过 “加密”选项卡可以配置以下参数：

刷新。允许刷新当前屏幕值以查看新添加的证书。

启用该服务器的 SSL。启用此 Directory Proxy Server 实例的 SSL 加密。

使用该加密系列 RSA。使您可以设置此 Directory Proxy Server 实例的 “安全设备”、“证书”和 “密码设置”。

有关为您的系统设置加密的详细信息，请参阅第 69 页上的 “创建系统配置实例”。

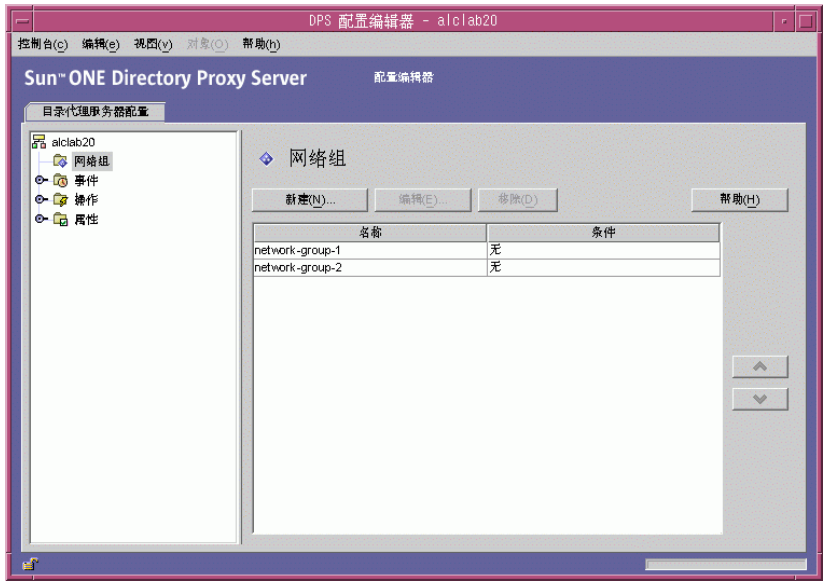
打开 Directory Proxy Server 配置编辑器控制台

按照以下步骤打开 Directory Proxy Server 配置编辑器控制台：

1. 在显示的图 4-6 中选择 “网络组”图标。
2. 选择组配置。
3. 单击 “编辑”。

Directory Proxy Server 配置编辑器控制台窗口随即打开。下图显示了 Directory Proxy Server 配置编辑器控制台。

图 4-7 Directory Proxy Server 配置编辑器控制台



左侧的导航树包含每个 Directory Proxy Server 基本配置对象的节点。展开一个主要节点将显示每个对象子类型的树节点。单击某个树节点将在右侧显示一个表，其中包含选定树节点指明的类型的所有当前对象。对象表 （其排序很重要），如网络组，具有一组向上 / 向下按钮，用于提高或降低各个对象的优先级。

表 4-1 列出了导航树中显示的配置对象类型。

表 4-1 Directory Proxy Server 配置编辑器控制台中的配置对象

配置对象类型	说明
网络组	每个网络组对象都标识一个特定的客户机群体，并指定一些限制，这些限制将在与该组匹配的客户机上强制实施。有关详细信息，请参阅第 79 页上的 “创建和管理组”。
事件	事件对象用于指定预设状态下发生的条件。可将条件附加到某些事件，如果条件符合，则 Directory Proxy Server 可以对这些事件执行某些操作。有关详细信息，请参阅第 133 页上的 “创建和管理事件对象”。
操作	操作用于指定事件发生时将执行的操作。有关详细信息，请参阅第 141 页上的 “创建和管理操作对象”。
属性	属性用于描述客户机上更为特殊的限制。每个组对象可能包括一组由属性对象定义的属性。有关详细信息，请参阅第 111 页上的 “定义和管理属性对象”。

第 5 章

启动、重新启动和停止 Directory Proxy Server

本章介绍如何启动、停止和重新启动 Directory Proxy Server 以及如何检查它的当前状态。

本章包含以下几个部分：

注 只有相应的目录服务器 （标识为*配置*目录）和管理服务器正在运行时，才可以使用 Directory Proxy Server 控制台。请务必在安装 Directory Proxy Server 期间指定的端口上启动管理服务器。为了最大限度地减少安全风险，请在使用了 Sun Java System 服务器控制台后关闭管理服务器。有关启动和关闭管理服务器的说明，请参阅第 50 页上的 “Sun Java System 管理服务器”。

启动和停止 Directory Proxy Server

安装 Directory Proxy Server 后，它将平稳运行、侦听和接受请求；并作为 UNIX 守护程序进程来运行。

可以使用以下方法启动和停止 Directory Proxy Server：

- 从 Sun Java System 服务器控制台 （本地和远程）
- 从命令行 （本地）

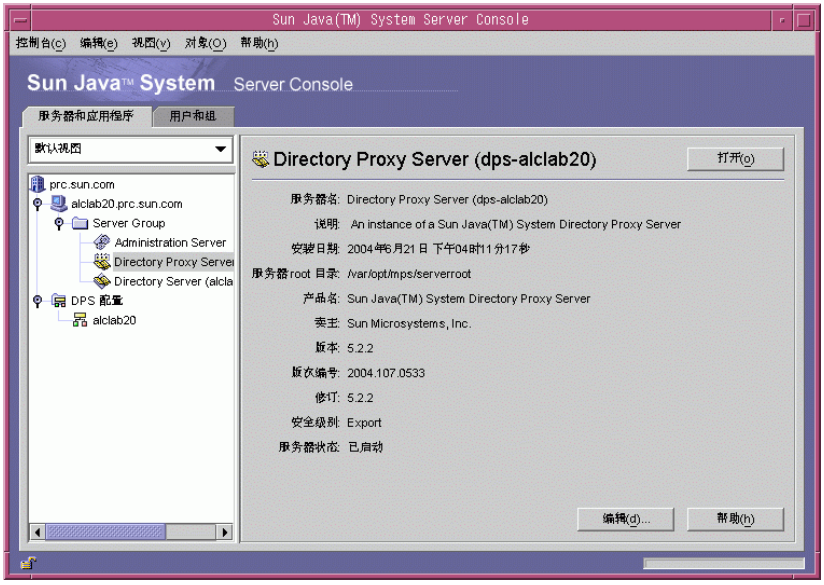
请注意，停止 Directory Proxy Server 会完全关闭它的所有组件、中断服务，直至服务器重新启动。如果主机崩溃或脱机，服务器就会停止，并且它正在服务的所有请求都将丢失。必须再次启动服务器才能恢复服务。

从 Sun Java System 服务器控制台启动和停止 Directory Proxy Server

可以使用 Sun Java System 服务器控制台来启动和停止安装在本地或远程主机上的 Directory Proxy Server。

➤ **启动或停止 Directory Proxy Server**

1. 登录到 Sun Java System 服务器控制台（请参阅第 51 页上的“登录到 Sun Java System 服务器控制台”）。
2. 在 “服务器和应用程序”选项卡中，展开主机名，然后展开包含要启动的 Directory Proxy Server 实例的 "Server Group"。



3. 选择一个 Directory Proxy Server 实例，然后单击 “打开”。 Directory Proxy Server 控制台随即打开。

4. 在 “任务”选项卡中，单击 “启动目录代理服务器”启动服务器，或单击 “停止目录代理服务器”停止服务器。

从命令行启动和停止 Directory Proxy Server

➤ **从命令行启动或停止 Directory Proxy Server**

1. 打开到服务器的终端窗口。
2. 在 UNIX 系统中，如果服务器在小于 1024 的端口上运行，请以超级用户身份登录；否则，请以超级用户身份或服务器的用户帐户登录。（缺省情况下，如果以超级用户身份运行 Directory Proxy Server，则它会将其用户 ID 更改为 `nobody`）。
3. 在命令行提示符下，请输入以下行：
   - 要启动 Directory Proxy Server，请输入：
     `<server-root>/dps-<hostname>/start-dps`
   - 要停止 Directory Proxy Server，请输入：
     `<server-root>/dps-<hostname>/stop-dps`

<server-root> 是保存 Directory Proxy Server 二进制文件的目录。该目录是在安装期间首次指定的。

<hostname> 是安装该 Directory Proxy Server 实例的主机的名称。

注 如果 Directory Proxy Server 已运行，则启动命令失败。请首先使用 stop-dps 命令停止服务器，然后再使用 start-dps 命令启动服务器。

重新启动 Directory Proxy Server

每当更改 Directory Proxy Server 配置时，必须保存更改，以便将其存储到配置目录中。所有配置更改都要求在保存这些更改后重新启动 Directory Proxy Server。如果需要重新启动，则控制台将会显示相应的提示。

重新启动期间， Directory Proxy Server 将重新读取其配置并将新配置用于以后的连接。已建立的客户机连接将继续使用旧配置，直至客户机断开连接。重新启动功能只能在 UNIX 平台使用。

可以使用以下方法重新启动 Directory Proxy Server：

- 从 Directory Proxy Server 控制台 （本地和远程）
- 从命令行 （仅限本地）

从命令行重新启动 Directory Proxy Server

➤ **从命令行重新启动 Directory Proxy Server**

1. 打开到服务器的终端窗口。
2. 在 Unix 系统中，以超级用户身份或者使用服务器的用户帐户 （如果通过这一方式启动了服务器）登录。
3. 在命令行提示符下，输入以下行：

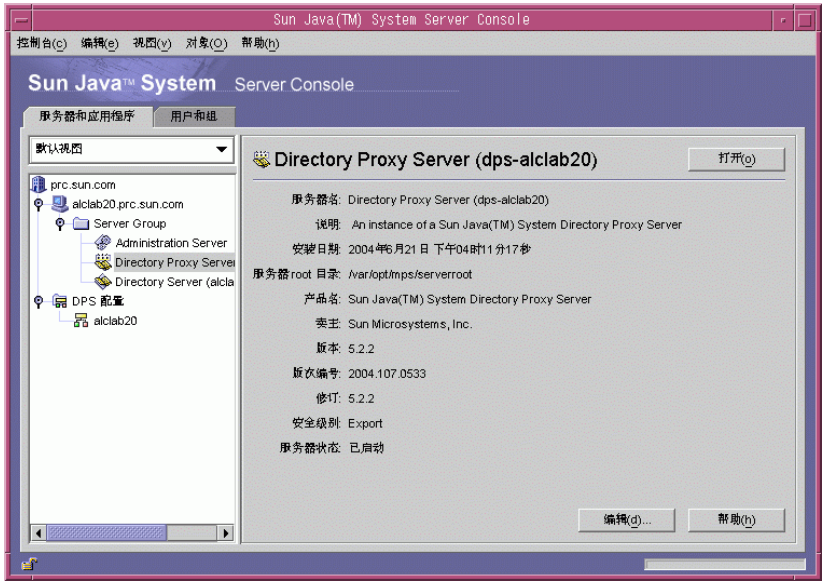
```
<server-root>/dps-<hostname>/restart-dps[.exe]
```

在 UNIX 平台上，从 Sun Java System 服务器控制台重新加载 Directory Proxy Server

在 UNIX 平台上，可以使用 Directory Proxy Server 控制台重新加载安装在本地或远程主机上的 Directory Proxy Server 配置。每当更改了 UNIX 平台上的 Directory Proxy Server 配置时，重新加载 Directory Proxy Server 配置都将使这些更改生效。在 NT 平台上，必须重新启动 Directory Proxy Server 配置。

➤ 从 Directory Proxy Server 控制台重新加载 Directory Proxy Server

1. 如果尚未查看 Directory Proxy Server 控制台，请登录到 Sun Java System 服务器控制台 （请参阅第 51 页上的 “登录到 Sun Java System 服务器控制台”）。
2. 在 “服务器和应用程序”选项卡中，展开主机名，然后展开包含要重新启动的 Directory Proxy Server 实例的 "Server Group"。



3. 选择要启动或停止的 Directory Proxy Server 实例，然后单击 “打开”。Directory Proxy Server 控制台随即打开。

4. 在 “任务”选项卡中，单击 “重新加载目录代理服务器配置”以重新加载服务器。

检查 Directory Proxy Server 系统状态

可以使用以下两种方法检查某个特定的 Directory Proxy Server 实例是处于启动状态还是停止状态：

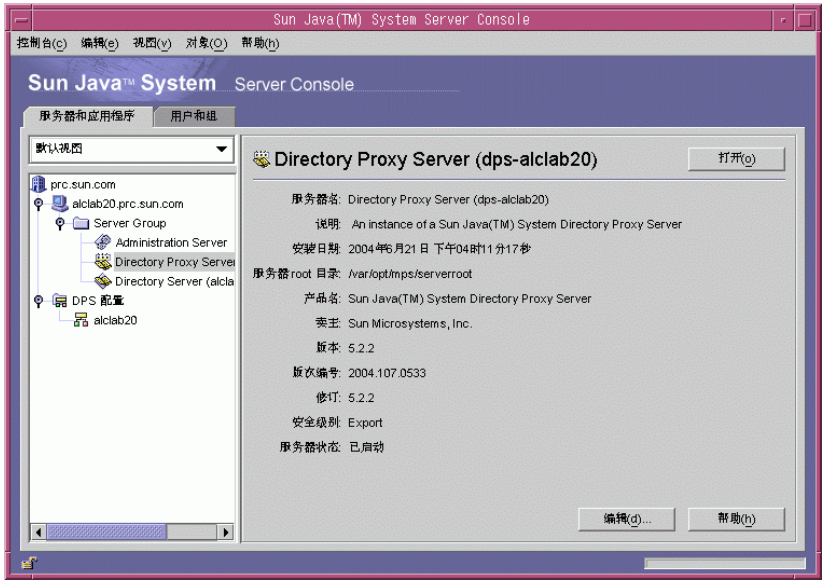
- 从 Sun Java System 服务器控制台 （本地和远程）
- 从命令行 （仅限本地）

从 Sun Java System 服务器控制台检查 Directory Proxy Server 状态

可以使用 Sun Java System 服务器控制台查明是否某个特定的 Directory Proxy Server 实例正在运行。

➤ 从 Sun Java System 服务器控制台检查 Directory Proxy Server 状态

1. 登录到 Sun Java System 服务器控制台（请参阅第 51 页上的“登录到 Sun Java System 服务器控制台”）。
2. 在“服务器和应用程序”选项卡中，选择要检查的 Directory Proxy Server 实例。



3. 在右侧窗格中，检查“服务器状态”字段。

   如果选中的 Directory Proxy Server 实例正在运行，则该状态将为*已启动*。否则，它将为*警报*、*停止*或者*未知*。当 SIE 名称为斜体时，还表示服务器实例处于停止状态。

从命令行检查 Directory Proxy Server 状态

➤ 从命令行确定 Directory Proxy Server 状态

1. 打开到服务器的终端窗口。
2. 在 Unix 系统中，以超级用户身份或者使用服务器的用户帐户（如果通过这一方式启动了服务器）登录。
3. 在命令行提示符下，输入以下行：

```
<server-root>/dps-<hostname>/status-dps[.exe]
```

从命令行启动和停止 Directory Proxy Server

Directory Proxy Server 程序作为 UNIX 守护程序进程或 NT 服务运行，通常在系统引导期间启动。

在所有平台上， Directory Proxy Server 的启动程序驻留在：

```
<server-root>/dps-<hostname>/start-dps
```

启动配置文件驻留在：

```
<server-root>/dps-<hostname>/etc/tailor.txt
```

Directory Proxy Server 可通过位于以下目录中的脚本启动或停止：

```
<server-root>/dps-<hostname>
```

如果 Directory Proxy Server 有效的用户 ID 与其实际的用户 ID 相同，那么在崩溃情况下它将仅生成一个 `core` 图像。因此，如果想让 Directory Proxy Server 生成一个核心，则必须将 `ids-proxy-sch-GlobalConfiguration` 对象类中的 `ids-proxy-con-userid` 特性设置为启动 Directory Proxy Server 进程的同一用户。缺省情况下，如果以超级用户身份运行 Directory Proxy Server，则其用户 ID 将更改为 `nobody`。

支持的标志

启动和停止脚本所支持的标志如表 5-1 中所述。

表 5-1 启动和停止脚本支持的标志

标志	说明
`-d`	出现此标志时， Directory Proxy Server 每次只处理一个传入的连接，并将更详细的内部跟踪信息发送到日志文件。该标志不能在正常的操作期间使用，因为它会阻止 Directory Proxy Server 守护程序与控制终端分离。
`-D`	此标志通知 Directory Proxy Server 向日志文件发送更详细的跟踪信息。Directory Proxy Server 将仍然处理多个客户机连接并作为守护程序运行。 `-d` 和 `-D` 标志应视为互斥的标志。
`-t <` 启动配置文件 >	该选项可用于指定备用启动配置文件。必须指定至该配置文件的绝对路径。
`-s`	该选项通知 Directory Proxy Server 使用 `LOG_DAEMON` 工具将初始日志消息发送到 `syslogd`。如果未定义环境变量 `dps_ROOT`，那么它就是缺省标志。

表 5-1 启动和停止脚本支持的标志 （续）

标志	说明
-M	如果指定此标志，Directory Proxy Server 将产生另一个进程来监视自己。在 Directory Proxy Server 意外退出的情况下，该监视进程会在 30 秒后重新启动 Directory Proxy Server。
-r	该标志用于将一个值附加到硬编码注册表路径的末尾。所产生的注册表路径将 Directory Proxy Server 服务指向其配置信息，如根或实例根名称。
-v	该标志打印 Directory Proxy Server 的版本信息。

重新启动 Directory Proxy Server

在 UNIX 平台上，可向 Directory Proxy Server 发送 SIGHUP 信号，使其重新读取它的配置。如果重新读取配置成功， Directory Proxy Server 将使用该新配置用于以后的连接。已建立的客户机连接将继续使用旧配置，直至客户机断开连接。

要让信号通知 Directory Proxy Server 重新读取其配置，请使用 hup-dps 命令，它位于 <server-root>/dps-<hostname> 中。

不能使用 HUP 信号工具更改某些特性值。要更改以下配置参数， Directory Proxy Server 必须关闭并重新启动。这些特性包括：

```
ids-proxy-con-listen-port
ids-proxy-con-listen-host
ids-proxy-con-ldaps-port
ids-proxy-con-foreground
ids-proxy-con-listen-backlog
ids-proxy-con-ssl-cert
ids-proxy-con-ssl-key
```

此外，也不能使用此工具更改日志属性 ids-proxy-sch-LogProperty。

在所有平台上， restart-dps 命令均位于 <server-root>/dps-<hostname> 中。重新启动命令只调用上述目录中的 stop-dps 和 start-dps 命令。

第 6 章

创建系统配置实例

系统参数是指影响 Directory Proxy Server 功能行为的那些参数。本章介绍如何指定和保存系统配置。

本章包含以下几个部分：

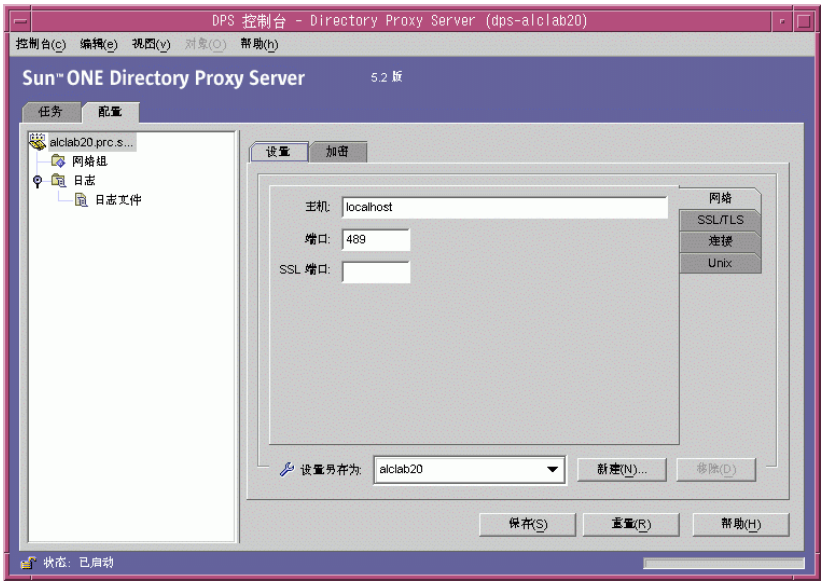
创建系统配置实例

本节说明如何配置 Directory Proxy Server 实例的系统特定参数。

➤ **创建系统配置对象**

1. 访问 Directory Proxy Server 控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。
2. 选择一个 Directory Proxy Server 实例，然后单击 “打开”。

3. 在 Directory Proxy Server 控制台上按 “配置”选项卡。



4. 单击 “新建”。

“新对象”窗口随即出现。

5. 在 “名称”字段中，键入系统配置的名称。名称必须是唯一的字母数字字符串。按 “确定”。

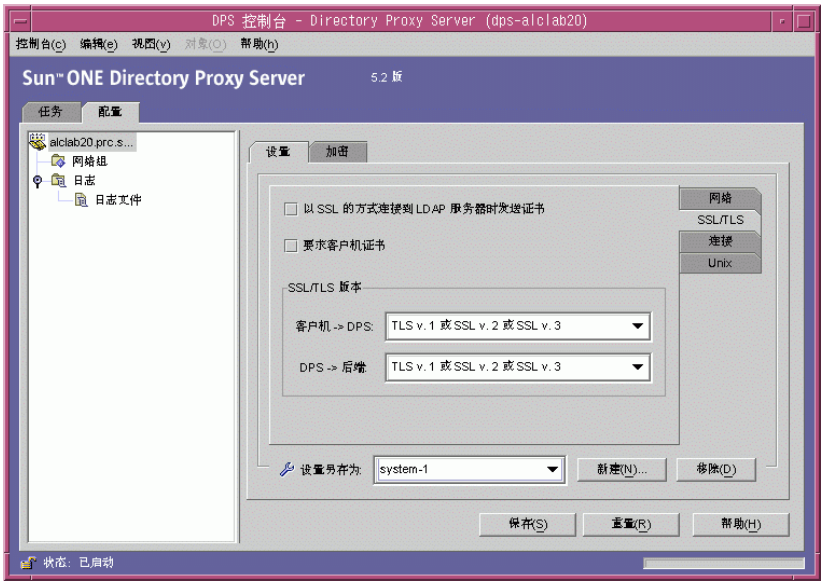
6. 在 “网络”选项卡中，指定此系统配置的常规设置：

   主机。输入 Directory Proxy Server 将在其上侦听连接的主机接口的名称。只有当运行 Directory Proxy Server 的主机上存在多个网络接口时才需要此特性。缺省情况下，主机名设置为 "localhost"，表明 Directory Proxy Server 在所有可用的网络接口上进行侦听。指定 "localhost" 将允许共享的系统属性。

   端口。输入 Directory Proxy Server 将在其上侦听传入连接的端口号。此字段的合法值为 1 到 65535。缺省值设置为 389，正如为 LDAP 指定的那样。此端口号必须与同一主机上运行的任何其他 LDAP 服务器使用的端口号不同。在 UNIX 平台上，若要在 1024 以下的端口号上进行侦听，就必须以超级用户身份来启动服务器。

   SSL 端口。输入一个表示将在其上侦听 LDAPS （通过 SSL 的 LDAP）连接的端口号。缺省情况下， Directory Proxy Server 不侦听来自 LDAPS 客户机的连接。必须提供该值 （例如 636）才能使用这一非标准功能来侦听客户机的 LDAPS 连接。该值必须与 “主机”值不同。该选项还要求 TLS/SSL 配置，此配置位于 “加密”选项卡中。

7. 按 SSL/TLS 选项卡。



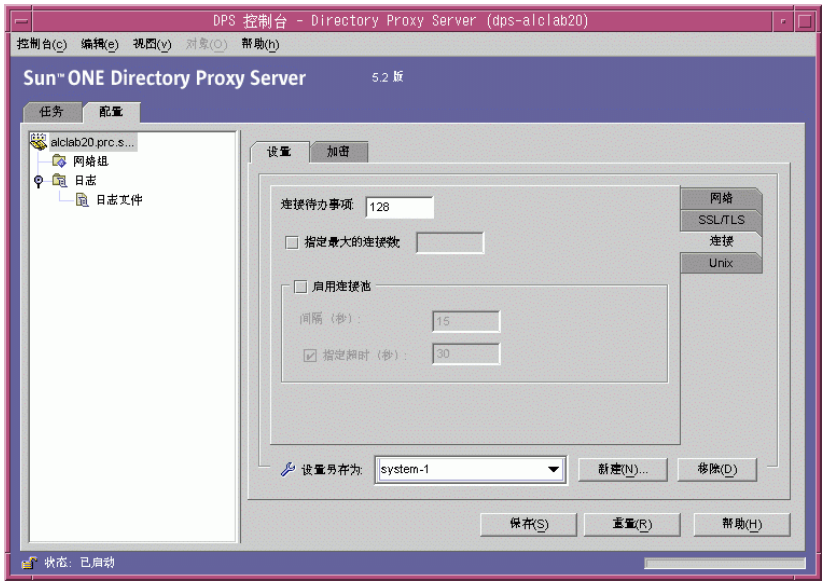
该窗口会显示缺省配置， Directory Proxy Server 可通过这一配置从服务器和客户机发送和请求 SSL 证书。该窗口提供了以下选项：

以 SSL 的方式连接到 LDAP 服务器时发送证书。如果希望 Directory Proxy Server 在建立 TLS 连接时将其证书发送到后端 LDAP 目录服务器，那么应启用此设置。缺省情况下禁用此设置。

要求客户机证书。启用此设置将指定 Directory Proxy Server 要求所有建立 SSL 会话的客户机都提交证书链。如果不提交证书链，则 Directory Proxy Server 将关闭连接。请注意，此选项不影响 Directory Proxy Server 和后端服务器之间的 SSL 会话。缺省情况下禁用此设置。

SSL/TLS 版本。选择“客户机”> Directory Proxy Server 旁边的下拉窗口以及 Directory Proxy Server >“后端”旁边的下拉窗口，为每种情况选择相应的 SSL/TLS 版本。如果为系统启用了 SSL，则必须指定一个版本。

8. 按 “连接”选项卡，指定 Directory Proxy Server 应如何维护其连接。



这将显示 Directory Proxy Server 连接待办事项值，允许指定最大的连接数，并允许设置连接池超时值。选择条目用于：

连接待办事项。输入大于零的值，用于指定侦听套接字队列中未完成连接的最大数。缺省值为 128 个连接。最大值依赖于基础操作系统配置。

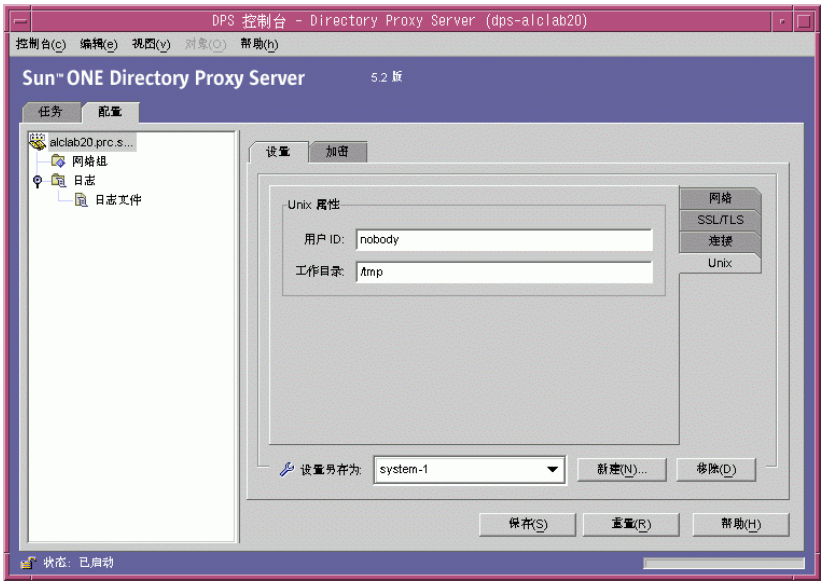
指定最大的连接数。选择该选项并输入一个值 （大于零），从而指定 Directory Proxy Server 将同时接受的客户机连接的最大数。若要获得不受限制的同时连接数，请不要选择此选项。

