Sun Java System Web Proxy Server 4.0.4 管理指南

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

文件号码 820–0860
2007 年 3 月

070423@17039

目录

前言

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，以下称为 Sun Java System Web Proxy Server 或简称为 Proxy Server）。

目标读者

本书适用于生产环境中的信息技术管理员。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
- 在终端窗口中发出命令

阅读本书之前

Sun Java System Web Proxy Server 可单独购买，也可作为 Sun Java Enterprise System 的一个组件购买，Sun Java Enterprise System 是一种支持分布在网络或 Internet 环境中的企业应用程序的软件基础结构。如果将 Sun Java System Web Proxy Server 作为 Java Enterprise System 的一个组件购买，您应熟悉 `http://docs.sun.com/coll/1286.2` 和 `http://docs.sun.com/coll/1382.2` 上的系统文档。

本书的结构

本指南分为几个部分，每个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 P–1 本指南的结构

部分	描述

表 P–1 本指南的结构 （续）

第 1 部分服务器基础知识	对 Proxy Server 及其管理进行概述： ■ 第 1 章 ■ 第 2 章
第 2 部分使用 Administration Server	提供有关配置 Administration Server 首选项、管理用户和组、确保 Proxy Server 的安全以及使用群集在服务器间共享配置的详细信息： ■ 第 3 章 ■ 第 4 章 ■ 第 5 章 ■ 第 6 章
第 3 部分配置和监视 Proxy Server	提供有关配置服务器首选项、设置访问控制以及监视服务器活动的详细信息： ■ 第 7 章 ■ 第 8 章 ■ 第 9 章 ■ 第 10 章
第 4 部分管理 Proxy Server	提供有关与 Proxy Server 如何处理请求相关的概念和任务的详细信息： ■ 第 11 章 ■ 第 12 章 ■ 第 13 章 ■ 第 14 章 ■ 第 15 章 ■ 第 16 章 ■ 第 17 章
第 5 部分附录	介绍访问控制列表 (access control list, ACL) 文件语法以及服务器性能调节： ■ 第 18 章 ■ 第 19 章

Proxy Server 文档集

文档集列出了与 Proxy Server 相关的 Sun 文档。Proxy Server 文档的 URL 为 `http://docs.sun.com/coll/1311.4` 和 `http://docs.sun.com/coll/1579.2`。有关 Proxy Server 的介绍，请参阅下表中的书籍（按照它们列出的顺序）：

表 P–2 Sun Java System Web Proxy Server 文档

文档标题	内容
《Sun Java System Web Proxy Server 4.0.4 发行说明》	Proxy Server 发行版： ■ 软件和文档的最新信息 ■ 新增功能 ■ 支持的平台和环境 ■ 系统要求 ■ 已知问题和解决方法
《Sun Java System Web Proxy Server 4.0.4 Installation and Migration Guide》	执行安装和迁移任务： ■ 安装 Sun Java System Web Proxy Server ■ 从版本 3.6 迁移到版本 4
《Sun Java System Web Proxy Server 4.0.4 管理指南》	执行管理任务： ■ 使用管理界面和命令行界面 ■ 配置服务器首选项 ■ 管理用户和组 ■ 监视和记录服务器活动 ■ 使用证书和公钥加密以确保服务器的安全 ■ 控制服务器访问 ■ 代理和路由 URL ■ 高速缓存 ■ 过滤内容 ■ 使用反向代理 ■ 使用 SOCKS
《Sun Java System Web Proxy Server 4.0.4 Configuration File Reference》	编辑配置文件
《Sun Java System Web Proxy Server 4.0.4 NSAPI Developer's Guide》	创建自定义 Netscape Server 应用编程接口 (Netscape Server Application Programming Interface, NSAPI) 插件

相关书籍

有关 Sun Java Enterprise System (Java ES) 及其组件的所有文档的 URL 为 `http://docs.sun.com/prod/entsys.5` 和 `http://docs.sun.com/prod/entsys.5?l=zh`。

默认路径和文件名

下表介绍了本书中使用的默认路径和文件名。

表 P–3 默认路径和文件名

占位符	描述	默认值
install-dir	表示 Sun Java System Web Proxy Server 的基本安装目录。	Solaris 和 Linux 安装：/opt/sun/proxyserver40 Windows 安装：\Sun\ProxyServer40

印刷约定

下表介绍了本书中使用的印刷约定。

表 P–4 印刷约定

字体	含义	示例
`AaBbCc123`	命令、文件和目录的名称；计算机屏幕输出	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `machine_name% you have mail.`
`AaBbCc123`	用户键入的内容，与计算机屏幕输出的显示不同	`machine_name%` **`su`** `Password:`
AaBbCc123	要使用实名或值替换的占位符	删除文件的命令为 `rm` *filename*。
AaBbCc123	书名、保留未译的新词或术语以及要强调的词（注意：有些强调的项目在联机时以粗体显示。）	阅读《用户指南》的第 6 章。 **高速缓存**是存储在本地的副本。 请**勿**保存文件。

命令中的 shell 提示符示例

下表显示了默认提示符和超级用户提示符。

表 P–5 Shell 提示符

Shell	提示符
UNIX 和 Linux 系统上的 C shell	`machine_name%`

表 P–5 Shell 提示符 （续）

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

符号约定

下表介绍了本书使用符号。

表 P–6 符号约定

符号	说明	示例	含义
`[ ]`	包含可选参数和命令选项。	`ls [-l]`	`-l` 选项不是必需的。
`{ | }`	包含为所需命令选项提供的一组选择。	`-d {y|n}`	`-d` 选项要求您使用 `y` 参数或 `n` 参数。
`${ }`	表示一个变量引用。	`${com.sun.javaRoot}`	引用 `com.sun.javaRoot` 变量的值。
-	连接需同时按下的多个击键。	Ctrl-A	在按 A 键的同时按 Ctrl 键。
+	连接需连续按下的多个击键。	Ctrl+A+N	按 Ctrl 键，将其松开，然后依次按后续键。
→	表示图形用户界面中的菜单项选定。	"File" → "New" → "Templates"	从 "File" 菜单中，选择 "New"。从 "New" 子菜单中，选择 "Templates"。

文档、支持和培训

Sun Web 站点提供有关以下附加资源的信息：

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

搜索 Sun 产品文档

除了从 docs.sun.com℠ Web 站点搜索 Sun 产品文档之外，还可以使用搜索引擎，方法是在搜索字段中键入以下语法：

search-term `site:docs.sun.com`

例如，要搜索 "broker"，请键入：

```
broker site:docs.sun.com
```

要在搜索中包含其他 Sun Web 站点（例如，java.sun.com、www.sun.com 和 developers.sun.com），请在搜索字段中用 `sun.com` 代替 `docs.sun.com`。

第三方 Web 站点引用

本文档引用了第三方 URL 以提供其他相关信息。

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

Sun 欢迎您提出意见

Sun 致力于提高其文档的质量，并十分乐意收到您的意见和建议。为了共享您的意见，请访问 `http://docs.sun.com`，并单击 "Send Comments"（发送意见）。在联机表单中，请提供完整的文档标题和文件号码。文件号码是一个 7 位或 9 位的数字，可以在书的标题页或文档的 URL 中找到。例如，本书的文件号码为 820–0860。

◆ ◆ ◆ 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，其中简要说明了此发行版的新增功能，并概述了用于管理和配置 Proxy Server 的基于 Web 的用户界面。

本章包含以下各节：

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 是一种用于高速缓存并过滤 Web 内容，同时提高网络性能的系统。它具备与整个网络基础结构集成、跨平台支持以及集中管理的能力。作为一个网络通信流量管理器，它可以有效地对信息进行分发和管理，从而减少网络通信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，因为它可为内容分发提供安全网关并起到 Internet 通信流量控制点的作用。

此发行版的新增功能

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

- 新式 HTTP 内核
- 支持 Linux 和 Solaris™ x86 平台
- 在所有平台上均支持新式 SSL（Secure Sockets Layer，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，易于管理
- 新增了 NSAPI（Netscape Server Application Programming Interface，Netscape Server 应用编程接口）过滤器

- 提高了 LDAP（Lightweight Directory Access Protocol，轻量目录访问协议）性能
- 改进了可伸缩性和性能
- 改进了内容过滤
- 实现了 `server.xml` 配置文件

有关新增功能和增强功能的信息，请参见 Sun Java System Web Proxy Server **发行说明**，其网址为：`http://docs.sun.com/app/docs/coll/1311.4` 和 `http://docs.sun.com/app/docs/coll/1579.2`。

入门

通过 Administration Server 和 Server Manager 的基于 Web 的用户界面来管理和配置 Sun Java System Web Proxy Server。Administration Server 用于管理系统上安装的所有 Proxy Server 实例的公共配置，Server Manager 用于配置各个服务器实例的设置。

本节包含以下主题：

注 – 您必须在浏览器中启用 Cookies 才能运行配置服务器所需的 CGI 程序。

Administration Server 概述

Administration Server 是基于 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 Administration Server 后，可通过启动浏览器并输入 URL 来访问 Administration Server。URL 由在安装过程中指定的主机名和端口号确定，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，请参见第 39 页中的 “允许多个管理员”。

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，并对这些选项卡所提供的任务进行了简要说明。

- Servers－管理、添加、删除和迁移 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）、自定义和查看访问日志及错误日志

- 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、组和及组织单元
- Security－创建新的信任数据库、请求和安装 VeriSign 及其他证书、更改密钥对文件密码、查看和管理安装的证书、添加或替换证书撤销列表 (Certificate Revocation List, CRL) 和已泄密密钥列表 (Compromised Key List, 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

不管您位于哪个选项卡或页面，都会显示以下按钮：

- Version－显示 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

▼ 访问 Administration Server

1 **启动浏览器，并转至反映在安装过程中为 Administration Server 指定的主机名和端口号的 URL，例如** `http://myserver.mycorp.com:1234`

2 **出现提示时，键入在安装过程中指定的用户名和密码。**

此时将显示 Administration Server 的用户界面。

有关使用 Administration Server 的更多信息，请参见第 2 章。另请参见 Administration Server 选项卡和页面的联机帮助。

Server Manager 概述

Server Manager 是基于 Web 的用户界面，用于启动、停止和配置 Sun Java System Web Proxy Server 的各个实例。

Server Manager 设置按照与特定任务相对应的选项卡进行组织。以下是 Server Manager 选项卡的列表，并对这些选项卡所提供的任务进行了简要说明。

- 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、设置密码大小
- Routing－启用和禁用代理、设置路由首选项、转发客户机凭据、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、连接和路由条目
- URLs－查看、创建和管理 URL 映射及重定向

- Caching－设置高速缓存细节、添加和修改高速缓存分区、在现有分区中移动段、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、抑制外出的标头、设置 MIME 过滤器和 HTML 标记过滤器、根据需要压缩内容
- 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、请求和安装 VeriSign 及其他证书、更改密钥对文件密码、查看和管理安装的证书、添加或替换证书撤销列表 (Certificate Revocation List, CRL) 和已泄密密钥列表 (Compromised Key List, 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

不管您位于哪个选项卡或页面，都会显示以下按钮：

- Version－显示 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。该链接表明已经进行了更改，服务器必须重新启动。要应用更改，请单击该链接并指定所需的操作。

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

▼ 访问 Server Manager

1. **按照第 28 页中的 “ Administration Server 概述 ”中的说明访问 Administration Server。**
   "Servers" 选项卡中将显示 Administration Server。
2. **在 "Manage Servers" 页面中，单击所要管理的服务器实例的链接。**
   此时将显示 Server Manager 用户界面。

配置文件

Sun Java System Web Proxy Server 的配置和行为由一组配置文件确定。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。也可以手动编辑这些文件。

配置文件位于目录 *instance-dir*/config，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。配置文件的数量和名称取决于已启用或装入的组件。该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不可少的配置文件及其内容。

表 1–1 必不可少的配置文件

文件	包含
server.xml	大多数服务器配置（此 Proxy Server 发行版的新增功能）
magnus.conf	服务器初始化全局信息
obj.conf	用于处理客户机请求的指令
mime.types	有关确定请求的资源内容类型的信息

有关这些文件和其他配置文件的详细信息，请参见 Proxy Server 4.0.4 **配置文件参考**。

正则表达式

您可以使用正则表达式来识别资源和配置 Proxy Server，以便以不同的方式处理来自不同 URL 的请求。您可以在使用 Administration Server 和 Server Manager 用户界面执行各种任务时指定正则表达式。有关使用正则表达式的详细信息，请参见第 16 章。

◆ ◆ ◆ 第 2 章

2 管理 Sun Java System Web Proxy Server

本章介绍有关使用 Administration Server 管理 Sun Java System Web Proxy Server 的基本知识。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。

本章包含以下各节：

有关配置 Administration Server 首选项的详细信息，请参见第 3 章。有关使用服务器群集管理多个 Proxy Server 的详细信息，请参见第 6 章。

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，请参见第 34 页中的 “停止 Administration Server”。

在 UNIX 或 Linux 上启动 Administration Server

1. 从命令行中，转至 *server-root*/proxy-admserv，然后
2. 键入 ./start 以启动 Administration Server（或者键入 ./restart 以重新启动 Administration Server）。

在 Windows 上启动 Administration Server

在 Windows 上，可以通过以下任一方法启动 Administration Server：

- 使用“开始” -> “程序” -> "Sun Microsystems" -> "Sun Java System Web Proxy Server *version*" -> "Start Admin"
- 使用“控制面板” -> “管理工具” -> “服务” ->"Sun Java System Web Proxy Server 4.0 Administration Server" -> “启动”
- 从命令提示符中，转至 *server-root*\proxy-admserv 并键入 startsvr.bat 以启动 Administration Server（或者键入 ./restart 以重新启动 Administration Server）。

