Sun Java™ System

Web Proxy Server 4 .0.1
管理指南

2005Q4

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

文件号码 819-3162

目录

关于本指南

本指南介绍如何配置和管理 Sun Java™ System Web Proxy Server 4（以前称为 Sun™ ONE Web Proxy Server 和 iPlanet™ Web Proxy Server；以下称作 Sun Java System Web Proxy Server，或简称 Proxy Server）。

本前言包含以下各节：

目标读者

本指南专为生产环境中的信息技术管理员而编写。本指南假设读者熟悉以下方面的知识：

- 执行基本系统管理任务
- 安装软件
- 使用 Web 浏览器
- 在终端窗口发命令

本书的结构

本指南分为几个部分，每一部分分别就特定的领域和任务进行论述。下表列出了本指南的各个部分及其内容。

表 1　　指南的结构

部分	说明
第 1 部分 服务器基础知识	就 Proxy Server 及其管理进行概述： • 第 1 章“Sun Java System Web Proxy Server 简介” • 第 2 章“管理 Sun Java System Web Proxy Server”
第 2 部分 使用 Administration Server	就配置 Administration Server 首选项、管理用户和组、保障 Proxy Server 安全以及使用群集在服务器间共享配置进行详细说明： • 第 3 章“设置管理首选项” • 第 4 章“管理用户和组” • 第 5 章“使用证书和密钥” • 第 6 章“管理服务器群集”
第 3 部分 配置和监视 Proxy Server	就配置服务器首选项、设置访问控制以及监视服务器活动进行详细说明： • 第 7 章“配置服务器首选项” • 第 8 章“控制对服务器的访问” • 第 9 章“使用日志文件” • 第 10 章“监视服务器”
第 4 部分 管理 Proxy Server	就 Proxy Server 处理请求方面的有关概念和任务进行详细说明： • 第 11 章“代理和路由选择 URL” • 第 12 章“高速缓存” • 第 13 章“通过代理服务器过滤内容” • 第 14 章“使用反向代理服务器” • 第 15 章“使用 SOCKS” • 第 16 章“管理模板和资源” • 第 17 章“使用客户机自动配置文件”
第 5 部分 附录	介绍访问控制列表 (ACL) 文件语法以及服务器性能调节： • 附录 A“ACL 文件语法” • 附录 B“调节服务器性能”

文档约定

下表列出了本指南所采用的文档约定。

表 2　　印刷约定

元素	用法
文件及目录路径	采取 UNIX® 格式，以正斜杠分隔目录名。
安装根目录	以 *server_root* 表示。默认安装目录为 `/proxyserver4`。
*斜体*文字	保留未译的术语以及要强调的词、路径中的环境变量、占位符。
等宽文字	代码示例、文件名、路径名、命令名、编程语言关键字、属性。
新词术语强调	新词或术语以及要强调的词。
《书名》	书名

相关文档

可在以下网址获得 HTML 和 PDF 格式的 Sun Java System Web Proxy Server 4 文档：

http://docs.sun.com/app/docs/prod/s1.webproxys#hic 及
http://docs.sun.com/app/docs/prod/s1.webproxys?l=zh#hic

下表列出了每本指南中介绍的任务和概念。

表 3　　Proxy Server 文档

要了解有关以下内容的信息	参见
Proxy Server 发行版： • 软件和文档的最新信息 • 新特性 • 支持的平台和环境 • 系统要求 • 已知问题和解决方法	发行说明
执行安装及迁移任务： • 安装 Sun Java System Web Proxy Server • 从版本 3.6 迁移到版本 4	Installation and Migration Guide

表 3　　Proxy Server 文档

要了解有关以下内容的信息	参见
执行管理和操控任务： • 使用管理及命令行界面 • 配置服务器首选项 • 管理用户和组 • 监视和记录服务器活动 • 使用证书和公共密钥加密以确保服务器的安全 • 控制服务器访问 • 代理及路由选择 URL • 高速缓存 • 过滤内容 • 使用反向代理服务器 • 使用 SOCKS	管理指南 （以及产品随带的联机帮助）
创建自定义 Netscape 服务器应用程序编程接口 (NSAPI) 插件	NSAPI Developer's Guide
编辑配置文件	Configuration File Reference

联系 Sun 技术支持

如果您遇到通过本文档无法解决的技术问题，请访问以下网址：

http://www.sun.com/service/contacting

反馈

Sun 致力于提高其文档的质量，并十分乐意收到您的意见和建议。要分享您的意见，请访问 http://docs.sun.com，然后单击用于发送意见的链接。请务必在联机表格中提供文档标题和文件号码。提出意见时您还需要在表格中输入文件的英文文件号码和标题。本文件的英文文件号码是 819-3650，文件标题为《Sun Java System Web Proxy Server 4.0.1 2005Q4 Administration Guide》。

第三方 Web 站点引用

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。

服务器基础知识

第 1 章

Sun Java System Web Proxy Server 简介

本章将对 Sun Java™ System Web Proxy Server 进行概括介绍，其中简要说明了本发行版本的新增功能，并概述了用于管理、配置和操控 Proxy Server 的基于 Web 的用户界面。

本章包括以下各节：

关于 Sun Java System Web Proxy Server

Sun Java System Web Proxy Server 是在高性能 Internet 和内联网环境下实现 HTTP 高速缓存和加速的基础。Proxy Server 是一个功能强大的系统，用于高速缓存和过滤 Web 内容以及提高网络性能。它具备与整个网络基础结构的紧密集成、跨平台支持以及集中管理能力。作为一个网络流量管理器，它可以有效地对信息进行分配和管理，从而减少了网络流量和用户等待时间。借助 Proxy Server，还可以确保用户能够安全而富有成效地访问网络资源，因为它可为内容分配提供安全网关并起到 Internet 流量控制点的作用。

本发行版本的新增功能

Sun Java System Web Proxy Server 4 包括以下增强功能：

- 新式 HTTP 内核
- 支持 Linux 以及 Solaris™ x86 平台
- 在所有平台上均支持新式 SSL（安全套接字层）
- 在所有平台上均实现了多线程体系结构
- 改进了管理界面、图形用户界面，更加易于操控
- 新增了 NSAPI（Netscape 服务器应用程序编程接口）过滤器
- 提高了 LDAP（轻量目录访问协议）性能
- 提高了可伸缩性和性能
- 改进了内容过滤
- 实现了 `server.xml` 配置文件

可在 Proxy Server 发行说明中找到有关新特性和增强功能的更多信息，该文档位于以下网址：
http://docs.sun.com/app/docs/prod/s1.webproxys#hic 及
http://docs.sun.com/app/docs/prod/s1.webproxys?l=zh#hic

入门

Sun Java System Web Proxy Server 使用 Administration Server 和 Server Manager 的基于 Web 的用户界面进行管理和配置，可通过浏览器访问这些用户界面。Administration Server 用来管理系统上安装的所有 Proxy Server 实例的公共配置，而 Server Manager 用来配置单个服务器实例的设置。

本节包括以下主题：

注 要运行配置服务器所必需的 CGI 程序，必须在浏览器中启用 Cookie。

Administration Server 概述

Administration Server 是一个基于 Web 的用户界面，用于管理系统上安装的所有 Sun Java System Web Proxy Server 实例的公共配置。

启动了 Administration Server 之后（参见第 31 页的“启动 Administration Server”），可通过启动浏览器并输入 URL 来访问 Administration Server。该 URL 由安装期间所指定的主机名和端口号决定。例如：`http://myserver.mycorp.com:1234`。

可以将 Administration Server 的访问权限授予多个管理员。有关分布式管理的更多信息，参见第 40 页的“允许多个管理员”。

访问 Administration Server

1. 启动浏览器并输入相应的 URL，该 URL 反映了安装期间为 Administration Server 指定的主机名和端口号。例如：`http://myserver.mycorp.com:1234`。
2. 出现提示时，输入安装期间所指定的用户名和口令。将显示 Administration Server 的用户界面。

Administration Server 设置按照与特定任务相对应的选项卡进行组织。下表列出了 Administration Server 的选项卡，并对这些选项卡的用途进行了简要说明。

表 1-1 Administration Server 的选项卡

选项卡	用途
Servers	管理、添加、删除、迁移 Proxy Server
Preferences	关闭 Administration Server、编辑侦听套接字、配置超级用户访问、配置分布式管理（允许多个管理员）、自定义和查看访问及错误日志
Global Settings	配置目录服务、指定访问控制、配置 SNMP 主代理设置
Users and Groups	添加和管理用户、组以及组织单位
Security	创建新的信任数据库、申请和安装 VeriSign 及其他证书、更改密钥对文件口令、查看和管理已安装证书、添加或替换“证书撤销列表”(CRL) 和“已暴露密钥列表”(CKL)、管理 CRL 和 CKL、迁移 3.x 证书
Cluster	控制群集中的远程服务器、添加和删除远程服务器、修改服务器信息

不管您处于哪个选项卡或页面，都会显示以下按钮：

- **Version**——显示有关 Sun Java System Web Proxy Server 的版本信息
- **Refresh**——刷新当前页面
- **Help**——显示当前页面的联机帮助

有关使用 Administration Server 的更多信息，参见第 31 页的第 2 章“管理 Sun Java System Web Proxy Server”。另参见 Administration Server 选项卡和页面的联机帮助。

Server Manager 概述

Server Manager 是一个基于 Web 的用户界面，用于启动、停止和配置 Sun Java System Web Proxy Server 的单个实例。

访问 Server Manager

1. 访问 Administration Server，具体的操作说明请参见第 27 页的“Administration Server 概述”。Administration Server 将显示 "Servers" 选项卡。
2. 在 "Manage Servers" 页面中，单击所要管理的服务器实例的链接。将显示 Server Manager 用户界面。

Server Manager 设置按照与特定任务相对应的选项卡进行组织。下表列出了 Server Manager 的选项卡，并对这些选项卡的用途进行了简要说明。

表 1-2　Server Manager 的选项卡

选项卡	用途
Preferences	启动和停止服务器、查看服务器设置、恢复配置信息、配置系统首选项、调节 Proxy Server 性能、添加和编辑侦听套接字、管理 MIME 类型、管理访问控制、配置 ACL 和 DNS 高速缓存、配置 DNS 本地子域、配置 HTTP 保持活动设置、设置加密算法规模
Routing	启用和禁用服务器代理、设置路由选择首选项、转发客户机凭证、启用 Java IP 地址检查、创建和编辑自动配置文件、设置连接模式、更改默认 FTP 传输模式、设置 SOCKS 名称服务器 IP 地址、配置 HTTP 请求负载平衡
SOCKS	启动和停止 SOCKS 服务器，以及创建和管理 SOCKS 验证、连接及路由选择条目
URLs	查看、创建和管理 URL 映射及重定向

表 1-2　Server Manager 的选项卡

选项卡	用途
Caching	设置高速缓存细节、添加和修改高速缓存分区、在现有分区间移动区段、设置高速缓存容量、设置垃圾收集模式、调节高速缓存、调度垃圾收集、调节垃圾收集设置、配置特定资源的高速缓存、启用本地主机的高速缓存、更改文件高速缓存设置、设置高速缓存批量更新、查看有关记录的高速缓存 URL 的信息、配置 ICP 邻域中的代理服务器、创建和更新代理阵列成员列表、配置代理阵列成员、查看 PAT 文件中的信息
Filters	创建过滤器文件、设置内容 URL 重写、设置用户代理限制和请求阻止、抑制外出标头、设置 MIME 过滤器和 HTML 标记过滤器、按即时请求压缩内容
Server Status	查看日志文件、归档日志、设置日志首选项、生成报告、监视当前活动、配置和控制 SNMP 子代理
Security	创建新的信任数据库、申请和安装 VeriSign 及其他证书、更改密钥对文件口令、查看和管理已安装证书、添加或替换“证书撤销列表”(CRL) 和“已暴露密钥列表”(CKL)、管理 CRL 和 CKL、迁移 3.x 证书
Templates	创建、删除、应用和查看模板，以及删除资源

不管您处于哪个选项卡或页面，都会显示以下按钮：

- **Version**——显示有关 Sun Java System Web Proxy Server 的版本信息
- **Refresh**——刷新当前页面
- **Help**——显示当前页面的联机帮助

有时，您可能还会在 "Refresh" 按钮下面看到一个 "Restart Required" 链接。这表明已进行过更改，为此而要求重新启动服务器。要应用更改，请单击该链接，然后指定所需的操作。

有关使用 Server Manager 的更多信息，参见本指南中的相关任务。另参见 Server Manager 选项卡和页面的联机帮助。

配置文件

Sun Java System Web Proxy Server 的配置和行为由一组配置文件决定。在管理界面中配置的设置将会在这些配置文件中反映出来。还可以手动编辑这些文件。

这些配置文件位于 *instance_dir*/config 目录中，其中 *instance_dir* 是指服务器实例。config 目录包含用于控制不同组件的各种配置文件。配置文件的确切数目和名称取决于已启用或加载的组件。此目录始终包含四个对于服务器操作必不可少的配置文件。下表列出了这四个必备的配置文件及其内容。

表 1-3　　必备配置文件

文件	内容
server.xml	服务器配置中的绝大部分（本 Proxy Server 发行版本的新增功能）
magnus.conf	全局服务器初始化信息
obj.conf	用于处理客户机请求的指令
mime.types	用于确定所请求资源内容类型的信息

有关上述及其他配置文件的详细信息，参见 Proxy Server Configuration File Reference。

正则表达式

可以使用正则表达式来识别资源和配置 Proxy Server，以便以不同方式处理来自不同 URL 的请求。正则表达式可以在使用 Administration Server 用户界面和 Server Manager 用户界面执行各种任务时指定。有关使用正则表达式的详细信息，参见第 319 页的第 16 章“管理模板和资源”。

第 2 章

管理 Sun Java System Web Proxy Server

本章介绍使用 Administration Server 管理 Sun Java System Web Proxy Server 的基础知识。Administration Server 是基于 Web 的用户界面，用于管理、添加、删除和迁移服务器。

本章包括以下部分：

有关配置 Administration Server 首选项的详细信息，参见第 37 页的第 3 章“设置管理首选项”。有关使用服务器群集管理多个 Proxy Server 的详细信息，参见第 109 页的第 6 章“管理服务器群集”。

启动 Administration Server

本节介绍如何在不同的平台上启动 Administration Server。有关停止 Administration Server 的信息，参见第 32 页的“停止 Administration Server”。

在 UNIX 或 Linux 上启动 Administration Server

- 在命令行中转到 *server_root*/`proxy-admserv` 并键入 `./start`，以启动 Administration Server（或键入 `./restart` 以重新启动 Administration Server）。

在 Windows 上启动 Administration Server

- 使用“开始”>“程序”> "Sun Microsystems" > "Sun Java System Web Proxy Server *version*" > "Start Admin"

  - 或 -

  使用“控制面板”>“管理工具”>“服务”> "Sun Java System Web Proxy Server 4.0" > “启动”

  - 或 -

- 在命令提示符中转到 *server_root*\proxy-admserv 并键入 startsvr.bat，以启动 Administration Server（或键入 ./restart 以重新启动 Administration Server）。

启动 Administration Server 后，即可以通过启动浏览器并输入 URL 来访问它，该 URL 的内容是在安装过程中为 Administration Server 指定的主机名和端口号（例如，http://myserver.mycorp.com:1234）。系统将提示您输入用户名和口令，这两者也都是在安装过程中指定的。

可以将 Administration Server 的访问权限授予一个以上管理员。有关分布式管理的更多信息，参见第 40 页的“允许多个管理员”。

停止 Administration Server

本节介绍如何在不同的平台上停止 Administration Server。有关启动 Administration Server 的信息，参见第 31 页的“启动 Administration Server”。

在 UNIX 或 Linux 上停止 Administration Server

- 访问 Administration Server，单击 "Preferences" 选项卡，单击 "Shutdown Server" 链接，然后单击 "OK"。

  - 或 -

- 在命令行中转到 *server_root*/proxy-admserv/ 并键入 ./stop。

在 Windows 上停止 Administration Server

- 使用“服务”窗口中的 "Sun Java System Proxy Server 4.0 Administration Server" 服务：“控制面板”>“管理工具”>“服务”

  - 或 -

- 在命令提示符中转到 *server_root*\proxy-admserv 并键入 stopsvr.bat。

运行多个 Proxy Server

要在系统中运行多个 Proxy Server，必须安装和配置多个服务器实例。下列程序介绍如何添加服务器实例。

安装多个服务器实例

1. 访问 Administration Server。
2. 在 "Servers" 选项卡上，单击 "Add Server"。
3. 填写要求提供的信息，然后单击 "OK"。有关特定字段的更多信息，参见联机帮助。
4. 需要时可以单击成功添加新服务器实例后所显示的 "Success" 页面上的 "Configure Your New Server" 链接。此时将显示 "Server Manager" 界面，它用于配置服务器实例。

删除服务器实例

可以使用 Administration Server 来删除 Proxy Server 实例。此操作无法撤消，因此请先确定是真的想要删除该服务器实例，然后再执行下列步骤。

删除服务器实例

1. 访问 Administration Server。
2. 在 "Servers" 选项卡上，单击 "Remove Server"。
3. 从下拉式列表中选择要删除的服务器实例。
4. 要执行删除操作，请选中 "Confirming Server Removal" 复选框并单击 "OK"。

从 Proxy Server 3.6 迁移

可以将 Sun™ One Web Proxy Server 3.6（也称作 iPlanet™ Web Proxy Server）迁移到 Sun Java System Web Proxy Server 4。版本 3.6 的服务器会得到保留，同时会创建一个新的具有相同设置的版本 4 的服务器。有关从版本 3.6 向版本 4 服务器迁移的更多信息，参见 Proxy Server Installation and Migration Guide。另参见 Proxy Server 用户界面中有关迁移的联机帮助页面。有关迁移证书的信息，参见本指南中的第 79 页的“迁移证书”。

第 2 部分

使用 Administration Server

第 3 章

设置管理首选项

本章介绍如何使用 Administration Server 配置管理首选项。要运行配置服务器所需的 CGI 程序，必须在浏览器中启用 Cookie。

本章包括以下部分：

创建和管理侦听套接字

必须先由侦听套接字接受请求，然后将其发送给正确的服务器，服务器才能够处理请求。安装 Proxy Server 时会自动创建一个侦听套接字 (`ls1`)。此侦听套接字使用 IP 地址 `0.0.0.0` 和在安装过程中指定为 Administration Server 端口号的端口号。

使用 Administration Server 的 "Edit Listen Sockets" 页面添加、编辑和删除侦听套接字。必须至少有一个用于访问服务器的侦听套接字。如果侦听套接字是列表中唯一的一个，则无法将其删除。

本节包括以下主题：

添加侦听套接字

添加侦听套接字

1. 访问 Administration Server 并单击 "Preferences" 选项卡。
2. 单击 "Edit Listen Sockets" 链接。
3. 单击 "New" 按钮。
4. 指定设置，然后单击 "OK"。有关特定字段的更多信息，参见联机帮助。

编辑侦听套接字

编辑侦听套接字

1. 访问 Administration Server 并单击 "Preferences" 选项卡。
2. 单击 "Edit Listen Sockets" 链接。
3. 单击想要编辑的侦听套接字的链接，进行所需的更改，然后单击 "OK"。

删除侦听套接字

删除侦听套接字

1. 访问 Administration Server 并单击 "Preferences" 选项卡。
2. 单击 "Edit Listen Sockets" 链接。
3. 选择要删除的侦听套接字旁的复选框，然后单击 "OK"。系统将提示您确认删除。必须至少有一个用于访问服务器的侦听套接字。如果侦听套接字是列表中唯一的一个，则无法将其删除。

更改超级用户设置

可以为 Administration Server 配置超级用户访问。这些设置只影响超级用户帐户。如果 Administration Server 使用分布式管理，则还必须为允许的管理员配置更多访问控制。

注意 如果使用 Sun Java™ System Directory Server 来管理用户和组，必须在更改超级用户名或口令**前**先更新目录中的超级用户条目。如果不先更新目录，将无法访问 Administration Server 中的 "Users and Groups" 界面。要解决此问题，必须使用确实可以访问该目录的管理员帐户访问 Administration Server，或使用 Directory Server 的控制台或配置文件来更新该目录。

更改 Administration Server 的超级用户设置

1. 访问 Administration Server 并单击 "Preferences" 选项卡。
2. 单击 "Control Superuser Access" 链接。
3. 进行所需的更改并单击 "OK"。有关特定字段的更多信息，参见联机帮助。

超级用户的用户名和口令保存在一个名为 `admpw` 的文件中，该文件位于 *server_root*`/proxy-admserv/config`。该文件的格式为 *username*`:`*password*。可以查看此文件以获得用户名，但口令已加密，因此无法读出。如果忘记了口令，可以编辑 `admpw` 文件，将加密的口令删除即可。然后可以进行以下操作：

1. 在填写用户名但不填写口令的情况下访问 Administration Server。
2. 单击 "Preferences" 选项卡。
3. 单击 "Control Superuser Access" 链接。
4. 提供新口令，然后单击 "OK"。

注意 因为 `admpw` 文件是可编辑的，所以将服务器计算机安置在一个安全的地方并限制对其文件系统的访问是非常重要的。

在 UNIX 和 Linux 系统上，可以考虑更改文件所有权，只允许超级用户或运行 Administration Server 守护进程的系统用户对其执行写操作。在 Windows 系统上，可以将文件所有权限制为 Administration Server 使用的用户帐户。

允许多个管理员

通过分布式管理，多个管理员可以更改服务器的特定部分。必须先安装目录服务器，然后才能启用分布式管理。默认目录服务必须基于 LDAP。

进行分布式管理时有两个级别的用户：超级用户和管理员。

- 超级用户是 *server_root*/proxy-admserv/config/admpw 中所列的用户。这是在安装过程中指定的用户名和口令。此用户对 Administration Server 中除 "Users and Groups" 表单外的所有表单都具有完全访问权限，是否能够访问除外的表单取决于超级用户在 LDAP 服务器中是否有有效帐户。
- 管理员可以直接访问特定服务器（包括 Administration Server）的 "Server Manager" 表单。他们可以看到的表单取决于为他们配置的访问控制规则（通常由超级用户来配置）。管理员可以执行有限的管理任务，还可以进行会影响其他用户的更改，如添加用户或更改访问控制。

有关访问控制的更多信息，参见第 135 页的第 8 章“控制对服务器的访问”。

启用分布式管理

1. 确认已安装了目录服务器。
2. 访问 Administration Server。
3. 安装目录服务器后，如果尚未创建管理组，则还需要创建管理组。创建组：
   a. 单击 "Users and Groups" 选项卡。
   b. 单击 "Create Group" 链接。
   c. 在 LDAP 目录中创建一个 administrators 组，然后添加用户的名称，将为这些用户授予配置 Administration Server 或在其服务器根目录中安装的任何服务器的权限。有关特定字段的更多信息，参见联机帮助。

      该 administrators 组中的所有用户都具有对 Administration Server 的完全访问权限，但可以使用访问控制来限制允许他们配置的服务器和表单。

      访问控制表一经创建，分布式管理组即添加到该列表中。如果更改了 administrators 组的名称，必须手动编辑访问控制表以更改其引用的组。
4. 单击 "Preferences" 选项卡。
5. 单击 "Configure Distributed Administration" 链接。
6. 选择 "Yes"，指定 administrators 组，然后单击 "OK"。

指定日志文件选项

Administration Server 日志文件记录有关 Administration Server 的数据，包括所遭遇错误的类型及有关服务器访问的信息。可以通过查看这些日志来监视服务器活动和排除故障。可以使用 "Log Preferences" 页面上的众多选项指定 Administration Server 日志中记录的数据的类型和格式。可以选择 "Common Logfile Format"，它提供固定数量的服务器信息；也可以创建更符合自己要求的自定义日志文件格式。

要访问 "Administration Server Log Preferences" 页面，请单击 "Preferences" 选项卡，然后单击 "Set Access Log Preferences" 或 "Set Error Log Preferences" 链接。有关日志文件和日志文件选项设置的详细信息，参见第 163 页的第 9 章“使用日志文件”。另参见联机帮助。

查看日志文件

Administration Server 日志文件位于 *server_root*/proxy-admserv/logs。可以通过 Proxy Server 管理控制台或使用文本编辑器查看错误日志和访问日志。

访问日志文件

访问日志文件记录向服务器发送的请求及从服务器收到的响应的相关信息。

查看访问日志文件

1. 访问 Administration Server 并单击 "Preferences" 选项卡。
2. 单击 "View Access Log" 链接。

有关特定字段的更多信息，参见联机帮助。另参见第 163 页的第 9 章“使用日志文件”。

错误日志文件

错误日志列出了日志文件创建以来服务器遇到的所有错误。它还包含有关服务器的提示性消息，如服务器的启动时间及谁曾尝试登录但未成功。

查看错误日志文件

1. 访问 Administration Server 并单击 "Preferences" 选项卡。
2. 单击 "View Error Log" 链接。

有关特定字段的更多信息，参见联机帮助。另参见第 163 页的第 9 章“使用日志文件”。

使用目录服务

可以使用 LDAP 在单个目录服务器中存储和管理用户名和口令之类的信息。还可以配置服务器，使其允许用户从多个易于访问的网络位置检索目录信息。有关使用目录服务的更多信息，参见第 43 页的第 4 章“管理用户和组”。

限制服务器访问

当 Proxy Server 评判外来的请求时，将根据一组称作访问控制条目 (ACE) 的、以分层结构组织的规则来确定访问权限，然后使用匹配的条目确定是应允许还是应拒绝该请求。每个 ACE 都指定了服务器是否应继续检查分层结构中的下一个 ACE。ACE 的集合称为访问控制表 (ACL)。

可以针对是访问 Administration Server 还是服务器实例内的特定资源（如文件、目录和文件类型）来配置访问控制。在 Administration Server 中的 "Global Settings" 选项卡中配置对 Administration Server 的访问控制。在 Server Manager 中的 "Preferences" 选项卡中配置对服务器实例内资源的访问控制。有关访问控制设置的更多信息，参见第 135 页的第 8 章“控制对服务器的访问”。

注 必须先启用分布式管理，然后才能对服务器访问进行限制。有关更多信息，参见第 40 页的“允许多个管理员”。

SNMP 主代理设置

简单网络管理协议 (SNMP) 是一种用于交换有关网络活动的数据的协议。通过使用子代理和主代理在网络管理站与服务器间传送此信息。

SNMP 主代理设置使用 Administration Server 中的 "Global Settings" 选项卡进行配置。主代理随 Administration Server 一起安装。有关 SNMP 及代理设置的详细信息，参见第 187 页的第 10 章“监视服务器”。另参见 Administration Server 中 "Global Settings" 选项卡主代理页面及 Server Manager 中 "Server Status" 选项卡子代理页面的联机帮助。

第 4 章

管理用户和组

本章介绍如何添加、删除、修改和管理可以访问 Proxy Server 的用户和组。

本章包括以下各节：

访问有关用户和组的信息

可以通过 Administration Server 访问有关用户帐户、组列表、访问权限、组织单位以及用户和组特有信息的应用程序数据。

用户和组信息存储在文本格式的平面文件或支持 LDAP（轻量目录访问协议）的目录服务器（如 Sun Java™ System Directory Server）中。LDAP 是一种开放的目录访问协议，它通过 TCP/IP（传输控制协议 /Internet 协议）运行，可以扩展到全局大小，几百万个条目。

关于目录服务

可以通过目录服务从一个源管理所有用户信息。使用 Proxy Server 可以配置三种不同类型的目录服务：LDAP、密钥文件和摘要文件。

如果没有配置其他目录服务，新创建的第一个目录服务的值将被设置为 `default`，无论其是何种类型。创建目录服务时，将使用目录服务的详细信息更新 *server_root*`/userdb/dbswitch.conf` 文件。

本节包括以下主题：

LDAP 目录服务

使用 LDAP 目录服务时，用户和组信息存储在基于 LDAP 的目录服务器中。

如果 LDAP 服务是默认服务，将按下例所示更新 `dbswitch.conf` 文件：

```
directory default
ldap://test22.india.sun.com:589/dc%3Dindia%2Cdc%3Dsun%2Cdc%3Dcom
default:binddn cn=Directory Manager
default:encoded bindpw YWRtaW5hZG1pbg==
```

如果 LDAP 服务不是默认服务，将按下例所示更新 `dbswitch.conf` 文件：

```
directory ldap
ldap://test22.india.sun.com:589/dc%3Dindia%2Cdc%3Dsun%2Cdc%3Dcom
ldap:binddn cn=Directory Manager
ldap:encoded bindpw YWRtaW5hZG1pbg==
```

密钥文件目录服务

密钥文件是一个文本文件，其中包含散列格式的用户口令及用户所属的组的列表。仅当要使用 HTTP 基本验证时，才能使用密钥文件格式。有关此验证方法的更多信息，参见第 150 页的“指定用户和组”。

创建基于密钥文件的数据库时，将按下例所示更新 `dbswitch.conf` 文件：

```
directory keyfile file
keyfile:syntax keyfile
keyfile:keyfile D:\test22\keyfile\keyfiledb
```

摘要文件目录服务

摘要文件基于加密的用户名和口令存储用户和组信息。

摘要文件格式是为支持 HTTP 摘要验证的使用而提供的，但它也支持基本验证，因此可以用于这两种验证方法。有关这些方法的更多信息，参见第 150 页的“指定用户和组”。

创建基于摘要的数据库时，将按下例所示更新 `dbswitch.conf` 文件：

```
directory digest file
digest:syntax digest
digest:digestfile D:\test22\digest\digestdb
```

注 要配置分布式管理，默认目录服务必须是基于 LDAP 的目录服务。

配置目录服务

在 Administration Server 的 "Global Settings" 选项卡上创建和配置目录服务。然后在 Administration Server 的 "Users and Groups" 选项卡上创建和管理用户、组和组织单位。

本节包括以下主题：

- 创建目录服务
- 编辑目录服务

创建目录服务

创建目录服务

1. 访问 Administration Server 并单击 "Global Settings" 选项卡。
2. 单击 "Configure Directory Service" 链接。
3. 在 "Create New Service of Type" 下拉式列表中选择要创建的目录服务类型，然后单击 "New"。将显示该目录服务的配置页面。
4. 提供配置信息，然后单击 "Save Changes"。有关特定字段的更多信息，参见联机帮助。

注 如果没有配置其他目录服务，新创建的第一个目录服务的值将被设置为 `default`，无论其是何种类型。

编辑目录服务

编辑目录服务

1. 访问 Administration Server 并单击 "Global Settings" 选项卡。
2. 单击 "Configure Directory Service" 链接。
3. 单击想要编辑的目录服务的链接，进行所需的更改，然后单击 "Save Changes"。有关特定字段的更多信息，参见联机帮助。

了解标识名 (DN)

Administration Server 中的 "Users and Groups" 选项卡用于创建或修改用户、组和组织单位。用户是指 LDAP 数据库中的个人，如公司的雇员。组是指共享某个常用属性的两个或更多个用户。组织单位是指工作单位内的子分支机构，它使用 `organizationalUnit` 对象类。本章后文中将对用户、组和组织单位做更为详尽的介绍。

企业中的每个用户和组都由一个标识名 (DN) 属性来表示。DN 属性是一个文本字符串，它包含关联的用户、组或对象的标识信息。每当更改用户或组目录条目时，就需要使用 DN。例如，每次为应用程序（如邮件或发布）创建或修改目录条目、配置访问控制及配置用户帐户时，都必须提供 DN 信息。Proxy Server 的 "Users and Groups" 界面用于创建或修改 DN。

以下示例显示的是 Sun Microsystems 某个雇员的典型 DN：

```
uid=doe,e=doe@sun.com,cn=John Doe,o=Sun Microsystems Inc.,c=US
```

本示例中各缩写的含义如下：

- `uid` 是用户 ID
- `e` 是电子邮件地址
- `cn` 是用户的通用名称
- `o` 是工作单位
- `c` 是国家

DN 可能包括多种名称 - 值对，用于标识支持 LDAP 的目录中的证书主题和条目。

使用 LDIF

如果目前没有目录或要向现有目录中添加新的子树，则可以使用目录服务器的 LDIF（轻量目录交换格式）导入功能。此功能接受包含 LDIF 的文件并尝试使用 LDIF 条目生成目录或新的子树。还可以使用目录服务器的 LDIF 导出功能将当前目录导出到 LDIF。此功能会创建一个 LDIF 格式的文件，用来表示您的目录。可以使用 `ldapmodify` 命令行实用程序（如果可用）和相应的 LDIF 更新语句来添加或编辑条目。

要使用 LDIF 向数据库添加条目，请先在某个 LDIF 文件中定义条目，然后从目录服务器导入该 LDIF 文件。

创建用户

Administration Server 中的 "Users and Groups" 选项卡用于创建和修改用户条目。用户条目包含有关数据库中的单个用户或对象的信息。

注 务必通过确保用户对资源不具有未经授权的访问权限来保证服务器的安全性。Proxy Server 使用基于 ACL 的授权和验证模式。有关基于 ACL 的安全性的更多信息，参见第 135 页的第 8 章“控制对服务器的访问”。有关其他安全性信息，另参见第 71 页的第 5 章“使用证书和密钥”。

本节包括以下主题：

在基于 LDAP 的验证数据库中创建用户

向基于 LDAP 的目录服务添加用户条目时，将使用底层的基于 LDAP 的目录服务器的服务对用户进行验证和授权。本节列出使用基于 LDAP 的验证数据库时需要考虑的指导原则，并介绍如何通过 Proxy Server Administration Server 来添加用户。

创建基于 LDAP 的用户条目的指导原则

使用 Proxy Server 管理控制台在基于 LDAP 的目录服务中创建新用户条目时，请考虑以下指导原则：

- 如果输入名字和姓，将自动填写用户的全名和用户 ID。生成的用户 ID 由用户名字的第一个字母和后跟的用户姓组成。例如，如果用户的姓名为 Billie Holiday，将自动把用户 ID 设置为 `bholiday`。如果您愿意，可以用自己选择的 ID 替换该用户 ID。
- 用户 ID 必须是唯一的。Administration Server 通过从搜索基（基 DN）开始向下搜索整个目录来确定该用户 ID 是否已被使用，从而确保该用户 ID 的唯一性。不过，请注意，如果使用目录服务器 `ldapmodify` 命令行实用程序（如果可用）创建用户，将无法确保用户 ID 的唯一性。如果目录中存在重复的用户 ID，受影响的用户将无法验证到该目录。
- 基 DN 指定默认情况下作为目录查找起点的标识名，同时也是目录树中放置所有 Proxy Server Administration Server 条目的位置。DN 是对目录服务器中条目名称的字符串表示。
- 创建新用户条目时须至少指定以下用户信息：
  - 姓
  - 全名
  - 用户 ID
- 如果为目录定义了任何组织单位，可以使用 Administration Server 中 "Create User" 页面上的 "Add New User To" 列表指定要放置新用户的位置。默认位置是目录的基 DN（或根点）。

创建基于 LDAP 的用户条目

要创建用户条目，请阅读以下部分中概述的指导原则，然后执行下面的过程：第 48 页的“创建基于 LDAP 的用户条目的指导原则”。

在基于 LDAP 的验证数据库中创建用户

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Create User" 链接。
3. 从下拉式列表中选择 LDAP 目录服务，然后单击 "Select"。
4. 在显示的页面中输入信息。有关特定字段的更多信息，参见联机帮助。另参见第 49 页的“目录服务器用户条目”。
5. 单击 "Create" 创建用户条目，或单击 "Create and Edit" 创建用户条目并随即进入刚创建的条目的编辑页面。

目录服务器用户条目

关于目录服务器用户条目的注释：

- 用户条目使用 `inetOrgPerson`、`organizationalPerson` 和 `person` 对象类。
- 默认情况下，用户标识名的格式如下：

  `cn=`*full name*`,ou=`*organization*`, . . . ,o=`*base organization*`,c=`*country*

  例如，如果在组织单位 Marketing 内为 Billie Holiday 创建了用户条目，且目录的基 DN 是 `o=Ace Industry, c=US`，则 DN 将是：

  ```
  cn=Billie Holiday,ou=Marketing,o=Ace Industry,c=US
  ```

  不过，请注意，可以将此格式更改为基于用户 ID (uid) 的标识名。
- 用户表单字段上的值以 LDAP 属性形式存储。

  下表列出了在 Proxy Server 界面中创建新用户时显示的字段和相应的 LDAP 属性。

表 4-1 LDAP 属性——创建用户条目

用户字段	LDAP 属性
Given Name	`givenName`
Surname	`sn`
Full Name	`cn`
User ID	`uid`

表 4-1 LDAP 属性——创建用户条目

用户字段	LDAP 属性
Password	`userPassword`
E-mail Address	`mail`

下表列出了编辑用户条目时会附加显示的字段和相应的 LDAP 属性。

表 4-2 LDAP 属性——编辑用户条目

用户字段	LDAP 属性
Title	`title`
Phone Number	`telephoneNumber`

在密钥文件验证数据库中创建用户

密钥文件是一个文本文件，其中包含散列格式的用户口令及用户所属的组的列表。

在密钥文件验证数据库中创建用户

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Create User" 链接。
3. 从下拉式列表中选择基于密钥文件的目录服务，然后单击 "Select"。
4. 在显示的页面中输入信息，然后单击 "Create User"。有关特定字段的更多信息，参见联机帮助。

在摘要文件验证数据库中创建用户

摘要文件验证数据库以加密形式存储用户和组信息。

在摘要文件验证数据库中创建用户

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Create User" 链接。
3. 从下拉式列表中选择基于摘要文件的目录服务，然后单击 "Select"。
4. 在显示的页面中输入信息，然后单击 "Create User"。有关特定字段的更多信息，参见联机帮助。

注 使用 Proxy Server ACL 用户界面创建使用摘要验证的 ACL 时，必须指定相同的领域字符串。有关更多信息，参见第 146 页的“设置访问控制”。

管理用户

通过 Administration Server "Users and Groups" 选项卡上的 "Manage Users" 页面编辑用户属性。在此页面中，可以查找、更改、重命名和删除用户条目。

本节包括以下主题：

查找用户信息

编辑用户条目前，必须先查找并显示条目，如以下过程中所述。

查找用户信息

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Users" 链接。
3. 从下拉式列表中选择目录服务，然后单击 "Select"。对于密钥文件或摘要文件目录服务，将显示用户列表。对于基于 LDAP 的目录服务，将显示搜索字段。

4. 查找用户信息：

   对于密钥文件和摘要文件目录服务，请单击用户的链接以显示编辑页面，然后进行更改。有关特定字段的更多信息，参见联机帮助。

   对于基于 LDAP 的目录服务，请执行以下操作：

   a. 在 "Find User" 字段中为要编辑的条目输入描述性值。可以输入任何以下类型的值：

      - 名称。输入全称或部分名称。将返回与搜索字符串完全匹配的所有条目。如果未找到这样的条目，将查找包含该搜索字符串的所有条目。如果未找到这样的条目，将查找发音与搜索字符串类似的所有条目。
      - 用户 ID。如果只输入部分用户 ID，将返回所有包含该字符串的条目。
      - 电话号码。如果只输入部分号码，将返回结尾号码与搜索号码相同的所有条目。
      - 电子邮件地址。包含 (@) 符号的任何搜索字符串均被认为是电子邮件地址。如果找不到完全匹配项，将执行搜索来查找以该搜索字符串开头的所有电子邮件地址。
      - 使用星号 (*) 可以获得当前目录中的所有条目。将该字段留空也可以实现这一目的。
      - 任意 LDAP 搜索过滤器。任何包含等号 (=) 的字符串均被认为是搜索过滤器。

      还可以使用 "Find All Users Whose" 部分中的下拉式菜单来缩小搜索结果的范围。有关更多信息，参见第 53 页的“生成自定义搜索查询”。

   b. 在 "Look Within" 字段中，选择要在其中搜索条目的组织单位。默认值为目录的根点（最顶端的条目）。

   c. 在 "Format" 字段中指定是否对输出进行格式设置，以便在屏幕上显示或在打印机上打印。

   d. 在本过程中的任何阶段单击 "Find" 按钮时，将显示与搜索条件匹配的所有用户。

   e. 单击要显示的条目的链接。

生成自定义搜索查询

对于 LADP 服务，可以通过 "Find All Users Whose" 部分生成自定义搜索过滤器。使用各字段来缩小 "Find User" 搜索返回的搜索结果的范围。

左侧的下拉式列表指定搜索依据的属性。下表列出了可用的搜索属性选项。

表 4-3 搜索属性选项

选项	搜索匹配项
Full name	每个条目的全名
Last name	每个条目的姓
User ID	每个条目的用户 ID
Phone number	每个条目的电话号码
E-mail address	每个条目的电子邮件地址

中间的下拉式列表指定要执行的搜索类型。下表列出了可用的搜索类型选项。

表 4-4 搜索类型选项

选项	描述
Contains	执行子串搜索。将返回属性值包含指定搜索字符串的条目。例如，如果知道用户的姓名可能包含单词 "Dylan"，则可以通过此选项使用搜索字符串 "Dylan" 来查找该用户的条目。
Is	执行精确匹配搜索（指定等同项搜索）。如果知道用户属性的确切值，请使用此选项。例如，知道用户姓名的准确拼写。
Isn't	返回属性值与搜索字符串不精确匹配的所有条目。使用此选项在目录中查找姓名不是 "John Smith" 的所有用户。请注意，使用此选项可能导致返回极大数量的条目。
Sounds like	执行近似或语音搜索。如果知道属性的值但不知道其拼写，请使用此选项。例如，如果不知道用户姓名的拼写是 "Sarret"、"Sarette" 还是 "Sarett"。
Starts with	执行子串搜索。返回属性值以指定的搜索字符串开头的所有条目。例如，知道用户姓名以 "Miles" 开头，但不知道姓名的其余部分。
Ends with	执行子串搜索。返回属性值以指定搜索字符串结尾的所有条目。例如，知道用户姓名以 "Dimaggio" 结尾，但不知道姓名的其余部分。

右侧的文本字段用于输入搜索字符串。要显示在 "Look Within" 字段中指定的目录中包含的所有用户条目，请输入星号 (*) 或将此字段留空。

编辑用户信息

编辑用户条目

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Users" 链接。
3. 按以下部分中所述显示用户条目：第 51 页的“查找用户信息”。
4. 进行所需的更改。有关特定字段的更多信息，参见联机帮助。

注	可能需要更改编辑用户页面未显示的属性值。在这种情况下，请使用目录服务器的 `ldapmodify` 命令行实用程序（如果可用）。

有关更改用户的用户 ID 的信息，参见第 55 页的“重命名用户”。

管理用户口令

以下过程介绍如何更改或创建用户口令。

更改或创建用户口令

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Users" 链接。
3. 按以下部分中所述显示用户条目：第 51 页的“查找用户信息”。
4. 进行所需的更改。有关特定字段的更多信息，参见联机帮助。

对于 LDAP 数据库，还可以通过单击用于编辑用户口令信息的页面（可以从 "Manage Users" 页面访问）上的 "Disable Password" 按钮来禁用用户口令。这样一来，不必删除用户的目录条目就可以阻止其登录服务器。输入新口令后即可再次授予该用户访问权限。

重命名用户

对于 LDAP 数据库，重命名特性只会更改用户 ID，不会影响所有其他字段。无法使用重命名特性将一个组织单位中的条目移入另一个组织单位。

重命名用户条目

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Users" 链接。
3. 按以下部分中所述显示用户条目：第 51 页的“查找用户信息”。
4. 单击编辑用户页面上的 "Rename User" 按钮，在显示的页面上输入用户 ID，然后单击 "Save Changes"。

注 重命名条目时，可以通过将 `keepOldValueWhenRenaming` 参数设置为 `false`（默认值）来指定 Administration Server 不再保留旧值。该参数位于以下文件中：

server_root`/proxy-admserv/config/dsgw-orgperson.conf`

删除用户

删除用户条目

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Users" 链接。
3. 按以下部分中所述显示用户条目：第 51 页的“查找用户信息”。
4. 单击 "Delete User" (LDAP) 或 "Remove User"（密钥文件和摘要文件）。

创建组

组是 LDAP 数据库中用来描述一组对象的对象。Sun Java System 服务器组由共享某个通用属性的用户组成。例如，一组对象可能是就职于公司市场部的若干雇员。这些雇员可能属于一个名为 Marketing 的组。

对于 LDAP 服务，定义组成员资格的方法有两种：静态和动态。静态组显式地枚举其成员对象。静态组是一个通用名称 (Common Name, CN)，它包含 uniqueMembers 和 / 或 memberURLs 和 / 或 memberCertDescriptions。对于静态组，其成员并不共享某个通用属性，但 cn=*groupname* 属性除外。

动态组让您可以使用 LDAP URL 来定义一组只适用于组成员的规则。对于动态组，其成员的确共享某个或一组通用属性，这些属性在 memberURL 过滤器中定义。例如，如果需要一个包含 Sales 部门中所有雇员的组，并且这些雇员已位于 LDAP 数据库中的 ou=Sales,o=Airius.com 之下，则可以使用以下成员 URL 定义一个动态组：

```
ldap:///ou=Sales,o=sun??sub?(uid=*)
```

结果是，该组将包含树中 ou=Sales,o=sun 点下具有 uid 属性的所有对象。也就是说，包含所有 Sales 成员。

对于静态组和动态组，如果使用 memberCertDescription，则其成员可以通过证书共享某个通用属性。请注意，这只在 ACL 使用 SSL 方法时才适用。

创建新组后，即可向其中添加用户（成员）。

本节包括以下主题：

关于静态组

对于 LDAP 服务，Administration Server 让您可以通过在任意数量的用户的 DN 中指定相同的组属性来创建静态组。静态组不会发生变化，除非向其中添加用户或从中删除用户。

创建静态组的指导原则

使用 Administration Server 界面创建新静态组时，请考虑以下指导原则：

- 静态组可以包含其他静态或动态组。
- 如果为目录定义了组织单位，请使用 Administration Server 界面中 "Create Group" 页面上的 "Add New Group To" 列表指定放置新组的位置。默认位置为目录的根点（最顶端的条目）。
- 有关编辑组的更多信息，参见第 62 页的“编辑组条目”。

创建静态组

创建静态组

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Create Group" 链接。
3. 从 "Type of Group" 下拉式列表中选择 "New Group"，然后单击 "Go"。
4. 在 "Create Group" 页面中输入信息。有关特定字段的更多信息，参见联机帮助。
5. 单击 "Create" 创建组，或单击 "Create and Edit" 创建组并随即进入刚创建的组的编辑页面。

关于动态组

对于 LDAP 服务，如果想要基于任何属性自动将用户分组或想要将 ACL 应用于某些包含匹配 DN 的组，则可以通过 Proxy Server 创建动态组。例如，可以创建这样一个组，该组自动包括任何包含属性 `department=marketing` 的 DN。如果为 `department=marketing` 应用搜索过滤器，搜索将返回一个组，其中包含具有属性 `department=marketing` 的所有 DN。接下来可以使用基于此过滤器的搜索结果定义一个动态组。随后可以为生成的动态组定义 ACL。

动态组是如何实现的

Proxy Server 在 LDAP 服务器模式中以 `objectclass=groupOfURLs` 方式实现动态组。一个 `groupOfURLs` 类可以有零个或更多个 `memberURL` 属性，每个属性都是一个 LDAP URL，描述目录中的一组对象。组的成员将是这些对象集的总和。例如，下面的组只包含一个成员 URL：

```
ldap:///o=mcom.com??sub?(department=marketing)
```

该示例描述的是 `o=mcom.com` 下部门为 `marketing` 的所有对象所组成的集合。LDAP URL 可以包含搜索基 DN、范围和过滤器，但不能包含主机名和端口。这意味着只能引用同一个 LDAP 服务器上的对象。LDAP URL 支持所有范围。有关 LDAP URL 的更多信息，参见第 58 页的“创建动态组的指导原则”。

DN 会自动包含在内，不需要向组中逐一添加每个 DN。组是动态变化的，因为每次 ACL 验证需要进行组查找时，Proxy Server 都会执行 LDAP 服务器搜索。ACL 文件中使用的用户和组名称与 LDAP 数据库中对象的 `cn` 属性相对应。

注 Proxy Server 使用 `cn` 属性作为 ACL 的组名称。

从 ACL 到 LDAP 数据库的映射将同时在 dbswitch.conf 文件（它将 ACL 数据库名称与实际的 LDAP 数据库 URL 关联）和 ACL 文件（它定义要为各 ACL 使用的数据库）中进行定义。例如，如果想让名为 staff 的组中的成员资格具有基本访问权限，ACL 代码将查找对象类为 groupOf*anything* 且 CN 的设置为 staff 的对象。该对象通过两种方法来定义组的成员：显式地枚举成员 DN（与对静态组的 groupOfUniqueNames 的做法相同），或指定 LDAP URL（例如，groupOfURLs）。

注 组可以同时是动态和静态的。组对象可以同时有 objectclass=groupOfUniqueMembers 和 objectclass=groupOfURLs。因此，uniqueMember 和 memberURL 属性均有效。组的成员资格是其静态和动态成员的总和。

动态组对服务器性能的影响

使用动态组会影响服务器性能。如果正在测试组成员资格，而该 DN 不是静态组的成员，则 Proxy Server 将检查数据库基 DN 中的所有动态组。Proxy Server 确定是否每个 memberURL 都匹配，方法是检查其基 DN 和范围并与用户的 DN 进行比较，然后使用用户的 DN 作为基 DN，并使用 memberURL 作为过滤器来执行基搜索。此过程可能包括大量单个搜索。

创建动态组的指导原则

使用 Administration Server 界面创建新动态组时，请考虑以下指导原则：

- 动态组不能包含其他组。
- 使用以下格式输入组的 LDAP URL（不包括主机和端口信息，因为这些参数会被忽略）：

  ldap:///*base_dn*?*attributes*?*scope*?(*filter*)

  下表列出了 LDAP URL 的必需参数。

表 4-5 LDAP URL 的必需参数

参数名	描述
base_dn	搜索基的 DN，或在 LDAP 目录中执行所有搜索的起始点。此参数往往被设置为目录的后缀或根，如 o=mcom.com。
attributes	搜索将返回的属性列表。要指定一个以上属性，请使用逗号来分隔各属性（例如，cn,mail,telephoneNumber）。如果不指定属性，将返回所有属性。检查动态组成员资格时将忽略此参数。

表 4-5 LDAP URL 的必需参数

参数名	描述
scope	此参数是必需的。 搜索范围，其值可以是： • base 只检索有关 URL 中指定的标识名（base_dn）的信息。 • one 检索有关 URL 中指定的标识名（base_dn）的下一级条目的信息。此范围不包括基本条目。 • sub 检索有关 URL 中指定的标识名（base_dn）下所有级别条目的信息。此范围包括基本条目。
(filter)	此参数是必需的。 应用于指定搜索范围内的条目的搜索过滤器。如果使用的是 Administration Server 界面，则必须指定此属性。括号是必需的。

attributes、scope 和 (filter) 参数是根据它们在 URL 中的位置来进行标识的。即使不想指定任何属性，仍必须使用问号 (?) 来分隔该字段。

继续介绍创建动态组的指导原则：

- 如果为目录定义了组织单位，请使用 Administration Server 界面中 "Create Group" 页面上的 "Add New Group To" 列表指定放置新组的位置。默认位置为目录的根点（最顶端的条目）。
- 有关编辑组的更多信息，参见第 62 页的“编辑组条目”。

创建动态组

创建动态组

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Create Group" 链接。
3. 从 "Type of Group" 下拉式列表中选择 "Dynamic Group"，然后单击 "Go"。
4. 在 "Create Group" 页面中输入信息。有关特定字段的更多信息，参见联机帮助。
5. 单击 "Create" 创建组，或单击 "Create and Edit" 创建组并随即进入刚创建的组的编辑页面。

管理组

对于 LDAP 服务，Administration Server 让您可以通过 Administration Server 的 "Users and Groups" 选项卡上的 "Manage Groups" 页面来编辑组和管理组成员资格。

本节包括以下主题：

查找组条目

编辑组条目前，必须先查找并显示条目，如以下过程中所述。

查找组条目

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Groups" 链接。
3. 在 "Find Group" 字段中输入要查找的组的名称。可以输入任何以下类型的值：
   - 名称。输入全称或部分名称。将返回与搜索字符串完全匹配的所有条目。如果未找到这样的条目，将查找包含该搜索字符串的所有条目。如果未找到这样的条目，将查找发音与搜索字符串类似的所有条目。
   - 使用星号 (*) 可以获得当前位于目录中的所有组。将该字段留空也可以实现这一目的。
   - 任意 LDAP 搜索过滤器。包含等号 (=) 的任何字符串均被认为是搜索过滤器。

   还可以使用 "Find All Groups Whose" 部分生成自定义搜索过滤器，缩小搜索结果的范围。有关更多信息，参见第 61 页的“Find All Groups Whose 部分”。

4. 在 "Look Within" 字段中，选择要在其中搜索条目的组织单位。默认值为目录的根点（最顶端的条目）。
5. 在 "Format" 字段中指定是否对输出进行格式设置，以便在屏幕上显示或在打印机上打印。
6. 在本过程中的任何阶段单击 "Find" 按钮时，将显示与搜索条件匹配的所有组。
7. 单击要显示的条目的链接。

Find All Groups Whose 部分

对于 LADP 服务，可以通过 "Find All Groups Whose" 部分生成自定义搜索过滤器。使用此部分中的字段可以缩小要不然将由 "Find Group" 返回的搜索结果的范围。

左侧的下拉式列表指定搜索要依据的属性。可用选项如下：

- **Name。**搜索每个条目的全名以查找匹配项。
- **Description。**搜索每个组条目的描述以查找匹配项。

中间的下拉式列表指定要执行的搜索类型。可用选项如下：

- **Contains。**执行子串搜索。将返回属性值包含指定搜索字符串的条目。例如，如果知道组名可能包含单词 "Administrator"，请在此选项中使用搜索字符串 "Administrator" 来查找组条目。
- **Is。**执行精确匹配搜索。如果知道组属性的确切值，请使用此选项。例如，知道组名的准确拼写。
- **Isn't。**返回属性值与搜索字符串不精确匹配的所有条目。如果要在目录中查找所有名称中不包含 "administrator" 的组，请使用此选项。不过请注意，使用此选项可能导致返回极大数量的条目。
- **Sounds like。**执行近似或语音搜索。如果知道属性的值，但不能确定其拼写，请使用此选项。例如，不知道组名的拼写是 "Sarret's list"、"Sarette's list" 还是 "Sarett's list"。
- **Starts with。**执行子串搜索。返回属性值以指定的搜索字符串开头的所有条目。例如，知道组名以 "Product" 开头，但不知道名称的其余部分。
- **Ends with。**执行子串搜索。返回属性值以指定搜索字符串结尾的所有条目。例如，知道组名以 "development" 结尾，但不知道名称的其余部分。

在右侧的文本字段中输入搜索字符串。要显示 "Look Within" 目录中包含的所有组条目，请输入星号 (*) 或将此字段留空。

编辑组条目

编辑组条目

以下过程只适用于 LDAP 服务。

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Groups" 链接。
3. 按以下部分中所述找到要编辑的组：第 60 页的“查找组条目”。
4. 进行所需的更改。有关特定字段和按钮的更多信息，参见联机帮助。

注 可能需要更改组编辑页面未显示的属性值。在这种情况下，请使用目录服务器的 `ldapmodify` 命令行实用程序（如果可用）。

添加组成员

向组添加成员

以下过程只适用于 LDAP 服务。

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Groups" 链接。
3. 按以下部分中所述找到并显示要管理的组：第 60 页的“查找组条目”，然后单击 "Group Members" 旁的 "Edit" 按钮。显示的页面中将列出所有现有的组成员。还会显示搜索字段。
   - 要将用户条目添加到成员列表，必须在 "Find" 下拉式列表中选择 "Users"。
   - 要将组条目添加到组，必须选择 "Groups"。
4. 在 "Matching" 文本字段中输入搜索字符串。请输入以下选项之一：
   - 名称。输入全称或部分名称。将返回其名称与搜索字符串完全匹配的所有条目。如果未找到这样的条目，将查找包含该搜索字符串的所有条目。如果未找到这样的条目，将查找发音与搜索字符串类似的所有条目。
   - 用户 ID。如果只输入部分用户 ID，将返回所有包含该字符串的条目。
   - 电话号码。如果只输入部分号码，将返回结尾号码与搜索号码相同的所有条目。

- 电子邮件地址。包含 (@) 符号的任何搜索字符串均被认为是电子邮件地址。如果找不到完全匹配项，将执行搜索来查找以该搜索字符串开头的所有电子邮件地址。
- 如果输入星号 (*) 或将此字段留空，将返回当前位于目录中的所有条目或组。
- 任意 LDAP 搜索过滤器。包含等号 (=) 的任何字符串均被认为是搜索过滤器。

5. 单击 "Add" 查找 LDAP 数据库中所有匹配的条目并将它们添加到组中。如果不希望将搜索返回的某些条目添加到组中，请单击 "Remove From List" 列中相应的复选框。（请注意，还可以构建一个搜索过滤器来匹配要从组中删除的条目，然后单击 "Remove"。有关更多信息，参见第 63 页的“从组成员列表中删除条目”。）
6. 完成组成员列表后，单击 "Save Changes"。条目将添加到组成员列表。

向组成员列表中添加组

对于 LDAP 服务，可以向组成员列表中添加组（而不是单个成员）。这样做将使所添加的组的成员成为接收组的成员。例如，如果 Neil Armstrong 是 Engineering Managers 组的成员，而您使 Engineering Managers 组成为 Engineering Personnel 组的成员，则 Neil Armstrong 也将成为 Engineering Personnel 组的成员。

要将组添加到另一个组的组成员列表中，可以像添加用户条目那样添加该组。有关更多信息，参见第 62 页的“添加组成员”。

从组成员列表中删除条目

以下过程只适用于 LDAP 服务。

从组成员列表中删除条目

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Groups" 链接。
3. 按以下部分中所述找到要管理的组：第 60 页的“查找组条目”，然后单击 "Group Members" 旁的 "Edit" 按钮。
4. 对于要从列表中删除的每个成员，单击 "Remove From List" 列中相应的复选框。还可以构建一个搜索过滤器来匹配要从组中删除的条目，然后单击 "Remove"。有关创建搜索过滤器的更多信息，参见第 62 页的“添加组成员”。
5. 单击 "Save Changes"。将从组成员列表中删除条目。

管理拥有者

对于 LDAP 服务，管理组拥有者列表的方法与管理组成员列表的方法相同。

下表列出了本指南中提供有更多信息的主题。

表 4-6 管理拥有者

要	参见
向组中添加拥有者	第 62 页的“添加组成员”
向拥有者列表中添加组	第 63 页的“向组成员列表中添加组”
从拥有者列表中删除条目	第 63 页的“从组成员列表中删除条目”

管理另参见

另参见是对可能与当前组相关的其他目录条目的引用。用户可以通过它们轻松地找到与当前组相关的人员和其他组的条目。管理另参见的方法与管理组成员列表的方法相同。

下表列出了本指南中提供了更多信息的主题。

表 4-7 管理另参见

要	参见
向另参见添加用户	第 62 页的“添加组成员”
向另参见 添加组	第 63 页的“向组成员列表中添加组”
从另参见删除条目	第 63 页的“从组成员列表中删除条目”

重命名组

以下过程只适用于 LDAP 服务。重命名组条目时，只有组的名称会被更改。无法使用 "Rename Group" 特性将一个组织单位的条目移入另一个组织单位。例如，一个公司可能具有以下组织单位：

- Marketing 和 Product Management 组织单位
- Marketing 组织单位下名为 Online Sales 的组

在本例中，可以将组 Online Sales 重命名为 Internet Investments，但无法通过重命名条目使 Marketing 组织单位下的 Online Sales 变成 Product Management 组织单位下的 Online Sales。

重命名组

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Groups" 链接，按以下部分中所述找到想要管理的组：第 60 页的“查找组条目”。
3. 单击 "Rename Group" 按钮，在显示的页面上指定新的组名称，然后单击 "Save Changes"。

删除组

以下过程只适用于 LDAP 服务。

删除组

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Groups" 链接。
3. 按以下部分中所述找到想要管理的组：第 60 页的“查找组条目”，然后单击 "Delete Group"。

注	将不会删除组的单个成员，只会删除组条目。

创建组织单位

对于 LDAP 服务，组织单位可以包含若干个组，通常代表分支机构、部门或其他独立实体。DN 可以存在于一个以上组织单位中。

创建组织单位

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Create Organizational Unit" 链接。
3. 输入信息并单击 "Create"。有关特定字段的更多信息，参见联机帮助。

有关组织单位的注释：

- 新组织单位使用 `organizationalUnit` 对象类进行创建。
- 新组织单位的标识名具有如下格式：

  `ou=`*new organization*`,ou=`*parent organization*`, . . . ,o=`*base organization*`,c=`*country*

例如，如果在组织单位 West Coast 内创建名为 Accounting 的新组织单位，而基 DN 为 `o=Ace Industry,c=US`，则新组织单位的 DN 将是：

```
ou=Accounting,ou=West Coast,o=Ace Industry,c=US
```

管理组织单位

对于 LDAP 服务，通过 Administration Server 的 "Users and Groups" 选项卡上的 "Manage Organizational Units" 页面编辑和管理组织单位。

本节包括以下主题：

查找组织单位

以下过程只适用于 LDAP 服务。

查找组织单位

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Organizational Units" 链接。
3. 在 "Find Organizational Unit" 字段中输入要查找的单位的名称。可以输入任何以下类型的值：
   - 名称。输入全称或部分名称。将返回与搜索字符串完全匹配的所有条目。如果未找到这样的条目，将查找包含该搜索字符串的所有条目。如果未找到这样的条目，将查找发音与搜索字符串类似的所有条目。

- 使用星号 (*) 可以获得当前位于目录中的所有组。将该字段留空也可以实现这一目的。
- 任意 LDAP 搜索过滤器。包含等号 (=) 的任何字符串均被认为是搜索过滤器。

还可以使用 "Find All Units Whose" 部分中的下拉式菜单来缩小搜索结果的范围。有关更多信息，参见第 67 页的“Find All Units Whose 部分”。

4. 在 "Look Within" 字段中，选择要在其中搜索条目的组织单位。默认值为目录的根点（最顶端的条目）。
5. 在 "Format" 字段中指定是否对输出进行格式设置，以便在屏幕上显示或在打印机上打印。
6. 在本过程中的任何阶段单击 "Find" 按钮时，将显示与搜索条件匹配的所有组织单位。
7. 单击要显示的条目的链接。

Find All Units Whose 部分

对于 LADP 服务，可以通过 "Find All Units Whose" 部分生成自定义搜索过滤器。使用该部分中的字段可以缩小要不然将由 "Find Organizational Unit" 返回的搜索结果的范围。

左侧的下拉式列表指定搜索要依据的属性。可用选项如下：

- **Unit name。**搜索每个条目的全名以查找匹配条目。
- **Description。**搜索每个组织单位条目的描述以查找匹配项。

中间的下拉式列表指定要执行的搜索类型。可用选项如下：

- **Contains。**执行子串搜索。将返回属性值包含指定搜索字符串的条目。例如，如果知道组织单位的名称可能包含单词 "Administrator"，请在此选项中使用搜索字符串 "Administrator" 来查找组织单位条目。
- **Is。**执行精确匹配搜索。如果知道组织单位属性的确切值，请使用此选项。例如，知道组织单位名称的准确拼写。
- **Isn’t。**返回属性值与搜索字符串不精确匹配的所有条目。也就是说，如果要在目录中查找所有名称中不包含 "administrator" 的组织单位，请使用此选项。不过请注意，使用此选项可能导致返回极大数量的条目。
- **Sounds like。**执行近似或语音搜索。如果知道属性的值，但不能确定其拼写，请使用此选项。例如，不知道组织单位名称的拼写是 "Sarret’s list"、"Sarette’s list" 还是 "Sarett’s list"。

- **Starts with。**执行子串搜索。返回属性值以指定的搜索字符串开头的所有条目。例如，知道组织单位名称以 "Product" 开头，但不知道名称的其余部分。
- **Ends with。**执行子串搜索。返回属性值以指定搜索字符串结尾的所有条目。例如，知道组织单位名称以 "development" 结尾，但不知道名称的其余部分。

在右侧的文本字段中输入搜索字符串。要显示 "Look Within" 目录中包含的所有组织单位条目，请输入星号 (*) 或将此字段留空。

编辑组织单位属性

以下过程只适用于 LDAP 服务。

编辑组织单位条目

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Organizational Units" 链接。
3. 按以下部分中所述找到想要编辑的组织单位：第 66 页的“查找组织单位”。
4. 进行所需的更改。有关特定字段的更多信息，参见联机帮助。

注 可能需要更改组织单位编辑页面未显示的属性值。在这种情况下，请使用目录服务器的 `ldapmodify` 命令行实用程序（如果可用）。

重命名组织单位

以下过程只适用于 LDAP 服务。重命名组织单位条目时，只有组织单位的名称会被更改。无法使用重命名特性将一个组织单位中的条目移入另一个组织单位。

重命名组织单位条目

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Organizational Units" 链接。
3. 按以下部分中所述找到想要编辑的组织单位：第 66 页的“查找组织单位”。
4. 单击 "Rename" 按钮，在显示的页面上输入新的组织单位名称，然后单击 "Save Changes"。

删除组织单位

以下过程只适用于 LDAP 服务。

删除组织单位条目

1. 访问 Administration Server 并单击 "Users and Groups" 选项卡。
2. 单击 "Manage Organizational Units" 链接。
3. 按以下部分中所述找到想要删除的组织单位：第 66 页的“查找组织单位”。
4. 单击 "Delete" 按钮，然后在出现的确认框中单击 "OK"。

第 5 章

使用证书和密钥

本章介绍如何使用证书和密钥验证来确保 Sun Java System Web Proxy Server 的安全性。Proxy Server 集成了所有 Sun Java System 服务器的安全体系结构，并建立在行业标准和公共协议基础之上，以获取最大程度的互操作性和一致性。

本章假设读者熟悉公共密钥加密的基本概念，包括加密和解密、公用密钥和专用密钥、数字证书和加密协议。有关更多信息，参见 Introduction to SSL。此文档所在网址为 http://docs.sun.com/source/816-6156-10/index.htm

本章包括以下各节：

基于证书的验证

验证是确认身份的过程。在网络交互环境中，验证是一方对另一方信任识别的过程。证书是支持验证的一种方法。

证书中包含的数字数据用于指定个人、公司或其他实体的名称，并证明证书中包含的公共密钥属于该实体。

客户机和服务器都可以拥有证书。服务器验证指客户机对服务器进行的信任识别（对被认为要对位于特定网络地址的服务器负责的组织进行识别）。客户机验证指服务器对客户机进行的信任识别（对被认为使用客户机软件的人员进行识别）。客户机可以有多个证书，如同一个人可以有几个不同的身份一样。