启用连接池。启用连接池模块，通过此模块 Directory Proxy Server 将预先连接到目录服务器。该设置的缺省值为禁用。如果启用连接池，则 Directory Proxy Server 将尝试重新使用现有连接与后端 LDAP 服务器相连。如果后端服务器位于广域网 (WAN) 上，则启用此选项可大大提高性能。输入下列值：

间隔。输入秒数 （大于或等于 1），用于指定时间间隔 （以秒为单位），Directory Proxy Server 将按此间隔对传入请求取样以预期未来活动。缺省值为 15。

指定超时。选择此选项并输入秒数 （大于或等于零），用于指定一段时间 （以秒为单位），在此时间段之后将终止 LDAP 服务器上的空闲连接。如果不选中此复选框，则不应用超时。缺省值为 30。该值应该小于后端 LDAP 服务器的空闲连接超时值。

9. 按 UNIX 选项卡。

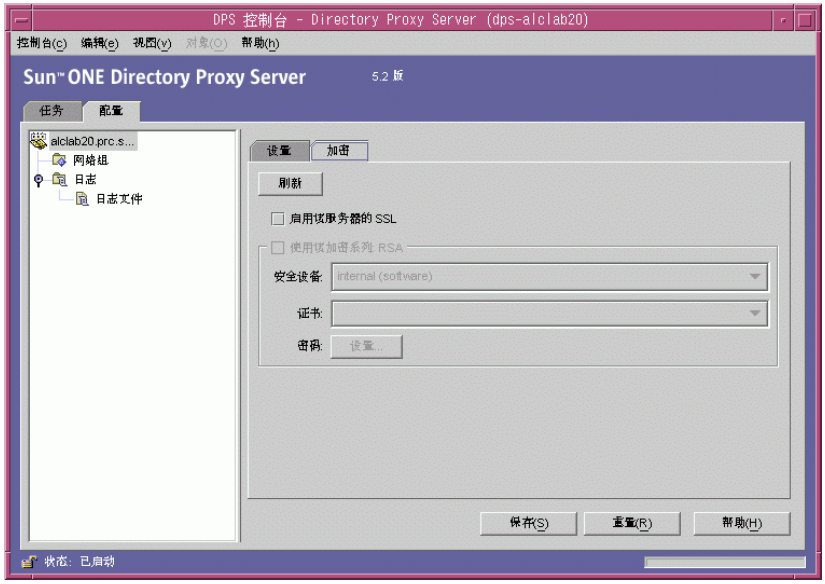


此面板只包含与 UNIX 环境中的 Directory Proxy Server 有关的特性。

用户 ID。输入 Directory Proxy Server 运行时使用的用户 ID。如果将 Directory Proxy Server 以超级用户身份来运行，则它将其 uid 更改为此处指定的某个值。缺省设置是切换为 *nobody*。

工作目录。输入 Directory Proxy Server 将从中运行的目录。 Directory Proxy Server 在启动时将其工作目录更改为此特性值指定的目录。缺省值为 `/tmp`。

10. 选择“加密”选项卡并为启用 SSL 的通信配置 Directory Proxy Server。有关为 SSL 通信配置服务器的信息，请参阅第 159 页上的 “配置安全性”。



通过 “加密”选项卡可以配置以下参数：

刷新。单击此按钮可刷新当前的屏幕值。刷新屏幕可查看最近创建的证书。

启用该服务器的 SSL。选择此框可启用 Directory Proxy Server 侦听安全连接所需的 SSL/TLS 信息。如果指定了 SSL 端口，必须启用此设置才能保存该配置。

使用该加密系列 RSA。选择此框可设置此 Directory Proxy Server 实例的 “安全设备”、“证书”和 “密码设置”。

安全设备。单击下拉窗口从可用的选项中进行选择。缺省值为 “内部 （软件）”。

证书。单击下拉窗口从可用的选项中进行选择。

密码。选择 “设置”以设置 SSL 2.0、 SSL 3.0 和 TLS 密码首选项。按 SSL 2.0、 SSL 3.0 和 TLS 选项卡，并选择各个选项卡所需密码旁边的复选框。

11. 单击 “保存”以保存对象。

    Directory Proxy Server 配置被修改，并提示重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

12. 重复步骤 4 到步骤 11 以创建任何其他对象。

13. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

注 对 “设置”选项卡中的 “主机”、“端口”和 “SSL 端口”字段的更改要求停止和启动 Directory Proxy Server。

有关停止和启动 Directory Proxy Server 的说明，请参阅第 59 页上的 “启动和停止 Directory Proxy Server”。

保存配置

`dpsconfig2ldif` 公用程序用于下载 Directory Proxy Server 配置并将其保存到 LDIF 文件中。在以下位置可找到该公用程序：

```
<Install Root>/bin/dps_utilities/dpsconfig2ldif
```

该公用程序需要两个参数：

参数	含义
-t *filename*	*Filename* 是至启动配置文件的路径。这通常是 etc 目录中的 tailor.txt 文件。
-o *filename*	在其中输出配置的文件的名称。

第 7 章

创建和管理组

当 LDAP 客户机从 LDAP 目录请求服务时，它将连接到 Directory Proxy Server，后者在客户机配置文件中识别客户机的访问权限，确定是否允许该客户机从目录请求服务，施加配置的限制，然后将请求转发到相应的目录。本章说明如何配置 Directory Proxy Server 以识别客户机及使用 Directory Proxy Server 配置编辑器控制台施加任意限制。

本章包含以下几个部分。

组概述

Directory Proxy Server 网络组对于了解 Directory Proxy Server 如何工作非常关键 - 它们定义 Directory Proxy Server 应如何识别 LDAP 客户机及 Directory Proxy Server 应对与该组匹配的客户机施加哪些限制。必须清楚地了解 Directory Proxy Server 组，以便使用它们有效地控制 LDAP 客户机的目录访问。

使用网络组识别以下项目：

- 客户机
- Directory Proxy Server 可将客户机请求转发给一组 LDAP 目录。
- 客户机在与其目录组进行互操作时可执行的一组操作。

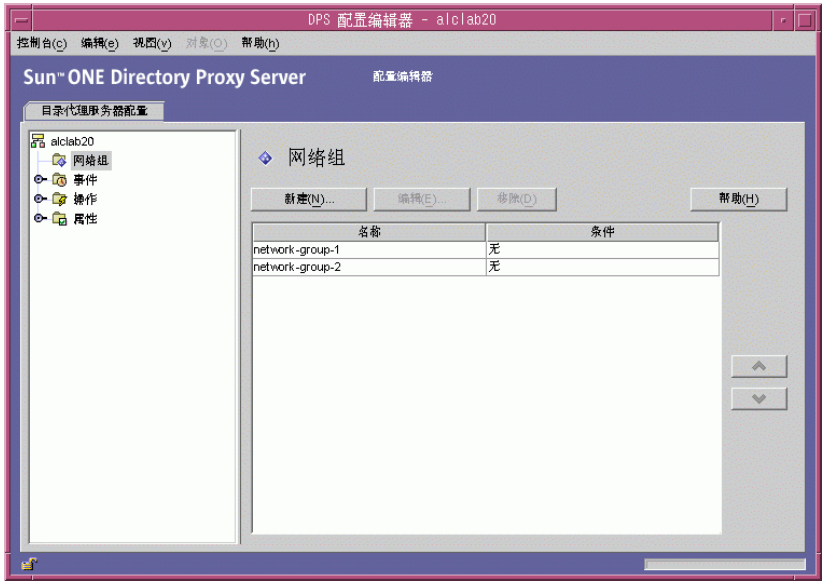
- 客户机与其目录组进行互操作时可访问的数据。（由于通过 Directory Proxy Server 可以隐藏某些条目并重命名目录中的特性，因此您可以有效控制客户机可以查看的目录中所包含的数据。）

Directory Proxy Server 通过尝试将连接的原始特性与组的条件相匹配来确定客户机的组成员资格。服务器按优先级的降序 （从最高到最低的优先级）检查当前配置的组。满足连接的原始特性的第一个网络组条件将接收该连接。为此，必须根据一般和特殊条件创建单独的组，并按从最特殊到最普通的优先级对这些组排序。

如果未找到与客户机匹配的组，那么客户机的请求将被拒绝并且连接将关闭。为此， Directory Proxy Server 配置中必须至少存在一个组条目。

组的优先级顺序由其在 Directory Proxy Server 配置编辑器控制台 “网络组”窗口中的位置指定 （请参阅图 7-1）。在此窗口中，列表底端组的优先级小于顶端组的优先级。未定义使用相同优先级计算组的顺序。

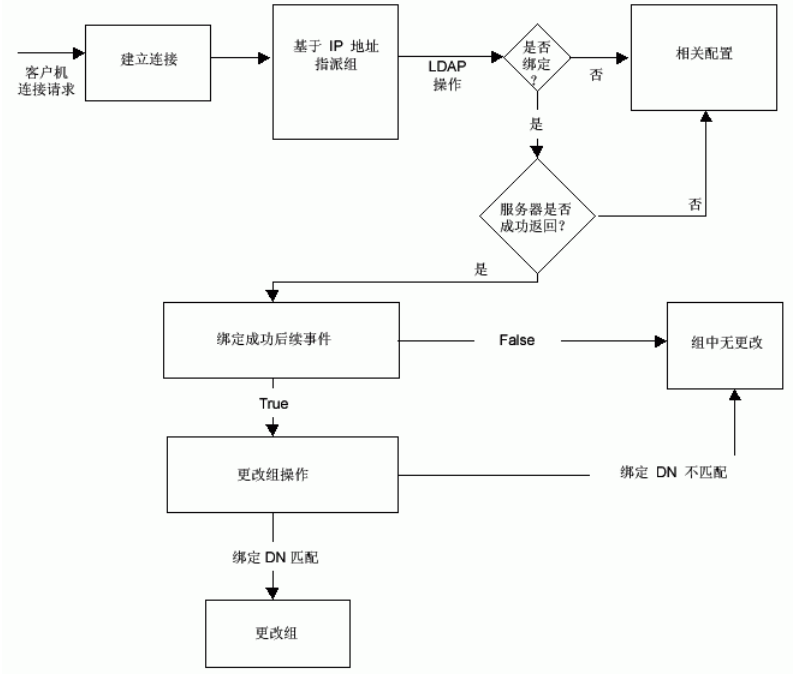
图 7-1 Directory Proxy Server 配置编辑器控制台：网络组



请注意，首先根据客户机所连接的网络地址 （如 IP 地址和 / 或域名）将其识别到某个组中。客户机在成功绑定后可更改它们的组；有关详细信息，请参阅第 133 页上的 “创建和管理事件对象”。客户机获得某组中的成员资格后，就意味着该组的所有属性都将应用于客户机。

图 7-2 说明了 Directory Proxy Server 如何计算组以响应客户机的查询。

图 7-2 确定组成员资格的 Directory Proxy Server 决策树



组的网络条件可基于以下条件：

- IP 地址或主机的网络掩码
  - 单个 IP 地址 （例如， `129.153.129.14`）
  - IP Quad/ 匹配位 （例如， `129.153.129.0/24`）
  - IP Quad/ 匹配 Quad （例如， `129.153.129.0/255.255.255.128`）
- 主机的域名
  - 全名 （例如， `box.eng.sun.com`）
  - 后缀名 （例如， `.eng.sun.com`）

请注意，如果域名后缀规则用于识别客户机，那么请确保将 DNS 设置为返回 DNS 查询的全限定名称。如果返回短名称，则此功能将不起作用。

- 特殊条件
  - `ALL` （用于 “catch-all” 组。）

- `0.0.0.0`（用于未将其初始成员资格考虑在内的组，例如，只用于客户机绑定时进行切换的组。）

要进一步了解 Directory Proxy Server 如何计算组，请查看表 7-1 中列出的示例组。该表显示了 5 个组，根据特殊到普通的网络条件创建，并按优先级的降序列出。

表 7-1 示例组

优先级	组名	网络条件
5	Admin-machine	129.153.129.72
4	IT-management-subnet	129.153.120.0/24
3	Operations	.ops.sun.com
2	Catch-all	ALL
1	Trusted	0.0.0.0

当 LDAP 客户机从 LDAP 目录请求服务时， Directory Proxy Server 将检查该请求是否来自 IP 地址 `129.153.129.72`。如果不是，Directory Proxy Server 检查该请求是否匹配 `129.153.129.0/24`。如果不匹配， Directory Proxy Server 检查该请求是否源自 `.ops.sun.com`。如果不是， Directory Proxy Server 将该连接放在 `catch-all` 组中，然后移到决策树的下一步 （请参阅图 7-2）。

图 7-3 显示的是 Directory Proxy Server 配置编辑器控制台的一部分，您可在其中创建组。

图 7-3 Directory Proxy Server 网络组定义

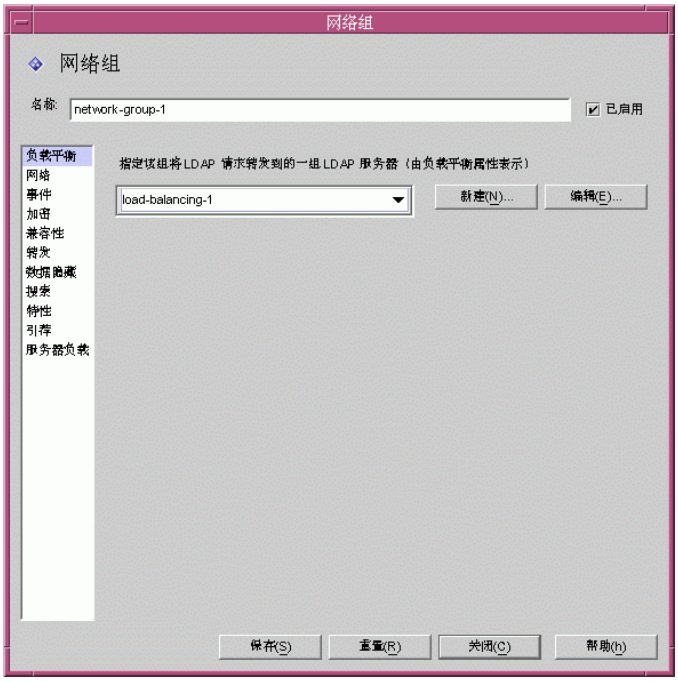


表 7-2 汇总了可在创建网络组时指定的条件。

表 7-2 网络组的可用条件列表

条件	说明
负载平衡	使您可以指定一组由负载平衡属性表示的 LDAP 服务器，该组将 LDAP 请求转发到此 LDAP 服务器组。第 124 页上的 “负载平衡属性”。
网络	使您可以为客户机指定连接详细信息和其他网络条件，以便将它们的请求排序或过滤到相应的组中。
事件	使您可以指定与组关联的事件 （如果有），以便该组中的客户机成功绑定到指定目录后能够有效地更改组。显示事件的现有对象列表；有关详细信息，请参阅第 84 页上的 “创建组”。
加密	使您可以为组指定加密条件 （例如，指定客户机是否可以请求 SSL 会话）。
兼容性	LDAP v2 规范 (RFC 1777) 不允许客户机在一次会话中绑定多次。然而，某些客户机却希望具有此功能。此选项可设置为与这些客户机进行互操作。
转发	使您可以指定将绑定、比较和其他 LDAP 请求传递给服务器的条件。

表 7-2 网络组的可用条件列表 （续）

条件	说明
数据隐藏	使您可以指定目录中哪些子树、条目或条目的特性将在组中隐藏。显示“禁止的条目”属性的现有对象列表；有关详细信息，请参阅第 115 页上的 “禁止的条目属性”。
搜索	使您可以指定搜索组的范围和大小限制。显示 “搜索大小限制”属性的现有对象列表；有关详细信息，请参阅第 128 页上的 “搜索大小限制属性”。
特性	使您可以指定阻止某些搜索种类和比较操作应用于 LDAP 服务器的规则。显示 “特性重命名”属性的现有对象列表；有关详细信息，请参阅第 112 页上的 “特性重命名属性”。
引荐	使您可以指定组是否应转发、跟随还是放弃服务器返回的引荐。请注意，不执行 LDAPv3 的客户机将不识别转发引荐。该设置适用于除搜索持续引荐之外的所有引荐。
服务器负载	使您可以指定详细信息，如组连接的总数、每个连接的同时操作数和总操作数、每个 IP 地址的同时操作数等。

创建组

本节说明如何使用 Directory Proxy Server 配置编辑器控制台创建组。在开始创建组之前，请先阅读第 79 页上的 “组概述”并了解 Directory Proxy Server 组的重要性。在创建所需的组并按优先级排序后，请先测试该配置以查看组能否按要求过滤客户机请求。

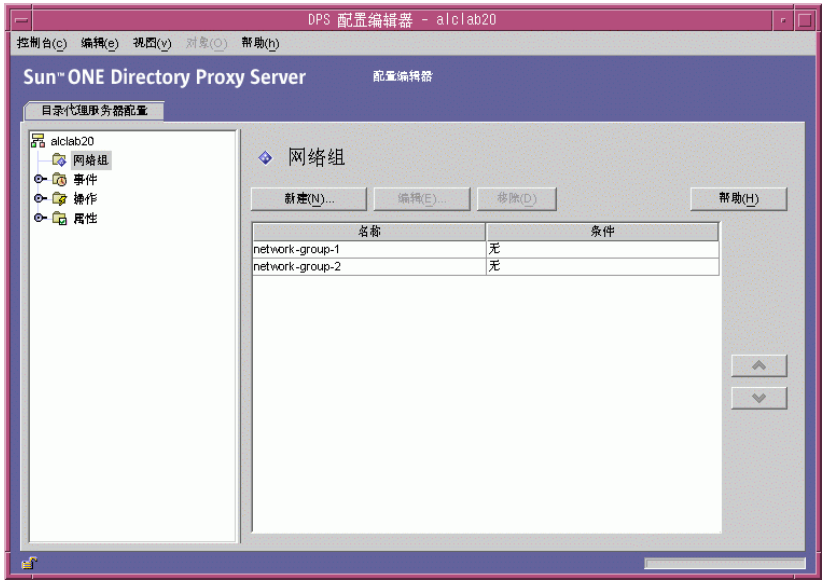
请注意，创建网络组时您有机会指定各种条件。本节所提供的说明按其在用户界面中出现的顺序显示了所有这些条件，并根据您的判断设置组的相应条件。

➤ 在 Directory Proxy Server 中创建网络组

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

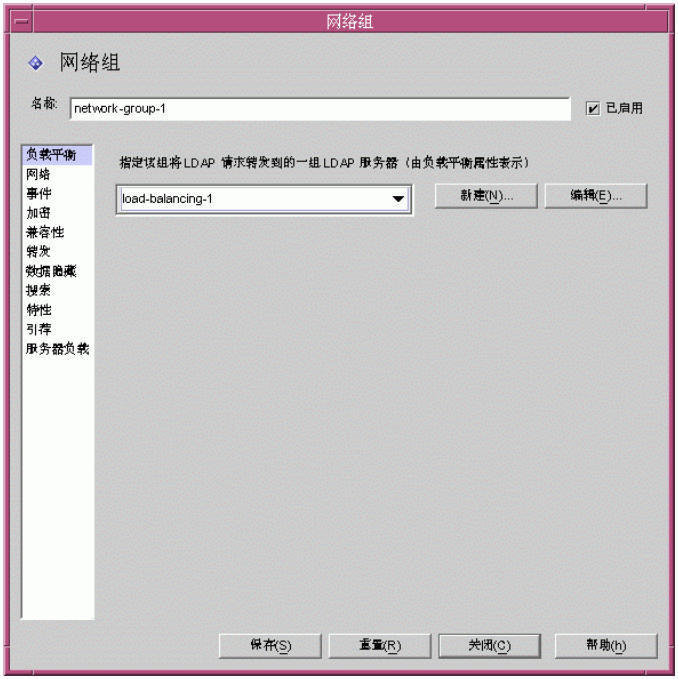
2. 在导航树中，选择“网络组”。

   右侧窗格将显示现有组的列表。



3. 单击 “新建”。

   “网络组”窗口随即出现。



4. 在 “名称”字段中，键入组名称。名称必须是唯一的字母数字字符串。

5. 请确保选中了 “已启用”选项；缺省情况下，该选项处于选中状态。对于是 Directory Proxy Server 配置一部分的组而言，必须选中此选项。取消选择此选项将禁用配置中的组。

6. 如果需要，可从下拉菜单中指定负载平衡属性。该属性会识别此组将 LDAP 请求转发到的 LDAP 服务器组，以便使用 “负载平衡”属性处理客户机的请求。相关的下拉列表显示 “负载平衡”属性的现有对象，如第 124 页上的 “负载平衡属性”中所述。选择相应的对象。缺省情况下，不选中任何对象 （< 无 >）。如果没有对象，则可通过单击 “新建”按钮立即创建一个。

   新建。显示新建 “负载平衡”属性的对话框。

   编辑。显示编辑现有 “负载平衡”属性的对话框。

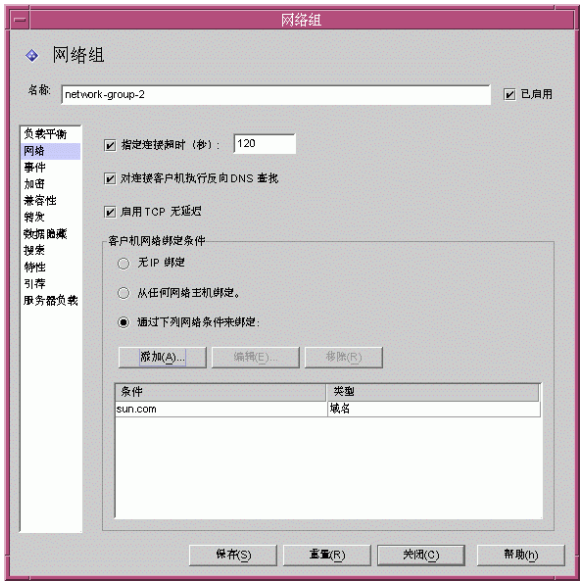
7. 要指定组的网络条件以便排序或过滤请求，请选择左侧框中的 “网络”。然后参考屏幕上的元素说明指定相应的网络值，如下所示：

   指定连接器超时值。缺省情况下，不显示值，这也意味着连接未超时。

   对连接客户机启用反向 DNS 查找。

   选择 “启用 TCP 无延迟”。

   定义 “客户机网络绑定条件”。



   该屏幕上的元素说明如下：

   指定连接超时。选择此框以输入一个客户机不活动时间段，经过这段时间后，Directory Proxy Server 可以关闭到该客户机的连接。该值必须为数字 （以秒为单位），通常为 120 或更大。缺省情况下，不显示值，这也意味着连接未超时。请注意，如果未启用 TCP 保活，则必须具有此特性才能防止 Directory Proxy Server 不被断开的客户机连接阻塞。

   对连接客户机执行反向 DNS 查找。缺省情况下，该选项处于启用状态。如果禁用了 “反向 DNS 查找”，则 Directory Proxy Server 将不执行反向 DNS 查找来查找连接客户机的域名。禁用 “反向 DNS 查找”有时可以大大提高 Directory Proxy Server 的性能。如果已经将域名或域名后缀用作 “客户机网络绑定条件”中的值，则绝不能禁用 “反向 DNS 查找”，否则 Directory Proxy Server 将无法正常工作。必须配置 DNS 才能返回完整的主机名以查找查询。

   启用 TCP 无延迟。缺省情况下，该选项处于启用状态。如果禁用该选项，则

Directory Proxy Server 将对服务器自身与此组中的客户机之间的连接禁用 Nagle 算法。只有 Directory Proxy Server 和客户机之间的网络带宽很小时，才应禁用 “TCP 无延迟”；然而，这可能导致性能大大降低。

客户机网络绑定条件。使用此部分可以指定哪些客户机可以在本网络组中进行绑定。

无 IP 绑定。只有当客户机绑定到组时进行切换的情况下，才选择该选项。缺省情况下，此选项处于选中状态。如果组仅用于客户机绑定时进行切换，则取消选中该选项。

从任何网络主机绑定。如果允许所有主机与此网络组进行绑定，则选择该选项。

通过下列网络条件来绑定。选择该选项可指定与网络组匹配的主机域名或 IP 地址；此时，组必须指定将要绑定到的主机域名或 IP 地址。

添加。显示添加网络条件的对话框。有下面四个选项：“域名”、“IP 地址”、“IP 地址和位”和 “IP 地址和 Quad”。

编辑。显示编辑网络条件的对话框。

移除。显示移除网络条件的对话框。

域名。指定可以绑定到网络组的客户机的域名后缀或全名，例如，`foo.sun.com`。请注意，缺省情况下， Directory Proxy Server 不假定任何域名后缀；因此必须提供完整域名。带有前导句点的域名后缀 （例如， `.sun.com`）将使其域名以该后缀结尾的所有主机都匹配。

另外还要注意，如果域名后缀规则用于识别客户机，那么请确保将 DNS 设置为返回 DNS 查询的全限定名称。如果返回短名称，则此功能将不起作用。

IP 地址。指定以小数点形式表示的单个 IP 地址，例如， `198.214.11.1`。

IP 地址和位。指定以 < 网络号 >/< 掩码位 > 形式表示的 IP 网络掩码。例如，`198.241.11.0/24`。前半部是网络号，后半部表示匹配所必需的网络号的位数。

IP 地址和 Quad。指定以小数点 Quad 对形式表示的 IP 网络掩码，例如，`198.241.11.0/255.255.255.128`。前半部是网络号，后半部表示匹配所必需的网络号的位数。例如， `198.214.11.0/255.255.255.128` 将与 IP 地址为 `198.214.11.63` 的主机匹配，但不匹配 IP 地址为 `198.214.11.191` 的主机。