启动 Administration Server 后便可以对其进行访问，方法是启动浏览器并提供可反映在安装过程中为 Administration Server 指定的主机名和端口号的 URL，例如 http://myserver.mycorp.com:1234。系统将提示您输入用户名和密码，这两者也是在安装过程中指定的。

可以授权多个管理员访问 Administration Server。有关分布式管理的更多信息，请参见第 39 页中的 “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，请参见第 33 页中的 “启动 Administration Server” 。

在 UNIX 或 Linux 上停止 Administration Server

在 UNIX 或 Linux 上，可以通过以下两种方法之一停止 Administration Server：

- 使用管理界面：
  1. 访问 Administration Server。
  2. 选择 "Preferences" 选项卡。
  3. 单击 "Shutdown Server" 链接。
  4. 单击 "OK"。
- 从命令行中，转至 *server-root*/proxy-admserv/ 并键入 ./stop。

在 Windows 上停止 Administration Server

在 Windows 上，可以通过以下两种方法之一停止 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” -> "Sun Java System Web Proxy Server 4.0 Administration Server" -> “停止”
- 从命令提示符中，转至 *server-root*\proxy-admserv 并键入 stopsvr.bat。

运行多个 Proxy Server

要在系统上运行多个 Proxy Server，必须安装并配置多个服务器实例。以下过程将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. **提供所需的信息并单击 "OK"。**
   有关特定字段的更多信息，请参见联机帮助。
4. **如果需要，请在成功添加新服务器实例后显示的 "Success" 页面上单击 "Configure Your New Server" 链接。**
   将显示 Server Manager 界面。可以使用此界面配置服务器实例。

删除服务器实例

可以使用 Administration Server 删除 Proxy Server 实例。此过程无法撤消，因此在执行以下过程之前，请确定您要删除服务器实例。

▼ 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. **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（也称为 iPlanet Web Proxy Server）迁移到 Sun Java System Web Proxy Server 4。将保留版本 3.6 服务器，并创建具有相同设置的新版本 4 服务器。有关将服务器从版本 3.6 迁移到版本 4 的更多信息，请参见《Sun Java System Web Proxy Server 4.0.4 Installation and Migration Guide》。另请参见 Proxy Server 用户界面中与迁移相关的页面的联机帮助。有关迁移证书的信息，请参见本指南中的第 77 页中的 “从先前版本迁移证书”。

◆ ◆ ◆ 第 3 章

3 设置管理首选项

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

本章包含以下各节：

创建和管理侦听套接字

在服务器处理请求之前，请求必须先由侦听套接字接受，然后再定向到正确的服务器。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` 以及安装过程中指定为 Administration Server 端口号的端口号。

可以使用 Administration Server 的 "Edit Listen Sockets" 页面添加、编辑和删除侦听套接字。您必须至少具有一个用于访问服务器的侦听套接字。如果某个侦听套接字为唯一列出的侦听套接字，则不能将其删除。

本节介绍如何添加、编辑和删除侦听套接字。

▼ 添加侦听套接字

1. **访问 Administration Server 并选择 "Preferences" 选项卡。**
2. **单击 "Edit Listen Sockets" 链接。**

3. **单击 "New" 按钮。**
4. **指定设置并单击 "OK"。**
   有关特定字段的更多信息，请参见联机帮助。

▼ 编辑侦听套接字

1. **访问 Administration Server 并选择 "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. **进行所需的更改并单击 "OK"。**

▼ 删除侦听套接字

1. **访问 Administration Server 并选择 "Preferences" 选项卡。**
2. **单击 "Edit Listen Sockets" 链接。**
3. **选中要删除的侦听套接字旁边的复选框并单击 "OK"。**
4. **系统提示确认删除时，单击 "OK"。**
   您必须至少具有一个用于访问服务器的侦听套接字。如果某个侦听套接字为唯一列出的侦听套接字，则不能将其删除。

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，必须为允许的管理员配置附加访问控制。

注意 – 如果使用 Sun Java System Directory Server 管理用户和组，则在更改超级用户的用户名或密码**之前**，必须更新目录中的超级用户条目。如果不先更新目录，将不能访问 Administration Server 中的 "Users and Groups" 界面。然后，必须使用确实可以访问该目录的管理员帐户来访问 Administration Server，或者使用 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 并选择 "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，请参见联机帮助。

   超级用户的用户名和密码保存在 *server-root*/proxy-admserv/config 内名为 admpw 的文件中。该文件的格式为 *username* :*password*。您可以查看该文件来获取用户名，但是密码已加密，不可读取。如果忘记了密码，可以更改为新密码。

▼ 更改超级用户密码

1. **编辑 admpw 文件并删除加密的密码。**
2. **只使用用户名而不使用密码来访问 Administration Server。**
3. **单击 "Preferences" 选项卡。**
4. **单击 "Control Superuser Access" 链接。**
5. **提供新密码并单击 "OK"。**

注意 – 由于可以对 admpw 文件进行编辑，因此必须将服务器计算机放在安全的位置，并且必须限制对其文件系统的访问。

在 UNIX 和 Linux 系统上，可以考虑更改文件的所有权，以便只有 root 用户或任何运行 Administration Server 守护进程的系统用户才能进行写操作。在 Windows 系统上，可以将文件的所有权限制到 Administration Server 使用的用户帐户。

允许多个管理员

多个管理员可以通过分布式管理来更改服务器的特定部分。必须安装目录服务器，然后才能启用分布式管理。默认的目录服务必须基于 LDAP。

分布式管理的两个用户级别为超级用户和管理员。

- 超级用户是指在 *server-root*/proxy-admserv/config/admpw 中列出的用户。这是在安装过程中指定的用户名和密码。此用户对 Administration Server 中除 "Users and Groups" 表单（对其的访问权限取决于在 LDAP 服务器中具有有效帐户的超级用户）之外的所有表单具有完全访问权限。
- 管理员可以直接进入特定服务器（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（通常由超级用户配置）。管理员可以执行有限的管理任务，并且还可以进行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，请参见第 8 章。

▼ 启用分布式管理

1. **检验是否安装了目录服务器。**
2. **访问 Administration Server。**
3. **（可选）安装了目录服务器之后，还可能需要创建管理组（如果尚未创建）。要创建组，请执行以下操作：**

   a. **单击 "Users and Groups" 选项卡。**

   b. **单击 "Create Group" 链接。**

   c. **在 LDAP 目录中创建一个管理员组并添加用户的名称（您授予这些用户相应权限以配置 Administration Server 或在其服务器根目录中安装的任何服务器）。**

      有关特定字段的更多信息，请参见联机帮助。

      管理员组中的所有用户都具有 Administration Server 的完全访问权限，但是可以使用访问控制来限制他们能够配置的服务器和表单。

      创建访问控制列表之后，分布式管理组将被添加到该列表中。如果更改管理员组的名称，必须手动编辑访问控制列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"，指定管理员组，然后单击 "OK"。**

指定日志文件选项

Administration Server 日志文件记录了有关 Administration Server 的数据，包括遇到的错误类型以及有关服务器访问的信息。通过日志信息，可以监视服务器活动和解决问题。您可以使用 "Log Preferences" 页面上的许多选项来指定 Administration Server 日志中记录的数据类型和格式。还可以选择通用日志文件格式 (Common Logfile Format)，它提供固定数量的服务器信息，也可以创建更符合您要求的自定义日志文件格式。

要访问 Administration Server 的 "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。有关日志文件以及设置日志文件选项的详细信息，请参见第 9 章。另请参见联机帮助。

查看日志文件

Administration Server 的日志文件位于 *server-root*`/proxy-admserv/logs` 中。您可以通过 Proxy Server 管理控制台或者使用文本编辑器来查看错误日志和访问日志。

访问日志文件

访问日志文件记录了有关对服务器的请求以及服务器的响应的信息。

▼ 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，请参见联机帮助。另请参见第 9 章。

错误日志文件

错误日志列出了自创建日志文件以来服务器遇到的所有错误。它还包含有关服务器的信息消息，例如服务器何时启动、谁尝试登录服务器但失败等。

▼ 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，请参见联机帮助。另请参见第 9 章。

使用目录服务

您可以在单个使用 LDAP 的目录服务器中存储和管理用户名和密码之类的信息。还可以配置该服务器，以便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，请参见第 4 章。

限制服务器访问

当 Proxy Server 评估传入的请求时，将根据一个称为访问控制条目 (Access Control Entries, ACE) 的分层结构规则确定访问权限，然后使用匹配的条目确定是否允许该请求。每个 ACE 都指定了服务器是否应当继续检查分层结构中的下一个 ACE。该 ACE 集合称为访问控制列表 (Access Control List, ACL)。

可以将访问控制配置为允许访问 Administration Server 以及服务器实例内的特定资源（例如文件、目录和文件类型）。通过 Administration Server 中的 "Global Settings" 选项卡，可以配置 Administration Server 的访问控制。通过 Server Manager 中的 "Preferences" 选项卡，可以配置服务器实例内资源的访问控制。有关设置访问控制的更多信息，请参见第 8 章。

注 – 必须启用分布式管理，然后才能限制服务器访问。有关更多信息，请参见第 39 页中的 “允许多个管理员”。

SNMP 主代理设置

简单网络管理协议 (Simple Network Management Protocol, SNMP) 是一种用于交换有关网络活动的数据的协议。此信息通过使用子代理和主代理在网络管理站与服务器之间进行传送。

可以使用 Administration Server 中的 "Global Settings" 选项卡配置 SNMP 主代理设置。主代理随 Administration Server 一起安装。有关 SNMP 和代理设置的详细信息，请参见第 10 章。另请参见 Administration Server 中 "Global Settings" 选项卡上主代理页面的联机帮助以及 Server Manager 中 "Server Status" 选项卡上子代理页面的联机帮助。

◆ ◆ ◆ 第 4 章

4 管理用户和组

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

本章包含以下各节：

访问用户和组的信息

使用 Administration Server 可以访问有关用户帐户、组列表、访问权限、组织单位以及其他特定于用户和组的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（Lightweight Directory Access Protocol，轻量目录访问协议）的目录服务器（如 Sun Java System Directory Server）中。LDAP 是通过 TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/Internet 协议）运行的开放式目录访问协议，可扩展到全局大小和上百万个条目。

关于目录服务

通过目录服务，可以从单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，则无论新创建的第一个目录服务是什么类型，都会设置为值 `default`。创建目录服务时，将会使用目录服务详细信息更新 *server-root*`/userdb/dbswitch.conf` 文件。

本节介绍 LDAP、密钥文件和摘要文件这三种类型的目录服务。

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%3Dcomdefault:binddn
cn=Directory Managerdefault: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%3Dcomldap:binddn
cn=Directory Managerldap: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密码以及该用户所属组的列表。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，请参见第 144 页中的 “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 filekeyfile:syntax keyfilekeyfile: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密码存储用户和组信息。