证书由证书授权机构 (CA) 颁发并进行数字签名。CA 可以是出售证书的公司，也可以是负责为公司的内联网或外联网颁发证书的部门。您可以将您充分信任的 CA 确定为其他用户身份的验证方。

除公共密钥和由证书标识的实体名称之外，证书还包括到期日期、颁发该证书的 CA 的名称和颁发该证书的 CA 的数字签名。

有关证书内容和格式的更多信息，参见 Introduction to SSL。

有关支持的证书扩展，参见 All About Certificate Extensions。此文档所在网址为 http://www.mozilla.org/projects/security/pki/nss/tech-notes/tn3.html

注 在激活加密之前必须安装服务器证书。

创建信任数据库

请求服务器证书之前，必须创建一个信任数据库。在 Proxy Server 中，Administration Server 和每个服务器实例都可以拥有自己的信任数据库。信任数据库只能在本地计算机上创建。

创建信任数据库时，您需要指定将用于密钥对文件的口令。您还需要此口令来启动使用加密通信的服务器。有关选择口令时的注意事项列表，参见第 105 页的“选择保密性强的口令”。

在信任数据库中，可以创建并存储公共密钥和专用密钥（称为密钥对文件）。密钥对文件将用于 SSL 加密。申请和安装服务器证书时将用到该密钥对文件。安装证书之后，证书将存储在信任数据库中。

密钥对文件以加密的形式存储在以下目录中：

server_root/alias/proxy-*serverid*-key3.db

Administration Server 中只能有一个信任数据库。每个服务器实例都可以拥有自己的信任数据库。

创建信任数据库

1. 访问 "Administration Server" 或 "Server Manager"，然后单击 "Security" 选项卡。
2. 单击 "Create Database" 链接。
3. 输入信任数据库的口令。
4. 再次输入口令，然后单击 "OK"。

使用 password.conf

默认情况下，Proxy Server 会在启动之前提示管理员输入密钥数据库口令。要重新启动无人参与的 Proxy Server，必须将口令保存在 password.conf 文件中。仅当系统受到充分保护时才可以这样做，以免文件和密钥数据库遭到破坏。

通常无法使用 /etc/rc.local 或 /etc/inittab 文件启动已启用 SSL 的 UNIX 服务器，因为该服务器在启动之前要求输入口令。尽管可以通过将口令以纯文本格式存储在某个文件中来自动启动启用了 SSL 的服务器，但建议不要使用这种方法。服务器的 password.conf 文件应归超级用户或安装服务器的用户所有，并且只有所有者具有此文件的读写权限。

在 UNIX 上，将启用了 SSL 的服务器的口令保存在 password.conf 文件中会带来很大的安全风险。任何可以访问该文件的用户都有权访问启用了 SSL 的服务器的口令。将启用了 SSL 的服务器的口令保存在 password.conf 文件中之前，请考虑可能带来的安全风险。

在 Windows 上，如果安装了 NTFS 文件系统，则应限制对包含 password.conf 文件（即使不使用该文件）的目录的访问权限，以保护包含该文件的目录。Administration Server 用户和 Proxy Server 用户应该具有对该目录的读写权限。保护该目录可以防止其他用户创建伪 password.conf 文件。您无法通过限制对 FAT 文件系统上的目录或文件的访问权限来保护它们。

自动启动启用了 SSL 的服务器

自动启动启用了 SSL 的服务器

1. 确保已启用 SSL。
2. 在 Proxy Server 实例的 `config` 子目录中创建新的 `password.conf` 文件。
   - 如果使用的是 Proxy Server 附带的内部 PKCS#11 软件加密模块，请输入以下信息：
     `internal:`*your_ password*
   - 如果使用的是其他 PKCS#11 模块（用于硬件加密或硬件加速器），请指定 PKCS#11 模块的名称，后跟口令。例如：
     `nFast:`*your_ password*

即使创建了 `password.conf` 文件之后，您在启动 Proxy Server 时始终会收到输入口令的提示。

申请和安装 VeriSign 证书

VeriSign 是 Proxy Server 首选的证书授权机构。该公司的技术可简化证书的申请过程。VeriSign 的优势在于能够直接将证书返回服务器。

为服务器创建证书信任数据库后，您可以申请一个证书并将其提交给 CA（证书授权机构）。如果公司有自己的内部 CA，则可以向该部门申请证书。如果打算从商业 CA 处购买证书，请选择一个 CA 并索要所需的特定格式信息。

Administration Server 中只能有一个服务器证书。每个服务器实例可以拥有自己的服务器证书。

本节包括以下主题：

申请 VeriSign 证书

申请 VeriSign 证书

1. 访问 "Administration Server" 或 "Server Manager"，然后单击 "Security" 选项卡。
2. 单击 "Request VeriSign Certificate" 链接。
3. 阅读显示的页面上列出的步骤，然后单击 "OK"。显示 "VeriSign Enrollment Wizard"，该向导可引导您完成申请过程。

安装 VeriSign 证书

安装 VeriSign 证书

1. 访问 "Administration Server" 或 "Server Manager"，然后单击 "Security" 选项卡。
2. 单击 "Install VeriSign Certificate" 链接。
3. 除非要使用外部加密模块，否则请从 "Cryptographic Module" 下拉式列表中选择 "Internal"。
4. 输入密钥对文件口令或 PIN。
5. 从下拉式列表中选择要检索的“事务 ID”，然后单击 "OK"。

申请和安装其他服务器证书

除 VeriSign 外，还可以从其他证书授权机构申请和安装证书。您的公司或组织可能会提供自己的内部证书。本节介绍如何申请和安装其他类型的服务器证书。

本节包括以下主题：

所需的 CA 信息

开始申请过程之前，请确保您了解 CA 所需的信息。所需信息的格式因 CA 而异，但通常会请您提供以下列出的信息。请注意，证书更新通常不需要这些信息中的大部分内容。

- **Requestor name。**将获发证书者的名称。
- **Telephone number。**申请者的电话号码。
- **Common name。**DNS 查找中使用的全限定主机名（例如，`www.example.com`）。
- **Email address。**您与 CA 之间进行通信联系时使用的企业电子邮件地址。
- **Organization。**您的公司、教育机构和组织等的正式法定名称。多数 CA 要求使用法律文件（例如营业执照副本）证实此信息。

- **Organizational unit**。您公司内部组织单位的说明。
- **Locality**。组织所在城市、公国或者国家 / 地区的说明。
- **State or Province**。企业所在的州或省。
- **Country**。您所在国家 / 地区名称的双字符缩写（ISO 格式）。例如，美国的国家代码为 US。

所有这些信息组合为一系列属性值对（称为标识名 (DN)），用于唯一标识证书的主题。

如果从商业 CA 处购买证书，则必须在 CA 颁发证书之前与之联络，以查明他们所需的其他信息。多数 CA 都要求您提供身份证明。例如，CA 需要验证您的公司名称和公司授权管理服务器的用户，并且可能会询问您是否具有使用您提供的信息的合法权利。

某些商业 CA 向出具较为详细身份证明的组织或个人提供内容更为详细且精确的证书。例如，您购买的证书可能会声明 CA 不仅证实了您是 `www.example.com` 计算机的合法管理员，而且您的公司从事商业活动已达三年且无重大客户诉讼案件。

申请其他服务器证书

申请其他服务器证书

1. 访问 "Administration Server" 或 "Server Manager"，然后单击 "Security" 选项卡。
2. 单击 "Request Certificate" 链接。
3. 指定这是一个新证书，还是证书更新。许多证书在一段时间（例如六个月或一年）后会到期。某些 CA 会自动发送证书更新。
4. 指定所需的证书申请提交方式：
   - 要使用电子邮件提交申请，请选择 "CA Email Address"，然后输入用于此类申请的相应电子邮件地址。
   - 要使用 CA 的 Web 站点提交申请，则请选择 "CA URL"，然后输入用于此类申请的相应 URL。
5. 从 "Cryptographic Module" 下拉式列表中，选择申请证书时密钥对文件要使用的加密模块。
6. 输入密钥对文件的口令。除非选择除 "Internal" 之外的加密模块，否则该口令是您创建信任数据库时指定的口令。服务器将使用该口令获取专用密钥并加密发送给 CA 的信息。然后将您的公共密钥和加密的信息发送给 CA。CA 使用公共密钥来解密您的信息。

7. 输入识别信息，例如姓名和电话号码。此信息的格式因 CA 而异。请注意，证书更新通常不需要此信息中的大部分内容。
8. 仔细检查输入的信息，确保准确，然后单击 "OK"。信息越准确，批准证书的速度可能就越快。如果申请将发至证书服务器，提交申请前会提示您检查表单信息。

服务器将生成包含您的信息的证书申请。该申请中包含使用专用密钥创建的数字签名。CA 使用数字签名验证申请从服务器计算机路由至 CA 的过程中是否未被篡改。极少数情况下，申请被篡改时，CA 通常会通过电话与您联络。

如果选择通过电子邮件发送申请，服务器将撰写包含申请的电子邮件消息，并将此消息发送给 CA。通常，证书会通过电子邮件返回。如果您指定了指向证书服务器的 URL，服务器将使用此 URL 向证书服务器提交申请。您可能收到电子邮件或其他方式的答复，具体方式因 CA 而异。

如果 CA 同意向您颁发证书，则会通知您。多数情况中，CA 会使用电子邮件向您发送证书。如果您的组织使用证书服务器，则可使用证书服务器的表单来搜索证书。

注 并不是所有从商业 CA 申请证书的用户都会获得证书。很多 CA 在颁发证书之前都需要您提供身份证明。而且，经常需要一天到几周的时间才能获得批准。您负责及时向 CA 提供所有必需的信息。

收到证书后即可安装。在此期间，您仍可使用未安装 SSL 的 Proxy Server。

安装其他服务器证书

从 CA 收到证书时，证书已通过您的公共密钥加密，因此只有您可以将其解密。只有输入正确的信任数据库口令，才能解密和安装证书。

证书有三种类型：

- 提供给客户机的您自己的服务器证书
- 证书链中使用的 CA 自己的证书
- 可信 CA 的证书

证书链是由各证书授权机构依次签署的一系列分层证书。CA 证书用于标识证书授权机构，以及签署由该机构颁发的证书。反过来，CA 证书又可以由父 CA 的 CA 证书签署，依此类推，直到根 CA。

注 如果您的 CA 未自动向您发送其证书，请进行申请。很多 CA 将他们的证书和您的证书在电子邮件中一并发送，您的服务器将同时安装这两个证书。

从 CA 收到证书时，证书已通过您的公共密钥加密，因此只有您可以将其解密。安装证书时，Proxy Server 将使用您指定的密钥对文件口令解密证书。如下列步骤所述，您可以将电子邮件保存在服务器可访问的位置，也可以复制电子邮件的文本，并准备将其粘贴到 "Install Certificate" 表单中。

安装其他服务器证书

1. 访问 "Administration Server" 或 "Server Manager"，然后单击 "Security" 选项卡。
2. 单击 "Install Certificate" 链接。
3. 在 "Certificate For" 旁，选择要安装的证书类型：
   - This Server
   - Server Certificate Chain
   - Certification Authority

   有关特定设置的更多信息，参见联机帮助。
4. 从下拉式列表中选择加密模块。
5. 输入密钥对文件口令。
6. 在步骤 3 中选择了 "Server Certificate Chain" 或 "Certification Authority" 时，请输入证书名称。
7. 通过执行以下操作之一，提供证书信息：
   - 选择 "Message Is In This File"，然后输入含有 CA 证书的文件的完整路径名。
   - 选择 "Message Text (with headers)"，然后复制并粘贴 CA 证书的内容。确保包含 "Begin Certificate" 和 "End Certificate" 标头，包含起始和终止连字符。
8. 单击 "OK"。
9. 选择以下任一选项：
   - "Add Certificate"（如果要安装新的证书）。
   - "Replace Certificate"（如果要安装证书更新）。

证书将存储在服务器的证书数据库中。例如：

server_root`/alias/proxy-`*serverid*`-cert8.db`

迁移证书

从 Sun ONE Web Proxy Server 3.6（也称为 iPlanet Web Proxy Server）迁移到 Sun Java System Web Proxy Server 4 时，包括信任数据库和证书数据库在内的文件会自动更新。

请确保 Proxy Server 4 Administration Server 对旧的 3.x 数据库文件有读取权限。这些文件是位于 *3.x_server_root*/alias 目录中的 *alias*-cert.db 和 *alias*-key.db。

只有对服务器启用了安全性时才能迁移密钥对文件和证书。也可以使用 Administration Server 和 Server Manager 中 "Security" 选项卡下的 "Migrate 3.x Certificates" 选项自动迁移密钥和证书。有关特定设置的信息，参见联机帮助。

在以前的版本中，证书和密钥对文件通过可由多个服务器实例使用的别名区分。Administration Server 管理所有别名及其委托证书。在 Sun Java System Web Proxy Server 4 中，Administration Server 和每个服务器实例都有自己的证书和密钥对文件，称为信任数据库而不是别名。

对于 Administration Server 本身而言，通过 Administration Server 管理信任数据库及其委托证书，对于服务器实例，则通过 Server Manager 进行管理。证书和密钥对数据库文件现在按使用它们的服务器实例命名。在以前的版本中，如果多个服务器实例共用同一别名，迁移时将为新服务器实例重命名证书和密钥对文件。

系统会迁移与服务器实例关联的整个信任数据库。以前数据库中列出的所有 CA 都会迁移到 Proxy Server 4 数据库中。如果出现重复的 CA，请使用以前的 CA，直到过期。请不要删除重复的 CA。

Proxy Server 3.x 证书迁移到支持的网络安全性服务 (NSS) 格式。将根据访问证书时使用的 "Proxy Server" 页面命名证书（即，从 "Administration Server Security" 选项卡或 "Server Manager Security" 选项卡）。

迁移证书

1. 从本地计算机访问 Administration Server 或 Server Manager，然后单击 "Security" 选项卡。
2. 单击 "Migrate 3.x Certificates" 链接。
3. 指定安装 3.6 服务器的根目录。
4. 指定此计算机的别名。
5. 输入管理员口令，然后单击 "OK"。

使用内置根证书模块

Proxy Server 附带的动态可装入根证书模块中有许多 CA 的根证书，包括 VeriSign。通过这一根证书模块，您可以更容易地将根证书升级到更高版本。以前必须逐一删除旧的根证书，然后再逐一安装新证书。现在，要安装常用的 CA 证书，只需在通过 Proxy Server 的后续版本获得新版本的根证书模块文件时，将原根证书模块文件更新到新版本即可。

因为根证书是作为 PKCS #11 加密模块实现的，所以无法删除该模块包含的根证书，管理这些证书时也不会提供删除证书的选项。要从服务器实例中删除根证书，可以通过删除服务器的 `alias` 文件中的以下内容来禁用根证书模块：

- `libnssckbi.so`（在多数 UNIX 平台上）
- `nssckbi.dll`（在 Windows 上）

如果以后要恢复根证书模块，可将扩展程序从 *server_root*`/bin/proxy/lib` (UNIX) 或 *server_root*`\bin\proxy\bin` (Windows) 复制回 `alias` 子目录。

您可以修改根证书的信任信息。信任信息将写入编辑的服务器实例的证书数据库中，而不是返回根证书模块本身。

管理证书

您可以查看、删除或编辑服务器上安装的各种证书的信任设置。其中包括您自己的证书和来自 CA 的证书。

管理证书

1. 访问 "Administration Server" 或 "Server Manager"，然后单击 "Security" 选项卡。
2. 单击 "Manage Certificates" 链接。
   - 如果要使用内部加密模块管理默认配置的证书，将显示所有已安装证书的列表，其中包括证书的类型和截止日期。所有证书都存储在 *server_root*`/alias` 目录中。
   - 如果使用硬件加速器等外部加密模块，必须首先为每个特定模块输入口令，然后单击 "OK"。证书列表将更新，以加入模块中所含的证书。
3. 单击要管理的证书的名称。随即显示一个页面，其中列有此类证书的管理选项。只有 CA 证书允许您设置或取消设置客户机信任。某些外部加密模块不允许删除证书。

4. 指定所需操作。可用选项如下：
   - "Delete Certificate" 或 "Quit"（对于内部获得的证书）
   - "Set client trust"、"Unset server trust" 或 "Quit"（对于 CA 证书）

证书信息中包含所有者和颁发证书的机构。通过信任设置，您可以设置客户机信任或取消设置服务器信任。对于 LDAP 服务器证书，服务器必须被信任。

安装和管理 CRL 和 CKL

证书撤销列表 (CRL) 和损坏的密钥列表 (CKL) 能够清楚地列出客户机或服务器用户应不再信任的所有证书和密钥。如果证书中的数据发生变化（例如，某位用户在证书到期之前更换了办公室或离开了组织），该证书将被撤回，其数据将显示在 CRL 中。如果密钥被更改或受到某种程度的损坏，密钥及其数据将显示在 CKL 中。CRL 和 CKL 都由 CA 生成并定期更新。请联络指定的 CA，获取这些列表。

本节包括以下主题：

安装 CRL 或 CKL

安装 CRL 或 CKL

1. 从 CA 获得 CRL 或 CKL 并下载到本地目录。
2. 访问 "Administration Server" 或 "Server Manager"，然后单击 "Security" 选项卡。
3. 单击 "Install CRL/CKL" 链接。
4. 选择以下任一选项：
   - Certificate Revocation List
   - Compromised Key List
5. 输入关联文件的完整路径名，然后单击 "OK"。显示 "Add Certificate Revocation List" 或 "Add Compromised Key List" 页面，列出 CRL 或 CKL 信息。如果数据库中已存在 CRL 或 CKL，将显示 "Replace Certificate Revocation List" 或 "Replace Compromised Key List" 页面。
6. 添加或替换 CRL 或 CKL。

管理 CRL 和 CKL

管理 CRL 和 CKL

1. 访问 "Administration Server" 或 "Server Manager"，然后单击 "Security" 选项卡。
2. 单击 "Manage CRL/CKL" 链接。显示 "Manage Certificate Revocation Lists"/"Compromised Key Lists" 页面，列出已安装的所有 CRL 和 CKL 及其截止日期。
3. 从 "Server CRLs" 或 "Server CKLs" 列表中选择证书。
4. 选择 "Delete CRL" 或 "Delete CKL" 删除 CRL 或 CKL，或者选择 "Quit" 返回管理页面。

设置安全首选项

获得证书后，即可开始确保您服务器的安全。如本节所述，Sun Java System Web Proxy Server 提供了许多安全元素。

加密是转换信息、使除预期接收者以外的任何人都无法识别信息的过程。解密是变换加密信息、使其重新可被识别的过程。Proxy Server 支持安全套接字层 (SSL) 和传输层安全性 (TLS) 加密协议。

加密算法是一种用于加密或解密的密码算法（一种数学函数）。SSL 和 TLS 协议包含了多个加密算法套件。某些加密算法比其他加密算法更强大、更安全。一般而言，加密算法使用的位越多，将数据解密越难。

在任何双向加密过程中，双方都必须使用相同的加密算法。由于可以使用多种加密算法，因此必须为服务器启用最常用的加密算法。

在安全连接过程中，客户机和服务器都同意使用可以进行通信的最强大的加密算法。您可以从 SSL 2.0、SSL 3.0 和 TLS 协议中选择加密算法。

注 SSL 2.0 后对安全性和性能进行了改善。除非存在无法使用 SSL 3.0 的客户机，否则请不要使用 SSL 2.0。客户机证书并非肯定都能使用 SSL 2.0 加密算法。

只靠加密过程并不足以确保服务器机密信息的安全。使用加密算法的同时还必须使用密钥，以达到真正的加密效果，或解密以前加密的信息。加密过程使用以下两种密钥获得此效果：公共密钥和专用密钥。使用公共密钥加密的信息只能使用关联的专用密钥进行解密。公共密钥随证书发布。受保护的只有关联的专用密钥。

有关各种加密算法套件的说明以及密钥和证书的更多信息，参见 Introduction to SSL。

要指定服务器可以使用的加密算法，请在 Proxy Server 用户界面的列表中进行选择。除非有充分的理由不使用特定的加密算法，否则应选择全部算法（尽管可能并不希望启用加密效果并非最优的加密算法）。

注意 请不要选择 "Enable No Encryption, Only MD5 Authentication"。如果客户机没有其他加密算法，服务器将默认使用此设置且不进行加密。

本节包括以下主题：

SSL 和 TLS 协议

Proxy Server 支持加密通信的 SSL 和 TLS 协议。SSL 和 TLS 独立于应用程序，并且其上可透明层叠更高级的协议。

SSL 和 TLS 协议支持用于服务器和客户机的相互验证、传输证书和建立会话密钥的各种加密算法。客户机和服务器可以支持各种加密算法套件或加密算法集合，这取决于各种因素：例如所支持的协议、公司有关加密强度的政策以及政府对加密软件出口的限制。在其他函数中，SSL 和 TLS 握手协议将确定服务器和客户机如何协商以决定将用来通信的加密算法套件。

使用 SSL 与 LDAP 通信

您应该要求 Administration Server 使用 SSL 与 LDAP 进行通信。

在 Administration Server 上启用 SSL

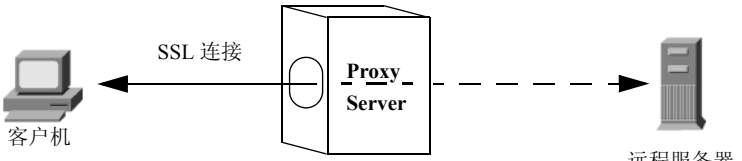
1. 访问 Administration Server 并单击 "Global Settings" 选项卡。
2. 单击 "Configure Directory Service" 链接。

3. 在显示的表中，单击目录服务的链接。显示 "Configure Directory Service" 页面。如果尚未创建基于 LDAP 的目录服务，请从 "Create New Service of Type" 下拉式列表中选择 "LDAP Server"，然后单击 "New" 以配置目录服务。有关为基于 LDAP 目录服务显示的特定字段的更多信息，参见联机帮助。
4. 选择 "Yes" 使用 SSL 进行连接，然后单击 "Save Changes"。

通过 Proxy Server 建立 SSL 隧道

当 Proxy Server（代理服务器）在转发方向运行而客户机又通过此代理服务器请求与安全服务器的 SSL 连接时，代理服务器会打开与安全服务器的连接，然后只双向复制数据，而不干预安全事务。此过程称为建立 SSL 隧道，如下图所示。

图 5-1 建立 SSL 连接时，Proxy Server 无法查看自己传送的数据。



要对 HTTPS URL 使用 SSL 隧道，客户机必须支持 SSL 和 HTTPS。HTTPS 通过对标准 HTTP 使用 SSL 实现。不支持 HTTPS 的客户机通过使用 Proxy Server 的 HTTPS 代理功能也可以访问 HTTPS 文档。

SSL 隧道是较低级的活动，不会影响应用程序级 (HTTPS)。SSL 隧道与未使用代理的 SSL 一样安全。中间存在的代理服务器不会对安全性构成任何负面影响或降低 SSL 的功能。

使用 SSL 时，数据流会被加密，因此代理服务器无法访问实际事务。因此，访问日志无法列出从远程服务器接收的状态码或标头长度。这也防止了代理服务器或其他任何第三方窃听事务。

由于代理服务器无法查看数据，因此无法验证客户机和远程服务器之间的通话协议是否为 SSL。这意味着代理服务器也无法阻止其他协议通过。您应将 SSL 限制为仅连接由 Internet 分配号码授权机构 (IANA) 分配的常用 SSL 端口，即 HTTPS 的 443 端口和 SNEWS 的 563 端口。如果有在其他端口运行安全服务器的站点，可以明确规定特例，允许某些主机连接其他端口。此操作通过 `connect://.*` 资源完成。

SSL 隧道功能实际上是一项类似于 SOCKS 的常规功能，它独立于协议，因此也可对其他服务使用此功能。Proxy Server 可为支持 SSL 的任何应用程序处理 SSL 隧道，而不仅仅是 HTTPS 和 SNEWS 协议。

配置 SSL 隧道

以下步骤说明如何配置 Proxy Server，以建立 SSL 隧道。

配置 SSL 隧道

1. 访问服务器实例的 Server Manager，然后单击 "Routing" 选项卡。
2. 单击 "Enable/Disable Proxying" 链接。
3. 从下拉式列表中选择 `connect://.*.443` 资源。`connect://` 方法是内部代理服务器表示法，在代理服务器外不适用。有关 `connect` 的更多信息，参见第 85 页的“SSL 隧道详细技术信息”中的以下描述。要允许连接其他端口，可使用模板中相似的 URL 模式。有关模板的更多信息，参见第 319 页的第 16 章“管理模板和资源”。
4. 选择 "Enable Proxying Of This Resource"，然后单击 "OK"。

注意 如果代理服务器配置错误，则可能发生滥用 SSL 代理来实现远程登录跳跃的情况。有些人会用代理服务器使远程登录连接显示为来自代理服务器主机，而非实际连接的主机。因此，除确实必要的端口外不能允许其他端口，并要对代理服务器使用访问控制（限制客户机主机）。

SSL 隧道详细技术信息

实际上，SSL 隧道使用 `CONNECT` 方法，将目标主机名和端口号作为参数，后跟空行：

```
CONNECT energy.example.com:443 HTTP/1.0
```

来自 Proxy Server 的成功应答如下，后跟空行：

```
HTTP/1.0 200 Connection established
Proxy-agent: Sun-Java-System-Web-Proxy-Server/4.0
```

随后在客户机和远程服务器之间建立连接，数据可双向传送，直至任何一方关闭连接。

实际上，为受益于基于 URL 模式的标准配置机制，主机名和端口号 (`energy.example.com:443`) 会自动映射到 URL 中，如下所示：

```
connect://energy.example.com:443
```

`connect://` 只是 Proxy Server 使用的内部表示法，以使配置更容易并与其他 URL 模式一致。在 Proxy Server 之外，不存在 `connect` URL，并且 Proxy Server 从网络收到此类 URL 时，会将其标记为无效并拒绝为该请求提供服务。

为侦听套接字启用安全性

您可以通过执行以下操作确保服务器侦听套接字的安全：

- 打开安全性
- 为侦听套接字选择服务器证书
- 选择加密算法

打开安全性

为侦听套接字配置其他安全设置之前，必须打开安全性。您可以在创建新的侦听套接字或编辑现有侦听套接字时打开安全性。

创建侦听套接字时打开安全性

1. 访问 Administration Server 或 Server Manager，然后单击 "Preferences" 选项卡。
2. 单击 "Add Listen Socket" 链接。
3. 输入所需的信息。要打开安全性，请从 "Security" 下拉式列表中选择 "Enabled"，然后单击 "OK"。请注意，如果尚未安装服务器证书，则只能选择 "Disabled"。有关特定设置的更多信息，参见联机帮助。

注	创建侦听套接字后，使用 "Edit Listen Sockets" 链接来配置安全性设置。

编辑侦听套接字时打开安全性

1. 访问 Administration Server 或 Server Manager，然后单击 "Preferences" 选项卡。
2. 单击 "Edit Listen Sockets" 链接。
3. 单击要编辑的侦听套接字的链接。
4. 要打开安全性，请从 "Security" 下拉式列表中选择 "Enabled"，然后单击 "OK"。请注意，如果尚未安装服务器证书，则只能选择 "Disabled"。

选择侦听套接字的服务器证书

您可以在 Administration Server 或 Server Manager 中配置侦听套接字，以使用您已申请和安装的服务器证书。

注 必须至少安装一个证书。

为侦听套接字选择服务器证书

1. 访问 Administration Server 或 Server Manager，然后单击 "Preferences" 选项卡。
2. 单击 "Edit Listen Sockets" 链接。
3. 单击要编辑的侦听套接字的链接。
4. 要打开安全性，请从 "Security" 下拉式列表中选择 "Enabled"，然后单击 "OK"。请注意，如果尚未安装服务器证书，则只能选择 "Disabled"。
5. 选择 "Enabled" 并单击 "OK" 后，请从 "Server Certificate Name" 下拉式列表中为侦听套接字选择服务器证书，然后单击 "OK"。

选择加密算法

要保护 Proxy Server 的安全性，应启用 SSL。您可以启用 SSL 2.0、SSL 3.0 和 TLS 加密协议并选择各种加密算法套件。可以在侦听套接字上为 Administration Server 启用 SSL 和 TLS 协议。在侦听套接字上为 Server Manager 启用 SSL 和 TLS 可为特定的服务器实例设置安全性首选项。必须至少安装一个证书。

注 在侦听套接字上启用 SSL 只适用于反向代理环境。换言之，只有将 Proxy Server 配置为执行反向代理时才可应用。

默认设置允许使用最常用的加密算法。除非有充分的理由不使用特定的加密算法套件，否则应全部选中。有关特定加密算法的更多信息，参见 Introduction to SSL。

系统将 TLS 回滚的默认和推荐设置设为 "Enabled"。这会将服务器配置为检测人为版本回滚攻击。要实现与某些未正确实现 TLS 规范的客户机的互操作性，可能要将此值设置为 "Disabled"。

请注意，禁用 TLS 回滚将使连接容易遭到版本回滚攻击。版本回滚攻击是一种机制，第三方可以通过这种机制强制客户机和服务器使用安全性较低的早期协议（例如 SSL 2.0）进行通信。由于 SSL 2.0 协议中存在已知的缺陷，因此无法检测到版本回滚攻击企图，这使得第三方更容易截取和解密加密的连接。

启用 SSL 和 TLS

1. 访问 Administration Server 或 Server Manager，然后单击 "Preferences" 选项卡。
2. 单击 "Edit Listen Sockets" 链接，然后单击要编辑的侦听套接字的链接。对于安全的侦听套接字，将显示可用的加密算法设置。

注 如果侦听套接字未启用安全性，则不会列出任何 SSL 和 TLS 信息。要使用加密算法，请确保已在选定侦听套接字上启用了安全性。有关更多信息，参见第 86 页的“为侦听套接字启用安全性”。

3. 选中所需加密设置对应的复选框，然后单击 "OK"。

注 对于 Netscape Navigator 6.0，请选择 TLS 和 SSL 3.0。对于 TLS 回滚也要选择 TLS，并确保禁用了 SSL 3.0 和 SSL 2.0。

在服务器上启用 SSL 后，其 URL 将使用 `https`，而非 `http`。指向启用了 SSL 的服务器上文档的 URL 具有以下格式：

`https://`*servername*`.`*domain*`.`*dom*`:`*port*

例如，`https://admin.example.com:443`。

如果使用默认的安全 HTTP 端口 (443)，则无需在 URL 中输入端口号。

全局配置安全性

安装启用了 SSL 的服务器将在 `magnus.conf` 文件（服务器的主配置文件）中为全局安全性参数创建指令条目。

设置 SSL 配置文件指令的值

1. 访问服务器实例的 Server Manager。
2. 确保为要配置的侦听套接字启用了安全性。有关更多信息，参见第 86 页的“为侦听套接字启用安全性”。
3. 手动编辑 `magnus.conf` 文件，并输入以下设置的值：
   - `SSLSessionTimeout`
   - `SSLCacheEntries`
   - `SSL3SessionTimeout`

这些 SSL 配置文件指令在下文说明。有关 magnus.conf 的更多信息，参见 Proxy Server Configuration File Reference。

SSLSessionTimeout

SSLSessionTimeout 指令用于控制 SSL 2.0 会话缓存。

语法

SSLSessionTimeout *seconds*

其中 *seconds* 是缓存的 SSL 会话保持有效的秒数。默认值为 100 秒。如果指定了 SSLSessionTimeout 指令，秒数的值将自动限定为 5 到 100 之间。

SSLCacheEntries

指定可以缓存的 SSL 会话的数量。

SSL3SessionTimeout

SSL3SessionTimeout 指令用于控制 SSL 3.0 和 TLS 会话缓存。

语法

SSL3SessionTimeout *seconds*

其中 *seconds* 是缓存的 SSL 3.0 会话保持有效的秒数。默认值为 86400 秒（24 小时）。如果指定了 SSL3SessionTimeout 指令，秒数的值将自动限定为 5 到 86400 之间。

使用外部加密模块

Proxy Server 支持以下使用外部加密模块（例如智能卡或令牌环）的方法：

- PKCS #11
- FIPS-140

激活 FIPS-140 加密标准前，必须添加 PKCS #11 模块。

本节包括以下主题：

安装 PKCS #11 模块

Proxy Server 支持公共密钥加密标准 (PKCS) #11，该标准定义了在 SSL 和 PKCS#11 模块之间通信所用的接口。PKCS #11 模块用于指向 SSL 硬件加速器的基于标准的连接。外部硬件加速器的导入证书和密钥存储在 secmod.db 文件中，该文件在安装 PKCS #11 模块时生成。文件位于 *server_root*/alias 目录中。

使用 modutil 安装 PKCS #11 模块

可使用 modutil 工具以 .jar 文件或对象文件的形式安装 PKCS #11 模块。

使用 modutil 安装 PKCS #11 模块

1. 确保包括 Administration Server 在内的所有服务器均已关闭。
2. 转至包含数据库的 *server_root*/alias 目录。
3. 将 *server_root*/bin/proxy/admin/bin 添加到 PATH 中。
4. 在 *server_root*/bin/proxy/admin/bin 中找到 modutil。
5. 设置环境。例如：
   - 在 UNIX 上：setenv

     LD_LIBRARY_PATH *server_root*/bin/proxy/lib:${LD_LIBRARY_PATH}
   - 在 Windows 上，将以下内容添加到 PATH

     LD_LIBRARY_PATH *server_root*/bin/proxy/bin

     您可以在以下目录中找到您计算机的 PATH：
     server_root/proxy-admserv/start。
6. 输入命令：modutil。将列出各种选项。
7. 执行所需的操作。

   例如，要在 UNIX 中添加 PCKS #11 模块，请输入：

   modutil -add（PKCS#11 文件的名称）-libfile（PKCS #11 的 libfile）
   -nocertdb -dbdir。（您的 db 目录）

使用 pk12util

使用 pk12util 可以从内部数据库中导出证书和密钥，并将其导入内部或外部 PKCS #11 模块。您可以将证书和密钥始终导出到内部数据库中，但多数外部令牌不会允许您导出证书和密钥。默认情况下，pk12util 使用名为 cert8.db 和 key3.db 的证书和密钥数据库。

使用 pk12util 导出

从内部数据库导出证书和密钥

1. 转至包含数据库的 *server_root*/alias 目录。
2. 将 *server_root*/bin/proxy/admin/bin 添加到 PATH 中。
3. 在 *server_root*/bin/proxy/admin/bin 中找到 pk12util。
4. 设置环境。例如：
   - 在 UNIX 上：setenv

     LD_LIBRARY_PATH/*server_root*/bin/proxy/lib:${LD_LIBRARY_PATH}
   - 在 Windows 上，将以下内容添加到 PATH

     LD_LIBRARY_PATH *server_root*/bin/proxy/bin

     您可以在以下目录中找到您计算机的 PATH：
     server_root/proxy-admserv/start。
5. 输入命令：pk12util。将列出各种选项。
6. 执行所需的操作。

   例如，在 UNIX 中输入：

   ```
   pk12util -o certpk12 -n Server-Cert [-d /server/alias] [-P https-test-host]
   ```
7. 输入数据库口令。
8. 输入 pkcs12 口令。

使用 pk12util 导入

将证书和密钥导入内部或外部 PKCS #11 模块

1. 转至包含数据库的 *server_root*/alias 目录。
2. 将 *server_root*/bin/proxy/admin/bin 添加到 PATH 中。
3. 在 *server_root*/bin/proxy/admin/bin 中找到 pk12util。
4. 设置环境。例如：
   - 在 UNIX 上：setenv

     LD_LIBRARY_PATH/*server_root*/bin/proxy/lib:${LD_LIBRARY_PATH}

- 在 Windows 上，将以下内容添加到 PATH

  LD_LIBRARY_PATH *server_root*/bin/proxy/bin

  您可以在以下目录中找到您计算机的 PATH：*server_root*/proxy-admserv/start。

5. 输入命令：pk12util。将列出各种选项。
6. 执行所需的操作。

   例如，在 UNIX 中输入：

   ```
   pk12util -i pk12_sunspot [-d certdir][-h "nCipher"][-P
   https-jones.redplanet.com-jones-]
   ```

   -P 必须跟在 -h 后面，并且必须是最后一个参数。

   输入正确的令牌名，包括引号之间的大写字母和空格。
7. 输入数据库口令。
8. 输入 pkcs12 口令。

使用外部证书启动服务器

如果服务器的证书安装在外部 PKCS #11 模块（例如，硬件加速器），服务器将无法使用该证书启动，除非对 server.xml 文件进行编辑，或按如下所述指定证书名。

服务器始终尝试使用名为 Server-Cert 的证书启动。但对于外部 PKCS #11 模块中的证书，其标识符中会包含模块的某个令牌名。例如，名为 smartcard0 的外部智能卡读取器上安装的服务器证书会被命名为 smartcard0:Server-Cert。

要使用安装在外部模块中的证书启动服务器，必须为在其上运行服务器的侦听套接字指定证书名称。

为侦听套接字选择证书名称

为侦听套接字选择证书名称

如果未在侦听套接字上启用安全性，则不会列出证书信息。要为侦听套接字选择证书名称，首先必须确保已对侦听套接字启用安全性。有关更多信息，参见第 86 页的“为侦听套接字启用安全性”。

1. 访问 Administration Server 或 Server Manager，然后单击 "Preferences" 选项卡。
2. 单击 "Edit Listen Sockets" 链接。
3. 单击要与证书关联的侦听套接字的链接。

4. 从 "Server Certificate Name" 下拉式列表中为侦听套接字选择服务器证书，然后单击 "OK"。该列表中包含了所有已安装的内部和外部证书。

您也可以手动编辑 `server.xml` 文件，让服务器使用该服务器证书启动。将 `SSLPARAMS` 中的 `servercertnickname` 属性更改为：

```
$TOKENNAME:Server-Cert
```

要查找 `$TOKENNAME` 使用的值，请转至服务器的 "Security" 选项卡并选择 "Manage Certificates" 链接。当您登录到存储 Server-Cert 的外部模块时，`$TOKENNAME:$NICKNAME` 表单的列表中将显示其证书。

注 如果尚未创建信任数据库，您为外部 PKCS #11 模块请求或安装证书时将创建一个信任数据库。创建的默认数据库没有口令，且无法访问。外部模块将工作，但您不能申请和安装服务器证书。如果创建的默认数据库没有口令，请使用 "Security" 选项卡上的 "Create Database" 页面来设置口令。

FIPS-140 标准

通过 PKCS #11 API 可以与执行加密操作的软件或硬件模块进行通信。在 Proxy Server 上安装 PKCS #11 之后，可将服务器配置为与 (FIPS)-140 兼容（FIPS 代表“联邦信息处理标准”）。这些库只存在于 SSL 3.0 中。

启用 FIPS-140

1. 按照 FIPS-140 中的说明安装该插件。
2. 访问 Administration Server 或 Server Manager，然后单击 "Preferences" 选项卡。
3. 单击 "Edit Listen Sockets" 链接。对于安全侦听套接字，"Edit Listen Socket" 页面将显示可用的安全设置。

注 要使用 FIPS-140，请确保已在选定侦听套接字上启用了安全性。有关更多信息，参见第 86 页的“为侦听套接字启用安全性”。

4. 从 SSL 版本 3 的下拉式列表中选择 "Enabled"（如果尚未选择）。
5. 选择适当的 FIPS-140 加密算法套件，然后单击 "OK"：
   - 启用 168 位加密 Triple DES 和 SHA 验证 (FIPS)
   - 启用 56 位加密 DES 和 SHA 验证 (FIPS)

设置客户机安全要求

执行可确保服务器安全的所有步骤后，可以为客户机设置其他安全要求。

客户机验证对于 SSL 连接并非必不可少，但的确能为将加密信息发送给正确接收方提供额外的保证。您可在反向代理服务器中使用客户机验证，以确保内容服务器不会与未授权的代理服务器或客户机共享信息。

本节包括以下主题：

要求客户机验证

您可以为 Administration Server 和每个服务器实例启用侦听套接字，以要求客户机验证。启用客户机验证后，必须具备客户机证书，服务器才能将响应发送给查询。

Proxy Server 支持通过将客户机证书中的 CA 与用于签署客户机证书的信任 CA 相匹配来验证客户机证书。您可以在 "Security" 选项卡上的 "Manage Certificates" 页面中查看用于签署客户机证书的信任 CA 的列表。

您可以对 Proxy Server 进行配置，以拒绝没有来自可信 CA 的客户机证书的任何客户机。要接受或拒绝信任的 CA，必须为 CA 设置客户机信任。有关更多信息，参见第 80 页的“管理证书”。

如果证书已过期，Proxy Server 将记录错误、拒绝证书并向客户机返回一条消息。也可以从 "Manage Certificates" 页面中查看已过期的证书。

您可以对服务器进行配置，以便从客户机证书收集信息并将其与 LDAP 目录中的用户条目相匹配。这样可以确保客户机具有有效的证书和 LDAP 目录中的条目。而且还可以确保客户机证书与 LDAP 目录中的证书相匹配。要了解如何进行此操作，参见第 97 页的“将客户机证书映射到 LDAP”。

您可以将客户机证书和访问控制结合使用，以便除了来自信任的 CA 以外，与证书关联的用户还必须与访问控制规则 (ACL) 相匹配。有关更多信息，参见第 143 页的“使用访问控制文件”。

要求客户机验证

1. 访问 Administration Server 或 Server Manager，然后单击 "Preferences" 选项卡。
2. 单击 "Edit Listen Sockets" 链接。
3. 单击要对其要求客户机验证的侦听套接字对应的链接。
4. 使用 "Client Authentication" 下拉式列表对侦听套接字要求客户机验证，然后单击 "OK"。

反向代理服务器中的客户机验证

在反向代理服务器中，可根据以下方案中任何一个配置客户机验证：

- **代理服务器 - 验证 - 客户机。**使用此方案时，可以允许具有符合要求证书的所有客户机访问，或只允许具有符合要求的证书并且是您 Proxy Server 的访问控制列表上的认可用户的客户机访问。
- **内容服务器 - 验证 - 代理服务器。**使用此方案时，您可以确保内容服务器与 Proxy Server 而非其他服务器构成实际连接。
- **代理服务器 - 验证 - 客户机和内容服务器 - 验证 - 代理服务器。**此方案可为反向代理服务器提供最佳的安全性和验证。

有关如何配置这些方案的信息，参见第 95 页的“在反向代理服务器中设置客户机验证”。

在反向代理服务器中设置客户机验证

安全反向代理服务器中的客户机验证为确保连接的安全性提供了进一步的保障。以下说明阐述如何根据所选方案配置客户机验证。

注	每个方案均假定您同时拥有安全的“客户机 - 代理服务器”连接和安全的“代理服务器 - 内容服务器”连接。

代理服务器 - 验证 - 客户机

配置“代理服务器 - 验证 - 客户机”方案

1. 按照“设置反向代理服务器”主题中配置安全“客户机 - 代理服务器”和安全“代理服务器 - 内容服务器”方案的说明操作，该主题列于第 289 页的第 14 章“使用反向代理服务器”。

2. 访问服务器实例的 Server Manager，然后单击 "Preferences" 选项卡。
3. 单击 "Edit Listen Sockets" 链接，然后在显示的表中单击所需侦听套接字的链接。（使用 "Add Listen Socket" 链接可配置和添加侦听套接字。）
4. 指定客户机验证要求：

   要允许具备有效证书的所有用户访问：

   - 在 "Security" 部分，使用 "Client Authentication" 设置要求在此侦听套接字上进行客户机验证。请注意，如果尚未安装服务器证书，此设置将不可见。

   要仅允许既具备有效证书又在访问控制中被指定为可接受用户的用户访问：

   a. 在 "Security" 部分，将 "Client Authentication" 设置保留为关闭状态。请注意，如果尚未安装服务器证书，此设置将不可见。
   b. 在该服务器实例的 Server Manager "Preferences" 选项卡上，单击 "Administer Access Control" 链接。
   c. 选择一个 ACL，然后单击 "Edit" 按钮。显示 "Access Control Rules For" 页面（如果提示，请先进行验证）。
   d. 打开访问控制（如未选中 "Access control Is On" 复选框，请将其选中）。
   e. 将 Proxy Server 设置为作为反向代理服务器进行验证。有关更多信息，参见第 295 页的“设置反向代理服务器”。
   f. 单击所需访问控制规则的 "Rights" 链接，在下部框中指定访问权限，然后单击 "Update" 更新该条目。
   g. 单击 "Users/Groups" 链接。在下部框中，指定用户和组，选择 SSL 作为验证方法，然后单击 "Update" 更新此条目。
   h. 单击上部框中的 "Submit"，保存输入内容。

   有关访问控制设置的更多信息，参见第 135 页的第 8 章“控制对服务器的访问”。

内容服务器 - 验证 - 代理服务器

配置“内容服务器 - 验证 - 代理服务器”方案

1. 按照第 295 页的“设置反向代理服务器”中对配置安全“客户机 - 代理服务器”和安全“代理服务器 - 内容服务器”方案的说明进行操作。
2. 在内容服务器上，打开客户机验证。

注 您可以将此方案修改为与 Proxy Server 进行非安全客户机连接、与内容服务器进行安全连接，并使内容服务器验证 Proxy Server。要执行此操作，必须关闭加密，并使代理服务器仅按以下步骤所述初始化证书。

代理服务器 - 验证 - 客户机和内容服务器 - 验证 - 代理服务器

配置“代理服务器 - 验证 - 客户机和内容服务器 - 验证 - 代理服务器”方案

1. 按照配置“代理服务器 - 验证 - 客户机”方案的说明进行操作，相关说明见第 95 页的“代理服务器 - 验证 - 客户机”。
2. 在内容服务器上，打开客户机验证。

将客户机证书映射到 LDAP

本节介绍 Proxy Server 将客户机证书映射到 LDAP 目录中的条目时使用的过程。

服务器收到来自客户机的请求后，在处理请求之前会索要客户机的证书。某些客户机会在向服务器发送请求的同时发送客户机证书。

注 将客户机证书映射到 LDAP 之前，还必须配置所需的 ACL。有关更多信息，参见第 135 页的第 8 章“控制对服务器的访问”。

服务器将尝试查看该 CA 是否与 Administration Server 中的某个信任 CA 相匹配。如果不匹配，Proxy Server 将结束此连接。如果能够找到匹配的 CA，服务器将继续处理请求。

验证证书是来自信任的 CA 之后，服务器会通过执行以下操作将证书映射到某个 LDAP 条目：

- 将颁发者和主题 DN 从客户机证书映射到 LDAP 目录中的分支点。
- 在 LDAP 目录中搜索与客户机证书的主题（最终用户）相关信息相匹配的条目。
- （可选）验证客户机证书是否与对应于 DN 的 LDAP 条目中的证书相匹配。

服务器使用名为 `certmap.conf` 的证书映射文件来确定如何进行 LDAP 搜索。映射文件将告诉服务器要使用客户机证书中的哪些值（例如最终用户的名称、电子邮件地址等）。服务器将使用这些值搜索 LDAP 目录中的用户条目，但服务器首先必须确定从 LDAP 目录中的哪个位置开始搜索。证书映射文件也会告诉服务器开始搜索的位置。

服务器了解开始搜索的位置和需要搜索的内容（上述第一点）之后，将在 LDAP 目录中执行搜索（第二点）。如果未找到匹配条目或找到多个匹配条目，并且映射**未**设置为验证证书，搜索将失败。

下表列出了预期的搜索结果行为。请注意，可在 ACL 中指定预期行为。例如，可指定在证书匹配失败后，Proxy Server 只接受您访问。有关如何设置 ACL 首选项的更多信息，参见第 143 页的“使用访问控制文件”。

表 5-1 LDAP 搜索结果

LDAP 搜索结果	证书验证打开	证书验证关闭
未找到条目	验证失败	验证失败
只找到一个条目	验证失败	验证成功
找到多个条目	验证失败	授权失败

服务器在 LDAP 目录中找到匹配条目和证书后，即可使用该信息处理事务。例如，某些服务器使用证书 - 到 -LDAP (certificate-to-LDAP) 映射来确定对某台服务器的访问权限。

使用 certmap.conf 文件

证书映射用于确定服务器在 LDAP 目录中查找用户条目的方式。您可以使用 `certmap.conf` 配置证书（按名称指定）映射到 LDAP 条目的方式。您可以编辑此文件并添加条目，以与 LDAP 目录的组织结构相符并列出希望用户拥有的证书。用户可以基于 `subjectDN` 中使用的用户 ID、电子邮件或其他任何值进行身份验证。具体而言，映射文件可定义以下信息：

- 服务器应从 LDAP 树中的哪个位置开始搜索
- 在 LDAP 目录中进行搜索时，服务器应用作搜索条件的证书属性
- 服务器是否要进行其他验证过程

证书映射文件位于以下位置：

server_root`/userdb/certmap.conf`

该文件包含了一个或多个已命名的映射，每个映射都应用于不同的 CA。映射的语法如下：

`certmap` *name issuerDN*
name`:`*property* [*value*]

第一行用于指定条目的名称以及形成 CA 证书中唯一名称的属性。*name* 是任意的，可以定义为愿意使用的任何名称。但是，*issuerDN* 必须与颁发客户机证书的 CA 的颁发者 DN 完全匹配。例如，以下两行颁发者 DN 仅在分隔属性的空格上有所差异，但服务器将其视为两个不同的条目：

```
certmap sun1 ou=Sun Certificate Authority,o=Sun,c=US
certmap sun2 ou=Sun Certificate Authority, o=Sun, c=US
```

提示 如果使用的是 Sun Java System Directory Server，并遇到匹配颁发者 DN 问题，请检查 Directory Server 错误日志中是否存在有用的信息。

上述映射中的第二行和随后的行将各属性与值相匹配。`certmap.conf` 文件中包含六个默认属性（可以使用证书 API 自定义属性）：

- `DNComps` 是一系列由逗号分隔的属性，用于确定服务器从 LDAP 目录何处开始搜索匹配用户（即客户机证书的所有者）信息的条目。服务器从客户机证书中收集这些属性的值，并用这些值形成 LDAP DN，然后即可确定服务器从 LDAP 目录的哪个位置开始搜索。例如，如果将 `DNComps` 设置为使用 DN 的 `o` 和 `c` 属性，服务器将从 LDAP 目录中的 `o=`*org*、`c=` *country* 条目开始搜索，其中 *org* 和 *country* 将替换为证书 DN 中的值。

  请注意以下情况：

  - 如果映射中不存在 `DNComps` 条目，服务器将使用 `CmapLdapAttr` 设置或客户机证书中的整个主题 DN（即最终用户的信息）。
  - 如果 `DNComps` 条目存在但没有对应的值，服务器将在整个 LDAP 树中搜索与过滤器匹配的条目。

- `FilterComps` 是一系列由逗号分隔的属性，用于通过收集客户机证书中用户 DN 的信息来创建过滤器。服务器将使用这些属性的值，以形成用于匹配 LDAP 目录中各条目的搜索条件。如果服务器在 LDAP 目录中找到了一个或多个与从证书中收集到的用户信息相匹配的条目，则表示搜索成功并且服务器可以选择执行某个验证。

  例如，如果将 `FilterComps` 设置为使用电子邮件和用户 ID 属性 (`FilterComps=e,uid`)，服务器将在目录中搜索电子邮件和用户 ID 的值与从客户机证书中收集到的最终用户信息相匹配的条目。电子邮件地址和用户 ID 是非常好的过滤器，因为他们在目录中通常是唯一的。过滤器需要非常具体，才能只与 LDAP 数据库中的唯一条目匹配。

  过滤器的属性名应该是证书中的属性名，而不能是 LDAP 目录中的属性名。例如，某些证书中，用户的电子邮件地址的属性为 `e`，而 LDAP 则称该属性为 `mail`。

下表列出了 x509v3 证书的属性。

表 5-2 x509v3 证书的属性

属性	说明
c	国家 / 地区
o	组织
cn	通用名称
l	位置
st	状态
ou	组织单位
uid	UNIX/Linux 用户 ID
email	电子邮件地址

- verifycert 告诉服务器是否要将客户机的证书与在 LDAP 目录中找到的证书相比较。它使用两个值：on 和 off。只有 LDAP 目录中包含证书时才需要使用此属性。此功能有助于确保最终用户使用的证书有效且未被撤回。
- CmapLdapAttr 是 LDAP 目录中包含该用户所有证书的主题 DN 的属性名称。该属性的默认值为 certSubjectDN。该属性不是标准的 LDAP 属性，因此要使用该属性，必须扩展 LDAP 模式。有关更多信息，参见 Introduction to SSL。

  如果 certmap.conf 文件中存在此属性，服务器将在整个 LDAP 目录中搜索属性（以此属性命名）与主题的完整 DN（从证书中获得）相匹配的条目。如果未找到任何条目，服务器将使用 DNComps 和 FilterComps 映射重试搜索。

  当使用 DNComps 和 FilterComps 匹配条目遇到困难时，这种用于将证书与 LDAP 条目相匹配的方法非常有用。
- Library 是值为指向共享库或 DLL 的路径名的属性。只有使用证书 API 创建自己的属性时才需要使用此属性。
- InitFn 是值为自定义库中 init 函数名称的属性。只有使用证书 API 创建自己的属性时才需要使用此属性。

有关这些属性的更多信息，参阅相关示例，具体见第 101 页的“映射样例”。

创建自定义属性

您可以使用客户机证书 API 创建自己的属性。创建自定义映射后，就可以引用以下格式的映射：

name:library *path_to_shared_library*
name:InitFN *name_of_init_function*

例如：

```
certmap default1 o=Sun Microsystems, c=US
default1:library /usr/sun/userdb/plugin.so
default1:InitFn plugin_init_fn
default1:DNComps  ou o c
default1:FilterComps l
default1:verifycert on
```

映射样例

certmap.conf 文件中应至少包含一个条目。以下示例说明了使用 certmap.conf 的不同方式。

示例 1

本示例说明只有一个默认映射的 certmap.conf 文件：

```
certmap default default
default:DNComps ou, o, c
default:FilterComps e, uid
default:verifycert on
```

在本示例中，服务器在包含 ou=*orgunit*, o=*org*, c=*country* 条目的 LDAP 分支点处开始搜索，其中的斜体文本被替换为客户机证书中主题 DN 的值。

然后，服务器将使用证书中的电子邮件地址和用户 ID 的值在 LDAP 目录中搜索匹配的条目。找到匹配的条目时，服务器将比较客户机发送的证书和存储在目录中的证书，以验证该证书。

示例 2

以下示例文件中包括两个映射：一个是默认映射，另一个用于 US Postal Service：

```
certmap default default
default:DNComps
default:FilterComps e, uid
```

```
certmap usps ou=United States Postal Service, o=usps, c=US
usps:DNComps ou,o,c
usps:FilterComps e
usps:verifycert on
```

当服务器接收除 US Postal Service 之外任何人的证书时，会使用默认映射，从 LDAP 树的顶部开始并搜索与客户机的电子邮件和用户 ID 相匹配的条目。如果证书来自 US Postal Service，则服务器将在含有组织单位的 LDAP 分支处开始搜索与电子邮件地址相匹配的条目。另请注意，如果证书来自 US Postal Service，服务器将验证该证书。其他证书不会被验证。

注意 证书中的颁发者 DN（即 CA 的信息）必须与映射的第一行中所列的颁发者 DN 一致。在以上示例中，来自颁发者 DN（即 `o=United States Postal Service,c=US`）的证书就不匹配，因为 `o` 和 `c` 属性之间没有空格。

示例 3

以下示例使用 `CmapLdapAttr` Property 在 LDAP 数据库中搜索名为 `certSubjectDN` 的属性，该属性的值与客户机证书中的整个主题 DN 完全匹配。

```
certmap myco ou=My Company Inc, o=myco, c=US
myco:CmapLdapAttr certSubjectDN
myco:DNComps  o, c
myco:FilterComps mail, uid
myco:verifycert on
```

如果客户机证书主题为：

```
uid=Walt Whitman, o=LeavesOfGrass Inc, c=US
```

服务器将首先搜索包含以下信息的条目：

```
certSubjectDN=uid=Walt Whitman, o=LeavesOfGrass Inc, c=US
```

如果找到了一个或多个匹配的条目，服务器将继续验证各条目。如果未找到匹配的条目，服务器会使用 `DNComps` 和 `FilterComps` 搜索匹配的条目。在本示例中，服务器会在 `o=LeavesOfGrass Inc, c=US` 下的所有条目中搜索 `uid=Walt Whitman`。

注 本示例假设 LDAP 目录中包含带有 `certSubjectDN` 属性的条目。

设置更强大的加密算法

利用 Server Manager "Preferences" 选项卡上的 "Set Cipher Size" 选项可以选择使用 168 位、128 位或 56 位大小的密钥进行访问 或无大小限制。您可以指定不符合限制条件时使用的文件。如果未指定文件，Proxy Server 将返回 "Forbidden" 状态。

如果选择用于访问的密钥大小与 "Security Preferences" 下的当前加密算法设置不一致，Proxy Server 将显示一个弹出对话框，警告您需要启用带有更大密钥大小的加密算法。

密钥大小限制的实现基于 `obj.conf` 中的 NSAPI `PathCheck` 指令，而不是 `Service fn=key-toosmall`。该指令为：

`PathCheck fn="ssl-check" [secret-keysize=`*nbits*`] [bong-file=`*filename*`]`

其中，*nbits* 是密钥所需的最小位数，*filename* 是不符合限制条件时所用文件的名称。

如果未启用 SSL 或未指定 `secret-keysize` 参数，`PathCheck` 将返回 `REQ_NOACTION`。如果当前会话的密钥大小小于指定的 `secret-keysize`，函数将返回状态为 `PROTOCOL_FORBIDDEN` 的 `REQ_ABORTED`（如果未指定 `bong-file`），或者返回 `REQ_PROCEED`，并将路径变量设置为 `bong-file` *filename*。而且，如果不符合密钥大小限制条件，当前会话的 SSL 会话缓存项将失效，以便下次当同一台客户机连接到服务器时，发生完整的 SSL 握手。

注 "Set Cipher Size" 表单在添加 `PathCheck fn=ssl-check` 时会删除在对象中找到的任何 `Service fn=key-toosmall` 指令。

设置更强大的加密算法

1. 访问服务器实例的 Server Manager，然后单击 "Preferences" 选项卡。
2. 单击 "Set Cipher Size" 链接。
3. 从下拉式列表中，选择要对其应用更强大加密算法的资源，然后单击 "Select"。也可以指定正则表达式。有关更多信息，参见第 319 页的第 16 章“管理模板和资源”。
4. 选择密钥大小的限制：
   - 168 位或更大
   - 128 位或更大
   - 56 位或更大
   - 无限制
5. 指定要拒绝访问的消息所在的文件位置，然后单击 "OK"。

有关加密算法的更多信息，参见 Introduction to SSL。

其他安全注意事项

除有人会试图破解您的加密以外，还存在着其他安全风险。网络面临的风险来自外部和内部的黑客，他们使用各种方法试图访问您的服务器以及服务器上的信息。除了在服务器上启用加密外，还应采取额外的安全防护措施。例如，将服务器计算机放在一个安全的房间内，以及不允许任何不信任的人将程序上载到您的服务器中。本节介绍了一些可使服务器更安全的重要事项：

本节包括以下主题：

限制物理访问

这种简单的安全方法常常会被忘记。将服务器计算机放在一个上锁的房间中，只有授权人员才能进入该房间。这样可以防止任何人攻击服务器计算机本身。而且，如果计算机有管理（超级用户）口令，请对妥善保护此口令。

限制管理访问

如果使用远程配置，请确保设置了访问控制，只允许少数用户和计算机进行管理。如果希望管理服务器为最终用户提供对 LDAP 服务器或本地目录信息的访问权限，请考虑维护两台管理服务器和使用群集管理。这样启用了 SSL 的管理服务器可用作主服务器，而另一台管理服务器则用于最终用户的访问。有关群集的更多信息，参见第 109 页的第 6 章“管理服务器群集”。

您还应为 Administration Server 打开加密功能。如果不使用 SSL 连接进行管理，通过不安全的网络执行远程服务器管理时应该格外小心。因为任何人都可以截取您的管理口令并重新配置您的服务器。

选择保密性强的口令

您可以在服务器中使用多个口令：管理口令、专用密钥口令、数据库口令等。管理口令是所有口令中最重要的一个，因为持有该口令的用户可以在您的计算机上配置任何服务器。专用密钥口令是另一个最重要的口令。如果有人获取了您的专用密钥和专用密钥口令，则可以创建虚设服务器（伪装成您的服务器），或截取和更改服务器的通信信息。

口令最好便于您自己记忆，别人又无法猜到。例如，您可以将 *MCi12!mo* 记成 "My Child is 12 months old!"。孩子的名字和生日等都是不安全的口令。

创建难以破解的口令

以下这些简单的指导可帮助您创建更安全的口令。不必在一个口令中应用以下所有规则，但使用的规则越多，口令就越难以破解。一些提示：

- 口令长度应为 6 到 14 个字符
- 请不要使用非法字符：*、" 或空格
- 请不要使用词典单词（任何语言）
- 请不要使用常见字母替换，例如将 E 替换为 3 或将 L 替换为 1
- 尽可能多地包含以下字符：
  - 大写字母
  - 小写字母
  - 数字
  - 符号

更改口令或 PIN

最好定期更改您的信任数据库 / 密钥对文件口令或 PIN。如果 Administration Server 启用了 SSL，启动服务器时会需要此口令。定期更改口令可以对服务器提供进一步的保护。

只能在本地计算机上更改此口令。有关更该口令时的注意事项列表，参见第 105 页的“创建难以破解的口令”。

更改信任数据库 / 密钥对文件口令

1. 访问 "Administration Server" 或 "Server Manager"，然后单击 "Security" 选项卡。
2. 单击 "Change Key Pair File Password" 链接。

3. 从 "Cryptographic Module" 下拉式列表中，选择要在其中更改口令的安全令牌。默认情况下，内部密钥数据库的安全令牌为 "Internal"。如果安装了 PKCS #11 模块，将列出所有的安全令牌。
4. 输入当前口令。
5. 输入新口令。
6. 再次输入新口令，并单击 "OK"。

确保您的密钥对文件受到保护。Administration Server 将密钥对文件存储在 *server_root*/alias 目录中。

了解备份磁带上是否存储了该文件以及其他人是否能够通过其他方式截取该文件也很重要。如果存储了该文件，则必须像保护服务器一样尽力保护备份。

限制服务器上的其他应用程序

请谨慎决定在充当服务器的计算机上运行的所有应用程序。利用服务器上运行的其他程序中的漏洞可以避开服务器的安全保护。请禁用所有不必要的程序和服务。例如，UNIX sendmail 守护进程难以安全配置，并可被设置为在服务器计算机上运行其他有害程序。

UNIX 和 Linux

小心选择从 inittab 和 rc 脚本启动的进程。请不要在服务器计算机中运行 telnet 或 rlogin。也不应在服务器计算机上运行 rdist。此命令可发布文件，但也能用来更新服务器计算机上的文件。

Windows

请谨慎决定与其他计算机共享的驱动器和目录。而且，要考虑哪些用户具有帐户或 Guest 权限。请慎重决定在服务器上安装哪些程序，或允许其他用户安装哪些程序。其他用户的程序可能存在安全漏洞。更糟糕的是，有人可能会上载专门用于破坏您的安全性的恶意程序。允许在您的服务器上安装程序之前一定要仔细检查这些程序。

禁止客户机缓存 SSL 文件

通过在 HTML 文件的 <HEAD> 部分中添加以下行，可以防止客户机高速缓存加密前的文件：

```
<meta http-equiv="pragma" content="no-cache">
```

限制端口

禁用计算机上未使用的所有端口。使用路由器或防火墙配置可以防止到除绝对最小端口集以外的任何端口的拨入连接。这意味着获取计算机上 Shell 的唯一方法就是通过物理方式使用服务器计算机，而该计算机应已处于受限区域内。

了解服务器的限制

服务器提供了服务器和客户机之间的安全连接。客户机获得信息之后，服务器既无法控制信息的安全性，也无法控制对服务器计算机本身及其目录和文件的访问。

了解这些限制有助于您理解要避免的情况。例如，您可以通过 SSL 连接获取信用卡号，但这些号码是否存储在服务器计算机上的安全文件中呢？SSL 连接终止后这些号码会怎样呢？请务必为客户机通过 SSL 发送给您的任何信息提供安全保护。

第 6 章

管理服务器群集

本章介绍建立 Sun Java System Web Proxy Server 群集的概念，并说明如何才能使用群集在服务器间共享配置。

本章包括以下各节：

关于服务器群集

群集是可以通过单个 Administration Server 进行管理的一组 Sun Java System Web Proxy Server。每个群集均须包括一个指定为主 Administration Server 的服务器。

通过将服务器组织成群集，可以：

- 创建一个中心位置来管理所有的 Proxy Server
- 在服务器之间共享一个或多个配置文件
- 通过一个主 Administration Server 启动和停止所有服务器
- 查看特定服务器的访问日志和错误日志

群集使用指导原则

以下列表提供了将各组 Proxy Server 配置成多个群集的指导原则：

- 在创建任何群集之前，必须先安装要包括在特定群集中的所有服务器。
- 群集中的所有服务器必须为同一类型（UNIX 或 Windows）。群集必须是同类的。
- 群集中的所有服务器均必须为 Proxy Server 版本 4。仅支持向群集添加 Proxy Server 版本 4 服务器。
- 所有 Administration Server 必须使用同一协议，HTTP 或 HTTPS。如果更改群集中某个 Administration Server 的协议，则必须更改所有 Administration Server 的协议。有关更多信息，参见第 112 页的“修改服务器信息”。
- 所有群集专用 Administration Server 必须与主 Administration Server 具有相同的用户名和口令。可使用分布式管理在每个 Administration Server 上配置多个管理员。
- 必须将一个群集专用 Administration Server 指定为主 Administration Server（具体选择哪个服务器无关紧要）。
- 主 Administration Server 必须有权访问每一个群集专用 Administration Server。主 Administration Server 将检索所有已安装 Sun Java System Web Proxy Server 的有关信息。

建立群集

以下是建立 Proxy Server 群集所要采取的一般步骤。

建立 Proxy Server 群集

1. 安装要包括在群集中的 Proxy Server。确保主 Administration Server 可使用群集的 Administration Server 的用户名和口令进行验证。为此，可以使用默认用户名和口令或配置分布式管理。
2. 安装将要包含主 Administration Server 的 Proxy Server，确保用户名和口令与步骤 1 中的设置一致。
3. 将服务器添加到群集列表中。有关更多信息，参见第 111 页的“向群集添加服务器”。
4. 对远程服务器进行管理，方法是从 "Control Cluster" 页面访问其 Server Manager 界面，或是将配置文件从群集中的一台服务器复制到另一台服务器。