请注意，使用域名或域名后缀要求启用 “对连接客户机执行反向 DNS 查找”。

8. 要将事件驱动的操作与组关联 （例如，将客户机从一个组更改到另一个组），请选择左侧框中的 “事件”并在右侧框中指定相应的值。

该屏幕上的元素说明如下：

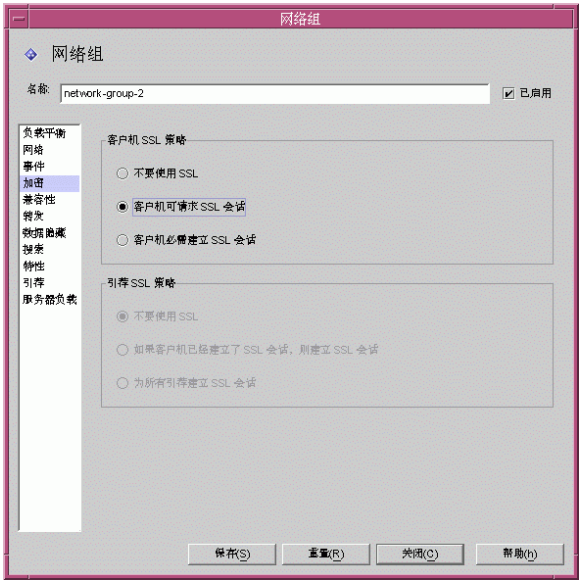
绑定后续操作。下拉列表显示了 OnBindSuccess 事件的现有对象，如第 134 页上的 “创建 OnBindSuccess 事件对象”中所述。选择客户机成功完成绑定操作后将执行的对象名称。缺省情况下，不选中任何对象 （< 无 >）。如果没有对象，则可通过单击 “新建”按钮立即创建。

SSL 后续操作。下拉列表显示了 OnSSLEstablished 事件的现有对象，如第 137 页上的 “创建 OnSSLEstablished 事件对象”中所述。选择客户机成功建立 SSL 会话后将执行的对象名称。如果没有对象，则可通过单击 “新建”按钮立即创建。

编辑。显示编辑事件行为的对话框。

新建。显示新建事件的对话框。

9. 要指定组的加密条件 （例如，要指定客户机是否可以请求 SSL 会话），请选择左侧框中的 “加密”并在右侧框中指定相应的值。



该屏幕上的元素说明如下：

客户机 SSL 策略。配置客户机 SSL 策略。

不要使用 SSL。如果不希望使用 SSL 加密，则选择此选项。

客户机可请求 SSL 会话。如果组中的客户机将通过请求 SSL 来建立 SSL 会话，则选择此选项。

客户机必须建立 SSL 会话。如果组中的客户机必须建立 SSL 会话后才能执行任意操作，则选择此选项。

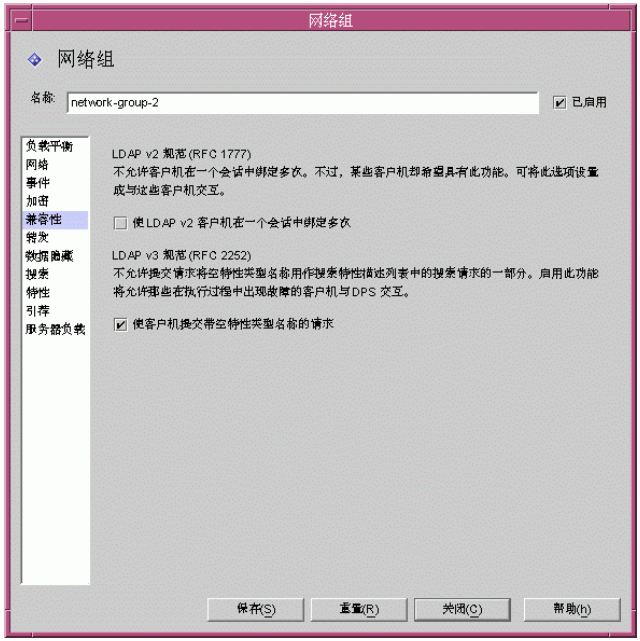
引荐 SSL 策略。跟随引荐时配置 SSL 策略。

不要使用 SSL。如果不希望使用 SSL 加密，则选择此选项。

如果客户机已经建立了 SSL 会话，则建立 SSL 会话。如果启用了该选项，并且如果客户机已经与 Directory Proxy Server 建立了 SSL 会话，则 Directory Proxy Server 将只启动该组客户机的 SSL。

为所有引荐建立 SSL 会话。对于引荐而言，如果 Directory Proxy Server 将在转发操作前启动 SSL 会话，则启用此选项。

10. 要指定组的兼容性条件 （例如，允许客户机在一次会话中绑定多次），请选择左侧框中的 “兼容性”并在右侧框中指定相应的值。



该屏幕上的元素说明如下：

使 LDAP v2 客户机在一个会话中绑定多次。 LDAP v2 规范 (RFC 1777) 不允许客户机在一次会话中绑定多次。然而，某些客户机却希望具有此功能。如果希望该组允许客户机提交带有特性请求列表中的一个或多个特性 （作为 NULL）的搜索请求，则选择该选项。该兼容性功能允许 Directory Proxy Server 与某些中断的基于 JAVA 的客户机进行互操作。请注意，特性请求列表中的 NULL 特性名称与 LDAP 协议相违背。缺省情况下，此选项设置为 TRUE。

使客户机提交带空特性类型名称的请求。如果即使请求未识别其特性类型名，也希望组允许客户机提交这些请求，则选择此选项。

11. 要指定组的请求转发条件，请选择左侧框中的 “转发”并在右侧框中指定相应的值。

    当 Directory Proxy Server 已经从客户机接受了连接并匹配了某个组后，它将等待客户机发送 LDAP 操作。 Directory Proxy Server 使用 “客户机 DN”、“允许匿名绑定”、“允许简单绑定”和 “允许 SASL 绑定”来决定是将绑定请求传递给服务器，还是拒绝绑定请求并关闭客户机的连接。

    如果客户机的绑定通过了已启用的测试，则 Directory Proxy Server 就会将其转发给服务器。如果服务器接受绑定，则建立连接。然而，如果服务器返回了绑定请求的错误提示，则 Directory Proxy Server 会将该错误提示转发给客户机，而且如果客户机正在使用 LDAPv2，则将关闭到客户机的连接。

“绑定”选项卡中的元素说明如下：

允许所有客户机。缺省情况下，该选项处于启用状态，即允许所有客户机的访问。

拒绝具有非从属性 DN 的客户机。如果希望组检查识别名 (DN)，则选择此选项。在其绑定中提供了非从属于该指定 DN 的识别名的任何客户机都将被拒绝。使用 “浏览”按钮浏览 LDAP 目录以便构造 DN。

允许匿名绑定。缺省情况下，该选项处于启用状态，此时即使客户机未提供口令也允许绑定。禁用该选项将禁止匿名绑定。

允许简单绑定。缺省情况下，该选项处于启用状态，即允许客户机提供明文口令。禁用该选项将禁止明文口令验证的绑定请求。

允许 SASL 绑定。缺省情况下，该选项处于启用状态，它指定允许 SASL 绑定。禁用该选项将禁止 SASL 验证。

12. 选择 “操作”选项卡并指定允许转发的操作。

缺省情况下，Directory Proxy Server 将转发搜索和比较请求。Directory Proxy Server 还识别非绑定请求并关闭到 LDAP 服务器的连接。

“操作”选项卡中的元素说明如下：

允许搜索操作。缺省情况下，该选项处于启用状态。禁用该选项可防止 Directory Proxy Server 将搜索请求转发给服务器。

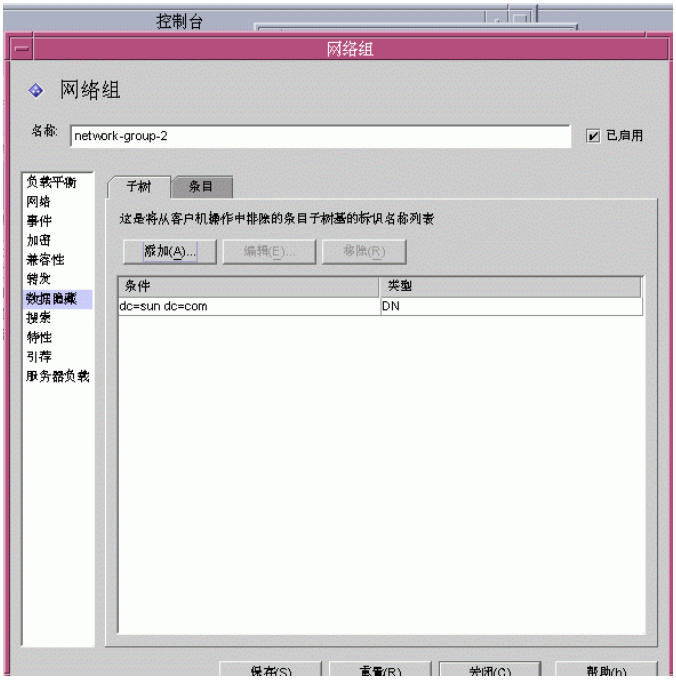
允许比较操作。缺省情况下，该选项处于启用状态。禁用该选项可防止 Directory Proxy Server 将比较请求转发给该服务器。

允许添加、删除、修改、修改 DN 和扩展操作。缺省情况下， Directory Proxy Server 不转发添加、修改、删除、修改 DN 或扩展操作请求。要允许转发这些操作，请启用允许的相应操作。

请注意，如果希望客户机可以协商 “启动 TLS”，则必须启用 “允许扩展操作”。

13. 要指定组的数据隐藏条件，请选择左侧框中的 “数据隐藏”并在右侧框中指定相应的值。

    使用 “子树”选项卡指定要隐藏的目录树部分，使用 “条目”选项卡指定要隐藏的条目或特性。



“子树”选项卡中的元素说明如下：

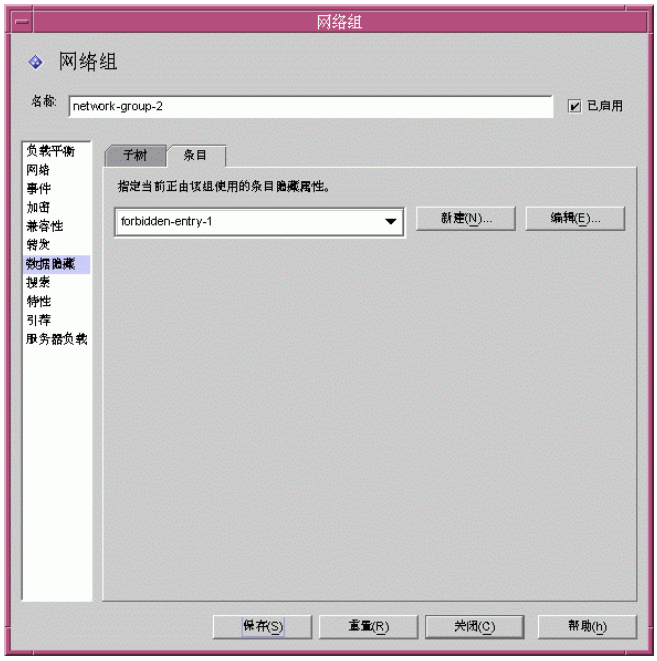
隐藏条目子树。请求禁止的子树条目或该子树下条目的操作将被拒绝，并返回访问权限不够的错误。匹配搜索过滤并且位于禁止的子树内的条目将被丢弃。请注意，该选项不会从作为结果一部分返回的条目中移除那些其值位于此子树下的 DN 语法特性。

添加。显示一个对话框，用于将识别名添加到要排除的条目子树基列表中。如果在网络组中不存在识别名，则缺省允许访问该目录中的所有条目。该列表中的条目具有 dn 语法。

编辑。显示编辑识别名的对话框。

移除。移除该列表中的识别名。

14. 选择 “条目”选项卡并指定要隐藏的条目或特性。



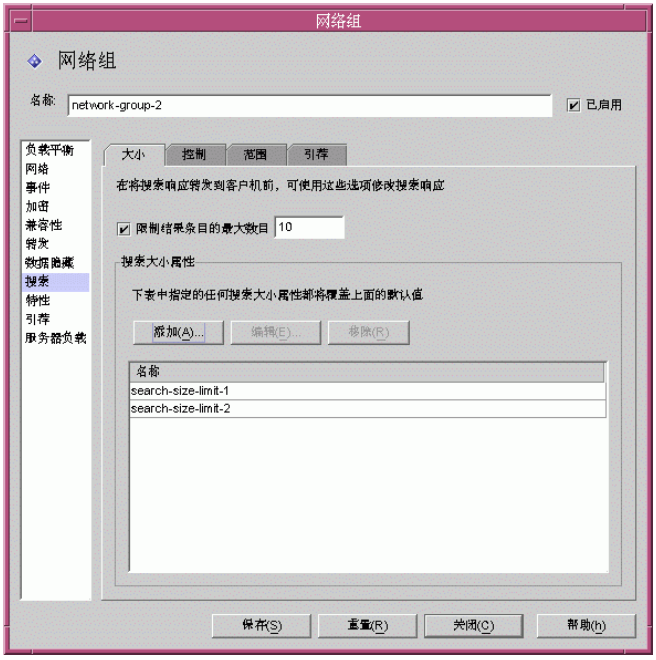
“条目”选项卡中的元素说明如下：

指定当前正由该组使用的条目隐藏属性。下拉列表显示了 “禁止的条目”属性的现有对象，如第 115 页上的 “创建禁止的条目属性对象”中所述。选择对象的名称。缺省情况下，不选中任何对象 （< 无 >）。如果没有对象，则可通过单击 “新建”按钮立即创建。

新建。显示新建 “禁止的条目”属性的对话框。

编辑。显示编辑现有 “禁止的条目”属性的对话框。

15. 要指定组的搜索特性，请选择左侧框中的 “搜索”并在右侧框中指定相应的值。



“大小”选项卡中的元素说明如下：

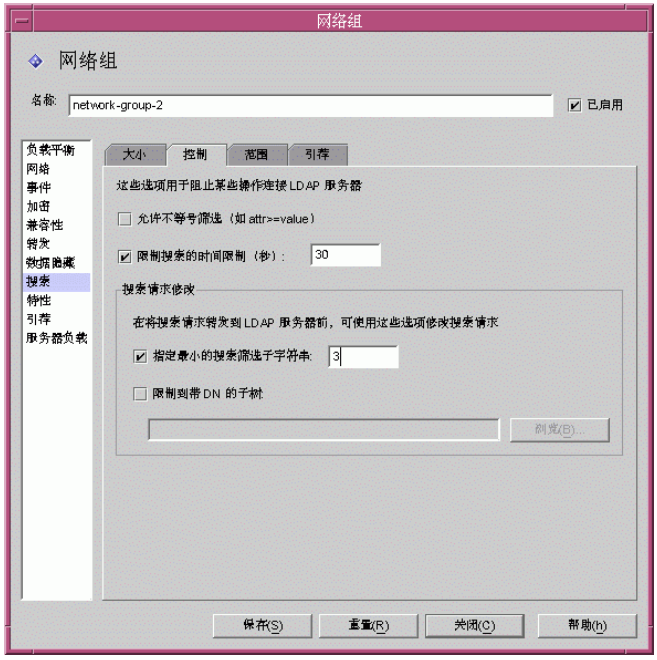
限制结果条目的最大数目。启用该选项可以指定单个搜索操作一次可返回到客户机的最大结果条目数。该值可以是任何大于零的数，如果达到该值，将向客户机发送 `administrativeLimitExceeded` 错误，并放弃后续条目。如果禁用该属性，则缺省不放弃条目。

添加。显示添加 “搜索大小限制”属性的对话框。有关详细信息，请参阅第 128 页上的 “创建搜索大小限制属性对象”。

编辑。显示编辑 “搜索大小限制”属性的对话框。

移除。显示移除 “搜索大小限制”属性的对话框。（此操作在不显示对话框的情况下从组中移除属性。）

16. 选择 “控制”选项卡并指定控制搜索过滤的条件。



“控制”选项卡中的元素说明如下：

允许不等号筛选。缺省情况下，该选项处于启用状态。允许不等号过滤将指定是否允许客户机请求包含不等号过滤 (`attr>=value`) 和 (`attr<=value`) 的搜索。如果网络组不允许执行不等号搜索，则禁用该选项。

限制搜索的时间限制。启用此选项并为网络组输入一个值 （以秒为单位），以指定搜索操作的最大时间限制 （以秒为单位）。如果客户机指定的时间限制大于此选项中给定的值，则为此网络组指定的值将覆盖客户机的请求。缺省情况下，该选项处于禁用状态，网络组将允许客户机设置任何时间限制，包括无限制。

指定最小的搜索筛选子字符串。启用该选项并输入一个值，以便指定搜索过滤中子字符串的最小允许长度。该值为大于 1 的数。如果禁用该选项，则搜索过滤中缺省允许使用任何大小的子字符串。如果希望限制由 Web Robot 执行的搜索种类，则应在网络组中启用该选项。例如，值为 2 时将阻止像 (`cn=A*`) 这样的搜索。

注 此特性不影响存在过滤 (attrname=*)。要禁止某些存在过滤，请使用禁止比较配置。

限制到带 DN 的子树。启用该选项并指定所有操作的子树基。该选项具有 dn 语法。如果禁用该选项，则对最小基没有限制。

其目标条目位于最小基条目或最小基条目之下的操作将不受此选项的影响。如果目标条目高于最小基条目，并且操作为子树搜索，则将查询发送到服务器之前将重写查询，以便将此目标条目更改为最小基。如果目标条目没有位于最小基之下或者位于最小基之上，则请求将被拒绝，并返回无此对象错误。

例如，如果将 “限制到带 DN 的子树”设置为：

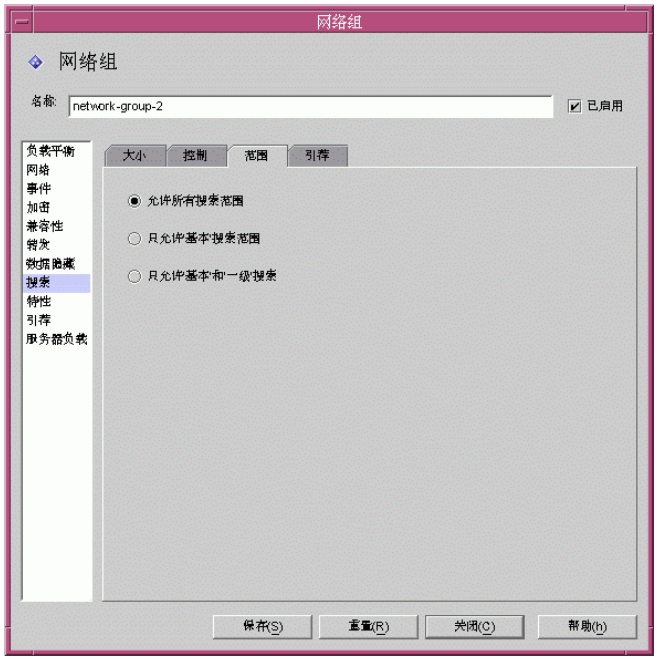
o=sun, st=California, c=US

并且收到了 `st=California, c=US` 子树搜索，则搜索将被重写，服务器将执行如下子树搜索：

o=sun, st=California, c=US

浏览。显示一个对话框，用于帮助构造有效的 DN。

17. 选择 “范围”选项卡并指定搜索范围 （客户机可在搜索请求中指定的范围）。



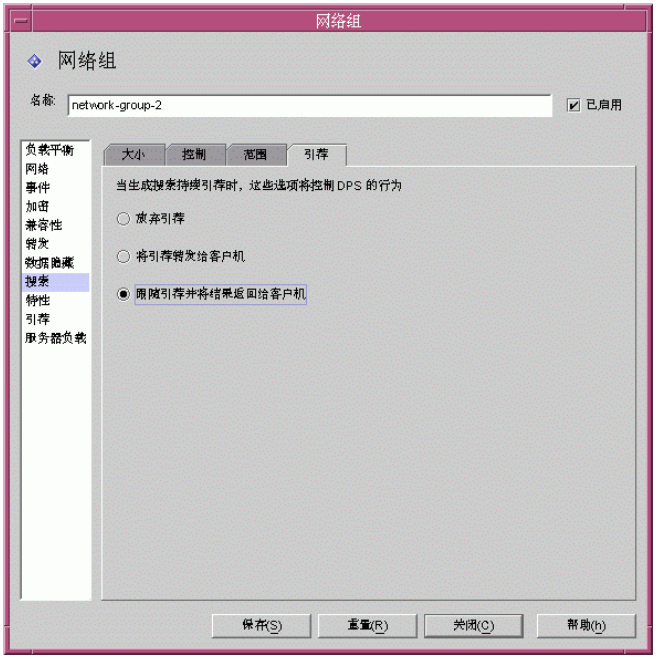
“范围”选项卡中的元素说明如下：

允许所有搜索范围。缺省情况下，该选项处于启用状态，允许客户机进行全范围的搜索。

只允许 ‘基本’搜索范围。启用该选项将只允许基本搜索范围。

只允许 ‘基本’和 ‘一级’搜索。启用该选项将只允许基本和一级搜索。

18. 选择 “引荐”选项卡并指定搜索过程中生成搜索持续引荐后将完成的操作。



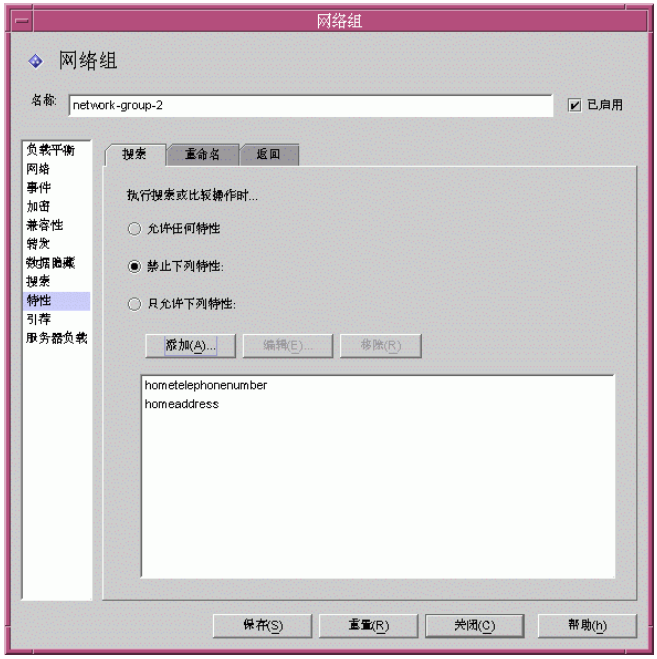
“引荐”选项卡中的元素说明如下：

放弃引荐。缺省情况下，该选项处于启用状态，即在搜索过程中如果生成引荐，则将其放弃。

将引荐转发给客户机。启用该选项将只转发搜索持续引荐。

跟随引荐并将结果返回给客户机。启用该选项将跟随并返回搜索持续引荐的结果。搜索持续引荐是一种特殊的引荐，查询的原始目录服务器通过它已经满足部分查询，但该目录服务器又引荐了其他目录服务器，其中有更多的数据满足查询。该选项可用于隐藏目录信息树中命名环境由其他 LDAP 服务器控制的部分。它还阻止客户机查找该服务器运行的网络地址和端口。

19. 要指定组的特性条件，请选择左侧框中的 “特性”并在右侧框中指定相应的值。



“搜索”选项卡中的元素说明如下：

该选项卡用于阻止某些种类的搜索和比较操作连接到 LDAP 服务器。如果客户机的请求属于此限制，则 Directory Proxy Server 将向客户机返回访问权限不够的错误。

允许任何特性。缺省情况下，该选项处于启用状态，可允许所有特性用于搜索过滤和比较。

禁止下列特性。启用该选项指定客户机无法在搜索过滤或比较请求中使用的特性名称。

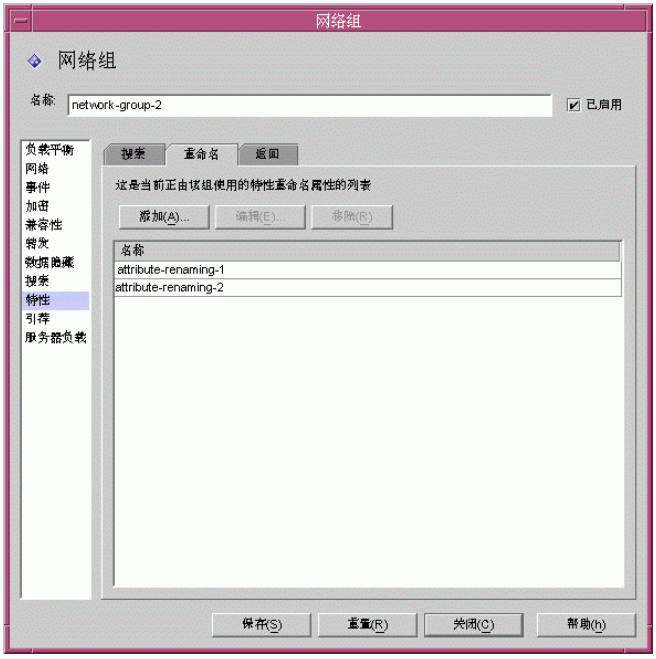
只允许下列特性。启用该选项指定可用在搜索过滤或比较请求中的特性名称。如果网络组表中有一个或多个特性值，而且比较与其中的特性值都不匹配，则请求将被 Directory Proxy Server 拒绝。如果网络组表中没有任何特性，并且某个特性与任何特性都不匹配，则该特性可被客户机使用。例如，如果希望客户机只可以搜索 cn、 dn 和 mail 特性，则可将这些特性添加到表中。

添加。显示一个对话框，允许将特性添加到该表中。必须指定是禁止还是允许这些特性。

编辑。显示一个对话框，用于编辑表中选定的特性。

移除。移除表中的特性。

20. 选择 “重命名”选项卡并指定特性重命名的规则。



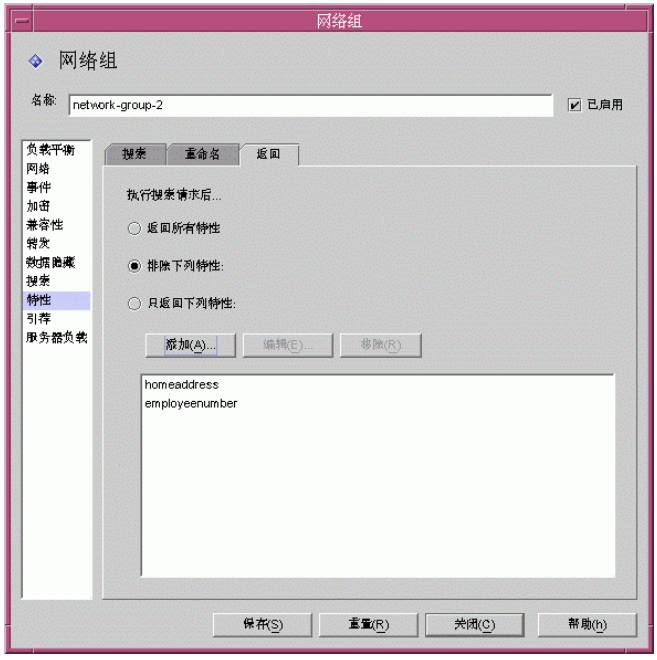
“重命名”选项卡中的元素说明如下：

添加。显示一个对话框，从中将一个或多个现有特性重命名属性添加到下列由该网络组使用的表中。（请参阅第 113 页上的 “创建特性重命名属性对象”。）

编辑。显示一个对话框，从中编辑选定的特性重命名属性。

移除。从表中移除特性重命名属性。

21. 选择 “返回”选项卡并指定在将服务器返回的搜索结果转发给客户机前，应用到这些搜索结果的限制。



“返回”选项卡中的元素说明如下：

返回所有特性。缺省情况下，该选项处于启用状态，允许返回所有特性。

排除下列特性。启用该选项以指定将从搜索结果条目中排除的特性名称。

只返回下列特性。启用该选项以指定从搜索结果中返回的特性名称 （如果存在）。

如果作为搜索结果一部分的返回特性不存在于 “只返回下列特性”表中，则不返回这些特性。如果表为空并且它们不在 “排除下列特性”表中，则返回这些特性。

添加。显示一个对话框，允许将特性添加到该表中。必须在上面指定是禁止还是允许这些特性。

编辑。显示一个对话框，用于编辑表中选定的特性。

移除。移除表中的特性。

22. 要指定组的引荐（例如，该组是将转发、跟随还是放弃服务器返回的引荐），请选择左侧框中的“引荐”并在右侧框中指定相应的值。

该屏幕上的元素说明如下：

放弃引荐。如果网络组将放弃服务器返回的所有引荐，则启用此选项。

将引荐转发到客户机。缺省情况下，该选项处于启用状态，将转发由服务器返回的引荐。

跟随引荐并将结果返回给客户机。如果网络组将转发服务器返回的引荐，并将结果返回给客户机，则启用此选项。

绑定策略。当操作被引荐而且正在跟随引荐时，此选项控制绑定策略。

请注意，对于使用 SASL 机制绑定的客户机， Directory Proxy Server 无法重复进行绑定。因此，如果指定了“必选”而且客户机使用了 SASL 机制进行绑定，则此引荐操作将被拒绝。