摘要文件格式旨在支持使用 HTTP 摘要验证，但也支持基本验证，因此可以将该格式同时用于这两种验证方法。有关这些方法的更多信息，请参见第 144 页中的 “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 filedigest:syntax digestdigest:digestfile D:\\test22\\digest\
\digestdb
```

注 – 要配置分布式管理，默认目录服务必须为基于 LDAP 的目录服务。

配置目录服务

可在 Administration Server 的 "Global Settings" 选项卡中创建和配置目录服务。然后，可以在 Administration Server 的 "Users and Groups" 选项卡中创建和管理用户、组以及组织单位。

本节介绍如何创建和编辑目录服务。

▼ 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. **从 "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"。**
   此时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，请参见联机帮助。

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，无论其类型如何都是如此。

▼ 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. **单击要编辑的目录服务的链接。**

4 **进行所需的更改，然后单击 "Save Changes"。**
有关特定字段的更多信息，请参见联机帮助。

了解标识名 (Distinguished Name, 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 LDAP 数据库中的个人，如公司的雇员。组是共享某个通用属性的两个或多个用户。组织单位是组织中的子部门，它使用 `organizationalUnit` 对象类。本章稍后会对用户、组和组织单位进行更为详细的介绍。

企业中的每个用户和组都由一个标识名 (distinguished name, 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、配置访问控制以及配置用户帐户时，均需要提供 DN 信息。Proxy Server 的 "Users and Groups" 界面可用于创建或修改 DN。

以下示例显示了一个典型的 Sun Microsystems 雇员 DN：

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

该示例中缩写的含义如下：

- `uid` 是用户 ID
- `e` 是电子邮件地址
- `cn` 是用户的通用名称
- `o` 是组织
- `c` 是国家或地区。

DN 可以包括很多名称-值对，用于标识支持 LDAP 的目录中的证书主题和条目。

使用 LDIF

如果当前没有目录，或者想要向现有目录中添加新子树，可以使用目录服务器的 LDIF（Lightweight Directory Interchange Format，轻量目录交换格式）导入功能。此功能将接受一个包含 LDIF 的文件并尝试由 LDIF 条目生成一个目录或新子树。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。此功能将创建一个 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 向数据库中添加条目，请首先在 LDIF 文件中定义各个条目，然后通过目录服务器导入该 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 – 请务必确保用户在未授权的情况下不能访问资源，以保护服务器的安全。Proxy Server 使用基于 ACL 的授权和验证模型。有关基于 ACL 的安全性的更多信息，请参见第 8 章。有关其他安全性信息，另请参见第 5 章。

本节介绍如何在基于 LDAP 的验证数据库、密钥文件验证数据库和摘要文件验证数据库中创建用户。

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，将使用一个基于 LDAP 的基础目录服务器的服务对用户进行验证和授权。本节列出了使用基于 LDAP 的验证数据库时应考虑的准则，并介绍了如何通过 Proxy Server Administration Server 添加用户。

创建基于 LDAP 的用户条目的准则

使用 Proxy Server 管理控制台在基于 LDAP 的目录服务中创建新的用户条目时，应考虑以下准则：

- 如果提供名和姓，将会自动填写该用户的全名和用户 ID。生成的用户 ID 由用户名字的第一个首字母后跟姓组成。例如，如果用户的姓名为 Billie Holiday，用户 ID 将被自动设置为 `bholiday`。如果您愿意，可以用您喜欢的 ID 代替该用户 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以查看该用户 ID 是否已被使用来确保该用户 ID 的唯一性。但是请注意，如果使用目录服务器 `ldapmodify` 命令行实用程序（如果可用）来创建用户，则不能确保用户 ID 的唯一性。如果您的目录中存在重复的用户 ID，受影响的用户将无法在该目录中得到验证。
- 基 DN 指定的标识名是默认情况下查找目录的起点，也是您的目录树中放置所有 Proxy Server Administration Server 条目的位置。标识名 (DN) 是条目名称在目录服务器中的字符串表示。
- 创建新用户条目时，必须至少指定以下用户信息：
  - 姓
  - 全名
  - 用户 ID

  如果为目录定义任何组织单位，可以使用 Administration Server 的 "Create User" 页面中的 "Add New User To" 列表来指定要放置新用户的位置。默认位置是目录的基 DN 或根点。

目录服务器用户条目

请注意有关目录服务器用户条目的以下信息：

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

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

  例如，如果在组织单位 Marketing 中创建 Billie Holiday 用户条目，并且目录的基 DN 是 `o=Ace Industry,c=US`，那么该用户的 DN 为：

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

  此格式可以更改为基于用户 ID (user ID, uid) 的标识名。
- 用户表单字段中的值存储为 LDAP 属性。

  下表列出在 Proxy Server 界面中创建或编辑新用户时将显示的字段以及对应的 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`
Password	`userPassword`
E-mail Address	`mail`
Title	`title`
Phone Number	`telephoneNumber`

创建基于 LDAP 的用户条目

要创建用户条目，请阅读第 47 页中的 “创建基于 LDAP 的用户条目的准则”中概述的准则，然后执行以下过程。

▼ 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 **提供所显示的页面中要求的信息。**
有关特定字段的更多信息，请参见联机帮助。
另请参见第 48 页中的 “目录服务器用户条目” 。

5 **单击 "Create" 以创建用户条目，或者单击 "Create and Edit" 以创建用户条目并进入刚创建的条目的编辑页面。**

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密码以及该用户所属组的列表。

▼ 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 **键入所显示的页面中要求的信息，然后单击 "Create User"。**
有关特定字段的更多信息，请参见联机帮助。

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 **键入所显示的页面中要求的信息，然后单击 "Create User"。**
有关特定字段的更多信息，请参见联机帮助。

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，请参见第 139 页中的 “设置访问控制” 。

管理用户

可以在 Administration Server 中的 "Users and Groups" 选项卡的 "Manage Users" 页面上编辑用户属性。在此页面上，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

在编辑用户条目之前，必须首先查找并显示该条目。对于基于 LDAP 的目录服务，可以提供要编辑的条目的描述性值。

可以提供任何以下信息：

- 姓名。输入全名或部分名。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，将返回包含该搜索字符串的所有条目。如果未找到包含搜索字符串的条目，将查找所有发音与搜索字符串类似的条目。
- 用户 ID。如果仅输入部分用户 ID，将返回所有包含该字符串的条目。
- 电话号码。如果您只输入部分号码，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。任何包含 @ 符号的搜索字符串均被认为是电子邮件地址。如果找不到精确的匹配，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。
- 任何 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。
- 使用星号 (*) 可以查看当前目录中的所有条目。保留该字段为空也可以实现这一目的。

生成自定义搜索查询

对于 LDAP 服务，"Find All Users Whose" 部分允许您生成自定义搜索过滤器。使用这些字段可以缩小 "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所基于的属性。下表列出了可用的搜索属性选项。

表 4–2 搜索属性选项

选项	搜索匹配条目
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的类型。下表列出了可用的搜索类型选项。

表 4–3 搜索类型选项

选项	描述
Contains	执行子字符串搜索。将返回属性值包含指定搜索字符串的条目。例如，如果您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" 来查找该用户条目。
是	查找精确匹配的条目（指定相等搜索）。如果您知道用户属性的精确值，则可以使用此选项。例如，您知道用户姓名的精确拼写。
isn't	返回属性值与搜索字符串不精确匹配的所有条目。使用此选项可查找目录中姓名不是 "John Smith" 的所有用户。请注意，使用此选项可能导致返回大量条目。
Sounds like	执行近似搜索。如果您知道属性的值，但不知道如何拼写，可以使用此选项。例如，您不知道用户姓名的拼写是 "Sarret"、"Sarette" 还是 "Sarett"。
Starts with	执行子字符串搜索。返回属性值以指定的搜索字符串开头的所有条目。例如，您知道用户的姓名以 "Miles" 开头，但不知道其余部分。
Ends with	执行子字符串搜索。返回属性值以指定的搜索字符串结尾的所有条目。例如，您知道用户的姓名以 "Dimaggio" 结尾，但不知道其余部分。

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，请键入星号 (*) 或保留该字段为空。

▼ 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一种目录服务，然后单击 "Select"。**

对于密钥文件或摘要文件目录服务，将会显示一个用户列表。对于基于 LDAP 的目录服务，将显示搜索字段。

4 **查找用户信息：**

对于密钥文件或摘要文件目录服务，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，请参见联机帮助。

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值。**

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，请参见第 50 页中的 “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，指定应将输出格式设置为用来显示在屏幕上还是用打印机打印。**

d. **在此过程中的任何阶段，单击 "Find" 按钮。**

此时将显示与搜索条件相匹配的所有用户。

e. **单击要显示的条目的链接。**

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 **按第 50 页中的 “ 查找用户信息 ”中所述显示用户条目。**

4 **进行所需的更改。**

有关特定字段的更多信息，请参见联机帮助。

注 – 要更改编辑用户页面中未显示的属性值，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，请参见第 53 页中的 “重命名用户”。

管理用户密码

以下过程说明了如何更改或创建用户密码。

▼ 更改或创建用户密码

1. **访问 Administration Server 并单击 "Users and Groups" 选项卡。**
2. **单击 "Manage Users" 链接。**
3. **按第 50 页中的 “ 查找用户信息 ”中所述显示用户条目。**
4. **进行所需的更改。**

   有关特定字段的更多信息，请参见联机帮助。

   对于 LDAP 数据库，还可通过单击用于编辑用户密码信息的页面（通过 "Manage Users" 页面进行访问）上的 "Disable Password" 按钮来禁用用户密码。执行此操作无须删除用户的目录条目即可防止用户登录到服务器。通过提供新密码可再次允许用户访问。

重命名用户

对于 LDAP 数据库，重命名功能仅更改用户 ID。所有其他字段保持不变。不能使用重命名功能将条目从一个组织单位移到另一个组织单位。

▼ 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. **按第 50 页中的 “ 查找用户信息 ”中所述显示用户条目。**
4. **单击编辑用户页面上的 "Rename User" 按钮。**
5. **在所显示的页面上键入用户 ID，然后单击 "Save Changes"。**

注 – 通过将 `keepOldValueWhenRenaming` 参数设置为 `false`（默认值），可以指定 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. **按第 50 页中的“ 查找用户信息 ”中所述显示用户条目。**
4. **单击相应的按钮。**
   - 对于 LDAP 服务器，单击 "Delete User"。
   - 对于密钥文件数据库和摘要文件数据库，单击 "Remove User"。

创建组

组是描述 LDAP 数据库中一组对象的对象。Sun Java System 服务器组由共享某个通用属性的用户组成。例如，一组对象可以是您公司市场部的一些雇员。这些雇员可能属于一个名为 Marketing 的组。

对于 LDAP 服务，可通过静态和动态两种方法定义组的成员资格。静态组显式枚举出其成员对象。静态组是包含 `uniqueMembers`、`memberURLs` 或 `memberCertDescriptions` 的通用名称 (common name, CN)。静态组的成员并不共享某个通用属性，但 `cn=groupname` 属性除外。

动态组允许您使用 LDAP URL 来定义仅与组成员相匹配的规则集。动态组的成员共享一个通用属性或一组在 `memberURL` 过滤器中定义的属性。例如，如果需要一个包含 Sales 中所有雇员的组，而这些雇员已经存在于 LDAP 数据库的 `ou=Sales,o=Airius.com` 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=*)
```

随后，此组将包含在树中 `ou=Sales,o=sun` 点下具有 `uid` 属性的所有对象。

对于静态组和动态组，如果您使用 `memberCertDescription`，其成员将可以通过证书共享某个通用属性。只有在 ACL 使用 SSL 方法时才能这样共享通用属性。

创建新组后，可以向其中添加用户（成员）。

本节包含以下主题：

关于静态组

对于 LDAP 服务，使用 Administration Server，您可以通过在任意数量用户的 DN 中指定相同的组属性来创建静态组。只有在向组中添加用户或从组中删除用户时静态组才会发生变化。

创建静态组的准则

使用 Administration Server 界面创建新静态组时，请考虑以下准则：

- 静态组可以包含其他静态或动态组。
- 如果为目录定义组织单位，可以使用 Administration Server 界面的 "Create Group" 页面中的 "Add New Group To list" 列表指定要放置新组的位置。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，请参见第 60 页中的 “编辑组条目”。

▼ 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. **键入 "Create Group" 页面中要求的信息。**
   有关特定字段的更多信息，请参见联机帮助。
5. **单击 "Create" 以创建组，或者单击 "Create and Edit" 以创建组并显示刚创建的组的编辑页面。**

关于动态组

对于 LDAP 服务，如果您希望基于任何属性自动将用户分组，或者希望将 ACL 应用于包含匹配 DN 的特定组，Proxy Server 允许您创建动态组。例如，可以创建一个自动包含任何具有属性 `department=marketing` 的 DN 的组。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。然后，您可以从基于此过滤器的搜索结果中定义一个动态组。随后，您可以为所获得的动态组定义一个 ACL。

如何实现动态组

Proxy Server 在 LDAP 服务器模式中以 objectclass=groupOfURLs 方式实现动态组。groupOfURLs 类可以具有零个或多个 memberURL 属性，每个属性都是描述目录中一组对象的 LDAP URL。组的成员是这些对象集合的总和。例如，下面的组仅包含一个成员 URL：

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

该示例描述了一个由 o=mcom.com 下部门为 marketing 的所有对象组成的集合。LDAP URL 可以包含搜索基 DN、范围和过滤器，但不包含主机名和端口。所以您只能引用同一个 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，请参见第 57 页中的 “创建动态组的准则”。

DN 会自动包含在内，因而无需向组中逐一添加每个 DN。由于每次 ACL 验证需要查找组时 Proxy Server 都将执行一次 LDAP 服务器搜索，因此组是动态变化的。ACL 文件中使用的用户姓名和组名与 LDAP 数据库中的对象的 cn 属性相对应。

注 – Proxy Server 使用 cn 属性作为 ACL 的组名。

从 ACL 到 LDAP 数据库的映射同时定义在 dbswitch.conf 文件（将 ACL 数据库名与实际 LDAP 数据库 URL 关联）和 ACL 文件（定义哪些 ACL 使用哪些数据库）中。例如，如果要使名为 staff 的组中的所有成员具有基本访问权限，ACL 代码将查找对象类为 groupOf*anything* 且 CN 设置为 staff 的对象。该对象可通过两种方法来定义组的成员，即显式枚举成员 DN（与对静态组的 groupOfUniqueNames 的操作相同），或指定 LDAP URL（例如，groupOfURLs）。

注 – 组可以同时是动态和静态的。组对象可以同时具有 objectclass=groupOfUniqueMembers 和 objectclass=groupOfURLs。因此，uniqueMember 和 memberURL 属性都是有效属性。组的全体成员是其静态成员和动态成员的集合。

动态组对服务器性能的影响

使用动态组会对服务器性能产生影响。如果您正在测试组成员资格，而 DN 不是静态组的成员，Proxy Server 将检查数据库基 DN 中的所有动态组。Proxy Server 通过根据用户 DN 检查每个 memberURL 的基 DN 和范围来确定每个 memberURL 是否匹配。这样，Proxy Server 使用用户 DN 作为基 DN 并使用 memberURL 作为过滤器来执行基搜索。这一过程可能涉及大量的单个搜索操作。

创建动态组的准则

使用 Administration Server 界面创建新动态组时，请考虑以下准则：

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

  `ldap:///` *base-dn*?*attributes*? *scope*?(*filter*)

根据 `attributes`、`scope` 和 `(filter)` 参数在 URL 中的位置来标识它们。即使不想指定任何属性，也必须包含用于分隔该字段的问号 (?)。

- 如果为目录定义组织单位，可以使用 Administration Server 界面的 "Create Group" 页面中的 "Add New Group To" 列表指定要放置新组的位置。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，请参见第 60 页中的 “编辑组条目” 。

下表列出了 LDAP URL 的必需参数。

表 4–4 LDAP URL 的必需参数

参数名	描述
`base_dn`	搜索基 DN 或在 LDAP 目录中执行所有搜索的起点。此参数通常被设置为目录的后缀或根，例如 `o=mcom.com`。
`attributes`	搜索将返回的属性列表。要指定多个属性，请使用逗号分隔这些属性（例如，`cn,mail,telephoneNumber`）。如果未指定任何属性，将返回所有属性。请注意，检查动态组成员资格时将忽略此参数。
`scope`	此参数是必需的。 搜索范围，其值可以是： ■ `base` 仅检索有关 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)` 下面所有级别的条目的信息。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。