向群集添加服务器

在将 Proxy Server 添加到群集后，将会指定其 Administration Server 和端口号。如果该 Administration Server 包含多台服务器的信息，则其中的所有服务器都将添加到群集中。可在以后删除个别服务器。

注 如果远程 Administration Server 包含一个群集的信息，则不会添加该远程群集中的服务器。主 Administration Server 只添加实际安装在远程计算机上的服务器。

向群集添加远程服务器

1. 确保主 Administration Server 已开启。
2. 访问主 Administration Server，然后单击 "Cluster" 选项卡。
3. 单击 "Add Server" 链接。
4. 选择远程 Administration Server 所使用的协议：
   - "HTTP" 用于通常的 Administration Server
   - "HTTPS" 用于安全 Administration Server
5. 输入远程 Administration Server 出现于 `magnus.conf` 文件中的全限定主机名（例如，`plaza.example.com`）。
6. 输入远程 Administration Server 的端口号。
7. 输入远程 Administration Server 的管理员用户名和口令，然后单击 "OK"。主 Administration Server 将尝试与远程服务器进行联络。如果成功，系统会提示您确认是否将服务器添加到群集。

注 启用群集控制后，群集的主服务器会在 `proxy-`*serverid*`/config/cluster/`*server_name*`/proxy-`*serverid* 目录中为群集中的每个从属服务器创建多个文件。这些文件是不可配置的。

修改服务器信息

Administration Server 的 "Cluster" 选项卡上的 "Modify Server" 选项只用于在从属服务器上更改了从属管理端口信息之后对其进行更新。如果更改了群集中某个远程 Administration Server 的端口号，还必须修改群集中所存储的有关该 Administration Server 的信息。对从属 Administration Server 进行其他任何更改都需要先删除该服务器，然后在更改完之后再将其回添到群集中。

修改群集中服务器的有关信息

1. 访问主 Administration Server，然后单击 "Cluster" 选项卡。
2. 单击 "Modify Server" 链接。将按服务器唯一标识符列出各个服务器。
3. 选择要修改的服务器，根据需要进行更改，然后单击 "OK"。

从群集中删除服务器

从群集中删除服务器

1. 访问主 Administration Server，然后单击 "Cluster" 选项卡。
2. 单击 "Remove Server" 链接。
3. 选择要从群集中删除的远程服务器，然后单击 "OK"。删除的服务器无法再通过群集进行访问。只能通过其自身的 Administration Server 对其进行访问。

控制服务器群集

通过 Proxy Server 可以采用以下方式来控制群集中的远程服务器：

- 启动和停止这些服务器
- 查看远程服务器的访问日志和错误日志

- 传送配置文件（如果主 Administration Server 具有一个以上的 Proxy Server 实例，则可将文件从这些服务器中的任何一个传送到已添加至群集的任何从属服务器）。请注意，群集必须是同类的。群集中所有服务器的类型必须相同（即，或者是 UNIX 或者是 Windows）。从不同的平台传送配置文件可能会导致服务器挂起或崩溃。配置文件有：
  - `server.xml`
  - `magnus.conf`
  - `obj.conf`
  - `mime.types`
  - `socks5.conf`
  - `bu.conf`
  - `icp.conf`
  - `parray.pat`
  - `parent.pat`

控制群集中的服务器

1. 访问主 Administration Server，然后单击 "Cluster" 选项卡。
2. 单击 "Control Cluster" 链接。
3. 选择要控制的服务器，然后根据需要做出选择。可随时单击 "Reset" 按钮，将元素重置为进行更改之前其中所含的值。
   - 从下拉式列表中选择 "Start"、"Stop" 或 "Restart"，然后单击 "Go"。系统将提示您确认所选操作。
   - 从下拉式列表中选择 "View Access" 或 "View Error"，然后输入要在日志文件中查看的最后一行的行号。单击 "Go" 显示该信息（单击所显示的 "Cluster Execution Report" 中的 "View" 按钮）。
   - 传送配置文件：
     - 选择要传送的配置文件
     - 选择文件所在的服务器
     - 单击 "Go" 传送信息

第 3 部分

配置和监视 Proxy Server

第 7 章

配置服务器首选项

本章介绍 Proxy Server 的系统设置以及如何配置这些设置。系统设置将影响整个 Proxy Server。这些设置包括代理服务器使用的用户帐户及侦听的端口等选项。

本章包括以下各节：

启动 Proxy Server

本节介绍如何在不同平台上启动 Proxy Server。服务器在安装后即会运行，侦听并接受请求。

从管理界面启动 Proxy Server

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Start/Stop Server" 链接。显示 "Start/Stop Server" 页面。
3. 单击 "On" 按钮。

"Start/Stop Server" 页面会显示服务器的状态。

在 UNIX 或 Linux 上启动 Proxy Server

- 在命令行中转到 *server_root*/proxy-server*id*，然后键入 ./start 启动 Proxy Server。
- 使用 start。如果要将此脚本与 init 一起使用，必须在 /etc/inittab 中加入启动命令 prxy:2:respawn:*server_root*/proxy-server*id*/start -start -i。

在 Windows 上启动 Proxy Server

- 使用“开始”>“程序”> "Sun Microsystems" > "Sun Java System Web Proxy Server *version*" > "Start Proxy Server"
- 使用“控制面板”>“管理工具”>“服务”> "Sun Java System Web Proxy Server 4.0 (proxy-server*id*)" >“启动”
- 在命令提示符下转到 *server_root*\proxy-server*id*，然后键入 startsvr.bat 启动 Proxy Server。

启动启用了 SSL 的服务器

要启动启用了 SSL 的服务器，需要提供口令。尽管可以通过将口令以纯文本格式存储在某个文件中来自动启动启用了 SSL 的服务器，但建议不要使用这种方法。

注意 将启用了 SSL 的服务器的口令以纯文本格式存放在服务器启动脚本中会带来很大的安全风险。任何可以访问该文件的用户都有权访问启用了 SSL 的服务器的口令。在将启用了 SSL 的服务器的口令保存为纯文本格式之前，请考虑可能带来的安全风险。

服务器的启动脚本、密钥对文件和密钥口令应归超级用户所有（如果服务器是由非超级用户安装的，则应属于该用户帐户），并且只有所有者具有读 / 写权限。

在 UNIX 或 Linux 上自动启动启用了 SSL 的服务器

1. 使用文本编辑器打开 `start` 文件。
2. 找到脚本中的 `-start` 行并插入以下内容：

   `echo "`*`password`*`"|`

   其中 *password* 是您选择的 SSL 口令。

   例如，如果 SSL 口令是 `examples`，则该行编辑后类似于：

   ```
   -start)
     echo "examples"|./$PRODUCT_BIN -d $PRODUCT_SUBDIR/config $@
   ```

停止 Proxy Server

本节介绍在不同平台上停止 Proxy Server 的各种方法。

从管理界面停止 Proxy Server

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Start/Stop Server" 链接。显示 "Start/Stop Server" 页面。
3. 单击 "Off" 按钮。

"Start/Stop Server" 页面会显示服务器的状态。

在 UNIX 或 Linux 上停止 Proxy Server

- 在命令行中转至 *server_root*`/proxy-server`*id*，然后键入 `./stop`。

注 如果使用 `etc/inittab` 文件重新启动服务器，则必须在尝试停止服务器之前从 `/etc/inittab` 文件中删除启动服务器的相应行并键入 `kill -1 1`。否则，服务器将在停止后自动重新启动。

- 使用 `stop` 来完全关闭服务器。这将中断服务，直至重新启动。如果将 `etc/inittab` 文件设置为自动重新启动（使用 `respawn`），则必须在关闭服务器之前删除 `etc/inittab` 中与代理服务器相关的行；否则服务器将自动重新启动。

关闭服务器后，服务器可能需要几秒钟时间完成关闭过程并将状态更改为 "Off"。

如果系统崩溃或脱机，服务器将停止，正在处理的任何请求都将丢失。

注 如果在服务器中安装了安全性模块，则需要在启动或停止服务器之前输入相应的口令。

在 Windows 上停止 Proxy Server

- 使用“开始”>“程序”> "Sun Microsystems" > "Sun Java System Web Proxy Server *version*" > "Stop Proxy Server"
- 在命令提示符下转到 *server_root*\proxy-server*id*，然后键入 stopsvr.bat 停止 Proxy Server。
- 使用“服务”窗口中的 "Sun Java System Proxy Server 4.0 (proxy-server*id*)" 服务：“控制面板”>“管理工具”>“服务”

重新启动 Proxy Server

本节介绍在不同平台上重新启动 Proxy Server 的各种方法。

重新启动服务器（UNIX 或 Linux）

您可以使用以下方法之一启动服务器：

- 手动重新启动。
- 自动从 inittab 文件重新启动

  请注意，如果所使用的 UNIX 或 Linux 版本不是源自 System V（例如 SunOS 4.1.3），则无法使用 inittab 文件。
- 系统重新引导时，自动使用 /etc/rc2.d 中的守护进程重新启动。

由于安装脚本无法编辑 /etc/rc.local 或 /etc/inittab 文件，因此必须使用文本编辑器对其进行编辑。如果不知道如何编辑这些文件，请向系统管理员咨询或参见系统文档。

从命令行重新启动 Proxy Server

1. 如果服务器在端口号低于 1024 的端口上运行，请以超级用户身份登录；否则以超级用户或使用服务器用户帐户登录。
2. 在命令行提示符下，键入下面一行文本并按 Enter 键：

   server_root/proxy-server*id*/restart

   其中 *server_root* 是服务器的安装目录。

- 您可以在该行的末尾使用可选参数 -i。-i 选项使服务器在 inittab 模式下运行。这样，如果服务器进程中止或崩溃，inittab 将重新启动服务器。此选项还可以防止将服务器置于后台进程。

使用 inittab 重新启动服务器

在 /etc/inittab 文件的一行中添加以下文本：

prxy:23:respawn:*server_root*/proxy-server*id*/start -start -i

其中 *server_root* 是服务器的安装目录，proxy-server*id* 是服务器的目录。

-i 选项可以防止将服务器置于后台进程。

停止服务器之前必须删除此行。

使用系统 RC 脚本重新启动服务器

如果使用 /etc/rc.local 或您系统的等效文件，请将下面一行文本添加到 /etc/rc.local 文件中：

server_root/proxy-server*id*/start

将 *server_root* 替换为服务器的安装目录。

重新启动服务器 (Windows)

可以使用以下方法重新启动服务器

- 使用“服务控制面板”。

在 Windows 上重新启动服务器

1. 使用“控制面板”>“管理工具”>“服务”>
2. 从服务列表中选择 "Sun Java System Web Proxy Server 4.0 (proxy-server*id*)"。
3. 在“属性”窗口中，将“启动类型”更改为“自动”，使系统在每次启动或重新引导计算机时启动服务器。
4. 单击“确定”。

设置终止超时

服务器停止后，将不再接收新的连接，而只是等待所有未完成的连接完成。服务器超时前的等待时间可以在 magnus.conf 文件中配置。默认情况下，该时间设置为 30 秒。要更改此值，将下面一行文本添加到 magnus.conf 文件中：

TerminateTimeout *seconds*

其中 *seconds* 代表服务器在超时之前等待的秒数。

配置此值的优点是服务器将等待更长时间以便连接完成。但是，由于服务器通常从非响应的客户机打开连接，因此增加终止超时可能会增加服务器关闭所用的时间。

查看服务器设置

在安装过程中会为 Proxy Server 配置一些设置。通过 Server Manager 可以查看上述以及其他系统设置。"View Server Settings" 页面将列出 Proxy Server 的所有设置。如果尚未保存和应用更改，此页面还会通知此信息。在此情况下，需要保存更改并重新启动 Proxy Server 才能开始使用新配置。

有两种类型的设置：技术和内容。服务器的内容设置取决于如何配置服务器。通常，代理服务器会列出所有模板、URL 映射和访问控制。对于单个模板，此页面将列出模板名称、模板的正则表达式和模板设置，如高速缓存设置。

Proxy Server 的技术设置来自 `magnus.conf` 文件和 `server.xml` 文件，内容设置来自 `obj.conf` 文件。上述文件位于服务器根目录下名为 `proxy-`*id*`/config` 的子目录中。

查看 Proxy Server 的设置

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "View Server Settings" 链接。显示 "View Server Settings" 页面。

查看和恢复配置文件的备份

可以查看或恢复配置文件（`server.xml`、`magnus.conf`、`obj.conf`、`mime types`、`server.xml.clfilter`、`magnus.conf.clfilter`、`obj.conf.clfilter`、`socks5.conf`、`bu.conf`、`icp.conf`、`parray.pat`、`parent.pat`、`proxy-id.acl`）的备份副本。当前配置出现问题时，可利用此功能恢复到以前的配置。例如，如果对代理服务器的配置进行了若干更改，之后代理服务器并未按预想的方式工作（例如，您拒绝了对某个 URL 的访问，但代理服务器却仍为该请求提供服务），则可返回以前的配置，然后重新更改配置。

查看以前的配置

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Restore Configuration" 链接。将显示 "Restore Configuration" 页面。该页面将按日期和时间顺序列出所有以前的配置。
3. 单击 "View" 链接显示特定版本的技术设置和内容设置的列表。

恢复配置文件的备份副本

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Restore Configuration" 链接。将显示 "Restore Configuration" 页面。该页面将按日期和时间顺序列出所有以前的配置。

3. 单击要恢复的版本的 "Restore" 链接。

   如果要将所有文件恢复到某个特定时间的状态，单击表中最左侧列的 "Restore to *time*" 链接（*time* 为要恢复到的日期和时间）。

还可以设置 "Restore Configuration" 页面上显示的备份数量。

设置显示的备份数量

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Restore Configuration" 链接。将显示 "Restore Configuration" 页面。
3. 在 "Set Number Of Sets Of Backups" 字段中，输入要显示的备份数。
4. 单击 "Change" 按钮。

配置系统首选项

"Configure System Preferences" 页面允许设置或更改服务器的基本特征。通过此页面可以更改服务器用户、进程数、侦听队列大小、代理服务器超时以及代理服务器的中断超时。还可以启用 DNS、ICP、代理服务器阵列和父阵列。

修改系统首选项

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Configure System Preferences" 链接。将显示 "Configure System Preferences" 页面。
3. 根据需要更改选项，然后单击 "OK"。
4. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
5. 单击 "Restart Proxy Server" 按钮以应用更改。

上述选项将在以下各节介绍。

Server User

"Server User" 是代理服务器使用的用户帐户。作为代理服务器用户输入的用户名应该已经存在，并且是标准用户帐户。服务器启动时，其运行情况与由此用户启动一样。

如果要避免新建用户帐户，可以选择由在同一台主机上运行的其他服务器使用的帐户。如果运行的是 UNIX 代理服务器，则可选择 nobody 用户。但是，对于某些系统，nobody 用户可以拥有文件却不能运行程序，因而不适合用作代理服务器用户名。

在 UNIX 系统上，代理服务器产生的所有进程都分配给该服务器用户帐户。

Processes

"Processes" 字段显示服务请求可用的进程数量。默认情况下，该字段值为 1。除非需要，否则请勿修改此设置。

Listen Queue Size

"Listen Queue Size" 字段指定侦听套接字上的最大暂挂连接数。

DNS

“域名服务”(DNS) 将 IP 地址恢复为主机名。Web 浏览器与服务器连接时，服务器获取的只是客户机的 IP 地址，例如 `198.18.251.30`。服务器没有获取主机名信息，如 `www.example.com`。对于访问日志记录和访问控制，服务器可将 IP 地址解析为主机名。在 "Configure System Preferences" 页面中，可以指定服务器是否将 IP 地址解析为主机名。

ICP

“Internet 高速缓存协议”(ICP) 是一种消息传递协议，该协议可以使高速缓存彼此通信。高速缓存可以就是否存在高速缓存的 URL 及这些 URL 的最佳检索位置，使用 ICP 发送查询和回复。可以在 "Configure System Preferences" 页面启用 ICP。有关 ICP 的更多信息，参见第 257 页的“通过 ICP 邻域进行路由选择”。

Proxy Array

代理服务器阵列是作为一个高速缓存使用的多个代理服务器的阵列，其目的是实现分布式高速缓存。如果在 "Configure System Preferences" 页面启用了 "Proxy Array" 选项，则意味着配置的代理服务器是某代理服务器阵列的成员，而且该阵列中的所有其他成员都是其同级服务器。有关使用代理服务器阵列的更多信息，参见第 265 页的“通过代理服务器阵列进行路由选择”。

Parent Array

父阵列是代理服务器或代理服务器阵列路由经过的代理服务器阵列。因此，如果代理服务器访问远程服务器之前路由经过上游代理服务器阵列，则此上游代理服务器阵列将被视为父阵列。有关将父阵列用于代理服务器的更多信息，参见第 276 页的“通过父代理服务器阵列进行路由选择”。

Proxy Timeout

代理超时是代理服务器因超时终止请求之前，来自远程服务器的相邻网络数据包间允许的最大时间间隔。代理超时的默认值为 5 分钟。

注	远程服务器使用服务器推送功能时，如果页面间的延迟超过代理超时，可能在完成传输之前即终止连接。请改为使用客户机拉曳功能，向代理服务器发送多个请求。

调节 Proxy Server

"Tune Proxy" 页面允许通过更改默认参数调节代理服务器的性能。

更改默认调节参数

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Tune Proxy" 链接。将显示 "Tune Proxy" 页面。
3. 为了更好地满足您的要求，可能需要修改 FTP 列表的宽度。增加列表宽度可以显示更长的文件名，从而减少文件名截尾长度。默认宽度为 80 个字符。
4. 单击 "OK"。
5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

添加和编辑侦听套接字

在服务器能够处理请求之前，必须先通过侦听套接字接受请求，然后将请求定向到正确的服务器。安装 Proxy Server 时，将自动创建一个侦听套接字 ls1。此侦听套接字使用 IP 地址 `0.0.0.0` 和在安装过程中指定为代理服务器端口号的端口号。不能删除默认的侦听套接字。

使用 Server Manager 的 "Add Listen Socket" 和 "Edit Listen Sockets" 页面添加、编辑和删除侦听套接字。

本节包括以下主题：

添加侦听套接字

添加侦听套接字

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Add Listen Socket" 链接。将显示 "Add Listen Socket" 页面。
3. 指定侦听套接字的内部名称。创建侦听套接字后不能更改此名称。
4. 指定侦听套接字的 IP 地址。IP 地址可以用点分对或 IPv6 记法表示，也可以是 `0.0.0.0`、`any`、`ANY` 或 `INADDR_ANY`（所有 IP 地址）。
5. 指定要在其上创建侦听套接字的端口号。有效值为 `1` 至 `65535` 之间的值。对于 UNIX，创建在端口 1 至 1024 进行侦听的套接字需要超级用户权限。请将 SSL 侦听套接字配置为侦听端口 443。
6. 指定要在由服务器发送至客户机的任一 URL 的主机名部分中使用的服务器名称。这会影响服务器自动生成的 URL，但不会影响存储在服务器中的目录和文件的 URL。如果服务器使用别名，则此名称应为别名。
7. 从下拉式列表中指定为侦听套接字启用还是禁用安全性。
8. 单击 "OK"。
9. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
10. 单击 "Restart Proxy Server" 按钮以应用更改。

编辑侦听套接字

编辑侦听套接字

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Edit Listen Sockets" 链接。将显示 "Edit Listen Sockets" 页面。
3. 在 "Configured Sockets" 表中，单击要编辑的侦听套接字的链接。将显示 "Edit Listen Sockets" 页面。
4. 对以下选项进行所需更改：

- **General**
  - **Listen Socket ID。**侦听套接字的内部名称。创建侦听套接字后不能更改此名称。
  - **IP Address。**侦听套接字的 IP 地址。IP 地址可以用点分对或 IPv6 记法表示。也可以为 `0.0.0.0`、`any`、`ANY` 或 `INADDR_ANY`（所有 IP 地址）。
  - **Port。**要在其上创建侦听套接字的端口号。有效值为 1 至 65535 之间的值。对于 UNIX，创建在端口 1 至 1024 进行侦听的套接字需要超级用户权限。请将 SSL 侦听套接字配置为侦听端口 443。
  - **Server Name。**此侦听套接字的默认服务器。
- **Security**

如果禁用安全性，则只显示以下参数：

- **Security。**启用或禁用选定侦听套接字的安全性。

如果启用安全性，将显示以下参数：

- **Security。**启用或禁用选定侦听套接字的安全性。
- **Server Certificate Name。**从下拉式列表中选择已安装的证书，以用于此侦听套接字。
- **Client Authentication。**指定在此侦听套接字上是否需要客户机验证。默认情况下，此项是 "Optional"。
- **SSL Version 2。**启用或禁用 SSL 版本 2。默认情况下会禁用此项。
- **SSL Version 2 Ciphers。**列出此套件中的所有加密算法。通过选中或取消选中相应的框为所编辑的侦听套接字选择要启用的加密算法。默认版本将处于取消选中状态。
- **SSL Version 3。**启用或禁用 SSL 版本 3。默认情况下会启用此项。

- **TLS。**启用或禁用 TLS（即用于加密通信的“传输层安全性”协议）。默认情况下会启用此项。
- **TLS Rollback。**启用或禁用 TLS 回滚。请注意，禁用 TLS 回滚将使连接容易遭到版本回滚攻击。默认情况下会启用此项。
- **SSL Version 3 and TLS Ciphers。**列出此套件中的所有加密算法。通过选中或取消选中相应的框为所编辑的侦听套接字选择要启用的加密算法。默认版本将处于选中状态。

- **Advanced**
  - **Number Of Acceptor Threads。**侦听套接字的接收方线程数。建议值为计算机中处理器的数目。默认值为 1，有效值为 1 至 1024 之间的值。

  Protocol Family。套接字系列类型。有效值包括 `inet`、`inet6` 和 `nca`。对于 IPv6 侦听套接字，请使用值 `inet6`。指定 `nca` 可以使用 Solaris™ 网络高速缓存和加速器。

5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

删除侦听套接字

删除侦听套接字

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Edit Listen Sockets" 链接。
3. 选择要删除的侦听套接字旁的复选框，然后单击 "OK"。系统将提示您确认删除。可以删除任何侦听套接字，除非该侦听套接字是实例的唯一侦听套接字。
4. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
5. 单击 "Restart Proxy Server" 按钮以应用更改。

MIME 类型

“多用途 Internet 邮件扩展”(MIME) 类型是多媒体电子邮件和消息传递的标准。可以根据文件的 MIME 类型过滤文件，代理服务器提供了一个页面，通过该页面可以创建用于服务器的新 MIME 类型。代理服务器将此新类型添加到 `mime.types` 文件中。有关根据 MIME 类型阻止文件的更多信息，参见第 285 页的“按 MIME 类型过滤”。

本节包括以下主题：

创建新的 MIME 类型

创建 MIME 类型

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Create/Edit MIME Types" 链接。将出现 "Create/Edit MIME Types" 页面。该页面显示代理服务器的 `mime.types` 文件中列出的所有 MIME 类型。
3. 从下拉式列表中指定 MIME 类型的类别。此类别可以是 `type`、`enc` 或 `lang`。其中 `type` 是文件或应用程序类型、`enc` 是用于压缩的编码，而 `lang` 是语言编码。有关类别的更多信息，参见联机帮助。
4. 指定出现在 HTTP 头中的内容类型。
5. 指定文件后缀。"File Suffix" 指映射到 MIME 类型的文件扩展名。要指定多个扩展名，请用逗号分隔各项。文件扩展名应该是唯一的。换言之，不应将一个文件扩展名映射到两个 MIME 类型。
6. 单击 "New" 按钮添加 MIME 类型。

编辑 MIME 类型

编辑 MIME 类型

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Create/Edit MIME Types" 链接。出现的 "Create/Edit MIME Types" 页面显示代理服务器的 `mime.types` 文件中列出的所有 MIME 类型。

3. 可以通过单击 MIME 类型的 "Edit" 链接编辑任何 MIME 类型。
4. 进行所需更改，然后单击 "Change MIME Type" 按钮。

删除 MIME 类型

删除 MIME 类型

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Create/Edit MIME Types" 链接。出现的 "Create/Edit MIME Types" 页面显示代理服务器的 `mime.types` 文件中列出的所有 MIME 类型。
3. 可以通过单击 MIME 类型的 "Remove" 链接删除任何 MIME 类型。

管理访问控制

"Administer Access Control" 页面可用于管理访问控制列表 (ACL)。ACL 使您可以控制哪些客户机可以访问您的服务器。ACL 可以屏蔽某些用户、组或主机以允许或拒绝对服务器部分内容的访问，并设置验证以便仅使有效用户和组可以访问服务器部分内容。有关访问控制的更多信息，参见第 135 页的第 8 章“控制对服务器的访问”。

管理访问控制列表

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Administer Access Control" 链接。显示 "Administer Access Control" 页面。
3. 选择资源、现有 ACL，或键入 ACL 名称，然后单击 "Edit" 按钮。将显示 "Access Control Rules for" 页面。
4. 进行所需更改，然后单击 "Submit"。有关访问控制的更多信息，参见“设置服务器实例的访问控制”，此主题列于第 135 页的第 8 章“控制对服务器的访问”。

配置 ACL 高速缓存

"Configure ACL Cache" 用于启用或禁用代理服务器验证高速缓存、设置代理服务器验证高速缓存目录、配置高速缓存表大小和设置条目到期时间。

配置 ACL 高速缓存

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Configure ACL Cache" 链接。将显示 "Configure ACL Cache" 页面。
3. 可以启用或禁用代理服务器验证高速缓存。
4. 从 "Proxy Auth User Cache Size" 下拉式列表中，选择用户高速缓存中的用户数。默认大小为 200。
5. 从 "Proxy Auth Group Cache Size" 下拉式列表中，选择可以为单个 UID/ 高速缓存条目高速缓存的组 ID 数。默认大小为 4。
6. 选择高速缓存条目到期前的秒数。每次引用高速缓存中的某个条目时，都将计算其耗用时间并对照此值进行检查。如果其耗用时间大于或等于 "Proxy Auth Cache Expiration" 值，将不使用此条目。如果将此值设置为 0，则会关闭高速缓存。

   如果将其设置为一个较大的值，则每次更改 LDAP 条目时，可能都需要重新启动 Proxy Server。例如，如果将该值设置为 120 秒，Proxy Server 可能会在两分钟内与 LDAP 服务器不同步。如果不经常更改 LDAP 条目，请使用一个较大的值。默认到期时间值为 2 分钟。
7. 单击 "OK"。
8. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

了解 DNS 高速缓存

Proxy Server 支持 DNS 高速缓存，以减少代理服务器将 DNS 主机名解析为 IP 地址时执行 DNS 查找的次数。

配置 DNS 高速缓存

"Configure DNS Cache" 页面用于启用或禁用 DNS 高速缓存、设置 DNS 高速缓存的大小、设置 DNS 高速缓存条目的到期时间，以及启用或禁用反向 DNS 高速缓存。

配置 DNS 高速缓存

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Configure DNS Cache" 链接。将显示 "Configure DNS Cache" 页面。
3. 可以启用或禁用 DNS 高速缓存。
4. 从 "DNS Cache Size" 下拉式列表中选择可以存储在 DNS 高速缓存中的条目数。默认大小为 1024。
5. 可以设置 DNS 高速缓存的到期时间。如果 DNS 高速缓存条目到达预设的到期时间，Proxy Server 会将其从高速缓存中清除。默认 DNS 到期时间为 20 分钟。
6. 可以启用或禁用未找到主机名时缓存错误。
7. 单击 "OK"。
8. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

配置 DNS 子域

某些 URL 含有的主机名带有多级子域。如果第一个 DNS 服务器未能解析主机名，代理服务器检查 DNS 的时间会很长。可以设置 Proxy Server 将 "host not found" 消息返回客户机之前检查的级别数。

例如，如果客户机请求 `http://www.sj.ca.example.com/index.html`，代理服务器将主机名解析为 IP 地址的时间将会很长，因为代理服务器可能需要遍历 4 个 DNS 服务器，才能找到主机的 IP 地址。由于这些查找会花费很长时间，可以对代理服务器进行配置，使其必须使用超过某个数量的 DNS 服务器时，放弃查找 IP 地址。

设置代理服务器遍历的子域级别

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Configure DNS Subdomains" 链接。将显示 "Configure DNS Subdomains" 页面。
3. 从下拉式列表中选择一个资源，或指定一个正则表达式。
4. 从 "Local Subdomain Depth" 下拉式列表中，选择级别数。
5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

配置 HTTP 保持活动

"Configure HTTP Client" 页面用于在代理服务器上启用保持活动功能。

代理服务器支持 HTTP 保持活动数据包。默认情况下，代理服务器不使用保持活动连接。但对于某些系统，使用保持活动功能可以提高代理服务器的性能。保持活动功能是一种 TCP/IP 功能，即在完成请求后继续使连接保持打开状态，从而客户机可以快速重新使用这一打开的连接。

在标准的基于 Web 的客户机 / 服务器事务中，客户机可以建立与服务器的多个连接，请求多个文档。例如，如果客户机请求的 Web 页面中含有几个图像，则客户机需要单独请求各个图形文件。重新建立连接是很费时的。

配置 HTTP 保持活动

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Configure HTTP Client" 链接。将显示 "Configure HTTP Client" 页面。
3. 从下拉式列表中选择一个资源。选择 HTTP 或 HTTPS 资源，在 Proxy Server 上配置保持活动或指定正则表达式。
4. 通过单击相应的 "Keep Alive" 选项，指定 HTTP 客户机是否应使用持久连接。
5. 在 "Keep Alive Timeout" 字段中指定使持久连接操持打开状态的最大秒数。默认值是 29。
6. 通过选择相应 "Persistent Connection Reuse" 选项，可以指定 HTTP 客户机是否可以对所有类型的请求重新使用现有持久连接。默认值是 "off"，并且对于非 GET 请求和含有主体的请求，不允许再使用持久连接。
7. 在 "HTTP Version String" 字段中指定 HTTP 协议版本字符串。除非遇到具体的协议互操作性问题，否则不要指定此参数。
8. 在 "Proxy Agent Header" 字段中指定 Proxy Server 产品名和版本。
9. 在 "SSL Client Certificate Nickname" 字段中指定提供给远程服务器的客户机证书的别名。
10. 选择相应的 "SSL Server Certificate Validation" 选项，以指示 Proxy Server 是否必须验证远程服务器提供的证书。
11. 单击 "OK"。
12. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
13. 单击 "Restart Proxy Server" 按钮以应用更改。

第 8 章

控制对服务器的访问

本章介绍如何控制对 Administration Server 及由 Proxy Server 提供的数据的访问。可以限制对服务器提供的所有数据或其提供的特定 URL 的访问。例如，可以指定只有特定的人才能访问某些 URL，或指定这些人以外的人才能够查看文件。可以允许所有客户机访问 HTTP 的 URL，但对 FTP 的访问做出限制。还可以基于主机名或域名限制对 URL 的访问。例如，当 Proxy Server 为多个内部 Web 服务器提供服务，但只希望特定人员才可以访问存储在其中一台服务器上的保密研究项目时，就可以这样做。

必须先启用分布式管理并在 LDAP 数据库中配置管理组，才能对 Administration Server 使用访问控制。使用本章中信息的前提条件是已完成了上述任务。

本章包括以下部分：

什么是访问控制？

可以通过访问控制来确定哪些人可以访问 Proxy Server 及这些人可以访问服务器的哪些部分。可以控制允许对整个服务器进行访问，还是只允许对服务器的某些部分（如目录、文件、文件类型等）进行访问。对收到的请求进行评估时，将根据有次序的一系列规则（称为访问控制条目 (ACE)）来确定访问权限。Proxy Server 通过寻找匹配的条目来决定是应允许还是应拒绝访问。每个 ACE 都指定了服务器是否应继续检查分层结构中的下一个条目。ACE 的集合称为访问控制表 (ACL)。收到请求后，Proxy Server 将在 `obj.conf` 文件中查找对某个 ACL 的引用，然后使用该 ACL 来确定访问权限。默认情况下，服务器具有一个 ACL 文件，其中包含多个 ACL。

根据以下条件允许或拒绝访问：

- 谁在进行请求（用户 - 组）
- 请求来自何方（主机 -IP）
- 请求的发生时间（例如，一天中的某个时间）
- 使用的连接类型 (SSL)

本节包括以下主题：

用户 - 组的访问控制

可以只允许特定的用户或组访问服务器。用户 - 组访问控制要求用户先输入用户名和口令，然后才能访问服务器。服务器会将客户机证书中的信息或客户机证书本身与某个目录服务器条目进行比较。

Administration Server 只使用基本验证。如果要求在 Administration Server 上进行客户机验证，必须手动编辑 `obj.conf` 中的 ACL 文件，将方法更改为 SSL。

用户 - 组验证由为服务器配置的目录服务执行。有关更多信息，参见第 45 页的“配置目录服务”。

目录服务用来实现访问控制的信息可以来自以下资源之一：

- 内部平面文件类型数据库
- 外部 LDAP 数据库

当服务器使用基于 LDAP 的外部目录服务时，对于服务器实例将支持以下类型的用户 - 组验证方法：

- Default
- Basic
- SSL
- Digest
- Other

当服务器使用基于文件的内部目录服务时，对于服务器实例支持的用户 - 组验证方法将包括：

- Default
- Basic
- Digest

用户 - 组验证要求用户先证明自己的身份，才能进行访问。进行验证时，用户通过输入用户名和口令、使用客户机证书或摘要验证插件来证明自己的身份。使用客户机证书时需要加密。

默认验证

默认验证是首选方法。"Default" 设置使用 `obj.conf` 文件中的默认方法，如果 `obj.conf` 中没有设置，将使用 "Basic"。如果选中 "Default"，ACL 规则将不会在 ACL 文件中指定方法。如果选择 "Default"，则只需对 `obj.conf` 文件中的一行进行编辑即可方便地更改所有 ACL 的方法。

基本验证

基本验证要求用户先输入用户名和口令，然后才能访问服务器。这是默认设置。必须在 LDAP 数据库（如 Sun Java System Directory Server）或某个文件中创建并存储一个用户和组的列表。所使用的目录服务器安装到的服务器根目录必须不同于 Proxy Server 的服务器根目录，或必须使用安装在远程计算机上的目录服务器。

当用户尝试访问要求进行用户 - 组验证的资源时，会收到要求输入用户名和口令的提示。服务器收到上述信息时它们可能已加密，也可能未加密，具体取决于是否为服务器启用了加密（即启用了 SSL）。

注意	如果使用无 SSL 加密的基本验证，则将以不加密的文本形式在网络中发送用户名和口令。网络包可能会被截取，因此用户名和口令可能会被盗用。基本验证与 SSL 加密和 / 或主机 -IP 验证结合使用时效果最佳。使用摘要验证可以避免此问题。

验证后用户将看到以下内容：

- 请求的资源（如果验证成功）
- 拒绝访问的消息（如果用户名或口令无效）

可以自定义显示给未经授权的用户的消息。有关更多信息，参见第 154 页的“访问被拒绝时的响应”。

SSL 验证

使用安全性证书，服务器可以用两种方式确认用户的身份：

- 使用客户机证书中的信息作为身份的证明
- 验证 LDAP 目录中发布的客户机证书（附加验证）

将服务器配置为使用证书信息来验证客户机时，服务器将：

- 检查证书是否来自可信 CA（证书授权机构）。如果不是，验证将失败，事务也随之结束。要了解如何启用客户机验证，参见第 82 页的“设置安全首选项”。
- 如果证书来自可信 CA，服务器将使用 `certmap.conf` 文件将证书映射到某个用户的条目。要了解如何配置证书映射文件，参见第 98 页的“使用 certmap.conf 文件”。
- 如果证书正确进行了映射，则检查为该用户指定的 ACL 规则。即使证书的映射正确，ACL 规则仍可能会拒绝该用户的访问。

为控制对特定资源的访问而要求进行客户机验证和要求对与服务器的所有连接进行客户机验证是不同的。如果将服务器配置为对所有连接都要求进行客户机验证，则客户机只能提供由可信 CA 颁发的有效证书。如果将服务器配置为使用 SSL 方法进行对用户和组的验证，则必须满足以下条件：

- 客户机必须提供由可信 CA 颁发的有效证书
- 证书必须映射到 LDAP 中的有效用户
- 访问控制表必须进行正确评估

要求通过访问控制进行客户机验证时，必须为 Proxy Server 启用 SSL 加密算法。有关启用 SSL 的更多信息，参见第 71 页的第 5 章“使用证书和密钥”。

要成功访问要求进行 SSL 验证的资源，客户机证书必须来自 Proxy Server 信任的 CA。如果将 Proxy Server 的 `certmap.conf` 文件配置为将浏览器中的客户机证书与目录服务器中的客户机证书进行比较，则必须在该目录服务器中发布客户机证书。不过，`certmap.conf` 文件也可以配置为仅将证书中的选定信息与目录服务器条目进行比较。例如，可以将 `certmap.conf` 配置为只将浏览器证书中的用户 ID 和电子邮件地址与目录服务器条目进行比较。有关 `certmap.conf` 和证书映射的更多信息，参见第 71 页的第 5 章“使用证书和密钥”。另参见 Proxy Server Configuration File Reference。

摘要验证

可以将 Proxy Server 配置为使用基于 LDAP 或文件的目录服务来执行摘要验证。

摘要验证使用户能够基于用户名和口令进行验证，但不必以明文形式发送用户名和口令。浏览器使用用户的口令和 Proxy Server 提供的某些信息，通过 MD5 算法创建摘要值。

当服务器使用基于 LDAP 的目录服务来执行摘要验证时，还将在服务器端使用摘要验证插件计算此摘要值，并将该值与客户机提供的摘要值进行比较。如果这些摘要值相匹配，用户将通过验证。要进行这种验证，目录服务器必须能够访问明文形式的用户口令。Sun Java System Directory Server 自带一个双向口令插件，它使用对称加密算法以加密形式存储数据，以后可以将数据解密为其原来的形式。只有 Directory Server 保存了数据的密钥。

对于基于 LDAP 的摘要验证，必须启用该双向口令插件和 Proxy Server 自带的摘要验证专用插件。要将 Proxy Server 配置为可以处理摘要验证，请在 `dbswitch.conf` 文件（位于 *server_root*`/userdb/`）中设置数据库定义的 `digestauth` 属性。

服务器将尝试基于指定的 ACL 方法验证 LDAP 数据库，如表 8-1 所示。如果不指定 ACL 方法，要求进行验证时服务器将使用摘要验证或基本验证，不要求进行验证时服务器将使用基本验证。

下表列出了验证数据库支持和不支持的摘要验证。

表 8-1 摘要验证盘问数据生成

ACL 方法	验证数据库支持	验证数据库不支持
默认 未指定	摘要和基本	基本
基本	基本	基本
摘要	摘要	错误

在 `method=digest` 的情况下处理 ACL 时，服务器将尝试通过以下方式进行验证：

- 查找 Authorization 请求标头。如果未找到，将生成要求进行摘要验证的 401 响应，并且进程将停止。
- 查找授权类型。如果验证类型是“摘要”，则服务器将：
  - 检查现时数据。如果不是由此服务器新生成的有效现时数据，则会生成 401 响应，且进程将会停止。如果现时数据已过期，则将在 `stale=true` 时生成 401 响应，且进程将会停止。

    可以通过更改 `magnus.conf` 文件（位于 *server_root*`/proxy-server_name/config/`）中 `DigestStaleTimeout` 参数的值来配置现时数据保持不过期的时间。要设置该值，请将下面一行文本添加到 `magnus.conf` 文件中：

    `DigestStaleTimeout` *seconds*

    其中 *seconds* 表示现时数据保持不过期的秒数。指定的秒数过后，现时数据将过期并要求用户进行新的验证。
  - 检查领域。如果未找到匹配项，则将生成 401 响应，且进程将会停止。
  - 如果验证目录基于 LDAP，则检查 LDAP 目录中是否存在用户；如果验证目录基于文件，则检查文件数据库中是否存在用户。如果未找到，则将生成 401 响应，且进程将会停止。
  - 从目录服务器或文件数据库获取 `request-digest` 值，并查找与客户机的 `request-digest` 匹配的值。如果未找到匹配项，则将生成 401 响应，且进程将会停止。
  - 构建 `Authorization-Info` 标头并将其插入服务器标头。

安装摘要验证插件

对于使用基于 LDAP 的目录服务的摘要验证，必须安装摘要验证插件。此插件将计算服务器端的摘要值，并将该值与客户机提供的摘要值进行比较。如果这些摘要值相匹配，用户将通过验证。

如果使用的是基于文件的验证数据库，则不需要安装摘要验证插件。

在 UNIX 上安装摘要验证插件

摘要验证插件包含一个共享库，在下面的两个文件中都可以找到它：

- `libdigest-plugin.lib`
- `libdigest-plugin.ldif`

在 UNIX 上安装摘要验证插件

1. 确保此共享库所在的服务器计算机便是安装 Sun Java System Directory Server 的服务器计算机。
2. 确保知道 Directory Manager 的口令。
3. 修改 `libdigest-plugin.ldif` 文件，将所有对 `/path/to` 的引用更改为安装了摘要验证插件共享库的位置。
4. 要安装插件，请输入以下命令：

```
% ldapmodify -D "cn=Directory Manager" -w password -a <
libdigest-plugin.ldif
```

在 Windows 上安装摘要验证插件

必须将若干个 `.dll` 文件从 Proxy Server 安装复制到 Sun Java System Directory Server 服务器计算机，Directory Server 才可以与摘要插件一起正常启动。

在 Windows 上安装摘要验证插件

1. 访问 Proxy Server 以下目录中的共享库：

   server_root`\bin\proxy\bin`

2. 复制以下文件：
   - `nsldap32v50.dll`
   - `libspnr4.dll`
   - `libplds4.dll`

3. 将这些文件粘贴到以下任一位置：
   - `\Winnt\system32`
   - Sun Java System Directory Server 的安装目录：*server_root*`\bin\sldap\server`

将 Sun Java System Directory Server 设置为使用 DES 算法

对存储摘要口令的属性进行加密需要使用 DES 算法。

将 Directory Server 设置为使用 DES 算法

1. 启动 Sun Java System Directory Server Console。
2. 打开 iDS 5.0 实例。
3. 选择 "Configuration" 选项卡。
4. 单击插件旁的 + 号。
5. 选择 DES 插件。
6. 选择 "Add" 添加一个新属性。
7. 输入 `iplanetReversiblePassword`。
8. 单击 "Save"。
9. 重新启动 Sun Java System Directory Server 实例。

注 要在 `iplanetReversiblePassword` 属性中为用户设置摘要验证口令，输入的内容必须包括 `iplanetReversiblePasswordobject` 对象。

其他验证

可以使用访问控制 API 创建自定义验证方法。

主机 -IP 的访问控制

可以限制对 Administration Server 及其文件和目录的访问，只将它们提供给使用特定计算机的客户机。可以指定想要允许或拒绝其访问的计算机的主机名或 IP 地址。使用主机 -IP 验证来访问文件或目录对用户来说是一个无缝的过程。用户不必输入用户名或口令就可立即访问文件和目录。

因为可能会有一个以上用户都在使用某台计算机，所以将主机 -IP 验证与用户 / 组验证结合使用效果更佳。如果同时使用这两种验证方法，则访问时将要求提供用户名和口令。

主机 -IP 验证不要求在服务器上配置 DNS（域名服务）。如果选择使用主机 -IP 验证，则网络中必须正在运行 DNS，且已将服务器配置为使用 DNS。要启用 DNS，请访问服务器的 Server Manager，单击 "Preferences" 选项卡，然后单击 "Configure System Preferences"。将会显示 DNS 设置。

启用 DNS 会使 Proxy Server 的性能下降，因为服务器将被迫执行 DNS 查找。为减小 DNS 查找对服务器性能的影响，可以只为访问控制和 CGI 解析 IP 地址，而不是为每个请求都解析 IP 地址。如果要这样做，则请在 `obj.conf` 中进行以下指定：

```
AddLog fn="flex-log" name="access" iponly=1
```

使用访问控制文件

对 Administration Server 或其上的文件或目录使用访问控制时，这些设置将存储在一个扩展名为 `.acl` 的文件中。访问控制文件存储在目录 *server_root*`/httpacl` 中，其中 *server_root* 为服务器的安装位置。例如，如果将服务器安装在 `/usr/Sun/Servers` 中，则 Administration Server 和您服务器上配置的每个服务器实例的 ACL 文件将位于 `/usr/Sun/Servers/httpacl/` 中。

主 ACL 文件为 `generated-proxy-`*serverid*`.acl`。临时工作文件为 `genwork-proxy-`*serverid*`.acl`。如果使用 Administration Server 配置访问，则将会有这两个文件。不过，如果想要进行更复杂的限制，则可以创建多个文件，然后在 `server.xml` 文件中引用这些文件。还有几个特性只能在编辑这些文件时才能使用。例如，有一个特性可以基于一天中的某个时间或一周中的某一天来限制对服务器的访问。

有关访问控制文件及其语法的更多信息，参见第 349 页的附录 A“ACL 文件语法”。有关 `server.xml` 的更多信息，参见 Proxy Server Configuration File Reference。

配置 ACL 用户高速缓存

默认情况下，Proxy Server 会将用户和组验证结果存放在 ACL 用户高速缓存中。可以使用 `magnus.conf` 文件中的 `ACLCacheLifetime` 指令来控制 ACL 用户高速缓存的有效时间。每次引用高速缓存中的某个条目时，都将计算其寿命并检查 `ACLCacheLifetime`。如果该条目的寿命大于或等于 `ACLCacheLifetime`，则不再使用

它。默认值为 120 秒。将该值设置为 0（零）将关闭高速缓存。如果将此值设置得很大，则每次更改 LDAP 条目时可能都需要重新启动 Proxy Server。例如，如果将此值设置为 120 秒，则在长达两分钟的时间内，Proxy Server 可能会与 LDAP 目录不同步。仅当 LDAP 目录不经常更改时才设置一个较大的值。

使用 `magnus.conf` 的参数 `ACLUserCacheSize` 可以配置高速缓存中最多可以保留的条目数。此参数的默认值为 200。新条目将添加到列表的开头，当高速缓存达到其最大大小时，列表末尾的条目将被删除以便容纳新条目。

还可以使用 `magnus.conf` 的参数 `ACLGroupCacheSize` 来设置每个用户条目最多可以高速缓存的组成员资格数。此参数的默认值是 4。遗憾的是，组中用户的非成员资格将不会被高速缓存，这将导致每个请求都要对 LDAP 目录进行多次访问。

使用客户机证书控制访问

如果在服务器上启用了 SSL，则可以将客户机证书与访问控制联用。要这样做就必须指定访问特定资源时将要求提供客户机证书。如果在服务器上启用了此特性，则拥有证书的用户只需在其首次尝试访问受限资源时输入其名称和口令。用户的身份一经建立，服务器就会将其登录名和口令映射到该特定证书。从这时起，用户在访问需要进行客户机验证的资源时将不再需要输入其登录名或口令。当用户尝试访问受限资源时，其客户机将向服务器发送客户机证书，服务器将依照其映射列表对证书进行核对。如果该证书属于已获得访问授权的用户，则将为其提供该资源。

注 为控制对特定资源的访问而要求进行客户机验证和要求对与服务器的所有连接进行客户机验证是不同的。此外还请注意，对所有 SSL 连接都要求提供客户机证书时，系统并不会自动将证书映射到数据库中的用户。要这样做就必须指定访问指定的资源时将要求提供客户机证书。

访问控制如何工作

当服务器收到对某个页面的请求时，将使用 ACL 文件中的规则来判断是否应允许访问。这些规则可以引用发送该请求的计算机的主机名或 IP 地址，还可以引用 LDAP 目录中存储的用户和组。

下面的示例介绍了 ACL 文件可能会包含的内容，并提供了访问控制规则的示例。

```
version 3.0;
# The following "es-internal" rules protect files such
# as icons and images related to Sun Java System Web Proxy Server.
# These "es-internal" rules should not be modified.
  acl "es-internal";
  allow (read, list, execute,info) user = "anyone";
  deny (write, delete) user = "anyone";

# The following rules deny access to the directory "web"
# to everyone not in the directory server and deny everyone
# in the directory server who is not in GroupB.
# Only the users in GroupB are allowed read, execute, list,
# and info permissions. GroupA cannot gain access to the
# directory "web" even though (in the ACL rule below) they
# can access the directory "my_stuff". Furthermore, members
# of GroupB cannot write or delete files.
  acl "path=/export/user/990628.1/docs/my_stuff/web/";
  authenticate (user,group) {
     database = "default";
     method = "basic";
  };
  deny (all)
  (user = "anyone");

  allow (read,execute,list,info)
  (group = "GroupB");

# The following rule denies everyone not in the directory
# server and denies everyone in the directory server except
# users with the ID of "SpecificMemberOfGroupB". The ACL rule
# in this setting also has a requirement that the user
# connect from a specific IP address. The IP address setting
# in the rule is optional, and has been added for extra
# security. Also, this ACL rule has a Customized prompt
# of "Presentation Owner". This Customized prompt appears
# in the username and password dialog box in the client's
# browser.

  acl "path=/export/user/990628.1/docs/my_stuff/web/presentation.html";
  authenticate (user,group) {
     database = "default";
     method = "basic";
     prompt = "Presentation Owner";
  };
  deny (all)
  (user = "anyone" or group = "my_group");
  allow (all)
  (user = "SpecificMemberOfGroupB") and
  (ip = "208.12.54.76");

# The following ACL rule denies everyone not in the directory
# server and everyone in the directory server except for
# GroupA and GroupB access to the directory "my_stuff"
```

```
acl "path=/export/user/990628.1/docs/my_stuff/";
authenticate (user,group) {
   database = "default";
   method = "basic";
};
deny (all)
(user = "anyone");
allow (read,execute,list,info)
(group = "GroupA,GroupB");
```

例如，如果某个用户请求访问以下 URL：
`http://server_name/my_stuff/web/presentation.html`

Proxy Server 将先检查整个服务器的访问控制。如果整个服务器的 ACL 的设置为 "Continue"，则服务器将查找目录 `my_stuff` 的 ACL。如果存在某个 ACL，服务器将检查该 ACL 中的 ACE，然后继续移动到下一个目录。此过程将继续，直至找到的某个 ACL 拒绝了访问，或到达所请求的 URL（在本例中是文件 `presentation.html`）的最后一个 ACL。

要使用 Server Manager 为本例设置访问控制，可以仅为该文件创建一个 ACL，也可以为指向该文件的每个资源都创建一个 ACL。也就是说，一个用于整个服务器，一个用于 `my_stuff` 目录，一个用于 `my_stuff/web` 目录，一个用于该文件。

注 如果有一个以上匹配的 ACL，服务器将使用最后一个匹配的 ACL 语句。

设置访问控制

本节介绍施加访问限制的步骤。可以设置针对所有服务器的全局访问控制规则，也可以设置只针对特定服务器的访问控制规则。例如，人力资源部门可以创建一些 ACL，这些 ACL 允许所有通过验证的用户查看其自己的工资单数据，但只将以更新数据为目的的访问权限授予负责工资单的人力资源部门人员。

本节包括以下主题：

- 设置全局访问控制
- 设置服务器实例的访问控制

注 必须先配置并激活分布式管理，才可以设置全局访问控制。

设置全局访问控制

设置所有服务器的访问控制

1. 访问 Administration Server 并单击 "Global Settings" 选项卡。
2. 单击 "Administer Access Control" 链接。
3. 从下拉式列表中选择管理服务器 (`proxy-admserv`)，单击 "Go" 装入数据，然后单击 "New ACL"（或 "Edit ACL"）。
4. 出现提示时进行验证。将显示 "Access Control Rules For" 页面。Administration Server 有两行默认的访问控制规则，它们是无法编辑的。
5. 选择 "Access Control Is On"（如果尚未选择）。
6. 要将一个默认 ACL 规则添加到该表的最后一行，请单击 "New Line" 按钮。要更改访问控制限制的位置，单击上箭头或下箭头。
7. 单击 "Users/Groups" 列中的 "Anyone"。下部框中将显示 "User/Group" 页面。
8. 选择允许其访问的用户和组，然后单击 "Update"。单击 "Group" 或 "User" 的 "List" 按钮时将会提供列表供您从中选择。有关上述设置的更多信息，参见联机帮助。另参见第 150 页的“指定用户和组”。
9. 单击 "From Host" 列中的 "Anyplace"。下部框中将显示 "From Host" 页面。
10. 指定允许其访问的主机名和 IP 地址，然后单击 "Update"。有关上述设置的更多信息，参见联机帮助。另参见第 151 页的“指定 "From Host"”。
11. 单击 "Programs" 列中的 "All"。下部框中将显示 "Programs" 页面。
12. 选择 "Program Groups" 或在 "Program Items" 字段中输入允许其访问的具体文件名，然后单击 "Update"。有关上述设置的更多信息，参见联机帮助。另参见第 152 页的“限制对程序的访问”。
13. （可选）单击 "Extra" 列中的 "X" 可以添加自定义 ACL 表达式。下部框中将显示 "Customized Expressions" 页面。有关更多信息，参见第 153 页的“编写自定义表达式”。
14. 选中 "Continue" 列中的复选框（如果尚未将其选中）。服务器将对下一行限制进行评判，然后才能确定是否允许该用户进行访问。创建多行限制时，请按先笼统后具体的顺序进行创建。
15. （可选）单击垃圾箱图标可从访问控制规则中删除相应行。
16. （可选）单击 "Response When Denied" 链接可指定用户在访问被拒绝时会收到的响应。下部框中将显示 "Access Deny Response" 页面。选择所需的响应，视需要指定其他信息，然后单击 "Update"。有关上述设置的更多信息，参见第 154 页的“访问被拒绝时的响应”。
17. 单击 "Submit" 将新的访问控制规则存储在 ACL 文件中，或单击 "Revert" 将页面中的元素重置为更改前所具有的值。

设置服务器实例的访问控制

使用 Server Manager 可以创建、编辑或删除特定服务器实例的访问控制。如果是进行删除，请勿删除 ACL 文件中的全部 ACL 规则。至少要保留一个 ACL 文件，并且其中至少要包含一个 ACL 规则，以便启动服务器。删除所有 ACL 规则并重新启动服务器将导致语法错误。

设置服务器实例的访问控制

1. 访问服务器实例的 Server Manager，然后单击 "Preferences" 选项卡。
2. 单击 "Administer Access Control" 链接。
3. 使用以下方法之一选择一个 ACL：
   - "Select A Resource" 将显示使用 ACL 限制访问的资源。从下拉式列表中选择一个资源，或单击 "Regular Expression" 来指定一个正则表达式。有关更多信息，参见 Proxy Server 管理指南中的第 319 页的第 16 章“管理模板和资源”。
   - "Select An Existing ACL" 将列出所有启用的 ACL。未启用的现有 ACL 将不会显示在此列表中。从下拉式列表中进行选择。
   - 可以通过 "Type In The ACL Name" 创建名称式 ACL。只有在熟悉 ACL 文件时才适合使用此选项。如果要对资源应用名称式 ACL，则必须手动编辑 `obj.conf`。有关更多信息，参见第 349 页的附录 A“ACL 文件语法”。
4. 单击相应的 "Edit" 按钮。将显示 "Access Control Rules For" 页面。
5. 选择 "Access Control Is On"（如果尚未选择）。
6. 要将一个默认 ACL 规则添加到该表的最后一行，请单击 "New Line" 按钮。要更改访问控制限制的位置，单击上箭头或下箭头。
7. 要编辑此服务器实例的 ACL，请单击 "Action" 列中的操作。下部框中将显示 "Allow/Deny" 页面。
8. 选择 "Allow"（如果尚未选择它作为默认值），然后单击 "Update"。有关 "Allow" 或 "Deny" 的更多信息，参见第 150 页的“设置操作”。
9. 单击 "Users/Groups" 列中的 "Anyone"。下部框中将显示 "User/Group" 页面。
10. 选择允许其访问的用户和组，指定验证信息，然后单击 "Update"。单击 "Group" 或 "User" 的 "List" 按钮时将会提供列表供您从中选择。有关上述设置的更多信息，参见联机帮助。另参见第 150 页的“指定用户和组”。
11. 单击 "From Host" 列中的 "Anyplace"。下部框中将显示 "From Host" 页面。
12. 指定允许其访问的主机名和 IP 地址，然后单击 "Update"。有关上述设置的更多信息，参见联机帮助。另参见第 151 页的“指定 "From Host"”。

13. 单击 "Rights" 列中的 "All"。下部框中将显示 "Access Rights" 页面。
14. 指定此用户的访问权限，然后单击 "Update"。有关更多信息，参见第 152 页的“限制对程序的访问”。
15. （可选）单击 "Extra" 列中的 "X" 可以添加自定义 ACL 表达式。下部框中将显示 "Customized Expressions" 页面。有关更多信息，参见第 153 页的“编写自定义表达式”。
16. 选中 "Continue" 列中的复选框（如果尚未将其选中）。服务器将对下一行限制进行评判，然后才能确定是否允许该用户进行访问。创建多行限制时，请按先笼统后具体的顺序进行创建。
17. （可选）单击垃圾箱图标可从访问控制规则中删除相应行。请勿删除 ACL 文件中的所有 ACL 规则。至少要保留一个 ACL 文件，并且其中至少要包含一个 ACL 规则，以便启动服务器。如果删除了 ACL 文件中的所有 ACL 规则，然后尝试重新启动服务器，则会收到语法错误。
18. （可选）单击 "Response When Denied" 链接可指定用户在访问被拒绝时会收到的响应。下部框中将显示 "Access Deny Response" 页面。选择所需的响应，视需要指定其他信息，然后单击 "Update"。有关上述设置的更多信息，参见第 154 页的“访问被拒绝时的响应”。
19. 单击 "Submit" 将新的访问控制规则存储在 ACL 文件中，或单击 "Revert" 将页面中的元素重置为更改前所具有的值。

选择访问控制选项

以下主题介绍设置访问控制时可以选择的各种选项。对于 Administration Server，头两行被设置为默认值，无法进行编辑。

本节包括以下主题：

设置操作

可以指定当请求符合访问控制规则时服务器执行的操作。

- **Allow** 意味着用户或系统可以访问请求的资源
- **Deny** 意味着用户或系统不能访问该资源

服务器将逐一检查访问控制条目 (ACE) 列表来确定访问权限。例如，第一个 ACE 通常为拒绝每个用户。如果将第一个 ACE 设置为 "Continue"，则服务器将检查列表中的第二个 ACE，如果该 ACE 匹配，则将使用下一个 ACE。如果未选择 "Continue"，将拒绝任何用户访问该资源。服务器将继续向下检查列表，直到找到不匹配的 ACE 或虽然匹配但未设置为 "Continue" 的 ACE。最后一个匹配的 ACE 将确定是允许还是拒绝访问。

指定用户和组

使用用户和组验证时，将提示用户输入用户名和口令，然后才能访问在访问控制规则中指定的资源。

Proxy Server 将检查存储在 LDAP 服务器（如 Sun Java System Directory Server）或基于文件的内部验证数据库中的用户和组的列表。

可以允许或拒绝数据库中每个用户的访问，也可以使用通配符模式允许或拒绝特定用户的访问，还可以从用户和组的列表中选择允许或拒绝其访问的用户。

用户界面中的 "Access Control Rules For" 页面将为 "Users/Groups" 显示以下元素。

- **Anyone (No Authentication)** 是默认设置，表示任何用户都可以在不输入用户名或口令的情况下访问该资源。不过，用户仍可能会被拒绝访问，这要视其他设置（如主机名或 IP 地址）而定。对于 Administration Server，这意味着为分布式管理指定的 administrators 组中的任何用户都可以访问各个页面。
- **Authenticated People Only**
    - **All In The Authentication Database** 将匹配在数据库中拥有条目的任何用户。
    - **Only The following People** 指定要匹配的用户和组。可以用逗号分隔各个条目以分别列出用户或用户组，也可以使用通配符模式，还可以从数据库中存储的用户和组的列表中选择。**Group** 将匹配指定的组中的所有用户。**User** 将匹配指定的个别用户。对于 Administration Server，用户还必须是为分布式管理指定的 administrators 组的成员。

- **Prompt For Authentication** 指定在验证对话框中显示的消息文本。可以使用此文本来描述用户需要输入的内容。用户大约会看到该提示的前 40 个字符，具体视操作系统而定。大多数浏览器可以高速缓存用户名和口令，并将其与提示文本相关联。这意味着如果用户访问服务器中具有相同提示的区域（文件和目录），将不必再次键入用户名和口令。反之，如果要强制用户针对不同区域再次进行验证，则必须为该资源的 ACL 更改提示。
- **Authentication Methods** 指定服务器从客户机获取验证信息所使用的方法。Administration Server 只提供了基本验证方法。Server Manager 提供以下验证方法：
  - **Default** 使用在 `obj.conf` 文件中指定的默认方法。如果 `obj.conf` 中没有设置，则使用 "Basic"。如果选择 "Default"，ACL 规则将不会在 ACL 文件中指定方法。如果选择 "Default"，则只需对 `obj.conf` 文件中的一行进行编辑即可方便地更改所有 ACL 的方法。
  - **Basic** 将使用 HTTP 方法从客户机获取验证信息。仅当为服务器启用了加密（启用了 SSL）时，才会对用户名和口令加密。否则将以明文形式发送用户名和口令，如果被截取，则会为他人所获悉。
  - **SSL** 将使用客户机证书来验证用户。要使用此方法，必须为服务器启用 SSL。启用加密后，就可以结合使用 "Basic" 和 "SSL" 方法。
  - **Digest** 使用的验证机制可以让浏览器不必以明文形式发送用户名和口令，就可以基于用户名和口令对用户进行验证。浏览器使用用户的口令和 Proxy Server 提供的某些信息，通过 MD5 算法创建摘要值。还将在服务器端使用摘要验证插件计算此摘要值，并将该值与客户机提供的摘要值进行比较。
  - **Other** 使用通过访问控制 API 创建的自定义方法。
- **Authentication Database** 指定服务器用于验证用户的数据库。只能通过 Server Manager 使用此选项。如果选择 "Default"，服务器将查找配置为默认值的目录服务中的用户和组。如果想要将各个 ACL 配置为使用其他数据库，请选择 "Other"，然后指定数据库。必须在 *server_root*`/userdb/dbswitch.conf` 中指定非默认数据库和 LDAP 目录。如果为某个自定义数据库使用访问控制 API，请选择 "Other"，然后输入数据库名称。

指定 "From Host"

可以基于发出请求的计算机限制对 Administration Server 的访问。

用户界面中的 "Access Control Rules For" 页面将为 "From Host" 显示以下元素。

- **Anyplace** 允许所有用户和系统进行访问
- **Only From** 只允许特定主机名或 IP 地址进行访问

如果选择 "Only From" 选项，请在 "Host Names" 或 "IP Addresses" 字段中输入通配符模式或以逗号分隔的列表。按主机名进行限制比按 IP 地址进行限制更灵活。如果某个用户的 IP 地址发生变化，将不需要更新此列表。不过，按 IP 地址进行限制更可靠。如果针对已连接客户机进行的 DNS 查找失败，将无法使用主机名限制。

对于匹配计算机的主机名或 IP 地址的通配符模式，将只能使用 * 通配符表示法。例如，要允许或拒绝访问特定域中的所有计算机，可以输入匹配该域中所有主机的通配符模式，如 `*.example.com`。可以为访问 Administration Server 的超级用户设置不同的主机名和 IP 地址。

对于主机名，* 必须替换名称中的整个部分。也就是说，`*.example.com` 是可以接受的，但 `*users.example.com` 是不可接受的。当 * 出现在主机名中时，它必须是最左侧的字符。例如，`*.example.com` 是可以接受的，但 `users.*.com` 是不可接受的。

对于 IP 地址，* 必须替换地址中的整个字节。例如，`198.95.251.*` 是可以接受的，但 `198.95.251.3*` 是不可接受的。当 * 出现在 IP 地址中时，它必须是最右侧的字符。例如，`198.*` 是可以接受的，但 `198.*.251.30` 是不可接受的。

限制对程序的访问

对程序的访问只能通过 Administration Server 进行限制。通过限制对程序的访问可以只允许指定的用户查看 Server Manager 页面，并确定他们是否有权配置该服务器。例如，可以允许一些管理员配置 Administration Server 的 "Users and Groups" 部分，但拒绝其访问 "Global Settings" 部分。

可以配置不同的用户来访问不同的功能域。一旦用户获得了对若干选定功能域的访问权限，在其登录后，即可使用且只能够使用这些功能域的 Administration Server 页面。

用户界面中的 "Access Control Rules For" 页面将为 "Programs" 显示以下元素。

- **All Programs** 允许或拒绝访问所有程序。默认情况下，管理员可以访问某个服务器的所有程序。
- 可以通过 **Only The Following** 指定用户有权访问的程序。
    - **Program Groups** 反映的是 Administration Server 的选项卡（例如，"Preferences" 和 "Global Settings"），并代表对这些页面的访问权限。当管理员访问 Administration Server 时，服务器将使用其用户名、主机和 IP 地址来确定其可以查看的页面。
    - 可以通过在 **Program Items** 字段中输入页面名称来控制对程序内特定页面的访问。

设置访问权限

服务器实例的访问权限只能由 Server Manager 设置。访问权限限制对服务器上文件和目录的访问。除了允许或拒绝所有访问权限外，还可以指定规则来允许或拒绝部分访问权限。例如，可以向用户授予只读文件访问权限，这样他们可以查看信息，但不能更改文件。

用户界面中的 "Access Control Rules For" 页面将为 "Rights" 显示以下元素。

- **All Access Rights** 是默认设置，用于允许或拒绝所有权限。
- 可以通过 **Only The following Rights** 选择要允许或拒绝的权限组合：
  - **Read** 允许用户查看文件，包括 HTTP 方法 GET、HEAD、POST 和 INDEX。
  - **Write** 允许用户更改或删除文件，其中包括 HTTP 方法 PUT、DELETE、MKDIR、RMDIR 和 MOVE。要删除文件，用户必须同时拥有写权限和删除权限。
  - **Execute** 允许用户执行服务器端应用程序，如 CGI 程序、Java applet 和代理程序。
  - **Delete** 允许拥有写权限的用户删除文件或目录。
  - **List** 允许用户访问不包含 `index.html` 文件的目录中的文件的列表。
  - **Info** 允许用户接收有关 URI 的信息，例如，`http_head`。

编写自定义表达式

可以为 ACL 输入自定义表达式。只有在熟悉 ACL 文件的语法和结构时，才适合选择此选项。有若干特性只有在编辑 ACL 文件或创建自定义表达式时才可以使用。例如，可以基于一天中的某个时间和 / 或一周中的某一天来限制对服务器的访问。