始终。如果 Directory Proxy Server 跟随连接到此网络组的客户机引荐时应始终匿名绑定，则选择此选项。

任意。如果客户机使用基于口令的绑定时网络组就应使用简单绑定，否则网络组使用匿名绑定，则选择此选项。这是缺省设置。

必选。如果客户机使用的不是基于口令的绑定时网络组应拒绝引荐的操作，则

选择此选项。

指定每个操作最大的引荐数。请输入大于或等于零的整数。这将限制单个操作将跟随的最大引荐数。缺省值为 15。值为零时表示不受任何限制。

引荐 SSL 策略。要启用 “引荐 SSL 策略面板”，必须启用加密视图上的 “SSL 可用”选项。

如果客户机已经建立了 SSL 会话，则建立 SSL 会话。如果客户机已经与 Directory Proxy Server 建立 SSL 会话时网络组将只启动 SSL，则启用此选项。这是缺省设置。

为所有引荐建立 SSL 会话。对于一个引荐，如果组将在转发操作之前启动 SSL 会话，则启用 “为所有引荐建立 SSL 会话”。

23. 要指定组的服务器负载条件，请选择左侧框中的 “服务器负载”并在右侧框中指定相应的值。

该屏幕上的元素说明如下：

每个连接的同时操作数。选择此选项以限制 Directory Proxy Server 处理该组中每个连接的同时操作数。该值为大于零的整数。如果该特性不存在，则不强制实施任何限制。例如，如果将该值设置为 1，则将强制该组中的所有客户机执行同步 LDAP 操作。除了放弃操作的请求外，其他同时请求都将失败，并出现“服务器忙”错误。

每个连接的总操作数。选择此选项以限制 Directory Proxy Server 允许该组中每个连接的操作总数。该值为大于零的整数。如果客户机超过了组中一个连接允许的最大操作数，则该连接将由 Directory Proxy Server 关闭。如果该特性不存在，则表示不设置任何限制。

到该组的同时连接数。选择此选项以限制到该网络组的同时操作数，并指定该操作数。

每个 IP 地址的同时连接数。选择此选项以限制客户机从单个 IP 地址获得的同时连接数。缺省情况下允许任意的连接数。

24. 单击 “保存” 创建该组。

    Directory Proxy Server 配置被修改，并提示重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

25. 重复步骤 3 到步骤 24 以创建所有其他组。

26. 转到 “网络组” 窗口 （请参阅步骤 2）并按优先级对组进行相应地排序。

27. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

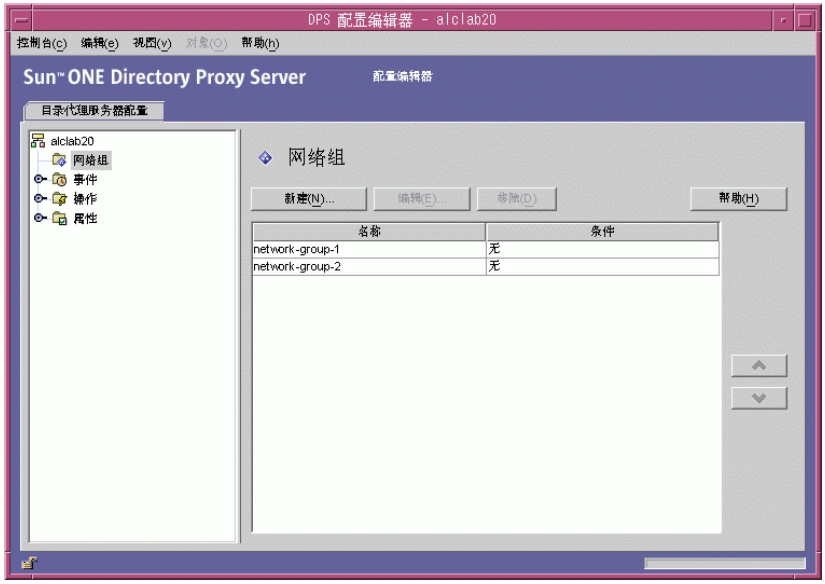
修改组

➤ **修改组**

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

2. 在导航树中选择 “网络组”。

   右侧窗格将显示现有组的列表。



3. 在列表中，选择要修改的组并单击 “编辑”。

4. 进行所需的修改。

5. 单击 “保存”以保存更改。

   Directory Proxy Server 配置被修改，并提示重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

6. 重复步骤 3 到步骤 5 以修改所有其他组。

7. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

删除组

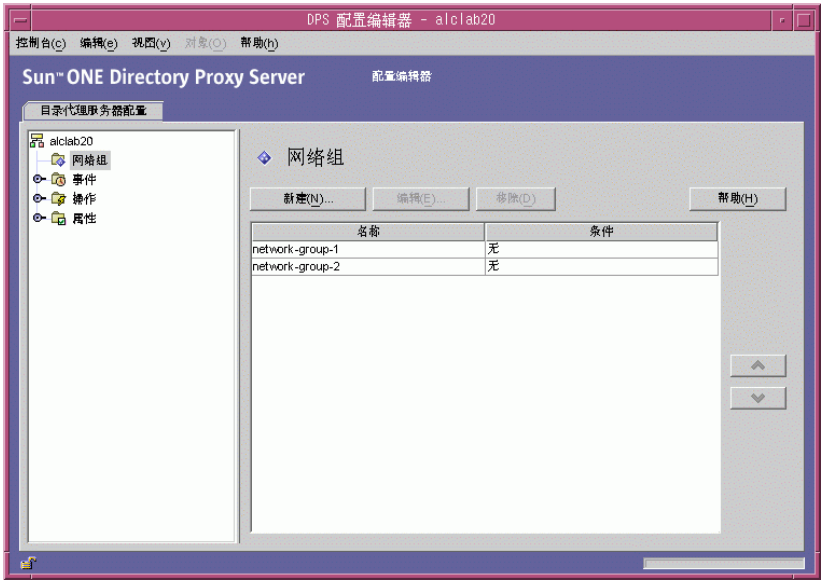
可以从 Directory Proxy Server 配置中删除任何不需要的网络组。

➤ **删除组**

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

2. 在导航树中选择 “网络组”。

   右侧窗格将显示现有组的列表。



3. 在列表中选择要删除的组，然后单击 “移除”。

4. 确认操作。

   删除的组名现已从列表中删除。 Directory Proxy Server 配置被修改，并提示重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

5. 重复步骤 3 和步骤 4 以删除任何其他组。

6. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

第 8 章

定义和管理属性对象

如本书的部署一章所述， Directory Proxy Server 可以作为 *LDAP 访问路由器*使用，帮助您保护专用目录信息免受未经授权的访问，同时使您可以安全地发布公共信息。服务器可以处理数以千计的 LDAP 客户机请求，并可以在将每一个请求路由到目录服务器之前对其应用精细的访问控制规则和协议过滤规则。

Directory Proxy Server 中的属性对象使您能够指定 LDAP 客户机必须遵循的专门限制。然后，您可以将这些属性包括在需要应用这些限制的其他条目中。本章概述了每一个属性，同时介绍如何使用 Directory Proxy Server 配置编辑器控制台创建属性对象。

本章包含以下几个部分：

特性重命名属性

通常， LDAP 目录包含有关组织内的人员以及网络资源之类的实体信息。对于每个实体，目录中都有一个条目。目录中的所有条目都通过其识别名 (DN) 来标识，并用一组特性及其值来表示。每个条目都有一个对象类别特性，该特性指定条目所描述的对象的类型，并定义条目所包含的其他特性的集合。每个特性都描述条目的一个特征。例如，条目可以属于对象类别 `organizationalPerson`，这表示该条目代表特定组织中的某位人员。此对象类允许 `givenname` 和 `telephoneNumber` 特性。向这些特性指定的值给出了该条目所代表的人员的姓名和电话号码。

在许多目录部署中， LDAP 客户机端定义的特性并不映射到服务器端定义的特性。为了便于这种设置中的客户机和服务器之间的通信， Directory Proxy Server 支持特性的重命名，即， Directory Proxy Server 可以在将客户机查询传递到目录服务器之前将其中的特性重命名为目录服务器理解的形式，并且在将服务器响应传递给客户机之前也执行相同的操作。

图 8-1 说明了如何将 Directory Proxy Server 的特性重命名功能用于架构映射。

图 8-1 使用特性重命名属性映射架构

注，在电子邮件客户程序中，人员的姓氏是名为 “surname”的特性的值，而在 LDAP 服务器中，姓氏是由名为 “sn”的特性指定的。当 Directory Proxy Server 映射这两个特性时，只有特性名称受影响，而特性值保持不变。

可以使用特性重命名属性来定义用于控制客户机和服务器特性重命名的规则。您可以指定需要映射到相应服务器特性的客户机特性的名称 （反之亦然）。这样，如果客户机请求中包含服务器未知的特性名称，那么 Directory Proxy Server 就能够将该名称映射为服务器已知的名称，从而帮助客户机与服务器进行通信。同样，当服务器发回响应时， Directory Proxy Server 会将任何客户机未知的特性转换为已知形式。

下面的一节说明如何从 Directory Proxy Server 配置编辑器控制台为特性重命名属性创建对象。

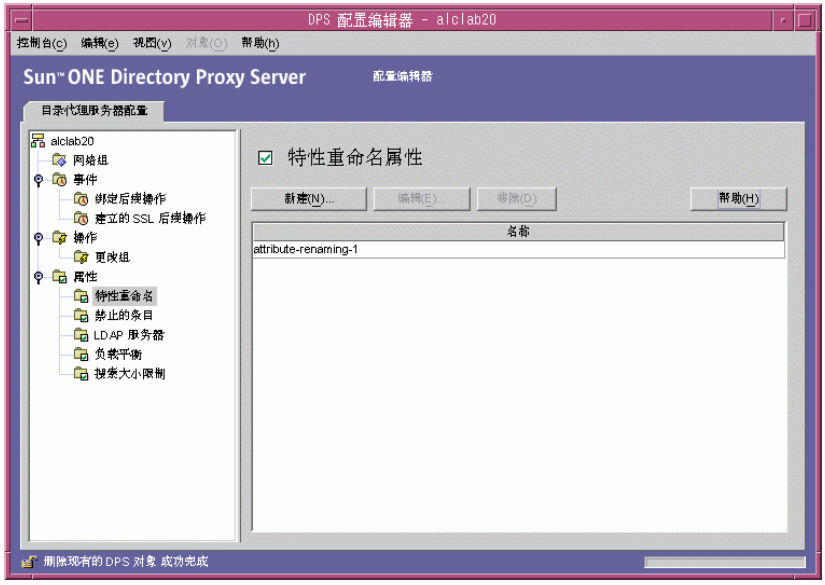
注 您为特性重命名属性创建的任何对象都必须同时具有服务器和客户机特性。否则， Directory Proxy Server 将无法启动。

创建特性重命名属性对象

➤ **识别要重命名的客户机和服务器特性**

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。
2. 在导航树中，展开 “属性”节点，然后选择 “特性重命名”。

   右侧窗格显示特性重命名属性的现有对象的列表。



3. 单击 “新建”。

   “特性重命名属性”窗口随即出现。

4. 在 “名称”字段类型中，键入属性对象的名称。名称必须是唯一的字母数字字符串。

注 特性名称只能由 7 位字符组成。

5. 在其余的字段中，指明用于映射的特性：

   特性重命名值可以写成由句点分隔的十进制数；例如， `2.5.4.10`。特性重命名值还可以为特性类型指派一个或多个文本名称。这些名称必须以字母开头，并且只能包含 ASCII 字母、数字字符和连字符。该值区分大小写。

   服务器已知的特性名称。输入值以指定服务器已知的特性名称。

   客户机已知的特性名称。输入值以指定客户机已知的特性名称。

   如果客户机请求中包含由 “客户机已知的特性名称”指定的特性名称，则可将其转换成 “服务器已知的特性名称”的值。同样，如果服务器发送的结果中包含 “服务器已知的特性名称”中指定的特性名称，则可将其转换成 “客户机已知的特性名称”的值。

6. 单击 “保存”以创建对象。

   Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

7. 重复步骤 3 到步骤 6 以创建任何其他对象。

8. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

禁止的条目属性

由于各种原因， LDAP 目录中的某些条目 （或代表这些条目的特性）需要对 LDAP 客户机隐藏。例如，如果目录中包含所有雇员的条目，并且这些条目中的每一个条目都包含雇员数据的相关特性，例如姓名、电子邮件地址、部门、办公地点、办公室电话号码以及家庭电话号码，那么您可以隐藏所有雇员的家庭电话号码，使其对客户机不可见。

禁止的条目是指 LDAP 目录中需要对 LDAP 客户机隐藏的条目。为便于这种设置中客户机和目录服务器之间的通信， Directory Proxy Server 支持禁止的条目，即， Directory Proxy Server 可以对 LDAP 客户机隐藏 LDAP 条目和这些条目的特性。

可以使用 “禁止的条目”属性来定义规则以控制目录条目及其特性的隐藏。此属性使您能够以多种方式指定需要隐藏的条目或条目特性的列表。例如，您可以指定：

- 您希望隐藏的条目的 DN 或这些条目中的特性。
- 由您希望隐藏的条目的 DN 或这些条目中的特性组成的正则表达式 （例如， `.*OU=INTERNAL.*`）。
- 条目的特性名称 / 值对 （例如， `secret:yes`）。如果某个条目的特性名称 / 值对与任一指定的特性名称 / 值对匹配，则隐藏该条目或其部分内容。

下面一节介绍如何从 Directory Proxy Server 配置编辑器控制台创建禁止的条目属性对象。

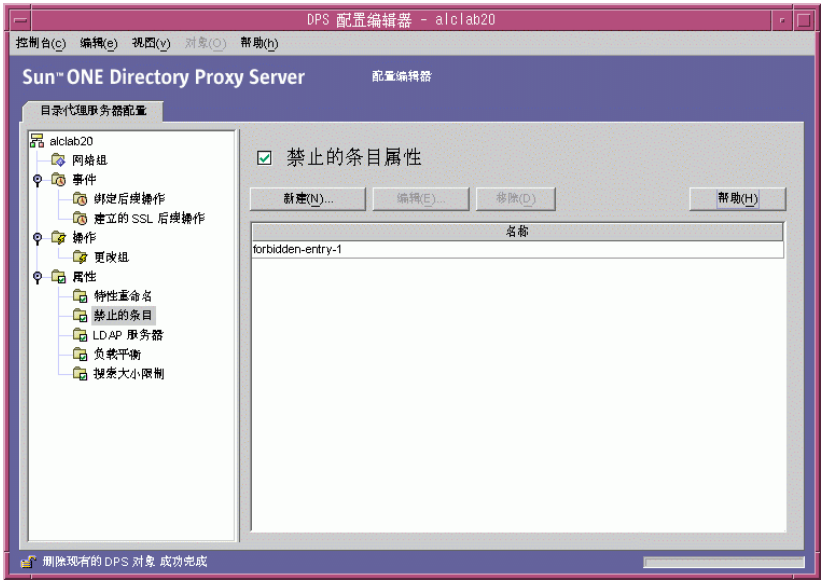
创建禁止的条目属性对象

➤ **识别要对客户机隐藏的条目或特性**

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

2. 在导航树中，展开 “属性”节点，然后选择 “禁止的条目”。

   右侧窗格显示禁止的条目属性的现有对象列表。



3. 单击 “新建”。

   “禁止的条目属性”窗口随即出现。

4. 在 “名称”字段中，键入属性对象的名称。名称必须是唯一的字母数字字符串。

5. 在 “条目匹配”选项卡中，指定相应的值；该选项卡显示此属性的名称以及要隐藏的 LDAP 条目等设置。

   添加。显示一个菜单，用于添加隐藏 LDAP 条目的条件。条件可以为下列类型：精确 DN、正则 DN 表达式或特性 / 值对。可在一个条目中键入或浏览现有条目的目录信息树。

   精确 DN。显示一个对话框，从中可输入要隐藏的条目的 DN。

   正则 DN 表达式。显示一个对话框，从中可以输入要隐藏的条目的正则 DN 表达式。应该以标准形式来指定 DN 正则表达式，也就是说， RDN 部分和等号 "=" 之间没有空格，特性名称和值必须都是大写字母。

   例如，要将任一 DN 与 "ou=internal" 的 RDN 部分匹配，您必须指定如下内容：

   .*OU=INTERNAL.*

   如果 “特性过滤”选项卡包含要被包括的特性名称，当某个特性与其中所列的内容之一不匹配时，则不返回此特性。如果 LDAP 条目中的特性与 “特性过滤”选项卡中要排除的任何特性都不匹配，则返回该条目。

   下面这本书可以用作正则表达式的参考资料：*Mastering Regular Expressions*，Friedl 和 Oram 著， O'Reilly 出版， ISBN：1565922573。

   特性 / 值对。显示用于指定特性名称 / 值对的对话框。如果某个条目的特性名称 / 值对与任一指定的特性名称 / 值对匹配，则隐藏该条目或其部分内容。

   例如，如果您希望限定具有 "ou=internal" 或 "secret=yes" 的所有条目作为其特性之一，那么您可以指定下列内容：特性为 "ou" 并且值为 "internal"。

   编辑。显示一个对话框，用于编辑表中当前选择的条目。

   移除。移除表中当前选择的条目。

6. 选择 “特性筛选”选项卡，并指定相应的值。

该选项卡包含允许要排除或要特别包含的某些特性的设置：

排除整个条目。选择此选项以表明不执行任何特性过滤，而且将隐藏整个条目。

只从条目中排除下列特性。选择此选项以表明该表包含要从条目 （与以上任一规范匹配）中排除的特性名称列表。

只包括条目中的下列特性。选择此选项以表明该表包含特性名称列表，这些特性名称可以作为与以上任一规范匹配的条目的组成部分返回。

7. 单击 “保存”以创建对象。

Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

8. 重复步骤 3 到步骤 7 以创建任何其他对象。

9. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

LDAP 服务器属性

在目录部署中， Directory Proxy Server 位于 LDAP 客户机和 LDAP 目录服务器之间。在将来自 LDAP 客户机的请求路由到 LDAP 目录服务器之前，对这些请求进行过滤，并在将来自目录服务器的响应传递到客户机之前，对响应进行过滤。Directory Proxy Server 还支持在一组复制的目录服务器之间进行自动负载平衡和自动故障转移及故障回复。

可以使用 LDAP 服务器属性来标识 Directory Proxy Server 应该将其用作后端服务器的目录服务器。当定义此属性时，应指定 Directory Proxy Server 所需的所有详细信息，例如，目录服务器的 IP 地址或全限定主机名，目录服务器在其上侦听客户机连接的端口号，服务器支持的 LDAP 版本，用于在 Directory Proxy Server 和此服务器之间进行通信的版本，等等，以便与目录服务器进行通信。

下面一节介绍如何从 Directory Proxy Server 配置编辑器控制台创建 LDAP 服务器属性对象。

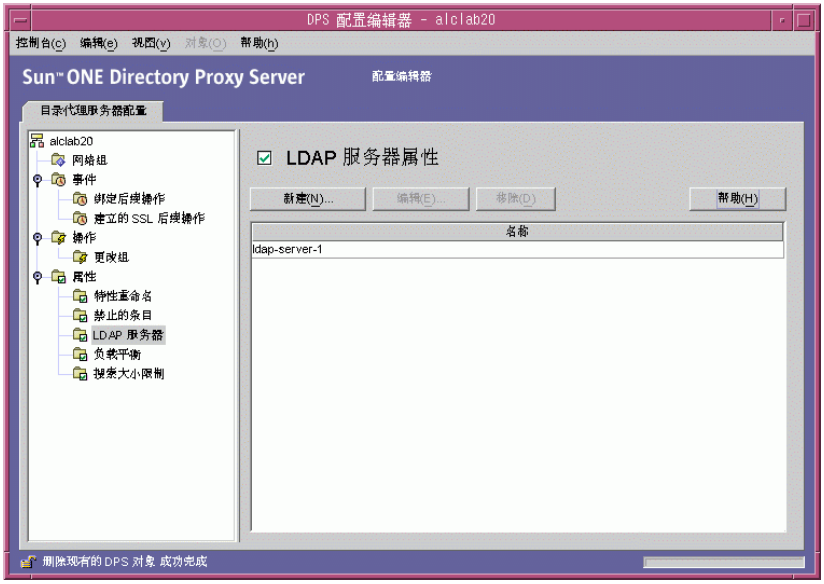
创建 LDAP 服务器属性对象

➤ **标识要与 Directory Proxy Server 进行通信的目录服务器**

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

2. 在导航树中，展开 “属性”节点，然后选择 “LDAP 服务器”。

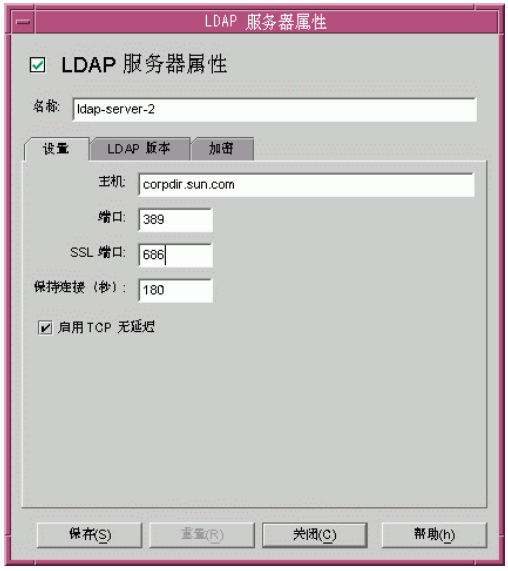
   右侧窗格显示 LDAP 服务器属性的现有对象的列表。



3. 单击 “新建”。

   “LDAP 服务器属性”窗口随即出现。

4. 在 “名称”字段中，键入属性对象的名称。名称必须是唯一的字母数字字符串。



5. 在 “设置”选项卡中，指定此属性引用的 LDAP 服务器的基本设置。

主机。输入一个值以指定运行后端 LDAP 服务器的主机的完整域名或 IP 地址。此特性为强制属性。

端口。输入一个端口号，指定后端 LDAP 服务器在其上运行的端口。如果没有此特性，则使用缺省的端口 （端口号为 389）。

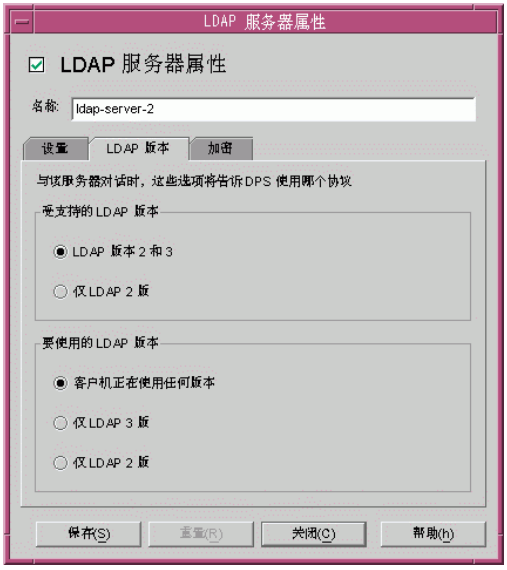
SSL 端口。输入一个端口号，指定后端 LDAP 服务器在其上侦听 LDAPS （通过 SSL 的 LDAP）连接的端口。如果后端 LDAP 服务器不支持 LDAPS，则不要为此特性设置任何值。

保持连接。输入秒数，经过这段时间后， Directory Proxy Server 将试探不响应的服务器，以确定到 LDAP 目录服务器的网络链接是否关闭，或者确定 LDAP 目录服务器是否已经不响应。如果连接到 Directory Proxy Server 的客户机具有挂起的操作，而且如果在此处指定的秒数之后 Directory Proxy Server 尚未从连接的 LDAP 服务器接收到任何数据，则 Directory Proxy Server 将通过打开另一

个通信信道来测试 LDAP 服务器的可用性。如果 Directory Proxy Server 这样操作不成功，那么它会将故障转移到另一台 LDAP 服务器 （如果可用）。此特性的缺省值为 180 秒。如果 LDAP 服务器与 Directory Proxy Server 不在同一本地网络，则建议增大此值。

启用 TCP 无延迟。禁用此选项将导致 Directory Proxy Server 对那些与此服务器的连接使用 Nagel 算法。只有当 Directory Proxy Server 和此对象条目定义的服务器之间的网络带宽非常有限时，才必须禁用该选项。缺省情况下，启用此设置。

6. 选择 “LDAP 版本”选项卡，并指定相应的值。



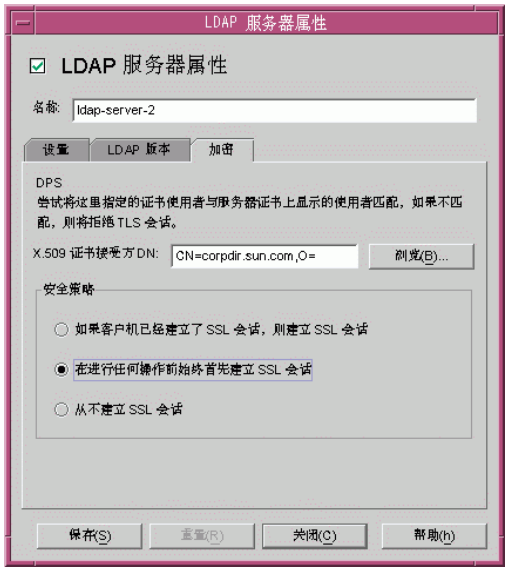
该选项卡显示一些设置，表明此服务器支持哪些 LDAP 版本，以及 Directory Proxy Server 和此服务器之间的通信应该使用哪个版本。

受支持的 LDAP 版本。从现有的两个选项中选择一个：“LDAP 版本 2 和 3”或者 “仅 LDAP 2 版”。缺省值为 “LDAP 版本 2 和 3”。

要使用的 LDAP 版本。从现有的三个选项中选择一个：“客户机正在使用任何版本”、“仅 LDAP 3 版”或者 “仅 LDAP 2 版”。当与此条目定义的后端服务器对话时，该特性将告知 Directory Proxy Server 使用哪个首选的 LDAP 协议版本。缺省情况下，选中 “客户机正在使用任何版本”。