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. **提供 "Create Group" 页面中要求的信息。**
   有关特定字段的更多信息，请参见联机帮助。
5. **单击 "Create" 以创建组，或者单击 "Create and Edit" 以创建组并显示刚创建的组的编辑页面。**

管理组

对于 LDAP 服务，使用 Administration Server，您可以在其 "Users and Groups" 选项卡的 "Manage Groups" 页面中编辑组和管理组成员资格。

本节包括以下主题：

查找组条目

在编辑组条目之前，必须首先查找并显示该条目，如以下过程所述。

▼ 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" 字段中键入要查找的组的名称。**

您可以提供任何以下信息：

- 使用星号 (*) 可以查看当前驻留在目录中的所有组。保留该字段为空也可以实现这一目的。
- 任何 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并缩小搜索结果的范围。有关更多信息，请参见第 59 页中的 “查找满足条件的所有组” 。
- 名称。提供全名或部分名。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，将返回包含该搜索字符串的所有条目。如果未找到包含搜索字符串的项，将查找所有发音与搜索字符串类似的项。

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，指定应将输出格式设置为用来显示在屏幕上还是用打印机打印。**

6 **要在此过程中的任何阶段显示满足条件的所有组，请单击 "Find" 按钮。**

7 **单击要显示的条目的链接。**

查找满足条件的所有组

对于 LDAP 服务，"Find All Groups Whose" 部分允许您生成自定义搜索过滤器。使用此部分中的字段可以缩小 "Find Group" 返回的搜索结果的范围。

左侧的下拉式列表指定搜索所基于的属性。可以使用以下选项：

- **Name**。搜索每个条目的全名以找出匹配的条目。
- **Description**。搜索每个组条目的描述以找出匹配的条目。

中间的下拉式列表指定要执行的搜索的类型。可以使用以下选项：

- **Contains**。执行子字符串搜索。将返回属性值包含指定搜索字符串的条目。例如，如果您知道组的名称可能包含单词 "Administrator"，则可以通过此选项使用搜索字符串 "Administrator" 来查找该组条目。
- **Is**。找到精确匹配的条目。如果您知道组属性的精确值，可以使用此选项。例如，您知道组名的精确拼写。
- **Isn't**。返回属性值与搜索字符串不精确匹配的所有条目。如果想要查找目录中名称不包含 "administrator" 的所有组，可以使用此选项。但是请注意，使用此选项可能导致返回大量条目。
- **Sounds like**。执行近似搜索。如果您知道属性的值，但不能确定其拼写，可以使用此选项。例如，您不知道组名的拼写是 "Sarret's list"、"Sarette's list" 还是 "Sarett's list"。

- **Starts with**。执行子字符串搜索。返回属性值以指定的搜索字符串开头的所有条目。例如，您知道组名以 "Product" 开头， 但不知道其余部分。
- **Ends with**。执行子字符串搜索。返回属性值的结尾与指定搜索字符串匹配的所有条目。例如，如果您知道组名以 "development" 结尾， 但不知道其余部分。

在右侧的文本字段中，输入搜索字符串。要显示在 "Look Within" 目录中包含的所有组条目，请输入星号 (*) 或保留此字段为空。

编辑组条目

▼ 编辑组条目

以下过程仅适用于 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. **按第 58 页中的“ 查找组条目 ”中所述找到要编辑的组。**
4. **进行所需的更改。**
   有关特定字段和按钮的更多信息，请参见联机帮助。

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

添加组成员

▼ 向组中添加成员

以下过程仅适用于 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. **按第 58 页中的“ 查找组条目 ”中所述找到并显示要管理的组，然后单击 "Group Members" 旁边的 "Edit" 按钮。**
   所显示的页面中将列出全部现有组成员。还将显示搜索字段。
   - 要向成员列表中添加用户条目，必须在 "Find" 下拉式列表中选择 "Users"。

- 要向组中添加组条目，必须选择 "Groups"。

4 **在 "Matching " 文本字段中，输入搜索字符串。提供任何以下选项的信息。**

- 姓名。输入全名或部分名。将返回姓名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，将返回包含该搜索字符串的所有条目。如果未找到包含搜索字符串的项，将查找所有发音与搜索字符串类似的项。
- 用户 ID。如果您仅输入部分用户 ID，将返回所有包含该字符串的条目。
- 电话号码。如果您只输入部分号码，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。任何包含 @ 符号的搜索字符串均被认为是电子邮件地址。如果找不到精确的匹配，将执行搜索并返回以该搜索字符串开头的所有电子邮件地址。
- 输入星号 (*) 或保留该字段为空可以查看当前驻留在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" 以在 LDAP 数据库中查找所有匹配的条目，然后将这些条目添加到组中。**

6 **（可选）如果不想将搜索返回的条目添加到组中，请单击 "Remove From List" 列中对应的复选框。您还可以构建一个搜索过滤器以匹配要从组中删除的条目，然后单击 "Remove"。有关更多信息，请参见第 61 页中的 “ 从组成员列表中删除条目 ”。**

7 **完成组成员列表后，单击 "Save Changes"。这些条目将添加到组成员列表中。**

向组成员列表中添加组

对于 LDAP 服务，可以向组的成员列表中添加组而不是各个成员。属于被包括的组的任何用户将成为接收组的成员。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，那么 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一样添加该组。有关更多信息，请参见第 60 页中的 “添加组成员”。

从组成员列表中删除条目

此过程仅适用于 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 **找到要管理的组。**

有关更多信息，请参见第 58 页中的 “查找组条目” 。单击 "Group Members" 旁边的 "Edit" 按钮。

4 **指出要删除的成员。**

- 要仅删除一些成员，请单击 "Remove From List" 列中对应的复选框。
- 要基于通用条件删除成员，请构建一个搜索过滤器，以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，请参见第 60 页中的 “添加组成员” 。

5 **单击 "Save Changes"。**

这些条目将从组成员列表中删除。

管理所有者

对于 LDAP 服务，管理组所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可提供更多信息的主题。

表 4–5 管理所有者

目标	请参见
向组中添加所有者	第 60 页中的 “添加组成员”
向所有者列表中添加组	第 61 页中的 “向组成员列表中添加组”
从所有者列表中删除条目	第 61 页中的 “从组成员列表中删除条目”

管理 "See Alsos"

"See Alsos" 是对可能与当前组相关的其他目录条目的引用。利用这些引用，用户可以很容易地找到与当前组相关的用户条目和其他组条目。管理 "See Alsos" 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可提供更多信息的主题。

表 4–6 管理 "See Alsos"

要	请参见
向 "See Alsos" 添加用户	第 60 页中的 “添加组成员”

表 4–6 管理 "See Alsos" （续）

要	请参见
向 "See Alsos" 添加组	第 61 页中的 “向组成员列表中添加组”
从 "See Alsos" 中删除条目	第 61 页中的 “从组成员列表中删除条目”

重命名组

此过程仅适用于 LDAP 服务。重命名组条目时，仅更改组的名称。不能使用 "Rename Group" 功能将条目从一个组织单位移到另一个组织单位。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，您可以将 Online Sales 重命名为 Internet Investments，但是不能通过重命名条目使 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，并按第 58 页中的 “查找组条目”中所述找到要管理的组。**
3. **单击 "Rename Group" 按钮。**
4. **在所显示的页面上指定新的组名，然后单击 "Save Changes"。**

删除组

此过程仅适用于 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. **按第 58 页中的 “查找组条目”中所述找到要管理的组，然后单击 "Delete Group"。**

注 – 组的各个成员不会被删除。仅删除组条目。

创建组织单位

对于 LDAP 服务，组织单位可以包括很多组，通常具有部门、分部或其他独立实体。DN 可以存在于多个组织单位中。

- 使用 `organizationalUnit` 对象类可创建新的组织单位。
- 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*

▼ 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，然后单击 "Create"。**

   有关特定字段的更多信息，请参见联机帮助。

   例如，如果在组织单位 West Coast 中创建一个名为 Accounting 的新组织单位，并且您的基 DN 为 `o=Ace Industry, c=US`，则新组织单位的 DN 为：

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

管理组织单位

对于 LDAP 服务，可通过 Administration Server 的 "Users and Groups" 选项卡中的 "Organizational Units" 页面来编辑和管理组织单位。

本节包含以下主题：

- 第 64 页中的 “查找组织单位”
- 第 66 页中的 “编辑组织单位属性”
- 第 66 页中的 “重命名组织单位”
- 第 67 页中的 “删除组织单位”

查找组织单位

此过程仅适用于 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 "Organizational Units" 链接。**
3. **在 "Find Organizational Unit" 字段中输入您要查找的单位的名称。**

   您可以输入以下任何信息：

   - 名称。输入全名或部分名。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，将返回包含该搜索字符串的所有条目。如果未找到包含搜索字符串的条目，将查找所有发音与搜索字符串类似的条目。
   - 使用星号 (*) 可以查看当前驻留在您目录中的所有组。保留该字段为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，请参见第 65 页中的 “查找满足条件的所有单位”。
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，指定应将输出格式设置为用来显示在屏幕上还是用打印机打印。**
6. **在此过程中的任何阶段，单击 "Find" 按钮。**

   此时将显示与搜索条件相匹配的所有组织单位。
7. **单击要显示的条目的链接。**

查找满足条件的所有单位

对于 LDAP 服务，利用 "Find All Units Whose" 部分可以生成自定义搜索过滤器。使用此部分中的字段可以缩小 "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所基于的属性。可以使用以下选项：

- **Unit name**。搜索每个条目的全名找出匹配的条目。
- **Description**。搜索每个组织单位条目的描述找出匹配的条目。

中间的下拉式列表指定要执行的搜索的类型。可以使用以下选项：

- **Contains**。执行子字符串搜索。将返回属性值包含指定搜索字符串的条目。例如，如果您知道组织单位的名称可能包含单词 "Administrator"，则可以通过此选项使用搜索字符串 "Administrator" 来查找该组织单位条目。
- **Is**。找到精确匹配的条目。如果您知道组织单位属性的精确值，可以使用此选项。例如，您知道组织单位名称的精确拼写。

- **Isn't**。返回属性值与搜索字符串不精确匹配的所有条目。即，如果要查找目录中名称不包含 "administrator" 的所有组织单位，可以使用此选项。但是请注意，使用此选项可能导致返回大量条目。
- **Sounds like**。执行近似搜索。如果您知道属性的值，但不能确定其拼写，可以使用此选项。例如，您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**。执行子字符串搜索。返回属性值以指定的搜索字符串开头的所有条目。例如，您知道组织单位名称以 "Product" 开头， 但不知道其余部分。
- **Ends with**。执行子字符串搜索。返回属性值的结尾与指定搜索字符串匹配的所有条目。例如，您知道组织单位名称以 "development" 结尾， 但不知道其余部分。

在右侧的文本字段中，输入搜索字符串。要显示在 "Look Within" 目录中包含的所有组织单位条目，请输入星号 (*) 或保留此字段为空。

编辑组织单位属性

此过程仅适用于 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 "Organizational Units" 链接。**
3. **按第 64 页中的 “ 查找组织单位 ”中所述找到要编辑的组织单位。**
4. **进行所需的更改。**
   有关特定字段的更多信息，请参见联机帮助。

注 – 要更改组织单位编辑页面中未显示的属性值，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

此过程仅适用于 LDAP 服务。重命名组织单位条目时，仅更改组织单位的名称。不能使用重命名功能将条目从一个组织单位移到另一个组织单位。

▼ 重命名组织单位

1 访问 Administration Server 并单击 "Users and Group" 选项卡。

2 单击 "Manage Organizational Units" 链接。

3 按第 64 页中的“ 查找组织单位 ”中所述找到要编辑的组织单位。

4 单击 "Rename" 按钮。

5 在所显示的页面中键入新的组织单位名称，然后单击 "Save Changes"。

删除组织单位

此过程仅适用于 LDAP 服务。

▼ 删除组织单位

1 访问 Administration Server 并单击 " Users and Groups" 选项卡。

2 单击 "Manage Organizational Units" 链接。

3 按第 64 页中的“ 查找组织单位 ”中所述找到要删除的组织单位。

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

本章介绍了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 引入了所有 Sun Java System 服务器的安全体系结构，并且以行业标准和公共协议为基础，最大程度地保证了互操作性和一致性。

本章假定您已熟悉公钥加密的基本概念，包括加密和解密、公钥和私钥、数字证书以及加密协议。

本章包含以下各节：

确保 Administration Server 访问的安全性

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，需要确保其安全性。

默认 Administration Server 页面在 HTTP 模式下启动。可用的 Proxy Server 实例以列表的形式显示在标题 "Manage Servers" 的下方。要管理任何 Proxy Server 实例，请单击列表中的名称。单击 Proxy Server 实例的名称时，将显示该实例的 Server Manager 页面。

在 Server Manager 页面中，单击该页面左上角的 "Manage Servers" 链接可返回到 Administration Server 页面。

安全性功能（如基于证书的验证、创建信任数据库、配置 SSL、申请并安装证书、设置安全性首选项等）可应用于 Administration Server 和各个 Proxy Server 实例。对于 Administration Server 的安全性相关的配置，请使用 Administration Server 页面上显示的 "Preferences" 选项卡和 "Security" 选项卡。对于 Proxy Server 实例相关的安全性配置，请使用该实例的 Server Manager 页面上显示的 "Preferences" 选项卡和 "Security" 选项卡。