以下自定义表达式显示了如何基于一天中的某个时间及一周中的某一天来限制访问。本示例假定 LDAP 目录中有两个组。"Regular" 组可以在星期一至星期五每天上午 8:00 至下午 5:00 之间进行访问。"Critical" 组可以在任何时间进行访问。

```
allow (read)
{
    (group=regular and dayofweek="mon,tue,wed,thu,fri");
    (group=regular and (timeofday>=0800 and timeofday<=1700));
    (group=critical)
}
```

有关有效语法和 ACL 文件的更多信息，参见第 349 页的附录 A“ACL 文件语法”。

禁用访问控制

取消选定 "Access Control Rules For" 页面上标签为 "Access Control Is On" 的选项时，将会收到一个提示，询问是否要删除 ACL 中的记录。如果单击 "OK"，将从 ACL 文件中删除该资源的 ACL 条目。

如果想取消激活 ACL，可以通过在文件 `generated-proxy-`*serverid*`.acl` 中每个 ACL 行的开头添加 # 符号，使 ACL 行变为注释。

在 Administration Server 中，可以为特定服务器实例创建和启用访问控制，而为其他服务器禁用访问控制（默认设置）。例如，可以通过 Administration Server 拒绝对 Server Manager 页面的任何访问。在启用分布式管理并为其他服务器禁用访问控制（默认设置）的情况下，管理员仍可以访问和配置这些服务器，但不能配置 Administration Server。

访问被拒绝时的响应

Proxy Server 提供了访问被拒绝时的默认消息，需要时可以自定义这一响应。也可以为每个访问控制对象创建不同的消息。

默认情况下，对于 Administration Server，用户收到的将是 *server_root*`/httpacl/admin-denymsg.html` 中包含的 "Permission Denied" 消息。

更改 "Access Denied" 消息

1. 单击 "Access Control Rules For" 页面上的 "Response When Denied" 链接。
2. 选择所需的响应，视需要输入其他信息（确保用户可以访问将其重定向到的响应），然后单击 "Update"。
3. 单击 "Submit" 保存所做更改，或单击 "Revert" 将页面中的元素的值重置为更改前所具有的值。

限制对服务器区域的访问

本节介绍一些常用的对服务器及其内容的访问限制。每个过程的步骤详细说明了必须执行的具体操作。不过，仍然必须完成以下部分中介绍的步骤：第 148 页的“设置服务器实例的访问控制”。

本节包括以下主题：

限制对整个服务器的访问

可能需要为某个组中的用户授予访问权限，这些用户从子域中的计算机访问服务器。例如，公司某部门可能有一个服务器，您只希望来自网络特定子域中的计算机的用户能够对其进行访问。

限制对整个服务器的访问

按照设置服务器实例的访问控制中介绍的步骤（参见第 148 页的“设置服务器实例的访问控制”）执行以下操作：

1. 访问服务器实例的 Server Manager。
2. 在 "Preferences" 选项卡上，单击 "Administer Access Control" 链接。
3. 从下拉式列表中选择整个服务器，单击 "Select"，然后单击相应的 "Edit" 按钮。将显示 "Access Control Rules For" 页面。
4. 添加一个新规则以拒绝所有用户的访问。
5. 添加另一个新规则以允许特定组的访问。
6. 使用 "From Host" 指定想要限制的主机名和 IP 地址。
7. 单击 "Submit" 保存所做更改。

限制对目录（路径）的访问

可以允许某个组中的用户读取或运行由该组的所有者控制的目录中的应用程序、子目录及文件。例如，项目经理可以更新状态信息，供项目组查看。

限制对目录的访问

按照设置服务器实例的访问控制中介绍的步骤（参见第 148 页的“设置服务器实例的访问控制”）执行以下操作：

1. 访问服务器实例的 Server Manager。
2. 在 "Preferences" 选项卡上，单击 "Administer Access Control" 链接。
3. 从下拉式列表中选择所需的资源，然后单击 "Edit"。
4. 创建一个新规则并保留默认设置，以拒绝任何位置的任何用户的访问。
5. 创建另一个新规则，允许特定组中的用户只具有读权限和执行权限。
6. 再创建一个新规则，允许特定用户拥有全部权限。
7. 取消选定后两个规则的 "Continue"。
8. 单击 "Submit" 保存所做更改。

限制对文件类型的访问

可以限制对文件类型的访问。例如，可能想只允许特定用户创建在服务器上运行的程序。任何用户都可以运行程序，但只有组中的指定用户才可以创建或删除程序。

限制对文件类型的访问

按照设置服务器实例的访问控制中介绍的步骤（参见第 148 页的“设置服务器实例的访问控制”）执行以下操作：

1. 访问服务器实例的 Server Manager。
2. 在 "Preferences" 选项卡上，单击 "Administer Access Control" 链接。
3. 单击 "Select A Resource" 部分中的 "Regular Expression"，然后指定正则表达式。例如：`*.cgi`。
4. 单击 "Edit"。
5. 创建一个新规则，为所有用户授予读权限。
6. 创建另一个规则，仅为指定组授予写权限和删除权限。
7. 单击 "Submit" 保存所做更改。

对于文件类型限制，应使两个 "Continue" 复选框都保持选中状态。收到对某个文件的请求时，服务器将先检查该文件类型的 ACL。

将在 `obj.conf` 中创建一个 `PathCheck` 函数，其中可以包含文件或目录的通配符模式。ACL 文件中的条目将如下所示：`acl"*.cgi";`

基于一天中的某个时间限制访问

可以将对服务器的写访问和删除访问限制为只允许在指定的时间或指定的日期进行。

基于一天中的某个时间限制访问

按照设置服务器实例的访问控制中介绍的步骤（参见第 148 页的“设置服务器实例的访问控制”）执行以下操作：

1. 访问服务器实例的 Server Manager。
2. 在 "Preferences" 选项卡上，单击 "Administer Access Control" 链接。
3. 从 "Select A Resource" 部分中的下拉式列表选择整个服务器，然后单击 "Edit"。
4. 创建一个新规则，为所有用户授予读权限和执行权限。这意味着，如果某个用户想要添加、更新或删除文件或目录，将不会应用此规则，服务器将搜索另一个匹配的规则。
5. 创建另一个新规则，拒绝为所有用户授予写权限和删除权限。
6. 单击 "X" 链接，创建一个自定义表达式。
7. 输入允许在一周中的哪些天及一天中的哪些时间进行访问。例如：

```
user = "anyone" and
dayofweek = "sat,sun" or
(timeofday >= 1800 and
timeofday <= 600)
```

8. 单击 "Submit" 保存所做更改。只要自定义表达式中存在错误，就会产生错误消息。请进行更正并再次提交。

基于安全性限制访问

可以为同一服务器实例配置 SSL 和非 SSL 侦听套接字。基于安全性限制访问使您可以为只应通过安全通道传输的资源创建保护。

基于安全性限制访问

按照设置服务器实例的访问控制中介绍的步骤（参见第 148 页的“设置服务器实例的访问控制”）执行以下操作：

1. 访问服务器实例的 Server Manager。
2. 在 "Preferences" 选项卡上，单击 "Administer Access Control" 链接。
3. 从 "Select A Resource" 部分中的下拉式列表选择整个服务器，然后单击 "Edit"。
4. 创建一个新规则，为所有用户授予读权限和执行权限。这意味着，如果某个用户想要添加、更新或删除文件或目录，将不会应用此规则，服务器将搜索另一个匹配的规则。
5. 创建另一个新规则，拒绝为所有用户授予写权限和删除权限。
6. 单击 "X" 链接，创建一个自定义表达式。
7. 输入 `ssl="on"`。例如：

```
user = "anyone" and ssl="on"
```

8. 单击 "Submit" 保存所做更改。只要自定义表达式中存在错误，就会产生错误消息。请进行更正并再次提交。

保护对资源的访问

本节介绍在启用分布式管理后，为通过 Proxy Server 保护访问控制所必须执行的其他任务。

本节包括以下主题。

- 保护对服务器实例的访问
- 启用基于 IP 的访问控制

保护对服务器实例的访问

要配置 Proxy Server 来控制对服务器实例的访问，请编辑 *server_root*/httpacl/*.proxy-admserv.acl 文件来指定要向其授予访问控制权限的用户。例如：

```
acl "proxy-server_instance";
authenticate (user,group) {
database = "default";
method = "basic";
};
deny absolute (all) user != "UserA";
```

启用基于 IP 的访问控制

如果引用 ip 属性的访问控制条目位于与 Administration Server 有关的 ACL 文件 (gen*.proxy-admserv.acl) 中，请完成下面的步骤 1 和步骤 2。

如果引用 ip 属性的访问控制条目位于与某个服务器实例有关的 ACL 文件中，请只为该 ACL 完成下面的步骤 1。

启用基于 IP 的访问控制

1. 编辑 *server_root*/httpacl/gen*.proxy-admserv.acl 文件，除了在验证列表中添加 user 和 group 外，还要再添加 ip，如下所示：

   ```
   acl "proxy-admserv";
   authenticate (user,group,ip) {
   database = "default";
   method = "basic";
   };
   ```

2. 添加以下访问控制条目：

   ```
   deny absolute (all) ip !="ip_for_which_access_is_allowed";
   ```

   例如：

   ```
   acl "proxy-admserv";
   authenticate (user,group,ip) {
   database = "default";
   method = "basic";
   };
   deny absolute (all) ip !="205.217.243.119";
   ```

创建基于文件验证的 ACL

Proxy Server 支持使用基于文件的验证数据库，这些数据库在平面文件中以文本格式存储用户和组信息。ACL 框架被设计为可以使用文件验证数据库。

注 Proxy Server 不支持动态平面文件。平面文件数据库将在服务器启动时装入。对这些文件所做的任何更改仅在重新启动服务器时才能生效。

本节包括以下主题：

- 创建基于文件验证的目录服务的 ACL
- 创建基于摘要验证的目录服务的 ACL

ACL 条目可以使用 `database` 关键字来引用用户数据库。例如：

```
acl "default";
    authenticate (user) {
...
    database="myfile";
...
};
```

server_root`/userdb/dbswitch.conf` 文件包含定义文件验证数据库及其配置的条目。例如：

```
directory myfiledb file
myfiledb:syntax keyfile
myfiledb:keyfile /path/to/config/keyfile
```

下表列出了文件验证数据库支持的参数。

表 8-2 文件验证数据库支持的参数

参数	描述
`syntax`	（可选）值为 `keyfile` 或 `digest`。如果未指定，默认值将是 `keyfile`。
`keyfile`	（`syntax=keyfile` 时是必需的）包含用户数据的文件的路径。
`digestfile`	（`syntax=digest` 时是必需的）包含摘要验证用户数据的文件的路径。

注意 文件验证数据库文件中行的最大长度是 255。如果任何行的长度超过此限制，服务器将无法启动，并会在日志文件中记录错误。

注 在尝试使用基于文件的验证数据库设置 ACL 前，请确保已配置了基于文件的验证目录服务。有关更多信息，参见第 45 页的“配置目录服务”。

创建基于文件验证的目录服务的 ACL

创建基于文件验证的目录服务的 ACL

1. 访问服务器实例的 Server Manager。
2. 在 "Preferences" 选项卡上，单击 "Administer Access Control" 链接。
3. 从下拉式列表中选择 ACL 文件，然后单击 "Edit"。
4. 在 "Access Control Rules For" 页面中，单击想要编辑的 ACL 条目的 "Users/Groups" 链接。下部框中将显示 "User/Group" 页面。
5. 在 "Authentication Database" 下的下拉式列表中指定密钥文件数据库。
6. 单击 "Update"，然后单击 "Submit" 保存所做更改。

依据基于密钥文件的文件验证数据库设置 ACL 时，将使用 ACL 条目（如下面给出的样例条目）更新 `dbswitch.conf` 文件：

```
version 3.0;
acl "default";
authenticate (user) {
     prompt = "Sun Java System Proxy Server 4.0";
     database = "mykeyfile";
     method = "basic";
};
deny (all) user = "anyone";
allow (all) user = "all";
```

创建基于摘要验证的目录服务的 ACL

文件验证数据库还支持适用于摘要验证的、基于 RFC 2617 的文件格式。将存储基于口令和领域的散列，而不会保留明文口令。

创建基于摘要验证的目录服务的 ACL

1. 访问服务器实例的 Server Manager。
2. 在 "Preferences" 选项卡上，单击 "Administer Access Control" 链接。
3. 从下拉式列表中选择 ACL 文件，然后单击 "Edit"。
4. 在 "Access Control Rules For" 页面中，单击想要编辑的 ACL 的 "Users/Groups" 链接。下部框中将显示 "User/Group" 页面。
5. 在 "Authentication Database" 下的下拉式列表中指定摘要数据库。
6. 单击 "Update"，然后单击 "Submit" 保存所做更改。

依据基于摘要验证的文件验证数据库设置 ACL 时，将使用 ACL 条目（如下面给出的样例条目）更新 `dbswitch.conf` 文件：

```
version 3.0;
acl "default";
authenticate (user) {
     prompt = "filerealm";
     database = "mydigestfile";
     method = "digest";
};

deny (all) user = "anyone";
allow (all) user = "all";
```

第 9 章

使用日志文件

您可以使用多种方法监视服务器的活动。本章介绍了通过记录和查看日志文件来监视服务器的方法。有关使用内置性能监视服务或 SNMP 的信息，参见第 187 页的第 10 章“监视服务器”。

本章包括以下各节：

关于日志文件

服务器日志文件记录服务器的活动。使用这些日志可以监视服务器，并在排除故障时为您提供帮助。错误日志文件位于服务器根目录下的 `proxy-server_name/logs/errors` 中，该文件列出了服务器曾遇到的所有错误。访问日志位于服务器根目录下的 `proxy-server_name/logs/access` 中，该文件记录了向服务器提出的请求以及服务器做出的响应方面的信息。可以配置 Proxy Server 访问日志文件中记录的信息。使用日志分析程序可以生成服务器统计信息。通过归档可以将服务器的错误日志文件和访问日志文件进行备份。

注 由于操作系统方面的限制，Proxy Server 无法在 Linux 上处理大于 2GB 的日志文件。达到最大文件大小后，日志记录就会停止。

UNIX 和 Windows 平台上的日志记录

本节介绍如何创建日志文件。此外，还包括以下主题：

- 默认错误日志记录
- 使用 syslog 记录日志
- 使用 Windows eventlog 记录日志

默认错误日志记录

在 UNIX 和 Windows 平台上，来自管理服务器的日志都集中存放在管理 `proxy-admserv/logs/` 目录中。来自服务器实例的日志集中存放在 `proxy-server_name/logs/` 目录中。

可以设置整个服务器的默认日志级别。可将标准输出和标准错误重定向到服务器的事件日志，并将日志输出定向到操作系统的系统日志。此外，还可以将标准输出和标准错误内容定向到服务器的事件日志。默认情况下，日志消息除了发送到指定的服务器日志文件以外，还将发送到标准错误。

使用 syslog 记录日志

syslog 适用于要求集中记录日志的稳定的可操作环境。对于经常需要使用日志输出来进行诊断和调试的环境，单独的服务器实例日志可能更易于管理。

注

- 如果将服务器实例和管理服务器的所有日志记录数据都存储在一个文件中，可能难于读取和调试。建议将 syslog 主日志文件仅用于已部署且正在顺利运行的应用程序。
- 日志记录消息与 Solaris 守护进程应用程序中的所有其他日志混合在一起。

通过将 syslog 日志文件与 syslogd 以及系统日志守护进程一起使用，可以将 `syslog.conf` 文件配置为：

- 将消息记入相应的系统日志
- 将消息写入系统控制台
- 将日志记录消息转发到一组用户，或通过网络将其转发到另一台主机上的另一个 syslogd

将日志记录到 syslog 意味着来自 Proxy Server 以及其他守护进程应用程序的日志都将集中存放在同一个文件中，因此在日志记录消息中增加了以下信息，以便标识来自特定服务器实例的 Proxy Server 专有消息：

- 唯一消息 ID
- 时间戳
- 实例名
- 程序名（proxyd 或 proxyd-wdog）
- 进程 ID（proxyd 进程的 PID）
- 线程 ID（可选）
- 服务器 ID

可以在 `server.xml` 文件中为管理服务器和服务器实例二者均配置 LOG 元素。

要详细了解 UNIX 操作环境中所使用的 syslog 日志记录机制，请在出现终端提示时使用以下 man 命令：

```
man syslog

man syslogd

man syslog.conf
```

使用 Windows eventlog 记录日志

要详细了解 Windows 操作环境中所使用的事件日志机制，请在 Windows 帮助系统索引中查找关键字“事件日志”。

日志级别

下表按严重性增高顺序定义了 Proxy Server 中的日志级别和消息。

表 9-1 日志级别

日志级别	描述
finest	表明调试信息详尽程度的消息。其中 finest 最详尽。
finer	
fine	
info	信息类型的消息，通常与服务器配置或服务器状态相关。这些消息不是指需要立即采取行动的错误。
warning	表明警告的消息。这种消息可能伴有异常情况。
failure	表明严重故障的消息，故障可能会妨碍应用程序的正常执行。
config	与各种静态配置信息相关的消息，可以帮助用户调试可能与特定配置有关的问题。
security	表明安全问题的消息。
catastrophe	表明致命错误的消息。

归档日志文件

可以将访问日志文件和错误日志文件设置为自动归档。在某一时间或在指定的时间间隔后，用户的日志将被轮转。Proxy Server 会保存旧的日志文件，并用含有保存日期和时间的名称为所保存的文件加上时间戳。

例如，可以将访问日志文件设置为每小时轮转一次，而 Proxy Server 会保存该文件并将其命名为“access.200505160000”，其中，将日志文件名、年月日和 24 时制时间连接在一起形成了单个字符串。根据所设置的日志轮转类型，日志归档文件的实际格式会有所不同。

Proxy Server 提供了两种用于归档文件的日志轮转类型：内部守护进程日志轮转和基于计时程序的日志轮转。

内部守护进程日志轮转

此类型的日志轮转发生在 HTTP 守护进程内，且只能在启动时进行配置。使用内部守护进程日志轮转，服务器可以在内部轮转日志，而无需重新启动。使用此方法轮转的日志将被保存为以下格式：

```
access.<YYYY><MM><DD><HHMM>
```

```
errors.<YYYY><MM><DD><HHMM>
```

可以指定用来轮转日志文件和开始新日志文件的基准时间。例如，如果轮转开始时间为晚 12:00，并且轮转间隔为 1440 分钟（一天），则当您保存并应用更改时，系统将立即创建一个新的日志文件，而不管当前的时间。日志文件将在每天的晚 12:00 进行轮转，而且将在晚 12:00 为访问日志加上时间戳并将其保存为 `access.200505172400`。同样，如果将间隔设置为 240 分钟（4 小时），开始时间为晚 12:00，则访问日志文件将包含从晚 12:00 到晚 4:00、从晚 4:00 到早 8:00 等时间段内收集到的信息。

如果启用了日志轮转，将在服务器启动时开始进行日志文件轮转。第一个要轮转的日志文件将收集从当前时间至下次轮转时间之间的信息。以上一个例子为例，如果将开始时间设置为晚 12:00，并将轮转间隔设置为 240 分钟，而当前的时间为早 6:00，则第一个要轮转的日志文件将包含从早 6:00 至早 8:00 之间收集到的信息，下一个日志文件将包含从早 8:00 至中午 12:00 的信息，依此类推。

基于调度程序的日志轮转

这种类型的日志轮转所基于的时间和日期存储在 `server.xml` 文件中，该文件位于 *server_root*`/proxy-`*server_name*`/config/` 目录。此方法可用于将日志文件立即归档，或使服务器在特定日期中的特定时间将日志文件归档。服务器的调度程序配置选项存储在 `server_root/proxy-`*server_name*`/config/` 目录的 `server.xml` 中。使用基于调度程序的方法轮转的日志将被保存为以下格式：

```
<original_filename>.<YYYY><MM><DD><HHMM>
```

例如，当在下午 4:30 进行轮转时，`access` 可能会变成 `access.200505171630`。

日志轮转在服务器启动时进行初始化。如果开启了轮转，Proxy Server 会创建一个带有时间戳的访问日志文件，并在服务器启动时开始轮转。

轮转开始以后，如果有需要记录到访问日志文件或错误日志文件的请求或错误，并且其发生在预定的“下次轮转时间”之后，则 Proxy Server 会创建一个带有新时间戳的日志文件。

注 您应该在运行日志分析程序之前将服务器日志归档。

要归档日志文件并指定是采用内部守护进程方法还是采用基于调度程序的方法，请使用 Server Manager 中的 "Archive Log" 页面。

设置访问日志首选项

在安装过程中，将为服务器创建名为 access 的访问日志文件。通过指定是否记录访问、记录日志时使用的格式，以及当客户机访问资源时服务器是否要查找客户机的域名，用户可以自定义任意资源的访问日志记录。

可以使用 Server Manager 中的 "Set Access Log Preferences" 页面来指定日志记录首选项，也可在 obj.conf 文件中手动配置以下指令。在 obj.conf 中，服务器调用函数 flex-init 来初始化灵活日志记录系统，并调用函数 flex-log 以灵活日志格式记录特定于请求的数据。为使用通用日志文件格式记录请求，服务器会调用 init-clf 来初始化 obj.conf 中使用的“通用日志”子系统，并调用 common-log 以通用日志格式（大多数 HTTP 服务器采用的格式）记录特定于请求的数据。

创建某个资源的访问日志后，将无法更改日志的格式，除非对它进行归档或为该资源创建一个新的访问日志文件。

更改现有日志文件的格式时，应首先删除 / 重命名现有的日志文件，也可以使用不同的文件名。

设置 Administration Server 的访问日志首选项

1. 访问 Administration Server 并单击 "Preferences" 选项卡。
2. 单击 "Set Access Log Preferences" 链接。将显示 "Set Access Log Preferences" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。
4. 指定是否记录客户机访问。这要求启用“域名服务”(DNS)。
5. 指定访问日志文件的绝对路径。默认情况下，日志文件保存在服务器根目录下的 logs 目录中。如果指定了部分路径，则服务器将假定该路径相对于服务器根目录下的 logs 目录。

   如果编辑的是整个服务器，则此字段的默认值为 $accesslog，在配置文件中，该变量表示服务器的访问日志文件。
6. 选择是否在访问日志中记录访问服务器的那些系统的域名或 IP 地址。

7. 选择要在访问日志中使用的日志文件格式的类型。可用选项如下：

   - **Use Common LogFile Format。**包括客户机的主机名、经过验证的用户名、请求日期和时间、HTTP 标头、返回给客户机的状态码，以及发送给客户机的文档的内容长度。
   - **Only Log。**使您可以选择要记录的信息。可从以下灵活日志格式项中进行选择：
     - **Client Hostname。**请求访问的客户机的主机名或 IP 地址（如果已禁用 DNS）。
     - **Authenticate User Name。**如果需要进行验证，您可以在访问日志中列出经过验证的用户名。
     - **System Date。**客户机请求的日期和时间。
     - **Full Request。**客户机所做的完整请求。
     - **Status。**服务器返回给客户机的状态码。
     - **Content Length。**发送至客户机的文档的内容长度（以字节计）。
     - **HTTP Header, "referer"。**引用者用于指定客户机从中访问当前页面的页面。例如，如果用户正在查看文本搜索查询的结果，则引用者将是用户从中访问文本搜索引擎的页面。引用者允许服务器创建回溯链接的列表。
     - **HTTP Header, "user-agent"。**用户代理信息包括客户机所用浏览器的类型、版本和客户机运行的操作系统，这些信息均来自于客户机向服务器发送的 HTTP 标头信息中的 User-agent 字段。
     - **Method。**所用的 HTTP 请求方法（如 GET、PUT 或 POST）。
     - **URI。**统一资源标识符。服务器上资源的位置。例如，对于 `http://www.a.com:8080/special/docs`，URI 为 `special/docs`。
     - **Query String Of The URI。**URI 中问号之后的所有内容。例如，对于 `http://www.a.com:8080/special/docs?find_this`，URI 的查询字符串为 `find_this`。
     - **Protocol。**使用的传输协议和版本。
   - 如果选择自定义格式，请在 "Custom Format" 字段中键入该格式。

8. 单击 "OK"。
9. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
10. 单击 "Restart Proxy Server" 按钮以应用更改。

设置服务器实例的访问日志首选项

1. 访问 Server Manager，然后单击 "Server Status" 选项卡。
2. 单击 "Set Access Log Preferences" 链接。将显示 "Set Access Log Preferences" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。
4. 指定是否记录客户机访问。这要求启用“域名服务”(DNS)。
5. 指定访问日志文件的绝对路径。默认情况下，日志文件保存在服务器根目录下的 logs 目录中。如果指定了部分路径，则服务器将假定该路径相对于服务器根目录下的 logs 目录。

   如果编辑的是整个服务器，则此字段的默认值为 `$accesslog`，在配置文件中，该变量表示服务器的访问日志文件。
6. 选择是否在访问日志中记录访问服务器的那些系统的域名或 IP 地址。
7. 选择日志文件应采用的格式：通用、扩展、扩展 2、仅限指定信息（"Only log" 单选按钮）或自定义。如果单击 "Only log"，则可以使用以下灵活日志格式项：
8. 选择要在访问日志中使用的日志文件格式的类型。服务器访问日志可以采用通用日志文件格式、扩展日志文件格式、扩展 2 日志文件格式、灵活日志格式或您自己的可自定义格式。通用日志文件格式是普遍受支持的格式，可提供服务器的固定信息。灵活日志格式允许（从 Proxy Server）选择要记录的内容。可自定义的格式使用参数块，用户可以指定这些参数块来控制记录的内容。

   - **Use Common LogFile Format。**包括客户机的主机名、经过验证的用户名、请求日期和时间、HTTP 标头、返回给客户机的状态码，以及发送给客户机的文档的内容长度。
   - **Use Extended LogFile Format。**包括通用日志文件格式的所有字段以及一些附加字段，如远程状态、代理服务器到客户机的内容长度、远程服务器到代理服务器的内容长度、代理服务器到远程服务器的内容长度、客户机到代理服务器的标头长度、代理服务器到客户机的标头长度、代理服务器到远程服务器的标头长度、远程服务器到代理服务器的标头长度以及传送时间。
   - **Use Extended2 LogFile Format。**包括扩展日志文件格式的所有字段以及一些附加字段，如客户机状态、服务器状态、远程状态、高速缓存完成状态以及实际路由。
   - **Only Log。**使您可以选择要记录的信息。可从以下灵活日志格式项中进行选择：
     - **Client Hostname。**请求访问的客户机的主机名或 IP 地址（如果已禁用 DNS）。

- **Authenticate User Name。**如果需要进行验证，您可以在访问日志中列出经过验证的用户名。
- **System Date。**客户机请求的日期和时间。
- **Full Request。**客户机所做的完整请求。
- **Status。**服务器返回给客户机的状态码。
- **Content Length。**发送至客户机的文档的内容长度（以字节计）。
- **HTTP Header, "referer"。**引用者用于指定客户机从中访问当前页面的页面。例如，如果用户正在查看文本搜索查询的结果，则引用者将是用户从中访问文本搜索引擎的页面。引用者允许服务器创建回溯链接的列表。
- **HTTP Header, "user-agent"。**用户代理信息包括客户机所用浏览器的类型、版本和客户机运行的操作系统，这些信息均来自于客户机向服务器发送的 HTTP 标头信息中的 User-agent 字段。
- **Method。**所用的 HTTP 请求方法（如 GET、PUT 或 POST）。
- **URI。**统一资源标识符。服务器上资源的位置。例如，对于 `http://www.a.com:8080/special/docs`，URI 为 `special/docs`。
- **Query String Of The URI。**URI 中问号之后的所有内容。例如，对于 `http://www.a.com:8080/special/docs?find_this`，URI 的查询字符串为 `find_this`。
- **Protocol。**使用的传输协议和版本。
- **Cache Finish Status。**此字段指定最新性检查是否已写入、刷新或返回高速缓存文件。
- **Remote Server Finish Status。**此字段指定向远程服务器发出的请求是已成功执行、已从客户机单击 Netscape Navigator 中的“停止”按钮中断，还是被错误条件异常中止。
- **Status Code From Server。**从服务器返回的状态码。
- **Route To Proxy (PROXY, SOCKS, DIRECT)。**检索资源时使用的路由。可通过以下几种方式检索文档：直接检索、通过代理服务器检索，或通过 SOCKS 服务器检索。
- **Transfer Time。**传送的时间长度（以秒或毫秒计）。
- **Header-length From Server Response。**来自服务器响应的标头长度。
- **Request Header Size From Proxy To Server。**从代理服务器到服务器的请求标头的大小。

- **Response Header Size Sent To Client**。发送到客户机的响应标头的大小。
- **Request Header Size Received From Client**。从客户机接收到的请求标头的大小。
- **Content-length From Proxy To Server Request**。由代理服务器发往服务器的文档的长度（以字节计）。
- **Content-length Received From Client**。来自客户机的文档的长度（以字节计）。
- **Content-length From Server Response**。来自服务器的文档的长度（以字节计）。
- **Unverified User From Client**。验证时为远程服务器指定的用户名。

○ 如果选择自定义格式，请在 "Custom Format" 字段中键入该格式。

9. 如果不想记录来自某些主机名或 IP 地址的客户机访问，请在 "host names" 和 "IP Addresses" 字段中键入相应的内容。对于服务器不应记录发起访问的主机，可键入这些主机的通配符模式。例如，`*.example.com` 不会记录域 example.com 中人员的访问。可以为主机名、IP 地址中的任一个或两者键入通配符模式。
10. 选择是否要在日志文件加入格式字符串。如果使用的是 Proxy Server 的日志分析程序，则应加入格式字符串。如果使用的是第三方分析程序，则可能不需要在日志文件中加入格式字符串。
11. 单击 "OK"。
12. 单击 "Restart Required"。将出现 "Apply Changes" 页面。
13. 单击 "Restart Proxy Server" 按钮以应用更改。

简易 Cookie 日志记录

Proxy Server 提供了一种使用 flexlog 功能记录特定 cookie 的简单方法。将 “`Req->headers.cookie.cookie_name`” 添加到配置文件 `obj.conf` 中用于初始化 `flex-log` 子系统的那一行。如果 cookie 变量存在于请求标头中，将记录 cookie 变量 `cookie_name` 的值；如果变量不存在，将记录 “-”。

设置错误日志记录选项

Proxy Server 允许配置要在服务器错误日志中记录的信息。

设置错误日志记录选项

1. 要从 Administration Server 中设置错误日志记录选项，请选择 "Preferences" 选项卡，然后单击 "Set Error Log Preferences" 链接。

   要从 Server Manager 中设置服务器实例的错误日志记录选项，请选择 "Server Status" 选项卡，然后单击 "Set Error Log Preferences" 链接。

2. 在 "Error Log File Name" 字段中指定存储来自服务器的消息的文件。
3. 在 "Log Level" 下拉式列表中，指定应记录在错误日志中的信息量。可用选项如下：
4. 如果要将标准输出重定向到错误日志，请选中 "Log Stdout" 复选框。
5. 如果要将标准错误输出重定向到错误日志，请选中 "Log Stderr" 复选框。
6. 选中 "Log To Console" 复选框，将日志消息重定向到控制台。
7. 如果要使用 UNIX syslog 服务或 Windows 的“事件日志”来产生和管理日志，请选中 "Use System Logging" 复选框。
8. 单击 "OK"。
9. 单击 "Restart Required"。将出现 "Apply Changes" 页面。
10. 单击 "Restart Proxy Server" 按钮以应用更改。

配置 LOG 元素

下表介绍了可在 `server.xml` 文件中配置的 LOG 元素属性：

表 9-2 LOG 属性

属性	默认值	描述
`file`	`errors`	指定存储来自服务器的消息的文件。
`loglevel`	`info`	控制由其他元素记录到错误日志中的消息的默认类型。允许的值如下所示（从高到低排列）： `finest`、`fine`、`fine`、`info`、`warning`、`failure`、`config`、`security` 和 `catastrophe`。

表 9-2 LOG 属性

属性	默认值	描述
logstdout	true	（可选）如果为 true，则将标准输出重定向到错误日志。合法值为 on、off、yes、no、1、0、true 和 false。
logstderr	true	（可选）如果为 true，则将标准错误输出重定向到错误日志。合法值为 on、off、yes、no、1、0、true 和 false。
logtoconsole	true	（可选，仅限 UNIX）如果为 true，则将日志消息重定向到控制台。
createconsole	false	（可选，仅限 Windows）如果为 true，则为标准错误输出创建一个 Windows 控制台。合法值为 on、off、yes、no、1、0、true 和 false。
usesyslog	false	（可选）如果为 true，则使用 UNIX syslog 服务或 Windows 的“事件日志”来产生和管理日志。合法值为 on、off、yes、no、1、0、true 和 false。

查看访问日志文件

您可以查看服务器的活动访问日志文件和已归档的访问日志文件。

要从 Administration Server 中查看 Administration Server 的访问日志，请选择 "Preferences" 选项卡，然后单击 "View Access Log" 链接。

要从 Server Manager 中查看服务器实例的访问日志，请选择 "Server Status" 选项卡，然后单击 "View Access Log" 链接。

以下是一个采用通用日志文件格式的访问日志示例（该格式在 "Log Preferences" 窗口中指定；有关更多信息，参见第 168 页的“设置访问日志首选项”）：

```
198.18.17.222 - - [20/May/2005:14:15:49 +0530] "GET http://www.example.com/
HTTP/1.1" 504 622
198.18.17.222 - abc [20/May/2005:14:16:09 +0530] "GET
http://www.test.com/report.zip HTTP/1.1" 504 630
```

表 9-3 对该访问日志样例中的最后一行进行了说明。

表 9-3 样例访问日志文件中最后一行的字段

访问日志字段	示例
客户机的主机名或 IP 地址	198.18.17.222 （在本例中，由于禁用了代理服务器的 DNS 查找设置，所以显现的是客户机的 IP 地址；如果启用了 DNS 查找，则出现的将是客户机的主机名。）
RFC 931 信息	-（RFC 931 标识未实现）
用户名	abc（客户机所输入的用于进行验证的用户名）
请求的日期 / 时间	20/May/2005:14:16:09 +0530
请求	GET
协议	HTTP/1.1
状态码	504
传送的字节数	630

查看错误日志文件

错误日志文件包含该文件创建以来服务器遇到的错误；还包含有关服务器的提示性信息（例如服务器的启动时间）。失败的用户验证也记录在此错误日志中。使用错误日志可以查找断开的 URL 路径或缺少的文件。

要从 Administration Server 中查看 Administration Server 的错误日志文件，请选择 "Preferences" 选项卡，然后单击 "View Error Log" 链接。

要从 Server Manager 中查看服务器实例的错误日志文件，请选择 "Server Status" 选项卡，然后单击 "View Error Log" 链接。

下面例举了错误日志中的三个条目。

```
20/May/2005:14:08:37] info ( 6141): CORE1116: Sun Java System Web Proxy
Server 4.0 B05/10/2005 01:26
20/May/2005:14:08:37] info ( 6142): CORE3274: successful server startup
20/May/2005:14:08:37] security (23246): for host 198.18.148.89 trying to GET
/, deny-service reports: denying service of /
```

使用日志分析程序

server_root/extras/log_anly 目录含有通过 Server Manager 用户界面运行的日志分析工具。此日志分析程序仅分析通用日志格式的文件。log_anly 目录下的 HTML 文档中介绍了此工具的参数。server-install/extras/flexanlg 目录含有用于灵活日志文件格式的命令行日志分析程序。但是，不管选择了何种日志文件格式，Server Manager 在默认情况下都会使用灵活日志文件报告工具。

使用日志分析程序可以生成有关默认服务器的统计数据，例如活动摘要、最常访问的 URL、一天中访问服务器的高峰时段等等。可以从 Proxy Server 或命令行运行日志分析程序。

在尝试运行 flexanlg 命令行实用程序之前必须设置库路径。各种平台的设置如下所示：

Solaris 和 Linux：

```
LD_LIBRARY_PATH=server_root/bin/proxy/lib:$LD_LIBRARY_PATH
```

AIX：

```
LIBPATH=server_root/bin/proxy/lib:$LIBPATH
```

HP-UX：

```
SHLIB_PATH=server_root/bin/proxy/lib:$SHLIB_PATH
```

Windows：

```
path=server_root\bin\proxy\bin;%path%
```

注 在运行日志分析程序之前，应将服务器日志归档。有关将服务器日志归档的更多信息，参见第 166 页的“归档日志文件”。

作为设置库路径的替代方法，还可以先转到 server_root/proxy-server*id* 目录，然后在命令提示符处键入 **./start -shell**。

如果使用扩展或扩展 2 日志记录格式，则除了指定要报告的信息之外，日志分析程序还会在输出文件内生成多个报告。以下各节将对这些报告进行介绍。

传送时间分配报告

传送时间分配报告显示代理服务器传送请求所花费的时间。此报告显示的信息按服务时间和完成百分比进行分类。下面是传送时间分配报告的一个样例。

By service time category:

```
< 1 sec [644%] ....................................

< 2 sec [33.3%] ...................

< 3 sec [ 2.7%] .

< 4 sec [ 1.7%] .

< 5 sec [ 0.6%]

< 6 sec [ 0.4%]

< 7 sec [ 0.2%]

< 8 sec [ 0.0%]

< 9 sec [ 0.0%]
```

By percentage finished:

```
< 1 sec [64.4%] ....................................

< 2 sec [97.7%] ..................................

< 3 sec [100.4%].........................................
```

状态码报告

状态码报告显示代理服务器从远程服务器接收和向客户机发送的状态码及其数目。状态码报告还会对上述所有状态码进行解释说明。下面是状态码报告的一个样例。

Code	-From remote-	-To client-	-Explanation-
200	338 [70.7%]	352 [73.6%]	OK
302	33 [6.9%]	36 [7.5%]	Redirect
304	90 [18.8%]	99 [20.7%]	Not modified
404	3 [0.6%]	3 [0.6%]	Not found
407		5 [1.0%]	Proxy authorization required
500		2 [0.4%]	Internal server error
504		6 [1.3%]	Gateway timeout

数据流报告

数据流报告显示从客户机到代理服务器、从代理服务器到客户机、从代理服务器到远程服务器以及从远程服务器到代理服务器的数据流（传送的字节数）。对于上述每种情况，该报告均会显示以标头和内容形式传送的数据量。数据流报告还会显示从高速缓存到客户机的数据流。下面是数据流报告的一个样例。

	Headers	**Content**	**Total**
- Client -> Proxy.....	0 MB	0 MB	0 MB
- Proxy -> Client.....	0 MB	2 MB	3 MB
- Proxy -> Remote.....	0 MB	0 MB	0 MB
- Remote -> Proxy.....	0 MB	2 MB	2 MB
Approx:			
- Cache -> Client.....	0 MB	0 MB	0 MB

请求和连接报告

请求和连接报告显示代理服务器从客户机接收的请求数、代理服务器与远程服务器进行的连接数（初始检索、最新性检查和刷新）以及代理服务器通过使用高速缓存文档避免的远程连接数。下面是请求和连接报告的一个样例。

```
- Total requests.............. 478
- Remote connections......... 439
- Avoided remote connects.... 39 [ 8.2%]
```

高速缓存性能报告

高速缓存性能报告显示客户机高速缓存、代理服务器高速缓存以及直接连接的性能。

Client Cache

注 当客户机对文档执行最新性检查时，如果远程服务器返回一条 304 消息，告知客户机文档并未修改，则客户机高速缓存即被命中。由客户机启动的最新性检查表明客户机自身在高速缓存中拥有文档的副本。

对于客户机的高速缓存，该报告将显示：

- **client and proxy cache hits**：一种客户机高速缓存命中情况，此时，代理服务器和客户机都具有所请求文档的副本，先通过查询远程服务器针对代理服务器的副本进行最新性检查，然后针对代理服务器的副本对客户机的请求进行评判。高速缓存性能报告将显示代理服务器所服务的此类请求数，以及它为这些请求服务所花费的平均时间。
- **proxy shortcut no-check**：一种客户机高速缓存命中情况，此时，代理服务器和客户机都具有所请求文档的副本，代理服务器（在未与远程服务器进行核查的情况下）告知客户机：客户机高速缓存中的文档是最新的。高速缓存性能报告将显示代理服务器所服务的此类请求数，以及它为这些请求服务所花费的平均时间。
- **client cache hits only**：一种客户机高速缓存命中情况，此时，只有客户机具有所请求文档的高速缓存副本。在此类请求中，代理服务器会直接为客户机的 If-modified-since GET 标头建立通信隧道。高速缓存性能报告将显示代理服务器所服务的此类请求数，以及它为这些请求服务所花费的平均时间。
- **total client cache hits**：客户机高速缓存总命中次数以及代理服务器为这些请求服务所花费的平均时间。

Proxy Cache

当客户机从代理服务器那里请求文档时，如果代理服务器的高速缓存中已有该文档，则代理高速缓存即被命中。对于代理服务器的高速缓存命中，该报告将显示：

- **proxy cache hits with check**：一种代理高速缓存命中情况，此时，代理服务器通过查询远程服务器对文档进行最新性检查。高速缓存性能报告将显示代理服务器所服务的此类请求数，以及它为这些请求服务所花费的平均时间。
- **proxy cache hits without check**：一种代理高速缓存命中情况，此时，代理服务器不查询远程服务器以对文档进行最新性检查。高速缓存性能报告将显示代理服务器所服务的此类请求数，以及它为这些请求服务所花费的平均时间。
- **pure proxy cache hits**：一种代理高速缓存命中情况，此时，客户机不具有所请求文档的高速缓存副本。高速缓存性能报告将显示代理服务器所服务的此类请求数，以及它为这些请求服务所花费的平均时间。

Proxy Cache Hits Combined

对于合并的代理高速缓存命中，该报告将显示：

- **total proxy cache hits**：命中代理服务器高速缓存的总次数以及代理服务器为这些请求服务所花费的平均时间。

Direct Transactions

直接事务是指没有命中高速缓存而直接从远程服务器到代理服务器再到客户机的事务。对于直接事务，该报告将显示：

- **retrieved documents**：直接从远程服务器检索的文档。高速缓存性能报告将显示代理服务器所服务的此类请求数、它为这些请求服务所花费的平均时间以及占事务总数的百分比。
- **other transactions**：以异于 200 或 304 的状态码返回的事务。高速缓存性能报告将显示代理服务器所服务的此类请求数，以及它为这些请求服务所花费的平均时间。
- **total direct traffic**：直接从客户机到远程服务器的请求（包括失败请求和成功检索的文档）。高速缓存性能报告将显示代理服务器所服务的此类请求数、它为这些请求服务所花费的平均时间以及占事务总数的百分比。

下面是高速缓存性能报告的一个样例。

```
CLIENT CACHE:
- Client & proxy cache hits... 86 reqs [18.0%] 0.21 sec/req
- Proxy shortcut no-check........ 13 reqs [ 2.7%] 0.00 sec/req
- Client cache hits only.....
- TOTAL client cache hits.......... 99 reqs [20.7%] 0.18 sec/req
PROXY CACHE:
- Proxy cache hits w/check........ 4 reqs [ 0.8%] 0.50 sec/req
- Proxy cache hits w/o check.. 10 reqs [ 2.1%] 0.00 sec/req
- Pure proxy cache hits...... 14 reqs [ 2.9%] 0.14 sec/req
PROXY CACHE HITS COMBINED:
- TOTAL proxy cache hits....... 113 reqs [23.6%] 0.18 sec/req
DIRECT TRANSACTIONS:
- Retrieved documents..313 reqs [65.5%]  0.90 sec/req 2 MB
- Other transactions.. 52 reqs [10.9%] 7.79 sec/req
- TOTAL direct traffic..365 reqs [76.4%] 1.88 sec/req 2 MB
```

传送时间报告

传送时间报告显示有关代理服务器处理事务所花时间的信息。此报告会显示以下各类值：

average transaction time：记录的所有传送时间的平均值。

average transfer time without caching：并非从高速缓存返回的事务（来自远程服务器的 200 响应）的平均传送时间。

average with caching, without errors：所有无错误事务（2xx 和 3xx 状态码）的平均传送时间。

average transfer time improvement：平均事务时间减去采用高速缓存且未出错情况下的平均传送时间。

下面是传送时间报告的一个样例。

```
- Average transaction time... 1.48 sec/req
- Ave xfer time w/o caching.. 0.90 sec/req
- Ave w/caching, w/o errors.. 0.71 sec/req
- Ave xfer time improvement.. 0.19 sec/req
```

每小时活动报告

对于所分析的每一个小时，每小时活动报告将显示：

- 平均负载值
- 不与远程服务器进行最新性检查时的高速缓存命中次数
- 当通过与远程服务器进行最新性检查证明文档是最新的并且在客户机高速缓存中时，命中代理服务器高速缓存的次数
- 当通过与远程服务器进行最新性检查证明文档是最新的并且**不**在客户机高速缓存中时，命中代理服务器高速缓存的次数
- 当与远程服务器进行的最新性检查导致部分文档更新时，命中代理服务器高速缓存的次数
- 当与远程服务器进行的最新性检查以 200 状态码返回所请求文档的一个新副本时，命中代理服务器高速缓存的次数

发生如下情况的请求数，即没有命中代理服务器的高速缓存而直接从远程服务器检索文档

从 Server Manager 运行日志分析程序

1. 访问 Server Manager，然后单击 "Server Status" 选项卡。
2. 单击 "Generate Report" 链接。将显示 "Generate Report" 页面。
3. 键入服务器的名称；此名称将出现在所生成的报告中。
4. 选择报告将以 HTML 格式还是以 ASCII 格式显示。
5. 选择所要分析的日志文件。
6. 如果要将结果保存在文件中，请在 "Output File" 字段键入输出文件名。如果将该字段留为空白，报告结果将打印至屏幕。对于大型日志文件，应将结果保存到文件中，因为打印输出到屏幕可能需要很长时间。

7. 选择是否为某些服务器统计信息产生合计。可以产生以下合计：
   - **Total Hits**。自启用访问日志记录以来服务器收到的总命中次数。
   - **304 (Not Modified) Status Codes**。使用所请求文档的本地副本的次数，而不是服务器返回相应页面的次数。
   - **302 (Redirects) Status Codes**。服务器因原始 URL 转移而重定向到新 URL 的次数。
   - **404 (Not Found) Status Codes**。服务器找不到所请求文档或服务器因客户机不是授权用户而未提供该文档的次数。
   - **500 (Server Error) Status Codes**。发生服务器相关错误的次数。
   - **Total Unique URLs**。自启用访问日志记录以来所访问的唯一 URL 数目。
   - **Total Unique Hosts**。自启用访问日志记录以来曾访问过服务器的唯一主机数目。
   - **Total Kilobytes Transferred**。自启用访问日志记录以来服务器所传送的千字节数。
8. 选择是否生成常规统计信息。如果选择生成统计信息，请选择以下选项：
9. **Find Top *Number* Seconds Of Log**。基于最近几秒钟内的信息生成统计信息。
10. **Find Top *Number* Minutes Of Log**。基于最近几分钟内的信息生成统计信息。
11. **Find Top *Number* Hours Of Log**。基于最近几小时内的信息生成统计信息。
12. **Find *Number* Users (If Logged)**。基于此数量的用户的信息生成统计信息。
13. **Find Top *Number* Referers (If Logged)**。基于此数量的引用者的信息生成统计信息。
14. **Find Top *Number* User Agents (If Logged)**。基于有关用户代理的信息（例如，浏览器类型、浏览器版本和操作系统）生成统计信息。
15. **Find Top *Number* Miscellaneous Logged Items (If Logged)**。基于此数量的用户的信息生成统计信息。
16. 选择是否生成列表。如果选择了生成列表，请从以下列表中指定要生成列表的项。
    - **URLs Accessed**。显示访问过的 URL。
      - ***Number* Most Commonly Accessed URL**。显示最常访问的 URL 或者访问次数超过指定次数的 URL。
      - **URLs That Were Accessed More Than *Number* Times**。显示访问次数超过指定次数的 URL。

- **Hosts Accessing Your Server**。显示访问过 Proxy Server 的主机。
  - ***Number* Hosts Most Often Accessing Your Server**。显示最常访问服务器的主机或者访问服务器的次数超过指定次数的主机。
  - **Hosts That Accessed Your Server More Than *Number* Times**。显示访问服务器的次数超过指定次数的主机。

17. 指定要以何顺序查看结果。按照各部分要在报告中出现的顺序，为以下各项赋予从 1 至 3 的优先级。如果选择不生成其中任何一项优先级，该部分将自动被忽略。包括以下选项：
    - Find Totals
    - General Statistics
    - Make Lists
18. 单击 "OK"。报告将显示在新窗口中。

从命令行运行日志分析程序

要从命令行分析访问日志文件，请运行 `flexanlg` 工具，它位于 `server-install/extras/flexanlg` 目录。

要运行 `flexanlg`，请在命令提示符处键入以下命令和选项：

```
./flexanlg [-n name] [-x] [-r] [-p order] [-i file]* [ -m metafile ]*
[-o file][-c opts] [-t opts] [-l opts]
```

标有 * 的选项可以重复。

下面将介绍语法。（键入 ./flexanlg -h，可以获得相应的英文联机信息。）：

```
-P: 代理日志格式                                          默认值：no
-n servername: 服务器的名称
-x: 以 HTML 格式输出                                          默认值：no
-r: 将 IP 地址解析为主机名                        默认值：no
-p [c,t,l]: 输出顺序（计数、时间统计和列表）   默认值：ctl
-i filename: 输入日志文件                              默认值：none
-o filename: 输出日志文件                                  默认值：stdout
-m filename: 元文件                                        默认值：none
-c [h,n,r,f,e,u,o,k,c,z]: 对这些项进行计数 -        默认值：hnreuokc
    h: 总命中次数
    n: "304 Not Modified" 状态码（使用本地副本）
    r: "302 Found" 状态码（重定向）
    f: "404 Not Found" 状态码（文档未找到）
    e: "500 Server Error" 状态码（配置不当）
    u: 唯一 URL 总数
    o: 唯一主机总数
    k: 总传送千字节数
    c: 高速缓存所保存的总千字节数
    z: 不对任何项进行计数。
-t [sx,mx,hx, xx,z]: 查找时间统计 -       默认值：s5m5h10u10a10r10x10
    s(number): 查找最近 (number) 秒的日志
    m(number): 查找最近 (number) 分钟的日志
    h(number): 查找最近 (number) 小时的日志
    u(number): 查找最上面 (number) 个用户的日志
    a(number): 查找最上面 (number) 个用户代理的日志
    r(number): 查找最上面 (number) 个引用者的日志
    x(number): 查找最上面 (number) 个杂项关键字
    z: 不查找任何时间统计。
-l [cx,hx]: 生成列表 -                                  默认值：c+3h5
    c(x,+x): 最常访问的 URL
           (x: 仅列出 x 个条目)
           (+x: 仅当访问过 x 次以上时列出)
    h(x,+x): 最常访问服务器的主机（或 IP 地址）
           (x: 仅列出 x 个条目)
           (+x: 仅当访问过 x 次以上时列出)
    z: 不生成任何列表。
```

查看事件 (Windows)

除了将错误记录到服务器错误日志之外，Proxy Server 还会将严重的系统错误记录到“事件查看器”中。“事件查看器”可用于监视系统中发生的事件。在打开错误日志之前，可以使用“事件查看器”查看因基础配置问题而引起的错误。

使用“事件查看器”

1. 从“开始”菜单中依次选择“程序”和“管理工具”。在“管理工具”程序组中选择“事件查看器”。
2. 从“日志”菜单中选择“应用程序”。

   应用程序日志将显示在“事件查看器”中。来自 Proxy Server 的错误带有一个源标签 `proxy-server`*id*。
3. 从“查看”菜单中选择“查找”，在日志中搜索这类标签之一。从“查看”菜单中选择“刷新”，查看更新后的日志条目。

   有关“事件查看器”的更多信息，参阅系统文档。

第 10 章

监视服务器

本章介绍监视服务器的方法，其中包括内置监视工具和简单网络管理协议 (SNMP)。

正如监视网络中的其他设备那样，您可以将 SNMP 与 Sun Java System 管理信息库 (MIB) 以及网络管理软件（如 HP OpenView）结合使用来实时监视服务器。

注 在 Windows 上，在安装 Proxy Server 4 之前，请确保系统上已安装了 Windows SNMP 组件。

可以使用统计特性或 SNMP 来实时查看服务器的状态。在 UNIX 或 Linux 上，如果计划使用 SNMP，必须为 Proxy Server 对其进行配置。本章提供了在 UNIX 或 Linux 上与 Proxy Server 一起使用 SNMP 所需的信息。

本章包括以下各节：

使用统计信息监视服务器

您可以使用统计特性来监视服务器的当前活动。统计信息显示了服务器处理的请求的数目以及这些请求的处理状况。如果交互式服务器监视器报告该服务器处理的请求过多，您可能需要调整服务器配置或系统的网络内核以容纳这些请求。默认情况下禁用统计信息，因为收集统计信息会增加 Proxy Server 的系统开销。一旦启用统计信息，服务器便会开始收集和保存统计信息。

启用统计信息后，您可以查看以下方面的统计信息：

- 连接
- DNS
- 保持活动
- 高速缓存
- 服务器请求

交互式服务器监视器会报告各种服务器统计信息的合计。有关这些统计信息的说明，参见联机帮助中的 "Monitor Current Activity" 页面。

处理 Proxy Server 统计信息

可使用一个称为 `stats-xml` 的内置函数来收集 Proxy Server 统计信息。必须启用此函数方可从 Server Manager 中查看统计信息，或使用 `perfdump` 函数生成报告。还可使用 `stats-xml` 函数来启用事件探查，它是通过使用自定义 NSAPI 函数监视统计信息所必需的。在服务器上启用统计信息和事件探查后，将会对 `obj.conf` 文件中的一个称为 `stats-init` 的服务器函数进行初始化，以开始统计信息的收集。

```
Init profiling="on" fn="stats-init"
```

还会创建一条 `NameTrans` 指令，它允许您从浏览器窗口中访问统计信息。

```
NameTrans fn="assign-name" name="stats-xml"
from="(/stats-xml|/stats-xml/.*)
```

启用统计信息时，最后还会添加一条 `Service` 指令，用以在选择了 `NameTrans` 指令时处理 `stats-xml` 函数。

```
<Object name="stats-xml">

Service fn="stats-xml"

</Object>
```

注 收集统计信息时将会更新 obj.conf 中的 Init 函数。因此，必须停止并启动服务器方可使这些更改生效。

可使用以下 URL 检索 stats-xml 输出：

http://*computer_name:proxyport*/stats-xml/proxystats.xml

此请求将返回一个含有 Proxy Server 统计信息的 XML 页面。一些浏览器允许在浏览器窗口中查看数据，而另外一些则要求将数据保存至外部文件，用外部查看器进行查看。若不能对所分析数据的不同视图解析统计信息，则此信息的用途将不十分明显。可借助第三方工具来完成此处理过程。若没有解析工具，则最好是通过 Server Manager 或 perfdump SAF 来观察 stats-xml 输出。

限制对 stats-xml 输出的访问

如果要对可以通过浏览器查看服务器 stats-xml 统计信息的用户进行限制，应为 /stats-xml URI 创建一个 ACL。

还必须在 obj.conf 文件的 stats-xml 对象定义中引用该 ACL 文件。例如，如果为 /stats-xml URI 创建了一个命名 ACL，则需要在该对象定义的 PathCheck 语句中引用该 ACL 文件，如下所示：

```
<Object name="stats-xml">

PathCheck fn="check-acl" acl="stats.acl"

Service fn="stats-xml"

</Object>
```

启用统计信息

必须先在 Proxy Server 上激活统计信息，才能对性能进行监视。可以通过 Server Manager 或通过编辑 obj.conf 和 magnus.conf 文件来完成此操作。为监视和调节创建自动化工具或编写自定义程序的用户可能更愿意直接处理 stats-xml。

注意 启用统计信息 / 事件探查后，服务器的所有用户都可以使用统计信息。

从 Server Manager 中启用统计信息

1. 访问 Server Manager，然后单击 "Server Status" 选项卡。
2. 单击 "Monitor Current Activity" 链接。将显示 "Monitor Current Activity" 页面。
3. 对于 "Activate Statistics/Profiling?" 元素选择 "Yes" 选项以启用数据信息。
4. 单击 "OK"。

5. 单击 "Restart Required"。将出现 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

使用 `stats-xml` 启用数据信息

1. 在 obj.conf 中的默认对象下添加下面一行：

```
NameTrans fn="assign-name" name="stats-xml"
from="(/stats-xml|/stats-xml/.*)"
```

2. 向 `obj.conf` 添加以下 Service 函数：

```
<Object name="stats-xml">

Service fn="stats-xml"

</Object>
```

3. 将 `stats-init` SAF 添加至 `magnus.conf`。

以下是 `obj.conf` 中的 `stats-init` 的一个示例：

```
Init profiling="on" fn="stats-init" update-interval="5"
```

上述示例表明您还可以指定以下各项：

- **update-interval。**两次更新统计信息的间隔周期（以秒计）。设置越高（频率越低），性能越好。最小值为 1；默认值为 5。
- **profiling。**激活 NSAPI 性能事件探查。默认值为 "no"，它只能略微提高服务器性能。然而，如果通过用户界面激活统计信息，则默认情况下会开启事件探查。

使用统计信息

启用统计信息后，即可获得有关服务器实例运行状况的各种信息。统计信息被划分成多个功能区。

访问统计信息

1. 访问 Server Manager，然后单击 "Server Status" 选项卡。
2. 单击 "Monitor Current Activity" 链接。
3. 从 "Select Refresh Interval" 下拉式列表中选择刷新间隔。

   刷新间隔是两次更新所显示统计信息间隔的秒数。
4. 从 "Select Statistics To Be Displayed" 下拉式列表中选择要显示的统计信息种类。有关统计信息类型的更多信息，参见第 191 页的“在 Server Manager 中显示统计信息”。

5. 单击 "Submit"。

   如果服务器实例正在运行且已启用了统计信息 / 事件探查，您会看到一个显示有所选统计信息种类的页面。该页面每隔 5-15 秒更新一次，具体依所选择的刷新间隔而定。

6. 从下拉式列表中选择进程 ID。

   可通过 Server Manager 查看当前活动，但是这些类别并不完全与服务器的调节相关。建议使用 Perfdump 统计信息来调节服务器。

在 Server Manager 中显示统计信息

本节介绍如何才能在 Server Manager 中查看 `proxystats.xml` 数据子集。

可以采用合计图、最大值图、峰数图和条形图来查看与 Proxy Server 连接、DNS 处理、保持活动值、高速缓存和服务器请求有关的信息。

下节将介绍可为上述各项获得的信息类型。

连接统计信息

可从 Server Manager 获得以下连接统计信息：

- 连接总数
- 最大已排队连接数
- 已排队连接的峰数
- 当前已排队连接数
- 进程数

DNS 统计信息

可从 Server Manager 获得以下 DNS 统计信息：

- 最大 DNS 高速缓存条目数
- 进程数
- DNS 高速缓存命中次数（还会以条形图形式显示）
- DNS 高速缓存未命中次数（还会以条形图形式显示）

保持活动统计信息

可从 Server Manager 获得以下保持活动统计信息：

- 最大保持活动连接数
- 保持活动超时值。
- 进程数
- 保持活动命中次数（还会以条形图形式显示）
- 保持活动刷新次数（还会以条形图形式显示）
- 保持活动拒绝次数（还会以条形图形式显示）
- 保持活动超时次数（还会以条形图形式显示）

高速缓存统计信息

可从 Server Manager 获得以下文件高速缓存统计信息：

- 高速缓存最长时效（以秒计）
- 堆高速缓存最大大小
- 内存高速缓存映射最大大小
- 进程数
- 高速缓存命中次数（还会以条形图形式显示）
- 高速缓存未命中次数（还会以条形图形式显示）
- 信息高速缓存命中次数（还会以条形图形式显示）
- 信息高速缓存未命中次数（还会以条形图形式显示）
- 内容高速缓存命中次数（还会以条形图形式显示）
- 内容高速缓存未命中次数（还会以条形图形式显示）

服务器请求统计信息

可从 Server Manager 获得以下服务器统计信息：

- 总请求数
- 接收字节数
- 发送字节数
- 进程数
- 按 HTTP 服务器代码细分的请求数（还会以条形图形式显示）。例如，HTTP 服务器代码 200 表示请求已完成。

使用 perfdump 实用程序监视当前活动

prfdump 实用程序是 Proxy Server 中内置的一个服务器应用程序函数 (SAF)，用于从 Proxy Server 内部统计信息中收集各种性能数据片段并以 ASCII 文本形式进行显示。与通过 Server Manager 可获得的统计信息种类相比，利用 perfdump 应用程序可监视更多种统计信息。

利用 perfdump 可将统计信息结成一体。不再是监视单个进程，而是将统计信息乘以进程数，这样可以从总体上更加准确地了解服务器的情况。

启用 perfdump 实用程序

只有在启用了 `stats-xml` 函数之后才能启用 perfdump SAF，而且只能通过直接编辑 `obj.conf` 文件来启用它。

启用 perfdump SAF：

1. 在 `obj.conf` 文件的默认对象后面添加以下对象：

   ```
   <Object name="perf">

   Service fn="service-dump"

   </Object>
   ```

2. 向默认对象添加以下内容：

   ```
   NameTrans fn=assign-name from="/.perf" name="perf"
   ```

3. 重新启动服务器软件。

4. 通过输入以下 URL 访问 perfdump：

`http://`*computer_name:proxyport*`/.perf`

可请求 perfdump 统计信息，并指定浏览器的自动刷新频率（以秒计）。以下示例的刷新设置为每隔 5 秒一次：

`http://`*computer_name:proxyport*`/.perf?refresh=5`

perfdump 输出样例

下面为 perfdump 输出样例：

```
proxyd pid: 6751

Sun Java System Web Proxy Server 4.0 B05/02/2005 15:32 (SunOS DOMESTIC)

Server started Thu May 19 13:15:14 2005
Process 6751 started Thu May 19 13:15:14 2005

ConnectionQueue:
----------------------------------------
Current/Peak/Limit Queue Length            0/1/4096
Total Connections Queued                   1
Average Queue Length (1, 5, 15 minutes)    0.00, 0.00, 0.00
Average Queueing Delay                     0.09 milliseconds

ListenSocket ls1:
------------------------
Address                   http://0.0.0.0:8081
Acceptor Threads          1

KeepAliveInfo:
--------------------
KeepAliveCount        0/256
KeepAliveHits         0
KeepAliveFlushes      0
KeepAliveRefusals     0
KeepAliveTimeouts     0
KeepAliveTimeout      30 seconds

SessionCreationInfo:
------------------------
Active Sessions           1
Keep-Alive Sessions       0
Total Sessions Created    48/128

CacheInfo:
------------------
enabled             yes
CacheEntries        0/1024
Hit Ratio           0/0 (  0.00%)
Maximum Age         0

Native pools:
----------------------------
NativePool:
```

```
Idle/Peak/Limit               1/1/128
Work Queue Length/Peak/Limit  0/0/0

Server DNS cache disabled

Async DNS disabled

Performance Counters:
------------------------------------------------
                           Average         Total      Percent

Total number of requests:                      1
Request processing time:    0.2559        0.2559

default-bucket (Default bucket)
Number of Requests:                            1    (100.00%)
Number of Invocations:                         7    (100.00%)
Latency:                    0.2483        0.2483    ( 97.04%)
Function Processing Time:   0.0076        0.0076    (  2.96%)
Total Response Time:        0.2559        0.2559    (100.00%)

Sessions:
----------------------------
Process  Status     Function

6751     response   service-dump
```

有关这些参数的更多信息，参见《Sun ONE Web Server 6.1 Performance Tuning, Sizing, and Scaling Guide》第二章中的 “Using Statistics to Tune Your Server”，网址为：

http://docs.sun.com/source/817-6249/index.html

限制对 perfdump 输出的访问

如果要对可以通过浏览器查看服务器 perfdump 统计信息的用户进行限制，需要为 /.perf URI 创建一个 ACL。

还必须在 obj.conf 文件的 perf 对象定义中引用该 ACL 文件。例如，如果为 /.perf URI 创建了一个命名 ACL，则需要在该对象定义的 PathCheck 语句中引用该 ACL 文件，如下所示：

```
<Object name="perf">

PathCheck fn="check-acl" acl="perf.acl"

Service fn="service-dump"

</Object>
```

使用性能存储桶

性能存储桶允许您定义存储桶并将其链接到各不相同的服务器函数。每次调用其中某个函数时，服务器都会收集统计数据并将其添加到存储桶中。例如，send-cgi 和 NSServletService 函数分别用于为 CGI 请求和 Java servlet 请求提供服务。可以定义两个存储桶来为 CGI 请求和 servlet 请求维护单独的计数器，也可创建一个存储桶来对两种类型的动态内容请求进行计数。收集此信息的开销很少，对服务器性能的影响通常可以忽略不计。之后，可以使用 perfdump 实用程序来访问此信息。存储桶中存储着以下信息：

- **Name of the bucket。**此名称用于将存储桶与函数相关联。
- **Description。**对存储桶所关联函数的描述。
- **Number of requests for this function。**致使此函数被调用的总请求数。
- **Number of times the function was invoked。**此数目可能与函数的请求数不一致，因为对于单个请求，有些函数可能会执行一次以上。
- **Function latency or the dispatch time。**服务器调用函数所花费的时间。
- **Function time。**花在函数本身的时间。

default-bucket 由服务器预定义。它将为不与任何用户定义存储桶关联的函数记录统计信息。

配置

必须为 magnus.conf 和 obj.conf 文件中的性能存储桶指定所有配置信息。只有默认存储桶才会自动启用。

首先，必须按第 193 页的“使用 perfdump 实用程序监视当前活动”中所述启用性能测量。

以下示例展示了如何在 magnus.conf 中定义新的存储桶：

```
Init fn="define-perf-bucket" name="acl-bucket" description="ACL bucket"

Init fn="define-perf-bucket" name="file-bucket" description="Non-cached
responses"

Init fn="define-perf-bucket" name="cgi-bucket" description="CGI Stats"
```

上面的示例会创建三个存储桶：acl-bucket、file-bucket 和 cgi-bucket。要使这些存储桶与函数相关联，请向想要测量性能的 obj.conf 函数添加 bucket=*bucket-name*。

示例

```
PathCheck fn="check-acl" acl="default" bucket="acl-bucket"

...

Service method="(GET|HEAD|POST)" type="*~magnus-internal/*"
fn="send-file" bucket="file-bucket"

...

<Object name="cgi">

ObjectType fn="force-type" type="magnus-internal/cgi"

Service fn="send-cgi" bucket="cgi-bucket"

</Object>
```