当您具有 Directory Proxy Server 需要跟随引荐的 LDAPv2 客户机时，此选项很有用。在这种情况下，Directory Proxy Server 本身需要作为 LDAPv3 客户机连接到后端服务器，以便后端服务器可以向其发回引荐。如果引用该属性的网络组允许多个 LDAP 版本 2 绑定，则只能选择 LDAP 版本 3。

7. 选择 “加密”选项卡，并指定相应的值。



该选项卡显示的设置与由此属性引用的 LDAP 服务器的安全通信相关。

X.509 证书接受方 DN。指定 LDAP 服务器的证书接受方名称。如果已指定，则 Directory Proxy Server 尝试将该证书接受方与 LDAP 服务器证书的现有接受方匹配，如果不匹配，则拒绝 TLS 会话。（此特性允许 Directory Proxy Server 对它正在连接的 LDAP 服务器进行验证。如果未设置此特性， Directory Proxy Server 就会接受任何名称。）

安全策略。选择其中一个选项，这些选项定义了 Directory Proxy Server 和后端服务器之间连接的安全策略：“如果客户机已经建立了 SSL 会话，则建立 SSL 会话”、“在进行任何操作前始终首先建立 SSL 会话”或 “从不建立 SSL 会话”。

8. 单击 “保存”以创建对象。

Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

9. 重复步骤 3 到步骤 8 以创建任何其他对象。

10. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

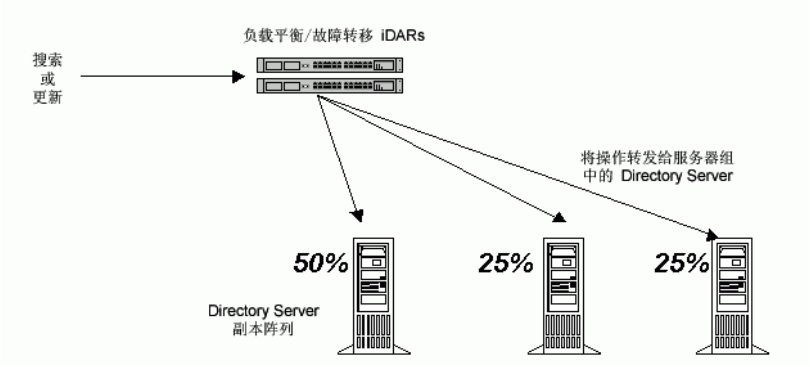
负载平衡属性

Directory Proxy Server 通过在一组复制的 LDAP 目录服务器之间提供自动负载平衡和自动故障转移及故障回复，实现了目录部署的高可用性。为了让 Directory Proxy Server 做到这一点，需要标识 Directory Proxy Server 应该使用的目录服务器，并指定客户机负载如何在这些服务器之间分配。

使用 “负载平衡”属性来配置 Directory Proxy Server 以进行负载平衡。此属性允许您标识 Directory Proxy Server 应该与其进行通信的后端目录服务器，并指定每个目录服务器应该接收到的总客户机负载的百分比。配置完毕后， Directory Proxy Server 就遵照配置中定义的负载条件将客户机查询自动分配给不同的目录服务器。如果一个目录服务器不可用， Directory Proxy Server 会将该服务器的负载百分比按比例在可用服务器之间分配 （根据它们的负载百分比）。如果所有的后端 LDAP 服务器都不可用， Directory Proxy Server 就开始拒绝客户机查询。

图 8-2 显示了在一组三个目录服务器副本之间分配的客户机负载。

图 8-2 一组 LDAP 目录副本之间的负载平衡



Directory Proxy Server 中的负载平衡是基于会话的。这就意味着，选择客户机的查询将定向到哪一台特定目录服务器的决策功能针对每个客户机会话只应用一次，尤其是在客户机会话开始时。该会话中的所有后续客户机查询都将被定向到在会话开始时选择的同一目录服务器。

Directory Proxy Server 可以进行负载平衡的后端目录服务器的数目取决于多种因素，其中一些如下所示：

- 运行 Directory Proxy Server 的主机的大小
- 可用的网络带宽

- Directory Proxy Server 接收到的混合查询
- 客户机会话的长度
- Directory Proxy Server 配置

一般而言，如果大多数会话持续时间短暂，并且查询的计算量密集，则 Directory Proxy Server 可以支持较少的目录服务器。计算量密集的查询是那些需要检查整个消息的查询，例如使用特性重命名功能 （请参阅第 112 页上的 “特性重命名属性”）。

当目录服务器由于以下原因而变得不可用时， Directory Proxy Server 就会进行检测：连接尝试因拒绝连接错误而返回，或者连接尝试出现超时。由于这两种情况均发生在会话初期，并且尚未对该会话进行任何操作，因此 Directory Proxy Server 会将故障转移到另一台服务器 （只要这台服务器确实可用）。在连接尝试超时的情况下，客户机在获取响应时可以感觉到明显的延迟。如果 Directory Proxy Server 和后端服务器之间的连接突然丢失，那么 Directory Proxy Server 就会向受影响的客户机返回所有未完成操作的 `LDAP_BUSY` 错误。随后， Directory Proxy Server 将该客户机会话的故障转移到另一台目录服务器。

为了避免 Directory Proxy Server 成为目录部署的单一故障点，建议您至少使用两台 Directory Proxy Server，在其前面应用一个 IP。这在第 31 页上的 “Directory Proxy Server 部署方案”中进行了描述。在不可能这样部署 Directory Proxy Server 的情况下，我们建议您使用 -M 开关，该开关将让 Directory Proxy Server 监视其本身。

Directory Proxy Server 使用监视进程在其后端服务器上进行运行状况检查。如果使用了负载平衡，则该功能将自动启用。 Directory Proxy Server 每隔 10 秒钟就会为它的每个后端目录服务器对 Root DSE 执行一次匿名搜索操作。如果其中之一变得不可用或没有响应， Directory Proxy Server 就会将其从活动的负载平衡服务器集合中移除。当服务器再次可用时，则会再次将它引入到活动的负载平衡服务器集中。为了使监视功能有效地发挥作用，必须根据 `idsktune</code>` 公用程序的建议配置 Directory Proxy Server 在其上运行的主机。当服务器只启用其安全端口时， Directory Proxy Server 将尝试安全地执行运行状况检查。

下面一节介绍如何从 Directory Proxy Server 配置编辑器控制台创建负载平衡属性对象。

注 您为负载平衡属性创建的任何对象必须至少具有一个 LDAP 服务器属性，百分比加起来必须为 100%。否则， Directory Proxy Server 将无法启动。

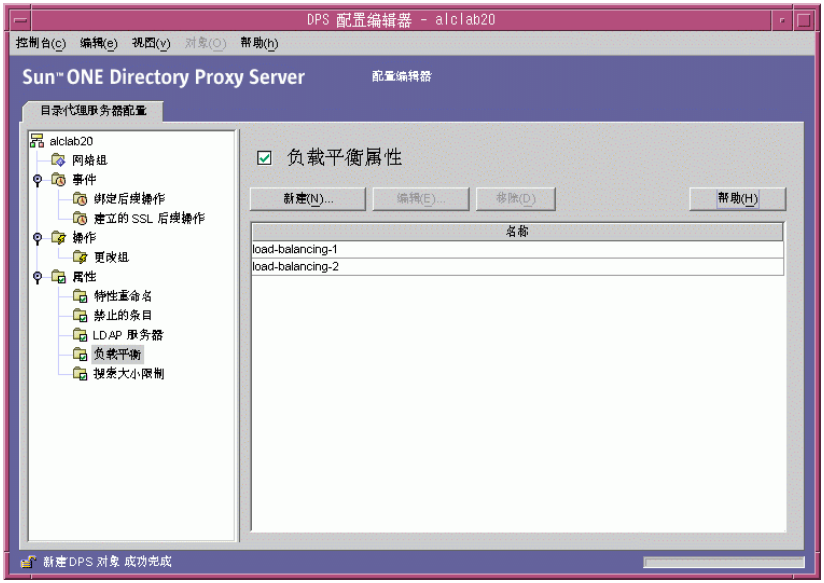
创建负载平衡属性对象

本节介绍如何配置 Directory Proxy Server 以进行负载平衡。在创建负载平衡属性对象之前，要确保标识 Directory Proxy Server 应该用于平衡客户机负载的 LDAP 目录服务器。有关详细信息，请参阅第 119 页上的 “LDAP 服务器属性”。

➤ 定义一组目录服务器的负载平衡

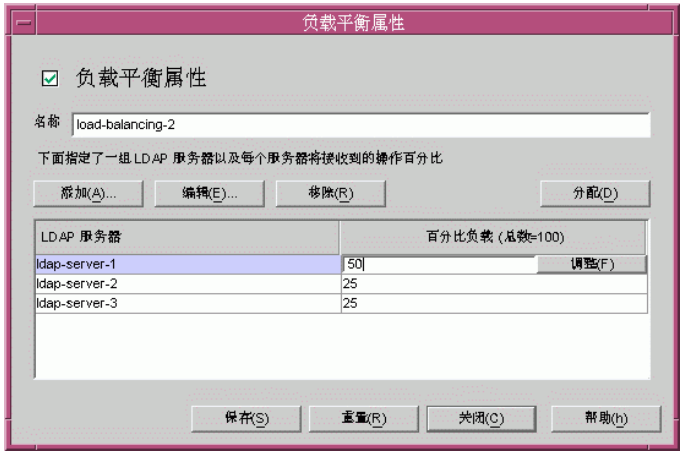
1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。
2. 在导航树中，展开 “属性”节点，然后选择 “负载平衡”。

   右侧窗格显示 “负载平衡”属性的现有对象的列表。



3. 单击“新建”。

   “负载平衡属性”窗口随即出现。



4. 在“名称”字段中，键入属性对象的名称。名称必须是唯一的字母数字字符串。

5. 使用其余的表单元素来获取希望的结果。

   要编辑百分比，请单击包含 LDAP 服务器的行旁边的“百分比负载”列，键入一个 0 和 100 之间的数字，并单击“调整”按钮。此操作将百分比分配给当前行，并尝试让所有百分比的总和为 100。当前百分比总和显示在“百分比负载”列标题中。

   添加。显示一个对话框，用于添加对 LDAP 服务器属性的引用。缺省情况下，添加的第一台服务器将分配 100% 的负载，随后添加的服务器将获得 0% 的负载。

   编辑。显示一个对话框，用于编辑表中当前选定的项目。

   移除。从将在其中执行负载平衡的服务器列表中移除当前选择的 LDAP 服务器。

   分配。在表中当前引用的所有 LDAP 服务器之间平均分配百分比负载。

6. 单击“保存”以创建对象。

   Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

7. 重复步骤 3 到步骤 6 以创建任何其他对象。

8. 重新启动服务器，如第 62 页上的“重新启动 Directory Proxy Server”中所述。

搜索大小限制属性

LDAP 目录通常作为一个组织的中心信息库，让跨组织部署的 LDAP 客户机可以查找信息。 LDAP 客户机一般通过搜索特定信息（使用搜索过滤器）来查找信息。当搜索一个条目时，客户机通常会指定与该条目类型相关的特性；例如，当您搜索人员条目时，可以使用 CN 特性来搜索具有特定常用名的人员。

Directory Proxy Server 可以处理数以千计的 LDAP 客户机请求，并可以将其配置为对 LDAP 目录应用精细的访问控制策略，例如，控制哪个用户可以在目录信息树 (DIT) 的不同部分执行不同类型的操作。您还可以配置 Directory Proxy Server 以禁止某些类型的操作，如 Web 拖网者和机器人所执行的用来收集一个目录中包含的信息的操作。

可以使用 “搜索大小限制”属性以便基于搜索基和搜索范围来应用大小限制。如果此属性对象条目中指定的搜索基和搜索范围都不与给定的搜索相匹配，则大小限制缺省为在 “网络组”对象条目中指定的大小限制，如第 79 页上的 “创建和管理组”中所述。

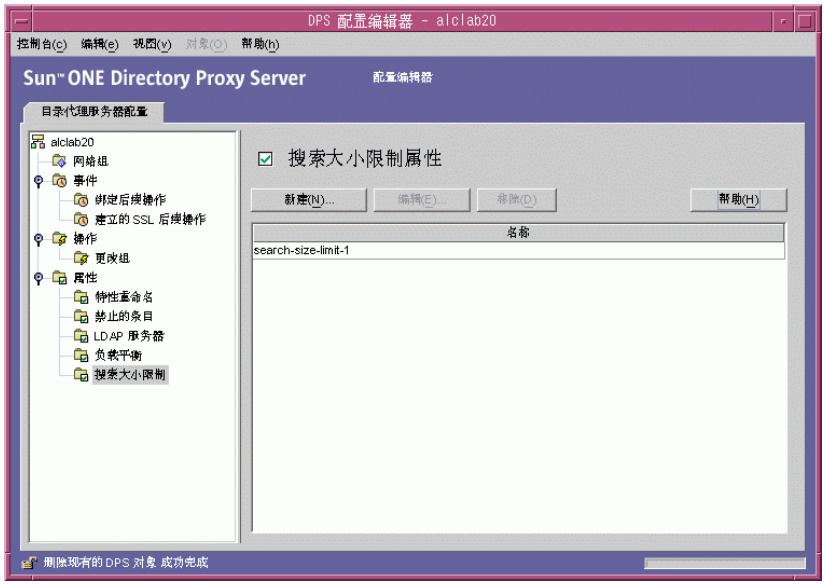
下面一节介绍如何从 Directory Proxy Server 配置编辑器控制台创建搜索大小限制属性对象。

创建搜索大小限制属性对象

➤ **定义搜索大小限制**

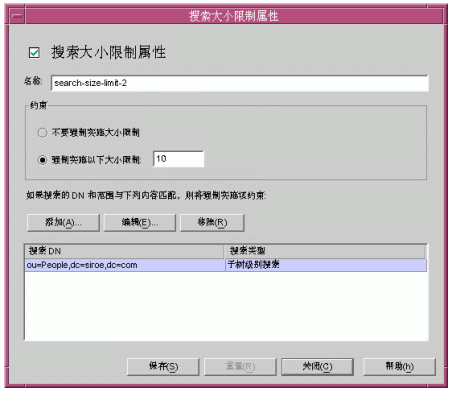
1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

2. 在导航树中，展开 “属性”节点，然后选择 “搜索大小限制”。



3. 单击 “新建”。

“搜索大小限制属性”窗口随即出现。



4. 在 “名称”字段中，键入属性对象的名称。名称必须是唯一的字母数字字符串。

5. 使用其余的表单元素来获取希望的结果：

   约束。指定是否强制实施大小限制约束。

   不要强制实施大小限制。选择此选项可指定不强制实施大小限制。

   强制实施以下大小限制。选择此选项并输入一个整数值，以指定要强制实施的大小限制。

   添加。显示用于添加大小限制条件的菜单。条件必须为下面的两种类型之一：一级搜索和子树级别搜索。

   一级搜索。显示一个对话框，从中可输入 DN 并将其添加到条件表中。如果一级搜索的搜索基 DN 与条件表中为一级搜索指定的某个识别名匹配，则指定的大小限制将被强制实施为该搜索的大小限制。

   子树级别搜索。显示用于输入 DN 的对话框。如果子树搜索的搜索基 DN 与条件表中为子树级别搜索指定的某个识别名匹配，则指定的大小限制将被强制实施为该搜索的大小限制。

   编辑。显示一个对话框，用于编辑表中当前选择的条目。

   移除。移除表中当前选择的条目。

6. 单击 “保存”以创建对象。

   Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

7. 重复步骤 3 到步骤 6 以创建任何其他对象。

8. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

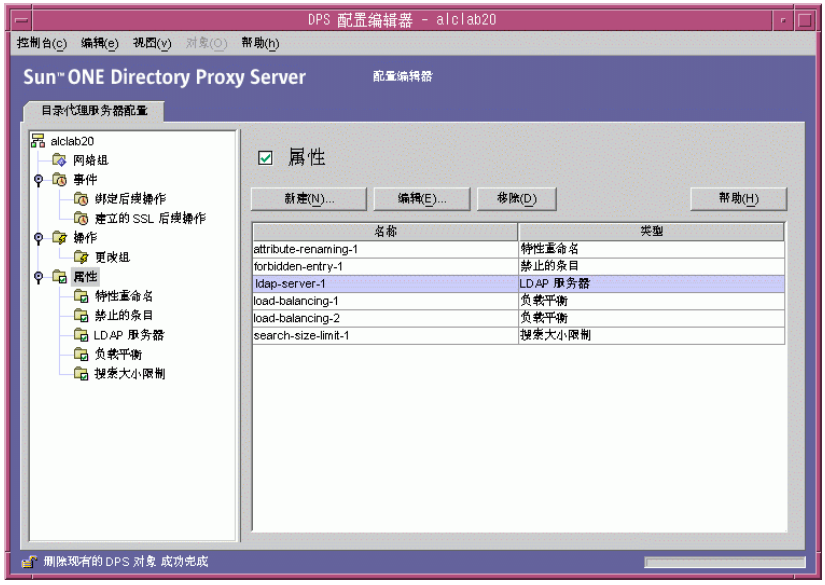
修改属性对象

➤ **修改属性对象**

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

2. 在导航树中，选择 “属性”节点。

   右侧窗格显示现有属性对象的列表。要查看与特定属性有关的对象，请展开 “属性”节点，然后选择您关心的属性。



3. 在该列表中，选择要修改的对象并单击 “编辑”。
4. 进行所需的修改。
5. 单击 “保存”以保存更改。

   Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

6. 重复步骤 3 到步骤 5 以修改任何其他对象。
7. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

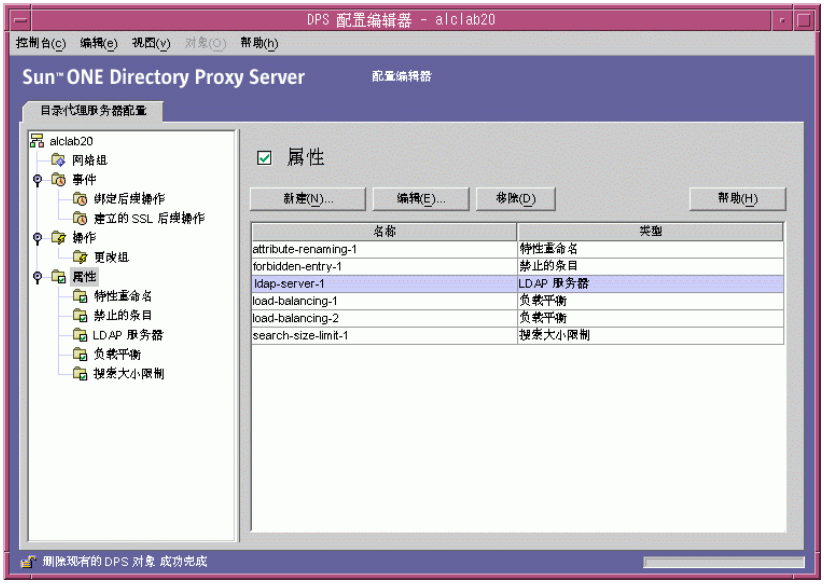
删除属性对象

可以从 Directory Proxy Server 配置中删除任何不需要的属性对象。在删除一个对象之前，请确保它未在任何其他配置条目中使用。

➤ 删除属性对象

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。
2. 在导航树中，选择 “属性”节点。

   右侧窗格显示现有属性对象的列表。要查看与特定属性有关的对象，请展开 “属性”节点，然后选择您关心的属性。



3. 在该列表中，选择要删除的对象并单击 “移除”。
4. 确认操作。

   Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。
5. 重复步骤 3 到步骤 4 以删除任何其他对象。
6. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

第 9 章

创建和管理事件对象

Directory Proxy Server 支持事件驱动的操作。您可以配置 Directory Proxy Server 以在特定事件发生时执行指定的操作。本章介绍如何使用 Directory Proxy Server 配置编辑器控制台创建和管理事件对象。

本章包含以下几个部分：

事件概述

事件是 Directory Proxy Server 运行时在某一点所处的状态。您可以使用事件对象来指定 Directory Proxy Server 在预设状态下进行计算的条件。作为定义事件对象的一部分，还应指定在满足这些条件时 Directory Proxy Server 应执行的操作。有关操作的详细信息，请参阅第 141 页上的 “创建和管理操作对象”。

Directory Proxy Server 可以识别或跟踪两种事件类型：

- OnBindSuccess 事件－当客户机成功完成绑定操作后计算此事件。
- OnSSLEstablished 事件－当客户机成功建立 SSL 会话后计算此事件。此事件没有任何相关的条件，始终执行其操作列表。

可以只基于上述这两个事件来定义事件对象。例如，可以定义一个事件对象，用于在客户机成功完成绑定时执行检测。此定义的一部分可以是在事件发生时执行某项操作，例如，更改此客户机的访问组。有关组的详细信息，请参阅第 79 页上的 “创建和管理组”。

创建事件对象

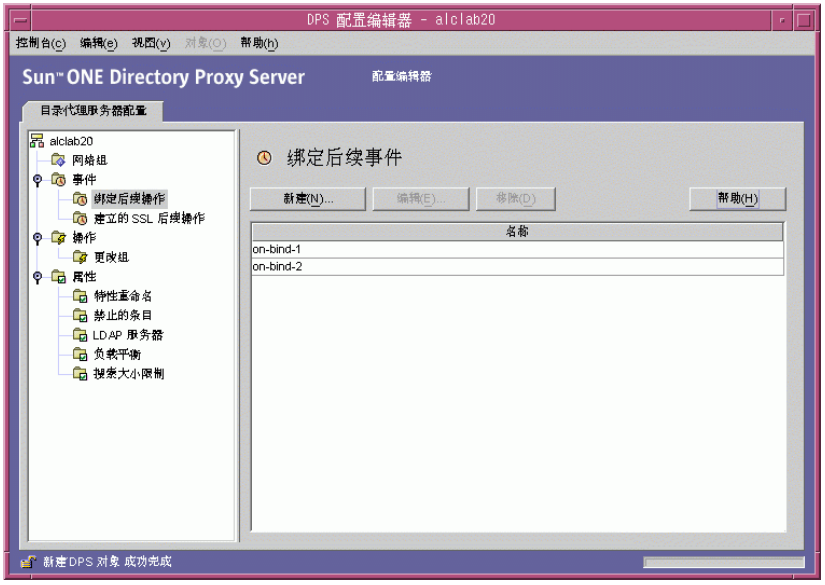
本节说明如何创建基于 OnBindSuccess 和 OnSSLEstablished 事件的事件对象。有关这些事件的详细信息，请参阅第 133 页上的 “事件概述”。

创建 OnBindSuccess 事件对象

➤ **创建基于 OnBindSuccess 事件的事件对象**

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。
2. 在导航树中，展开 “事件”节点，然后选择 “绑定后续操作”。

   右侧窗格将显示基于 OnBindSuccess 事件的现有事件对象的列表。



3. 单击“新建”。

   “绑定后续事件”窗口随即出现。

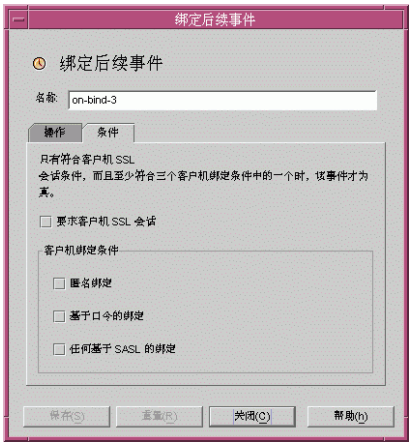
4. 在“名称”字段中，键入事件对象的名称。名称必须是唯一的字母数字字符串。

5. 在“操作”选项卡中，选择事件发生时 （即事件的计算值为 TRUE）要执行的操作。

   新建。也可以通过单击“新建”按钮定义新的操作对象。

   编辑。单击“编辑”按钮以修改与当前所选操作对象相关的参数。

6. 选择 “条件”选项卡并指定条件。



仅当满足指定的条件时该事件的计算值才为 TRUE，即此选项卡中指定的条件经计算后值必须为 TRUE，这样才能执行 “操作”选项卡中指定的操作。只有满足客户机 SSL 会话条件，而且至少满足三个客户机绑定条件中的一个条件时，该条件才为 TRUE。

要求客户机 SSL 会话。选择此选项表明只有当客户机已经与 Directory Proxy Server 建立了 SSL 会话时，条件的计算值才为 TRUE。缺省值为 FALSE。

客户机绑定条件。条件为如下选项之一：“匿名绑定”、“基于口令的绑定”和 “任何基于 SASL 的绑定”。

匿名绑定。选择此选项表明只有当满足客户机 SSL 会话要求而且客户机正好成功完成了匿名绑定时，条件的计算值才为 TRUE。

基于口令的绑定。选择此选项表明只有当满足客户机 SSL 会话要求而且客户机正好成功完成了基于口令的绑定时，条件的计算值才为 TRUE。

任何基于 SASL 的绑定。选择此选项表明只有当满足客户机 SSL 会话要求，而且客户机正好使用任一 SASL 机制成功完成绑定时，条件的计算值才为 TRUE。

7. 单击 “保存”以创建事件对象。

   Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

8. 重复步骤 3 到步骤 7 以创建任何其他对象。

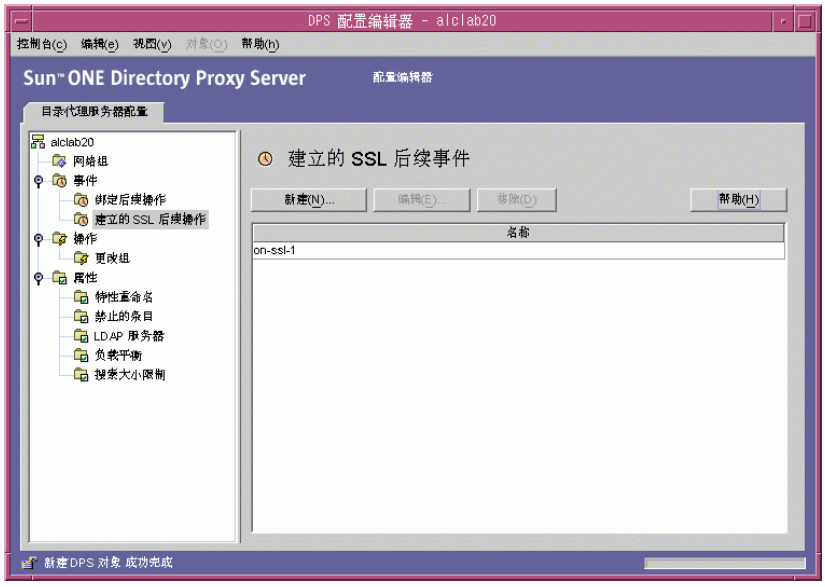
9. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

创建 OnSSLEstablished 事件对象

➤ **创建基于 OnSSLEstablished 事件的事件对象**

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。
2. 在导航树中，展开 “事件”节点，然后选择 “建立的 SSL 后续事件”。

   右侧窗格将显示基于 OnSSLEstablished 事件的现有事件对象的列表。



3. 单击 “新建”。

   “建立的 SSL 后续事件”窗口随即出现。

4. 在 “名称”字段中，键入事件对象的名称。名称必须是唯一的字母数字字符串。
5. 在 “操作”部分中，选择事件发生时 （即事件的计算值为 TRUE 时）要执行的操作。