要在安全模式下启动 Administration Server，需要使用 HTTPS 而不是默认 HTTP 进行访问。

以下各节详细介绍了这些安全性功能。

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的保密确认。证书是支持验证的一种方法。

证书中包含的数字数据指定了个人、公司或其他实体的名称，并证明证书中包含的公钥属于该实体。

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保密确认，或者对假定为负责特定网络地址服务器的组织的确认。客户机验证指服务器对客户机进行的保密确认，或者对假定为正在使用客户机软件的用户的确认。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 (Certificate Authority, CA) 颁发并进行数字签名。CA 可以是销售证书的公司，也可以是负责为您公司的内联网或外部网颁发证书的部门。您可以将您充分信任的 CA 确定为其他用户身份的检验者。

证书包括以下信息。

- 公钥
- 由证书标识的实体的名称
- 到期日期
- 颁发证书的 CA 的名称
- 颁发 CA 的数字签名

注 – 在激活加密之前必须安装服务器证书。

创建信任数据库

申请服务器证书之前，必须创建信任数据库。在 Proxy Server 中，Administration Server 和每个服务器实例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密码。您还需要此密码来启动使用加密通信的服务器。有关选择密码时应考虑的一系列准则，请参见第 102 页中的 “选择强密码”。

在信任数据库中，可以创建并存储公钥和私钥（称为密钥对文件）。密钥对文件用于 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，并单击 "Security" 选项卡。**
2. **单击 "Create Database" 链接。**
3. **键入信任数据库的密码。**
4. **再次键入密码，然后单击 "OK"。**

使用 password.conf

默认情况下，Proxy Server 在启动之前会提示管理员输入密钥数据库密码。要重新启动无人参与的 Proxy Server，必须将密码保存在 `password.conf` 文件中。仅当系统具有充分的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，不能使用 `/etc/ rc.local` 或 `/etc/inittab` 文件启动启用了 SSL 的 UNIX 服务器，因为该服务器在启动前要求输入密码。虽然可以通过将密码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，但这样做会不安全。服务器的 `password.conf` 文件应归 root 用户或安装服务器的用户所有，并且只有所有者对该文件拥有读写权限。

在 UNIX 上，将启用了 SSL 的服务器的密码保存在 `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 的服务器的密码。将启用了 SSL 的服务器的密码保存在 `password.conf` 文件中之前，请考虑可能带来的安全风险。

在 Windows 上，如果使用的是 NTFS 文件系统，应通过限制访问来对包含 `password.conf` 文件的目录进行保护，即使不使用该文件也应该这样做。Administration Server 用户和 Proxy Server 用户应该对该目录拥有读写权限。保护该目录可以防止其他用户创建伪 `password.conf` 文件。在 FAT 文件系统上，无法通过限制访问来保护目录或文件。

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. **确保已启用了 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，请键入以下信息：`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，并后跟密码，例如：`nFast:`*your-password*

     即使在创建了 `password.conf` 文件之后，您在启动 Proxy Server 时始终会收到输入密码的提示。

申请和安装 VeriSign 证书

VeriSign 是 Proxy Server 的首选证书授权机构。该公司的技术简化了证书申请过程。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（Certificate Authority，证书授权机构）。如果您的公司有自己的内部 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。

▼ 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 link." 链接。**
3. **查看所显示的页面中列出的步骤，然后单击 "OK"。**
   "VeriSign Enrollment Wizard" 将引导您完成该过程。

▼ 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. **如果不计划使用外部加密模块，请从 "Cryptographic Module" 下拉式列表中选择 "Internal"。**
4. **键入密钥对文件密码或 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

除了 VeriSign，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。

本节包含以下主题：

所需的 CA 信息

在启动申请过程之前，确保已清楚 CA 需要的信息。不同的 CA 要求的信息的格式会有所不同，但通常都会要求您提供以下所列信息。对于证书更新，以下大部分信息通常不是必需的。

- **申请者名称。**依据其颁发证书的名称。
- **电话号码。**申请者的电话号码。

- **通用名称**。DNS 查找中使用的全限定主机名，例如 `www.example.com`。
- **电子邮件地址**。您与 CA 进行通信联系时使用的企业电子邮件地址。
- **组织**。您的公司、教育机构和组织等的法定名称。多数 CA 需要您使用法律文档（例如营业执照副本）验证此信息。
- **组织单位**。您的公司内部组织单位的说明。
- **地址**。组织所在的城市、公国或国家/地区的说明。
- **省/自治区/直辖市**。企业所在的省/自治区/直辖市。
- **国家/地区**。您所在国家/地区的名称的双字符缩写（以 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 (distinguished name, DN)），用于唯一标识证书的主题。

如果从商业 CA 处购买证书，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，还可能询问您是否拥有使用您提供的信息的合法权限。

某些商业 CA 向出具较为详细标识的组织或个人提供内容详细且精确的证书。例如，您可以购买一个证书，声明 CA 不仅验证了您是 `www.example.com` 计算机的合法管理员，而且验证了您的公司是已从事三年商业活动且无未决的客户诉讼案件的公司。

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. **指定是否要提交证书申请：**
   - 要使用电子邮件提交申请，请选择 "CA Email Address"，然后输入这些申请相应的电子邮件地址。
   - 要使用 CA 的 Web 站点提交申请，请选择 "CA URL"，然后键入这些申请相应的 URL。
5. **从 "Cryptographic Module" 下拉式列表中，选择在申请证书时要用于密钥对文件的加密模块。**

6 **键入密钥对文件的密码。**

除非选择了加密模块而不是 "Internal"，否则在创建信任数据库时指定该密码。服务器将使用该密码获取专私钥并加密发送给 CA 的消息，然后将您的公钥和加密的消息发送给 CA。CA 使用公钥来解密您的消息。

7 **提供您的标识信息，如姓名和电话号码。**

此信息的格式因 CA 而异。对于证书更新，以下大部分信息通常都不需要。

8 **再次检查您的工作以确保准确性，然后单击 "OK"。**

信息越准确，批准证书的速度可能就越快。如果要将申请发送至证书服务器，您将在提交申请之前收到验证格式信息的提示。

服务器将生成包含您的信息的证书申请。该申请中包含使用私钥创建的数字签名。CA 使用数字签名来验证在从服务器计算机向 CA 的路由过程中申请是否被更改。极少数情况下申请会被更改，这时 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，服务器将发送包含该申请的电子邮件到 CA。通常，证书会在随后通过电子邮件发送给您。如果您指定了指向证书服务器的 URL，服务器将使用该 URL 向证书服务器提交申请。您可能会收到电子邮件响应或某种其他方式的响应，视 CA 而定。

如果 CA 同意向您颁发证书，将会通知您。多数情况下，CA 会使用电子邮件向您发送证书。如果您的组织使用的是证书服务器，可以使用证书服务器的表单搜索证书。

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。另外，审批通常可能会花费一天到几周不等的时间。您应向 CA 及时提供所有需要的信息。

在收到证书后，安装该证书。在此期间，您仍然可以使用未安装 SSL 的 Proxy Server。

安装其他服务器证书

您从 CA 收到的证书会使用您的公钥加密，因此只有您可以将其解密。只有输入正确的信任数据库密码，才能解密和安装证书。

证书包含三种类型：

- 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
- 信任的 CA 的证书

证书链是由连续证书授权机构签名的一系列分层证书。CA 证书用于标识证书授权机构以及对该机构颁发的证书进行签名。反过来，CA 证书又可以由父 CA 的 CA 证书签名，依此类推，直到根 CA。

注 – 如果 CA 没有自动向您发送他们的证书，请申请该证书。很多 CA 在电子邮件中包含他们的证书和您的证书，您的服务器将同时安装这两个证书。

您从 CA 收到的证书会使用您的公钥加密，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密码将其解密。您可以将电子邮件保存在服务器可以访问的位置中，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，如以下过程所述。

▼ 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，选择要安装的证书的类型：**
   - This Server
   - Server Certificate Chain
   - Certification Authority

   有关特定设置的更多信息，请参见联机帮助。
4. **从下拉式列表中选择加密模块。**
5. **键入密钥对文件密码。**
6. **只有在步骤 3 中选择了 "Server Certificate Chain" 或 "Certification Authority" 时，才需要键入证书名称。**
7. **通过执行以下操作之一提供证书信息：**
   - 选择 "Message Is In This File"，然后键入包含 CA 证书的文件的完整路径名。
   - 选择 "Message Text"（包含标头），然后复制并粘贴 CA 证书的内容。请确保包含标头 Begin Certificate 和 End Certificate，其中包含起始和终止连字符。
8. **单击 "OK"。**
9. **指出是添加新证书还是更新现有证书。**
   - 添加证书（如果要安装新的证书）。
   - 替换证书（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

从先前版本迁移证书

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，将会自动更新相应的文件（包括信任数据库和证书数据库）。

确保 Proxy Server 4 Administration Server 拥有旧 3.x 数据库文件的读取权限。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保护时，才可以迁移密钥对文件和证书。您也可以使用 Administration Server 和 Server Manager 的 "Security" 选项卡中的 "Migrate 3.x Certificates" 选项自动迁移密钥和证书。有关特定设置的信息，请参见联机帮助。

在以前的版本中，证书和密钥对文件由别名引用，该别名可以由多个服务器实例使用。Administration Server 管理所有的别名及其委托证书。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。

从 Administration Server 可以为其本身管理信任数据库及其委托证书，从 Server Manager 可以为服务器实例管理信任数据库及其委托证书。证书和密钥对数据库文件按使用它们的服务器实例命名。如果是在以前的版本中，多个服务器实例共享同一个别名，迁移时将为新服务器实例重命名证书和密钥对文件。

与服务器实例关联的整个信任数据库将被迁移。以前数据库中列出的所有 CA 将被迁移到 Proxy Server 4 数据库。如果出现重复的 CA，请使用以前的 CA，直到它过期。请不要尝试删除重复的 CA。

Proxy Server 3.x 证书将被迁移为支持的网络安全服务 (Network Security Services, NSS) 格式。证书将根据是从 Administration Server 还是从 Server Manager 的 "Security" 选项卡访问了 Proxy Server 页面，来进行相应命名。

▼ 迁移证书

1. **从本地计算机访问 Administration Server 或 Server Manager，然后选择 "Security" 选项卡。**
2. **单击 "Migrate 3.x Certificates" 链接。**
3. **指定安装 3.6 版服务器的根目录。**
4. **指定此计算机的别名。**

5 **键入管理员密码，然后单击 "OK"。**

使用内置根证书模块

Proxy Server 附带的动态可加载根证书模块包含许多 CA（包括 VeriSign）的根证书。通过根证书模块，可以更容易地将根证书升级到更高的版本。以前，您需要逐个删除旧的根证书，然后再逐个安装新的证书。要安装常用的 CA 证书，现在可以只将根证书模块文件更新到更高的版本，因为它在以后版本的 Proxy Server 中将可用。

由于根证书是作为 PKCS #11 加密模块实现的，因此您将无法删除其中包含的证书。管理这些证书时，不会提供用于删除的选项。要删除服务器实例的根证书，可通过删除服务器的 `alias` 目录中的以下条目来禁用根证书模块。

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

如果要恢复根证书模块，可以将 `libnssckbi.so` 或 `nssckbi.dll` 从 *server-root*`/bin/proxy/lib` (UNIX) 或 *server-root*`\\ bin\\proxy\\bin` (Windows) 复制到 `alias` 子目录中。

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、删除或编辑自己的证书或服务器上安装的 CA 证书的信任设置。

▼ 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到期日期。所有证书都存储在 *server-root*`/alias` 目录中。
  - 如果要使用外部加密模块（例如硬件加速器），必须先为每个特定模块键入密码，然后单击 "OK"。证书列表将更新，以便在模块中包含这些证书。

3 **单击要管理的证书的名称。**

此时将显示一个页面，其中包含该类型证书的管理选项。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。**

可以使用以下选项：

- "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 (Certificate revocation list, CRL) 和已泄密密钥列表 (compromised key list, CKL) 公开客户机用户或服务器用户不应再信任的任何证书和密钥。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变更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 均由 CA 生成并由 CA 定期更新。与特定 CA 联系以获取这些列表。

本节介绍如何安装和管理 CRL 和 CKL。

▼ 安装 CRL 或 CKL

1 **从 CA 获取 CRL 或 CKL，并将其下载到本地目录。**

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 **键入关联文件的完整路径名，然后单击 "OK"。**

此时将显示 "Add Certificate Revocation List" 或 "Add Compromised Key List" 页面，其中列出了 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

1 **访问 Administration Server 或 Server Manager，然后单击 "Security" 选项卡。**

2 **单击 "Manage CRL/CKL" 链接。**

此时将显示 "Manage Certificate Revocation Lists /Compromised Key Lists" 页面，其中列出了所有已安装的 CRL 和 CKL 及其到期日期。

3 **从 "Server CRLs" 或 "Server CKLs" 列表中选择一个证书。**

4 **选择 "Delete CRL" 或 "Delete CKL" 可删除 CRL 或 CKL。.**

5 **退出以返回到管理页面。**

设置安全性首选项

获得证书后，就可以开始保护您的服务器。Sun Java System Web Proxy Server 提供了许多安全性元素，将在本节中讨论。

加密是变换信息的过程，使信息变得对除预定接受者之外的任何用户都不可理解。解密是变换已加密信息的过程，使信息再次变得可理解。Proxy Server 支持安全套接字层 (Secure Sockets Layer, SSL) 和传输层安全 (Transport Layer Security, TLS) 加密协议。