性能报告

可以使用 perfdump 实用程序来访问存储桶中的服务器统计信息。性能存储桶信息位于 perfdump 所返回报告的最后一部分。

该报告含有以下信息：

- Average、Total 和 Percent 列给出了所请求的每一个统计数据。
- Request Processing Time 是服务器处理迄今已收到的所有请求所需的总时间。
- Number of Requests 是函数的总请求数。
- Number of Invocations 是函数的总调用次数。此数目与请求数的不同之处在于：处理一个请求时可能会多次调用某个函数。此行的百分比列是参照所有存储桶的总调用次数计算得出的。
- Latency 是 Proxy Server 为调用函数做准备所花费的时间（以秒计）。
- Function Processing Time 是 Proxy Server 花在函数内部的时间（以秒计）。Function Processing Time 和 Total Response Time 的百分比是比照总的 Request Processing Time 计算得出的。
- Total Response Time 为 Function Processing Time 与 Latency 之和（以秒计）。

以下是通过 perfdump 可以获得的性能存储桶信息的一个示例：

```
Performance Counters:
------------------------------------------------
                           Average         Total      Percent

Total number of requests:                      1
Request processing time:    0.2559        0.2559

default-bucket (Default bucket)
Number of Requests:                            1    (100.00%)
Number of Invocations:                         7    (100.00%)
Latency:                    0.2483        0.2483    ( 97.04%)
Function Processing Time:   0.0076        0.0076    (  2.96%)
Total Response Time:        0.2559        0.2559    (100.00%)
```

SNMP 基本原理

SNMP 是用于交换有关网络活动的数据的协议。利用 SNMP，可以在被管理的设备和网络管理站 (NMS) 之间传输数据。被管理的设备即运行 SNMP 的任何设备：主机、路由器、代理服务器以及网络上的其他服务器。NMS 是用于对该网络进行远程管理的系统。NMS 软件通常提供图形来显示收集的数据，或使用这些数据确保服务器在特定的容限内运行。

NMS 通常是安装有一个或多个网络管理应用程序的功能强大的工作站。网络管理应用程序（例如 HP OpenView）以图形方式显示有关被管理设备（例如 Web 服务器）的信息。例如，它可能显示您的企业中服务器的打开或关闭情况，或者收到的错误消息的数量和类型。与代理服务器一起使用 SNMP 时，将通过使用两种类型的代理（子代理和主代理）在 NMS 与服务器之间传送此信息。

子代理收集有关服务器的信息，并将该信息传递给服务器的主代理。每个服务器（Administration Server 除外）均有一个子代理。

注 对 SNMP 配置进行任何更改后，必须单击 "Apply Required"，然后重新启动 SNMP 子代理。

主代理与 NMS 进行通信。主代理随 Administration Server 一起安装。

您可以在一台主机上安装多个子代理，但是只能安装一个主代理。例如，如果在同一台主机上安装了 Directory Server、Proxy Server 和 Messaging Server，则每个服务器的子代理都将与同一个主代理进行通信。

管理信息库

Proxy Server 存储着与网络管理有关的变量。主代理可以访问的变量称为被管理对象。这些对象在称为管理信息库 (MIB) 的树状结构中定义。通过 MIB 可对 Proxy Server 网络配置、状态和统计信息进行访问。使用 SNMP 可从 NMS 中查看此信息。MIB 树的顶层表明 Internet 对象标识符具有四个子树：directory (1)、mgmt (2)、experimental (3) 和 private (4)。private (4) 子树包含 enterprises (1) 节点。enterprises (1) 节点中的每个子树都被分配给一个单独的企业，企业是注册有自己特定 MIB 扩展的组织。然后，企业可以在其子树下创建特定产品的子树。由企业创建的 MIB 位于 enterprises (1) 节点下。Sun Java System 服务器 MIB 也位于 enterprises (1) 节点下。每个 Sun Java System 服务器子代理都提供了一个用于 SNMP 通信的 MIB。服务器通过发送包含这些变量的消息或陷阱将重要事件报告给 NMS。NMS 还可以查询服务器的 MIB 来获取数据，或是以远程方式更改 MIB 中的变量。每个 Sun Java System 服务器均有各自的 MIB。所有 Sun Java System 服务器 MIB 都位于：

```
server_root/plugins/snmp
```

Proxy Server 的 MIB 是一个称为 proxyserv40.mib 的文件。此 MIB 包含与 Proxy Server 的网络管理有关的各种变量的定义。可以使用 Proxy Server MIB 来查看有关 Proxy Server 的管理信息，以及实时监视服务器。

设置 SNMP

一般而言，要使用 SNMP，必须在系统上安装并运行一个主代理和至少一个子代理。要启用子代理，需要先安装主代理。

设置 SNMP 的过程根据不同的系统而不同。

开始前，应当验证两件事情：

- 您的系统是否已经运行了 SNMP 代理（操作系统的本机代理）。
- 如果是，该本机 SNMP 代理是否支持 SMUX 通信？（如果使用的是 AIX 平台，则您的系统支持 SMUX。）

有关如何验证这些信息的信息，参见您的系统文档。

注 在更改了 Administration Server 中的 SNMP 设置、安装了新的服务器或删除了现有服务器后，您必须执行以下步骤：

- (Windows) 重新启动 Windows SNMP 服务或重新引导系统。
- (UNIX) 使用 Administration Server 重新启动 SNMP 主代理。

表 1 启用 SNMP 主代理和子代理的过程概述。

如果服务器满足以下条件	请执行以下过程。这些过程将在后续各节中详细讨论。
• 当前没有运行本机代理	1. 启动主代理。 2. 为系统上安装的每个服务器启用子代理。
• 本机代理当前正在运行 • 无 SMUX • 不需要继续使用本机代理	1. 为 Administration Server 安装主代理时，停止本机代理。 2. 启动主代理。 3. 为系统上安装的每个服务器启用子代理。
• 本机代理当前正在运行 • 无 SMUX • 需要继续使用本机代理	1. 安装代理服务器 SNMP 代理。 2. 启动主代理。 3. 启动代理服务器 SNMP 代理。 4. 使用主代理端口号以外的其他端口号重新启动本机代理。 5. 为系统上安装的每个服务器启用子代理。
• 本机代理当前正在运行 • 支持 SMUX	1. 重新配置 SNMP 本机代理。 2. 为系统上安装的每个服务器启用子代理。

使用代理服务器 SNMP 代理 (UNIX)

如果已有一个本机代理正在运行，并且想要继续与 Proxy Server 主代理一起同时使用它，则需要使用代理服务器 SNMP 代理。在开始之前，请确保停止本机主代理。（有关详细信息，参见您的系统文档。）

注 要使用代理服务器代理，需要先安装后启动。还必须使用 Proxy Server 主代理运行端口号以外的端口号，重新启动本机 SNMP 主代理。

本节包括以下主题：

- 安装代理服务器 SNMP 代理
- 启动代理服务器 SNMP 代理
- 重新启动本机 SNMP 守护进程

安装代理服务器 SNMP 代理

如果某个 SNMP 代理正在系统上运行，并且您希望继续使用本机 SNMP 守护进程，请执行以下各节中的步骤：

1. 安装 SNMP 主代理。参见第 203 页的“安装 SNMP 主代理”。
2. 安装并启动代理服务器 SNMP 代理，然后重新启动本机 SNMP 守护进程。参见第 200 页的“使用代理服务器 SNMP 代理 (UNIX)”。
3. 启动 SNMP 主代理。参见第 204 页的“启用和启动 SNMP 主代理”。
4. 启用子代理。参见第 208 页的“启用子代理”。

要安装 SNMP 代理服务器代理，请编辑 CONFIG 文件（可为此文件指定另一不同名称），使其包含 SNMP 守护进程将要侦听的端口。该文件位于服务器根目录下的 `plugins/snmp/sagt` 中。其中还需要包括代理服务器 SNMP 代理将要转发的 MIB 树和陷阱。

下面是一个 CONFIG 文件示例：

```
AGENT AT PORT 1161 WITH COMMUNITY public
SUBTREES        1.3.6.1.2.1.1,
                   1.3.6.1.2.1.2,
                   1.3.6.1.2.1.3,
                   1.3.6.1.2.1.4,
                   1.3.6.1.2.1.5,
                   1.3.6.1.2.1.6,
                   1.3.6.1.2.1.7,
                   1.3.6.1.2.1.8
FORWARD ALL TRAPS;
```

启动代理服务器 SNMP 代理

要启动代理服务器 SNMP 代理，请在命令提示符处输入：

```
# sagt -c CONFIG&
```

重新启动本机 SNMP 守护进程

启动代理服务器 SNMP 代理后，需要在 CONFIG 文件中指定的端口重新启动本机 SNMP 守护进程。要启动本机 SNMP 守护进程，请在命令提示符处输入：

```
# snmpd -P port_number
```

其中 *port_number* 是在 CONFIG 文件中指定的端口号。例如，在 Solaris 平台上，若要使用上述 CONFIG 文件示例中的端口，则应输入：

```
# snmpd -P 1161
```

重新配置 SNMP 本机代理

如果 SNMP 守护进程运行在 AIX 上，则它支持 SMUX。因此，无需安装主代理。但是，您必须更改 AIX SNMP 守护进程配置。

AIX 使用多个配置文件来屏蔽其通信。需要更改 snmpd.conf（其中一个配置文件）以使 SNMP 守护进程接受从 SMUX 子代理收到的消息。有关更多信息，参见 snmpd.conf 的联机手册页。您需要添加一行以定义每个子代理。

例如，您可以将此行添加到 snmpd.conf 中：

```
smux 1.3.6.1.4.1.1.1450.1 "" IP_address net_mask
```

IP_address 是运行子代理的主机的 IP 地址，*net_mask* 是该主机的网络掩码。

注 请勿使用回送地址 127.0.0.1 ；而应使用实际的 IP 地址。

安装 SNMP 主代理

要配置 SNMP 主代理，您必须以超级用户身份安装 Administration Server 实例。但是，即使是非超级用户，也可以通过配置 SNMP 子代理以便与主代理一起工作，从而在 Web 服务器实例上完成基本 SNMP 任务（例如 MIB 浏览）。

安装主 SNMP 代理

1. 以超级用户身份登录。
2. 检查端口 161 上是否运行有 SNMP 守护进程 (`snmpd`)。

   如果没有运行 SNMP 守护进程，请转到步骤 4。

   如果运行有 SNMP 守护进程，请确保知道如何重新启动它以及它支持哪些 MIB 树。
3. 如果运行有 SNMP 守护进程，请中止其进程。
4. 在 Administration Server 中，从 "Global Settings" 选项卡中选择 "Set SNMP Master Agent Trap" 页面。
5. 键入正在运行网络管理软件的系统的名称。
6. 键入网络管理系统用来侦听陷阱的端口号。（常用的端口是 162。）有关陷阱的更多信息，参见第 208 页的“配置陷阱目标”。
7. 键入要在陷阱中使用的团体字符串。有关团体字符串的更多信息，参见第 207 页的“配置团体字符串”。
8. 单击 "OK"。
9. 在 Administration Server 中，从 "Global Settings" 选项卡中选择 "Set SNMP Master Agent Community" 页面。
10. 键入主代理的团体字符串。
11. 选择团体的操作。
12. 单击 "New"。

启用和启动 SNMP 主代理

主代理操作在名为 CONFIG 的代理配置文件中进行了定义。您可以使用 Server Manager 编辑 CONFIG 文件，也可以手动编辑该文件。要启用 SNMP 子代理，必须先安装 SNMP 主代理。

如果在重新启动主代理时出现类似于 “System Error: Could not bind to port” 的绑定错误，请使用 `ps -ef | grep snmp` 检查 magt 是否在运行。如果正在运行，请使用 `kill -9 pid` 命令结束该进程。然后，SNMP 的 CGI 将重新开始工作。

本节包括以下主题：

在其他端口上启动主代理

管理界面不会在 161 以外的端口上启动 SNMP 主代理。

手动在其他端口上启动主代理

1. 编辑 */server_root*/plugins/snmp/magt/CONFIG 以指定所需的端口。
2. 运行以下启动脚本：

   ```
   cd /server_root/proxy-admserv

   ./start -shell /server_root/plugins/snmp/magt/magt

   /server_root/plugins/snmp/magt/CONFIG

   /server_root/plugins/snmp/magt/INIT
   ```

然后，主代理将在所希望的端口上启动。但是，用户界面能够检测出主代理正在运行。

手动配置 SNMP 主代理

手动配置 SNMP 主代理

1. 以超级用户身份登录。
2. 检查端口 161 上是否运行有 SNMP 守护进程 (snmpd)。

   如果运行有 SNMP 守护进程，请确保知道如何重新启动它以及它支持哪些 MIB 树。然后中止其进程。
3. 编辑位于服务器根目录下 plugins/snmp/magt 中的 CONFIG 文件。
4. （可选）在 CONFIG 文件中定义 sysContact 和 sysLocation 变量。

编辑主代理的 CONFIG 文件

手动配置 SNMP 主代理

1. 以超级用户身份登录。
2. 检查端口 161 上是否运行有 SNMP 守护进程 (snmpd)。

   如果运行有 SNMP 守护进程，请确保知道如何重新启动它以及它支持哪些 MIB 树。然后中止其进程。
3. 编辑位于服务器根目录下 plugins/snmp/magt 中的 CONFIG 文件。
4. （可选）在 CONFIG 文件中定义 sysContact 和 sysLocation 变量。

定义 sysContact 和 sysLocation 变量

您可以编辑 CONFIG 文件，为指定了 sysContact 和 sysLocation MIB-II 变量的 sysContact 和 sysLocation 添加初始值。此示例中 sysContact 和 sysLocation 的字符串放在了引号内。任何包含空格、换行符、制表符等的字符串都必须放在引号内。您也可以用十六进制记数法来指定值。

下面是一个 CONFIG 文件示例，其中定义了 sysContract 和 sysLocation 变量：

```
COMMUNITY          public
                   ALLOW ALL OPERATIONS

MANAGER            nms2
                   SEND ALL TRAPS TO PORT 162
                   WITH COMMUNITY public
```

```
INITIAL            sysLocation "Server room
987 East Cannon Road
Mountain View, CA 94043
USA"

INITIAL            sysContact "Jill Dawson
email: jdawson@example.com"
```

配置 SNMP 子代理

您可以配置 SNMP 子代理以监视服务器。

配置 SNMP 子代理

1. 访问 Server Manager，然后单击 "Server Status" 选项卡。
2. 单击 "Configure SNMP Subagent" 链接。将显示 "Configure SNMP Subagent" 页面。
3. 在 "Master Host" 字段中输入服务器的名称和域。
4. 输入服务器的描述，包括操作系统信息。
5. 输入负责该服务器的组织。
6. 在 "Location" 字段中输入服务器的绝对路径。
7. 在 "Contact" 字段中，输入负责该服务器的人员的姓名和联系信息。
8. 选择 "On" 启用 SNMP 统计信息收集。
9. 单击 "OK"。
10. 单击 "Restart Required"。将出现 "Apply Changes" 页面。
11. 单击 "Restart Proxy Server" 按钮以应用更改。

启动 SNMP 主代理

安装 SNMP 主代理后，您可以手动启动它或通过 Administration Server 启动。

手动启动 SNMP 主代理

要手动启动主代理，请在命令提示符处输入以下命令：

```
# magt CONFIG INIT&
```

INIT 文件是包含 MIB-II 系统组信息（包括系统位置和联系信息）的非易失性文件。如果 INIT 尚不存在，则会在首次启动主代理时创建它。如果 CONFIG 文件中的管理器名称无效，将导致主代理启动失败。

要在非标准端口上启动主代理，请使用以下两种方法之一：

方法一：在 CONFIG 文件中，为主代理用来侦听来自管理器的 SNMP 请求的每个接口指定传输映射。传输映射允许主代理接受标准端口和非标准端口上的连接。主代理还可以在非标准端口上接受 SNMP 通信。并发 SNMP 的最大数目受限于目标系统对每个进程的打开的套接字或文件描述符数目的限制。下面是一个传输映射条目示例：

```
TRANSPORT           extraordinary   SNMP
                    OVER UDP SOCKET
                     AT PORT 11161
```

手动编辑 CONFIG 文件后，您应当在命令提示符处键入以下命令以便手动启动主代理：

```
# magt CONFIG INIT&
```

方法二：编辑 /etc/services 文件，以允许主代理接受标准端口和非标准端口上的连接。

使用 Administration Server 启动 SNMP 主代理

使用 Administration Server 启动 SNMP 主代理

1. 登录 Administration Server。
2. 在 Administration Server 中，从 "Global Settings" 选项卡中选择 "Control SNMP Master Agent" 页面。
3. 单击 "Start"。

还可以通过 "Control SNMP Master Agent" 页面停止和重新启动 SNMP 主代理。

配置 SNMP 主代理

启用了主代理并在主机上启用了某个子代理后，需要配置主机的 Administration Server。这要求指定团体字符串和陷阱目标。

配置团体字符串

团体字符串是 SNMP 代理用来进行授权的文本字符串。这意味着网络管理站在发送给代理的每条消息中都带有一个团体字符串。然后，代理就可以验证网络管理站是否被授权获取信息。团体字符串在 SNMP 包中发送时没有被隐藏；字符串以 ASCII 文本格式发送。

可以通过 Administration Server 中的 "Set SNMP Master Agent Community" 页面为 SNMP 主代理配置团体字符串。还可以定义特定团体所能执行的与 SNMP 相关的操作。在 Administration Server 中，还可以查看、编辑和删除已配置的团体。

配置陷阱目标

SNMP 陷阱是 SNMP 代理发送给网络管理站的消息。例如，当接口的状态由打开变为关闭时，SNMP 代理将发送一个陷阱。SNMP 代理必须知道网络管理站的地址，以便知道向何处发送陷阱。可以从 Proxy Server 中为 SNMP 主代理配置此陷阱目标。还可以查看、编辑和删除已配置的陷阱目标。使用 Proxy Server 配置陷阱目标时，其实是对 `CONFIG` 文件进行编辑。

启用子代理

安装了 Administration Server 附带的主代理后，您必须在尝试启动它之前为您的服务器实例启用子代理。有关安装主代理的更多信息，参见第 203 页的“安装 SNMP 主代理”。您可以使用 Server Manager 启用子代理。

要在 UNIX 或 Linux 平台上停止 SNMP 功能，必须先停止子代理，然后再停止主代理。如果先停止主代理，可能无法停止子代理。如果发生这种情况，请重新启动主代理，停止子代理，然后停止主代理。

要启用 SNMP 子代理，请使用 Server Manager 中的 "Configure SNMP Subagent" 页面，然后从 "Control SNMP Subagent" 页面中启动子代理。有关更多信息，参见联机帮助中的相应小节。

启用子代理后，便可通过 "Control SNMP Subagent" 页面 或 Windows 的服务控制面板来启动、停止或重新启动该子代理。

注	对 SNMP 配置进行任何更改后，必须单击 "Apply Required"，然后重新启动 SNMP 子代理。

了解 SNMP 消息

GET 和 SET 是 SNMP 所定义的两种类型的消息。GET 和 SET 消息由网络管理站 (NMS) 发送给主代理。您可以通过 Administration Server 使用其中一个或两个都使用。

SNMP 以协议数据单元 (PDU) 形式交换网络信息。这些单元包含有关存储在被管理设备（例如 Web 服务器）上的变量的信息。这些变量（也称为被管理对象）具有值和标题，值和标题将在需要时报告给 NMS。由服务器发送给 NMS 的协议数据单元也称为“陷阱”。下面举例说明了 GET、SET 和“陷阱”消息的使用。

NMS 启动的通信。NMS 将从服务器请求信息，或者更改存储在服务器 MIB 中的变量的值。例如：

1. NMS 将消息发送给 Administration Server 主代理。消息可能是数据请求（一条 GET 消息），也可能是在 MIB 中设置变量的指令（一条 SET 消息）。
2. 主代理将消息转发给相应的子代理。
3. 子代理将检索数据或更改 MIB 中的变量。
4. 子代理将数据或状态报告给主代理，然后主代理将消息（一条 GET 消息）转发回 NMS。
5. NMS 通过其网络管理应用程序以文本或图形方式显示该数据。

服务器启动的通信。发生重要事件时，服务器子代理将向 NMS 发送一条消息（或“陷阱”）。例如：

1. 子代理通知主代理服务器已停止。
2. 主代理发送一条消息（或“陷阱”），将该事件报告给 NMS。
3. NMS 通过其网络管理应用程序以文本或图形方式显示该信息。

第 4 部分

管理 Proxy Server

第 11 章

代理和路由选择 URL

本章介绍代理服务器如何处理请求。还介绍了如何为特定资源启用代理，以及如何配置代理服务器以将 URL 路由到不同的 URL 或服务器。

本章包括以下各节：

为资源启用 / 禁用代理

可以对资源打开或关闭代理功能。资源可以是单个 URL、带有某些通用设置的成组 URL 或整个协议。您可以控制是否对整个服务器、各种资源或模板文件中指定的资源启用代理。这意味着可以通过禁用某资源的代理拒绝对一个或多个 URL 的访问。可以全局应用此方法，以拒绝或允许对资源的所有访问。（也可以通过使用 URL 过滤器允许或拒绝对资源的访问。） 有关 URL 过滤器的更多信息，参见第 280 页的“过滤 URL”。

为资源启用代理

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Enable/Disable Proxying" 链接。将显示 "Enable/Disable Proxying" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。
4. 可以为指定的资源选择一个默认设置。可以选择不代理该资源（禁用代理），或者启用该资源的代理。可用选项如下：

- **Use Default Setting Derived From A More General Resource。**此资源将使用更通用的资源的设置（包括此设置）。
- **Do Not Proxy This Resource。**不能通过代理服务器访问此资源。
- **Enable Proxying Of This Resource。**代理服务器允许客户机访问此资源（前提是客户机通过其他安全和验证检查）。如果为某资源启用代理，**则会启用所有方法**。系统会为该资源启用所有读取方法（包括 SSL 隧道的 GET、HEAD、INDEX、POST 和 CONNECT 方法）和写入方法（包括 PUT、MKDIR、RMDIR、MOVE 和 DELETE 方法）。除非有其他安全检查，否则客户机将拥有所有读写访问权限。

5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

通过其他代理服务器路由选择

"Set Routing Preferences" 页面用于对代理服务器进行配置，使之使用派生默认配置或直接连接，或者通过代理服务器阵列、ICP 邻域、其他代理服务器或 SOCKS 服务器路由某些资源。

为资源配置路由选择

为资源配置路由选择

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Set Routing Preferences" 链接。将显示 "Set Routing Preferences" 页面。
3. 从下拉式列表中选择资源，或者单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。

4. 为正在配置的资源选择与要使用的路由选择类型对应的单选按钮。可以选择下列选项之一：

- **Derived Default Configuration。**代理服务器使用更通用的模板（即包含较短且匹配的正则表达式的模板）确定使用远程服务器还是使用另一代理服务器。例如，如果代理服务器将所有 `http://.*` 请求路由到另一代理服务器，将所有 `http://www.*` 请求路由到远程服务器，则可以为 `http://www.example.*` 请求创建派生默认配置路由选择，然后该请求会因 `http://www.*` 模板的设置而直接转到远程服务器。
- **Direct Connections。**请求将始终直接转到远程服务器，而不经过代理服务器。
- **Route Through A SOCKS Server。**对指定资源的请求将通过 SOCKS 服务器路由。如果选择此选项，则需指定代理服务器用来路由的 SOCKS 服务器的名称（或 IP 地址）和端口号。
- **Route Through。**允许指定是否通过代理服务器阵列、ICP 邻域、父阵列和 / 或代理服务器进行路由。如果在此处选择多种路由选择方法，代理服务器将遵循表单上显示的层级进行路由（即，代理服务器阵列、重定向、ICP、父阵列、另一代理服务器）。有关通过代理服务器进行路由选择的更多信息，参见第 216 页的“链接 Proxy Server”。

  有关通过 SOCKS 服务器进行路由选择的信息，参见第 216 页的“通过 SOCKS 服务器路由选择”。有关通过代理服务器阵列、父阵列或 ICP 邻域进行路由选择的信息，参见第 231 页的第 12 章“高速缓存”。

注 要在非默认端口（除 443 外的端口）启用连接请求的路由选择，需要在 `obj.conf` 文件中将 `ppath` 参数更改为 `connect://.*`。

5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

链接 Proxy Server

可以使代理服务器通过访问另一代理服务器获得某些资源，而不是访问远程服务器。这意味着可以将多个代理服务器链在一起。链接是在防火墙后组织多个代理服务器的有效方式。利用链接还可以建立分层结构的高速缓存。

通过其他代理服务器路由

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Set Routing Preferences" 链接。将显示 "Set Routing Preferences" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。
4. 在页面的 "Routing Through Another Proxy" 部分选择 "Route Through" 选项。
5. 选中 "Another Proxy" 复选框。
6. 在 "Another Proxy" 字段中，输入路由要经过的代理服务器的名称或 IP 地址。
7. 单击 "OK"。
8. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

通过 SOCKS 服务器路由选择

如果网络上已有远程 SOCKS 服务器在运行，可以将代理服务器配置为与其连接以获得特定资源。

通过 SOCKS 服务器路由

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Set Routing Preferences" 链接。将显示 "Set Routing Preferences" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。
4. 在页面的 "Routing Through Another Proxy" 部分选择 "Route Through" 选项。
5. 选择 "Route Through SOCKS Server" 选项。
6. 指定代理服务器用来进行路由的 SOCKS 服务器的名称（或 IP 地址）和端口号。

7. 单击 "OK"。

注 启用通过 SOCKS 服务器进行路由选择后，应该使用 "SOCKS v5 Routing" 页面创建代理路由。代理路由能确定可通过代理服务器路由经过的 SOCKS 服务器访问的 IP 地址。还可指定 SOCKS 服务器是否直接连接到主机。

8. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

将客户机 IP 地址转发到服务器

"Forward Client Credentials" 页面用于对代理服务器进行配置，使之将客户机凭证发送到远程服务器。

配置代理服务器发送客户机 IP 地址

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Forward Client Credentials" 链接。将显示 "Forward Client Credentials" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。
4. 根据需要更改下列选项：
   - **Client IP Addressing Forwarding。**请求文档时，Proxy Server 不将客户机的 IP 地址发送到远程服务器，而是充当客户机，并将自己的 IP 地址发送到远程服务器。但是，在以下情况下可能需要传送客户机的 IP 地址：
     - 如果您的代理服务器在内部代理服务器链中。
     - 如果您的客户机需访问要求知道客户机的 IP 地址的服务器。可以使用模板仅将客户机的 IP 地址发送到特定服务器。

     选择以下选项之一，将代理服务器配置为发送客户机 IP 地址：
     - **Default。**允许 Proxy Server 转发客户机的 IP 地址。
     - **Blocked。**不允许代理服务器转发客户机的 IP 地址。
     - **Enabled Using HTTP Header。**可以指定代理服务器转发 IP 地址时使用的 HTTP 标头。默认 HTTP 标头称为 `Client-ip`，但可以使用您选择的任何标头发送 IP 地址。

- **Client Proxy Authentication Forwarding。**选择以下选项之一，将代理服务器配置为发送客户机的验证详细信息：
  - **Default。**允许 Proxy Server 转发客户机的验证详细信息。
  - **Blocked。**不允许代理服务器转发客户机的验证详细信息。
  - **Enabled Using HTTP Header。**可以指定代理服务器转发验证详细信息时使用的 HTTP 标头。
- **Client Cipher Forwarding。**选择以下选项之一配置代理服务器，使之将客户机的 SSL/TLS 加密算法套件名称发送到远程服务器：
  - **Default。**允许 Proxy Server 将客户机的 SSL/TLS 加密算法套件名称转发到远程服务器。
  - **Blocked。**不允许代理服务器将客户机的 SSL/TLS 加密算法套件名称转发到远程服务器。
  - **Enabled Using HTTP Header。**可以指定代理服务器将客户机的 SSL/TLS 加密算法套件名称转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头称为 `Proxy-cipher`，但可以使用您选择的任何标头发送客户机 SSL/TLS 加密算法套件的名称。
- **Client Keysize Forwarding。**选择以下选项之一配置代理服务器，使之将客户机的 SSL/TLS 密钥大小发送到远程服务器：
  - **Default。**允许 Proxy Server 将客户机的 SSL/TLS 密钥大小转发到远程服务器。
  - **Blocked。**不允许代理服务器将客户机的 SSL/TLS 密钥大小转发到远程服务器。
  - **Enabled Using HTTP Header。**可以指定代理服务器将客户机的 SSL/TLS 密钥大小转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头称为 `Proxy-keysize`，但可以使用您选择的任何标头发送客户机的 SSL/TLS 密钥大小。
- **Client Secret Keysize Forwarding。**选择以下选项之一配置代理服务器，使之将客户机的 SSL/TLS 密钥大小发送到远程服务器：
  - **Default。**允许 Proxy Server 将客户机的 SSL/TLS 密钥大小转发到远程服务器。
  - **Blocked。**不允许代理服务器将客户机的 SSL/TLS 密钥大小转发到远程服务器。

- **Enabled Using HTTP Header。**可以指定代理服务器将客户机的 SSL/TLS 密钥大小转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头称为 `Proxy-secret-keysize`，但可以使用您选择的任何标头发送客户机的 SSL/TLS 密钥大小。

❍ **Client SSL Session ID Forwarding。**选择以下选项之一配置代理服务器，使之将客户机的 SSL/TLS 会话 ID 发送到远程服务器：

- **Default。**允许 Proxy Server 将客户机的 SSL/TLS 会话 ID 转发到远程服务器。
- **Blocked。**不允许代理服务器将客户机的 SSL/TLS 会话 ID 转发到远程服务器。
- **Enabled Using HTTP Header。**可以指定代理服务器将客户机的 SSL/TLS 会话 ID 转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头称为 `Proxy-ssl-id`，但可以使用您选择的任何标头发送客户机的 SSL/TLS 会话 ID。

❍ **Client Issuer DN Forwarding。**选择以下选项之一配置代理服务器，使之将客户机的 SSL/TLS 证书颁发者的标识名发送到远程服务器：

- **Default。**允许 Proxy Server 将客户机的 SSL/TLS 证书的颁发者的标识名转发到远程服务器。
- **Blocked。**不允许代理服务器将客户机的 SSL/TLS 证书颁发者的标识名转发到远程服务器。
- **Enabled Using HTTP Header。**可以指定代理服务器将客户机的 SSL/TLS 证书颁发者的标识名转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头称为 `Proxy-issuer-dn`，但可以使用您选择的任何标头发送客户机 SSL/TLS 证书颁发者的标识名。

❍ **Client User DN Forwarding。**选择以下选项之一配置代理服务器，使之将客户机的 SSL/TLS 证书主体的标识名发送到远程服务器：

- **Default。**允许 Proxy Server 将客户机的 SSL/TLS 证书主体的标识名转发到远程服务器。
- **Blocked。**不允许代理服务器将客户机的 SSL/TLS 证书主体的标识名转发到远程服务器。
- **Enabled Using HTTP Header。**可以指定代理服务器将客户机的 SSL/TLS 证书主体的标识名转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头称为 `Proxy-user-dn`，但可以使用您选择的任何标头发送客户机 SSL/TLS 证书主体的标识名。

- **Client SSL/TLS Certificate Forwarding。**选择以下选项之一配置代理服务器，使之将客户机的 SSL/TLS 证书发送到远程服务器：
  - **Default。**允许 Proxy Server 将客户机的 SSL/TLS 证书转发到远程服务器。
  - **Blocked。**不允许代理服务器将客户机的 SSL/TLS 证书转发到远程服务器。
  - **Enabled Using HTTP Header。**可以指定代理服务器将客户机的 SSL/TLS 证书转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头称为 `Proxy-auth-cert`，但可以使用您选择的任何标头发送客户机的 SSL/TLS 证书。
- **Client Cache Information Forwarding。**选择以下选项之一配置代理服务器，使之将有关本地高速缓存命中次数的信息发送到远程服务器：
  - **Default。**允许 Proxy Server 将有关本地高速缓存命中次数的信息转发到远程服务器。
  - **Blocked。**不允许代理服务器将有关本地高速缓存命中次数的信息转发到远程服务器。
  - **Enabled Using HTTP Header。**可以指定代理服务器将有关本地高速缓存命中次数的信息转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头称为 `Cache-info`，但可以使用您选择的任何标头发送有关本地高速缓存命中次数的信息。
- **Set Basic Authentication Credentials。**选择以下选项之一配置代理服务器，以发送 HTTP 请求：
  - **User。**指定要验证的用户。
  - **Password。**指定用户口令。
  - **Using HTTP Header。**可以指定代理服务器传送凭证时使用的 HTTP 标头。

5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

允许客户机检查 IP 地址

为维护网络安全，客户机可能具有将访问权限仅限于某些 IP 地址的功能。为了使客户机可以使用此功能，代理服务器提供了对检查 Java IP 地址的支持。这一支持允许客户机在代理服务器中查询用于检索资源的 IP 地址。启用此功能后，客户机可以请求代理服务器发送源服务器的 IP 地址，代理服务器会将该 IP 地址附在标头中。客户机知道源服务器的 IP 地址后，即可立即以显式方式指定以后连接使用相同的 IP 地址。

检查 Java IP 地址

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Check Java IP Address" 链接。将显示 "Check Java IP Address" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。
4. 选择单选按钮以启用或禁用 Java IP 地址检查，或者使用 Java IP 地址检查的默认配置。

注 默认选项使用从更通用的模板（即包含较短且匹配的正则表达式的模板）派生的默认配置确定应启用还是禁用 Java IP 地址检查。

5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

客户机自动配置

如果代理服务器支持许多客户机，则可使用客户机自动配置文件来配置所有浏览器客户机。自动配置文件包含一个 JavaScript 函数，该函数用于确定访问各种 URL 时 Navigator 所使用的代理服务器（如果有）。有关此功能的更多信息，参见第 325 页的第 17 章“使用客户机自动配置文件”。

设置网络连通性模式

可将代理服务器计算机连接到网络或者从网络断开连接。此功能方便了在可用于演示的便携计算机上安装代理服务器的过程。

代理服务器从网络断开连接时，文档直接从高速缓存返回——代理服务器无法进行最新性检查，因此文档检索速度相当快（文档可能不是最新的，有关高速缓存的更多信息，参见第 231 页的第 12 章“高速缓存”）。

另外，如果未连接到网络，则连接始终不会挂起，这是因为代理服务器知道没有网络，也就不会尝试连接远程服务器。在网络断开但代理服务器计算机仍在运行时可以使用此无网络设置。

注 请牢记，运行与网络断开连接的代理服务器意味着最终将从高速缓存访问过期的数据。而且，在无网络条件下运行也消除了使用代理安全功能的必要性。

Proxy Server 提供四种网络连通性模式：

- 默认模式派生自最通用的匹配对象的配置。
- 标准模式是代理服务器的标准操作模式。如果文档不在高速缓存中，则代理服务器从内容服务器检索文档。如果文档在高速缓存中，则会对照内容服务器中的文档对其进行检查，以确定是否是最新文档。如果高速缓存的文件已更改，则使用当前副本将其替换。
- 快速演示模式用于在网络可用时提供流畅的演示。如果文档在高速缓存中，则不联络内容服务器，也不检查文档是否已更改。此模式消除了因等待内容服务器响应而产生的任何等待时间。如果文档不在高速缓存中，则从内容服务器检索并存入高速缓存。快速演示模式比标准模式等待时间少，但由于该模式在保存文档副本后不再进行最新检查，所以有时会返回过期数据。
- 无网络模式专为便携式计算机未连接网络的情况而设计。如果文档在高速缓存中，则代理服务器返回文档。如果文档不在高速缓存中，则代理服务器返回错误。代理服务器始终不尝试联络内容服务器，这样可以防止代理服务器因尝试使用不存在的连接而挂起和超时。

更改代理服务器的运行模式

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Set Connectivity Mode" 链接。将显示 "Set Connectivity Mode" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。
4. 选择要使用的模式。
5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

更改默认 FTP 传送模式

FTP 提供两种不同的方法在 FTP 服务器与客户机（代理服务器充当客户机）之间建立数据连接。这两种模式称为 PASV 和 PORT 模式 FTP。

- **Passive Mode (PASV)。**从代理服务器启动数据连接，FTP 服务器接受连接。由于此模式不必接受外来连接，因而使运行代理服务器的站点更安全。
- **Active Mode (PORT)。**从远程 FTP 服务器启动数据连接，代理服务器接受外来的连接。如果代理服务器受防火墙保护，防火墙可能会禁用来自 FTP 服务器的外来 FTP 数据连接，即 PORT 模式可能不起作用。

某些 FTP 站点运行防火墙，使 PASV 模式对代理服务器不起作用。因此，可以将代理服务器配置为使用 PORT 模式 FTP。可以为整个服务器启用 PORT 模式，也可以仅为特定 FTP 服务器启用此模式。

注 即使启用了 PASV 模式，如果远程 FTP 服务器不支持 PASV 模式，代理服务器仍将使用 PORT 模式。

如果代理服务器受防火墙保护，使 PORT 模式 FTP 不起作用，则不能启用 PORT 模式。如果为资源选择默认模式，则代理服务器使用源自更通用资源的模式。如果未指定，则使用 PASV 模式。

设置 FTP 模式

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Set FTP Mode" 链接。将显示 "Set FTP Mode" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。
4. 选择 FTP 传送模式
5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

指定 SOCKS 名称服务器 IP 地址

如果将代理服务器配置为通过 SOCKS 服务器建立外发连接，可能需要以显示方式指定 SOCKS 名称服务器的 IP 地址。

如果使用 DNS 服务器（而非防火墙内的内部 DNS 服务）解析外部主机名，则应指定名称服务器 IP 地址。

指定 SOCKS 名称服务器 IP 地址

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Set SOCKS Name Server" 链接。将显示 "Set SOCKS Name Server" 页面。
3. 在文本字段中输入 DNS 名称服务器的 IP 地址。
4. 单击 "OK"。

注 用于指定 SOCKS 名称服务器的 IP 地址的功能过去只能通过 SOCKS_NS 环境变量访问。如果设置环境变量并使用 "SOCKS Name Server Setting" 表单指定名称服务器 IP 地址，则代理服务器使用在表单上指定的 IP 地址，而非环境变量。

5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

配置 HTTP 请求负载平衡

"Configure HTTP Request Load Balancing" 页面用于在指定的源服务器中分配负载。

配置 HTTP 请求负载平衡

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Configure HTTP Request Load Balancing" 链接。将显示 "Configure HTTP Request Load Balancing" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。
4. 在 "Server" 字段中指定源服务器的 URL。如果给定多个服务器参数，则 Proxy Server 将在指定的源服务器中分配负载。

5. 在 "Sticky Cookie" 字段中指定 cookie 的名称，当其出现在响应中时，会导致随后的请求保留在此源服务器。默认值为 `JSESSIONID`。
6. 在 "Sticky Parameter" 字段中指定用于检查路由信息的 URI 参数的名称。如果 URI 参数出现在请求 URI 中，并且其值包含冒号，后接路由 ID，则请求将“保留”在由此路由 ID 标识的源服务器中。默认值为 `jsessionid`。
7. 在 "Route Header" 字段中指定用于将路由 ID 发送至源服务器的 HTTP 请求标头的名称。默认值为 `proxy-jroute`。
8. 在 "Route Cookie" 字段中指定 Proxy Server 在响应中遇到 "Sticky Cookie" 时生成的 cookie 的名称。默认值为 `JROUTE`。
9. 单击适当的 "Rewrite Host" 选项，以指示是否重写 Host HTTP 请求标头，以便与服务器参数指定的主机匹配。
10. 单击适当的 "Rewrite Location" 选项，以指示是否应重写与服务器参数匹配的 Location HTTP 响应标头。
11. 单击适当的 "Rewrite Content Location" 选项，以指示是否应重写与服务器参数匹配的 Content-location HTTP 响应标头。
12. 选中相应复选框，指示是否应重写与服务器参数匹配的 *headername* HTTP 响应标头，其中 *headername* 是用户定义的标头名称。在 "Headername" 字段中指定标头名称。
13. 单击 "OK"。
14. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
15. 单击 "Restart Proxy Server" 按钮以应用更改。

管理 URL 和 URL 映射

Server Manager 允许将 URL 映射到其他服务器，有时称为镜像服务器。客户机使用镜像 URL 访问代理服务器时，代理服务器从镜像服务器检索请求的文档，而不从 URL 中指定的服务器检索。客户机不会知道请求将转到其他服务器。也可以重定向 URL，在这种情况下，代理服务器只向客户机返回重定向的 URL（而不返回文档），以便客户机随后可以请求新文档。还可以用映射将 URL 映射到文件，在 PAC 和 PAT 映射中即如此。

本节包括以下主题：

- 创建 URL 映射
- 查看、编辑或删除现有 URL 映射
- 重定向 URL

创建 URL 映射

要映射 URL，请指定 URL 前缀以及映射目标位置。以下各节介绍各种类型的 URL 映射。可以创建四种类型的 URL 映射：

- 正则映射将一个 URL 前缀映射到另一个 URL 前缀。例如，可对代理服务器进行配置，使其每次收到开始 `http://www.example.com` 的请求时，即转到特定 URL。
- 反向映射将一个已重定向的 URL 前缀映射到另一个 URL 前缀。当内部服务器向代理服务器发送已重定向的响应而不发送文档时，反向代理服务器即使用此类映射。有关更多信息，参见第 289 页的第 14 章“使用反向代理服务器”。
- 正则表达式映射将与表达式匹配的所有 URL 映射到一个 URL。例如，可以将与 .*job.* 匹配的所有 URL 映射到一个特定 URL（此 URL 可能解释代理服务器为什么不允许用户转到特定 URL）。
- 客户机自动配置将 URL 映射到存储在代理服务器上的特定 `.pac` 文件。有关自动配置文件的更多信息，参见第 325 页的第 17 章“使用客户机自动配置文件”。
- 代理服务器阵列表 (PAT) 将 URL 映射到存储在代理服务器上的特定 `.pat` 文件。只能在主代理服务器中创建此类映射。有关 PAT 文件和代理服务器阵列的更多信息，参见第 265 页的“通过代理服务器阵列进行路由选择”。

访问 URL 的客户机被发送到相同或不同服务器上的其他位置。资源已移动时，或者需要在未使用结尾斜杠访问目录时保持相对链接的完整性，此功能会很有用。

例如，假定有一个名为 hi.load.com 的高负载 Web 服务器，您想要将它镜像到另一个名为 mirror.load.com 的服务器。对于转到 hi.load.com 计算机的 URL，可以将代理服务器配置为使用 mirror.load.com 计算机。

源 URL 前缀必须未进行转义，但在目标（镜像）URL 中，只需要转义在 HTTP 请求中非法的字符。

注意 切勿在前缀中使用结尾斜杠！

创建 URL 映射

1. 访问 Server Manager，然后单击 "URLs" 选项卡。
2. 单击 "Create Mapping" 链接。将显示 "Create Mapping" 页面。

3. 选择要创建的映射类型。

   - **Regular Mappings**。将一个 URL 前缀映射到另一个 URL 前缀。例如，可对代理服务器进行配置，使其每次收到开始 `http://www.example.com` 的请求时，即转到特定 URL。如果选择此选项，该页面的下部将显示以下选项：

     - **Rewrite Host**。单击适当的选项，指示是否重写 Host HTTP 标头，以与 `"to"` 参数指定的主机匹配。

   - **Reverse Mappings**。将一个已重定向的 URL 前缀映射到另一个 URL 前缀。当内部服务器向代理服务器发送已重定向的响应而不发送文档时，反向代理服务器即使用此类映射。有关反向代理服务器的更多信息，参见第 289 页的第 14 章“使用反向代理服务器”。如果选择此选项，该页面的下部将显示以下选项：

     - **Rewrite Location**。单击适当的选项，指示是否重写 Location HTTP 响应标头。

     - **Rewrite Content Location**。单击适当的选项，指示是否重写 Content-location HTTP 响应标头。

     - **Rewrite Headername**。选择该复选框，指示是否重写 *headername* HTTP 响应标头，其中 *headername* 是用户定义的标头名。

   - **Regular Expression**。将与此表达式匹配的所有 URL 映射到一个 URL。有关正则表达式的更多信息，第 319 页的第 16 章“管理模板和资源”。

   - **Client Autoconfiguration**。将 URL 映射到存储在 Proxy Server 上的特定 .pac 文件。有关自动配置文件的更多信息，第 325 页的第 17 章“使用客户机自动配置文件”。

   - **Proxy Array Table (PAT)**。将 URL 映射到存储在 Proxy Server 上的特定 `.pat` 文件。只能在主代理服务器中创建此类映射。有关 PAT 文件和代理服务器阵列的更多信息，参见“通过代理服务器阵列进行路由选择”，此主题位于第 231 页的第 12 章“高速缓存”。

4. 键入映射源前缀。对于正则映射和反向映射，此前缀应该是要替代的 URL。

   对于正则表达式映射，此 URL 前缀应该是所有 URL 要与之匹配的正则表达式。如果还为映射选择了模板，此正则表达式仅对模板的正则表达式中的 URL 起作用。

   对于客户机自动配置映射和代理服务器阵列表映射，URL 前缀应是客户机访问的完整 URL。

5. 键入映射目标。

   对于除客户机自动配置和代理服务器阵列表以外的所有映射类型，此项应是要映射到的完整 URL。对于客户机自动配置映射，此值应是到位于代理服务器硬盘上的 .pac 文件的绝对路径。对于代理服务器阵列表映射，此值应是到位于主代理服务器本地磁盘上的 .pat 文件的绝对路径。

6. 从下拉式列表中选择模板名称，如果不想应用模板则将此值保留为 "NONE"。
7. 单击 "OK" 创建映射。
8. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

查看、编辑或删除现有 URL 映射

更改现有映射

1. 访问 Server Manager，然后单击 "URLs" 选项卡。
2. 单击 "View/Edit Mappings" 链接。将显示 "View/Edit Mappings" 页面。
3. 要编辑映射，请单击它旁边的 "Edit" 链接。可以编辑受该映射影响的前缀、映射 URL 和模板。单击 "OK" 确认所做的更改。
4. 要删除映射，请单击要编辑的映射，然后单击该映射旁的 "Remove" 链接。
5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

重定向 URL

可以配置代理服务器，使之向客户机返回重定向的 URL，而不是获取并返回文档。重定向后，客户机会知道原来请求的 URL 已被重新定向到其他 URL。通常，客户机会立即请求已重定向的 URL。Netscape Navigator 会自动请求已重定向的 URL——用户不必再次明确请求该文档。

当您想拒绝对某个区域的访问时，URL 重定向很有用，因为可将用户重定向到说明访问为何被拒绝的 URL。

重定向一个或多个 URL

1. 访问 Server Manager，然后单击 "URLs" 选项卡。
2. 单击 "Redirect URLs" 链接。将显示 "Redirect URLs" 页面。

3. 输入作为 URL 前缀的源 URL。
4. 输入要重定向到的 URL。此 URL 既可以是 URL 前缀，也可以是固定的 URL。

   如果选择使用 URL 前缀作为重定向的目标 URL，请选择 "URL prefix" 字段旁的单选按钮，并输入一个 URL 前缀。如果选择使用固定 URL，请选择 "Fixed URL" 字段旁的单选按钮，并输入一个固定 URL。
5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

第 12 章

高速缓存

本章介绍 Sun Java™ System Web Proxy Server 如何对文档进行高速缓存，还介绍了如何使用联机页面来配置高速缓存。

本章包括以下各节：

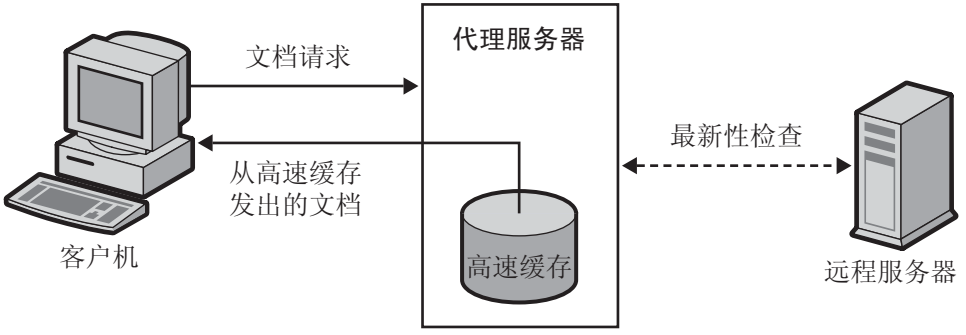
高速缓存的工作原理

对于使用代理服务器访问远程服务器而不是直接访问远程服务器的客户机，高速缓存降低了网络通信流量并缩短了响应时间。

客户机向代理服务器请求 Web 页或文档时，代理服务器会在将文档发送给客户机的同时将文档从远程服务器复制到其本地高速缓存目录结构。

如果客户机请求的是以前请求过并已复制到代理服务器高速缓存中的文档，代理服务器将从高速缓存返回文档，而不是再次从远程服务器检索文档（参见图 12-1）。如果代理服务器确定文件不是最新的，将从远程服务器刷新该文档并更新其高速缓存，然后再将文档发送到客户机。

图 12-1 代理服务器文档检索



高速缓存中的文件由 Sun Java™ System Web Proxy Server 垃圾收集实用程序 (CacheGC) 自动进行维护。CacheGC 会自动定期清理高速缓存来确保其不会被过期文档弄乱。

了解高速缓存结构

高速缓存由一个或更多个分区组成。从概念上讲，分区是指磁盘上留作高速缓存之用的存储区域。如果想要让高速缓存跨越若干个磁盘，则至少需要为每个磁盘配置一个高速缓存分区。可以单独管理各个分区。也就是说，可以单独启用、禁用和配置某个分区，而所有其他分区均不受影响。

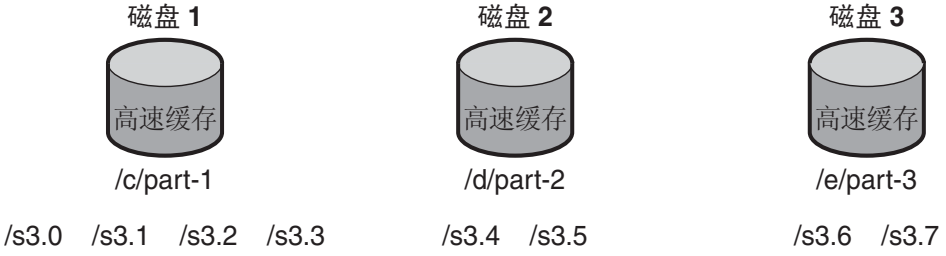
在一个位置存储大量高速缓存的文件会降低性能，因此，好的做法是在每个分区中创建若干个目录或区段。区段是高速缓存结构中仅次于分区的下一个级别。高速缓存的所有分区最多可以有 256 个区段。高速缓存区段数必须为 2 的乘方（例如，1、2、4、8、16、...、256）。

高速缓存分层结构中的最低级别是子区段。子区段是指区段内的目录。每个区段有 64 个子区段。高速缓存的文件存储在子区段，即高速缓存的最低级别中。

图 12-2 显示了具有分区和区段的高速缓存结构的一个示例。在该图中，高速缓存目录结构将全部高速缓存分成了三个分区。第一个分区包含四个高速缓存区段，后两个分区各包含两个区段。

每个高速缓存区段的表示方法是：以 s 代表区段，其后是区段号。以显示为 s3.4 的区段为例，3 表示高速缓存区段数 ($2^3 = 8$) 中 2 的幂次，4 表示区段号（共 8 个区段，依次标记为 0, ..., 7）。因此，s3.4 代表 8 个区段中的第 5 个区段。

图 12-2 高速缓存结构示例



高速缓存中的文件分布

Proxy Server 使用特定算法来确定应将文档存储在哪个目录。该算法可以确保均匀分布目录中的文档。均匀分布很重要，因为包含大量文档的目录容易引发性能问题。

Proxy Server 使用 RSA MD5（Message Digest 5，消息摘要 5）算法将 URL 简化为 16 字节的二进制数据，并使用该数据的 8 个字节来计算在高速缓存中存储文档时使用的 16 个字符的十六进制文件名。

设置高速缓存细节

可以通过设置高速缓存细节来启用高速缓存并控制 Proxy Server 将要缓存的协议类型。高速缓存细节包括以下项：

- 是启用还是禁用了高速缓存
- 高速缓存存储其临时文件的工作目录
- 将在其中记录高速缓存的 URL 的目录的名称
- 高速缓存的大小
- 高速缓存的容量
- 将要高速缓存的协议类型
- 何时刷新高速缓存的文档
- 代理服务器是否应跟踪文档的访问次数并将其回报给远程服务器

设置高速缓存细节

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Set Cache Specifics" 链接。将显示 "Set Cache Specifics" 页面。
3. 可以通过选择相应的选项来启用或禁用高速缓存。默认情况下将启用高速缓存。有关更多信息，参见第 235 页的“启用高速缓存”。
4. 输入工作目录。默认情况下工作目录位于代理服务器实例下。如果希望高速缓存目录位于其他位置，可以对其进行更改。有关更多信息，参见第 236 页的“创建高速缓存工作目录”。
5. 单击分区配置链接。将显示 "Add/Edit Cache Partitions" 页面。可以添加新的高速缓存分区或编辑现有的高速缓存分区。高速缓存大小是指最大允许高速缓存增长到的大小。高速缓存的最大大小是 32GB。有关更多信息，参见第 236 页的“设置高速缓存大小”。
6. 单击高速缓存容量配置链接。将显示 "Set Cache Capacity" 页面。可以在 "Set Cache Capacity" 页面上设置高速缓存容量。有关更多信息，参见第 236 页的“编辑高速缓存容量”。

7. 选中 "Cache HTTP" 复选框来启用对 HTTP 文档的高速缓存。如果决定要让代理服务器对 HTTP 文档进行高速缓存，则需要确定它应始终对高速缓存中的文档进行最新性检查，还是应按某一时间间隔进行检查。还可以启用或禁用 Proxy Server 向远程服务器报告高速缓存命中次数。有关更多信息，参见第 236 页的“高速缓存 HTTP 文档”。包括以下选项：

   - 选择 "Always Check That The Document Is Up To Date" 选项可确保 HTTP 文档始终是最新的。
   - 从 "Check Only If Last Check More Than" 下拉式列表中选择小时数可指定代理服务器的刷新间隔。可使用以下任一选项执行最新性检查：
     - **Use Last-modified Factor。**它是源服务器随文档一同发送的 last-modified 标头。
     - **Use Only Explicit Expiration Information。**代理服务器使用 Expires 标头来确定高速缓存条目是新条目还是过期条目。
   - 选择 "Never Report Accesses To Remote Server" 选项可禁止代理服务器向远程服务器报告访问次数。
   - 选择 "Report Cache Hits To Remote Server" 选项可跟踪文档的访问次数并将其回报给远程服务器。

8. 可以设置高速缓存的 FTP 文档的刷新间隔。选中 "Yes; Reload If Older Than" 复选框并从下拉式列表中选择值来设置时间间隔。有关更多信息，参见第 239 页的“高速缓存 FTP 和 Gopher 文档”。
9. 可以设置高速缓存的 Gopher 文档的刷新间隔。选中 "Yes; Reload If Older Than" 复选框并从下拉式列表中选择值来设置时间间隔。有关更多信息，参见第 239 页的“高速缓存 FTP 和 Gopher 文档”。
10. 单击 "OK"。
11. 单击 "Restart required"。将显示 "Apply Changes" 页面。
12. 单击 "Restart Proxy Server" 按钮以应用更改。

以下各节介绍有关 "Set Cache Specifics" 页面上所列元素的更多信息，并帮助您确定最适合自身需要的设置。

启用高速缓存

对于代理服务器用户来说，高速缓存是减少网络通信流量的有效方法。由于不再需要从远程服务器检索文档，因此对于客户机而言，高速缓存还缩短了响应时间。启用高速缓存时代理服务器将能够最有效地发挥作用。

创建高速缓存工作目录

高速缓存文件位于高速缓存分区下。在 "Set Cache Specifics" 页面上指定的工作目录往往是高速缓存的父目录。所有高速缓存的文件均以有组织的目录结构形式出现在高速缓存目录下。如果更改了高速缓存目录的名称或将其移动到了其他位置，则须将新位置告知代理服务器。

可以将高速缓存目录结构扩展至多个文件系统，这样便可使一个大的高速缓存结构散布在多个较小的磁盘上，而不用将其全部存放在一个大的磁盘中。每个代理服务器均须拥有各自的高速缓存目录结构，也就是说，多个代理服务器不能同时共享高速缓存目录。

设置高速缓存大小

高速缓存大小指示分区大小。高速缓存大小应始终小于高速缓存容量，因为它是高速缓存最大可以增长到的大小。所有分区大小的总和必须小于或等于高速缓存大小。

可供代理服务器高速缓存使用的磁盘空间大小对高速缓存性能有相当大的影响。如果高速缓存过小，Cache GC 必须更频繁地删除高速缓存的文档以腾出磁盘空间，还必须更频繁地从内容服务器检索文档，因而会降低性能。

高速缓存大小越大越好，因为高速缓存的文档越多，网络通信流量负载就越少，代理服务器所提供的响应时间也就越短。此外，如果用户不再需要高速缓存的文档，GC 会将它们删除。除非文件系统有限制，否则，高速缓存大小再大也不过分；过剩的空间只不过保持未用而已。

还可将高速缓存分割于多个磁盘分区。

注意 更改高速缓存结构是耗时的。

编辑高速缓存容量

可以通过 "Set Cache Specifics" 页面及 "Set Cache Capacity" 页面来编辑高速缓存容量。有关编辑高速缓存容量的更多信息，参见第 240 页的“设置高速缓存容量”。

高速缓存 HTTP 文档

从本质上讲，高速缓存 HTTP 文档不同于高速缓存 FTP 和 Gopher 文档。HTTP 文档提供了其他协议的文档所不具备的高速缓存功能。不过，通过适当设置和配置高速缓存，可以确保 Proxy Server 有效地高速缓存 HTTP、FTP 和 Gopher 文档。

所有 HTTP 文档都有一个描述性的标头部分，Proxy Server 使用该部分来比较和评判代理服务器高速缓存中的文档与远程服务器上的文档。代理服务器对 HTTP 文档执行最新性检查时，如果高速缓存中文档的版本已过期，代理服务器将向服务器发送请求，告知服务器返回文档。上一次请求后文档往往并没有发生变化，因此将不会传送文档。这种检查 HTTP 文档是否为最新的方法节约了带宽并缩短了等待时间。

为减少与远程服务器间的事务，可以通过 Proxy Server 为 HTTP 文档设置 "Cache Expiration" 设置。"Cache Expiration" 设置指示代理服务器估计向服务器发送请求前是否需要对 HTTP 文档进行最新性检查。代理服务器根据在标头中找到的 HTTP 文档的 "Last-Modified" 日期进行这种估计。

对于 HTTP 文档，还可以使用 "Cache Refresh" 设置。此选项指定代理服务器是始终进行最新性检查（将覆盖失效期设置）还是等待特定时间段后再进行检查。表 12-1 显示同时指定失效期设置和刷新设置时代理服务器将执行的操作。使用刷新设置可显著缩短等待时间和节约带宽。

表 12-1 对 HTTP 使用 "Cache Expiration" 和 "Cache Refresh" 设置

刷新设置	失效期设置	结果
始终执行最新性检查	（不适用）	始终执行最新性检查
用户指定的时间间隔	使用文档的 "expires" 标头	时间间隔到期时执行最新性检查
	使用文档的 Last-Modified 标头进行估计	估计值和 expires 标头中的较小值 *

* 对于变化频繁的文档，使用较小值可以防止从高速缓存中获取其过期数据。

设置 HTTP 高速缓存刷新间隔

如果决定要让 Proxy Server 对 HTTP 文档进行高速缓存，需要确定它应始终对高速缓存中的文档执行最新性检查，还是应基于 "Cache Refresh" 设置（最新性检查时间间隔）进行检查。例如，对于 HTTP 文档，合理的刷新间隔是四到八小时。刷新间隔越长，代理服务器与远程服务器的连接次数就越少。即使在刷新间隔期间代理服务器不执行最新性检查，用户也可以通过在客户端单击 "Reload" 按钮来强制刷新；该操作使代理服务器强制与远程服务器进行最新性检查。

可以在 "Set Cache Specifics" 页面或 "Set Caching Configuration" 页面上设置 HTTP 文档的刷新间隔。通过 "Set Cache Specifics" 页面可以配置全局高速缓存过程，而通过 "Set Caching Configuration" 页面可以控制特定 URL 和资源的高速缓存过程。

设置 HTTP 高速缓存失效期策略

还可以将服务器设置为只使用 last-modified 因子或显式失效期信息来检查高速缓存的文档是否是最新的。

显式失效期信息是某些 HTTP 文档中的标头，用来指定文件过期的日期和时间。使用显式 Expires 标头的 HTTP 文档并不多，因此最好根据 Last-modified 标头进行估计。

如果决定根据 Last-modified 标头对 HTTP 文档进行高速缓存，需要选择一个小数用于失效期估计。该小数（称为 LM 因子）将与上次修改时间和上次对文档执行最新性检查时间之间的间隔相乘，然后将结果数字与上次执行最新性检查到现在为止的时间进行比较。如果该数字比时间间隔小，则表示文档未过期。小数越小，就会使代理服务器更频繁地检查文档。例如，假定有一个文档，上次更改它是在十天前。如果将 last-modified 因子设置为 0.1，代理服务器将把该因子理解为文档可能会在一天内保持不变 (10 * 0.1 = 1)。在这种情况下，如果不到一天前对文档进行了检查，代理服务器将返回高速缓存中的文档。

仍使用本示例，如果将 HTTP 文档的高速缓存刷新设置的值设置为不足一天，代理服务器每天将进行不止一次的最新性检查。代理服务器将始终使用要求它更频繁地更新文件的值（高速缓存刷新或高速缓存失效期）。

可以在 "Set Cache Specifics" 页面或 "Set Caching Configuration" 页面上设置 HTTP 文档的失效期设置。通过 "Set Cache Specifics" 页面可以配置全局高速缓存过程，而通过 "Set Caching Configuration" 页面可以控制特定 URL 和资源的高速缓存过程。

向远程服务器报告 HTTP 访问情况

Sun Java™ System Web Proxy Server 对文档进行高速缓存后，再次刷新文档前文档可能已被访问许多次。对于远程服务器而言，向代理服务器发送将要由其进行高速缓存的一个副本只代表一次访问（或称“命中”）。Sun Java™ System Web Proxy Server 可以对最新性检查间隔期间访问代理服务器高速缓存中给定文档的次数进行计数，然后在下次刷新文档时通过另一个 HTTP 请求标头 (Cache-Info) 将该命中计数回传给远程服务器。这样一来，如果将远程服务器配置为可以识别该类型标头，就可以收到更准确的文档访问次数报告。

高速缓存 FTP 和 Gopher 文档

FTP 和 Gopher 不具有用来检查文档最新性的方法。因此，优化 FTP 和 Gopher 文档高速缓存的唯一方法是设置 "Cache Refresh" 时间间隔。"Cache Refresh" 时间间隔是指 Proxy Server 从远程服务器检索文档最新版本前等待的时间长度。如果不设置 "Cache Refresh" 时间间隔，即使高速缓存中的版本是最新的，代理服务器仍将检索这些文档。

设置 FTP 和 Gopher 高速缓存刷新间隔

如果要设置 FTP 和 Gopher 高速缓存刷新间隔，请选择一个自认为对代理服务器获取的文档安全的时间间隔。例如，如果存储很少发生变化的信息，请使用较大的值（若干天）。如果数据不断变化，您会希望至少每隔几小时就检索一次文件。刷新期间存在着将过期文件发送给客户机的风险。如果时间间隔足够短（几小时），在响应时间显著缩短的同时也大部分消除了这种风险。

可以在 "Set Cache Specifics" 页面或 "Set Caching Configuration" 页面上设置 FTP 和 Gopher 文档的高速缓存刷新间隔。通过 "Set Cache Specifics" 页面可以配置全局高速缓存过程，而通过 "Set Caching Configuration" 页面可以控制特定 URL 和资源的高速缓存过程。有关使用 "Set Cache Specifics" 页面的更多信息，参见第 234 页的“设置高速缓存细节”；有关使用 "Set Caching Configuration" 页面的更多信息，参见第 242 页的“配置高速缓存”。

注 如果 FTP 和 Gopher 文档间的差异很大（有些经常发生变化，有些则很少发生变化），请使用 "Set Caching Configuration" 页面为每种文档分别创建模板（例如，创建包含资源 `ftp://.*.gif` 的模板），然后设置适合该资源的刷新间隔。

创建和修改高速缓存

高速缓存分区是指留待高速缓存之用的磁盘或内存的预留部分。如果高速缓存容量发生变化，可能需要使用 "Add/Edit Cache Partitions" 页面来更改或添加分区。在此页面中，可以编辑分区的位置、助记名及最大和最小大小。还可查看该分区的高速缓存区段表。

添加高速缓存分区

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Add/Edit Cache Partitions" 链接。将显示 "Add/Edit Cache Partitions" 页面。

3. 单击 "Add Cache Partition" 按钮。将显示 "Cache Partition Configuration" 页面。
4. 为新分区输入适当的值。
5. 单击 "OK"。
6. 单击 "Restart required"。将显示 "Apply changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改

修改高速缓存分区

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Add/Edit Cache Partitions" 链接。将显示 "Add/Edit Cache Partitions" 页面。
3. 单击要更改的分区的名称。
4. 编辑信息。
5. 单击 "OK"。
6. 单击 "Restart required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

设置高速缓存容量

高速缓存容量值用于导出高速缓存目录结构。高速缓存目录中的最大区段数是根据高速缓存容量导出的。高速缓存容量与高速缓存目录中的高速缓存分层结构有直接关系。容量越大，分层结构越大。高速缓存容量应大于或等于高速缓存大小。如果已知自己打算在以后增加高速缓存大小（例如，通过添加外部磁盘的方式），则将容量设置为大于高速缓存大小可能会有所帮助。高速缓存容量最大可达 32 GB，具有 256 个区段。

设置高速缓存容量

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Set Cache Capacity" 链接。将显示 "Set Cache Capacity" 页面。
3. 从 "New Capacity Range" 下拉式列表中选择容量。
4. 单击 "OK"。
5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

管理高速缓存区段

代理服务器高速缓存被分成一个或更多个高速缓存区段。最多可以有 256 个区段。高速缓存区段数必须为 2 的乘方（例如，1、2、4、8、16、...、256）。最大容量为 32GB（最优），具有 256 个高速缓存区段。

如果选用 500MB 的高速缓存容量，安装程序会创建 4 个高速缓存区段 (500/125 = 4)；如果选择 2GB 的高速缓存容量，安装程序会创建 16 个区段 (2000/125 = 16)。为便于获得区段数，选择 125MB 作为每个区段的最优值。区段数越多，存储和分布的 URL 数就越大。

管理高速缓存区段

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Manage Sections" 链接。将显示 "Manage Sections" 页面。
3. 更改表中的信息。可以在现有分区间移动区段。
4. 单击 "OK"。
5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