   单击 “编辑”按钮以修改与当前所选操作相关的参数。也可以通过单击 “新建”按钮定义新的操作。
6. 单击 “保存”以创建事件对象。

   Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。
7. 重复步骤 3 到步骤 6 以创建任何其他对象。
8. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

修改事件对象

➤ **修改事件对象**

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

2. 在导航树中，选择 “事件”。

   右侧窗格将显示现有事件对象的列表。要查看与事件类型相关的对象，请展开 “事件”节点，然后选择您所关心的事件类型。

3. 在列表中，选择要修改的事件对象并单击 “编辑”。
4. 进行所需的修改。
5. 单击 “保存”以保存更改。

   Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

6. 重复步骤 3 到步骤 5 以修改任何其他对象。
7. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

删除事件对象

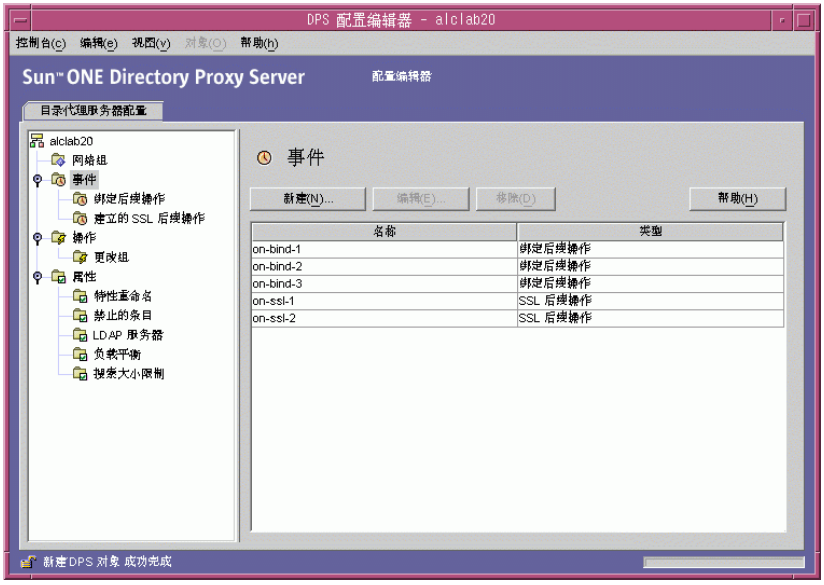
可以从 Directory Proxy Server 配置中删除任何不需要的事件对象。

➤ 删除事件对象

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

2. 在导航树中，选择 “事件”节点。

   右侧窗格将显示现有事件对象的列表。要查看与事件类型相关的对象，请展开 “事件”节点，然后选择您所关心的事件类型。



3. 在列表中，选择要删除的事件对象并单击 “移除”。

4. 在出现提示时，请确认您的操作。

   您删除的事件对象名称现已从列表中移除。 Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

5. 重复步骤 3 到步骤 4 以删除任何其他对象。

6. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

第 10 章

创建和管理操作对象

Directory Proxy Server 支持事件驱动的操作，即您可以配置 Directory Proxy Server 在特定事件发生时执行指定的操作。本章介绍如何使用 Directory Proxy Server 配置编辑器控制台创建和管理操作对象。

本章包含以下几个部分：

操作概述

操作是指 Directory Proxy Server 可执行的任务。如果事件对象定义的规则或条件的值为 `TRUE`，则将使用操作对象指定 Directory Proxy Server 应执行的操作。事件对象用于指定预设条件下由 Directory Proxy Server 计算的条件。有关事件的详细信息，请参阅第 133 页上的 “创建和管理事件对象”。

当前， Directory Proxy Server 可以执行一种称为 `ChangeGroup` 的操作。使用此操作可以配置 Directory Proxy Server，以便根据规则计算值将客户机从一个访问组更改到另一个访问组。有关组的详细信息，请参阅第 79 页上的 “创建和管理组”。

如果 LDAP 目录包含有关移动用户 （例如，从不同的 IP 地址或物理位置连接到该目录的用户）的信息，则更改组功能十分有用。您可以通过以下方式设置 Directory Proxy Server，即移动用户将使用动态 IP 地址连接到 Directory Proxy Server 并位于 “缺省”访问组中。“缺省”访问组的规则将基于 `OnBindSuccess` 事件，仅当移动用户所提供的绑定凭据通过验证后，该规则的计算值才为 “TRUE”。此规则还将配置 `ChangeGroup` 操作，以将移动用户的访问组从 “缺省”访问组更改为移动用户使用静态 IP 地址访问 Directory Proxy Server 时通常分配的访问组。

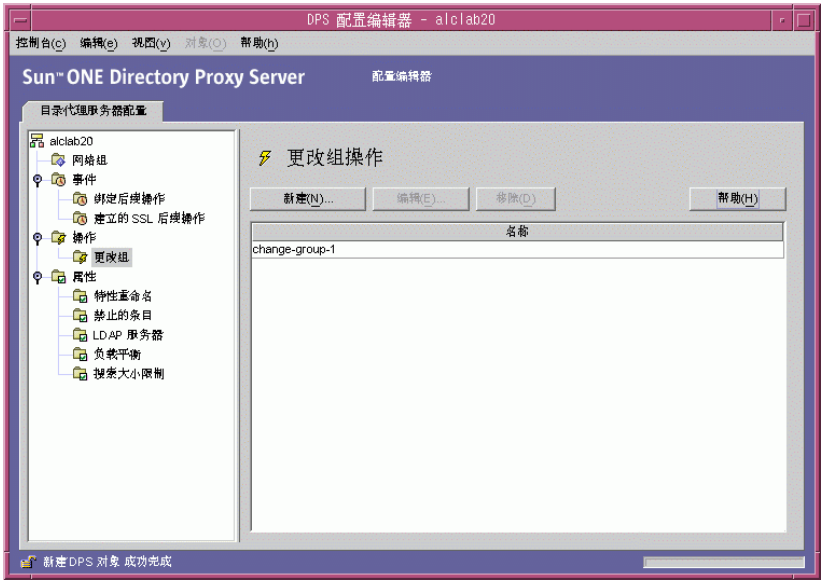
创建操作对象

您可以为某些事件发生时需要执行的操作创建对象。以下说明介绍了如何为更改组创建操作对象。

➤ 创建操作对象，以将客户机从一个组更改到另一个组

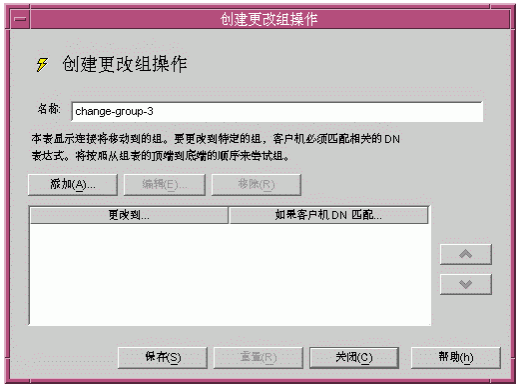
1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。
2. 在导航树中，展开 “操作”节点，然后选择 “更改组”。

   右侧窗格将显示现有操作对象的列表。



3. 单击“新建”。

   “创建更改组操作”窗口随即出现。



4. 在“名称”字段中，键入对象的名称。名称必须是唯一的字母数字字符串。

5. 在“操作”选项卡中，选择事件发生时（即事件的计算值为 TRUE 时）要执行的操作。

   更改到 ... 显示客户机可以更改到的组列表。对于要发生的更改，客户机必须匹配与每个组相关的 DN 表达式。要编辑与特定组或“无更改”条目相关的 DN 表达式，请单击表中的“如果客户机 DN 匹配”列。将从该列表顶端到底端进行计算，直到某个 DN 表达式匹配。因此，将最常见的 DN 表达式放在列表的底端很重要，这样可以计算所有表达式。

   必须对正则表达式进行规范化，即在 RDN 组件和等号 (=) 之间不应有空格，所有特性名称和特性值都必须大写。

   可以使用下面这本书作为正则表达式的参考资料：*Mastering Regular Expressions*， Friedl 和 Oram 著， O'Reilly 出版， ISBN：1565922573。

   添加。显示一个菜单，用于添加客户机连接可能更改到的组。组更改条目可以是下面的类型：“组更改条目”或“无更改条目”。

   组更改条目。显示一个对话框，根据相关 DN 表达式的计算值是否为 TRUE 来选择客户机将更改到的网络组。

   无更改条目。向表中添加一行，表明如果相关 DN 表达式的计算值为 TRUE，则“不”发生任何更改。这在为更改组列表计算“最少运算”的过程中很有用。

   编辑。显示一个对话框，用于编辑表中当前选择的条目。

   移除。移除表中当前选择的条目。

6. 单击 “保存”以创建操作对象。

   Directory Proxy Server 配置被修改，并提示您重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

7. 重复步骤 3 到步骤 6 以创建任何其他对象。

8. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

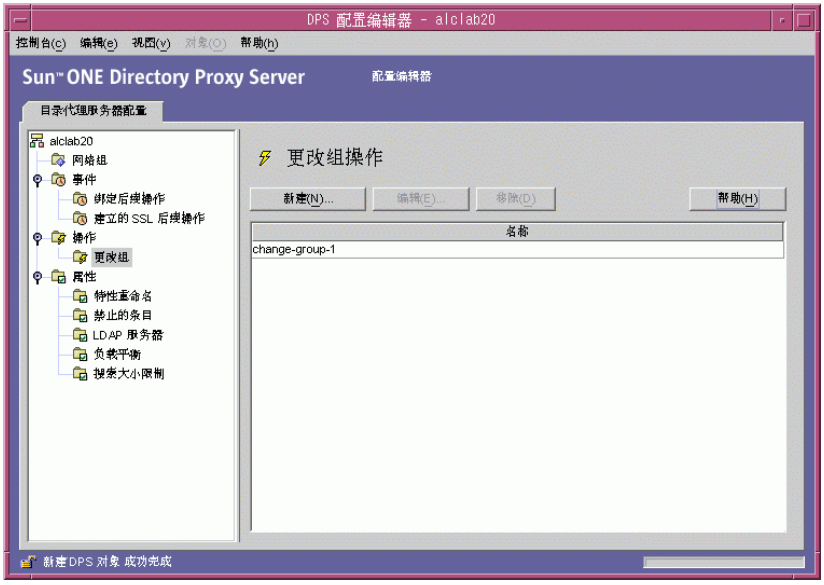
修改操作对象

➤ **修改操作对象**

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

2. 在导航树中，选择 “操作”。

   右侧窗格将显示现有操作对象的列表。



3. 在列表中，选择要修改的操作对象并单击 “编辑”。

4. 进行所需的修改。

5. 单击 “保存”以保存更改。

   Directory Proxy Server 配置被修改，并提示重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

6. 重复步骤 3 到步骤 5 以修改任何其他对象。

7. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

删除操作对象

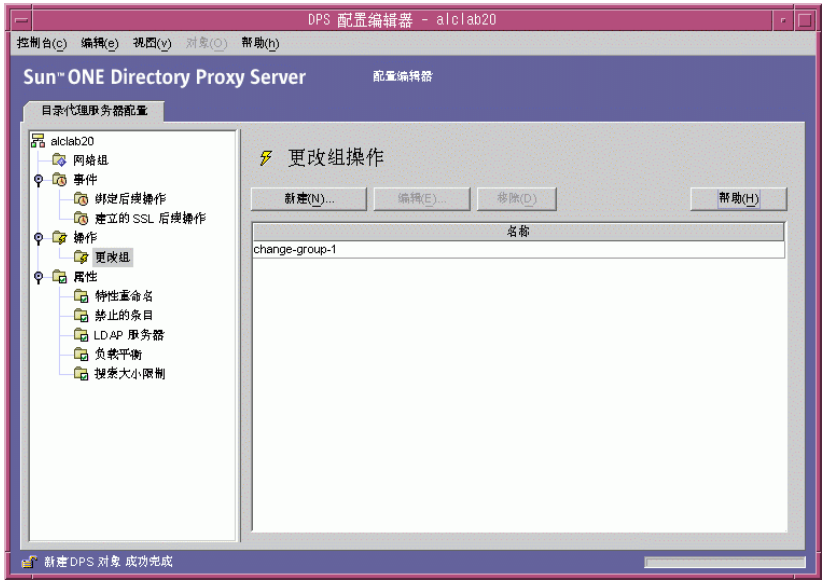
可以从 Directory Proxy Server 配置中删除任何不需要的操作对象。在删除操作对象之前，请确保它未在任何事件对象的配置中使用。

➤ **删除操作对象**

1. 访问 Directory Proxy Server 配置编辑器控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

2. 在导航树中，选择 “操作”。

   右侧窗格将显示现有操作对象的列表。



3. 在列表中，选择要删除的操作并单击 “移除”。

4. 确认操作。

   您删除的对象名称现在将从列表中移除。 Directory Proxy Server 配置被修改，并提示重新启动基于此配置的服务器。但是，此时请勿重新启动服务器。完成所有配置更改后可以执行此操作。

5. 重复步骤 3 到步骤 4 以删除任何其他对象。

6. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

第 11 章

配置和监视日志

本章说明如何配置 Directory Proxy Server 以记录日志项或消息，然后借助记录的日志项使用 Directory Proxy Server 控制台来监视其活动。

本章包含以下几个部分：

日志记录概述

Directory Proxy Server 可以维护两种类型的日志：

- 系统日志
- 审核日志

本节介绍这些日志。

系统日志

Directory Proxy Server 可以维护各种事件和系统错误的详尽日志记录，以便监视和调试系统。所有日志记录都可在文本文件中进行维护，并可将其存储在本地文件系统中以进行快速和便捷地检索。缺省情况下， Directory Proxy Server 将日志项写入以下文件：

```
<server-root>/dps-<hostname>/logs/fwd.log
```

日志文件中的每条消息都标记了时间。同时还有 Directory Proxy Server 内部的进程号和消息号。

出于标识和过滤的目的， Directory Proxy Server 记录的事件分为不同种类型。它们列在表 11-1 中。每类代表的消息具有相同或相似的性质，或属于特定的功能区域。基于配置，日志文件可记录属于一个或多个这种类别的日志项。

在 Directory Proxy Server 配置中，每个消息种类都对应于特定的日志级别。日志级别表明由服务器执行的日志记录级别，即，应如何详细地记录日志。

- 优先级越高意味着详细信息越少，因为只记录高优先级的事件。
- 优先级越低意味着详细信息越多，因为日志文件中记录了更多种类的事件。

表 11-1 以优先级的降序顺序列出了消息种类－紧急具有最高的优先级别，而详细跟踪具有最低的优先级别。

表 11-1 日志级别

日志级别或严重性	说明
强制	强制消息始终写入日志。这些消息表明 Directory Proxy Server 读取的配置、 Directory Proxy Server 启动时的版本号等。 具有此级别的消息无法配置。
紧急	这些消息表明 Directory Proxy Server 遇到了一些需要立即引起注意的问题。例如， *Directory Proxy Server process 1234 has exited, attempting restart in 10 seconds.*
异常	这些消息表明意外的错误情况，例如 Directory Proxy Server 从客户机 / 服务器接收到格式不正确的 LDAP 消息。例如， *Could not decode search request.*
警告	这些消息指定 Directory Proxy Server 能够忽略但必须由管理员进行检查的错误情况。例如， *Local host name lookup failed.System default group may not function correctly.*
通知	这些消息仅供参考。例如， *Received NULL continuation reference from server.Discarding...*
跟踪	这些是调试消息。例如， *Result received from server lderr =32, matched=o=sun.com, errtxt=no such object.* 跟踪消息包括协议转储。使用跟踪级别可以迅速生成极大的日志文件。
详细跟踪	这些消息提供更详细的调试信息，例如为回收连接请求的匿名绑定。这些消息通常供 Directory Proxy Server 工程 / 支持组使用。

通过 Directory Proxy Server，您可以指定日志记录的数量－能够使用日志级别根据事件的严重性过滤日志项。缺省情况下，该级别设置为警告。

注 日志级别是累加性的；即，如果选择警告作为日志级别，则将记录警告、异常和严重性级别消息。日志数据的量可能很大，尤其是较低（更详细）的日志记录级别。请确保主机具有足够的磁盘空间来存放所有日志文件。

另外，可以配置 Directory Proxy Server 将日志消息发送到 `syslog` 守护程序，而不发送到文件；无法将日志消息同时发送到文件和 `syslog` 守护程序。如果选择此配置，则应确保正确配置 `syslogd`。例如，要将所有消息写入某个特定文件 `/var/adm/messages` 中，必须在文件 `/etc/syslog.conf` 中添加以下行：

```
daemon.crit;daemon.warning;daemon.info;daemon.debug /var/adm/messages
```

注， Directory Proxy Server 使用 `daemon` 工具，它具有 `crit`、 `warning`、 `info` 和 `debug` 优先级或日志级别。表 11-2 显示了 syslog 事件和 Directory Proxy Server 事件之间的映射关系。

表 11-2 日志级别的映射

Directory Proxy Server 事件	syslog 事件
强制	info
紧急	crit
异常	err
警告	warning
通知	info
跟踪	info
详细跟踪	info

要循环 Directory Proxy Server 日志并控制其他日志记录功能，可使用以下对象类：

```
ids-proxy-sch-LogProperty
```

请参阅第 187 页上的 “dpsconfig2ldif”，以了解有关此对象类及其用法的详细信息。

审核日志

除了对系统和错误消息进行日志记录外， Directory Proxy Server 还可以维护所有事件和连接统计信息的审核跟踪－例如，可记录刚完成与 LDAP 目录绑定 / 解除绑定操作的客户机的 DN。

缺省情况下，没有将 Directory Proxy Server 配置为记录审核消息。可随时启用此功能。也可以指定是否将审核消息记录到与写入系统日志项相同的文件或备用文件中。除非配置为写入不同文件，否则，审核消息 （连同其他日志消息）将记录到写入系统日志项的同一文件中；有关详细信息，请参阅第 147 页上的 “系统日志”。

注	通过审核记录，您可以检测任何未经授权的访问或活动。因此建议您启用此功能。同时，作为安全措施，应定期检查 Directory Proxy Server 审核日志有无任何异常活动。

配置日志

要配置 Directory Proxy Server 以记录日志项，请执行以下步骤：

- 定义日志设置
- 指定日志记录属性

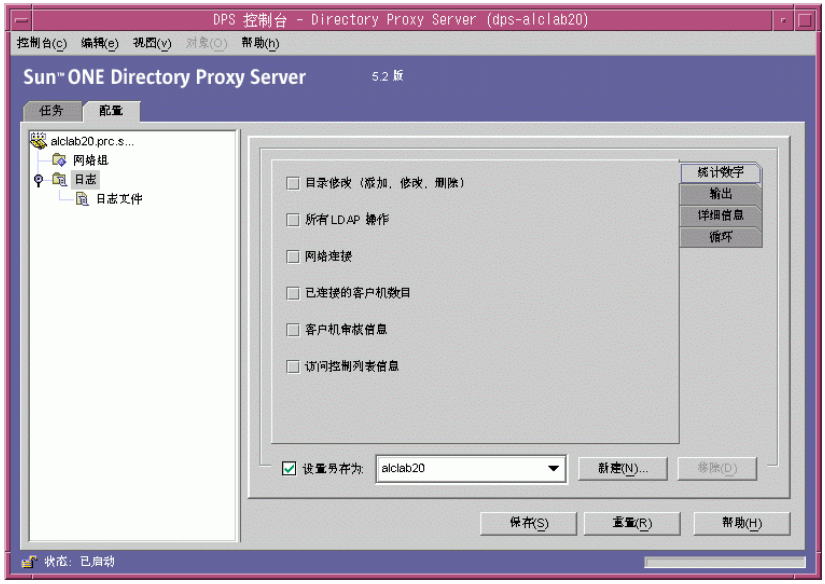
➤ 定义日志设置

只有在要创建或定义 “日志属性”的对象时，才需要该步骤。如果已经为日志属性创建了对象并且要使用其中的一个对象，那么请转至第 154 页上的 “指定日志记录属性”。

1. 访问 Directory Proxy Server 控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。

2. 选择 “配置”选项卡，然后在导航树中展开 “日志”。

   右侧窗格在右侧显示日志记录属性现有对象的列表。



3. 单击 “新建”定义新对象。

   “日志属性”窗口的 “统计数字”选项卡变为活动选项卡。

4. 在 “名称”字段中，键入对象的名称。名称必须是唯一的字母数字字符串。

5. 在 “统计数字”选项卡中，指定要记录的信息种类。

   选中与所需日志记录消息类型相关的复选框。缺省情况下，未选中任何选项。日志消息分为下列组：目录修改、所有 LDAP 操作、网络连接、已连接的客户机数目和客户机审核信息。

   目录修改。将记录有关写入目录的操作的统计信息，例如添加、修改和删除。

   所有 LDAP 操作。将记录有关所有 LDAP 操作的统计信息。

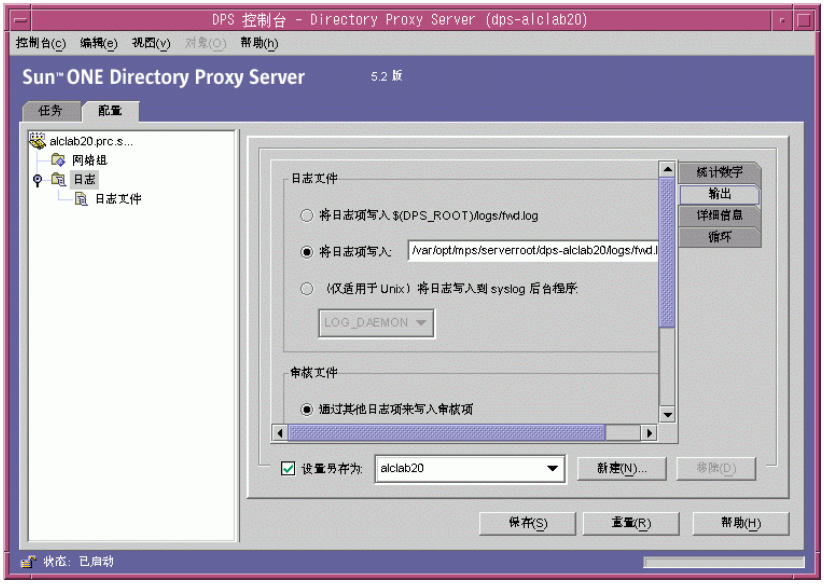
   网络连接。将记录有关网络连接的统计信息。

   已连接的客户机数目。将记录常规统计信息，例如连接了多少台客户机。

   客户机审核信息。将记录审核信息，例如刚完成绑定 / 解除绑定操作的客户机 DN。

   访问控制列表信息。包含可访问日志信息的用户列表。

6. 选择 “输出”选项卡，并指定应将日志项发送到的位置以及是否记录审核跟踪。



日志文件。显示一些选项，用于控制 Directory Proxy Server 将写入其日志项的位置。

将日志项写入 $(dps_ROOT)/logs/fwd.log。这是缺省设置， Directory Proxy Server 将其日志项写入到文件 `$(dps_ROOT)/logs/fwd.log` 中，其中 `$(dps_ROOT)` 是安装 Directory Proxy Server 的服务器根下的目录，一般为 `/usr/sunone/servers/dps-<hostname>` 或 `\Program\Files\sunone\Servers\dps-<hostname>`。

将日志项写入。指定 Directory Proxy Server 将其日志项定位到的备用文件。无论使用哪个平台，文件分隔符都必须遵循 UNIX 规范。

将日志写入到 syslog 后台程序。（仅适用于 UNIX）选择 Directory Proxy Server 将用于记录日志项的 syslog facility 代码。只有当 UNIX 主机上安装的 Directory Proxy Server 使用了此日志属性时，才应该选择此设置。

审核文件。显示一些选项，用于控制 Directory Proxy Server 将写入其审核日志项的位置。要使该功能生效，必须通过选择 “统计数字”选项卡中的 “客户机审核信息”选项来启用审核日志记录。

通过其他日志项来写入审核项。这是缺省设置， Directory Proxy Server 将其审核日志项写入到与以上日志文件设置所指定的同一输出中。

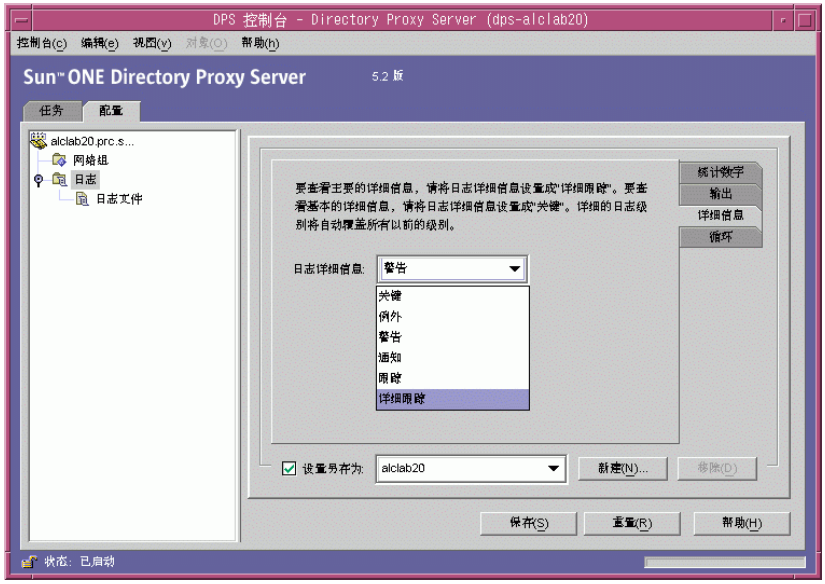
将日志项写入。指定 Directory Proxy Server 将其审核日志项定位到的备用

文件。无论使用哪个平台，文件分隔符都应该遵循 UNIX 规范。

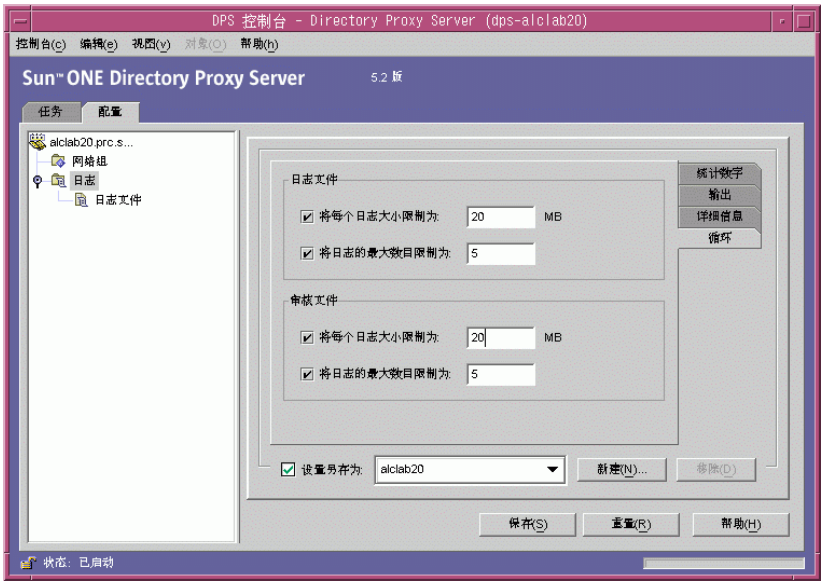
将审核写入到具有 facility 的 syslog 守护程序。（仅适用于 UNIX）选择 Directory Proxy Server 将用于记录审核项的 syslog facility 代码。只有当 UNIX 主机上托管的 Directory Proxy Server 使用了此日志属性时，才应该选择此设置。