加密算法是一种用于加密或解密的密码学算法（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且更安全。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，因此必须让服务器使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。您可以选择 SSL 2.0、SSL 3.0 和 TLS 协议的加密算法。

注 – 因为在 SSL 2.0 之后对 SSL 的安全性和性能进行了各种改进，所以除非客户机无法使用 SSL 3.0，否则不要使用 SSL 2.0。使用 SSL 2.0 加密算法无法为客户机证书提供保证。

单独的加密过程并不足以确保服务器机密信息的安全。密钥必须与加密算法一起使用才能产生实际的加密结果，或者解密先前加密的信息。加密过程使用以下两种密钥获得此结果：公钥和私钥。使用公钥加密的信息只能使用关联的私钥进行解密。公钥作为证书的一部分进行发布。只有关联的私钥受到安全保护。

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，请参见《SSL 介绍》。

您可以指定服务器将使用的加密算法。除非有充分的理由不使用特定的加密算法，否则应全部选中。您可能不希望启用非最优加密的加密算法。

注意 – 不要选择 "Enable No Encryption, Only MD5 Authentication"。如果客户端没有其他可用的加密算法，服务器将默认使用此设置且不进行加密。

本节包含以下主题：

SSL 和 TLS 协议

Proxy Server 支持SSL 和 用于加密通信的 TLS 协议。SSL 和 TLS 是独立的应用程序，并且更高级的协议可以在它们上面透明地分层排列。

SSL 和 TLS 协议支持各种加密算法，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。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。

注 – 此情况下，Proxy Server 充当 SSL 客户机，且必须已导入用于签署 SSL 服务器 LDAP 证书的根 CA 证书。如果 LDAP 的 SSL 证书不是由知名 CA 颁发，则必须将所使用的 CA 根密钥导入到 Proxy Server 密钥库中。

▼ 在 Administration Server 上使用 SSL 连接启用 LDAP

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

3 **在所显示的表中，单击目录服务链接。**

此时将显示 "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。有关针对基于 LDAP 的目录服务显示的特定字段的更多信息，请参见联机帮助。

4 **选择 "Yes" 可以对连接使用 SSL，然后单击 "Save Changes"。**

通过 Proxy Server 对 SSL 进行隧道操作

在正向运行 Proxy Server（代理）且客户机通过代理请求到安全服务器的 SSL 连接时，代理将打开到安全服务器的连接，并复制双向数据，且不介入安全事务。此过程称为 SSL 隧道，如下图所示。

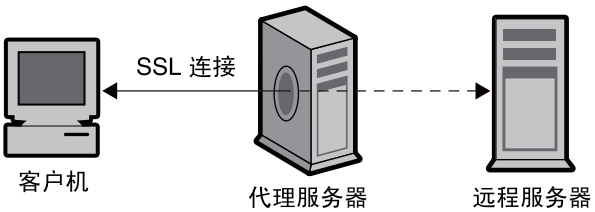

图 5–1 SSL 连接

要将 SSL 隧道与 HTTPS URL 一起使用，客户机必须支持 SSL 和 HTTPS。将 SSL 与常规 HTTP 一起使用可实现 HTTPS。不支持 HTTPS 的客户机仍然可以使用 Proxy Server 的 HTTPS 代理功能访问 HTTPS 文档。

SSL 隧道为较低层的活动，不会影响应用层 (HTTPS)。SSL 隧道与不使用代理的 SSL 一样安全。中间存在代理不会对安全性带来任何危害，也不会降低 SSL 的功能。

使用 SSL 时，数据流会被加密，这样代理将无权访问实际事务。因此，访问日志不能列出从远程服务器收到的状态码或标头长度。此过程也可防止代理或任何其他第三方对事务进行窃听。

由于代理不会看到数据，因此无法验证客户机与远程服务器之间使用的协议是否为 SSL。所以，代理也无法阻止其他协议通过。应将 SSL 连接限制为仅使用 Internet 号码分配机构 (Internet Assigned Numbers Authority, IANA) 指定的常用 SSL 端口，即端口 443（对于 HTTPS）以及 563（对于 SNEWS）。如果站点在其他某个端口上运行安全服务器，可以使用 `connect://.*` 资源，使显式异常允许到某主机上其他端口的连接。

SSL 隧道功能实际上一个类似于 SOCKS 的常规功能，它独立于协议，因此也可以将此功能用于其他服务。Proxy Server 可以对支持 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

以下步骤说明了如何配置 Proxy Server 对 SSL 进行隧道操作。

▼ 配置 SSL 隧道

1. **访问服务器实例的 Server Manager 并单击 "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://` 方法是内部代理表示法，不能存在于代理外部。有关 `connect` 的更多信息，请参见第 83 页中的 “SSL 隧道的技术详细信息” 。

   要允许到其他端口的连接，可以使用模板中类似的 URL 模式。有关模板的更多信息，请参见第 16 章。

4. **选择 "Enable Proxying Of This Resource" 然后单击 "OK"。**

注意 – 如果未正确配置代理，有人可能会利用代理使 telnet 连接看起来来自代理主机而不是实际连接主机。所以，在非绝对必要的情况下，不要允许使用任何其他端口，并且可以在代理上使用访问控制来限制客户机主机。

SSL 隧道的技术详细信息

SSL 隧道在内部将 `CONNECT` 方法与作为参数的目标主机名和端口号一起使用，后跟一个空行：

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

以下示例说明了 Proxy Server 的成功响应，并后跟一个空行：

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

然后，将在客户机与远程服务器之间建立连接。数据可以双向传输，直到任意一方关闭连接。

在内部，为了利用基于 URL 模式的典型配置机制，主机名和端口号会自动被映射到 URL，例如：

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

`connect://` 是 Proxy Server 为了使配置更简单，与其他 URL 模式更统一而采用的内部表示法。在 Proxy Server 外部，不存在 `connect` URL。如果 Proxy Server 收到来自网络的这样的 URL，它将标记该 URL 无效，并拒绝对请求提供服务。

为侦听套接字启用安全性

可以通过执行以下操作来确保服务器的侦听套接字的安全性：

- 打开安全性
- 为侦听套接字选择服务器证书
- 选择加密算法

注 – 只能在反向代理模式下启用安全性，而不能在正向代理模式下启用。

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. **提供所需的信息。**

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

---

4. **要打开安全性，请从 "Security" 下拉式列表中选择 "Enabled"，然后单击 "OK"。**
   如果未安装服务器证书，唯一的选择为 "Disabled"。有关特定设置的更多信息，请参见联机帮助。

▼ 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. **从 "Security" 下拉式列表中选择 "Enabled"，然后单击 "OK"。**
   如果未安装服务器证书，唯一的选择为 "Disabled"。

为侦听套接字选择服务器证书

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. **从 "Security" 下拉式列表中选择 "Enabled"，然后单击 "OK"。**
   如果未安装服务器证书，唯一的选择为 "Disabled"。
5. **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，可为特定服务器实例设置这些安全性首选项。必须至少安装一个证书。

注 – 只有将 Proxy Server 配置为执行反向代理时，在侦听套接字上启用 SSL 才适用。

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，否则应全部选中。

TLS 回滚的默认和推荐设置为 "Enabled"。此设置配置服务器检测“中间人版本回滚”攻击企图。为了实现与某些未正确实现 TLS 规范的客户机的互操作性，可能需要将 TLS 回滚设置为 "Disabled"。

禁用 TLS 回滚将使连接容易遭到版本回滚攻击。版本回滚攻击是第三方可以强制客户机和服务器使用旧的、不安全的协议（如 SSL 2.0）进行通信的一种机制。由于 SSL 2.0 协议具有已知的缺陷，因此无法检测“版本回滚”攻击企图将使第三方很容易截取并解密已加密的连接。

▼ 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，将会显示可用的加密算法设置。

   如果未在侦听套接字上启用安全性，将不会列出任何 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该安全性。有关更多信息，请参见第 84 页中的 “为侦听套接字启用安全性”。
3. **选中对应于所需加密设置的复选框，然后单击 "OK"。**
4. **为 Netscape Navigator 6.0 选择 TLS 和 SSL 3.0。为 TLS 回滚也选择 TLS，并确保 SSL 3.0 和 SSL 2.0 都已禁用。**

   在服务器上启用 SSL 后，其 URL 将使用 `https` 而不是 `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*, for example, `https://admin.example.com:443`

   如果使用默认的安全 HTTP 端口 (443)，将不需要在 URL 中输入该端口号。

全局配置安全性

安装启用了 SSL 的服务器将会在 `magnus.conf` 文件中创建指令条目，该文件是服务器的全局安全性参数的主配置文件。

SSLSessionTimeout

`SSLSessionTimeout` 指令用于控制 SSL 2.0 会话高速缓存。语法为：

`SSLSessionTimeout` *seconds*

其中 *seconds* 是高速缓存的 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

指定可以高速缓存的 SSL 会话的数量。

SSL3SessionTimeout

`SSL3SessionTimeout` 指令用于控制 SSL 3.0 和 TLS 会话高速缓存。语法为：

`SSL3SessionTimeout` *seconds*

其中 *seconds* 是高速缓存的 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。

▼ 为 SSL 配置文件指令设置值

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，请参见第 84 页中的 “为侦听套接字启用安全性”。
3. **手动编辑 `magnus.conf` 文件并提供以下设置的值：**
   - `SSLSessionTimeout`
   - `SSLCacheEntries`
   - `SSL3SessionTimeout`

   有关 `magnus.conf` 的更多信息，请参见《Sun Java System Web Proxy Server 4.0.4 Configuration File Reference》。

使用外部加密模块

Proxy Server 支持按照以下方法使用外部加密模块（如智能卡或令牌环）：

- PKCS #11
- FIPS-140

激活 FIPS-140 加密标准之前，必须添加 PKCS #11 模块。

本节包含以下主题：

安装 PKCS #11 模块

Proxy Server 支持公钥加密标准 (Public Key Cryptography Standard, PKCS) #11，该标准定义了在 SSL 和 PKCS #11 模块之间通信所使用的端口。PKCS #11 模块用于指向 SSL 硬件加速器的基于标准的连接。外部硬件加速器的已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。该文件位于 *server-root*`/alias` 目录中。

使用工具 `modutil` 安装 PKCS #11 模块

可以使用 `modutil` 工具安装 `.jar` 文件或对象文件形式的 PKCS #11 模块。

▼ 使用工具 modutil 安装 PKCS #11 模块

1. **确保关闭了所有服务器（包括 Administration Server）。**
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。**
   - 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`

     您会发现您计算机的 PATH 列在 *server-root*`/proxy-admserv/start` 下。
6. **在终端窗口中，键入 modutil。**

   将列出各种选项。
7. **执行所需的操作。**

   例如，要在 UNIX 中添加 PKCS #11 模块，请输入：

   `modutil -add`（*PKCS#11* **文件的名称**）`-libfile`（**用于** *PKCS #11* **的** *libfile*）`-nocertdb -dbdir`（**数据库目录**）。

使用工具 pk12util 导出

使用 `pk12util` 可以将证书和密钥从内部数据库导出，以及将其导入到内部或外部 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` 的证书数据库和密钥数据库。

▼ 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。**

- 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`

  您可以在以下位置找到您计算机的 PATH：*server-root*`/proxy-admserv/start`。

5 **在终端窗口中，键入** `pk12util`。
将列出各种选项。

6 **执行所需的操作。**
例如，在 UNIX 中键入

```
pk12util -o certpk12 -n Server-Cert [-d /server/alias] [-P https-test-host]
```

7 **键入数据库密码。**

8 **键入** `pkcs12` **密码。**

▼ 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，将以下内容添加到 `PATH`

  `LD_LIBRARY_PATH server-root/bin/proxy/bin`

  可在 *server-root*`/proxy-admserv/start` 中找到您计算机的 PATH。

5 **在终端窗口中，键入** `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` 之后，且必须是最后一个参数。

键入正确的令牌名称，包括大写字母和引号之间的空格。

7 **键入数据库密码。**

8 **键入 `pkcs12` 密码。**

使用外部证书启动服务器

如果将服务器证书安装到外部 PKCS #11 模块（如硬件加速器）中，在编辑 `server.xml` 文件或指定如下所示的证书名称之前，将无法使用该证书启动服务器。

服务器会始终尝试使用名为 Server-Cert 的证书启动。但是，外部 PKCS #11 模块中的证书在其标识符中包括模块的某个令牌名称。例如，名为 `smartcard0` 的外部智能卡读取器上安装的服务器证书应命名为 `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

如果未在侦听套接字上启用安全性，将不会列出证书的信息。要为侦听套接字选择证书名称，首先必须确保已在该侦听套接字上启用了安全性。有关更多信息，请参见第 84 页中的 “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。

但您也可以通过手动编辑 `server.xml` 文件要求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。

如果未创建信任数据库，当申请或安装外部 PKCS #11 模块的证书时，将会为您创建一个数据库。创建的默认数据库没有密码，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。如果创建了没有密码的默认数据库，请使用 "Security" 选项卡上的 "Create Database" 页面设置密码。

FIPS-140 标准

通过 PKCS #11 API，您可以与执行加密操作的软件或硬件模块进行通信。在 Proxy Server 上安装了 PKCS #11 之后，可以配置服务器使其符合 FIPS-140。FIPS 表示 联邦信息处理标准 (Federal Information Processing Standard)。这些库仅包含在 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 Sockets" 页面将显示可用的安全性设置。

   要使用 FIPS-140，请确保已在选定侦听套接字上启用了该安全性。有关更多信息，请参见第 84 页中的 “为侦听套接字启用安全性”。
4. **从 "SSL Version 3" 下拉式列表中选择 "Enabled"（如果尚未选定）。**
5. **选择相应的 FIPS-140 加密算法套件，然后单击 "OK"：**
   - 启用三重 DES（使用 168 位加密）和 SHA 验证 (FIPS)
   - 启用 DES（56 位加密）和 SHA 验证 (FIPS)