设置垃圾收集首选项

"Set Garbage Collection Preferences" 页面用于设置垃圾收集模式。

可以使用高速缓存垃圾收集器来删除高速缓存中的文件。垃圾收集既可以在自动模式下进行，也可以在显式模式下进行。显式模式是管理员使用 "Schedule Garbage Collection" 页面从外部进行调度的。选择其中一种模式，然后单击 "OK"。单击 "Restart Required"。将显示 "Apply Changes" 页面。单击 "Restart Proxy Server" 按钮以应用更改。

调度垃圾收集

可以通过 "Schedule Garbage Collection" 页面指定进行垃圾收集的日期和时间。

调度垃圾收集：

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Schedule Garbage Collection" 链接。将显示 "Schedule Garbage Collection"。

3. 从 "Schedule Garbage Collection At" 列表中选择进行垃圾收集的时间。
4. 指定在星期几进行垃圾收集。
5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

配置高速缓存

使用 "Set Caching Configuration" 页面可以配置想要对特定资源采用的高速缓存类型。可以为与指定的正则表达式模式匹配的 URL 指定若干个配置参数值。可以通过此特性根据高速缓存的文档的类型对代理服务器高速缓存进行精细控制。配置高速缓存可能需要确定以下各项：

- 高速缓存默认值
- 如何高速缓存需要进行验证的页面
- 如何高速缓存查询
- 最小和最大高速缓存文件大小
- 何时刷新高速缓存的文档
- 高速缓存失效期策略
- 客户机中断操作的高速缓存行为
- 到源服务器的失败连接的高速缓存行为

注 如果将某个资源的高速缓存默认值设置为 "Derived configuration" 或 "Don't cache"，高速缓存配置选项将不会在 "Set Caching Configuration" 页面中出现。不过，如果为资源选择了高速缓存默认值 "Cache"，就可以指定若干个其他配置项。

配置高速缓存

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Set Caching Configuration" 页面。将显示 "Set Caching Configuration" 页面。

3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮来输入正则表达式，然后单击 "OK"。
4. 更改配置信息。
5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

高速缓存配置元素

以下各节介绍 "Set Caching Configuration" 页面所列的各项。这些节中包括的信息将帮助您确定最适合自身需要的配置。

设置高速缓存默认值

可以通过代理服务器来确定特定资源的高速缓存默认值。资源是指符合所指定的某种条件的文件类型。例如，可能希望服务器自动高速缓存来自域 company.com 的所有文档。如果是这样，请单击 "Set Caching Configuration" 页面顶部的 "Regular Expression" 按钮，然后在出现的字段中输入

```
[a-z] *://[^/:]\.company\.com.*
```

。

默认情况下会选中 "Cache" 选项。服务器会自动高速缓存来自该域的所有可高速缓存的文档。有关正则表达式的更多信息，参见“了解正则表达式”。

注 如果将某个资源的高速缓存默认值设置为 "Derived configuration" 或 "Don't cache"，则不必为该资源配置高速缓存。不过，如果为资源选择了高速缓存默认值 "Cache"，就可以指定若干个其他配置项。有关这些项的列表，参见第 242 页的“配置高速缓存”。

也可以在 "Set Cache Specifics" 页面上设置 HTTP、FTP 和 Gopher 的高速缓存默认值。

高速缓存要求进行验证的页面

可以让服务器高速缓存要求进行用户验证的文件。如果选择让 Proxy Server 高速缓存这些文件，Proxy Server 会对高速缓存中的这些文件进行标记，这样当用户请求它们时，Proxy Server 便知道这些文件要求从远程服务器进行验证。

因为 Proxy Server 既不知道远程服务器的验证方式，也不知道用户的 ID 或口令，所以它只会在每次收到对要求进行验证的文档的请求时，强制同远程服务器进行最新性检查。因此，用户必须输入 ID 和口令才能获得文件的访问权。如果用户早先在 Navigator 会话中已访问过该服务器，Navigator 会自动发送验证信息，而不提示用户输入该信息。

如果不启用对要求进行验证的页面进行高速缓存，代理服务器将采用默认值，即不高速缓存这些页面。

高速缓存查询

高速缓存的查询仅适用于 HTTP 文档。可以限制高速缓存的查询的长度，也可以完全禁止对查询的高速缓存。查询越长，其重复的可能性越低，对其进行高速缓存所起的作用也就越小。

查询受以下高速缓存限制的制约：访问方法必须是 GET，文档不能被保护（除非已启用对验证过的页面进行高速缓存），响应必须至少有 Last-modified 标头。这就要求查询引擎指出可以高速缓存查询结果文档。如果存在 Last-modified 标头，查询引擎应支持有条件的 GET 方法（具有 If-modified-since 标头），以使高速缓存生效；否则，它应返回 Expires 标头。

设置最小和最大高速缓存文件大小

可以为 Proxy Server 高速缓存的文件设置最小和最大大小。如果网络连接速度快，可能需要设置最小大小。如果连接速度快，检索小文件的速度可能快到已没有必要让服务器对它们进行高速缓存。这种情况下，只需高速缓存较大的文件即可。可能需要设置最大文件大小，以确保大文件不会过多占用代理服务器的磁盘空间。

设置最新性检查策略

可以使用此选项来确保 HTTP 文档始终是最新的。还可以指定 Proxy Server 的刷新间隔。

设置失效期策略

可以使用 last-modified 因子或显式失效期信息来设置失效期策略。

设置客户机中断操作的高速缓存行为

如果仅检索到部分文档而客户机中断了数据传送，代理服务器能够出于高速缓存目的完成对文档的检索。如果已至少检索到文档的 25%，则默认情况下代理服务器会出于高速缓存目的完成对文档的检索。否则，代理将中断远程服务器连接并删除不完整的文件。可以增大或减小客户机中断百分比。

连接服务器失败时的行为

如果由于源服务器不可访问而导致对某个过时文档的最新性检查失败，可以指定代理服务器是否发送高速缓存中的过时文档。

高速缓存本地主机

如果从本地主机请求的 URL 缺少域名，Proxy Server 将不会对其进行高速缓存，以避免重复高速缓存。例如，如果用户从本地服务器请求

`http://machine/filename.html` 和

`http://machine.example.com/filename.html`，这两个 URL 可能都会出现在高速缓存中。由于这些文件来自本地服务器，因此对它们的检索速度可能快到已没有必要以任何方式对它们进行高速缓存。

不过，如果公司在许多远程位置都有服务器，可能需要高速缓存来自所有主机的文档，以减少网络通信流量和缩短访问这些文件所需的时间。

启用对本地主机的高速缓存

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Cache Local Hosts" 链接。将显示 "Cache Local Hosts" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮来输入正则表达式，然后单击 "OK"。有关正则表达式的更多信息，参见第 319 页的第 16 章 “管理模板和资源”。
4. 单击 "enabled" 按钮。
5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

配置文件高速缓存

默认情况下文件高速缓存处于启用状态。文件高速缓存设置包含在 `server.xml` 文件中。可以使用 Server Manager 更改文件高速缓存设置。

注 用户界面中显示有 "Configure File Cache" 页面，但在本 Proxy Server 4 版本中并未实现该功能

配置文件高速缓存

1. 在 Server Manager 中单击 "Preferences" 选项卡。
2. 单击 "File Cache Configuration" 链接。将显示 "File Cache Configuration" 页面。
3. 如果尚未选择 "Enable File Cache"，请选择它。
4. 选择是否传输文件。

   启用 "Transmit File" 时，服务器高速缓存会打开文件高速缓存中文件的文件描述符，而不是文件内容，并且会使用 PR_TransmitFile 将文件内容发送至客户机。"Transmit File" 处于启用状态时，通常由文件高速缓存进行的对大、中、小文件的区分便不再适用，因为只会对打开的文件描述符进行高速缓存。默认情况下在 Windows 上启用 "Transmit File"，在 UNIX 上则将其禁用。在 UNIX 上，只为对 PR_TransmitFile 具有本机 OS 支持的平台启用 "Transmit File"，这些平台目前包括 HP-UX 和 AIX。建议对于其他 UNIX/Linux 平台不要启用它。
5. 输入散列表大小。默认大小为最大文件数的两倍加 1。例如，如果将最大文件数设置为 1024，则默认散列表大小为 2049。
6. 输入有效高速缓存条目的最长时效（秒）。默认情况下此值的设置为 30。此设置用于控制高速缓存文件后继续使用高速缓存的信息的时间长度。时间久于 MaxAge 的条目将由同一文件的新条目替换，如果该文件是通过高速缓存引用的。根据内容是否定期更新（即修改现有文件）来设置最长时效。例如，如果内容每天按定时间隔更新四次，可将最长时效设置为 21600 秒（6 小时）。否则，可考虑将最长时效设置为修改内容文件后希望为其上一版本提供的最长服务时间。
7. 输入要高速缓存的 "Maximum Number of Files"。默认情况下，此项设置为 1024。
8. 输入中等和小文件大小限制（字节）。默认情况下 "Medium File Size Limit" 的设置为 537600，"Small File Size Limit" 的设置为 2048。

   高速缓存对小文件、中等文件和大文件的处理方法不同。通过将文件映射到虚拟内存（目前仅限 UNIX/Linux 平台）来对中等文件的内容进行高速缓存。通过分配堆空间并将文件读入其中来对小文件的内容进行高速缓存。尽管会对大文件的相关信息进行高速缓存，但不会对大文件（比中等文件大的文件）的内容进行高速缓存。区别对待小文件和中等文件的好处是，当有大量小文件时，可以避免浪费虚拟内存的许多页面的一部分。因此，"Small File Size Limit" 的值通常比 VM 页面大小略低。
9. 设置中等和小文件空间。中等文件空间是指用于映射所有中等大小文件的虚拟内存的大小（字节）。默认情况下此值的设置为 10485760。小文件空间是指用于高速缓存的堆空间（包括用于高速缓存小文件的堆空间）的大小（字节）。对于 UNIX/Linux 平台，默认情况下此项的设置为 1048576。
10. 单击 "OK"。

11. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
12. 单击 "Restart Proxy Server" 按钮以应用更改。

查看 URL 数据库

可以查看记录的所有高速缓存的 URL 的名称和属性。所显示的 URL 信息为按访问协议和站点名称分组的高速缓存的文档列表。在 "Search" 字段中键入域名可限制列表中出现的 URL。通过访问此信息可以执行各种高速缓存管理功能，如废止和删除高速缓存中的文档。

查看数据库中的 URL

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "View URL Database" 链接。将显示 "View URL Database" 页面。
3. 单击 "Regenerate" 按钮可生成最新的高速缓存的 URL 列表。如果想要查看特定 URL 的信息，请在 "Search" 字段中输入 URL 或正则表达式，然后单击 "Search" 按钮。
4. 如果想要查看按域名和主机分组的高速缓存数据库信息，请从列表中选择域名。将出现该域中主机的列表。单击某个主机的名称，将出现一个 URL 列表。
5. 单击某个 URL 的名称。将出现有关该 URL 的详细信息。

废止和删除高速缓存中的文件

可以通过 "View URL Database" 页面来废止和删除高速缓存中的文档。

废止或删除高速缓存的 URL

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "View URL Database" 链接。将显示 "View URL Database" 页面。
3. 单击 "Regenerate" 按钮。该操作会生成高速缓存数据库的快照。该快照构成了执行其余步骤的基础。
4. 如果知道想要废止或删除的特定 URL，请在 "Search" 字段中输入该 URL 或匹配该 URL 的正则表达式，然后单击 "Search" 按钮。如果想要查看按域名和主机分组的 URL，请从列表中选择域名。将出现该域中主机的列表。单击某个主机的名称，将出现一个 URL 列表。

5. 要废止单个文件，请选择这些文件 URL 旁的 "Ex" 选项，然后单击 "Exp/Rem Marked" 按钮。要废止列表中的所有文件，请单击表单底部的 "Exp All" 按钮。要删除高速缓存中的单个文件，请选择这些文件 URL 旁的 "Rm" 选项，然后单击 "Exp/Rem Marked" 按钮。要删除列表中的所有文件，请单击 "Rem All" 按钮。
6. 单击 "Regenerate" 按钮以重新生成快照。

注 使用 "Ex" 或 "Rm" 选项时将处理关联的文件，但不会在快照中反映所做更改。需要重新生成快照，才能看到更改。

使用高速缓存批量更新

可以通过 "Cache Batch Update" 特性将文件预先装入指定的 Web 站点，或在代理服务器不忙时对高速缓存中已有的文档执行最新性检查。通过 "Set Cache Batch Updates" 页面可以创建、编辑和删除多批 URL 及启用和禁用批量更新。

创建批量更新

通过指定要进行批量更新的文件，可以主动（而不是根据需要）对文件进行高速缓存。可以通过代理服务器对当前位于高速缓存中的若干个文件执行最新性检查，或预先装入特定 Web 站点的多个文件。

创建批量更新

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Set Cache Batch Updates" 链接。将显示 "Set Cache Batch Updates" 页面。
3. 在 "Create/Select A Batch Update Configuration" 旁的下拉式列表中选择 "New and Create"。
4. 单击 "OK"。将显示 "Set Cache Batch Updates" 页面。
5. 在 "Name" 部分中输入新批量更新条目的名称。
6. 在页面的 "Source" 部分中单击与要创建的批量更新类型对应的单选按钮。如果要对高速缓存中的所有文档执行最新性检查，请单击第一个单选按钮。如果要从给定的源 URL 开始以递归方式高速缓存各 URL，请单击第二个单选按钮。
7. 在 "Source" 部分字段中，确定要在批量更新中使用的文档。
8. 在 "Exceptions" 部分中，确定要排除在批量更新之外的任何文件。
9. 在 "Resources" 部分中，输入最大同时连接数及要遍历的最大文档数。

10. 在 "Timing" 部分中输入生成批量更新的开始和结束时间。任何时刻均只能有一个批量更新处于活动状态，所以最好不要覆盖其他批量更新配置。
11. 单击 "OK"。

注 不必启用批量更新即可创建、编辑和删除批量更新配置。不过，如果要按照 "Set Cache Batch Updates" 页面中设置的时间来更新批量更新，就必须启用更新。

12. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
13. 单击 "Restart Proxy Server" 按钮以应用更改。

编辑或删除批量更新配置

可以使用 "Set Cache Batch Updates" 页面来编辑或删除批量更新。如果需要将某些文件排除在外或想更频繁地更新批次，可能需要对批量更新进行编辑。还可能需要彻底删除批量更新配置。

编辑或删除批量更新配置

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Set Cache Batch Updates" 链接。将显示 "Set Cache Batch Updates" 页面。
3. 如果要编辑批次，请选择该批次的名称，然后在 "Create/Select A Batch Update Configuration" 旁的下拉式列表中选择 "Edit"。如果要删除批次，请选择该批次的名称，然后从下拉式列表中选择 "Delete"。
4. 单击 "OK"。将显示 "Set Cache Batch Updates" 页面。
5. 根据需要修改信息。
6. 单击 "OK"。
7. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
8. 单击 "Restart Proxy Server" 按钮以应用更改。

使用高速缓存命令行界面

代理服务器自带若干个命令行实用程序，可以通过它们配置、更改、生成和修复高速缓存目录结构。这些实用程序中大多数与 Server Manager 页面的功能完全相同，但在需要进行维护调度时可能需要使用这些实用程序（例如，作为计时程序作业）。所有实用程序都位于 `extras` 目录中。

运行命令行实用程序

1. 在命令行提示符中转到 *server_root*/proxy-server*id* 目录。
2. 键入 **`./start -shell`**

   以下各节介绍各种实用程序。

建立高速缓存目录结构

代理服务器有一个称作 `cbuild` 的实用程序，它是一个脱机高速缓存数据库管理器。可以通过该实用程序使用命令行界面来创建新的高速缓存结构或修改现有的高速缓存结构。可以使用 Server Manager 页面来使代理服务器能够使用新创建的高速缓存。该实用程序不更新 `server.xml` 文件。`cbuild` 无法调整有多个分区的高速缓存的大小。`server.xml` 文件有一个称作 `CACHE` 的元素，该元素有一个 `cachecapacity` 参数。通过 `cbuild` 创建或修改高速缓存时，应在 `server.xml` 文件中手动更新 `cachecapacity` 参数。

```
<PARTITION partitionname="part1" partitiondir="/home/build/install9
/proxy-server1/cache" maxsize="1600" minspace="5" enabled="true"/>
<CACHE enabled="true" cachecapacity="2000" cachedir="/tmp/cache">
```

可以在两种模式下调用 `cbuild` 实用程序。第一种模式是：

```
cbuild -d conf-dir -c cache-dir -s cache size
cbuild -d conf-dir -c cache-dir -s cache size -r
```

例如：

```
cbuild -d server_root/proxy-serverid/config -c server_root/proxy-serverid/cache
-s 512
cbuild -d server_root/proxy-serverid/config -c server_root/proxy-serverid/cache
-s 512 -r
```

其中：

- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*/proxy-server*id*/config。
- *cache-dir* 是高速缓存结构的目录。
- *cache size* 是高速缓存可以增长到的最大大小。该选项不能与 *cache-dim* 参数一起使用。最大大小是 65135 MB。
- -r 调整现有高速缓存结构的大小（前提是它只有一个分区）。创建新高速缓存时此参数不是必需的。

可以运行 cbuild 的第二种模式是：

```
cbuild -d conf-dir -c cache-dir -n cache-dim
```

```
cbuild -d conf-dir -c cache-dir -n cache-dim -r
```

例如：

```
cbuild -d server_root/proxy-serverid/config -c server_root/proxy-serverid/cache
-n 3
```

```
cbuild -d server_root/proxy-serverid/config -c server_root/proxy-serverid/cache
-n 3 -r
```

其中：

- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*/proxy-server*id*/config。
- *cache-dir* 是高速缓存结构的目录。
- *cache-dim* 确定区段数。例如，图 12-1 中的区段显示为 s3.4，其中的 3 表示大小。*cache-dim* 的默认值是 0，最大值是 8。
- -r 调整现有高速缓存结构的大小（前提是它只有一个分区）。创建新高速缓存时此参数不是必需的。

管理高速缓存 URL 列表

代理服务器有一个称作 urldb 的实用程序，用于管理高速缓存中的 URL 列表。可以使用该实用程序列出高速缓存的 URL。也可以有选择地废止和删除高速缓存数据库中高速缓存的对象。

可以根据 -o 选项将 urldb 命令分为三个组：

- 域
- 站点

- url

要列出域，请在命令行中输入以下内容：

```
urldb -o matching_domains -e reg_exp -d conf-dir
```

例如：

```
urldb -o matching_domains -e ".*phoenix.*" -d
server_root/proxy-serverid/config
```

其中

- matching_domains 列出匹配正则表达式的域
- *reg_exp* 是所使用的正则表达式
- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*/proxy-server*id*/config。

要列出域中所有匹配的站点，请在命令行中输入以下内容：

```
urldb -o matching_sites_in_domain -e reg_exp -m domain_name -d conf-dir
```

例如：

```
urldb -o matching_sites_in_domain -e ".*atlas" -m phoenix.com -d
server_root/proxy-serverid/config
```

其中

- matching_sites_in_domain 列出域中匹配正则表达式的所有站点
- *reg_exp* 是所使用的正则表达式
- *domain_name* 是域的名称
- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*/proxy-server*id*/config

要列出所有匹配的站点，请在命令行中输入以下内容：

```
urldb -o all_matching_sites -e reg_exp -d conf-dir
```

例如：

```
urldb -o all_matching_sites -e ".*atlas.*" -d server_root/proxy-serverid/config
```

其中

- all_matching_sites 列出匹配正则表达式的所有站点
- *reg_exp* 是所使用的正则表达式

- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*/proxy-server*id*/config

要列出站点中匹配的 url，请在命令行中输入以下内容：

```
urldb -o matching_urls_from_site -e reg_exp -s site_name -d conf-dir
```

例如：

```
urldb -o matching_urls_from_site -e "http://.*atlas.*" -s atlas.phoenix.com
-d server_root/proxy-serverid/config
```

其中

- matching_urls_from_site 列出站点中匹配正则表达式的所有 url
- *reg_exp* 是所使用的正则表达式
- *site_name* 是站点的名称
- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*/proxy-server*id*/config

要废止或删除站点中匹配的 url，请在命令行中输入以下内容：

```
urldb -o matching_urls_from_site -e reg_exp -s site_name -x e -d conf-dir
```

```
urldb -o matching_urls_from_site -e reg_exp -s site_name -x r -d conf-dir
```

例如：

```
urldb -o matching_urls_from_site -e "http://.*atlas.*" -s atlas.phoenix.com
-x e -d iserver_root/proxy-serverid/config
```

其中

- matching_urls_from_site 列出站点中匹配正则表达式的所有 url
- *reg_exp* 是所使用的正则表达式
- *site_name* 是站点的名称
- -x e 是用于废止高速缓存数据库中匹配的 URL 的选项。该选项不能用于域和站点模式
- -x r 是用于删除高速缓存数据库中匹配的 URL 的选项
- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*/proxy-server*id*/config

要列出所有匹配的 url，请在命令行中输入以下内容：

```
urldb -o all_matching_urls -e reg_exp -d conf-dir
```

例如：

```
urldb -o all_matching_urls -e ".*cgi-bin.*" -d
server_root/proxy-serverid/config
```

其中

- `all_matching_urls` 列出匹配正则表达式的所有 URL
- *reg_exp* 是所使用的正则表达式
- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*`/proxy-server`*id*`/config`

要废止或删除所有匹配的 url，请在命令行中输入以下内容：

```
urldb -o all_matching_urls -e reg_exp -x e -d conf-dir
urldb -o all_matching_urls -e reg_exp -x r -d conf-dir
```

例如：

```
urldb -o all_matching_urls -e ".*cgi-bin.*" -x e -d
server_root/proxy-serverid/config
```

其中

- `all_matching_urls` 列出匹配正则表达式的所有 URL
- *reg_exp* 是所使用的正则表达式
- `-x e` 是用于废止高速缓存数据库中匹配的 URL 的选项
- `-x r` 是用于删除高速缓存数据库中匹配的 URL 的选项
- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*`/proxy-server`*id*`/config`

要废止或删除 URL 列表，请在命令行中输入以下内容：

```
urldb -l url-list -x e -e reg_exp -d conf-dir
urldb -l url-list -x r -e reg_exp -d conf-dir
```

例如：

```
urldb -l url.lst -x e -e ".*cgi-bin.*" -d server_root/proxy-serverid/config
```

其中

- `url-list` 是需要废止的 URL 列表。该选项可用于提供 URL 列表。
- `-x e` 是用于废止高速缓存数据库中匹配的 URL 的选项。

- `-x r` 是用于删除高速缓存数据库中匹配的 URL 的选项。
- *reg_exp* 是所使用的正则表达式
- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*/proxy-server*id*/config。

管理高速缓存垃圾收集

可以通过 cachegc 实用程序将可能已过期或因存在时间过久而不能在目录中高速缓存（根据高速缓存大小约束）的对象清理出高速缓存数据库。

注 确保使用 cachegc 实用程序时代理服务器实例中没有运行 CacheGC。

可按以下方式使用 cachegc 实用程序：

cachegc -f *leave-fs-full-percent* -u *gc-high-margin-percent* -l *gc-low-margin-percen*t -e *extra-margin-percen*t -d *conf-dir*

例如：

cachegc -f 50 -u 80 -l 60 -e 5 -d *server_root*/proxy-server*id*/config

其中

- *leave-fs-full-percent* 确定高速缓存分区大小的百分比，低于该值时将不进行垃圾收集
- *gc-high-margin-percent* 控制最大高速缓存大小的百分比，达到该值时即会触发垃圾收集
- *gc-low-margin-percent* 控制作为垃圾收集器目标的最大高速缓存大小的百分比
- *extra-margin-percent* 由垃圾收集器用来确定要删除的高速缓存的百分比。
- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*/proxy-server*id*/config。

管理批量更新

bu 实用程序用于更新高速缓存，它在两种模式下工作。在第一种模式下，该实用程序循环遍历高速缓存数据库并通过发送对每个 URL 的 HTTP 请求更新高速缓存中存在的所有 URL。在第二种模式中，该实用程序从给定 URL 开始对从该 URL 到所指定深度的 URL 的所有链接执行广度优先遍历，获取页面并将其置于高速缓存中。bu 是一种符合 RFC 标准的爬虫程序。

`bu -n` *hostname* `-p` *port* `-t` *time-lmt* `-f` *contact-address* `-s` *sleep-time* `-o` *object* `-r n -d` *conf-dir*

例如：

`bu -n phoenix -p 80 -t 3600 -f admin@phoenix.com -s 60 -o nova -r n -d` *server_root*`/proxy-server`*id*`/config`

其中

- *hostname* 是运行代理服务器的机器的主机名。默认值为 localhost。
- *port* 是代理服务器运行时所使用的端口。默认端口是 `8080`。
- *time-lmt* 是实用程序运行的时间限制
- *contact-address* 确定将在 `bu` 发送来的 HTTP 请求中发送的联系地址。默认值是 `worm@proxy-name`。
- *sleep-time* 是两次连续请求间的休眠时间。默认值为 5 秒。
- *object* 是在当前正在执行的 `bu.conf` 中指定的对象
- `-r n` 选项确定是否遵循 `robot.txt` 策略。默认值为 `y`。
- *conf-dir* 是代理服务器实例的配置目录。它位于以下路径 *server_root*`/proxy-server`*id*`/config`。

使用 Internet 高速缓存协议 (ICP)

关于 ICP

Internet 高速缓存协议 (ICP) 是一种对象位置协议，通过该协议各高速缓存可以彼此通信。高速缓存可以就是否存在高速缓存的 URL 及这些 URL 的最佳检索位置，使用 ICP 发送查询和回复。在典型的 ICP 交换中，一个高速缓存会将有关特定 URL 的 ICP 查询发送给邻近的所有高速缓存。然后，这些高速缓存将回送 ICP 回复，指出其是否包含该 URL。如果这些高速缓存不包含该 URL，则回送 "MISS"。如果的确包含该 URL，则回送 "HIT"。

通过 ICP 邻域进行路由选择

ICP 可用于位于不同管理域中的代理服务器间的通信。它使某个管理域中的代理服务器高速缓存能够与另一个管理域中的代理服务器高速缓存进行通信。如果若干个代理服务器想进行通信，但无法全部从一个主代理服务器进行配置（因为它们处于代理服务器阵列中），则在这种情况下使用 ICP 进行通信是有效的。图 12-3 显示了不同管理域中代理服务器间的 ICP 交换。

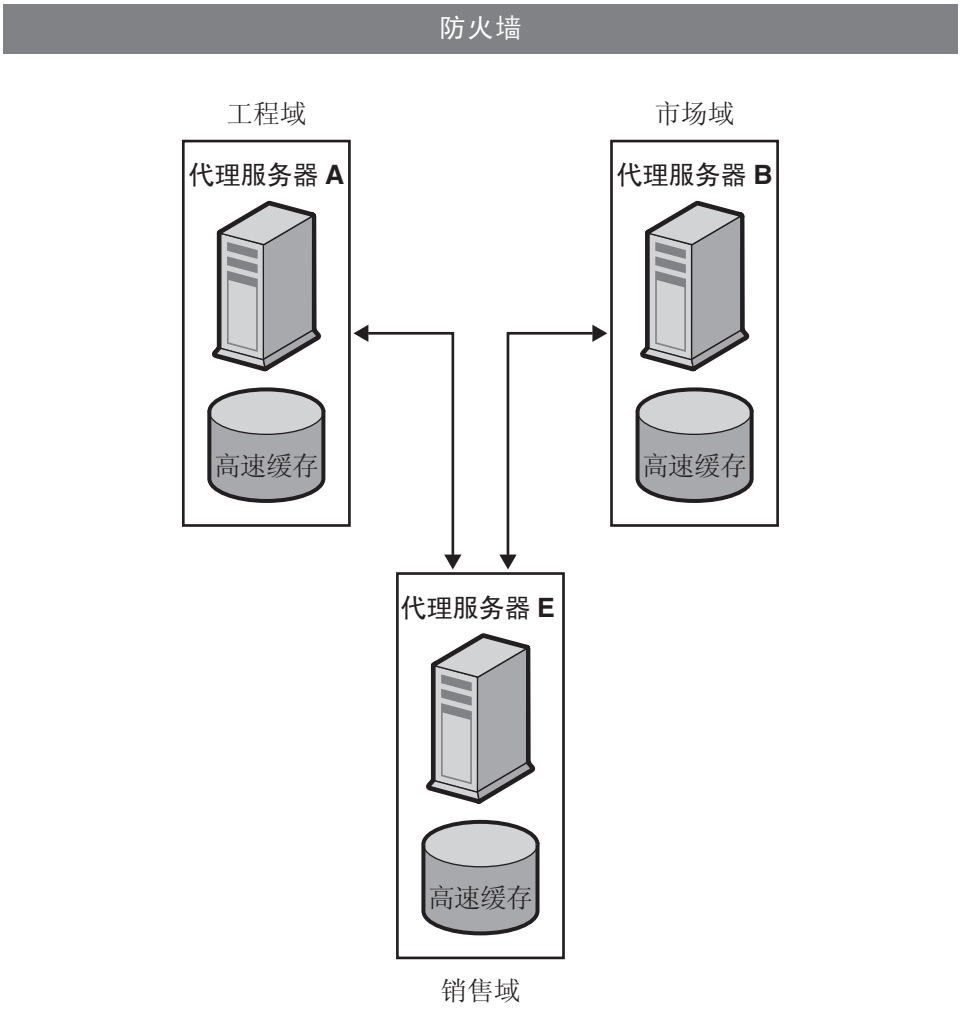
通过 ICP 彼此进行通信的代理服务器称作**近邻**。一个 ICP 邻域中最多只能有 64 个近邻。ICP 邻域中有两种类型的近邻：**父代理服务器**和**同级代理服务器**。如果其他近邻都没有请求的 URL，则只有父代理服务器方可访问远程服务器。ICP 邻域可以没有父代理服务器，也可以有一个以上的父代理服务器。ICP 邻域中的任何**非**父代理服务器近邻均被视为同级代理服务器。除非同级代理服务器被标记为 ICP 的默认路由并且 ICP 使用该默认路由，否则，同级代理服务器不能从远程服务器检索文档。

可以使用**轮询轮次**确定近邻接收查询的顺序。一个轮询轮次是一个 ICP 查询循环。必须为每个近邻分配一个轮询轮次。如果在轮询轮次一中配置了所有近邻，将在一个循环中查询所有近邻。也就是说，将同时查询所有近邻。如果将一些近邻配置在轮询轮次 2 中，将首先查询轮询轮次一中的所有近邻，如果没有近邻返回 "HIT"，将查询轮询轮次二中的所有代理服务器。轮询轮次的最大值是二。

因为 ICP 父代理服务器可能成为网络瓶颈，所有可以使用轮询轮次来减轻其负载。一个常用的设置是将所有同级代理服务器配置在轮询轮次一中，而将所有父代理服务器配置在轮询轮次二中。这样当本地代理服务器请求 URL 时，请求将首先转到邻域中的所有同级代理服务器。如果所有同级代理服务器都没有请求的 URL，将把请求转给父代理服务器。如果父代理服务器也没有请求的 URL，将从远程服务器进行检索。

ICP 邻域中的每个近邻必须至少有一个运行着的 ICP 服务器。如果某个近邻没有运行着的 ICP 服务器，将无法响应来自其近邻的 ICP 请求。如果 ICP 服务器没有运行，启用代理服务器上的 ICP 时将会启动 ICP 服务器。

图 12-3 ICP 交换



设置 ICP

1. 向 ICP 邻域添加父代理服务器。（只有在想要让父代理服务器位于 ICP 领域中时才需要执行此步骤。）有关向 ICP 邻域添加父代理服务器的更多信息，参见第 259 页的“向 ICP 邻域添加父代理服务器”。
2. 向 ICP 邻域添加同级代理服务器。有关向 ICP 邻域添加同级代理服务器的更多信息，参见第 261 页的“向 ICP 邻域添加同级代理服务器”。

3. 配置 ICP 邻域中的每个近邻。有关配置 ICP 近邻的更多信息，参见第 262 页的“配置单个 ICP 近邻”。
4. 启用 ICP。有关启用 ICP 的信息，参见第 264 页的“启用 ICP”。
5. 如果代理服务器的 ICP 邻域中有同级代理服务器或父代理服务器，请通过 ICP 邻域启用路由选择。有关通过 ICP 邻域启用路由选择的更多信息，参见第 264 页的“启用通过 ICP 邻域进行路由选择”。

向 ICP 邻域添加父代理服务器

向 ICP 邻域添加父代理服务器

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Configure ICP" 链接。将显示 "Configure ICP" 页面。
3. 在页面的 "Parent List" 部分中单击 "Add" 按钮。将显示 "ICP Parent" 页面。
4. 在 "Machine Address" 字段中输入要向 ICP 邻域添加的父代理服务器的 IP 地址或主机名。
5. 在 "ICP Port" 字段中输入父代理服务器侦听 ICP 消息所使用的端口号。
6. 在 "Multicast Address" 字段中，可以输入父代理服务器侦听的多址广播地址。多址广播地址是指多个服务器可以侦听的 IP 地址。代理服务器可以使用多址广播地址将一个查询发送到正在侦听该多址广播地址的所有近邻均可见的网络，从而不必将查询分别发送给每个近邻。使用多址广播是可选的。

注 不同轮询轮次中的近邻不能侦听同一多址广播地址。

7. 在 "TTL" 字段中，输入要将多址广播消息转发到的子网数。如果 "TTL" 的设置为 1，只会将多址广播消息转发到本地子网。如果 "TTL" 为 2，消息将发往隔一级的所有子网，依此类推。

注 多址广播使得两个不相关的近邻可以相互发送 ICP 消息。因此，如果想要阻止不相关的近邻接收来自 ICP 邻域中的代理服务器的 ICP 消息，应在 "TTL" 字段中设置较低的 TTL 值。

8. 在 "Proxy Port" 字段中，输入父代理服务器的端口。

9. 在 "Polling Round" 下拉式列表中，选择希望父代理服务器所处的轮询轮次。默认轮询轮次为 1。
10. 单击 "OK"。
11. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
12. 单击 "Restart Proxy Server" 按钮以应用更改。

在 ICP 邻域中编辑父代理服务器配置

编辑父代理服务器配置

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 选择 "Configure ICP" 链接。将显示 "Configure ICP" 页面。
3. 单击要编辑的父代理服务器旁的单选按钮。
4. 单击 "Edit" 按钮。
5. 修改相应的信息。
6. 单击 "OK"。
7. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
8. 单击 "Restart Proxy Server" 按钮以应用更改。

删除 ICP 邻域中的父代理服务器

删除 ICP 邻域中的父代理服务器

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 选择 "Configure ICP" 链接。将显示 "Configure ICP" 页面。
3. 单击要删除的父代理服务器旁的单选按钮。
4. 单击 "Delete" 按钮。
5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

向 ICP 邻域添加同级代理服务器

向 ICP 邻域添加同级代理服务器

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 选择 "Configure ICP" 链接。将显示 "Configure ICP" 页面。
3. 在页面的 "Sibling List" 部分中单击 "Add" 按钮。将显示 "ICP Sibling" 页面。
4. 在 "Machine Address" 字段中，输入要向 ICP 邻域添加的同级代理服务器的 IP 地址或主机名。
5. 在 "Port" 字段中，输入同级代理服务器侦听 ICP 消息所使用的端口号。
6. 在 "Multicast Address" 字段中，输入同级代理服务器侦听的多址广播地址。多址广播地址是指多个服务器可以侦听的 IP 地址。代理服务器可以使用多址广播地址将一个查询发送到正在侦听该多址广播地址的所有近邻均可见的网络，从而不必将查询分别发送给每个近邻。

注	不同轮询轮次中的近邻不应侦听同一多址广播地址。

7. 在 "TTL" 字段中，输入要将多址广播消息转发到的子网数。如果 "TTL" 的设置为 1，只会将多址广播消息转发到本地子网。如果 "TTL" 为 2，消息将发往隔一级的所有子网。

注	多址广播使得两个不相关的近邻可以相互发送 ICP 消息。因此，如果想要阻止不相关的近邻接收来自 ICP 邻域中的代理服务器的 ICP 消息，应在 "TTL" 字段中设置较低的 TTL 值。

8. 在 "Proxy Port" 字段中，输入同级代理服务器的端口。
9. 在 "Polling Round" 下拉式列表中，选择希望同级代理服务器所处的轮询轮次。默认轮询轮次为 1。
10. 单击 "OK"。
11. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
12. 单击 "Restart Proxy Server" 按钮以应用更改。

在 ICP 邻域中编辑同级代理服务器配置

编辑同级代理服务器配置

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 选择 "Configure ICP" 链接。将显示 "Configure ICP" 页面。
3. 单击要编辑的同级代理服务器旁的单选按钮。
4. 单击 "Edit" 按钮。
5. 修改相应的信息。
6. 单击 "OK"。
7. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
8. 单击 "Restart Proxy Server" 按钮以应用更改。

删除 ICP 邻域中的同级代理服务器

删除 ICP 邻域中的同级代理服务器

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 选择 "Configure ICP" 链接。将显示 "Configure ICP" 页面。
3. 单击要删除的同级代理服务器旁的单选按钮。
4. 单击 "Delete" 按钮。
5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

配置单个 ICP 近邻

需要在 ICP 邻域中配置每个近邻（或称本地代理服务器）。

在 ICP 邻域中配置本地代理服务器

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 选择 "Configure ICP" 链接。将显示 "Configure ICP" 页面。
3. 在 "Binding Address" 字段中，输入近邻服务器将要绑定到的 IP 地址。
4. 在 "Port" 字段中，输入近邻服务器侦听 ICP 所使用的端口号。

5. 在 "Multicast Address" 字段中，输入近邻侦听的多址广播地址。多址广播地址是指多个服务器可以侦听的 IP 地址。代理服务器可以使用多址广播地址将一个查询发送到正在侦听该多址广播地址的所有近邻均可见的网络，从而不必将查询分别发送给每个近邻。

   如果同时为近邻指定了多址广播地址和绑定地址，近邻将使用绑定地址发送回复，使用多址广播进行侦听。如果既未指定绑定地址也未指定多址广播地址，操作系统将决定使用哪个地址发送数据。

6. 在 "Default Route" 字段中，输入代理服务器的名称或 IP 地址，当邻近代理均未做出“命中”响应时，近邻应将请求路由到此代理服务器。如果在此字段中输入文字 origin，或将其留为空白，则默认情况下将会路由至源服务器。

注 如果从 "No Hit Behavior" 下拉式列表中选择 "first responding parent"，在 "Default Route" 字段中输入的路由将不起作用。如果选择默认的无命中行为，代理服务器将只使用该路由。

7. 在第二个 "Port" 字段中，输入默认路由机器的端口号，即在 "Default Route" 字段中输入的值。

8. 在 "On No Hits, Route Through" 下拉式列表中，选择当 ICP 邻域中所有同级代理服务器的高速缓存中均无请求的 URL 时近邻的行为。可以选择：

   - **first responding parent**。近邻将通过最先做出“未命中”响应的父代理服务器检索请求的 URL
   - **default route**。近邻将通过在 "Default Route" 字段中指定的机器检索请求的 URL。

9. 在 "Server Count" 字段中，输入将要服务于 ICP 请求的进程数。

10. 在 "Timeout" 字段中，输入每一轮次中近邻等待 ICP 响应的最大时间长度。

11. 单击 "OK"。

12. 单击 "Restart Required"。将显示 "Apply Changes" 页面。

13. 单击 "Restart Proxy Server" 按钮以应用更改。

启用 ICP

启用 ICP

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Configure System Preferences" 链接。将显示 "Configure System Preferences" 页面。
3. 选择对应于 ICP 的 "Yes" 单选按钮。
4. 单击 "OK"。
5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

启用通过 ICP 邻域进行路由选择

启用通过 ICP 邻域进行路由选择

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Set Routing Preferences" 链接。将显示 "Set Routing Preferences" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮来输入正则表达式，然后单击 "OK"。
4. 选择文本 "Route Through" 旁的单选按钮。
5. 选中 "ICP" 旁的复选框。
6. 如果希望客户机直接从拥有文档的 ICP 近邻检索文档，而不是通过另一个近邻来获取文档，请选中文本 "redirect" 旁的复选框。
7. 单击 "OK"。

注意 当前任何客户机都不支持重定向，所以目前不要使用该特性。

注 只有当代理服务器在 ICP 邻域中有其他同级代理服务器或父代理服务器时，才需要启用通过 ICP 邻域进行路由选择。如果代理服务器是另一个代理服务器的父代理服务器，并且它本身没有任何同级代理服务器或父代理服务器，则只需要为该代理服务器启用 ICP，而不需要启用通过 ICP 邻域进行路由选择。

8. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

使用代理服务器阵列

关于代理服务器阵列

可以通过分布式高速缓存的代理服务器阵列将多个代理服务器作为一个高速缓存来使用。也就是说，阵列中的每个代理服务器都将包含不同的高速缓存的 URL，浏览器或下游代理服务器可以检索这些 URL。代理服务器阵列可以防止有多个代理服务器时经常发生的高速缓存重复。代理服务器阵列通过基于散列的路由选择将请求路由到代理服务器阵列中正确的高速缓存中。

代理服务器阵列也允许增量式可伸缩性。也就是说，如果决定将另一个代理服务器添加到代理服务器阵列，每个成员的高速缓存都不会失效。只会将每个成员高速缓存中的 URL 的 $1/n$（其中 n 是阵列中的代理服务器数）重新分配给其他成员。

通过代理服务器阵列进行路由选择

对于通过代理服务器阵列的每个请求，散列函数将根据请求的 URL、代理服务器的名称及代理服务器的负载因子为阵列中的每个代理服务器分配一个分数，然后将请求路由到分数最高的代理服务器。

因为 URL 请求可能来自客户机和代理服务器，所以通过代理服务器阵列进行的路由选择有两种类型：**客户机到代理服务器路由选择**和**代理服务器到代理服务器路由选择**。

在客户机到代理服务器路由选择中，客户机使用代理服务器自动配置 (PAC) 机制来确定通过哪个代理服务器。不过，客户机不是使用标准的 PAC 文件，而是使用一种特殊的 PAC 文件，该文件通过计算散列算法来为请求的 URL 确定合适的路由，图 12-4 显示了客户机到代理服务器的路由选择。

在图 12-4 中，代理服务器阵列的每个成员均加载并轮询主代理服务器，以确定是否有对 PAT 文件的更新。客户机一旦下载了 PAC 文件，则只有在配置发生变化时才需要再次下载该文件。客户机通常在重新启动时下载 PAC 文件。

代理服务器可以根据通过管理界面建立的代理服务器阵列成员资格表 (PAT) 规格自动生成特殊的 PAC 文件。

在代理服务器到代理服务器路由选择中，代理服务器使用 PAT（代理服务器阵列表）文件而不是客户机使用的 PAC 文件来计算散列算法。PAT 文件是一种 ASCII 文件，它包含有关代理服务器阵列的信息，如代理服务器的机器名称、IP 地址、端口、负载因子、高速缓存大小等。要在服务器上计算散列算法，使用 PAT 文件比使用 PAC 文件（该文件是一种 JavaScript 文件，必须在运行时对其进行解析）要高效得多。不过，大多数客户机无法识别 PAT 文件格式，因此必须使用 PAC 文件。图 12-5 显示了代理服务器到代理服务器路由选择。

将在代理服务器阵列中的一个代理服务器（即主代理服务器）上创建 PAT 文件。代理服务器管理员必须确定将哪一个代理服务器作为主代理服务器。管理员可以通过此主代理服务器更改 PAT 文件，之后代理服务器阵列的所有其他成员可以手动或自动方式轮询主代理服务器来获悉这些更改。可以将每个成员都配置为自动根据这些更改生成 PAC 文件。

也可以将代理服务器阵列链接在一起，进行分层结构路由选择。如果代理服务器将收到的请求通过上游代理服务器阵列进行路由，则该阵列即为父代理服务器阵列。父代理服务器阵列是代理服务器经过的代理服务器阵列。也就是说，如果客户机从代理服务器 X 请求文档，而代理服务器 X 没有该文档，它将把请求发送给代理服务器阵列 Y，而不是直接将请求发送到远程服务器。因此，代理服务器阵列 Y 是一个父代理服务器阵列。在图 12-5 中，代理服务器阵列 1 是代理服务器阵列 2 的父代理服务器阵列。代理服务器阵列 2 的成员会加载并进行轮询，以确定是否有对父代理服务器阵列 PAT 文件的更新。它通常轮询父代理服务器阵列中的主代理服务器。将使用下载的 PAT 文件计算请求的 URL 的散列算法，之后代理服务器阵列 2 的成员就可以从代理服务器阵列 1 中分数最高的代理服务器中检索请求的 URL。在图 12-5 中，对于客户机请求的 URL，代理服务器 B 的分数最高。

图 12-4 客户机到代理服务器路由选择

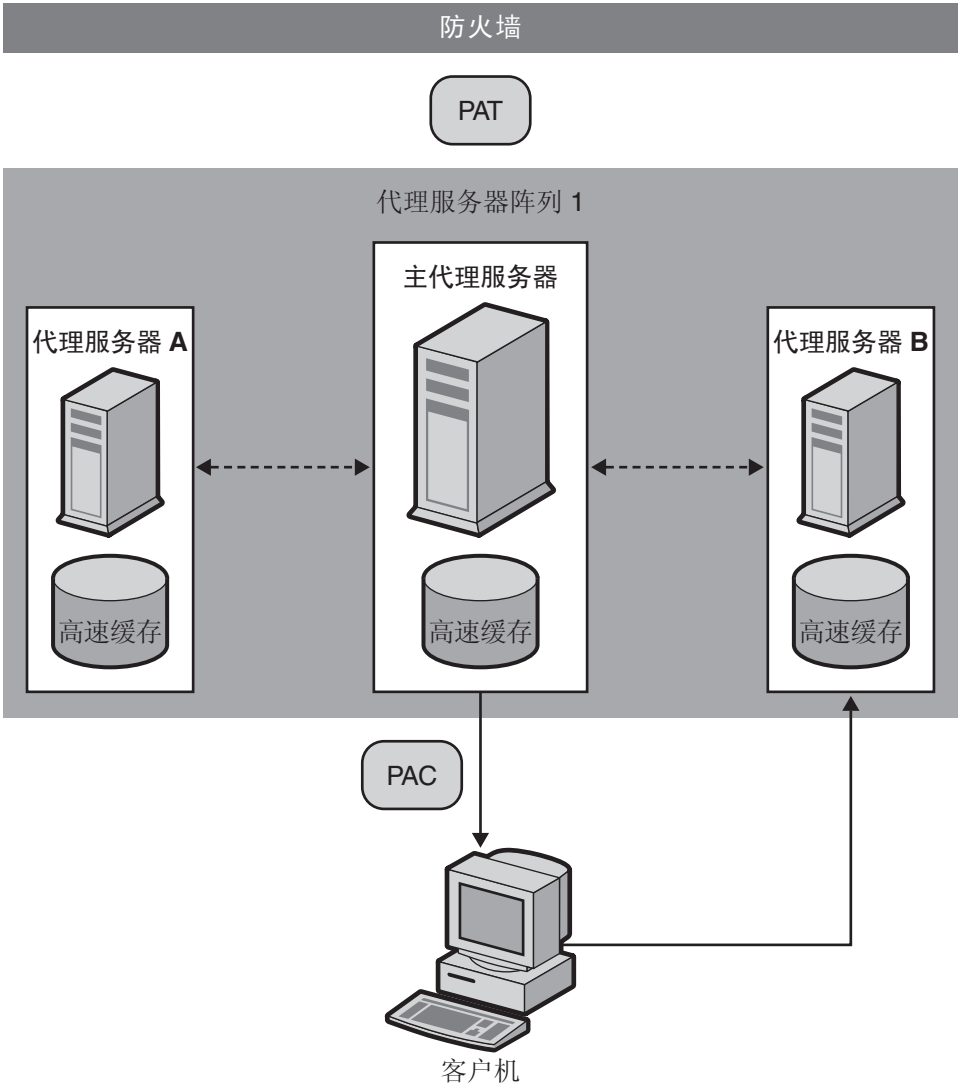
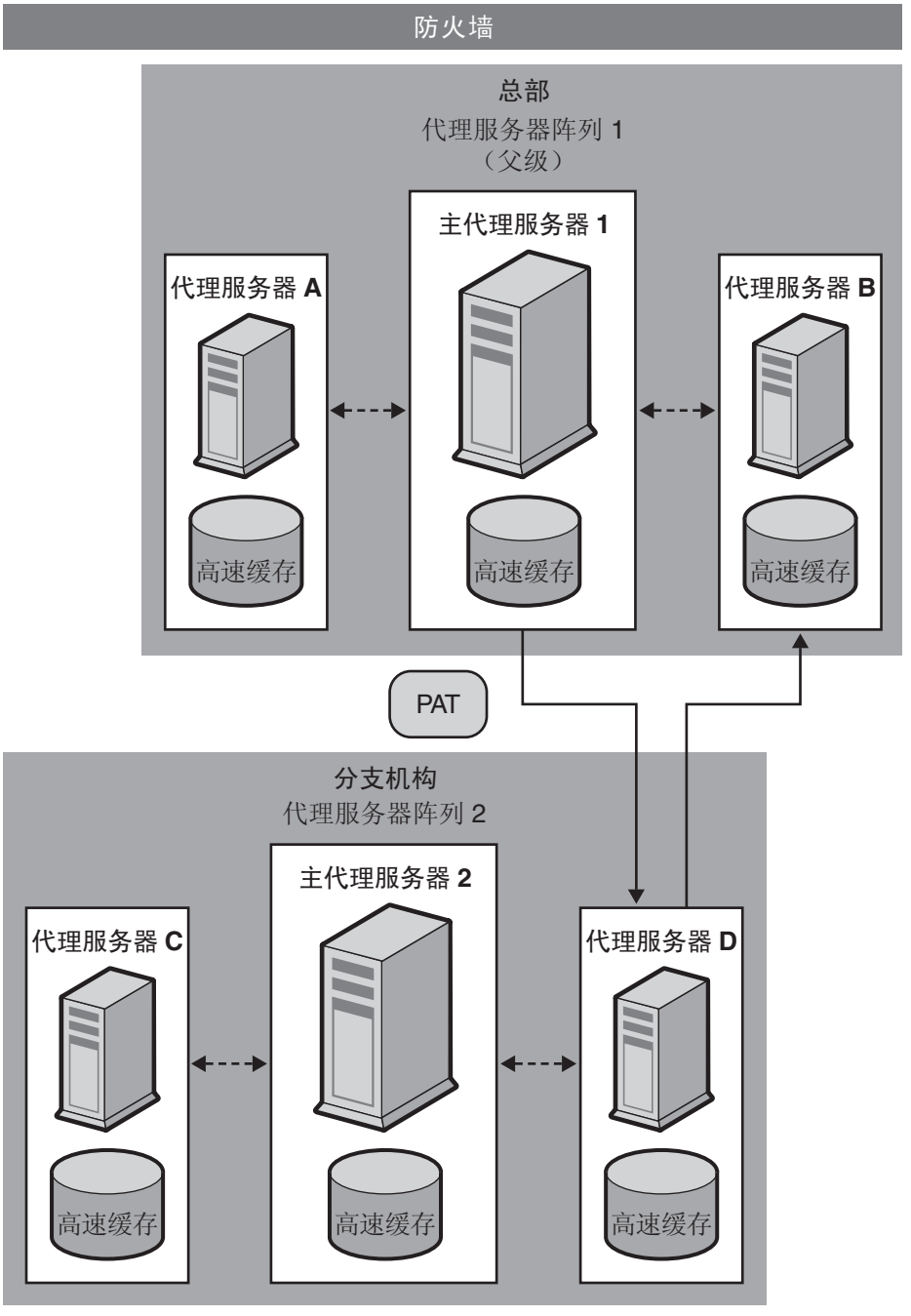


图 12-5 代理服务器到代理服务器路由选择



设置代理服务器阵列

1. 在主代理服务器中执行以下步骤：

   a. 创建代理服务器阵列。有关创建成员列表的更多信息，参见第 270 页的“创建代理服务器阵列成员列表”。

   b. 使用 PAT 文件生成 PAC 文件。如果使用客户机到代理服务器路由选择，只需生成 PAC 文件即可。有关使用 PAT 文件生成 PAC 文件的更多信息，参见第 275 页的“使用 PAT 文件生成 PAC 文件”。

   c. 配置阵列的主成员。有关配置主成员的更多信息，参见第 272 页的“配置代理服务器阵列成员”。

   d. 启用通过代理服务器阵列进行路由选择。有关启用通过代理服务器阵列进行路由选择的更多信息，参见第 273 页的“启用通过代理服务器阵列进行路由选择”。

   e. 创建 PAT 映射以将 URL “/pat” 映射到 PAT 文件。

   f. 启用代理服务器阵列。有关启用代理服务器阵列的更多信息，参见第 274 页的“启用代理服务器阵列”。

2. 在每个非主代理服务器中执行以下步骤：

   a. 配置阵列的非主成员。有关配置非主成员的更多信息，参见第 272 页的“配置代理服务器阵列成员”

   b. 启用通过代理服务器阵列进行路由选择。有关启用通过代理服务器阵列进行路由选择的更多信息，参见第 273 页的“启用通过代理服务器阵列进行路由选择”。

   c. 启用代理服务器阵列。有关启用代理服务器阵列的更多信息，参见第 274 页的“启用代理服务器阵列”。

注 如果代理服务器阵列要通过父代理服务器阵列进行路由，则还需要启用父代理服务器阵列并将每个成员配置为通过父代理服务器阵列进行路由以获得所需的 URL。有关父代理服务器阵列的更多信息，参见第 276 页的“通过父代理服务器阵列进行路由选择”。

创建代理服务器阵列成员列表

只应在阵列的主代理服务器中创建和更新代理服务器阵列成员列表。代理服务器阵列成员列表只需创建一次，但可以随时对其进行修改。通过创建代理服务器阵列成员列表，将生成分布到阵列中的所有代理服务器及任何下游代理服务器的 PAT 文件。

注意 只应通过阵列中的主代理服务器对代理服务器阵列成员列表进行更改或添加。阵列的所有其他成员只能读取成员列表。

1. 访问 Server Manager 并单击 "Caching" 选项卡
2. 单击 "Configure Proxy Array" 链接。将显示 "Configure Proxy Array" 页面。
3. 在 "Array name" 字段中，输入阵列的名称。
4. 在 "Reload Configuration Every" 字段中，输入 PAT 文件各次轮询间隔的分钟数。
5. 单击 "Array Enabled" 复选框。
6. 单击 "Create" 按钮。

注 务必在开始向成员列表添加成员之前单击 "OK"。

注 代理服务器阵列创建后 "Create" 按钮将变成 "OK" 按钮。

7. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
8. 为代理服务器阵列中的每个成员输入以下内容，然后单击 "OK"：
   - **Name**。要添加到成员列表中的代理服务器的名称
   - **IP Address**。要添加到成员列表中的代理服务器的 IP 地址
   - **Port**。此为成员针对 PAT 文件进行轮询所使用的端口。
   - **Load Factor**。一个反映应通过成员进行路由的相对负载的整数。
   - **Status**。成员的状态。此值可以为 "on" 或 "off"。如果禁用了某个代理服务器阵列成员，将会通过另一成员再次路由该成员的请求。

注 添加其他成员前应先添加主成员。

注 为要添加的每个代理服务器阵列成员输入信息后，请务必单击 "OK"。

9. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
10. 单击 "Restart Proxy Server" 按钮以应用更改。

编辑代理服务器阵列成员列表信息

可以随时更改代理服务器阵列成员列表中各成员的信息。只能通过主代理服务器编辑代理服务器阵列成员列表。

注意 只应通过阵列中的主代理服务器对代理服务器阵列成员列表进行更改或添加。如果通过阵列的任何其他成员修改此列表，所有更改都将丢失。

编辑代理服务器阵列中任何成员的成员列表信息

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Configure Proxy Array" 链接。将显示 "Configure Proxy Array" 页面。
3. 在 "Member" 列表中，选择要编辑的成员旁的单选按钮。
4. 单击 "Edit" 按钮。将显示 "Configure Proxy Array Member" 页面。
5. 编辑相应的信息。
6. 单击 "OK"。
7. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
8. 单击 "Restart Proxy Server" 按钮以应用更改。

注 如果想使更改生效并将其分布到代理服务器阵列的各个成员，需要更新 "Configure Proxy Array" 页面中的 "Configuration ID"，然后单击 "OK"。要更新配置 ID，只需将其值增加一即可。

删除代理服务器阵列成员

如果删除代理服务器阵列成员，将把其从代理服务器阵列中删除。只能通过主代理服务器删除代理服务器阵列成员。

注意 只应通过阵列中的主代理服务器对代理服务器阵列成员列表进行更改或添加。如果通过阵列的任何其他成员修改此列表，所有更改都将丢失。

删除代理服务器阵列的成员

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Configure Proxy Array" 链接。将显示 "Configure Proxy Array" 页面。
3. 在 "Member" 列表中，选择要删除的成员旁的单选按钮。
4. 单击 "Delete" 按钮。

注 如果想使更改生效并将其分布到代理服务器阵列的各个成员，需要更新 "Configure Proxy Array" 页面中的 "Configuration ID"，然后单击 "OK"。要更新配置 ID，只需将其值增加一即可。

5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

配置代理服务器阵列成员

只需对代理服务器阵列中的每个成员进行一次配置，而且必须通过成员本身进行配置。不能通过阵列的某个成员配置另一个成员。还需要配置主代理服务器。

配置代理服务器阵列的每个成员

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Configure Proxy Array Member" 链接。将显示 "Configure Proxy Array Member" 页面。
3. 在 "Proxy Array" 部分中，通过选择相应的单选按钮来指示成员是否需要轮询 PAT 文件。选项包括：
   - **Non-Master Member。**如果配置的成员不是主代理服务器，应选择此选项。任何不是主代理服务器的代理服务器阵列成员均需轮询 PAT 文件，以从主代理服务器检索它。

- **Master Member。**如果配置的是主代理服务器，应选择此选项。如果配置的是主代理服务器，PAT 文件将是本地文件，不需要进行轮询。

4. 在 "Poll Host" 字段中输入将要针对 PAT 文件进行轮询的主代理服务器的名称。
5. 在 "Port" 字段中输入主代理服务器接受 HTTP 请求的端口。
6. 在 "URL" 字段中输入主代理服务器上 PAT 文件的 URL。如果已在主代理服务器上创建了一个将 PAT 文件映射到 URL `/pat` 的 PAT 映射，应在 "URL" 字段中输入 **`/pat`**。
7. 在 "Headers File" 字段中，输入含有任何特殊标头的文件的完整路径名，这些标头必须与 PAT 文件的 HTTP 请求（如验证信息）一起发送。该字段为可选字段。
8. 单击 "OK"。
9. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
10. 单击 "Restart Proxy Server" 按钮以应用更改。

启用通过代理服务器阵列进行路由选择

启用通过代理服务器阵列进行路由选择

1. 访问 Server Manager 并单击 "Routing" 选项卡。
2. 单击 "Set Routing Preferences" 链接。将显示 "Set Routing Preferences" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮来输入正则表达式，然后单击 "OK"。
4. 选择 "Route Through" 选项。
5. 选择代理服务器阵列和 / 或父代理服务器阵列的复选框。
6. 如果选择通过代理服务器阵列进行路由并要将请求重定向到另一个 URL，请选中 "redirect" 复选框。重定向是指如果代理服务器阵列的成员收到不应由其提供服务的请求，它会告知客户机应联系哪个代理服务器来处理该请求。
7. 单击 "OK"。

注 只有当要配置的代理服务器是代理服务器阵列的成员时，才可以启用代理服务器阵列路由选择。如果存在父代理服务器阵列，就只能启用父代理服务器路由选择。两个路由选择选项互不相关。

注意 当前任何客户机都不支持重定向，所以目前不应使用该特性。

8. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

启用代理服务器阵列

启用代理服务器阵列

1. 访问 Server Manager 并单击 "Preferences" 选项卡。
2. 单击 "Configure System Preferences" 链接。将显示 "Configure System Preferences" 页面。
3. 单击与要启用的阵列（普通代理服务器阵列或父代理服务器阵列）类型对应的 "Yes" 选项。
4. 单击 "OK"。

注 如果不通过代理服务器阵列进行路由选择，则在禁用代理服务器阵列选项前应确保所有客户机都使用特殊的 PAC 文件正确地进行路由。如果禁用代理服务器阵列选项，则在 "Set Routing Preferences" 页面中应已设置了有效的备用路由选择选项，如显式代理服务器或直接连接。

5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

重定向代理服务器阵列中的请求

如果选择通过代理服务器阵列进行路由，需要指定是否要将请求重定向到另一个 URL。重定向是指如果代理服务器阵列的成员收到不应由其提供服务的请求，它会告知客户机应联系哪个代理服务器来处理该请求。

注意 当前任何客户机都不支持重定向，所以目前不应使用该特性。

使用 PAT 文件生成 PAC 文件

因为大多数客户机无法识别 PAT 文件格式，所以在客户机到代理服务器路由选择中，客户机使用代理服务器自动配置 (PAC) 机制来接收有关通过的代理服务器的信息。不过，客户机使用的不是标准的 PAC 文件，而是源自 PAT 文件的一种特殊的 PAC 文件。这种特殊的 PAC 文件通过计算散列算法来为请求的 URL 确定合适的路由。

可以使用 PAT 文件以手动或自动方式生成 PAC 文件。如果通过代理服务器阵列的某个成员手动生成 PAC 文件，该成员将立即根据 PAT 文件中的当前信息重新生成 PAC 文件。如果配置代理服务器阵列成员来自动生成 PAC 文件，该成员将在每次检测到 PAT 文件的修改版本后自动重新生成该文件。

注 如果没有为代理服务器使用代理服务器阵列特性，则应使用 "Create / Edit Autoconfiguration File" 页面生成 PAC 文件。有关更多信息，参见 第 325 页的第 17 章“使用客户机自动配置文件”。

使用 PAT 文件手动生成 PAC 文件

注 只能通过主代理服务器生成 PAC 文件。

通过 PAT 文件手动生成 PAC 文件

1. 访问主代理服务器的 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Configure Proxy Array" 链接。将显示 "Configure Proxy Array" 页面。
3. 单击 "Generate PAC" 按钮。将显示 "PAC Generation" 页面。
4. 如果要在 PAC 文件中使用自定义逻辑，请在 "Custom logic file" 字段中输入文件名称，该文件包含要在生成 PAC 文件时包括的自定义逻辑。将把此逻辑插入到 `FindProxyForURL` 函数中代理服务器阵列选择逻辑前。此函数通常用于不需要经过代理服务器阵列的本地请求。

   如果已在 "Configure Proxy Array Member" 页面中输入了自定义逻辑文件，将会用该信息填充此字段。需要时可以编辑自定义逻辑文件名，所做的更改还将传送到 "Configure Proxy Array Member" 页面。
5. 在 "Default Route" 字段中输入当阵列中的代理服务器不可用时客户机应采用的路由。

   如果已在 "Configure Proxy Array Member" 页面中输入了默认路由，将会用该信息填充此字段。需要时可以编辑默认路由，所做的更改还将传送到 "Configure Proxy Array Member" 页面。
6. 单击 "OK"。

7. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
8. 单击 "Restart Proxy Server" 按钮以应用更改。

使用 PAT 文件自动生成 PAC 文件

每次检测到更改时使用 PAT 文件自动生成 PAC 文件

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "Configure Proxy Array Member" 链接。将显示 "Configure Proxy Array Member" 页面。
3. 选中 "Auto-generate PAC File" 复选框。
4. 如果要在 PAC 文件中使用自定义逻辑，请在 "Custom logic file" 字段中输入文件名称，该文件包含要在生成 PAC 文件时包括的自定义逻辑。将把此逻辑插入到 `FindProxyForURL` 函数中代理服务器阵列选择逻辑前。

   如果已在 "Configure Proxy Array" 页面中输入并保存了自定义逻辑文件，将会用该信息填充此字段。需要时可以编辑自定义逻辑文件名，所做的更改还将传送到 "Configure Proxy Array" 页面。
5. 在 "Default Route" 字段中输入当阵列中的代理服务器不可用时客户机应采用的路由。
6. 如果已在 "Configure Proxy Array" 页面中输入并保存了默认路由，将会用该信息填充此字段。需要时可以编辑默认路由，所做的更改还将传送到 "Configure Proxy Array" 页面。
7. 单击 "OK"。
8. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

通过父代理服务器阵列进行路由选择

可以将代理服务器或代理服务器阵列成员配置为通过上游父代理服务器阵列进行路由，而不是直接转至远程服务器。

将代理服务器或代理服务器阵列成员配置为通过父代理服务器阵列进行路由

1. 启用父代理服务器阵列。有关启用阵列的更多信息，参见第 274 页的“启用代理服务器阵列”。
2. 启用通过父代理服务器阵列进行路由选择。有关启用通过阵列进行路由选择的更多信息，参见第 273 页的“启用通过代理服务器阵列进行路由选择”。

3. 访问 Server Manager 并单击 "Caching" 选项卡。
4. 单击 "Configure Proxy Array Member" 链接。将显示 "Configure Proxy Array Member" 页面。
5. 在页面 "Parent Array" 部分的 "Poll Host" 字段中，输入父代理服务器阵列中将针对 PAT 文件对其进行轮询的代理服务器的主机名。此代理服务器通常是父代理服务器阵列的主代理服务器。
6. 在页面 "Parent Array" 部分的 "Port" 字段中，输入父代理服务器阵列中将针对 PAT 文件对其进行轮询的代理服务器的 "Port" 号。
7. 在 "URL" 字段中输入主代理服务器上 PAT 文件的 URL。如果已在主代理服务器上创建了 PAT 映射，则应在此 "URL" 字段中输入该映射。
8. 在表单 "Parent Array" 部分的 "Headers File" 字段中，输入含有任何特殊标头的文件的完整路径名，这些标头必须与 PAT 文件的 HTTP 请求（如验证信息）一起发送。该字段为可选字段。
9. 单击 "OK"。
10. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
11. 单击 "Restart Proxy Server" 按钮以应用更改。

查看父代理服务器阵列信息

如果代理服务器阵列是通过父代理服务器阵列进行路由选择，则需要有关父代理服务器阵列成员的信息。此信息以 PAT 文件形式从父代理服务器阵列发出。此 PAT 文件中的信息将显示在 "View Parent Array Configuration" 页面中。

查看父代理服务器阵列信息

1. 访问 Server Manager 并单击 "Caching" 选项卡。
2. 单击 "View Parent Array Configuration" 链接。将显示 "View Parent Array Configuration" 页面。
3. 查看信息。