7. 选择 “详细信息”选项卡并指定日志级别－希望的日志记录详细信息量。

从下拉菜单中选择日志记录级别。



8. 选择 “循环”选项卡以控制衡量日志大小及循环的方法。



日志文件。显示一些选项，用于限制 Directory Proxy Server 日志文件的大小和最大数目。

将每个日志大小限制为。输入每个日志文件的最大大小 （以兆字节为单位）。

将日志的最大数目限制为。输入要创建和循环的日志文件的最大数目。

审核文件。显示一些选项，用于限制 Directory Proxy Server 审核文件的大小和最大数目。

将每个日志大小限制为。输入每个审核日志文件的最大大小 （以兆字节为单位）。

将日志的最大数目限制为。输入要创建和循环的审核日志文件的最大数目。

9. 单击 “保存”以保存更改。

   对象的名称现已显示在列表中。 Directory Proxy Server 配置已被修改，并提示您重新启动服务器。

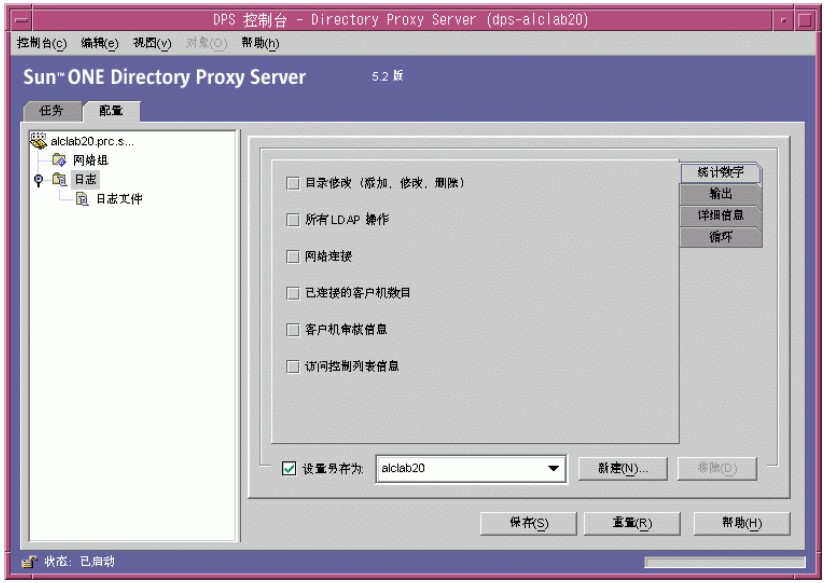
10. 重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

➤ 指定日志记录属性

在该步骤中，选择要用于日志记录消息的现有日志属性。

1. 访问 Directory Proxy Server 控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。
2. 选择 “配置”选项卡，然后在导航树中选择 “日志”。

   右侧窗格显示与当前系统属性指定的日志属性有关的信息。



3. 在 “设置另存为”下拉列表中，选择要使用的属性。
4. 单击 “保存”以保存更改。

   Directory Proxy Server 现已配置为按此配置中的定义记录消息。 Directory Proxy Server 配置被修改，并提示您重新启动服务器。
5. 选择 “任务”选项卡并重新启动服务器，如第 62 页上的 “重新启动 Directory Proxy Server”中所述。

监视日志

配置 Directory Proxy Server 以记录日志消息后，则可以通过查看日志消息来监视 Directory Proxy Server 活动。通过检查日志文件，您可以监视 Directory Proxy Server 操作的多个方面。

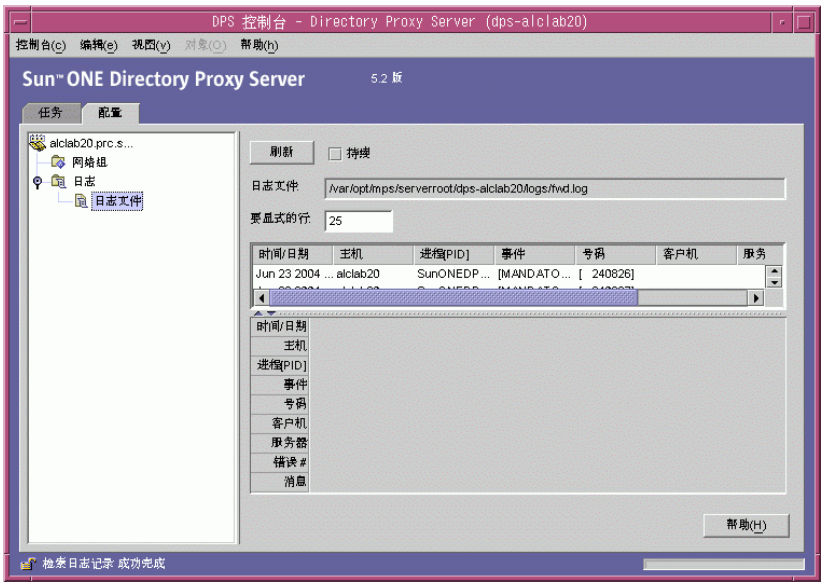
Directory Proxy Server 控制台提供了查看日志文件内容的简便机制。选择要查看的日志文件的内容是以表的形式显示的。该表处于拆分状态；上部的窗格以表格形式显示日志记录，下部的窗格详细显示当前选定的记录。每条日志记录包含的信息有：记录消息的日期和时间、消息的严重性以及日志的一般描述等。

打开日志文件进行查看后，便可以通过指定要显示的记录或条目数来部分读取其内容。

➤ 查看文件中的日志记录

1. 访问 Directory Proxy Server 控制台，如第 51 页上的 “访问 Directory Proxy Server 控制台”中所述。
2. 选择 “配置”选项卡，然后在导航树中展开 “日志”。
3. 选择 “日志文件”。

   右侧窗格显示记录到文件中的日志项的查看选项。可以选择当前日志属性中指定的任何日志文件； Directory Proxy Server 可包含单独的日志记录和审核信息文件 （如果这样配置）。



表格元素的描述如下：

刷新。读取日志并在下面的表中显示记录。

持续。选择该设置，可将该视图持续刷新为最新的日志记录。

日志文件。显示当前正在查看的文件的名称。

要显示的行。指定将从日志文件中读取的最大行数。

第 12 章

配置安全性

Directory Proxy Server 支持 SSL/TLS，以便在其客户机和后端目录服务器之间进行安全通信，详细信息，请参阅：

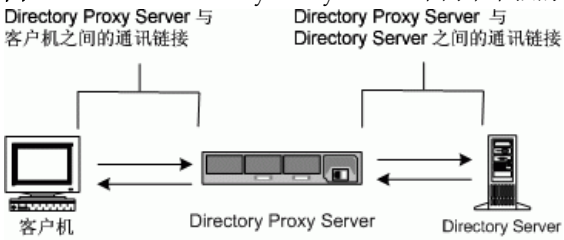
- 第 160 页上的 “准备设置 SSL 和 TLS”
- 第 161 页上的 “设置 SSL 通信”

本章假设您熟悉以下概念：

- 公共密钥加密
- 安全套接字层 (SSL) 协议
- Intranet、 Extranet 和 Internet 安全性
- 数字证书在企业中的作用

Directory Proxy Server 有两个可单独配置的通信链接。每个通信链接都可以是明文，也可以使用传输层安全性 (TLS) 或安全套接字层 (SSL) 协议进行加密。由于可以使用两个单独的通信链接，所以您可以在 LDAP 客户机和 Directory Proxy Server 之间以及 Directory Proxy Server 和 LDAP 目录之间配置启用 TLS 或 SSL 的通信。图 12-1 说明了 Directory Proxy Server 的此项功能。

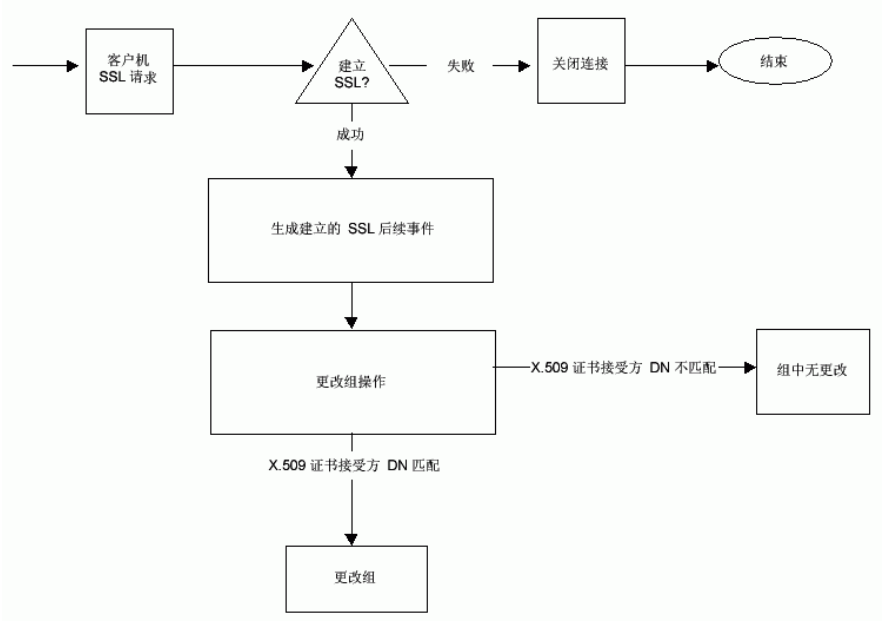
图 12-1 Directory Proxy Server 中两个单独的通信链接



Directory Proxy Server 可以验证客户机和服务器证书，条件是被验证的证书的受信任根 CA 证书已安装，并且可由 Directory Proxy Server 使用。

图 12-2 说明了 Directory Proxy Server 如何在 SSL 会话建立之后验证客户机提供给它的证书。

图 12-2 基于证书的客户机验证



准备设置 SSL 和 TLS

设置 SSL 和 TLS 需采用不同的方法，具体取决于您是使用内部安全设备、外部硬件设备还是两者都使用。本节将向您说明如何完成此设置。

为内部安全设备设置 SSL 或 TLS

要为内部安全设备设置 SSL 或 TLS，必须申请并安装证书。要申请证书，请运行“证书申请向导”。要安装证书，请运行 “证书安装向导”。出现提示时，请指定您希望在内部安全设备上安装证书。

为外部安全设备设置 SSL 或 TLS

要为外部安全设备（如 FORTEZZA）设置 SSL，请首先请安装外部设备制造商提供的 PKCS #11 模块。然后运行 “证书申请向导”，出现提示时，指定外部安全设备。

为内部和外部安全设备设置 SSL

企业中的某些服务器和客户机可能只使用内部安全设备，而其他的则可能同时使用内部和外部安全设备。如果服务器需要与同时运行内部和外部安全设备的产品进行通信，那么请*两次*运行 “证书申请向导”。首次使用期间，当出现提示时，请指定内部安全设备。在第二次使用期间，当出现提示时，请指定外部安全设备。

设置 SSL 通信

一般说来，要为 Directory Proxy Server 设置启用 SSL 的通信，需执行以下步骤：

- 为 Directory Proxy Server 安装服务器证书
- 在 Directory Proxy Server 和客户机之间建立 SSL 连接
- 在 Directory Proxy Server 和 LDAP 服务器之间建立 SSL 连接

为 Directory Proxy Server 安装服务器证书

在申请和安装证书时，需使用两个向导。可以使用 “证书申请向导”来申请新服务器证书或续订正在使用中的证书。可以使用 “证书安装向导”来安装您从*证书授权机构* (CA) 收到的证书。首次使用 “证书申请向导”时，它还将为您创建并安装*密钥和证书数据库*。

要为 Directory Proxy Server 安装服务器证书，请执行以下过程：

- 第 162 页上的 “生成服务器证书申请”。
- 第 163 页上的 “发送服务器证书申请”。
- 第 164 页上的 “安装证书”。
- 第 165 页上的 “安装 CA 证书或服务器证书链”。
- 第 166 页上的 “备份和恢复证书数据库”。

SSL 证书

Directory Proxy Server 可以安装三种类型的证书：服务器证书、服务器证书链，或受信任的 CA 证书。

*服务器证书*是仅与相应服务器关联的单一证书。它向客户机标识您的服务器。必须向 CA 申请这种类型的证书。要获取并安装服务器证书，请生成一份申请并将其发送给 CA。然后安装证书。

*服务器证书链*是您公司的内部证书服务器或已知 CA 自动为您生成的证书的集合。如果要进行标识身份证明，那么链中的证书可以追溯到原始的 CA。每当您获取或安装新服务器证书时，都需要提供此证明。

*受信任的 CA 证书*是您公司的内部证书服务器或已知 CA 自动为您生成的单一证书。受信任的 CA 证书用于验证客户机。

要获取受信任的 CA 证书，请首先访问内部证书服务器或 CA 的 Web 站点。复制必要的证书信息并将其保存到文件。然后使用 “证书安装向导”来安装证书。

可以在一台服务器上安装任意数量的 SSL 证书。在为目录服务器的实例安装 SSL 时，需要至少安装一个服务器证书和一个受信任的 CA 证书。

➤ 生成服务器证书申请

可以使用 Directory Proxy Server 生成证书申请，然后可以将该证书申请提交给证书授权机构 (CA)。

1. 在 Directory Proxy Server 导航树中，选择需要使用 SSL 加密的服务器实例。
2. 双击该服务器实例或单击 “打开”，以便打开服务器实例的管理窗口。
3. 从 “控制台”菜单中，选择 “安全” > “管理证书”。

   您也可以单击 “管理证书”任务。

   如果安全设备没有口令，则系统会提示您输入新口令。
4. 单击 “申请”，打开 “证书申请向导”。
5. 选择 “手动申请证书”，然后单击 “下一步”。

6. 输入申请的信息：

   服务器名称。（可选）输入您正在为其申请证书的机器的全限定主机名。

   组织。（可选）输入您的组织的名称。

   组织单位。（可选）输入您的分部、部门或其他组织单位。

   市 / 县。（可选）输入您的组织单位所在的城市或区县。

   省 / 自治区。（可选）输入您的组织单位所在的省份或自治区。

   国家 / 地区。（可选）从下拉菜单中选择您的组织单位所在的国家或地区。

   您可以使用以下按钮在申请表的两个视图之间切换：

   显示 DN。单击此按钮可显示识别名 (DN) 格式的申请者信息。只有当您在字段中输入信息时，才可以看到此按钮。

   显示字段。单击此按钮可在字段中显示申请者信息。只有您以 DN 格式输入信息时，才可以看到此按钮。

7. 单击 “下一步”。

8. 输入将存储此证书的安全设备的口令。

   如果您正在使用内部 （软件）安全设备，则输入的就是密钥和证书数据库的口令。如果您正在使用外部 （硬件）模块，则输入的将是您的智能卡或其他安全设备的口令。

9. 单击 “下一步”。

10. 选择下列选项之一：

    复制到剪贴板。单击以将您的证书申请复制到剪贴板。

    保存到文件。单击以将您的申请保存为文本文件。将提示您选择文件的名称和位置。

11. 单击 “完成”，关闭 “证书申请向导”。

➤ 发送服务器证书申请

生成服务器证书申请后，请将其发送到 CA 以进行处理。许多 CA 允许您通过其 Web 站点提交证书申请。其他的 CA 可能要求您向它们发送包含申请的电子邮件。

1. 使用电子邮件程序创建新的电子邮件。

2. 将证书申请粘贴到电子邮件中。

   如果您将证书申请保存到文件，那么请在文本编辑器中将其打开。将申请复制并粘贴到电子邮件的正文中。

   如果您将证书申请复制到剪贴板，那么请将其粘贴到电子邮件的正文中。

3. 输入申请的主题和收件人。取决于您正在使用的 CA，主题和收件人的类型会有所不同。有关详细信息，请参阅您的 CA Web 站点。

4. 将电子邮件发送到 CA。

提交申请后，必须等待 CA 对您的证书进行响应。取决于 CA 的不同，往返时间会有很大不同。如果您的公司具有内部 CA，则可能只需要一两天即可接收到您的证书。如果您正在使用外部 CA，则可能要花几个星期才能收到该 CA 对您申请的响应。

➤ 安装证书

取决于 CA 的不同，您可能会以电子邮件的形式收到证书，或者可能需要从 CA 的 Web 站点检索证书。具有证书后，您便可以将其备份并安装。

1. 在文本文件中保存您从 CA 收到的证书数据。

   如果您丢失了证书数据，则可以使用此备份文件重新安装证书。

2. 在 Directory Proxy Server 导航树中，选择您希望在其上安装证书的服务器实例。

3. 单击 “打开”，打开服务器实例的管理窗口。

4. 在 “任务”选项卡上，单击 “管理证书”任务按钮。

   也可以打开 “控制台”菜单，然后选择 “安全” > “管理证书”。

5. 单击 “服务器证书”选项卡。

6. 指定存储该证书的位置。

   如果希望将此证书存储在内部安全设备上，请从 “安全设备”下拉列表中选择内部 （软件），然后单击 “安装”。

   如果希望将此证书存储在外部硬件设备上，请从 “安全设备”下拉列表中选择设备，然后单击 “安装”。

7. 输入证书的位置或输入证书的文本。

   在该本地文件中。如果您的证书存储在系统上的文本文件中，请输入该文件的完整路径。

   在以下编码文本块中。如果您将证书复制到剪贴板中，请通过从 “剪贴板”按钮单击 “粘贴”，将证书的文本粘贴到文本字段中。

8. 单击 “下一步”。

   如果您上面输入的证书信息是有效的，则会看到包含该证书详细信息的页面。

9. 验证证书信息是否正确，然后单击 “下一步”。

10. 输入证书的名称，然后单击 “下一步”。

11. 输入将持有此证书的安全设备的口令。

    如果您在内部 （软件）安全设备上安装证书，请输入密钥和证书数据库的口令。如果您在外部 （硬件）安全设备上安装证书，请输入该设备的口令。

12. 单击 “完成”。

➤ 安装 CA 证书或服务器证书链

1. 从 CA 获取 CA 证书或服务器证书链。

2. 在 Directory Proxy Server 导航树中，选择您希望在其上安装 CA 证书的服务器实例。

3. 单击 “打开”，打开服务器实例的管理窗口。

4. 在 “任务”选项卡上，单击 “管理证书”任务按钮。

   也可以打开 “控制台”菜单，然后选择 “安全” > “管理证书”。

5. 选择 “CA 证书”选项卡，然后单击 “安装”。

6. 输入证书的位置或输入证书的文本：

   在该本地文件中。如果证书存储在系统上的文本文件中，请输入该文件的完整路径。

   在以下编码文本块中。如果您将证书复制到剪贴板中，请通过从 “剪贴板”按钮单击 “粘贴”，将证书的文本粘贴到文本字段中。

7. 单击 “下一步”。

   如果您上面输入的证书信息是有效的，则会看到包含该证书详细信息的页面。

8. 验证证书信息是否正确，然后单击 “下一步”。

9. 输入证书的名称，然后单击 “下一步”。

10. 为该证书选择信任选项：

    接受客户机的连接。如果希望信任此 CA 颁发的客户机证书，请选中此框。

    建立到其他服务器的连接。如果希望信任此 CA 颁发的服务器证书，请选中此框。

11. 单击 “完成”。

备份和恢复证书数据库

每当您安装证书时，都应该备份证书数据库。如果数据库遭到损坏，则可以从此备份中恢复证书信息。

➤ **备份证书数据库**

1. 打开服务器根文件夹。
2. 将 `alias` 文件夹中的所有文件复制到其他位置 （最好选择在不同的磁盘上）。

   该文件夹包含证书以及信任数据库的专用密钥。

➤ **从备份中恢复证书数据库**

1. 将备份文件复制到服务器根文件夹的 `alias` 子文件夹中。

警告 如果从备份中恢复证书数据库，则备份后安装的任何证书都将丢失。恢复证书数据库之前，要确保您拥有所有证书的副本，以便需要时重新安装。

在 Directory Proxy Server和客户机之间建立 SSL 连接

要在 Directory Proxy Server 和 LDAP 客户机之间建立 SSL 连接，请执行本部分介绍的过程。

➤ 将 Directory Proxy Server CA 证书添加到客户机信任数据库中

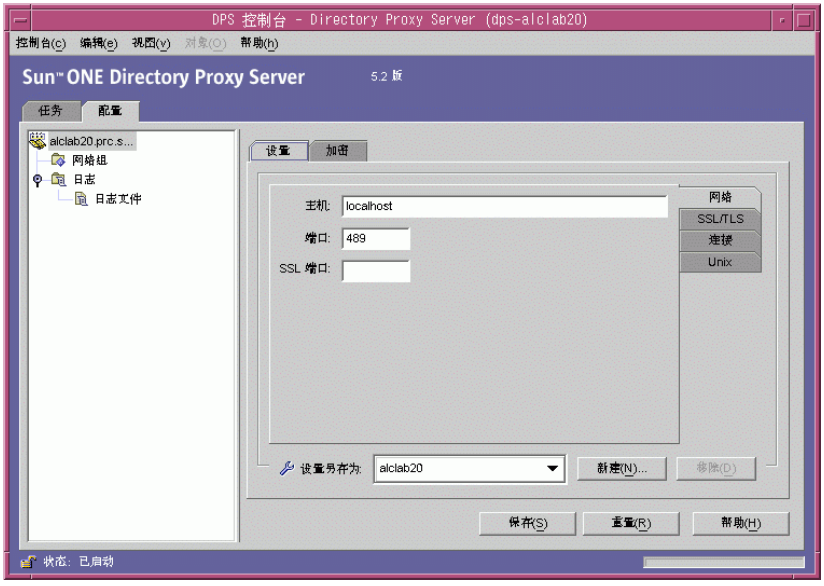
注 只有在客户机验证服务器证书时，该步骤才是必需的。所有 Netscape 和 Sun 客户机都要进行验证。但是，也有不进行验证的客户机。在这种情况下，设置信任不是必需的。

当 Directory Proxy Server 向 LDAP 客户机出示其证书时，客户机试图验证证书的有效性。作为此验证过程的一部分，客户机会检查颁发该证书的 CA 是否受客户机信任。因此，颁发了 Directory Proxy Server 服务器证书的 CA 根证书必须安装在客户机的信任数据库中。

在安装 Directory Proxy Server 服务器证书的最后一个步骤中，将 Directory Proxy Server CA 证书复制到文本文件中。遵循每个客户机应用程序的文档，并在其信任数据库中安装 CA 证书。

➤ 对 Directory Proxy Server 系统配置进行更改

通过 Directory Proxy Server 控制台窗口中的 “设置” 和 “加密” 选项卡，您可以为 Directory Proxy Server 定义启用 SSL 的通信条件。有关详细信息，请参阅第 69 页上的 “创建系统配置实例”。



对相应的系统配置实例进行以下更改，并保存所作的更改。

- 在 “设置”选项卡中，指定 “SSL 端口”字段中的值。Directory Proxy Server 将侦听您为 LDAPS （通过 SSL 的 LDAP）连接指定的端口号。缺省情况下，Directory Proxy Server 不侦听来自 LDAPS 客户机的连接。该值必须存在，以允许来自客户机的 LDAPS 连接，这些客户机使用备用端口 636 方法建立 TLS/SSL。该值必须不同于 “端口”字段中的值。（该选项还需要 “加密”选项卡上的 TLS/SSL 配置。）

  如果您需要查看参数的描述，请单击 “帮助”按钮。

- 在 "SSL/TLS" 选项卡中，指定所有需要的信息。

  如果您需要查看参数的描述，请单击 “帮助”按钮。

➤ **对 Directory Proxy Server 网络组进行更改**

Directory Proxy Server 使用网络组来标识客户机，并确定它们对包含在 LDAP 目录中的信息的访问特权；有关详细信息，请参阅第 79 页上的 “创建和管理组”。

在您配置的每个组中，设置 “加密”选项卡中的相应选项，以表明您是否希望强制客户机在发送任何 LDAP 操作之前开始 TLS 会话、让客户机自己决定，还是不允许客户机开始 TLS 会话。例如，您可能希望启用 “客户机可请求 SSL”和 “客户机必须建立 SSL 会话”选项。有关 “加密”选项卡中显示的选项的详细信息，请参阅第 84 页上的 “在 Directory Proxy Server 中创建网络组”中的步骤 9。

如果启用了跟随引荐，则应该检查 “引荐 SSL 策略”。通过选择窗口左侧列表中的 “引荐”来启用跟随引荐。

Directory Proxy Server 可以遵循后端服务器返回的引荐。返回的 LDAP URL 必须是 RFC 2255 格式。如果没有给出主机端口，则客户必须对要联系的相应 LDAP 服务器有一定了解。

Directory Proxy Server 将不具有主机或端口号的 LDAP URL 解释为颁发该引荐的相同主机的引荐。例如：

`ldap:///dc=central,dc=sun,dc=com`	对具有不同基的相同主机、端口的引荐。
`ldap://:10389/`	对相同主机但不同端口的引荐。
`ldap://host/`	对缺省端口 389 上的主机 “host”的引荐。

在 Directory Proxy Server 和 LDAP 服务器之间建立 SSL 连接

要在 Directory Proxy Server 和 LDAP 服务器之间建立 SSL 连接，请执行本部分介绍的过程。

➤ **安装 CA 证书或服务器证书链**

如果您希望 Directory Proxy Server 验证 LDAP 服务器提供给它的证书，则此步骤是必需的。有关详细信息，请参阅第 165 页上的 “安装 CA 证书或服务器证书链”。

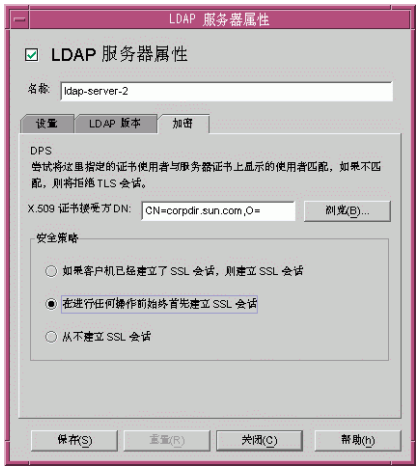
➤ **将 Directory Proxy Server CA 证书添加到 LDAP 服务器的信任数据库中**

当 Directory Proxy Server 向 LDAP 服务器出示其证书时，该服务器试图验证证书的有效性。作为此验证过程的一部分，服务器检查颁发 Directory Proxy Server 证书的 CA 是否受服务器信任。因此，颁发了 Directory Proxy Server 证书的 CA 的根证书必须安装在 LDAP 服务器的信任数据库中。

在安装 Directory Proxy Server 服务器证书的最后一个步骤中，将 Directory Proxy Server CA 证书复制到文本文件中。遵循每个 LDAP 服务器的文档，并在其信任数据库中安装 CA 证书。如果正在使用 Sun Java System 目录服务器，则可以使用 “管理证书向导”（该向导可以从目录服务器控制台的 “任务”选项卡启动），将 CA 证书添加到目录服务器的信任数据库中。

➤ 对 LDAP 服务器属性进行更改

通过 “LDAP 服务器属性”窗口中的 “加密”选项卡，您可以为每个 LDAP 服务器定义启用 SSL 的通信条件。有关详细信息，请参阅第 119 页上的 “创建 LDAP 服务器属性对象”。