设置客户机安全性要求

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性要求。

客户机验证对于 SSL 连接不是必要的，但是可以提供额外的保证，即已加密的信息将发送到正确的接收方。您可以在反向代理中使用客户机验证来确保，内容服务器不会与未经授权的代理或客户机共享信息。

本节包含以下主题：

- 第 95 页中的 “将客户机证书映射到 LDAP”
- 第 96 页中的 “使用 certmap.conf 文件”

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，将需要客户机证书，然后服务器才将响应发送给查询。

Proxy Server 支持通过将客户机证书中的 CA 与签名客户机证书时信任的 CA 相匹配，来验证客户机证书。您可以通过 "Security" 选项卡的 "Manage Certificates" 页面查看用于客户机证书签名的受信任 CA 列表。

您可以对 Proxy Server 进行配置，以拒绝不具有来自受信任 CA 的客户机证书的任何客户机。要接受或拒绝受信任的 CA，必须对 CA 设置客户机信任。有关更多信息，请参见第 78 页中的 “管理证书”。

如果证书已到期，Proxy Server 将记录错误、拒绝证书并向客户机返回一条消息。也可以在 "Manage Certificates" 页面上查看已到期的证书。

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。此过程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。要了解如何执行此操作，请参见第 95 页中的 “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，以便除了来自受信任的 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，请参见第 136 页中的 “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. **单击将要求客户机验证的侦听套接字的链接。**
4. **使用 "Client Authentication" 下拉式列表要求对侦听套接字进行客户机验证，然后单击 "OK"。**

反向代理中的客户机验证

在反向代理中，可以根据以下任何方案配置客户机验证：

- **代理验证客户机**。通过此方案，可允许具有可接受证书的所有客户机的访问，或者仅允许不但具有可接受证书，而且在 Proxy Server 的访问控制列表中为可识别用户的那些客户机的访问。

注 – 代理必须具有 CA 的用户根密钥，或者已签署了用户证书的自签署应用程序。用户必须具有已加载的 CA 的 Proxy Server 根密钥，或者已签署 Proxy Server 证书的自签署应用程序。

- **内容服务器验证代理服务器**。通过此方案，可确保内容服务器实际与 Proxy Server 建立连接而不是其他某个服务器。

注 – 代理服务器必须具有 CA 的内容服务器根密钥，或者已签署内容服务器证书的自签署应用程序。内容服务器必须具有 CA 的 Proxy Server 根密钥，或者已签署 Proxy Server 证书的自签署应用程序。

- **代理服务器验证客户机且内容服务器验证代理服务器**。此方案为反向代理提供最可靠的安全性和验证。

有关如何配置这些方案的信息，请参见第 93 页中的 “在反向代理中设置客户机验证”。

在反向代理中设置客户机验证

安全反向代理中的客户机验证为连接安全提供了进一步的保证。以下说明解释了如何根据所选择的方案配置客户机验证。

注 – 每种方案都假定，您既具有客户机到代理的安全连接，也具有代理到内容服务器的安全连接。

▼ 配置 “ 代理服务器验证客户机 ” 方案

1. **请遵循第 14 章的 “ 设置反向代理 ” 一节中有关配置客户机到代理的安全和代理到内容服务器的安全方案的说明。**
2. **访问服务器实例的 Server Manager 并单击 "Preferences" 选项卡。**
3. **单击 "Edit Listen Sockets" 链接，然后单击所显示表中需要的侦听套接字的链接。**
   （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：**

a. **允许具有有效证书的所有用户的访问：**

在 "Security" 部分中，使用 "Client Authentication" 设置要求对此侦听套接字进行客户机验证。如果尚未安装服务器证书，此设置将不可见。

b. **仅允许不但具有有效证书，而且还在访问控制中被指定为可接受用户的那些用户的访问：**

i. **在 "Security" 部分中，将 "Client Authentication" 设置保留为关闭状态。如果尚未安装服务器证书，此设置将不可见。**

ii. **在此服务器实例的 Server Manager "Preferences" 选项卡中，单击 "Administer Access Control" 链接。**

iii. **选择一个 ACL，然后单击 "Edit" 按钮。**

此时将显示 "Access Control Rules For" 页面（如果出现提示，将首先验证）。

iv. **打开访问控制（如果未选中 "Access control Is On" 复选框，请将其选中）。**

v. **将 Proxy Server 设置为作为反向代理进行验证。**

有关更多信息，请参见第 281 页中的 “设置反向代理”。

vi. **单击所需访问控制规则的 "Rights" 链接，在下面的框架中指定访问权限，然后单击 "Update" 以更新该条目。**

vii. **单击 "Users/Groups" 链接。在下面的框架中，指定用户和组，选择 SSL 作为验证方法，然后单击 "Update" 以更新该条目。**

viii. **在上面的框架中，单击 "Submit" 以保存条目。**

有关设置访问控制的更多信息，请参见第 8 章。

▼ 配置 “内容服务器验证代理服务器” 方案

1 **请遵循第 281 页中的 “设置反向代理”中有关配置客户机到代理服务器的安全和代理服务器到内容服务器的安全方案的说明。**

2 **在内容服务器中，打开客户机验证。**

您可以修改此方案，以便与 Proxy Server 进行不安全客户机连接，与内容服务器进行安全连接，并使内容服务器验证 Proxy Server。为此，必须关闭加密功能，并要求代理仅按以下步骤中所述来初始化证书。

▼ 配置“代理验证客户机且内容服务器验证代理”方案

1 **请遵循第 93 页中的“配置“代理服务器验证客户机”方案”中有关配置“代理服务器验证客户机”方案的说明。**

2 **在内容服务器中，打开客户机验证。**

将客户机证书映射到 LDAP

本节介绍 Proxy Server 用来将客户机证书映射到 LDAP 目录中的条目的过程。在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，请参见第 8 章。

服务器收到客户机的请求后，将在处理请求之前要求提供客户机的证书。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。

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。如果不存在匹配条目，Proxy Server 将结束连接。如果存在匹配条目，服务器将继续处理请求。

验证证书是来自受信任的 CA 之后，服务器会通过以下方式将证书映射到 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` 的证书映射文件确定如何执行 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。

服务器了解了开始搜索的位置和要搜索的内容之后，将在 LDAP 目录中执行搜索（第二步）。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。

下表列出了期望的搜索结果行为。您可以在 ACL 中指定期望的行为。例如，可以指定，如果证书匹配失败，Proxy Server 将仅接受您。有关如何设置 ACL 首选项的更多信息，请参见第 136 页中的 “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
恰好找到一个条目	验证失败	验证成功

表 5–1 LDAP 搜索结果 （续）

LDAP 搜索结果	证书验证打开	证书验证关闭
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，就可以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 文件配置证书（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，以匹配 LDAP 目录的组织和列出您希望用户拥有的证书。用户可以基于 subjectDN 中使用的用户 ID、电子邮件地址或任何其他值进行身份验证。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 目录中搜索条目时，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

可在以下位置中找到证书映射文件：

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。映射具有以下语法：

certmap *name issuerDNname* :*property* [*value*]

第一行用于指定条目的名称以及形成 CA 证书中标识名的属性。*name* 是任意的，可以根据自己的喜好进行定义。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，以下两个颁发者 DN 行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=UScertmap sun2 ou=Sun
Certificate Authority, o=Sun, c=US
```

注 – 如果使用的是 Sun Java System Directory Server 并在匹配颁发者 DN 时遇到问题，请检查 Directory Server 错误日志中是否存在有用的信息。

已命名的映射中的第二行和随后的行将属性与值相匹配。certmap.conf 文件具有六个默认属性。您也可以使用证书 API 自定义属性。默认属性包括：

- DNComps 是一系列以逗号分隔的属性，用于确定服务器从 LDAP 目录的哪个位置开始搜索匹配用户（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其搜索。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* 将替换为证书中 DN 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 树中搜索匹配过滤器的条目。

  FilterComps 是一系列逗号分隔的属性，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，这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 FilterComps 被设置为使用电子邮件地址和用户 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，因为它们在目录中通常是唯一的。过滤器必须非常具体，以仅仅匹配 LDAP 数据库中的某一条目。

  过滤器的属性名称必须是来自证书（而不是来自 LDAP 目录）的属性名称。例如，某些证书将 e 属性用于用户的电子邮件地址，而 LDAP 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	描述
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，客户机的证书是否应与在 LDAP 目录中找到的证书进行比较。该属性具有两个值：on 和 off。只有 LDAP 目录包含证书时，才应使用该属性。此功能有助于确保最终用户使用的证书有效且未被撤销。
- `CmapLdapAttr` 是 LDAP 目录中的属性名称，该名称包含属于该用户的所有证书的主题 DN。该属性的默认值是 `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，请参见《Introduction to SSL》。

  如果 `certmap.conf` 文件中存在此属性，服务器将在整个 LDAP 目录中搜索其特性（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。如果没有找到任何条目，服务器将会使用 `DNComps` 和 `FilterComps` 映射重新进行搜索。

  在使用 `DNComps` 和 `FilterComps` 匹配条目比较困难时，这种将证书与 LDAP 条目相匹配的方法非常有用。
- `Library` 是共享库或 DLL 的路径名。只有使用证书 API 创建自己的属性时，才可以使用此属性。
- `InitFn` 是自定义库中 `init` 函数的名称。只有使用证书 API 创建自己的属性时，才可以使用此属性。

有关这些属性的更多信息，请参阅第 98 页中的 “映射样例”中所述的示例。

创建自定义特性

客户机证书 API 可用于创建自己的属性。创建自定义映射后，就可以按照如下所示引用该映射：

name`:library` *path_to_shared_libraryname* `: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` 文件应至少包含一个条目。以下示例说明了 `certmap.conf` 的不同使用方法。

示例 #1 仅带有一个默认映射的 `certmap.conf` 文件

```
certmap default defaultdefault:DNComps ou, o, cdefault:FilterComps e,
uiddefault:verifycert on
```

使用本示例，服务器可以在包含 `ou=`*orgunit*, `o=`*org*, `c=`*country* 条目的 LDAP 分支点处开始搜索，其中斜体文本将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 带有两个映射的 certmap.conf 文件

以下示例文件中包括两个映射：一个是默认映射，另一个用于美国邮政总局 (US Postal Service)。

```
certmap default defaultdefault:DNCompsdefault:FilterComps e, uid

certmap usps ou=United States Postal Service, o=usps, c=USusps:DNComps
ou,o,cusps:FilterComps eusps:verifycert on
```

如果服务器收到的证书来自美国邮电总局以外的其他用户，服务器将使用默认映射，即从 LDAP 树的顶端启动并搜索与客户机电子邮件和用户 ID 相匹配的条目。如果证书来自美国邮电总局，服务器将从包含组织单位的 LDAP 分支启动并搜索匹配的电子邮件地址。服务器还将验证该证书。其他证书不会进行验证。

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 DN 的 `o` 和 `c` 属性之间没有空格。

示例 #3 搜索 LDAP 数据库

以下示例使用 `CmapLdapAttr` 属性在 LDAP 数据库中搜索名为 `certSubjectDN` 的属性，该属性的值与从客户机证书获取的整个主题 DN 完全匹配。本示例假定 LDAP 目录中包含带有 `certSubjectDN` 属性的条目。

```
certmap myco ou=My Company Inc, o=myco, c=USmyco:CmapLdapAttr
certSubjectDNmyco: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，服务器将使用 `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`。

设置更强大的加密算法

Server Manager 的 "Preferences" 选项卡中的 "Set Cipher Size" 选项为访问提供了 168 位、128 位或 56 位的密钥大小，或者无限制。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。

如果选择的用于访问的密钥大小与 "Security Preference" 下的当前加密算法设置不一致，Proxy Server 将显示一条警告，指出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* 是密钥中所需的最小位数，*filename* 是不符合限制条件时使用的文件的名称。

如果未启用 SSL，或者如果未指定 `secret-keysize` 参数，`PathCheck` 将返回 `REQ_NOACTION`。如果当前会话的密钥大小小于所指定的 `secret-keysize`，该函数将返回 `REQ_ABORTED`，如果未指定 `bong-file` 文件，将返回状态 `PROTOCOL_FORBIDDEN`。如果指定了 `bong-file`，该函数将返回 `REQ_PROCEED`，且路径变量将被设置为 `bong-file` *filename*。而且，如果不符合密钥大小限制条件，当前会话的 SSL 会话高速缓存条目将失效，因此下次当同一台客户机连接到服务器时，将发生完整的 SSL 握手。

注 – 添加了 `PathCheck fn=ssl-check` 后，"Set Cipher Size" 表单将会删除对象中发现的所有 `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 并单击 "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的加密算法的资源，然后单击 "Select"。也可以指定一个正则表达式。**

   有关更多信息，请参见第 16 章。
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 **指定用于拒绝访问的消息的文件位置，并单击 "OK"。**

有关加密算法的更多信息，请参见Introduction to SSL。

其他安全性注意事项

除了有人会尝试破坏加密之外，还存在其他安全性风险。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功能，还应采取额外的安全性预防措施。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个人将程序上载到您的服务器中。本节介绍使服务器更安全的一些重要内容。

本节包含以下主题：

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，只有授权的用户才能进入该房间。此策略可防止任何人攻击服务器计算机本身。而且，要保护好计算机的管理（根）密码（如果有）。