第 13 章

通过代理服务器过滤内容

本章介绍如何过滤 URL，以使代理服务器或者禁止访问该 URL，或者修改其返回给客户机的 HTML 和 JavaScript 内容。本章还将介绍如何才能基于客户机所使用的 Web 浏览器（用户代理）通过代理服务器来限制访问。

代理服务器允许使用 URL 过滤器文件来确定服务器所支持的 URL。例如，可以创建或购买一个包含所要限制 URL 的文本文件，而不用手动键入要支持的 URL 的通配符模式。利用此特性可创建一个含有 URL 的文件，以便能在多个不同的代理服务器上使用。

还可以基于各自的 MIME 类型来过滤 URL。例如，为防止计算机病毒的侵害，可以允许代理服务器高速缓存和发送 HTML 及 GIF 文件，但不允许它获取二进制或可执行文件。

本章包括以下各节：

过滤 URL

可以使用含 URL 的文件来配置代理服务器所检索的内容。可以建立一个代理服务器始终支持的 URL 列表，以及一个代理服务器始终不支持的 URL 列表。

例如，如果您是 Internet 服务提供商，希望所运行的代理服务器提供儿童适宜的内容，则可以建立一个准许儿童查看的 URL 列表。接着，可以使代理服务器仅检索准许的 URL；如果客户机试图转至不支持的 URL，则可使代理服务器返回默认的 “Forbidden” 消息，也可创建一个自定义消息，说明客户机无法访问该 URL 的原因。

要基于 URL 对访问进行限制，需要创建一个含有允许或限制的 URL 的文件。这可以通过 Server Manager 来完成。建立完该文件后，可设置一些限制。以下各节将对上述过程进行论述。

创建含 URL 的过滤器文件

过滤器文件是一个含有 URL 列表的文件。代理服务器使用的过滤器文件是纯文本文件，其中的 URL 行采用以下模式：

```
protocol://host:port/path/filename
```

可在以下三个部分中分别使用正则表达式：`protocol`、`host:port` 和 `path/filename`。例如，如果要为面向 netscape.com 域的所有协议创建一个 URL 模式，则应在文件中加入下面一行：

```
.*://.*\.example\.com/.*
```

此行仅在未指定端口号时才起作用。有关正则表达式的更多信息，参见第 319 页的第 16 章“管理模板和资源”中的“了解正则表达式”。

如果您想创建自己的文件而不使用 Server Manager，则应使用 Server Manager 页面创建一个空文件，然后将您的文本添加到该文件中，或用一个包含正则表达式的文件替换该文件。

创建过滤器文件

1. 访问 Server Manager，然后单击 "Filters" 选项卡。
2. 单击 "Restrict URL Filter Access" 链接。将显示 "Restrict URL Filter Access" 页面。
3. 从 "Create/Edit" 按钮旁的下拉式列表中选择 "New Filter"。
4. 在此下拉式列表右侧的文本框中键入过滤器文件的名称，然后单击 "Create/Edit" 按钮。将显示 "Filter Editor" 页面。

5. 使用 "Filter Content" 可滚动文本框输入 URL 及其正则表达式。"Reset" 按钮可清除此字段中的所有文本。

   有关正则表达式的更多信息，参见第 319 页的第 16 章“管理模板和资源”中的“了解正则表达式”。

6. 单击 "OK"。

代理服务器将创建该文件，然后返回到 "Restrict URL Filter Access" 页面。过滤器文件创建于 `proxy-server`*id*`/conf_bk` 目录。

设置过滤器文件的默认访问

拥有包含要使用的 URL 的过滤器文件后，就可以为这些 URL 设置默认访问。

设置过滤器文件的默认访问

1. 访问 Server Manager，然后单击 "Filters" 选项卡。
2. 单击 "Restrict URL Filter Access" 链接。将显示 "Restrict URL Filter Access" 页面。
3. 选择要与过滤器一起使用的模板。

   通常需要为整个代理服务器创建过滤器文件，但是也可以为 HTTP 创建一组过滤器文件，而为 FTP 创建另一组过滤器文件。

4. 使用 "URL Filter To Allow" 列表选择一个过滤器文件，其中含有您想要代理服务器支持的 URL。
5. 使用 "URL Filter To Deny" 列表选择一个过滤器文件，其中含有您想要代理服务器拒绝访问的 URL。
6. 选择当客户机请求被拒绝的 URL 时想要代理服务器向其返回的文本。可选择以下两个选项之一：
   - 可发送代理服务器生成的默认 “Forbidden” 响应。
   - 可发送一个文本或含自定义文本的 HTML 文件。在文本框中键入此文件的绝对路径。
7. 单击 "OK"。
8. 单击 "Restart required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

内容 URL 重写

Proxy Server 4 能够检查即将返回给客户机的内容并用其他字符串替换模式（如 URL）。有两个可以配置的参数——源字符串和目标字符串。Proxy Server 会寻找与源字符串匹配的文本，并以目标字符串中的文本取而代之。此特性仅在反向代理模式下起作用。

创建 URL 重写模式

1. 访问 Server Manager，然后单击 "Filters" 选项卡。
2. 单击 "Set Content URL Rewriting" 链接。将显示 "Set Content URL Rewriting" 页面。
3. 从下拉式列表中选择一个资源，或指定一个正则表达式。有关正则表达式的更多信息，参见第 319 页的第 16 章“管理模板和资源”中的“了解正则表达式”。
4. 在 "Source Pattern" 文本框中指定源字符串。
5. 在 "Destination Pattern" 文本框中指定目标字符串。
6. 在 "MIME Pattern" 文本框中指定内容类型。
7. 单击 "OK"。
8. 单击 "Restart required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

编辑 URL 重写模式

1. 访问 Server Manager，然后单击 "Filters" 选项卡。
2. 单击 "Set Content URL Rewriting" 链接。将显示 "Set Content URL Rewriting" 页面。
3. 单击所要编辑的 URL 重写模式旁的 "Edit" 链接。
4. 单击 "OK"。
5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

删除 URL 重写模式

1. 访问 Server Manager，然后单击 "Filters" 选项卡。
2. 单击 "Set Content URL Rewriting" 链接。将显示 "Set Content URL Rewriting" 页面。

3. 单击所要删除的 URL 重写模式旁的 "Remove" 链接。单击 "OK" 确认删除。
4. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
5. 单击 "Restart Proxy Server" 按钮以应用更改。

限制特定 Web 浏览器的访问

可以基于客户机 Web 浏览器的类型和版本限制对代理服务器的访问。根据请求时所有 Web 浏览器向服务器发送的用户代理标头进行限制。

基于客户机的 Web 浏览器限制对代理服务器的访问

1. 访问 Server Manager，然后单击 "Filters" 选项卡。
2. 单击 "Set User-Agent Restriction" 链接。将显示 "Set User-Agent Restriction" 页面。
3. 从下拉式列表中选择资源，或键入与特定的用户代理字符串相匹配的正则表达式，该字符串用于您希望 Proxy Server 支持的浏览器。如果要指定一个以上的客户机，请用括号将正则表达式括起来，并用 | 字符将多个条目隔开。有关正则表达式的更多信息，参见第 319 页的第 16 章“管理模板和资源”中的“了解正则表达式”。
4. 选中 "Allow Only User-Agents Matching" 选项。
5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

阻止请求

您可能需要基于上载内容类型来阻止文件上载及其他请求。

基于 MIME 类型阻止请求

1. 访问 Server Manager，然后单击 "Filters" 选项卡。
2. 单击 "Set Request Blocking" 链接。将显示 "Set Request Blocking" 页面。
3. 从下拉式列表中选择资源，或单击 "Regular Expression" 按钮输入正则表达式，然后单击 "OK"。

4. 单击与所需请求阻止类型相应的单选按钮。包括以下选项：
   - "Disabled"——禁用请求阻止
   - "Multipart MIME (File Upload)"——阻止所有文件上载
   - "MIME Types Matching Regular Expression" ——阻止与所输入的正则表达式匹配的 MIME 类型请求。有关正则表达式的更多信息，参见第 319 页的第 16 章“管理模板和资源”中的“了解正则表达式”。
5. 选择要阻止所有客户机的请求还是阻止与输入的正则表达式匹配的用户代理请求。
6. 单击单选按钮选择用于阻止请求的方法。选项包括：
   - "Any Method With Request Body"——阻止具有请求主体的所有请求（无论其使用何种方法）
   - "only for:"
     "POST"——阻止使用 POST 方法的文件上载请求
     "PUT"——阻止使用 PUT 方法的文件上载请求
   - "Methods Matching Regular Expression"——阻止使用所输入方法的所有文件上载请求
7. 单击 "OK"。
8. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

抑制外出标头

可以对代理服务器进行配置，使其从请求中删除外出标头（通常是出于安全原因）。例如，您可能需要防止 From 标头外发，因为它会暴露用户的电子邮件地址，或者，您可能需要过滤掉用户代理标头，这样外部服务器便无法确定您的组织所使用的 Web 浏览器。您可能还想在请求转发到 Internet 前删除仅在您的内联网中使用的日志记录或与客户机相关的标头。

此功能不影响经过特殊处理的标头或由代理本身生成的标头，也不影响使协议正常工作所需的标头（如 If-Modified-Since 和 Forwarded）。

虽然不能阻止代理产生转发的标头，但这不是一个安全问题。远程服务器可通过连接检测到正在连接的代理主机。在代理链中，来自内部代理服务器的转发标头可由一个外部代理服务器抑制。当您不想将内部代理服务器或客户机主机名暴露给远程服务器时，建议您以这种方式设置服务器。

抑制外出标头

1. 访问 Server Manager，然后单击 "Filters" 选项卡。
2. 单击 "Suppress Outgoing Headers" 链接。将显示 "Suppress Outgoing Headers" 页面。
3. 在 "Suppress Headers" 文本框中输入要抑制的请求标头列表，各标头之间以逗号分隔。例如，要抑制 From 和 User-Agent 标头，请键入 **`from,user-agent`**。键入的标头不区分大小写。有关正则表达式的更多信息，参见第 319 页的第 16 章“管理模板和资源”中的“了解正则表达式”。
4. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
5. 单击 "Restart Proxy Server" 按钮以应用更改。

按 MIME 类型过滤

可以对代理服务器进行配置，使其阻止与某种 MIME 类型匹配的某些文件。例如，可将代理服务器设置成阻止任何可执行文件或二进制文件，以使任何使用代理服务器的客户机均无法下载可能的计算机病毒。

如果想要代理服务器支持新的 MIME 类型，请在 Server Manager 中选择 "Preferences" > "Create/Edit MIME Types"，然后添加类型。有关创建 MIME 类型的更多信息，参见第 129 页的“创建新的 MIME 类型”。

可将过滤 MIME 类型与模板相结合，这样对于特定 URL 就能仅阻止某些 MIME 类型。例如，可阻止来自 `.edu` 域中任何计算机的可执行文件。

按 MIME 类型过滤

1. 访问 Server Manager，然后单击 "Filters" 选项卡。
2. 单击 "Set MIME Filters" 链接。将显示 "Set MIME Filters" 页面。
3. 选择要对过滤 MIME 类型使用的模板，或确保对整个服务器进行编辑。
4. 在 "Current filter" 文本框中，可键入与所要阻止的 MIME 类型匹配的正则表达式。

   例如，要过滤掉所有应用程序，可键入正则表达式 **`application/.*`**。这比检查每个应用程序类型的每个 MIME 类型更快。正则表达式不区分大小写。有关正则表达式的更多信息，参见第 319 页的第 16 章“管理模板和资源”中的“了解正则表达式”。
5. 选择要过滤的 MIME 类型。当客户机试图访问被阻止的文件时，代理服务器会返回“403 Forbidden”消息。

6. 单击 "OK"。
7. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
8. 单击 "Restart Proxy Server" 按钮以应用更改。

按 HTML 标记过滤

代理服务器允许指定在将文件传给客户机之前所要过滤掉的 HTML 标记。借此可以过滤掉一些对象，如嵌入在 HTML 文件中的 Java applet 和 JavaScript。要过滤 HTML 标记，请指定开始和结束 HTML 标记。这样，在将文件发送给客户机之前，代理服务器便会用空白替代这些标记中的所有文本和对象。

注 如果代理已配置为高速缓存原始（未编辑的）文件，它就会将该资源存储在高速缓存中。

过滤掉 HTML 标记

1. 访问 Server Manager，然后单击 "Filters" 选项卡。
2. 单击 "Set HTML Tag Filters" 链接。将显示 "Set HTML Tag Filters" 页面。
3. 选择要修改的模板。可以选择 "HTTP"，也可以选择一个仅指定某些 URL 的模板，例如，来自 `.edu` 域中主机的 URL。
4. 选中与所要过滤的任何默认 HTML 标记相应的过滤器框。包括以下默认标记：
   - "APPLET" 通常包围着 Java applet。
   - "SCRIPT" 表示 JavaScript 代码的开始。
   - "IMG" 指定内嵌图像文件。
5. 可输入要过滤的任何 HTML 标记。键入开始和结束 HTML 标记。

   例如，要过滤掉表单，可在 "Start Tag" 框中键入 **`FORM`**（HTML 标记不区分大小写），在 "End Tag" 框中键入 **`/FORM`**。如果要过滤的标记没有结束标记（如 `OBJECT` 和 `IMG`），可将 "End Tag" 框留空。
6. 单击 "OK"。
7. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
8. 单击 "Restart Proxy Server" 按钮以应用更改。

配置服务器的内容压缩

Proxy Server 支持 HTTP 内容压缩。通过内容压缩可以提高向客户机传送的速度，而且无需增加硬件开支即可提高内容量。内容压缩减少了内容的下载时间，对使用拨号连接和高流量连接的用户尤其有用。

采用内容压缩时，Proxy Server 会发出经过压缩的数据并指示浏览器如何即时解压缩数据，从而可以减少数据发送量并提高页面显示速度。

将服务器配置成按即时请求压缩内容

可以对 Proxy Server 进行配置，使其即时地压缩传输数据。动态生成的 HTML 页面仅在用户提出请求时才存在。

将服务器配置成按即时请求压缩内容

1. 访问 Server Manager，然后单击 "Filters" 选项卡。
2. 单击 "Compress Content on Demand" 链接。将显示 "Compress Content on Demand" 页面。
3. 从下拉式列表中选择资源，或指定一个正则表达式。有关正则表达式的更多信息，参见第 319 页的第 16 章“管理模板和资源”中的“了解正则表达式”。
4. 指定以下信息：
   - **Activate Compress Content on Demand?** 选择服务器是否应为选定资源提供预压缩内容。
   - **Vary Header。**指定是否插入 Vary: Accept-encoding 标头。选择 "yes" 或 "no"。如果设置为 "yes"，则当选择了压缩版本的文件时，始终会插入一个 Vary: Accept-encoding 标头。

     如果设置为 "no"，则决不会插入 Vary: Accept-encoding 标头。

     默认情况下，该值设置为 "yes"。
   - **Fragment Size。**指定压缩库 (`zlib`) 用于控制一次压缩量的内存段大小（以字节计）。默认值是 8096。
   - **Compression Level。**指定压缩的级别。请选择 1 至 9 之间的值。值为 1 时速度最快；值为 9 时压缩效果最好。默认值为 6，这将获得适中的速度和压缩效果。
5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

第 14 章

使用反向代理服务器

本章介绍如何使用 Proxy Server 作为反向代理服务器。反向代理服务器是代理服务器改用于特定目的时的代名称。可以在防火墙外部用它来向外部客户机表示一个安全内容服务器，以防从公司外部直接、不受监视地访问服务器数据。还可以使用它来进行复制，也就是说，可以在高用量服务器前面附加多个代理服务器来进行负载平衡。本章将介绍 Proxy Server 在防火墙内部或外部的替代用法。

本章包括以下各节：

反向代理服务器的工作原理

有两个反向代理模型。一个模型利用 Proxy Server 的安全特性来处理事务，另一个利用其高速缓存特性在高用量服务器上提供负载平衡。这两个模型与代理服务器习惯用法的区别在于它们并不严格在防火墙上运行。

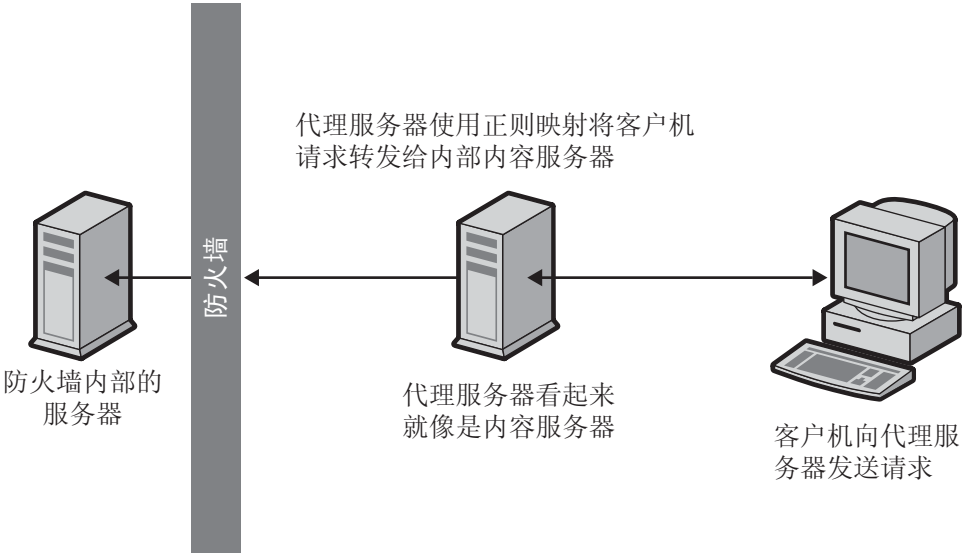
代理服务器充当服务器的替身

如果您的内容服务器具有必须保持安全的敏感信息，如信用卡号数据库，可在防火墙外部设置一个代理服务器作为内容服务器的替身。当外部客户机尝试访问内容服务器时，会将其送到代理服务器。实际内容位于内容服务器上，在防火墙内部受到安全保护。代理服务器位于防火墙外部，在客户机看来就像是内容服务器。

当客户机向站点提出请求时，请求将转到代理服务器。然后，代理服务器通过防火墙中的特定通路，将客户机的请求发送到内容服务器。内容服务器再通过该通道将结果回传给代理服务器。代理服务器将检索到的信息发送给客户机，好像代理服务器就是实际的内容服务器（参见图 14-1）。如果内容服务器返回错误消息，代理服务器会先行截取该消息并更改标头中列出的任何 URL，然后再将消息发送给客户机。如此可防止外部客户机获取内部内容服务器的重定向 URL。

这样，代理服务器就在安全数据库和可能的恶意攻击之间提供了又一道屏障。与有权访问整个数据库的情况相对比，就算是侥幸攻击成功，作恶者充其量也仅限于访问单个事务中所涉及的信息。未经授权的用户无法访问到真正的内容服务器，因为防火墙通路只允许代理服务器有权进行访问。

图 14-1 反向代理服务器就像是真正的内容服务器



可以配置防火墙路由器，使其只允许特定端口上的特定服务器（在本例中为其所分配端口上的代理服务器）有权通过防火墙进行访问，而不允许其他任何机器进出。

安全反向代理

当代理服务器与其他机器之间有一个或多个连接使用安全套接字层 (SSL) 协议加密数据时，即会进行安全反向代理。

安全反向代理有许多用途：

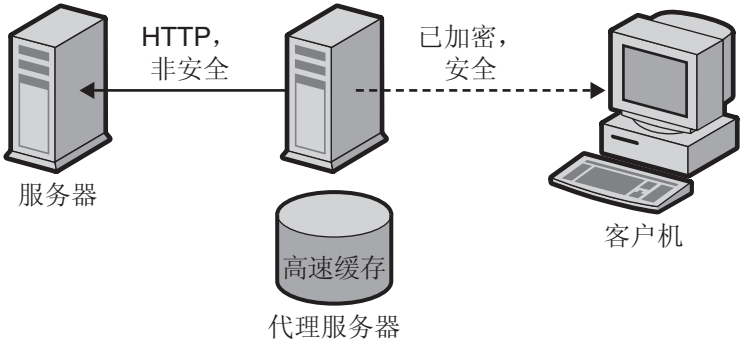
- 可以提供从防火墙外部代理服务器到防火墙内部安全内容服务器的加密连接。
- 可以允许客户机安全地连接到代理服务器，从而有利于安全地传输信息（如信用卡号）。

安全反向代理会造成各安全连接因加密数据所涉及的系统开销而变慢。但是，由于 SSL 提供了高速缓存机制，所以连接双方可以重复使用先前协商的安全参数，从而大大降低后续连接的系统开销。

配置安全反向代理服务器的方法有三种：

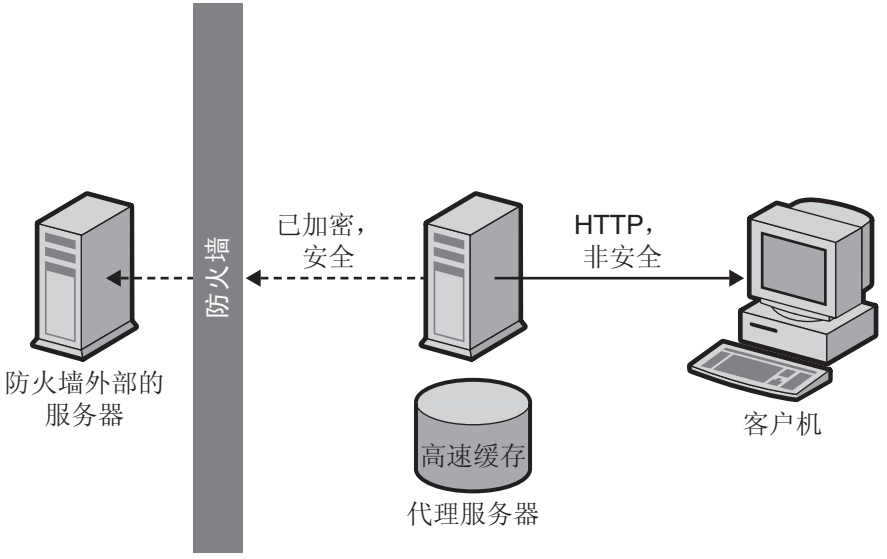
Secure client to proxy。如果未经授权的用户很少或根本没有机会访问代理服务器与内容服务器之间交换的信息，则此方案很有效（参见图 14-2）。

图 14-2 客户机安全连接到代理服务器



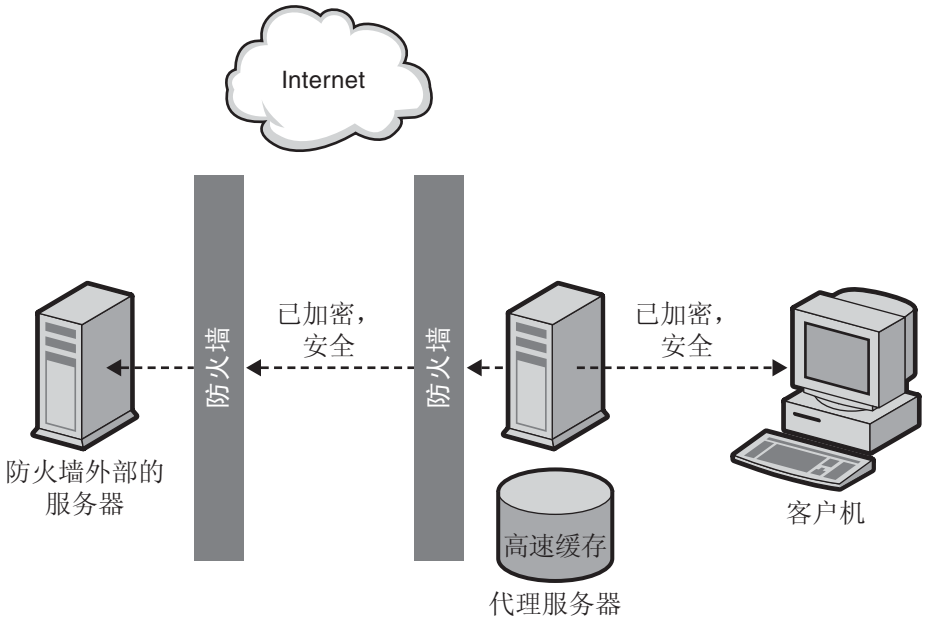
Secure proxy to content server。如果客户机在防火墙内部而内容服务器在防火墙外部，则此方案很有效。在此方案中，代理服务器可以充当站点之间的安全通道（参见图 14-3）

图 14-3 代理服务器安全连接到内容服务器



- **Secure client to proxy and secure proxy to content server**。如果需要保护服务器、代理服务器和客户机三者间所交换信息的安全，则此方案很有效。在此方案中，代理服务器既可起到站点间安全通道的作用，又可增加客户机验证的安全性（参见图 14-4）。

图 14-4 客户机安全连接到代理服务器并且代理服务器安全连接到内容服务器



有关如何设置上述每种配置的信息，参见第 295 页的“设置反向代理服务器”。

除了 SSL 之外，代理服务器还可以使用客户机验证，这种方法要求向代理服务器提出请求的计算机提供证书（或标识表单）以核实其身份。

负载平衡代理

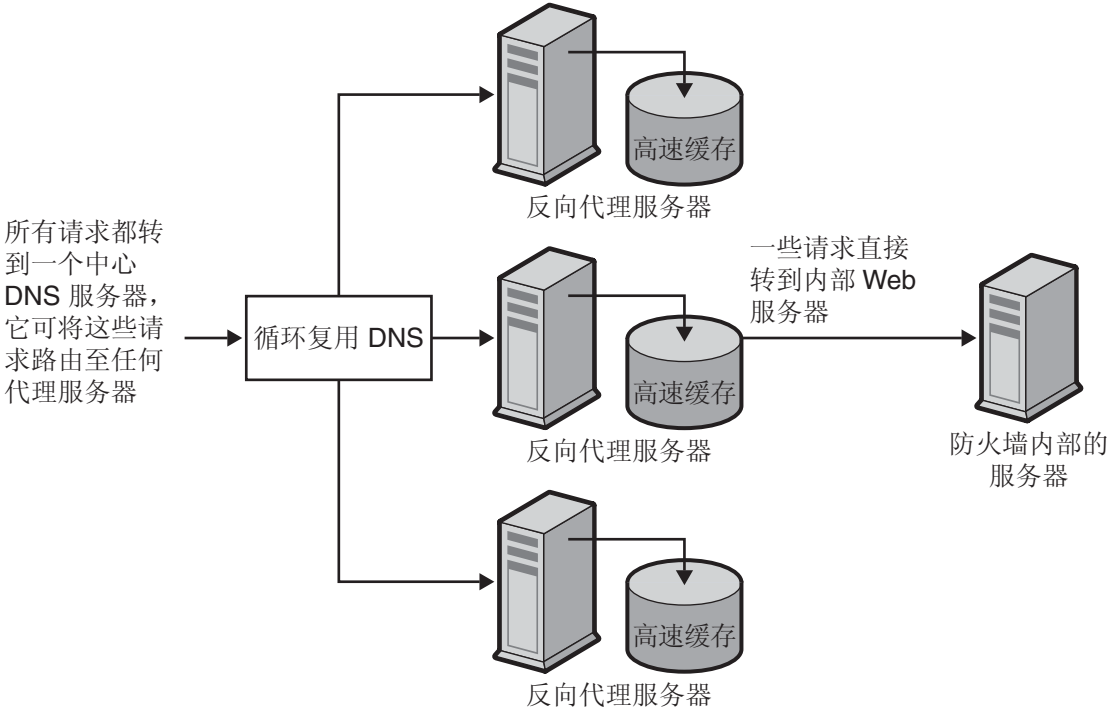
可以在一个组织内使用多个代理服务器来平衡各 Web 服务器间的网络负载。在此模型中，可以利用代理服务器的高速缓存特性，创建一个用于负载平衡的服务器池。此时，代理服务器可以位于防火墙的任意一侧。如果 Web 服务器每天都会接收大量的请求，则可以使用代理服务器分担 Web 服务器的负载并提高网络访问效率。

对于客户机发往真正服务器的请求，代理服务器起着中间调停者的作用。代理服务器会将所请求的文档存入高速缓存。如果有不止一个代理服务器，DNS 可以采用“循环复用法”选择其 IP 地址，随机地为请求选择路由。客户机每次都使用同一个 URL，但请求所采取的路由每次都可能经过不同的代理服务器。

可以使用多个代理服务器来处理对一个高用量内容服务器的请求，这样做的好处是内容服务器可以处理更高的负载，并且比其独自工作时更有效率。在初始启动期间，代理服务器首次从内容服务器检索文档，此后，对内容服务器的请求数会大大下降。

只有 CGI 请求和偶发的新请求必须一路直达内容服务器。其余的请求可以由代理服务器进行处理。下面对此进行举例说明。假定对服务器的请求中有 90% 都不是 CGI 请求（这表示它们可以进行高速缓存），而且内容服务器每天都会被命中 2 百万次。在此情况下，如果连接三个反向代理服务器，且每个代理服务器每天处理 2 百万次命中，则每天将能够处理大约 6 百万次命中。请求中有 10% 达到内容服务器，合计约为每个代理服务器每天 200,000 次命中，即总数仅为 600,000，从而效率显著提高。命中次数可从大约 2 百万次增加到 6 百万次，而内容服务器的负载却相应地从 2 百万次减少到 600,000 次。实际结果依具体情况而定。

图 14-5 用于负载平衡的代理服务器



设置反向代理服务器

要设置反向代理服务器，需要两个映射：一个正则映射和一个反向映射。

- 正则映射用于将请求重定向到内容服务器。当客户机从代理服务器请求文档时，代理服务器需要通过正则映射来获知应从何处获取实际文档。

注意 不能与提供自动配置文件的代理服务器一起使用反向代理服务器。这是因为该代理服务器可能会返回错误的结果。

- 反向映射用于为来自内容服务器的重定向产生代理服务器陷阱。代理服务器将截取重定向指令，然后更改重定向的 URL 以映射到代理服务器。例如，如果客户机所请求的文档已移动或未找到，内容服务器将向客户机返回一条消息，说明它无法在请求的 URL 处找到该文档。内容服务器会在该返回消息中添加一个 HTTP 标头，其中列出了用于获取已移动文件的 URL。为了保持内部内容服务器的保密性，代理服务器可以使用反向映射重定向该 URL。

假定您有一个称为 `http://http.site.com/` 的 Web 服务器并且想要为它设置一个反向代理服务器。可以将反向代理服务器称为 `http://proxy.site.com/`。

需按如下步骤创建一个**正则**映射和一个**反向**映射：

1. 访问 Server Manager，然后单击 "URLs" 选项卡。
2. 单击 "Create Mapping" 链接。将显示 "Create Mapping" 页面。
3. 在出现的页面中，输入单个映射的信息。例如：

   Regular mapping:

   Source prefix: `http://proxy.site.com`

   Source destination: `http://http.site.com/`
4. 单击 "OK"。返回到页面并创建第二个映射：

   Reverse mapping:

   Source prefix: `http://http.site.com/`

   Source destination: `http://proxy.site.com/`

5. 要进行更改，请单击 "OK"。

   单击 "OK" 按钮后，代理服务器即会添加一个或多个附加映射。要查看映射，请单击称为 "View/Edit Mappings" 的链接。附加映射将具有以下格式：

   from: /

   to: `http://http.site.com/`

   这些附加的自动映射针对的是以常规服务器形式连接到反向代理服务器的用户。第一个映射用于捕捉以常规代理服务器形式连接到反向代理服务器的用户。根据具体设置，通常只有第二个映射是必需的，但是这两个映射并存不会使代理服务器出现问题。

注 如果 Web 服务器有若干 DNS 别名，每个别名都应有一个相应的正则映射。如果 Web 服务器用自身的若干 DNS 别名生成重定向，这些别名中的每一个都应有一个相应的反向映射。

CGI 应用程序仍在原始服务器上运行，代理服务器从不亲自运行 CGI 应用程序。但是，如果 CGI 脚本指示结果可以进行高速缓存（通过发出 Last-modified 或 Expires 标头暗示存活时间非零），则代理服务器将会高速缓存结果。

注意 为 Web 服务器制作内容时，请牢记反向代理服务器也将为该内容提供服务，因此，指向 Web 服务器上文件的所有链接都应为相对链接。HTML 文件中**决不**能含有对主机名的引用，也就是说，所有链接都必须为页面链接：

`/abc/def`

而不能是全限定主机名，例如：

`http://http.site.com/abc/def`

设置安全反向代理服务器

设置安全反向代理服务器需要具备数字证书、证书授权机构和验证方面的知识。

设置安全反向代理服务器大体上与设置非安全反向代理服务器相同。唯一的区别是需要指定 HTTPS 作为要加密文件的协议。

以下指导说明阐述了如何根据所选择的配置方案来设置安全反向代理服务器。为了演示如何设置映射，这些指导说明假定您有一个称为 `http.site.com` 的 Web 服务器，并且您想要设置一个称为 `proxy.site.com` 的安全反向代理服务器。按所述步骤进行操作时，请用您的 Web 服务器和代理服务器的名称替代指示说明中使用的示例名称。

Secure Client to Proxy

1. 访问 Server Manager，然后单击 "URLs" 选项卡。
2. 单击 "Create Mapping" 链接。将显示 "Create Mapping" 页面。
3. 在出现的页面中，采用以下方式设置正则映射和反向映射：

   Regular mapping:

   Source prefix: `https://proxy.mysite.com`

   Source destination: `http://http.mysite.com/`

   Reverse mapping:

   Source prefix: `http://http.mysite.com/`

   Source destination: `https://proxy.mysite.com/`

4. 保存并应用所做的更改。

   要查看刚刚创建的映射，请单击称为 "View/Edit Mappings" 的链接。

注 此配置仅在代理服务器以安全模式运行时才起作用。换言之，必须启用加密，而且必须从命令行重新启动代理服务器。要从命令行重新启动代理服务器，请转到代理目录，然后键入 **`./start`**。

Secure Proxy to Content Server

1. 访问 Server Manager，然后单击 "URLs" 选项卡。
2. 单击 "Create Mapping" 链接。将显示 "Create Mapping" 页面。

3. 在出现的页面中，采用以下方式设置正则映射和反向映射：

   Regular mapping:

   Source prefix: `http://proxy.mysite.com`

   Source destination: `https://http.mysite.com/`

   Reverse mapping:

   Source prefix: `https://http.mysite.com/`

   Source destination: `http://proxy.mysite.com/`

4. 保存并应用所做的更改。要查看刚刚创建的映射，请单击称为 "View/Edit Mappings" 的链接。

注 此配置仅在内容服务器以安全模式运行时才起作用。

Secure Client to Proxy and Secure Proxy to Content Server

1. 访问 Server Manager，然后单击 "URLs" 选项卡。
2. 单击 "Create Mapping" 链接。将显示 "Create Mapping" 页面。
3. 在出现的页面中，采用以下方式设置正则映射和反向映射：

   Regular mapping:

   Source prefix: `https://proxy.mysite.com`

   Source destination: `https://http.mysite.com/`

   Reverse mapping:

   Source prefix: `https://http.mysite.com/`

   Source destination: `https://proxy.mysite.com/`

4. 保存并应用所做的更改。要查看刚刚创建的映射，请单击称为 "View/Edit Mappings" 的链接。

注 此配置仅在代理服务器和内容服务器以安全模式运行时才起作用。换言之，必须为代理服务器启用加密，而且必须从命令行重新启动代理服务器。要从命令行重新启动代理服务器，请转到代理目录，然后键入 **`./restart`**。

反向代理服务器中的虚拟多重主机

利用虚拟多重主机特性，原始服务器（就本处而言，即为反向代理服务器）可以响应多个 DNS 别名，就好像其中的每个地址都安装了不同的服务器。例如，可有以下 DNS 主机名：

- www
- specs
- phones

其中的每一个都可以映射到同一 IP 地址（反向代理服务器的 IP 地址）。然后，即可使反向代理服务器根据访问它时所用的 DNS 名做出不同的反应。

虚拟多重主机还允许您将单个反向代理服务器作为多个不同 * 域 * 的宿主服务器。例如：

- www.domain-1.com
- www.domain-2.com
- www.domain-3.com

请注意，可以将多个本地主机名以及多个域全都组合在单个代理服务器中：

- www
- specs
- phones
- www.domain-1.com
- www.domain-2.com
- www.domain-3.com

本节包括以下主题：

- 虚拟多重主机功能详述
- 虚拟多重主机重要说明

虚拟多重主机功能详述

为使虚拟多重主机特性起作用，需要先指定 DNS 主机名和域名（或别名），然后给出应将发送给相应主机名的请求定向到的目标 URL 前缀。例如，可有以下两个映射：

- `engr.domain.com -> http://int-engr.domain.com`
- `mktg.domain.com -> http://int-mktg.domain.com`

映射不必非得是从根到根；可以在目标 URL 中指定附加的 URL 路径前缀：

- `engr.domain.com -> http://internal.domain.com/engr`
- `mktg.domain.com -> http://internal.domain.com/mktg`

这同样也适用于虚拟域映射。例如，可以使用：

- `www.domain-1.com -> http://int-engr.domain.com`
- `www.domain-2.com -> http://int-mktg.domain.com`

系统将查看 HTTP "Host:" 标头，并根据该标头选择匹配的虚拟多重主机映射。如果没有匹配的多重主机映射，服务器将按映射在配置文件中的出现顺序继续查看其他映射。如果仍未找到任何匹配项，则服务器将不执行映射。当没有匹配项时，代理服务器通常会以 "Proxy denies fulfilling the request" 响应进行应答。

配置虚拟多重主机

1. 访问 Server Manager，然后单击 "URLs" 选项卡。
2. 单击 "Configure Virtual Multihosting" 链接。将显示 "Configure Virtual Multihosting" 页面。
3. 在 "Source Hostname (alias)" 字段中，指定此映射所适用的本地主机名（或 DNS 别名）。
4. 在 "Source Domain Name" 字段中，输入此映射所适用的本地域名。通常，此名称为自己网络的域名，除非您要对多个不同的 DNS 域使用多重主机。
5. 在 "Destination URL Prefix" 字段中，输入目标 URL 前缀。如果主机名和域名符合上述规定，则会将请求定向至此。
6. 如果使用模板，请从 "Use This Template" 下拉式列表中选择模板名；如果不想应用模板，请将该值保留为 "NONE"。
7. 单击 "OK"。
8. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
9. 单击 "Restart Proxy Server" 按钮以应用更改。

   对所要建立的每个虚拟多重主机映射重复上述步骤。

所有虚拟多重主机映射都出现在 "Configure Virtual Multihosting" 页面的底部。请注意，"Source Hostname (alias)" 和 "Source Domain Name" 字段连同代理服务器的端口号被合并成单个正则表达式，用于匹配 "Host:" 标头。

例如，如果主机名为 "www"、域为 "example.com"、端口号为 "8080"，则会显示以下正则表达式：

```
www(|.example.com)(|:8080)
```

这样可以保证与用户可能键入的或客户机可能发送的以下所有可能的组合进行匹配（即使端口号不是 80，某些客户机软件亦可将其省略，因为服务器显然知道自己正在侦听哪个端口号）：

- `www`
- `www:8080`
- `www.example.com`
- `www.example.com:8080`

虚拟多重主机重要说明

需要先禁用客户机自动配置特性，才能配置反向代理映射。这样做不会引起任何问题，因为客户机自动配置特性针对的是正向代理操作，而不是反向代理。

虚拟多重主机特性会建立自动反向映射。换言之，请不要为使用 "Virtual Multihosting" 页面输入的映射创建反向映射。

虚拟映射是用 `obj.conf` 中的 `virt-map` 函数指定的。

虚拟映射按 obj.conf 配置文件中指定的顺序进行匹配。如果虚拟映射前面有正则、反向、正则表达式或客户机自动配置映射，则会首先应用这些映射。同样，如果在虚拟映射中未找到匹配项，则会继续转换 `obj.conf` 中虚拟映射部分之后的下一个映射。

如果更改了代理服务器的端口号，则需要重新创建虚拟多重主机映射，因为它们现在的端口号不正确。

第 15 章

使用 SOCKS

本章介绍如何配置和使用 Sun Java System Web Proxy Server 随附的 SOCKS 服务器。Proxy Server 支持 SOCKS 版本 4 和 5。

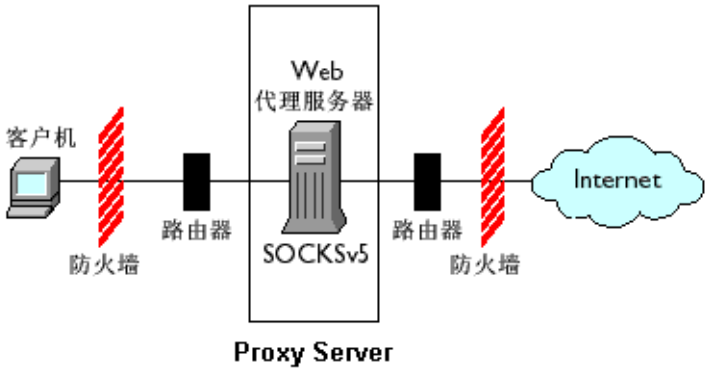
本章包括以下各节：

关于 SOCKS

SOCKS 是一种联网代理协议，用于重定向来自 SOCKS 服务器相对两侧主机的连接请求，通过该协议，无需直接 IP 可达性，一侧的主机便能够获得对另一侧主机的完全访问权。SOCKS 常被用作网络防火墙，以使 SOCKS 服务器后面的主机能够获得对 Internet 的完全访问权，同时又能防止在未经授权的情况下从 Internet 访问内部主机。

SOCKS 服务器是一个通用的防火墙守护进程，它基于点对点模式通过防火墙对访问进行控制。SOCKS 服务器可以对请求进行验证和授权、建立代理连接以及中转数据。SOCKS 服务器工作于网络层而非应用层，因此它对用于传送请求的协议或方法毫无所知。由于 SOCKS 服务器对协议毫无所知，所以可以使用它来传递 Proxy Server 不支持的那些协议（如 Telnet）。

图 15-1 SOCKS 服务器在网络中的位置



使用捆绑的 SOCKS v5 服务器

Sun Java System Web Proxy Server 包含自己的 SOCKS 守护进程，它认识其他 SOCKS 守护进程所使用的 `socks5.conf` 文件格式。此守护进程可以由 Proxy Server 用来为请求选择路由，也可以独立于 Proxy Server 运行以提供附加的网络功能。有关配置 Proxy Server 以通过 SOCKS 服务器路由请求的更多信息，参见第 314 页的“配置路由选择条目”。

Proxy Server 随附的 SOCKS 守护进程在默认情况下被禁用，可以从 Server Manager 界面的 "SOCKS" 选项卡或是从命令行来启用它。有关更多信息，参见第 306 页的“启动和停止 SOCKS v5 服务器”。

注 在 Proxy Server 4 中，SOCKS 守护进程的名称已从 `ns-sockd` 改为 `sockd`。

下面是使用 Proxy Server 随附的 SOCKS 服务器所必须采取的高级步骤：

1. 配置 SOCKS 服务器（参见第 306 页的“配置 SOCKS v5 服务器”）。
2. 如果 SOCKS 服务器即将在具有多个接口的计算机上运行，请创建 SOCKS 路由选择条目（参见第 314 页的“配置路由选择条目”）。
3. 创建验证条目（参见第 308 页的“配置 SOCKS v5 验证条目”）。
4. 创建连接条目（参见第 310 页的“配置 SOCKS v5 连接条目”）。
5. 启用 SOCKS 服务器（参见第 306 页的“启动和停止 SOCKS v5 服务器”）。

关于 socks5.conf

Sun Java System Web Proxy Server 使用 `socks5.conf` 文件来控制对 SOCKS 服务器及其服务的访问。每一行定义了 Proxy Server 在收到的请求与该行相符时所执行的操作。在 Server Manager 中所做的选择将被写入 `socks5.conf`。还可以手动编辑该文件。`socks5.conf` 文件位于如下的安装根目录 (*server_root*)：

server_root/`proxy-`*serverid*/`config` 目录

本节提供了有关 `socks5.conf` 的一般信息。有关该文件及其指令和语法的详细信息，参见 Proxy Server Configuration File Reference。

验证

可以将 SOCKS 守护进程配置成使用其服务时要求进行验证。验证基于连接客户机的主机名和端口号来进行。如果选择要求用户名和口令，则会针对 `socks5.conf` 文件所引用的用户名和口令文件进行信息验证。如果所提供的用户名和口令与口令文件中的列表不匹配，则拒绝访问。口令文件中的用户名和口令格式为 *username password*，其中用户名和口令以空格隔开。还可以禁止用户。若想要求进行用户名和口令验证，必须向 `socks5.conf` 添加 `SOCKS5_PWDFILE` 指令。有关该指令及其语法的更多信息，参见 Proxy Server Configuration File Reference 中的 `socks5.conf` 一节。

还可以针对已配置的 LDAP 服务器（而不仅仅是文件）执行用户名和口令验证。

访问控制

可使用 `socks5.conf` 文件中的一组有序行来执行访问控制。每一行均包含单个指令，用以允许或拒绝对资源的访问。指令按其在配置文件中的出现顺序进行处理。不符合任何允许指令的请求将被拒绝访问。

日志记录

SOCKS 守护进程会将错误消息和访问消息全都记入 SOCKS 日志文件。可在 `socks5.conf` 中指定日志文件位置和日志记录类型。

SOCKS 守护进程每小时还会生成一个统计条目，用以提供守护进程的统计信息。

调节

可以使用 `socks5.conf` 文件来确定 SOCKS 服务器使用的工作线程和接受线程的数目。这些数值会影响 SOCKS 服务器的性能。

有关工作线程和接受线程设置及其对性能的影响的更多信息，参见第 306 页的“配置 SOCKS v5 服务器”中的有关章节。

启动和停止 SOCKS v5 服务器

可以从 Server Manager 或命令行中启动和停止 SOCKS 服务器。

从 Server Manager 启动和停止 SOCKS 服务器

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Start/Stop SOCKS Server" 链接。
3. 启动或停止 SOCKS 服务器。

从命令行启动和停止 SOCKS 服务器

运行 *server_root*`/proxy-`*serverid* 目录中已有的脚本，其中 *server_root* 为安装根目录：

- `start-sockd` 用于启动 SOCKS 守护进程
- `stop-sockd` 用于停止 SOCKS 守护进程
- `restart-sockd` 用于重新启动 SOCKS 守护进程

配置 SOCKS v5 服务器

配置 SOCKS 服务器

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Configure SOCKS v5" 链接。

3. 在 "SOCKS Port" 字段中，输入 SOCKS 服务器将要侦听的端口号（默认情况下为 1080）。
4. 选择要使用的 SOCKS 选项。可用选项如下：
   - **Disable Reverse DNS Lookup。**对 SOCKS 服务器禁用反向 DNS 查找。反向 DNS 用于将 IP 地址转换成主机名。禁用反向 DNS 查找可优化网络资源的使用。默认情况下会禁用此选项（即，默认情况下会选中 "Disable Reverse DNS Lookup" 复选框）。如果禁用了反向 DNS 查找而使用主机名请求 URL，则服务器不会将主机名映射到 IP 地址。如果启用了反向 DNS 查找，则服务器将会执行映射，并向 SOCKS 日志文件添加一个条目，列出该 DNS 转换。
   - **Use Client-specific Bind Port。**允许客户机在“绑定”请求中指定端口。禁用此选项后，SOCKS 将忽略客户机请求的端口并指定一个随机端口。默认情况下将禁用此选项。
   - **Allow Wildcard As Bind IP Address。**允许客户机在“绑定”请求中指定一个全部由零组成的 IP 地址 (0.0.0.0)，它表示可以连接任何 IP 地址。禁用此选项后，客户机必须指定将要连接到绑定端口的 IP 地址，而且 SOCKS 服务器会拒绝绑定到 0.0.0.0 的请求。默认情况下将禁用此选项。
   - **Quench Updates。**禁用每小时一次自动写入 stat 文件。如果禁用，则每次请求时都会进行写入（参见第 306 页的“日志记录”）。

注 用户界面中显示有 "Quench Updates" 元素，但是它在本 Proxy Server 4 发行版本中并未实现。

5. 在 "Log File" 字段中，输入 SOCKS 日志文件的完整路径名。默认值为 *server_root*/proxy-*serverid*/logs/socks5.log。
6. 从 "Log Level" 下拉式列表中，选择日志文件应只包含警告和错误，还是应包含所有请求或是调试消息。
7. 选择 RFC 1413 ident 响应。Ident 允许 SOCKS 服务器确定客户机的用户名。一般而言，仅当客户机运行某种风格的 UNIX 时，此特性才起作用。可用选项如下：
   - **Don’t Ask。**从不使用 ident 来确定客户机的用户名。此为默认设置，建议使用。
   - **Ask But Don’t Require。**询问所有客户机的用户名，但不必非得提供。此选项使用 ident 仅为进行日志记录。
   - **Require。**询问所有客户机的用户名，并且仅允许访问做出了有效响应的客户机。

8. 在 "SOCKS Tuning" 部分，指定 SOCKS 服务器应使用的工作线程和接受线程的数目（这些数值对 SOCKS 服务器的性能有影响），然后单击 "OK"：

   - **Number Of Worker Threads。**默认值为 40。如果 SOCKS 服务器太慢，请增大工作线程数。如果服务器不稳定，则应减小该数值。更改此数值时，从默认值开始，根据需要增大或减小。典型的工作线程数介于 10 到 150 之间。绝对最大值是 512，但数量超过 150 往往会造成浪费且不稳定。
   - **Number Of Posted Accepts。**默认值为 1。如果 SOCKS 服务器丢弃连接，请增大接受线程数。如果服务器不稳定，则应减小该数值。更改此数值时，从默认值开始，根据需要增大或减小。典型的接受线程数介于 1 到 10 之间。绝对最大值是 512，但数量超过 60 往往会造成浪费且不稳定。这是一个非常重要的设置。如果在 SOCKS 服务器并未超负荷的情况下请求失败而且连接被丢弃，请调节此设置。

配置 SOCKS v5 验证条目

SOCKS 验证条目用于确定 SOCKS 守护进程应接受来自哪些主机的连接，以及 SOCKS 守护进程验证这些主机时应使用何种类型的验证。

本节包括以下主题：

创建验证条目

创建 SOCKS 验证条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Authentication" 链接。
3. 单击 "Add" 按钮。

4. 在 "Host Mask" 字段中，输入 SOCKS 服务器将要验证的主机的 IP 地址或主机名。如果输入的是 IP 地址，地址后面应跟一个正斜杠以及要应用于传入 IP 地址的掩码。SOCKS 服务器会将此掩码应用于 IP 地址来确定它是否是有效主机。请勿在主机掩码条目中使用空格。如果不输入主机掩码，则验证条目适用于所有主机。

   例如，可在 "host mask" 字段输入 155.25.0.0/255.255.0.0。如果主机的 IP 地址是 155.25.3.5，则 SOCKS 服务器会将该掩码应用于该 IP 地址，并断定主机的 IP 地址与验证记录所适用的 IP 地址 (155.25.0.0) 匹配。

5. 在 "Port Range" 字段中，输入 SOCKS 服务器将要验证的主机端口。请勿在端口范围条目中使用空格。如果不输入端口范围，则验证条目适用于所有端口。

   可以使用方括号 [ ] 包括范围两端的端口号，也可使用圆括号 ( ) 将它们排除在外。例如，[1000-1010] 表示其间包括 1000 和 1010 在内的所有端口号，而 (1000-1010) 表示其间不包括 1000 和 1010 在内的所有端口号。也可混合使用方括号和圆括号。例如，(1000-1010] 表示 1000 与 1010 之间不包括 1000 但包括 1010 在内的所有号码。

6. 从 "Authentication Type" 下拉式列表中选择验证类型。可用选项如下：

   - **Require user-password。**访问 SOCKS 服务器时需要用户名和口令。
   - **User-password, if available。**如果提供了用户名和口令，则应使用它们来访问 SOCKS 服务器（但它们并不是访问所必需的）。
   - **Ban。**禁止访问 SOCKS 服务器。
   - **None。**不必验证即可访问 SOCKS 服务器。

7. 从 "Insert" 下拉式列表中，选择此条目在 `socks5.conf` 文件中的位置，然后单击 "OK"。由于可以采用多种验证方法，所以必须指定其评判顺序。这样，如果客户机不支持所列的第一种验证方法，则会改用第二种方法。如果客户机不支持所列的任何验证方法，则 SOCKS 服务器不接受请求而断开连接。

编辑验证条目

编辑验证条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Authentication" 链接。
3. 选择要编辑的验证条目，然后单击 "Edit" 按钮。
4. 根据需要进行更改，然后单击 "OK"。

删除验证条目

删除验证条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Authentication" 链接。
3. 选择要删除的验证条目，然后单击 "Delete" 按钮。

移动验证条目

各条目按其在 `socks5.conf` 文件中出现的顺序进行评判。可以通过移动来更改其顺序。

移动验证条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Authentication" 链接。
3. 选择要移动的验证条目，然后单击 "Move" 按钮。
4. 从 "Move" 下拉式列表中，选择此条目在 `socks5.conf` 文件中的位置，然后单击 "OK"。

配置 SOCKS v5 连接条目

SOCKS 连接条目指定 SOCKS 守护进程应允许还是拒绝某个请求。

本节包括以下主题：

创建连接条目

创建连接条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Connections" 链接。
3. 单击 "Add" 按钮。
4. 从 "Authentication Type" 下拉式列表中，选择此访问控制行所适用的验证方法。
5. 从 "Connection Type" 下拉式列表中，选择该行所匹配的命令类型。可能的命令类型有：
   - **Connect**
   - **Bind**
   - **UDP**
   - **All**
6. 在 "Source Host Mask" 字段中，输入连接控制条目所适用的主机的 IP 地址或主机名。如果输入的是 IP 地址，地址后面应跟一个正斜杠以及要应用于源 IP 地址的掩码。SOCKS 服务器会将此掩码应用于源 IP 地址来确定它是否是有效主机。请勿在主机掩码条目中使用空格。如果不输入主机掩码，则连接条目适用于所有主机。

   例如，可在 "host mask" 字段输入 155.25.0.0/255.255.0.0。如果主机的 IP 地址是 155.25.3.5，则 SOCKS 服务器会将该掩码应用于该 IP 地址，并断定主机的 IP 地址与连接控制条目所适用的 IP 地址 (155.25.0.0) 匹配。
7. 在 "Port Range" 字段中，输入连接控制条目所适用的源计算机端口。请勿在端口范围条目中使用空格。如果不指定端口范围，则连接条目适用于所有端口。

   可以使用方括号 [ ] 包括范围两端的端口号，也可使用圆括号 ( ) 将它们排除在外。例如，[1000-1010] 表示其间包括 1000 和 1010 在内的所有端口号，而 (1000-1010) 表示其间不包括 1000 和 1010 在内的所有端口号。也可混合使用方括号和圆括号。例如，(1000-1010] 表示 1000 与 1010 之间不包括 1000 但包括 1010 在内的所有号码。
8. 在 "Destination Host Mask" 字段中，输入连接条目所适用的 IP 地址或主机名。如果输入的是 IP 地址，地址后面应跟一个正斜杠以及要应用于传入 IP 地址的掩码。SOCKS 服务器会将此掩码应用于目标计算机的 IP 地址来确定它是否是有效目标主机。请勿在主机掩码条目中使用空格。如果不输入目标主机掩码，则连接条目适用于所有主机。

例如，可在目标主机掩码字段中输入 155.25.0.0/255.255.0.0。如果目标主机的 IP 地址是 155.25.3.5，则 SOCKS 服务器会将该掩码应用于该 IP 地址，并断定目标主机的 IP 地址与代理条目所适用的 IP 地址 (155.25.0.0) 匹配。

9. 在 "Port Range" 字段中，输入连接控制条目所适用的目标主机端口。请勿在端口范围条目中使用空格。如果不输入端口范围，则连接条目适用于所有端口。

注 大多数 SOCKS 应用程序都请求端口 0 来执行绑定请求，这表示它们没有端口首选项。因此，与绑定相应的目标端口范围始终都应包括端口 0。

可以使用方括号 [ ] 包括范围两端的端口号，也可使用圆括号 ( ) 将它们排除在外。例如，[1000-1010] 表示其间包括 1000 和 1010 在内的所有端口号，而 (1000-1010) 表示其间不包括 1000 和 1010 在内的所有端口号。也可混合使用方括号和圆括号。例如，(1000-1010] 表示 1000 与 1010 之间不包括 1000 但包括 1010 在内的所有号码。

10. 在 "User Group" 字段中，输入想要允许或拒绝访问的组。如果未指定组，则连接条目适用于所有用户。
11. 从 "Action" 下拉式列表中，为所创建的连接选择允许或拒绝访问。
12. 从 "Insert" 下拉式列表中，选择此条目在 `socks5.conf` 文件中的位置，然后单击 "OK"。由于可以发出多个连接指令，所以必须指定其评判顺序。

编辑连接条目

编辑连接条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Connections" 链接。
3. 选择要编辑的连接条目，然后单击 "Edit" 按钮。
4. 根据需要进行更改，然后单击 "OK"。

删除连接条目

删除连接条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Connections" 链接。
3. 选择要删除的连接条目，然后单击 "Delete" 按钮。

移动连接条目

各条目按其在 `socks5.conf` 文件中出现的顺序进行评判。可以通过移动来更改其顺序。

移动连接条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Connections" 链接。
3. 选择要移动的连接条目，然后单击 "Move" 按钮。
4. 从 "Move" 下拉式列表中，选择此条目在 `socks5.conf` 文件中的位置，然后单击 "OK"。

配置 SOCKS v5 服务器链

可以采用与 Proxy Server 相同的方式将多个 SOCKS 服务器链在一起，这表示一个 SOCKS 服务器可以路经另一 SOCKS 服务器。

配置 SOCKS 服务器链

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Routing" 链接。
3. 在 "Server Chaining" 部分，输入用于向链式 Proxy Server 进行验证的用户名和口令（如果代理链中的下游代理服务器要求验证才会为请求提供服务），然后单击 "OK"。

配置路由选择条目

可以使用路由选择条目来配置 Proxy Server，使其通过 SOCKS 服务器为请求选择路由。路由选择条目有两种类型，即 SOCKS v5 路由和 SOCKS v5 代理路由：

- SOCKS v5 路由用于确定 SOCKS 守护进程应对特定 IP 地址使用哪个接口。
- SOCKS v5 代理路由用于确定哪些 IP 地址可通过另一 SOCKS 服务器进行访问，以及该 SOCKS 服务器是否直接连接到主机。通过 SOCKS 服务器进行路由选择时，代理路由很重要。

本节包括以下主题：

创建 SOCKS v5 路由选择条目

创建路由选择条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Routing" 链接。
3. 在 "Routing" 部分，单击 "Add" 按钮。
4. 在 "Host Mask" 字段中，输入与拨入和拨出连接必须经过的指定接口相对应的 IP 地址或主机名。如果输入的是 IP 地址，地址后面应跟一个正斜杠以及要应用于传入 IP 地址的掩码。SOCKS 服务器会将此掩码应用于 IP 地址来确定它是否是有效主机。请勿在主机掩码条目中使用空格。如果不输入主机掩码，则 SOCKS v5 条目适用于所有主机。

   例如，可在 "host mask" 字段输入 155.25.0.0/255.255.0.0。如果主机的 IP 地址是 155.25.3.5，则 SOCKS 服务器会将该掩码应用于该 IP 地址，并断定主机的 IP 地址与路由选择条目所适用的 IP 地址 (155.25.0.0) 匹配。

5. 在 "Port Range" 字段中，输入与拨入和拨出连接必须经过的指定接口相对应的端口。端口范围不能含有空格。如果不指定端口范围，则 SOCKS v5 条目适用于所有端口。

   可以使用方括号 [ ] 包括范围两端的端口号，也可使用圆括号 ( ) 将它们排除在外。例如，[1000-1010] 表示其间包括 1000 和 1010 在内的所有端口号，而 (1000-1010) 表示其间不包括 1000 和 1010 在内的所有端口号。也可混合使用方括号和圆括号。例如，(1000-1010] 表示 1000 与 1010 之间不包括 1000 但包括 1010 在内的所有号码。

6. 在 "Interface/Address" 字段中，输入拨入和拨出连接必须经过的接口的 IP 地址或名称。

7. 从 "Insert" 下拉式列表中，选择此条目在 `socks5.conf` 文件中的位置，然后单击 "OK"。由于可以采用多种路由选择方法，所以必须指定其评判顺序。

注 拨入和拨出连接都应使用指定的接口，否则，将会因传入路由不同于所配置的接口而收到错误消息。

创建 SOCKS v5 代理路由选择条目

创建代理路由选择条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Routing" 链接。
3. 在 "Proxy Routing" 部分，单击 "Add" 按钮。
4. 从 "Proxy Type" 下拉式列表中，选择所路经的 Proxy Server 的类型。可用选项如下：
   - **SOCKS v5**
   - **SOCKS v4**
   - **Direct connection**
5. 在 "Destination Host Mask" 字段中，输入连接条目所适用的 IP 地址或主机名。如果输入的是 IP 地址，地址后面应跟一个正斜杠以及要应用于传入 IP 地址的掩码。SOCKS 服务器会将此掩码应用于目标计算机的 IP 地址来确定它是否是有效目标主机。请勿在主机掩码条目中使用空格。如果不输入目标主机掩码，则连接条目适用于所有主机。

   例如，可在 "destination host mask" 字段输入 155.25.0.0/255.255.0.0。如果目标主机的 IP 地址是 155.25.3.5，则 SOCKS 服务器会将该掩码应用于该 IP 地址，并断定目标主机的 IP 地址与代理条目所适用的 IP 地址 (155.25.0.0) 匹配。

6. 在 "Destination Port Range" 字段中，输入代理条目所适用的目标主机端口。请勿在端口范围条目中使用空格。如果不指定端口范围，则代理条目适用于所有端口。

   可以使用方括号 [ ] 包括范围两端的端口号，也可使用圆括号 ( ) 将它们排除在外。例如，[1000-1010] 表示其间包括 1000 和 1010 在内的所有端口号，而 (1000-1010) 表示其间不包括 1000 和 1010 在内的所有端口号。也可混合使用方括号和圆括号。例如，(1000-1010] 表示 1000 与 1010 之间不包括 1000 但包括 1010 在内的所有号码。

7. 在 "Destination Proxy Address" 字段中，输入要使用的 Proxy Server 的主机名或 IP 地址。

8. 在 "Destination Proxy Port" 字段中，输入 Proxy Server 对于 SOCKS 请求将要侦听的端口号。

9. 从 "Insert" 下拉式列表中，选择此条目在 `socks5.conf` 文件中的位置，然后单击 "OK"。由于可以采用多种路由选择方法，所以必须指定其评判顺序。

编辑路由选择条目

编辑路由选择条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Routing" 链接。
3. 选择要编辑的条目，然后单击 "Edit" 按钮。
4. 根据需要进行更改，然后单击 "OK"。

删除路由选择条目

删除路由选择条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Routing" 链接。
3. 选择要删除的条目，然后单击 "Delete" 按钮。

移动路由选择条目

各条目按其在 socks5.conf 文件中出现的顺序进行评判。可以通过移动来更改其顺序。

移动路由选择条目

1. 访问服务器实例的 Server Manager，然后单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Routing" 链接。
3. 选择要移动的条目，然后单击 "Move" 按钮。
4. 从 "Move" 下拉式列表中，选择此条目在 socks5.conf 文件中的位置，然后单击 "OK"。

第 16 章

管理模板和资源

可以通过模板将 URL 组合在一起，这样便能够配置代理服务器对它们的处理方式。可以使代理服务器视客户机尝试检索的 URL 而采取不同的行为。例如，从特定域访问 URL 时可能要求客户机进行验证（键入用户名和口令）。或者可能拒绝访问指向图像文件的 URL。可以根据文件类型配置不同的高速缓存刷新设置。

本章包括以下各节：

关于模板

模板是 URL（称作资源）的集合。资源可以是单个 URL、具有某些共性的一组 URL 或整个协议。命名并创建模板，然后使用正则表达式将 URL 分配给该模板。这意味着可以对代理服务器进行配置，使其以不同方式处理对不同 URL 的请求。模板可以包括能够用正则表达式创建的任何 URL 模式。表 16-1 列出了默认资源并提供了其他模板的一些概念。

表 16-1 资源正则表达式通配符模式

正则表达式模式	配置的内容
`ftp://.*`	所有 FTP 请求
`http://.*`	所有 HTTP 请求
`https://.*`	所有安全的 HTTP 请求
`gopher://.*`	所有 Gopher 请求
`connect://.*:443`	到 HTTPS 端口的所有 SSL（安全）事务。
`http://home\.example\.com.*`	`home.example.com` Web 站点上的所有文档。
`.*\.gif.*`	任何包括字符串 `.gif` 的 URL
`.*\.edu.*`	任何包括字符串 `.edu` 的 URL
`http://.*\.edu.*`	任何转到 `.edu` 域中计算机的 URL

了解正则表达式

Proxy Server 让您可以使用正则表达式来识别资源。正则表达式指定字符串的模式。在代理服务器中，正则表达式用于查找 URL 中的匹配模式。

下面是正则表达式的一个示例：

```
[a-z]*://[^:/]*\.abc\.com.*>
```

该正则表达式匹配来自 `.abc.com` 域的所有文档。文档可以采用任何协议，可以使用任何文件扩展名。

表 16-2 包含正则表达式及其相应的含义。

表 16-2 正则表达式及其含义

表达式	含义
.	匹配除新行外的任意单个字符。
x?	匹配正则表达式 x 的零个或一个具体值。

表 16-2 正则表达式及其含义

表达式	含义
*x**	匹配正则表达式 x 的零个或更多个具体值。
x+	匹配正则表达式 *x* 的一个或更多个具体值。
x{n,m}	匹配字符 *x*，其中 *x* 至少出现 *n* 次，但不超过 *m* 次。
x{n,}	匹配字符 *x*，其中 *x* 至少出现 *n* 次。
x{n}	匹配字符 *x*，其中 *x* 正好出现 *n* 次。
[abc]	匹配方括号中包括的任意字符。
[^abc]	匹配方括号中未包括的任意字符。
[a-z]	匹配方括号中指定范围内的任意字符。
x	匹配字符 *x*，其中 *x* 不是特殊字符。
\x	取消特殊字符 *x* 的含义。
"x"	取消特殊字符 *x* 的含义。
xy	匹配正则表达式 *x* 具体值及后跟的正则表达式 *y* 具体值。
x|y	匹配正则表达式 *x* 或正则表达式 *y*。
^	匹配字符串的开头。
$	匹配字符串的结尾。
(x)	将正则表达式分组。