对相应的 LDAP 服务器属性对象进行以下更改，并保存所作的更改。

- 将 “安全策略”选项设置为相应的值，以便 Directory Proxy Server 始终与后端服务器建立 SSL/TLS，而绝不与后端服务器建立 TLS/SSL，或者当客户机对 Directory Proxy Server 执行相同操作时与后端服务器只建立 SSL/TLS。
- 将 “X.509 证书接受方 DN”字段设置为 LDAP 服务器的证书接受方名称（X.509 证书中的接受方特性）。如果已指定，则 Directory Proxy Server 将尝试匹配该证书接受方与 LDAP 服务器证书的现有接受方，如果不匹配，则拒绝 TLS 会话。（此特性允许 Directory Proxy Server 对它正在连接的 LDAP 服务器进行验证。如果未设置此特性， Directory Proxy Server 就会接受任何名称。）

第 IV 部分

附录

Directory Proxy Server 决策功能

本附录描述了 Directory Proxy Server 中针对某些特定功能的控制流。其中包括：

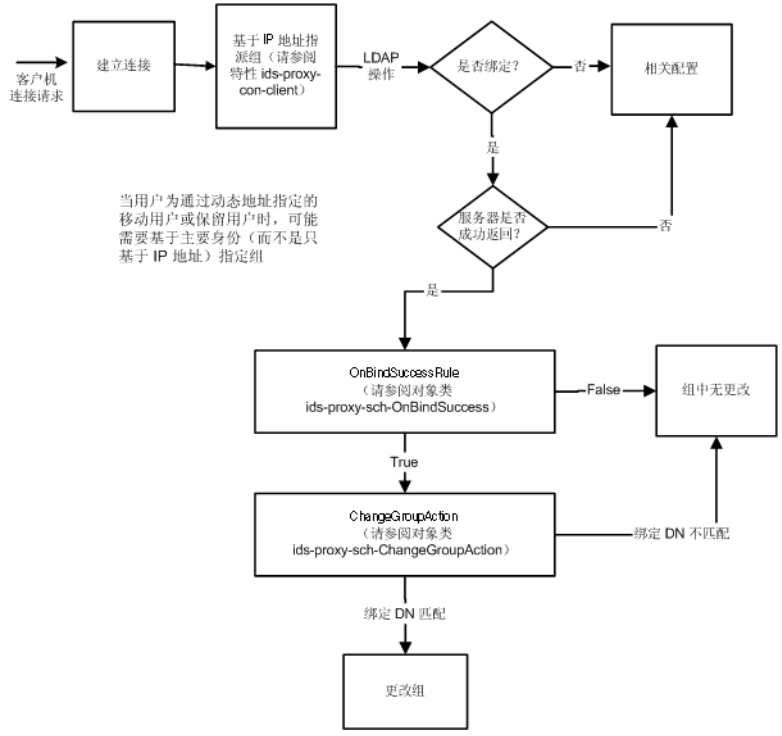
连接时建立组

当客户机与 Directory Proxy Server 建立连接时，它将检查 `ids-proxy-sch-NetworkGroup` 对象条目中的 `ids-proxy-con-Client` 特性，直到找到一个匹配项。将按照 `ids-proxy-con-priority` 特性所定义的最高优先级到最低优先级的顺序对 `ids-proxy-sch-NetworkGroup` 对象进行尝试。Directory Proxy Server 将客户机放在其 `ids-proxy-con-client` 特性匹配客户机的 IP 地址的第一个组中。如果找不到匹配的组，则关闭连接。

绑定时更改组

当客户机最初进行连接时，根据其 IP 地址将它置于一个组中。当客户机绑定到目录时，它可以移动到具有不同访问控制的不同组。要实现这一功能，初始组对象必须包括规则对象，在进行成功绑定操作时，将对该规则对象进行评估。如果该规则的值为 `TRUE`，则可以执行更改组操作将客户机移动到不同的组。图 A-1 显示了此功能。

图 A-1 绑定时更改组



配置 “绑定时更改组”

以下步骤说明了如何配置 Directory Proxy Server，以使其使用简单的绑定验证机制通过 "cn=Directory Manager" 在成功绑定时更改组。

➤ 配置 “绑定时更改组”

1. 创建一个新网络组，在成功进行绑定时用户 cn="Directory Manager" 将移到其中。有关详细信息，请参阅第 84 页上的 “创建组”。如果用户只有通过将其更改到组，才能成为该组的一部分，那么请在 “网络组”面板的 “网络”选项卡中设置 “无 IP 绑定”。此外，还要确保此组排在允许某些 IP 绑定的所有其他网络组后面。

2. 创建一个新 “更改组”操作。有关详细信息，请参阅第 142 页上的 “创建操作对象”。将 “更改为”设置为您在步骤 1 中创建的组的名称。将 “如果 DN 匹配”设置为 "cn=Directory Manager"。也可以将所有其他的 （即， ".*"）设置为 “无”（不更改组）。

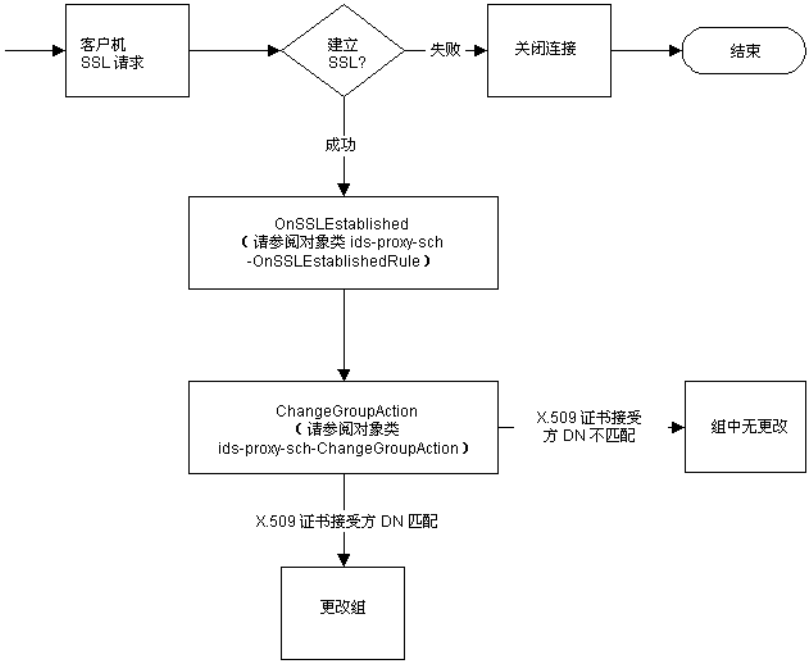
3. 创建绑定后续事件。有关详细信息，请参阅第 134 页上的 “创建事件对象”。在 “操作” 选项卡上，将其设置为您在步骤 2 中创建的更改组操作。在 “条件” 选项卡上，选择 “基于口令的绑定”。

4. 在步骤 1 中创建的 “网络组” 的 “事件” 选项卡上，选择您在步骤 3 中创建的 “绑定后续事件”。有关详细信息，请参阅第 107 页上的 “修改组”。

建立 TLS 时更改组

建立 TLS 时更改组类似于绑定时更改组机制，当客户机成功建立 TLS 会话时，可以更改组。当客户机建立 TLS 时，将评估 “SSL 已建立” 规则，此后将执行 “更改组” 操作。图 A-2 显示了此功能。

图 A-2 建立 TLS 时更改组



高可用性设置

如果您配置了一个以上的后端目录服务器，那么就可以设置 Directory Proxy Server，使其在其中一台后端服务器发生故障的情况下在这些服务器之间进行负载平衡，并将故障转移到另一台服务器。为了做到这一点，必须创建 “负载平衡属性”（请参阅第 124 页上的 “负载平衡属性”），并将它包括在您需要对其进行负载平衡的组对象中。您还需要为每一台后端服务器创建 “LDAP 服务器属性”（请参阅第 119 页上的 “LDAP 服务器属性”），并将它包括在 “负载平衡属性”中。在 “负载平衡属性”对象中，必须指定每一台后端服务器应该处理的负载量占总负载的百分比。进行了此项设置，在其中一台后端目录服务器发生故障的情况下，Directory Proxy Server 将在它们之间重新分配负载。在第一台服务器发生故障的情况下，它将客户机的故障从一台服务器转移到另一台服务器。如果其本身和 LDAP 服务器之间的网络链接发生故障或者如果 LDAP 服务器没有响应，那么 Directory Proxy Server 也将进行故障转移。

注 如果客户机使用 SASL 机制进行绑定，则 Directory Proxy Server 不能进行故障转移。

跟随引荐

可以设置 Directory Proxy Server，以使其为那些自身不能跟随引荐的 LDAPv2 客户机跟随引荐。后端 LDAP 目录服务器必须能够发送引荐，即，它必须支持 LDAP v3 标准。配置 Directory Proxy Server，以使其在自身和后端 LDAP 服务器之间使用 LDAP v3，以便 Directory Proxy Server 从目录服务器接收引荐。然后，设置组的引荐和持续引荐策略。

Directory Proxy Server常见问题、功能和疑难解答

本附录包含有关 Directory Proxy Server 的有用信息。它包含常见问题 (FAQ) 的解答、某些 Directory Proxy Server 功能的说明和疑难解答信息。

本附录包含以下几个部分：

Directory Proxy Server 常见问题

什么是 Directory Proxy Server？

Directory Proxy Server 是针对 LDAP 客户机和 LDAP 服务器的 LDAP 代理。基于 Directory Proxy Server 配置中定义的规则，来自 LDAP 客户机的请求被转发到 LDAP 服务器。来自服务器的结果也基于配置中定义的规则被传递回客户机。此过程对于连接到 Directory Proxy Server 的客户机是完全透明的，就像连接到任何 LDAP 服务器一样。

为什么需要 Directory Proxy Server？

许多企业希望使其目录信息的某些部分对于外部可见，而保留其他部分的目录信息为内部专有。利用 Directory Proxy Server，您可以轻松地实现此目标，而无需为外部客户机分配目录口令。 Directory Proxy Server 还可以被用作企业目录服务的具有负载平衡和故障转移功能的高可用性解决方案。

还提供了其他安全功能，例如防止拒绝服务的攻击和搜索限制。

Directory Proxy Server 支持什么版本的 LDAP 协议？

Directory Proxy Server 支持使用 LDAPv2 或 LDAPv3 协议的 LDAP 客户机或链式 LDAP 服务器。

Directory Proxy Server 是否支持安全验证和加密？

Directory Proxy Server 支持 SSLv3 服务，以便使用证书进行基于公共密钥的数据加密。 LDAP 客户机可用的安全验证和加密可以使用安全的 LDAP 端口或 Internet 传输层安全性 (TLS) 模型，该模型使用 Diffie-Hellman、数字签名标准 (DSA) 和 Triple-DES 算法。

Directory Proxy Server 能否与任何支持 LDAP 的 Directory Server 一起使用？

Directory Proxy Server 可与任何遵守 LDAP 协议的 Directory Server 一起使用。某些目录产品供应商在其市场宣传中声称实现了 LDAP，但事实上常常是另一码事。已经使用 Sun Java System Directory Server 对 Directory Proxy Server 进行了彻底的测试。

是否有配置公用程序可用来配置 Directory Proxy Server？

Directory Proxy Server 包括一个基于 Java 的 GUI （控制台），可用它来配置 Directory Proxy Server。该控制台使用 Directory Server 来存储它生成的配置。

功能

Directory Proxy Server 是否可以防止拒绝服务的攻击？

可以。您可以限制每个连接处理的同时操作数量，每个连接所允许的操作数量，同时连接的总数，每个定义组 （网络、子网或基于绑定 DN）的最大同时连接数，以及单一 IP 地址的最大同时连接数。

Directory Proxy Server 支持 “反向”代理吗？

从严格意义上来讲，Directory Proxy Server 是一种反向代理；然而，LDAP 协议不支持反向代理的概念。

Directory Proxy Server 是否可以防止 LDAP 目录拖网？

可以。拖网是指非常广泛的查询，被设计为用于下载您的大部分目录，这是许多站点希望禁止的行为。 Directory Proxy Server 可以以许多方式来禁止或限制拖网：

- 搜索的范围可以被限制为目录树的单个层次，完整的子树可以隐藏起来，可以对为响应查询而返回的条目数量设置硬性限制。
- 可以禁止不等号搜索，从而不允许基于排除而返回许多结果的搜索，也可以按长度限制子字符串搜索；例如，禁止搜索以字母 A-Z 开头的姓氏的所有条目。
- Directory Proxy Server 也可以配置为拒绝没有索引的搜索。没有索引的搜索效率比较低，并可能对性能造成负面影响。

Directory Proxy Server 是否可以对查询进行自动负载平衡？

Directory Proxy Server 支持在一组后端 LDAP 服务器之间进行自动服务器负载平衡。Directory Proxy Server 还支持在主 LDAP 服务器发生故障的情况下将故障自动转移到辅助 LDAP 服务器。

一台 Directory Proxy Server 可以对多少台 Directory Server 进行负载平衡？

目录服务器的性能需求及 Directory Proxy Server 进行的工作复杂性决定了 Directory Proxy Server 应该能够进行负载平衡的目录服务器的最佳数量。例如，如果 Directory Proxy Server 正在处理复杂的工作，如特性重命名，则配置 Directory Proxy Server 进行负载平衡处理的目录服务器数量应该减少。可以考虑添加更多 Directory Proxy Server 单元以补偿复杂的 Directory Proxy Server 配置对性能可能造成的影响。

是否可以过滤搜索请求？

可以。可以配置 Directory Proxy Server 以拒绝尝试搜索特定特性的搜索。此外，您可以配置 Directory Proxy Server 来修改传入的搜索请求，以符合指定的最低搜索标准、搜索范围以及时间限制。

是否可以过滤搜索结果？

可以。可以根据返回条目的数量和结果集合中包含的特性对结果进行过滤。也可以基于条目 DN 或内容对搜索结果条目进行过滤。

访问组是如何定义的？

基于客户机的网络地址，为客户机提供了对目录的不同访问级别。因此，可以将不同访问级别授予公司防火墙外的客户机、防火墙内的客户机、行政子网上的客户机甚至单台机器。此外，在客户机成功完成 LDAP 绑定操作或建立 SSL 会话之后，还可以更改访问级别。

Directory Proxy Server 是否支持受保护的口令验证？

可以。通过使用 SASL 机制，可以实现各种受保护的口令验证方案。这些机制必须由后端目录服务器提供支持。 Directory Proxy Server 不支持具有连接保护的 SASL 机制和 SASL EXTERNAL 机制。

Directory Proxy Server 是否自动跟随引荐？

跟随引荐是可以基于访问组来进行配置的。可以配置各种访问组以自动跟随引荐、返回引荐或放弃引荐。

Directory Proxy Server 是否缓存搜索结果信息？

Directory Proxy Server 不支持搜索结果缓存。

Directory Proxy Server 是否可以重命名特性？

Directory Proxy Server 可以在客户机和服务器之间透明地重命名特性名称。

疑难解答

我如何分析连接尝试的日志？

可以配置 Directory Proxy Server 以使用 `syslog` 或写入到指定的日志文件中。可以通过以下 ftp 免费从斯坦福大学获得一个称为 swatch 的流行 UNIX 公用程序：`ftp://ftp.stanford.edu/general/security-tools/swatch`。可以使用 Swatch 监视 Directory Proxy Server 生成的日志文件，并在发生定义的事件时通知管理员。

我已经将 Directory Proxy Server 配置为跟随引荐。然而，当我使用 LDAPv2 客户机执行搜索时，出现错误 32 （没有这样的对象）或某些其他错误。

Directory Proxy Server 为了从后端服务器接收引荐，必须使用 LDAPv3。应确保对每一个 LDAP 服务器属性选择了 “仅 LDAP 版本 3”。

我在日志文件中发现，即使所有后端服务器都在正常运行，某些空闲的客户机连接也定期进行故障转移。

后端目录服务器使空闲连接超时，并将其关闭。 Directory Proxy Server 会对这些关闭的连接进行故障转移。您必须为 Directory Proxy Server 设置空闲连接超时。这将清理空闲和遗漏的客户机连接，并预防一种形式的拒绝服务攻击。

是否有办法限制包含存在过滤的搜索请求？

Directory Proxy Server 不限制客户机使用存在过滤。有两种间接方式来解决此问题：

- 将 `ids-proxy-con-forbidden-compare` 特性设置为您不希望被比较的特性名称。此方法限制性太强，因为它将拒绝同时包含 (mail=*) 和 (mail=Andy*) 过滤的搜索。
- 使用 `ids-proxy-con-size-limit` 特性和 `ids-proxy-sch-SizeLimitProperty`。由于存在过滤 (attrName=*) 始终生成相同的结果 （假设数据未更改），可以使用 `ids-proxy-con-size-limit` 和 `ids-proxy-sch-SizeLimitProperty` 来限制损坏。虽然 LDAP 不要求以给定顺序返回条目，但在大多数 （所有）实施方案下，结果集合都将以排序的顺序或以未排序的顺序返回，并且每次都相同。因此，如果使用大小限制来配置 Directory Proxy Server （使用 size-limit 特性或 SizeLimitProperty），则每次都将只返回这些集合的前 n 个。由于这 n 个条目只能有两组，因此极大地降低了对目录进行拖网的风险。

请注意，只要有可能， Directory Proxy Server 就试图在请求本身中设置此大小限制，因此，目录服务器将不会承担发送所有条目的负荷。

通过大小限制属性，您可以选择在必要时使用异常的大小限制。例如，假设您有一个条目 o=A，在此条目下有 400 个组织单元。在其中的每个组织单元下都有一些人。如果您希望客户机看到所有的组织单元，但每次只能看到 5 个人，那么您可以设置 `SizeLimitProperty`，以使其不限制基本 o=A 搜索和一级范围搜索。对于所有其他搜索，则限制为 5。

当我尝试执行一项任务或执行某些控制台功能时，获得错误消息，需要我确保管理服务器正常运行，并且允许该主机连接到管理服务器。

登录到正在管理 Directory Proxy Server 的管理服务器上，其控制台产生错误消息。可能需要启动管理服务器主机上的 Sun Java System 控制台。打开您在其中未能成功尝试调用任务的、正在管理 Directory Proxy Server 的管理服务器的服务器控制台。单击“配置”选项卡，然后单击“网络”选项卡。在“连接限制”下，确保不限制未能成功尝试管理 Directory Proxy Server 的 Sun Java System 控制台的主机访问管理服务器。有关详细信息，请参阅《*Sun Java System 控制台服务器管理指南*》。

Directory Proxy Server 启动配置文件

本附录包含有关 Directory Proxy Server 配置文件的信息。其中包括：

配置文件概述

`tailor.txt` 文件包含 Directory Proxy Server 定位其主配置所需的引导程序信息。此文件中的指令指示 Directory Proxy Server 是否将为其主配置使用其他文件，或者 Directory Proxy Server 是否将从 LDAP 服务器请求其主配置。缺省情况下，Directory Proxy Server 会在安装的实例目录的 `etc` 子目录中查找启动配置文件 `tailor.txt`。请注意：通过使用命令行参数 `-t`，可以命令 Directory Proxy Server 使用替代文件作为其启动配置文件。

作为支持高可用性配置的辅助手段，启动配置文件可以为主配置的检索列出多个联系点。联系点是在启动配置文件内通过利用两个关键字来描述的：`Begin` 和 `End`。Directory Proxy Server 将按照给定顺序依次地处理联系信息。 Directory Proxy Server 对每一个联系点的操作取决于给定联系点的类型 （LDAP URL 或到文件的绝对路径名称）。

对基于 LDAP-URL 的联系点， Directory Proxy Server 将尝试联系给定的主机。如果主机不愿意或无法返回配置，那么 Directory Proxy Server 将继续与其下一个联系点联系 （如果有）。如果主机返回配置，那么 Directory Proxy Server 将编辑返回的内容，然后开始执行主配置的指令，如果配置被视为无效，则结束其执行。

对基于文件的联系点， Directory Proxy Server 将尝试加载给定的文件作为其主配置。如果指定的配置丢失或被视为无效，则 Directory Proxy Server 将结束其执行。Directory Proxy Server 遇到基于文件的联系点后，将不会再尝试移到下一个联系点。

在 Directory Proxy Server 从 LDAP 主机检索其主配置的情况下， Directory Proxy Server 可以使用以下三种方法之一来绑定到主机：匿名、简单或通过使用 SASL。

*匿名绑定*是通过省略 configuration_bind_pw 和 configuration_bind_dn 指令来实现的。换句话说，您的启动配置联系信息将指定 configuration_url 指令，而不指定其他指令。

*简单绑定*是通过使用 configuration_bind_pw 和 configuration_bind_dn 指令来支持的。

*SASL 绑定*要求指定 sasl_bind_mechanism、 conguration_bind_pw 和下列指令之一 （只有一个）：configuration_bind_dn 或 configuration_username。

启动配置关键字

每一个枚举的联系点都使用关键字 Begin 来表示联系点条目的开始。反之，每个联系点条目都使用关键字 End 来结束。启动配置文件中规定的每个指令都用一行来表示。不能识别也不支持启动配置内的续行。配置的选项是通过一个选项来指定的，后面是冒号和三个一组的值。

configuration_url

configuration_url 选项指定 LDAP 目录服务器和存储 Directory Proxy Server 配置的目录中，条目的识别名或 LDIF 格式的本地文件。例如，如果 Directory Proxy Server 配置存储在主机 ldap.sun.com 的 LDAP 目录中，而 LDAP 服务运行在端口 389 上，并且 Directory Proxy Server 条目的识别名是 “ids-proxy-con-Server-Name=Directory Proxy Server”，则应将下列内容添加到配置文件中：

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
End
```

如果配置被保留在 LDAP 服务器中，那么您可能需要在 ids-proxy-con-Server-Name=Directory Proxy Server 后面指定一个后缀，以便保持与主机目录命名环境的兼容性。例如：

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server,
ou=services, dc=sun, dc=com
End
```

每个启动配置指令都应该在配置文件内指定为一个相邻的行。

注 不要将 configuration_url 示例中的换行理解为将换行符插入到配置文件中的指令。

如果将配置存储在 LDIF 格式的文件 （即 <server-root>/dps-<hostname>/etc/tailor.ldif）中，则应在配置文件中添加下列内容：

```
Begin
configuration_url:
file://<server-root>/dps-<hostname>/etc/tailor.ldif#ids-proxy-con-S
erver-Name=Directory Proxy Server
End
```

configuration_bind_dn

configuration_bind_dn 选项指定当 Directory Proxy Server 绑定到 configuration_url 选项中指定的 LDAP 服务器时所使用的识别名。 Directory Proxy Server 将使用此识别名，并使用 configuration_bind_pw 的值作为口令执行简单绑定。例如：

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
configuration_bind_dn: cn=Directory Manager
configuration_bind_pw: encrypte
End
```

如果 configuration_url 是 “文件”的形式，则不需要并忽略 configuration_bind_dn 选项。请注意：configuration_bind_dn 和 configuration_username 指令是互相排斥的。

configuration_bind_pw

使用 configuration_bind_pw 选项来指定在绑定到 LDAP 目录时所使用的口令。使用该指令来指定简单绑定或基于 SASL 的绑定所要使用的口令。为了保证安全性，必须防止配置文件被非法读取。如果 configuration_url 是 “文件”的形式，则不需要并忽略 configuration_bind_pw 选项。（有关示例，请参阅 configuration_bind_dn。）

configuration_username

configuration_username 选项指定当 Directory Proxy Server 绑定到 configuration_url 选项中指定的 LDAP 服务器时所使用的用户名。此选项只有在使用 SASL 绑定机制的情况下才使用。请注意：configuration_bind_dn 和 configuration_username 指令是互相排斥的。

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
configuration_username: administrator
configuration_bind_pw: encrypte
sasl_bind_mechanism: CRAM-MD5
End
```

sasl_bind_mechanism

可以将 sasl_bind_mechanism 选项设置为 CRAM-MD5 或 DIGEST-MD5，具体情况取决于您希望 Directory Proxy Server 使用的 SASL 绑定机制。如果没有此选项，Directory Proxy Server 将执行简单绑定或匿名绑定。 DIGEST-MD5 比 CRAM-MD5 提供了更高的安全级别，但 DIGEST-MD5 没有像 CRAM-MD5 那样被广泛地采用。

命令参考

本附录介绍与 Directory Proxy Server 相关的有帮助的命令行程序。

本附录包含以下几个部分：

dpsconfig2ldif

`dpsconfig2ldif` 公用程序用于下载 Directory Proxy Server 配置并将其保存到 LDIF 文件中。在以下位置可找到 `dpsconfig2ldif` 公用程序：

```
<serverroot>/bin/dps_utilities/dpsconfig2ldif
```

`dpsconfig2ldif` 公用程序需要两个参数：

参数	说明
-t *filename*	*Filename* 是至启动配置文件的路径。这通常是 etc 目录中的 tailor.txt 文件。
-o *filename*	在其中输出配置的文件的名称。

dpsldif2config

`ImportConfigLdif` 公用程序导入 dpsconfig2ldif 生成的 LDIF 文件。可在以下位置找到 `dpsconfig2ldif` 公用程序：

```
<serverroot>/bin/dps_utilities/dpsldif2config
```

dpsconfig2ldif 公用程序需要以下参数：

参数	说明
ldif	包含 Directory Proxy Server 对象选项的 LDIF 文件的名称：
-C	要创建的配置名称 （如果未指定，则为 “imported-configuration”）
-h	目录主机名 （如果未指定，则为 localhost）
-p	目录端口号 （如果未指定，则为 389）
-D	目录用户 dn （如果未指定，则为匿名绑定）
-w	目录用户口令 （如果未指定，则为匿名绑定）
-v	详细

ImportConfigLdif 导入三种类型的对象：

- 共享配置 （即，位于 “Directory Proxy Server 配置”节点下的 “主控制台拓扑树”中的那些对象）
- 共享系统属性
- 共享日志属性

“Configuration Name”参数仅适用于刚刚介绍的 “共享配置”对象。从 LDIF 文件中 “按原样”添加 “系统”和 “日志”属性。如果具有给定参数名的共享配置对象不存在，则此脚本将使用给定的参数名创建一个新配置。如果已经存在具有给定名称的配置，则不会发生导入。如果 “系统”和 “日志”属性已存在于目录中，则不会添加它们。

导入了配置后，则必须重新启动 “主控制台”才能在 “拓扑树”中查看该配置。为了开始使用配置， Directory Proxy Server 实例服务器必须将其本身分配给每个配置：通过 Directory Proxy Server 控制台中的 “网络组”节点来分配共享的 “配置”；通过 Directory Proxy Server 控制台中的系统节点来分配 “系统属性”（“设置另存为 ...”）；通过 Directory Proxy Server 控制台中的 “日志”节点来分配 “日志属性”（“设置另存为 ...”）。

前期条件

- 您正在运行 Directory Proxy Server 5 2004Q2。

后期条件

- 在导入的 LDIF 文件中忽略 `belongs-to` 特性。

术语表

有关本文档集中使用的术语完整列表，请参阅 *Java Enterprise System 术语表*，网址为：http://docs.sun.com/doc/816-6873。

索引

F

G

H

J

L

M

N

O

P

Q

R

S

T

W

X

Y

Z