下例说明如何使用表 16-2 中的部分正则表达式。

```
[a-z]*://([^.:/]*[:/]|.*\.local\.com).*"
```

- `[a-z]*` 匹配任何协议的文档。
- `://` 匹配 (:) 后跟 (//)。
- `[^.:/]*[:/]` 匹配任何不包括 (.)、(:) 或 (/) 但后跟 (:) 或 (/) 的字符串。因此它匹配未完全限定的主机名和具有端口号的主机。
- `|.*\.local\.com` 不匹配 local.com 这样的全限定域名主机名，但匹配 .local.com 域中的文档。

- .*" 匹配具有任何文件扩展名的文档。

注 如表 16-2 中所做的说明，可以使用反斜杠将特殊字符转义或取消特殊字符的含义。句号和问号等字符有特殊含义，因此，如果使用这些字符来代表其自身，必须对它们进行转义。特别是句号，它存在于许多 URL 中。因此，要在正则表达式中取消句号的特殊含义，需要在其前面加上一个反斜杠。

了解通配符模式

可以创建通配符模式列表，通过它们能够指定可以从站点访问的 URL。通配符可以是正则表达式或 shell 表达式形式，具体视用途而定。一般而言：

- 为匹配目标 URL 的任何模式使用正则表达式。这些 URL 包括 <Object ppath=...>、URL 过滤器以及 NameTrans、PathCheck 和 ObjectType 函数。
- 为匹配外来客户机或用户 ID 的任何模式使用 shell 表达式，这些 ID 包括用于访问控制的用户名和组、外来用户的 IP 地址或 DNS 名称（例如，<Client dns=...>）。

使用正则表达式通配符模式可以指定若干个 URL。可以通过通配符按域名或按包含给定词语的任何 URL 进行过滤。例如，可能需要阻止访问包含字符串 “careers” 的 URL。要达到此目的，可以指定 `http://.*careers.*` 作为模板的正则表达式。

创建新模板

可以使用正则表达式通配符模式创建模板。然后可以配置只影响在该模板中指定的 URL 的特征。例如，可以为 `.GIF` 图像使用一种类型的高速缓存配置，而为纯 `.HTML` 文件使用另一种类型的高速缓存配置。

创建模板

1. 访问 Server Manager 并单击 "Templates" 选项卡。

   单击 "Create Template" 链接。将显示 "Create Template" 页面。

2. 在 "Template Name" 字段中，键入要创建的模板的名称，然后单击 "OK"。

   应键入易记的名称。Server Manager 提示您保存并应用更改。可以在为模板创建正则表达式后保存更改，如其余步骤中所述。

应用模板

应用模板

1. 访问 Server Manager 并单击 "Templates" 选项卡。
2. 单击 "Apply Template" 链接。将显示 "Apply Template" 页面。
3. 在 "URL Prefix Wildcard" 字段中键入正则表达式通配符模式，其中包括要在模板中包括的所有 URL。
4. 从 "Template" 列表中选择刚添加的新模板的名称。
5. 单击 "OK"。
6. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮以应用更改。

删除模板

可以删除现有模板。删除模板时将一并删除模板的所有关联配置。例如，如果为模板 TEST 中的所有 URL 设置了访问控制，则删除 TEST 模板时将同时删除对该模板包含的 URL 的访问控制。

删除模板

1. 访问 Server Manager 并单击 "Templates" 选项卡。
2. 单击 "Remove Template" 链接。将显示 "Remove Template" 页面。
3. 从 "Remove" 列表中选择模板。
4. 单击 "OK"。
5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

查看模板

可以查看和编辑在 Server Manager 中创建的模板。

编辑模板

1. 访问 Server Manager 并单击 "Templates" 选项卡。
2. 单击 "View Template" 链接。将显示 "View Template" 页面。模板显示在一个表格中，其中列出了模板的正则表达式和模板名称。
3. 要编辑现有模板，请单击 "Edit Template Assignment" 链接，随后将转到 "Apply Template" 页面。

删除资源

可以通过 "Remove Resource" 页面删除整个正则表达式对象及其相应的配置。例如，可以删除 gopher 资源，从而从代理服务器的配置文件中删除与该资源关联的所有设置。

删除资源

1. 访问 Server Manager 并单击 "Templates" 选项卡。
2. 单击 "Remove Resource" 链接。将显示 "Remove Resource" 页面。
3. 通过从 "Remove" 下拉式列表中进行选择来选取要删除的资源。
4. 单击 "OK"。
5. 单击 "Restart Required"。将显示 "Apply Changes" 页面。
6. 单击 "Restart Proxy Server" 按钮以应用更改。

第 17 章

使用客户机自动配置文件

如果有多个代理服务器支持众多客户机，可以使用客户机自动配置文件来配置所有浏览器客户机。自动配置文件包含一个 JavaScript 函数，该函数用于确定访问各种 URL 时浏览器所使用的代理服务器（如果有）。

浏览器会在启动时加载自动配置文件。每当用户单击 URL 链接或类型时，浏览器都会使用该配置文件来确定是否应使用代理服务器，若如此，还要确定应使用哪个代理服务器。利用此特性，可以快速配置组织中的所有浏览器实例。可以采用多种方式向客户机提供自动配置文件。

- 可将代理服务器用作返回自动配置文件的 Web 服务器。将浏览器指向代理服务器的 URL。通过使代理服务器担当 Web 服务器，可将自动配置文件保存在一个地方，这样，当需要进行更新时，只需更改一个文件即可。
- 可在 Web 服务器、FTP 服务器或是浏览器有权访问的任何网络目录上存储该文件。通过向浏览器提供该文件的 URL 来配置浏览器，使其可以找到该文件，因而可以使用任何常规的 URL。如果需要执行复杂计算（例如，如果组织中存在大型代理链），可以编写一个 Web 服务器 CGI 程序，根据该文件的具体访问者输出不同的文件。
- 可将自动配置文件与每个浏览器副本一起存储在本地；但是，如果需要更新该文件，则须将该文件的副本分发给每个客户机。

创建自动配置文件可以采用两种方式：可使用 Server Manager 中的页面，也可手动创建该文件。本章后面提供有创建此类文件的指示说明。

本章包括以下各节：

了解自动配置文件

将此特性放在本书进行记述的原因是，作为管理 Proxy Server 的人员，您很有可能也会创建和分发客户机自动配置文件。

自动配置文件的作用

自动配置文件的编写语言是 JavaScript，它是一种基于对象的小型脚本语言，用于开发客户机和服务器 Internet 应用程序。浏览器负责对 JavaScript 文件进行解释。

浏览器会在首次加载时下载自动配置文件。可将该文件保存在浏览器使用 URL 可以访问到该文件的任何位置。例如，可将该文件保存在 Web 服务器上。倘若浏览器可以使用 file:// URL 访问到该文件，甚至可以将其保存在网络文件系统上。

代理配置文件是用 JavaScript 编写的。该 JavaScript 文件定义了单个函数（称为 **FindProxyForURL**），用于确定浏览器应对每个 URL 使用的代理服务器（如果有）。浏览器会向该 JavaScript 函数发送两个参数：浏览器运行所在系统的主机名以及浏览器想要获取的 URL。该 JavaScript 函数会向浏览器返回一个值，告知它该如何继续执行。

利用自动配置文件可以针对各种类型的 URL、各种服务器甚至是一天的各个时间，指定不同的代理服务器（或根本不指定任何代理服务器）。换言之，可以有多个专门的代理服务器，例如，可使一个提供 .com 域服务，使另一个提供 .edu 域服务，而使再一个提供其他一切服务。这样即可将负载分开并提高代理服务器磁盘的使用效率，因为任何文件在高速缓存中均只有一个副本（而不是所有代理服务器全都存储相同的文档）。

自动配置文件还支持代理服务器故障转移，因此，如果某个代理服务器不可用，浏览器会透明地切换到另一个代理服务器。

以 Web 服务器形式访问代理服务器

可在代理服务器上存储一个或多个自动配置文件，并使代理服务器充当 Web 服务器，对于后者，自动配置文件是其仅有的文档。这样，代理服务器管理员即可维护组织中客户机所需的代理自动配置文件。还可以将这些文件保存在一个中心位置，如此一来，如果必须更新这些文件，则只需更新一次，所有浏览器客户机都会自动获得更新。

将代理自动配置文件保存在 *server- root*/proxy-server*id*/pac/ 目录中。在浏览器中输入代理自动配置文件的 URL，为此，只需在 "Proxies" 选项卡中键入该文件的 URL 即可。代理服务器的 URL 具有以下格式：

`http://`*`proxy.domain:port/URI`*

例如，URL 可以是 `http://proxy.example.com`。无需指定 URI（跟在 host:port 组合后面的 URL 部分）；但是，如果确要使用 URI，则可使用模板控制对各个自动配置文件的访问。例如，如果创建一个称为 /test 的 URI，其中含有一个称为 `/proxy.pac` 的自动配置文件，则可创建一个资源模式为 `http://proxy.mysite.com:8080/test/.*` 的模板。然后，可以使用该模板具体设置对该目录的访问控制。

可创建多个自动配置文件，并通过不同的 URL 对其进行访问。表 17-1 列出了一些示例 URI 以及客户机对其进行访问时将会使用的 URL。

表 17-1 样例 URI 及相应的 URL

URI（路径）	代理服务器的 URL
/	http://proxy.mysite.com
/employees	http://proxy.mysite.com/employees
/group1	http://proxy.mysite.com/group1
/managers	http://proxy.mysite.com/managers

对反向代理服务器使用 Pac 文件

鉴于反向代理服务器的工作方式，可能很难使代理服务器既担当反向代理服务器又为 `.pac` 文件提供服务。这是因为代理服务器在获得文件请求后，需要确定所请求的是本地 `.pac` 文件还是远程文档。

要使代理服务器在维护和服务于 `.pac` 文件之外还担当反向代理服务器，需要手动编辑 `obj.conf` 文件，以确保各 NameTrans 函数的顺序正确无误。

通过创建正则映射可使代理服务器担当反向代理服务器。这通常会示意代理服务器将所有请求路由至远程内容服务器。可添加代理自动配置文件，并将其映射到特定目录，如 /pac。在此情况下，任何要获取 `.pac` 文件的客户机都将使用如下的 URL：

`http://proxy.mysite.com/pac`

注意 但是，对于此映射，必须确保远程内容服务器没有类似的目录。

编辑 obj.conf 文件，以确保代理自动配置文件的指令和函数出现在其他任何映射之前。此类指令和函数必须最先出现，因为代理服务器在为请求提供服务之前，通常要先运行所有的 NameTrans 函数。然而，使用自动配置文件，代理服务器可立即识别路径并返回 .pac 文件。

以下是 obj.conf 文件的一个示例，它使用了反向代理服务器并维护着一个自动配置文件：

```
<Object name="default">
NameTrans from="file:" fn="map" to="ftp:"
NameTrans from="/pac" fn="pac-map" name="file" to="/ns-home/proxy/pac/proxy.pac"
NameTrans fn="redirect" from="http://foo.*" url="http://www.acme.com"
NameTrans from="/ns-icons" fn="pfx2dir" dir="/ns-home/ns-icons" name="file"
NameTrans fn="reverse-map" from="http://web.acme.com" to="http://proxy.acme.com:8080"
NameTrans fn="map" from="http://proxy.acme.com:8080" to="http://web.acme.com"
NameTrans fn="map" from="/" to="http://web.acme.com"
PathCheck fn="url-check"
Service fn="deny-service"
AddLog fn="flex-log" name="access"
AddLog fn="urldb-record"
</Object>
```

使用 Server Manager 页面创建自动配置文件

使用 Server Manager 页面创建自动配置文件

1. 访问 Server Manager，然后选择 "Routing" 选项卡。
2. 单击 "Create/Edit Autoconfiguration File" 链接。出现一个页面，其中列出了代理服务器系统上现有的任何自动配置文件。您可以单击自动配置文件对其进行编辑。余下的步骤将介绍如何创建新文件。
3. 键入客户机从代理服务器获取自动配置文件时使用的可选 URI，它是 URL 的路径部分。例如，键入 / 可使客户机以代理服务器主文档（类似于 Web 服务器的 index.html 文件）形式访问该文件，此时，客户机在访问代理服务器的自动配置文件时将只使用域名。可以使用多个 URI，并分别为各个 URI 创建自动配置文件。
4. 键入自动配置文件的名称，使用 .pac 扩展名。如果只有一个文件，可将其简单称为 proxy.pac（pac 是 proxy autoconfiguration（代理自动配置）的缩写）。所有自动配置文件都是含有单个 JavaScript 函数的 ASCII 文本文件。

5. 单击 "OK"。出现另一个页面。使用此页面创建自动配置文件。客户机按顺序完成此页面上的各项。此页面上的项目包括：

- **Never Go Direct To Remote Server** 示意 Navigator 始终使用您的代理服务器。可以指定一个辅助代理服务器，以便在您的代理服务器未运行时使用。
- **Go Direct To Remote Server When** 可在某些情况下绕过代理服务器。Navigator 按照以下选项在此页面上的列出顺序确定各种情况：
  - **Connecting To Non-fully Qualified Host Names** 示意 Navigator 在用户仅指定计算机名时直接转至服务器。例如，如果有一台称为 `winternal.mysite.com` 的内部 Web 服务器，用户可以只键入 `http://winternal`，而不用键入全限定域名。在这种情况下，Navigator 直接转至 Web 服务器而非代理服务器。
  - **Connecting To A Host In Domain** 允许指定多达三个 Navigator 可以直接访问的域名。指定域名时应以园点字符开头。例如，可键入 `.example.com`。
  - **Connecting To A Resolvable Host** 使 Navigator 在客户机可以解析主机时直接转至服务器。通常在将 DNS 设置为仅解析本地（内部）主机时使用此选项。连接本地网络之外的服务器时，客户机可以使用代理服务器。

注意 上述选项使客户机在每次请求时都询问 DNS。因而对性能造成负面影响，并体现在客户机上。由于性能影响，应避免使用此选项。

  - **Connecting To A Host In Subnet** 使 Navigator 在客户机访问特定子网中的服务器时直接转至该服务器。如果某组织在某个地理区域内分布许多子网，此选项会很有用。例如，某些公司可能只有一个域名，该域名适用于世界范围的各个子网，但每个子网均为某个特定区域所专有。

注意 上述选项使客户机在每次请求时都询问 DNS。因而对性能造成负面影响，并体现在客户机上。由于性能影响，应避免使用此选项。

  - **Except When Connecting To Hosts** 允许指定对于直接转至服务器规则的例外情况。例如，如果键入 `.example.com` 作为要直接转到的域，可以将转至 `home.example.com` 作为例外情况处理。这会示意 Navigator 在转至 `home.example.com` 时使用您的代理服务器，但直接转至 `example.com` 域中的其他任何服务器。
  - **Secondary Failover Proxy** 用于指定一个辅助代理服务器，以便在您的代理服务器未运行时使用。
  - **Failover Direct** 示意 Navigator 在您的代理服务器未运行时直接转至这些服务器。如果指定辅助故障转移代理服务器，Navigator 会在直接转至服务器前先试用辅助代理服务器。

6. 单击 "OK" 创建自动配置文件。该文件存储在 *server-root*/proxy-server*id*/pac 目录中。您将得到一条确认消息，说明该文件已正确创建。重复上述步骤，创建所需数量的自动配置文件。

创建了自动配置文件后，确保告诉所有使用您代理服务器的人员指向正确的自动配置文件，或亲自配置 Navigator 的各个副本。

手动创建自动配置文件

本节介绍如何手动创建自动配置文件。

代理自动配置文件是用客户端 JavaScript 编写的。每个文件均含有单个称为 **FindProxyForURL** 的 JavaScript 函数，用于确定浏览器应对每个 URL 使用的代理服务器（如果有）。浏览器会向该 JavaScript 函数发送两个参数：目标起始服务器的主机名以及浏览器想要获取的 URL。该 JavaScript 函数会向 Navigator 返回一个值，告知它该如何继续执行。下节将介绍函数语法和可能的返回值。

FindProxyForURL 函数

FindProxyFor URL 函数的语法如下：

```
function FindProxyForURL(url, host)
{
   ...
}
```

浏览器访问每个 URL 时，都会发送 **url** 和 **host** 参数并采用以下方式调用该函数：

```
ret = FindProxyForURL(url, host);
```

url 是正在浏览器中访问的完整 URL。

host 是从正在访问的 URL 中提取的主机名。这样做仅仅是为了方便；它与 **://** 和其后的第一个 **:** 或 **/** 之间的字符串相同。此参数中不包括端口号。可根据需要从 URL 中提取它。

ret（返回值）是一个用于描述配置的字符串。

函数返回值

自动配置文件含有函数 **FindProxyForURL**。此函数使用客户机主机名和所访问的 URL 作为参数。该函数会返回单个字符串，告知浏览器该如何继续执行。如果该字符串为空值，则不能使用任何代理服务器。该字符串可以包含表 17-2 所示的任意数目的组块，其间以分号隔开。

表 17-2 FindProxyForURL 返回值

返回值	结果发生的浏览器操作
`DIRECT`	不经过任何代理服务器直接与服务器进行连接。
`PROXY` *host:port*	使用指定的代理服务器和端口号。如果有多个以分号隔开的值，则使用第一个代理服务器。如果该代理服务器失败，则使用下一个代理服务器，依此类推。
`SOCKS` *host:port*	使用指定的 SOCKS 服务器。如果有多个以分号隔开的值，则使用第一个代理服务器。如果该代理服务器失败，则使用下一个代理服务器，依此类推。

如果浏览器遇到不可用的代理服务器，浏览器将在 30 分钟后自动重试先前无响应的代理服务器，一个小时后会再次进行尝试，依此类推，每次间隔时间为 30 分钟。这意味着，如果暂时关闭代理服务器，客户机至多在其重新启动后 30 分钟便会重新开始使用该代理服务器。

如果所有代理服务器均停用且未指定 DIRECT 返回值，浏览器将询问用户是否暂时忽略代理服务器而尝试直接进行连接。Navigator 将询问是否应在 20 分钟后重试代理服务器，接着过 20 分钟会再次询问，依此类推，每次间隔时间为 20 分钟。

在下例中，返回值告知浏览器使用端口 8080 上称为 `w3proxy.example.com` 的代理服务器，但如果该代理服务器不可用，浏览器将使用端口 8080 上称为 `proxy1.example.com` 的代理服务器：

```
PROXY w3proxy.example.com:8080; PROXY proxy1.example.com:8080
```

在下一个示例中，主代理服务器为 `w3proxy.example.com:8080`；如果该代理服务器不可用，浏览器将使用 `proxy1.example.com:8080`。如果两个代理服务器均不可用，则浏览器将直接转至服务器（过 20 分钟，浏览器会询问用户是否应重试第一个代理服务器）：

```
PROXY w3proxy.example.com:8080; PROXY proxy1.example.com:8080; DIRECT
```

JavaScript 函数与环境

JavaScript 有多个预定义的函数和环境条件，它们对于执行代理很有用。这些函数中的每一个均会检查是否满足某个特定条件，然后返回一个真值或假值。相关的实用程序函数例外，因为他们返回的是 DNS 主机名或 IP 地址。可在主 **FindProxyForURL** 函数中使用这些函数来确定要发送给浏览器的返回值。有关这些函数的具体使用方法，参见本章后面的示例。

本节将对每个函数或环境条件进行介绍。适用于浏览器与代理服务器集成的函数和环境条件有：

基于主机名的函数

- dnsDomainIs()
- isInNet()
- isPlainhost name()
- isResolvable()
- localHostOrDomainIs()

相关的实用程序函数：

- dnsDomainLevels()
- dnsResolve()
- myIpAddress()

基于 URL/主机名的条件：

- shExpMatch()

基于时间的条件：

- dateRange()
- timeRange()
- weekdayRange()

基于主机名的函数

通过基于主机名的函数，可以使用主机名或 IP 地址来确定要使用的代理服务器（如果有）。

dnsDomainIs(host, domain)

dnsDomainIs() 函数检测 URL 主机名是否属于给定的 DNS 域。如第 341 页的“示例 1：代理除本地主机外的所有服务器”和第 341 页的“示例 2：代理防火墙外面的本地服务器”中所示，当您要将浏览器配置成不对本地域使用代理服务器时，此函数很有用。

在某些情况下会基于 URL 所属的 DNS 域从一组代理服务器中选择接收请求的代理服务器，当您在这些情况下使用多个代理服务器进行负载平衡时，此函数也很有用。例如，如果负载平衡方式是将含有 .edu 的 URL 定向到一个代理服务器，而将含有 .com 的那些 URL 定向到另一个代理服务器，则可以使用 **dnsDomainIs()** 来检查 URL 主机名。

参数：
host 是 URL 中的主机名。

domain 是用以测试主机名的域名。

返回值：
true 或 false

示例：
以下语句将为 true：

```
dnsDomainIs("www.example.com", ".example.com")
```

以下语句将为 false：

```
dnsDomainIs("www", ".example.com")
dnsDomainIs("www.mcom.com", ".example.com")
```

isInNet(host, pattern, mask)

利用 **isInNet()** 函数可将 URL 主机名解析为 IP 地址，并测试其是否属于掩码所指定的子网。这与 SOCKS 所使用的 IP 地址模式匹配属于同一类型。参见第 342 页的“示例 4：直接连接到子网”。

参数：
host 为 DNS 主机名或 IP 地址。如果传递的是主机名，此函数会将其解析成 IP 地址。

pattern 是点分隔格式的 IP 地址模式

mask 为 IP 地址模式掩码，用于确定应对 IP 地址的哪些部分进行匹配。值为 0 表示忽略； 255 表示匹配。如果主机的 IP 地址与指定的 IP 地址模式匹配，则此函数为 true。

返回值：
true 或 false

示例：
仅当主机的 IP 地址与 198.95.249.79 完全匹配时，此语句才为 true：

```
isInNet(host, "198.95.249.79", "255.255.255.255")
```

仅当主机的 IP 地址与 198.95.*.* 匹配时，此语句才为 true：

```
isInNet(host, "198.95.0.0", "255.255.0.0")
```

isPlainhost name(host)

isPlainhost name() 函数检测所请求 URL 中的主机名是普通主机名还是全限定域名。如第 341 页的“示例 1：代理除本地主机外的所有服务器”和第 341 页的“示例 2：代理防火墙外面的本地服务器”中所示，如果要将 Netscape Navigator 直接连接到本地服务器，则此函数很有用。

参数：
host 为 URL 中的主机名（不包括端口号），只要该主机名不含域名（无带点段）。

返回值：
如果 **host** 是本地的，则为 true ；如果 **host** 是远程的，则为 false

示例：

```
isPlainhost name("host")
```

如果 **host** 形如 www，则返回 true ；如果 host 形如 `www.example.com`，则返回 false。

isResolvable(host)

如果防火墙内的 DNS 仅识别内部主机，则可使用 **isResolvable()** 函数来测试主机名相对于网络是内部的还是外部的。使用此函数，可将浏览器配置成对内部服务器使用直接连接，而仅对外部服务器使用代理服务器。在一些站点，防火墙内的内部主机能够解析其他内部主机的 DNS 域名，但所有外部主机均不可解析，对于此类站点，此函数将很有用。**isResolvable()** 函数通过询问 DNS 尝试将主机名解析成 IP 地址。参见第 342 页的“示例 3：仅代理未解析的主机”

参数：
host 是 URL 中的主机名。此函数会尝试解析该主机名，并在成功时返回 true。

返回值：
如果能解析主机名，则为 true ；如果不能，则为 false

示例：
```
isResolvable("host")
```

如果 **host** 形如 `www` 并且可通过 DNS 进行解析，则此函数返回 true。

localHostOrDomainIs(host, hostdom)

localHostOrDomainIs() 函数指定可以通过全限定域名或普通主机名访问的本地主机。参见第 341 页的“示例 2：代理防火墙外面的本地服务器”。

如果主机名与指定的主机名完全匹配，或者在主机名中没有与非限定主机名匹配的域名部分，则 **localHostOrDomainIs()** 函数返回 `true`。

参数：
host 是 URL 中的主机名。

hostdom 是要匹配的全限定主机名。

返回值：
true 或 false

示例：
以下语句为 true（完全匹配）：

```
localHostOrDomainIs("www.example.com", "www.example.com")
```

以下语句为 true（主机名匹配，未指定域名）：

```
localHostOrDomainIs("www", "www.example.com")
```

以下语句为 false（域名不匹配）：

```
localHostOrDomainIs("www.mcom.com", "www.example.com")
```

以下语句为 false（主机名不匹配）：

```
localHostOrDomainIs("home.example.com", "www.example.com")
```

相关的实用程序函数

利用相关的实用程序函数，可以查明域层级、运行 Netscape Navigator 的主机，或主机的 IP 地址。

dnsDomainLevels(host)

dnsDomainLevels() 函数查找 URL 主机名中的 DNS 层数（圆点数）。

参数：
host 是 URL 中的主机名。

返回值：
DNS 域层数（整数）。

示例：

```
dnsDomainLevels("www")
```

返回 0。

```
dnsDomainLevels("www.example.com")
```

返回 2。

dnsResolve(host)

dnsResolve() 函数解析给定主机（通常来自 URL）的 IP 地址。如果 JavaScript 函数须进行比现有函数所能完成的更高级的模式匹配，则此函数将很有用。

参数：
host 是要解析的主机名。将给定 DNS 主机名解析成 IP 地址，并以点分隔格式的字符串形式将其返回。

返回值：
字符串值形式的点四分 IP 地址

示例：
以下示例将返回字符串 198.95.249.79。

```
dnsResolve("home.example.com")
```

myIpAddress()

当 JavaScript 函数须根据运行浏览器的具体主机而采取不同行为时，**myIpAddress()** 函数将很有用。此函数将返回运行浏览器的那台计算机的 IP 地址。

返回值：
字符串值形式的点四分 IP 地址

示例：
如果在计算机 `home.example.com` 上运行 Navigator，下例将返回字符串 198.95.249.79。

```
myIpAddress()
```

基于 URL/ 主机名的条件

可通过匹配主机名或 URL 来进行负载平衡和路由选择。

shExpMatch(str, shexp)

shExpMatch() 函数匹配 URL 主机名或 URL 本身。此函数主要用于负载平衡以及指向不同代理服务器的 URL 的智能路由选择。

参数：
str 是要比较的任何字符串（例如，URL 或主机名）。

shexp 是用以进行比较的 shell 表达式。

如果字符串与指定的 shell 表达式匹配，则此表达式为 true。参见第 344 页的“示例 6：用 shExpMatch() 平衡代理负载”。

返回值：
true 或 false

示例：
第一个示例返回 true ；第二个返回 false。

```
shExpMatch("http://home.example.com/people/index.html",
           ".*/people/.*")

shExpMatch("http://home.example.com/people/yourpage/index.html",
           ".*/mypage/.*")
```

基于时间的条件

可以使 **FindProxyForURL** 函数根据日期、时间或星期几而采取不同的行为。

dateRange (day, month, year...)

dateRange() 函数检测特定日期或日期范围，如 1996 年 4 月 19 日到 1996 年 5 月 3 日。如果要使 **FindProxyForURL** 函数视当天日期而执行不同操作（例如，如果为其中一个代理服务器安排了定期停机维护时间），则此函数将很有用。

可采用多种方式指定日期范围：

```
dateRange(day)
dateRange(day1, day2)
dateRange(mon)
dateRange(month1, month2)
dateRange(year)
dateRange(year1, year2)
dateRange(day1, month1, day2, month2)
dateRange(month1, year1, month2, year2)
dateRange(day1, month1, year1, day2, month2, year2)
dateRange(day1, month1, year1, day2, month2, year2, gmt)
```

参数：

day 是一个介于 1 到 31 的整数，代表月号。

month 为以下月份字符串之一：

```
JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC
```

year 是一个四位整数，代表年度（例如，1996）。

gmt 或者为字符串 GMT 或者保留为空，前者将以格林威治标准时间进行时间比较，后者假定时间处于当地时区。可在任何调用配置文件中指定 GMT 参数，不过，它始终都是作为最后一个参数。如果只指定了单个值（对于每个类别：day、month、year），则此函数仅在与指定值匹配的日子才会返回真值。如果指定了两个值，则从指定的第一个时间到指定的第二个时间，结果均为 true。

示例：

以下语句在当地时区每月的第一天为 true。

```
dateRange(1)
```

以下语句在格林威治标准时间每月的第一天为 true。

```
dateRange(1, "GMT")
```

以下语句对于每月的上半月为 true。

```
dateRange(1, 15)
```

以下语句在每年的 12 月 24 日为 true。
```
dateRange(24, "DEC")
```

以下语句在 1995 年 12 月 24 日为 true。
```
dateRange(24, "DEC", 1995)
```

以下语句在一年的第一季度为 true。
```
dateRange("JAN", "MAR")
```

以下语句从每年的 6 月 1 日到 8 月 15 日为 true。
```
dateRange(1, "JUN", 15, "AUG")
```

以下语句从 1995 年 6 月 1 日直至 1995 年 8 月 15 日均为 true。
```
dateRange(1, "JUN", 15, 1995, "AUG", 1995)
```

以下语句从 1995 年 10 月到 1996 年 3 月为 true。
```
dateRange("OCT", 1995, "MAR", 1996)
```

以下语句在 1995 全年均为 true。
```
dateRange(1995)
```

以下语句从 1995 年初直至 1997 年末均为 true。
```
dateRange(1995, 1997)
```

timeRange (hour, minute, second...)

timeRange 函数检测某一特定日时间或某一时间范围，如晚 9 点到中午 12 点。如果要使 **FindProxyForURL** 函数视当时具体时间执行不同的操作，则此函数将很有用。

```
timeRange(hour)
timeRange(hour1, hour2)
timeRange(hour1, min1, hour2, min2)
timeRange(hour1, min1, sec1, hour2, min2, sec2)
```

参数：
hour 为小时，范围从 0 到 23。（0 表示午夜，23 表示晚上 11:00）

min 为分钟数，范围从 0 到 59。

sec 为秒数，范围从 0 到 59。

gmt 或者是字符串 GMT 或者未指定，前者表示 GMT 时区，后者表示当地时区。对于每一个参数配置文件均可以使用此参数，而且它始终是最后一个参数。

返回值：
true 或 false

示例：
以下语句从正午到下午 1:00 为 true。
```
timerange(12, 13)
```

以下语句从 GMT 正午时间到下午 12:59 为 true。
```
timerange(12, "GMT")
```

以下语句从上午 9:00 到下午 5:00 为 true。
```
timerange(9, 17)
```

以下语句在午夜到午夜过后 30 秒之间为 true。
```
timerange(0, 0, 0, 0, 0, 30)
```

weekdayRange(wd1, wd2, gmt)

weekdayRange() 函数检测某一特定星期日期或某一星期日期范围，如星期一到星期五。如果要使 **FindProxyForURL** 函数视具体星期日期而执行不同的操作，则此函数将很有用。

参数：
wd1 和 **wd2** 为以下任意一个星期日期字符串：
```
SUN MON TUE WED THU FRI SAT
```

gmt 或者是 GMT 或者省略，前者表示格林威治标准时间，后者表示当地时间。

只有第一个参数 wd1 是强制性的。wd2、gmt 中的任一个或两者皆可省略。

如果只有一个参数，则此函数将在该参数所表示的星期日期返回真值。如果指定字符串 GMT 作为第二个参数，则采用 GMT 时间，否则采用当地时区的时间。

如果 wd1 和 wd2 均被定义，则该条件在当前星期日期介于这两个星期日期之间时为 true。首末日期包括在内。参数顺序很重要；“MON,” “WED” 指星期一到星期三，而 “WED,” “MON” 是从星期三到下周的星期一。

示例：
以下语句从星期一到星期五（当地时区）为 true。
```
weekdayRange("MON", "FRI")
```

以下语句从格林威治标准时间星期一到星期五为 true。
```
weekdayRange("MON", "FRI", "GMT")
```

以下语句在当地时间星期六为 true。
```
weekdayRange("SAT")
```

以下语句在格林威治标准时间星期六为 true。
```
weekdayRange("SAT", "GMT")
```

以下语句从星期五到下星期一为 true（顺序很重要）
```
weekdayRange("FRI", "MON")
```

详细示例

示例 1：代理除本地主机外的所有服务器

在本例中，Netscape Navigator 直接连接到所有未完全限定的主机和处于本地域中的主机。其他一切情况均要经过称为 w3proxy.example.com:8080 的代理服务器。

注 如果代理服务器关闭，则自动进行直接连接。

```
function FindProxyForURL(url, host)
{
    if (isPlainhost name(host) ||
        dnsDomainIs(host, ".example.com") ||
        dnsDomainIs(host, ".mcom.com"))
        return "DIRECT";
    else
        return "PROXY w3proxy.example.com:8080; DIRECT";
}
```

示例 2：代理防火墙外面的本地服务器

本例与上一个示例类似，只是它将对防火墙外面的本地服务器使用代理服务器。如果存在属于本地域而位于防火墙之外的主机（如主 Web 服务器），并且只有通过代理服务器才能访问到这些主机，则使用 **localHostOrDomainIs()** 函数来处理这些例外情况：

```
function FindProxyForURL(url, host)
{
    if ((isPlainhost name(host) ||
    dnsDomainIs(host, ".example.com")) &&
    !localHostOrDomainIs(host, "www.example.com") &&
    !localHostOrDoaminIs(host, "merchant.example.com"))
        return "DIRECT";
    else
        return "PROXY w3proxy.example.com:8080; DIRECT";
}
```

本例对 example.com 域中除本地主机外的一切主机均使用代理服务器。主机 www.example.com 和 merchant.example.com 也要经过代理服务器。

依序处理例外情况可提高效率：**localHostOrDomainIs()** 函数仅对本地域中的 URL 才会执行，而不是对于每个 URL 都要执行。请特别留意**与**表达式前的**或**表达式周围的括号。

示例 3：仅代理未解析的主机

本例适用于所设内部 DNS 只能解析内部主机名的环境，其目的是仅对无法解析的主机使用代理服务器：

```
function FindProxyForURL(url, host)
{
    if (isResolvable(host))
            return "DIRECT";
        else
            return "PROXY proxy.mydomain.com:8080";
}
```

本例每次都需要询问 DNS，为此，应将它与其他规则组合在一起，以便仅在其他规则得不到结果时才询问 DNS：

```
function FindProxyForURL(url, host)
{

    if (isPlainhost name(host) ||
        dnsDomainIs(host, ".mydomain.com") ||
        isResolvable(host))
        return "DIRECT";
    else
        return "PROXY proxy.mydomain.com:8080";
}
```

示例 4：直接连接到子网

在本例中，给定子网中的所有主机将直接进行连接，而其他主机则要经过代理服务器：

```
function FindProxyForURL(url, host)
{
    if (isInNet(host, "198.95.0.0", "255.255.0.0"))
        return "DIRECT";
    else

        return "PROXY proxy.mydomain.com:8080";
}
```

通过在开头添加大量规则，可以最大程度地减少对 DNS 的使用：

```
function FindProxyForURL(url, host)
{
    if (isPlainhost name(host) ||
        dnsDomainIs(host, ".mydomain.com") ||
        isInNet(host, "198.95.0.0", "255.255.0.0"))
```

```
        return "DIRECT";
    else
        return "PROXY proxy.mydomain.com:8080";
}
```

示例 5：用 dnsDomainIs() 平衡代理负载

本例较为复杂。共有四个代理服务器，其中一个充当其他服务器的热备份，这样，如果其余三个当中有任何一个停机，第四个便会接替它工作。其余三个代理服务器基于 URL 模式分担负载，从而使它们的高速缓存变得更加有效（任何文档在这三个服务器上都只有一个副本，而不是在其中每一个上均有一个副本）。负载分配如表 17-3 所示。

表 17-3 平衡代理负载

代理服务器	用途
#1	.com 域
#2	.edu 域
#3	其他所有的域
#4	热备份

所有本地访问均应为直接访问。所有代理服务器都运行于 8080 端口。可以使用 JavaScript 中的 + 运算符来连接字符串。

```
function FindProxyForURL(url, host)
{
    if (isPlainhost name(host) || dnsDomainIs(host, ".mydomain.com"))
        return "DIRECT";

    else if (dnsDomainIs(host, ".com"))
        return "PROXY proxy1.mydomain.com:8080; " +
               "PROXY proxy4.mydomain.com:8080";

    else if (dnsDomainIs(host, ".edu"))
        return "PROXY proxy2.mydomain.com:8080; " +
               "PROXY proxy4.mydomain.com:8080";

    else
        return "PROXY proxy3.mydomain.com:8080; " +
               "PROXY proxy4.mydomain.com:8080";
}
```

示例 6：用 shExpMatch() 平衡代理负载

本例在本质上与示例 5 相同，只不过它使用的是 **shExpMatch()**，而不是 **dnsDomainIs()**。

```
function FindProxyForURL(url, host)
{
if (isPlainhost name(host) || dnsDomainIs(host, ".mydomain.com"))
    return "DIRECT";
else if (shExpMatch(host, "*.com"))
    return "PROXY proxy1.mydomain.com:8080; " +
          "PROXY proxy4.mydomain.com:8080";
else if (shExpMatch(host, "*.edu"))
    return "PROXY proxy2.mydomain.com:8080; " +
          "PROXY proxy4.mydomain.com:8080";
else
    return "PROXY proxy3.mydomain.com:8080; " +
          "PROXY proxy4.mydomain.com:8080";
}
```

示例 7：代理特定协议

可以设置代理服务器，使其用于特定的协议。大多数标准 JavaScript 功能都可以在 **FindProxyForURL()** 函数中使用。例如，要根据协议设置不同的代理服务器，可以使用 **substring()** 函数：

```
function FindProxyForURL(url, host)
{
    if (url.substring(0, 5) == "http:") {
        return "PROXY http-proxy.mydomain.com:8080";
    }
    else if (url.substring(0, 4) == "ftp:") {
        return "PROXY ftp-proxy.mydomain.com:8080";
    }
    else if (url.substring(0, 7) == "gopher:") {
        return "PROXY gopher-proxy.mydomain.com:8080";
    }
    else if (url.substring(0, 6) == "https:" ||
            url.substring(0, 6) == "snews:") {
        return "PROXY security-proxy.mydomain.com:8080";
    }
```

```
    else {
        return "DIRECT";
    }
}
```

使用 **shExpMatch()** 函数也可以实现此目的；例如：

```
...
if (shExpMatch(url, "http:*")) {
    return "PROXY http-proxy.mydomain.com:8080;
}

...
```

第 5 部分

附录

ACL 文件语法

访问控制列表 (ACL) 文件为文本文件，其所含列表定义了何人可以访问 Proxy Server 资源。默认情况下，Proxy Server 使用一个 ACL 文件，其中包含用于访问服务器的所有列表。也可以创建多个 ACL 文件，并在 `obj.conf` 文件中对其进行引用。

Proxy Server 4 使用的 ACL 文件语法不同于 Proxy Server 3.x 中使用的语法。本附录将介绍 ACL 文件及其语法。有关对 Proxy Server 及其资源进行访问控制的详细信息，参见第 135 页的第 8 章“控制对服务器的访问”。Proxy Server 4 发行版支持资源模板，相关说明见于第 319 页的第 16 章“管理模板和资源”。

本附录包含以下各节：

关于 ACL 文件和 ACL 文件语法

所有 ACL 文件都必须遵守特定的格式和语法。ACL 文件为包含一个或多个 ACL 的文本文件。所有 ACL 文件都必须以语法版本号开头。例如：

```
version 3.0;
```

只能有一个版本行，版本行可以位于任何注释行之后。Proxy Server 使用语法版本 3.0。通过在注释行开头使用 # 符号，可以在文件中加入注释。

文件中每个 ACL 的开头语句均定义了其类型。ACL 可以为以下三种类型之一：

- 路径 ACL 指定受其影响的资源的绝对路径。
- 资源 ACL 指定受其影响的模板，如 `http://`、`https://`、`ftp://` 等等。有关模板的更多信息，参见第 319 页的第 16 章“管理模板和资源”。

- 命名 ACL 指定在 obj.conf 文件的资源中引用的名称。服务器随带有一个默认的命名资源，任何用户均可对其进行读访问，而只有 LDAP 目录中的用户可对其进行写访问。尽管可以从 Proxy Server 用户界面创建命名 ACL，但必须在 obj.conf 文件的资源中手动引用该命名 ACL。

路径 ACL 和资源 ACL 可以包含通配符。有关通配符的更多信息，参见第 319 页的第 16 章“管理模板和资源”。

类型行以字母 acl 开头，然后将类型信息括在双引号中，其后跟有分号。例如：

```
acl "default";
acl "http://*.*";
```

所有 ACL 的每个类型信息必须具有唯一名称，即使在不同的 ACL 文件中也是如此。定义了 ACL 的类型后，可以用一个或多个语句定义与 ACL 一起使用的方法（验证语句）以及允许或拒绝哪些人员和计算机进行访问（授权语句）。以下各节介绍了这些语句的语法。

本节包括以下主题：

验证语句

ACL 可以任意指定服务器在处理 ACL 时必须使用的验证方法。以下为三种常规方法：

- 基本（默认）
- 摘要
- SSL

基本和摘要方法要求用户在访问资源之前输入用户名和口令。

SSL 方法要求用户具有客户机证书。要进行验证，必须为 Proxy Server 开启加密功能，而且用户的证书颁发者必须在可信 CA 列表中。

默认情况下，服务器对未指定方法的任何 ACL 都使用基本方法。服务器的验证数据库必须支持用户所发送的摘要验证。

每一验证行均必须指定服务器验证的属性（用户、组或是这两者）。以下验证语句出现在 ACL 类型行之后，它指定对与数据库或目录中的单个用户相匹配的用户进行基本验证：

```
authenticate(user) {
    method = "basic";
};
```

以下示例将 SSL 用作用户和组的验证方法：

```
authenticate(user, group) {
    method = "ssl";
};
```

以下示例允许用户名以单词 `sales` 开头的任何用户进行访问：

```
allow (all) user = "sales*";
```

如果将最后一行更改为 `group = sales`，则 ACL 将会失败，因为未对组属性进行验证。

授权语句

每个 ACL 条目可能包含一个或多个授权语句。授权语句用于指定允许或拒绝哪些用户访问服务器资源。

编写授权语句

编写授权语句时请使用以下语法：

```
allow|deny [absolute] (right[,right...]) attribute expression;
```

以 `allow` 或 `deny` 作为每一行的开头。通常，最好在第一条规则中拒绝所有人访问，接着在后续规则中具体指定允许哪些用户、组或计算机进行访问。这是因为规则具有分层结构。也就是说，如果您允许任何人访问名为 `/my_files` 的目录，而后又允许少数用户访问子目录 `/my_files/personal`，则对子目录的访问控制将不起作用，因为有权访问 `/my_files` 目录的任何人也都有权访问 `/my_files/personal` 目录。为防止出现上述情况，请为子目录创建一条规则，先拒绝任何人访问，然后允许少数需要访问的用户访问。

然而，在某些情况下，如果将默认 ACL 设置为拒绝所有人访问，其他 ACL 规则便不需要 "deny all" 规则。

下面一行语句用于拒绝所有用户的访问：

```
deny (all) user = "anyone";
```

授权语句的分层结构

ACL 的分层结构取决于资源。服务器收到对特定资源的请求时，会建立一个用于申请该资源的 ACL 列表。首先，服务器添加其 obj.conf 文件的 check-acl 语句中列出的命名 ACL。接着，它将附加匹配的路径 ACL 和资源 ACL。此列表的处理顺序与添加顺序相同。除非存在 "absolute" ACL 语句，否则将依次对所有语句求值。如果 "absolute allow" 或 "absolute deny" 语句的求值结果为 "true"，服务器将停止处理并接受此结果。

如果有一个以上的 ACL 匹配，服务器将使用最后一个匹配的语句。但是，如果您使用的是绝对语句，服务器将停止查找其他匹配项，而使用包含该绝对语句的 ACL。如果同一资源有两个绝对语句，服务器将使用文件中的第一个语句并停止查找其他匹配的资源。

```
version 3.0;
acl "default";
authenticate (user,group) {
  prompt="Sun Java System Web Proxy Server";
};
allow (read,execute,list,info) user = "anyone";
allow (write,delete) user = "all";

acl "http://*.*";
deny (all) user = "anyone";
allow (all) user = "joe";
```

属性表达式

属性表达式根据用户名、组名、主机名或 IP 地址来定义允许或拒绝何人访问。以下各行举例说明了如何授予不同人员或计算机访问权限：

- `user = "anyone"`
- `user = "smith*"`
- `group = "sales"`
- `dns = "*.mycorp.com"`
- `dns = "*.mycorp.com,*.company.com"`
- `ip = "198.*"`
- `ciphers = "rc4"`
- `ssl = "on"`

使用 timeofday 属性，还可以限制用户访问服务器的时间（以服务器上的当地时间为准）。例如，您可以使用 timeofday 属性将特定用户限制为在特定时间访问。

请使用 24 时制指定时间，例如，用 0400 指定上午 4:00 或用 2230 指定晚上 10:30。下列示例将名为 guests 的一组用户的访问时间限制在上午 8:00 到下午 4:59 之间：

```
allow (read)
    (group="guests") and
    (timeofday<0800 or timeofday=1700);
```

您还可以限制用户在星期几来访问服务器。请使用以下三个字母的缩写来指定星期几：Sun、Mon、Tue、Wed、Thu、Fri 和 Sat。

以下语句允许 premium 组中的用户在任意一天的任何时间进行访问。discount 组中的用户在周末可以全天访问，而在工作日可在上午 8 点到下午 4:59 以外的任何时间进行访问。

```
allow (read) (group="discount" and dayofweek="Sat,Sun") or
(group="discount" and (dayofweek="mon,tue,wed,thu,fri" and
(timeofday<0800 or timeofday=1700)))
or
(group="premium");
```

表达式运算符

可以在属性表达式中使用各种运算符。圆括号用于说明运算符的优先顺序。对于 user、group、dns 和 ip，可以使用以下运算符：

- and
- or
- not
- =（等于）
- !=（不等于）

对于 timeofday 和 dayofweek，可以使用以下运算符：

- 大于
- <（小于）
- =（大于等于）
- <=（小于等于）

默认的 ACL 文件

安装之后，*server_root*/httpacl/generated.proxy-*serverid*.acl 文件为服务器提供默认设置。在用户界面中创建设置之前，服务器会一直使用工作文件 genwork.proxy-*serverid*.acl。编辑 ACL 文件时，可以在 genwork 文件中进行更改，然后使用 Proxy Server 保存和应用更改。

常规语法项目

输入字符串可以包含以下字符：

- 字母 a 至 z
- 数字 0 至 9
- 句点和下划线

对于其他字符，必须用双引号将字符括起来。

单个语句可以独立成行并以分号结束。多个语句将置于大括号中。项目列表必须用逗号隔开并括在双引号中。

在 obj.conf 中引用 ACL 文件

可以在 obj.conf 文件中引用命名 ACL 或单独的 ACL 文件。这是通过在 PathCheck 指令中使用 check-acl 函数完成的。该行使用以下语法：

```
PathCheck fn="check-acl" acl="aclname"
```

其中，*aclname* 是 ACL 出现在任何 ACL 文件中的唯一名称。

例如，可以向 obj.conf 文件添加以下各行，使用名为 testacl 的 ACL 限制对某个目录的访问：

```
<Object ppath="https://"
PathCheck fn="check-acl" acl="testacl"
</Object
```

在上述示例中，第一行的对象声明了要对其进行访问限制的服务器资源。第二行的 PathCheck 指令使用 check-acl 函数将命名 ACL (testacl) 绑定到该指令出现于的对象。testacl ACL 可以出现于 server.xml 中所引用的任何 ACL 文件中。

调节服务器性能

许多元素影响 Proxy Server 环境中的性能，其中包括代理客户机、Proxy Server、源服务器及网络。本附录介绍用户可以进行的可能会提高 Proxy Server 性能的调整。

本附录包括以下部分：

注意 本附录内容仅供高级管理员使用。调节服务器时应十分小心，在进行任何更改前都必须备份配置文件。

常规性能考虑因素

本部分介绍需要在分析 Proxy Server 性能时加以考虑的一些常规方面。

本节包括以下主题：

访问日志记录

禁用访问日志记录可以提高 Proxy Server 的性能。不过，这样做是有代价的，因为将无从知晓哪些人访问过 Proxy Server 及他们请求了哪些页面。

可以通过将 `obj.conf` 文件中的下列指令变为注释来禁用 Proxy Server 访问日志记录：

```
Init fn="flex-init" access="$accesslog" format.access="%Ses->client.ip%
- %Req->vars.auth-user% [%SYSDATE%] \"%Req->reqpb.clf-request%\"
%Req->srvhdrs.clf-status% %Req->srvhdrs.content-length%"
...
AddLog fn="flex-log" name="access"
```

ACL 高速缓存调节

默认情况下 Proxy Server 将用户和组验证结果存放在 ACL 用户高速缓存中。可以使用 `magnus.conf` 文件中的 `ACLCacheLifetime` 指令来控制 ACL 用户高速缓存的有效时间。每次引用高速缓存中的某个条目时，都将计算其寿命并检查 `ACLCacheLifetime`。如果该条目的寿命大于或等于 `ACLCacheLifetime`，将不再使用它。

ACLCacheLifetime 的默认值为 120 秒，这表示在长达两分钟的时间内，Proxy Server 可能会与 LDAP 服务器不同步。如果将该值设置为 0（零），则会关闭高速缓存并强制 Proxy Server 在每次用户验证时都查询 LDAP 服务器。在实现访问控制时，这将对 Proxy Server 的性能产生负面影响。不过，如果将 ACLCacheLifetime 的值设置得很大，则每次更改 LDAP 条目时可能都需要重新启动 Proxy Server，因为这样大的值将强制 Proxy Server 查询 LDAP 服务器。请只在 LDAP 目录变化不频繁时才设置较大的值。

ACLUserCacheSize 是 magnus.conf 的一个参数，它配置的是高速缓存中最多可以保留的条目数。默认值为 200。新条目将添加到列表的开头，达到高速缓存的最大大小时，将删除列表尾部的条目以接纳新条目。

还可以使用 ACLGroupCacheSize 参数来设置每个用户条目最多可以高速缓存的组成员资格数。默认值为 4。遗憾的是，组中用户的非成员资格将不会被高速缓存，这将导致对于每个请求都要对 LDAP 目录进行多次访问。

缓冲区大小

可以指定服务器套接字处发送缓冲区的大小 (SndBufSize) 和接收缓冲区的大小 (RcvBufSize)。可以在 magnus.conf 文件中配置这些参数，在不同的 UNIX 和 Linux 操作系统上，它们的建议值也不同。参阅操作系统的文档来正确设置这些参数。

连接超时

可以使用 magnus.conf 文件中的 AcceptTimeout 指令来指定服务器在关闭连接前等待来自客户机的数据到达的秒数。如果数据在超时到期前未能到达，就会关闭连接。默认情况下将此项设置为 30 秒。在大多数情况下不需要更改此设置。可以通过将此项设置为比默认值小的值来释放线程，但这样做可能会使连接速度较慢的用户的连接中断。

错误日志级别

增大 server.xml 文件 LOG 标记中 loglevel 属性的值会使服务器在错误日志中生成和存储更多的信息。不过，这样做在向该文件写入条目时的确有一定代价。请只在调试故障时增大日志记录级别，不处于故障排除模式时将日志记录级别降至最低。

安全性要求

启用 SSL 可以提高 Proxy Server 的保密性和安全性，但也会影响性能，因为对数据包进行加密和解密会发生系统开销。您可以考虑将加密和解密处理工作交由硬件加速器卡来完成。

Solaris 文件系统高速缓存

Proxy Server 高速缓存不存储在随机访问存储器中。每次从高速缓存提取文档时都是对文件系统进行文件访问操作。您可以考虑使用 Solaris 文件系统高速缓存将 Proxy Server 高速缓存预先装入到内存中。这样一来，将从内存而不是文件系统中提取对高速缓存的文件的引用。

超时值

超时对服务器性能有显著影响。为 Proxy Server 设置最优的超时值有助于优化网络资源的使用。

有两个实例特定的 SAF（服务器应用程序函数）和一个全局参数可以用于配置 Proxy Server 内的超时值。

本节包括以下主题：

init-proxy SAF (obj.conf)

`init-proxy` 函数用于初始化 Proxy Server 的内部设置。尽管是在 Proxy Server 初始化过程中调用此函数，但还应在 `obj.conf` 文件中指定该函数以确保值的初始化正确。

此函数的语法如下所示：

```
Init fn=init-proxy
  timeout=seconds
  timeout-2=seconds
```

在上例中，可以将下列参数直接应用于 init-proxy SAF 的 Proxy Server 超时设置：

- timeout（代理超时）——代理超时参数指示服务器等待多长时间后中止闲置连接。如果设置较大的代理超时值，则会将宝贵的代理线程长时间调配给可能已关闭的客户机使用。如果设置得较小，则将中止运行需要很长时间才能产生结果（如数据库查询网关）的 CGI 脚本。

  要确定服务器的最佳代理超时值，请考虑以下问题：

  - Proxy Server 是否将要处理许多数据库查询或 CGI 脚本？
  - Proxy Server 将要处理的请求数是否少到可以随时腾出进程？

  只要对以上两个问题中任何一个的回答是肯定的，即可决定设置较大的代理超时值。建议的最大代理超时值为 1 小时。默认值为 300 秒（5 分钟）。

  通过访问 Server Manager 中 "Preferences" 选项卡的 "Configure System Preferences" 页面可以查看或修改代理超时值。以 "Proxy Timeout" 来代表此参数。

- timeout-2（中断超时）——中断超时值指示 Proxy Server 在客户机中止事务后必须继续向高速缓存文件写入的时间。换言之，如果客户机在 Proxy Server 几乎已完成对文档的高速缓存时中止了连接，则服务器可以继续对文档进行高速缓存，直至达到中断超时值为止。

  建议的最大中断超时值为 5 分钟。默认值为 15 秒。

http-client-config SAF (obj.conf)

http-client-config 函数用于配置 Proxy Server 的 HTTP 客户机。

此函数的语法如下所示：

```
Init fn=http-client-config
  keep-alive=(true|false)
  keep-alive-timeout=seconds
  always-use-keep-alive=(true|false)
  protocol=HTTP Protocol
  proxy-agent="Proxy-agent HTTP request header"
```

这些设置的定义如下：

- keep-alive——（可选）Boolean 值，指示 HTTP 客户机是否应尝试使用持久连接。默认值为 true。
- keep-alive-timeout——（可选）使持久连接保持打开状态的最大秒数。默认值为 29。

- always-use-keep-alive——（可选）Boolean 值，指示是否对于所有类型的请求 HTTP 客户机都可以重复使用现有持久连接。默认值为 false，即对于非 GET 请求和含有主体的请求，将不重复使用持久连接。
- protocol——（可选）HTTP 协议版本字符串。默认情况下，HTTP 客户机会根据 HTTP 请求的内容使用 HTTP/1.0 或 HTTP/1.1。一般情况下请不要使用 protocol 参数，除非遇到具体的协议互操作性问题。
- proxy-agent——（可选）代理服务器的代理程序 HTTP 请求标头的值。默认值为包含 Proxy Server 产品名称和版本的字符串。

KeepAliveTimeout (magnus.conf)

此参数确定服务器使客户机与 Proxy Server 间的 HTTP 保持活动连接或持久连接处于打开状态的最长时间（秒）。默认值为 30 秒。连接闲置时间超过 30 秒即会超时。最大值为 300 秒（5 分钟）。

注 magnus.conf 文件中的超时设置的作用对象是客户机与 Proxy Server 间的连接。obj.conf 文件 http-client-config SAF 中的超时设置的作用对象是 Proxy Server 与源服务器间的连接。

最新性检查

Proxy Server 通过从本地高速缓存提供文档而非自源服务器获取来提高性能。此方法的一个缺点是提供的文档可能是过期的。

Proxy Server 可以执行检查来确定文档是否是最新的，如果确定文档是旧文档，则会刷新高速缓存的版本。只应在必要时执行此最新性检查，因为频繁检查文档会降低 Proxy Server 的总体性能。

最新性检查在 "Caching" 选项卡的 "Set Cache Specifics" 页面上配置。默认设置为每两个小时检查一次是否有新文档。此信息在 ObjectType 指令中使用 max-uncheck 参数来设置。

为在提高服务器性能的同时确保文档是最新的，可以对最新性检查进行自定义，即确定与 last-modified 因子（下文中有介绍）关联的合理的文档生命周期。

Last-Modified 因子

last-modified 因子用于对文档的最新性处理进行微调。此因子根据已经记录的先前更改协助确定文档发生变化的可能性。

last-modified 因子是 .02 和 1.0 间的一个小数。将把它与上次实际修改文档的时间和上次对文档执行最新性检查的时间之间的间隔相乘，然后将结果数字与上次执行最新性检查到现在为止的时间进行比较。如果该数字比时间间隔小，则表示文档尚未过期。不过，如果它比时间间隔大，则表示文档已过期，将从源服务器获得新版本。

last-modified 因子使您能够确保对最近更改过的文档的检查频率高于对旧文档的检查频率。

应将 last-modified 因子设置为 0.1 与 0.2 之间的某个值。

DNS 设置

DNS 是用于将标准 IP 地址与主机名关联的系统。如果配置得不合理，此系统会占用宝贵的 Proxy Server 资源。要优化性能，请考虑以下措施：

- 启用 DNS 高速缓存

  通过选择 Server Manager 的 "Preferences" 选项卡的 "Configure DNS Cache" 链接来启用 DNS 高速缓存。选择对应于 DNS 高速缓存的 "Enabled" 单选按钮。

- 不记录客户机 DNS 名——只记录客户机 IP 地址

  通过选择 Server Manager 的 "Server Status" 选项卡的 "Set Access Log Preferences" 链接来禁用客户机 DNS 名称日志记录。如果选择 "IP Addresses" 单选按钮，则记录的将是 IP 地址而不是客户机主机名。

- 禁用反向 DNS

  反向 DNS 用于将 IP 地址转换成主机名。通过选择 Server Manager 的 "Preferences" 选项卡的 "Configure System Preferences" 链接来禁用反向 DNS。选择 "No" 单选按钮可禁用反向 DNS。

- 避免基于客户机主机名的访问控制

  在访问控制语句中使用客户机 IP 地址，而不使用主机名（如果可能的话）。

线程数

magnus.conf 文件中的 RqThrottle 参数指定 Proxy Server 最多可以处理的并发事务数。默认值为 128。可以通过更改此值来对服务器进行调节，最大限度缩短所执行事务的等待时间。

为计算并发请求数，服务器会对活动请求进行计数：新请求到达时将计数值加一；完成请求后将计数值减一。新请求到达时服务器会检查已处理的请求数是否达到了最大值。如果已达到限制，则会推迟处理新的请求，直到活动请求数降至最大值以内。

可以通过查看由 perfdump 生成的 SessionCreationInfo 部分的数据或 proxystats.xml 数据来监视并发请求数。可以通过该信息确定同总线程数（限制）相比的最大（峰值）并发请求数。下列信息来自 perfdump 输出：

```
SessionCreationInfo:
------------------------
Active Sessions          1
Keep-Alive Sessions      0
Total Sessions Created   48/128
```

Active Sessions 显示当前服务于请求的会话（请求处理线程）数。Keep-Alive Sessions 与 Active Sessions 类似，但它专用于显示客户机请求的保持活动连接数。Total Sessions Created 同时显示创建的会话数和最多允许的会话数。这些数字是 RqThrottle 的最小值和最大值。

注 RqThrottleMin 是服务器启动时至少需要启动的线程数。默认值为 48。也可以在 magnus.conf 文件中设置此参数，但默认情况下不显示该参数。

达到所配置的最大线程数并非表明情况一定是不理想的，而且遇到这种情况时也不必自动增加 RqThrottle 的值。达到此限制意味着在峰值负载下服务器需要这么多线程，但只要服务器能够及时为请求提供服务，就表明对服务器的调节是适当的。不过，此时连接将在连接队列中排队等待，因此存在溢出队列的可能。如果定期检查 perfdump 输出，并注意到创建的会话总数经常接近 RqThrottle 的最大值，则请考虑增大线程限制。

适当的 RqThrottle 值在 100 到 500 范围内，具体视负载情况而定。

外来连接池

可以使用 magnus.conf 中的 KeepAlive* 及相关设置对外来连接池进行调节，其中包括下列设置：

- MaxKeepAliveConnections
- KeepAliveThreads
- KeepAliveTimeout
- KeepAliveQueryMaxSleepTime
- KeepAliveQueryMeanTime
- ConnQueueSize
- RqThrottle
- acceptorthreads

注 有关这些参数的更多信息，参见《Sun ONE Web Server 6.1 Performance Tuning, Sizing, and Scaling Guide》的第 2 章，其网址为：

http://docs.sun.com/source/817-6249/index.html

在此版本的 Proxy Server 中无法配置外发连接池设置。

FTP 列表宽度

为了更适合具体需求，可能需要修改 FTP 列表的宽度。增加列表宽度可以显示更长的文件名，从而减少文件名截尾长度。默认宽度为 80 个字符。

可以通过选择 Server Manager 的 "Preferences" 选项卡的 "Tune Proxy" 链接来修改 FTP 列表宽度。

高速缓存体系结构

合理地设计高速缓存的体系结构可以提高服务器的性能。请在设计高速缓存体系结构时牢记以下建议：

- 分配负载
- 使用多个代理高速缓存分区
- 使用多个磁盘驱动器
- 使用多个磁盘控制器

适当的高速缓存设置对 Proxy Server 的性能至关重要。设计代理高速缓存时需要牢记的最重要的规则是分配负载。设置高速缓存时应使每个分区的大小在 1 G 字节左右，并且应使高速缓存分布在多个磁盘和多个磁盘控制器中。较之采用单个大容量高速缓存，这种布置能够带来更快的文件创建和检索速度。

高速缓存批量更新

可以通过高速缓存批量更新特性从指定的 Web 站点预先装入文件或对高速缓存中已有的文档执行最新性检查。通常在 Proxy Server 的负载处于最低水平时启动此特性。通过 "Cache Batch Updates" 表单可以批量创建、编辑和删除 URL 以及启用和禁用批量更新。

通过指定要进行批量更新的文件，可以主动（而不是根据需要）对内容进行高速缓存。可以通过 Proxy Server 对高速缓存中现有的若干个文件执行最新性检查，或预先装入某个 Web 站点的多个文件。

在具有服务器和代理服务器网络的大型站点中，管理员可能需要使用批量更新来预先装入 Web 的给定区域。批处理进程将对文档中的所有链接执行递归下降并在本地对内容进行高速缓存。此功能可能会成为远程服务器的负担，因此要谨慎使用。可以采取一些措施来防止进程无限期地执行递归，使用 `bu.conf` 配置文件中的参数可以对该进程进行一定程度的控制。

使用 Proxy Server 访问日志来确定哪些站点最常处于活动状态，并对这些站点执行批量更新来提高性能。

垃圾收集

垃圾收集是指检查 Proxy Server 高速缓存并删除旧（过时）文件的过程。垃圾收集进程会占用大量资源，因此可能需要对某些垃圾收集设置进行调节以提高其性能。

下列参数具有对垃圾收集进程进行微调的能力。可以在 "Tune Garbage Collection" 表单上查看或修改这些参数，选择 Server Manager 的 "Caching" 选项卡的 "Tune GC" 可以找到该表单。

本节包括以下主题：

gc hi margin percent 变量

`gc hi margin percent` 变量控制最大高速缓存大小的百分比，一旦达到该值，即会触发垃圾收集。

此值必须大于 `gc lo margin percent` 的值。

`gc hi margin percent` 的有效范围是 10% 到 100%。默认值为 80%（达到高速缓存容量的 80% 时将触发垃圾收集）。

gc lo margin percent 变量

`gc lo margin percent` 变量控制最大高速缓存大小的百分比，垃圾收集器以它为目标。

此值必须小于 `gc hi margin percent` 的值。

`gc lo margin percent` 的有效范围是 5% 到 100%。默认值为 70%（将目标定为垃圾收集后高速缓存的满容率达到 70%）。

gc extra margin percent 变量

如果垃圾收集是因分区大小接近最大允许大小 (gc hi margin percent) 以外的原因触发的，则垃圾收集器将使用由 gc extra margin percent 变量设置的百分比来确定要删除的高速缓存百分比。

gc extra margin percent 的有效范围是 0 到 100%。默认值为 30%（删除现有高速缓存文件的 30%）。

gc leave fs full percent 变量

gc leave fs full percent 值确定高速缓存分区大小的百分比，低于该值时将不会进行垃圾收集。此值可以防止垃圾收集器在某个其他应用程序独占磁盘空间时从高速缓存中删除所有文件。

gc leave fs full percent 的有效范围是 0（允许完全删除）到 100%（不删除任何内容）。默认值为 60%（允许高速缓存大小收缩到当前大小的 60%）。

Solaris 性能调节

可以使用 Solaris 内核中的各种参数来微调 Proxy Server 的性能。下表列出了其中的一些参数。

表 B-1 Solaris 性能调节参数

参数	范围	默认值	调节后的值	注释
rlim_fd_max	/etc/system	1024	8192	处理打开的文件描述符限制。应将预期负载（关联套接字、文件和管道的预期负载，如果有）计算在内。
rlim_fd_cur	/etc/system	64	8192	
sq_max_size	/etc/system	2	0	控制流驱动程序队列大小。如果将此参数设置为 0，则会使其大小不受限制，这样性能运行将不会由于缺少缓冲区空间而受影响。请在客户机上也设置此参数。
tcp_close_wait_interval	ndd/dev/tcp	240000	60000	请在客户机上也设置此参数。
tcp_conn_req_max_q	ndd/dev/tcp	128	1024	

表 B-1 Solaris 性能调节参数

参数	范围	默认值	调节后的值	注释
tcp_conn_req_max_q0	ndd/dev/tcp	1024	4096	
tcp_ip_abort_interval	ndd/dev/tcp	480000	60000	
tcp_keepalive_interval	ndd/dev/tcp	7200000	900000	对于通信流量大的 Web 站点，请降低此值。
tcp_rexmit_interval_initial	ndd/dev/tcp	3000	3000	如果重新传输量超过了 30-40%，请增加此值。
tcp_rexmit_interval_max	ndd/dev/tcp	240000	10000	
tcp_rexmit_interval_min	ndd/dev/tcp	200	3000	
tcp_smallest_anon_port	ndd/dev/tcp	32768	1024	请在客户机上也设置此参数。
tcp_slow_start_initial	ndd/dev/tcp	1	2	可以略微提高传输少量数据时的速度。
tcp_xmit_hiwat	ndd/dev/tcp	8129	32768	使用此参数来增大传输缓冲区。
tcp_recv_hiwat	ndd/dev/tcp	8129	32768	使用此参数来增大接收缓冲区。

有关这些参数的更多信息，参见《Sun ONE Web Server 6.1 Performance Tuning, Sizing, and Scaling Guide》的第 5 章，其网址为：

http://docs.sun.com/source/817-6249/index.html

索引

符号

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z