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。如果想要 Administration Server 为最终用户提供对 LDAP 服务器或本地目录信息的访问，请考虑维护两个 Administration Server 并使用群集管理。这样，启用了 SSL 的 Administration Server 将充当主服务器，另一个 Administration Server 供最终用户访问。有关群集的更多信息，请参见第 6 章。

您还应为 Administration Server 打开加密功能。如果未将 SSL 连接用于管理，那么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密码并重新配置您的服务器。

选择强密码

您可以在服务器中使用多个密码：管理密码、私钥密码、数据库密码等等。管理密码是最重要的密码，因为持有该密码的用户可以在您的计算机上配置任何服务器。私钥密码是第二重要的密码。拥有您的私钥和私钥密码的任何用户都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。

密码最好便于您自己记忆，别人又无法猜到。例如，可以将 *MCi12!mo* 记成 "My Child is 12 months old!"。不要使用孩子的姓名或生日作为密码。

创建难以破解的密码

遵循以下准则创建更强的密码。不必将以下所有规则都用于一个密码，但使用的规则越多，密码就越难以猜到。一些提示：

- 密码长度应为 6-14 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

更改密码或 PIN

请定期更改信任数据库/密钥对文件密码或 PIN。如果 Administration Server 中启用了 SSL，启动服务器时将需要此密码。定期更改密码可以增加对服务器的额外保护。

只能在本地计算机上更改此密码。有关更改密码时应考虑的准则列表，请参见第 102 页中的 “创建难以破解的密码” 。

▼ 更改信任数据库/密钥对文件密码

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，选择要更改密码的安全令牌。**
   默认情况下，内部密钥数据库的安全令牌为内部。如果安装了 PKCS #11 模块，将会列出了所有安全令牌。

4. **键入当前密码。**
5. **键入新密码。**
6. **再次键入新密码，然后单击 "OK"。**

   确保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。

   确定备份磁带中是否存储了该文件，以及是否可能会被某些人截取。如果存储了该文件，必须像保护服务器一样尽力保护您的备份。

限制服务器上的其他应用程序

所有应用程序都在作为服务器的同一台计算机上运行时需要格外小心。某些人可能会利用服务器上运行的其他程序中的漏洞来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 守护程序的安全难以配置，因此也就可以对其进行编程，以在服务器计算机上运行其他可能有危害的程序。

UNIX 和 Linux

小心选择从 inittab 和 rc 脚本启动的进程。请不要从服务器计算机中运行 telnet 或 rlogin。另外，服务器计算机上也不应包含 rdist。这可以分布文件，但也用于更新服务器计算机上的文件。

Windows

与其他计算机共享驱动器和目录时要格外小心。而且，要考虑哪些用户具有帐户或 guest 权限。在服务器上安装程序或者允许其他用户安装程序时要格外小心。其他用户的程序可能会存在安全漏洞。更糟糕的是，有人可能会上载怀有恶意的程序，目的就是破坏您的安全性。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。

禁止客户机高速缓存 SSL 文件

通过在 HTML 文件的 <HEAD> 部分中添加以下行，可以禁止客户机对预加密的文件进行高速缓存。

```
<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绝对最小端口集以外的任何端口的传入连接。此保护意味着，获取计算机中 shell 的唯一方法是实际使用服务器，该服务器应已放置在受限制的区域中。

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？请务必确保客户机通过 SSL 发送给您的所有信息的安全性。

◆ ◆ ◆ 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，并介绍如何使用群集在服务器之间共享配置。

本章包含以下各节：

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。每个群集必须包含一个指定为主 Administration Server 的服务器。

通过将服务器组织成群集，可以执行以下操作：

- 创建一个中心位置来管理所有 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 来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

使用群集的准则

请遵循以下准则将 Proxy Server 组配置成群集：

- 在创建任何群集之前，必须先安装要包含在特定群集中的所有服务器。
- 群集中所有服务器的类型必须相同（UNIX 或 Windows）。群集必须是同构的。
- 群集中的所有服务器都必须为 Proxy Server 版本 4。仅支持将 Proxy Server 版本 4 添加到群集中。
- 所有 Administration Server 必须使用相同的协议（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，请参第 108 页中的 “修改服务器信息”。
- 所有特定于群集的 Administration Server 的用户名和密码必须与主 Administration Server 的用户名和密码相同。可以使用分布式管理在每个 Administration Server 上配置多个管理员。
- 必须将一个特定于群集的 Administration Server 指定为主 Administration Server，选择哪个服务器无关紧要。
- 主 Administration Server 必须能够访问每个特定于群集的 Administration Server。主 Administration Server 将检索安装的所有 Sun Java System Web Proxy Server 的相关信息。

设置群集

以下是设置 Proxy Server 群集的一般步骤。

1. 安装要包含在群集中的 Proxy Server。

   确保主 Administration Server 可以使用该群集的 Administration Server 的用户名和密码进行验证。可以通过使用默认的用户名和密码或配置分布式管理来实现此目的。
2. 安装将包含主 Administration Server 的 Proxy Server，确保用户名和密码与步骤 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，请参见第 107 页中的 “将服务器添加到群集中”。
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。

将服务器添加到群集中

将 Proxy Server 添加到群集后，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。

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。

▼ 将远程服务器添加到群集中

1 **确保主 Administration Server 已打开。**

2 **访问主 Administration Server 并单击 "Cluster" 选项卡。**

3 **单击 "Add Server" 链接。**

4 **选择远程 Administration Server 使用的协议：**

- HTTP 用于普通的 Administration Server
- HTTPS 用于安全的 Administration Server

5 **键入 `magnus.conf` 文件中所显示的远程 Administration Server 的全限定主机名，例如 `plaza.example.com`。**

6 **键入远程 Administration Server 的端口号。**

7 **键入远程 Administration Server 的管理员用户名和密码，然后单击 "OK"。**

主 Administration Server 将尝试与远程服务器联系。如果联系成功，系统将提示您确认是否将服务器添加到群集中。

注 – 启用群集控制时，群集的主服务器将在 `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。如果更改群集中某个远程 Administration Server 的端口号，还必须修改存储在群集中的该 Administration Server 的信息。对从属 Administration Server 进行任何其他更改都要求先删除该服务器，然后进行更改，完成更改后再将其重新添加到群集中。

▼ 修改群集中服务器的信息

1. **访问主 Administration Server 并单击 "Cluster" 选项卡。**
2. **单击 "Modify Server" 链接。将显示按唯一服务器标识符列出的服务器。**
3. **选择要修改的服务器并进行所需的更改，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 并单击 "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并单击 "OK"。**

   无法再通过群集访问已删除的服务器，只能通过它自己的 Administration Server 进行访问。

控制服务器群集

使用 Proxy Server，您可以通过以下操作控制群集中的远程服务器：

- 启动和停止服务器。
- 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 具有多个 Proxy Server 实例，则可以将文件从其中任何一个服务器传送到已添加到群集中的任何从属服务器。群集必须是同构的。群集中所有服务器的类型必须相同（UNIX 或 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。配置文件包括：

- 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 并单击 "Cluster" 选项卡。**

2 **单击 "Control Cluster" 链接。**

3 **选择要控制的服务器并进行所需的选择。**

可随时单击 "Reset" 按钮将元素重置为进行任何更改之前它们所包含的值。

- 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行中最后一行的行号。单击 "Go" 以显示信息。在所显示的 "Cluster Execution Report" 中，单击 "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" 以传送信息

◆ ◆ ◆ 第 7 章

7 配置服务器首选项

本章介绍 Proxy Server 的系统设置及其配置方法。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和所侦听的端口等选项。

本章包含以下各节：

启动 Proxy Server

本节介绍如何在不同平台上启动 Proxy Server。安装该服务器后，它便会侦听并接受请求。

▼ 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。**
此时将显示 "Start/Stop Server" 页面。

3 **单击 "On" 按钮。**
"Start/Stop Server" 页面中将会显示服务器的状态。

在 UNIX 或 Linux 上启动 Proxy Server

您可以采用以下两种方式之一在 UNIX 或 Linux 上启动 Proxy Server :

- 从命令行转到 *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 start 命令 `prxy:2:respawn:`*server-root*`/proxy-server`*id*`/start -start -i`。

在 Windows 上启动 Proxy Server

您可以采用以下任何一种方式在 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”。
- 从命令提示符转到 *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，需要提供密码。尽管可以通过将密码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，但这样将会存在很大的安全风险。任何可以访问该文件的用户都有权访问启用了 SSL 的服务器的密码。在将启用了 SSL 的服务器的密码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、密钥对文件和密钥密码应归 root 用户所有，或者属于安装了服务器的非 root 用户的用户帐户，并且只有所有者才拥有对它们的读写权限。

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。**
此时将显示 "Start/Stop Server" 页面。

3 **单击 "Off" 按钮。**
"Start/Stop Server" 页面中将会显示服务器的状态。

在 UNIX 或 Linux 上停止 Proxy Server

您可以采用以下两种方式之一在 UNIX 或 Linux 上停止 Proxy Server：

- 从命令行转到 *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` 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` 文件设置为使用 `respawn` 自动重新启动，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，服务器将会停止并且其正在处理的任何请求都可能会丢失。

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提供相应的密码。

在 Windows 上停止 Proxy Server

您可以采用以下任何一种方式在 Windows 上停止 Proxy Server：

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

- 从命令提示符转到 *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 UNIX 或 Linux 服务器

您可以使用以下方法之一重新启动服务器：

- 手动重新启动服务器。
- 自动从 inittab 文件重新启动服务器。

  如果所使用的 UNIX 或 Linux 版本不是源自 System V（如 SunOS™ 4.1.3），则无法使用 inittab 文件。
- 系统重新引导时，使用 /etc/rc2.d 中的守护程序自动重新启动服务器。

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小于 1024 的端口上运行，请以 root 用户身份登录；否则以 root 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。此选项还可以防止服务器将其自身置于后台进程。

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-serverid/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 选项可以防止服务器将其自身置于后台进程。

在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 Windows 服务器

您可以通过服务控制面板或通过完成以下任务来重新启动服务器。

▼ 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”。这样，每次启动或重新引导计算机时，系统将会启动服务器。**
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，而是等待所有未完成的连接完成。在 magnus.conf 文件中，可以配置服务器超时前的等待时间。默认情况下，此值设置为 30 秒。要更改此值，请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需的时间。

查看服务器设置

在安装过程中，您可以为 Proxy Server 配置某些设置。通过 Server Manager 可以查看这些设置以及其他系统设置。"View Server Settings" 页面将列出 Proxy Server 的所有设置。此页面还会指示是否有未保存和未应用的更改。如果有未保存的更改，请保存更改并重新启动 Proxy Server，以便开始使用新配置。

服务器设置有两种类型：技术设置和内容设置。服务器的内容设置取决于如何配置服务器。通常，代理会列出所有模板、URL 映射和访问控制。对于单个模板，"View Server Settings" 页面将列出模板名称、模板的正则表达式以及模板设置（如高速缓存设置）。

代理服务器的技术设置来自 `magnus.conf` 文件和 `server.xml` 文件，内容设置来自 `obj.conf` 文件。这些文件位于服务器根目录下的 `proxy-`*`id`*`/config` 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。**
   此时将显示 "View Server Settings" 页面。

查看和恢复配置文件的备份

您可以查看或恢复以下配置文件的备份副本：`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`。通过此功能，可在当前配置出现问题时恢复到以前的配置。例如，如果在对代理配置进行若干更改后，代理并未按预期的方式工作（例如，您拒绝了对某个 URL 的访问，但代理却仍为该请求提供服务），则可恢复到以前的配置，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。**
   此时将显示 "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。**
   此时将显示 "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。**
   如果要将所有文件都恢复到某个特定时间的状态，请单击表中左列的 "Restore to *time*" 链接。*time* 为要恢复到的日期和时间。

▼ 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。**
   此时将显示 "Restore Configuration" 页面。
3. **在 "Set Number Of Sets Of Backups" 字段中，键入要显示的备份数量。**
4. **单击 "Change" 按钮。**

配置系统首选项

"Configure System Preferences" 页面用于设置或更改服务器的基本特征。通过该页面，可以执行以下操作：

- 更改服务器用户、进程数、侦听队列大小、代理超时以及代理服务器中断之后的超时
- 启用 DNS、ICP、代理阵列和父阵列

首选项选项包括：

- **Server User**。"Server User" 是代理使用的用户帐户。您输入的作为代理服务器用户的用户名应该已经存在，并且是一个标准的用户帐户。服务器启动时，其运行情况如同由此用户启动一样。

  如果要避免创建新的用户帐户，可以选择在同一主机上运行的其他服务器所使用的帐户，或者如果运行的是 UNIX 代理，则可选择用户 nobody。但是在某些系统上，用户 nobody 可以拥有文件却不能运行程序，因而不适合用作代理用户名。

  在 UNIX 系统上，代理产生的所有进程都被分配给服务器用户帐户。

- **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 (Domain Name Service, 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，可以指示服务器是否将 IP 地址解析为主机名。
- **ICP**。Internet 高速缓存协议 (Internet Cache Protocol, ICP) 是一种消息传递协议，该协议可以使高速缓存相互通信。高速缓存可使用 ICP 来发送有关高速缓存的 URL 是否存在，以及这些 URL 的最佳检索位置的查询和回复。可以在 "Configure System Preferences" 页面上启用 ICP。有关 ICP 的更多信息，请参见第 245 页中的 “通过 ICP 邻域进行路由选择”。
- **Proxy Array**。代理阵列是作为一个高速缓存使用的由多个代理组成的阵列，其目的是实现分布式高速缓存。如果在 "Configure System Preferences" 页面中启用代理阵列选项，则意味着配置的代理服务器是某代理阵列的成员，而且该阵列中的所有其他成员都是其同级服务器。有关使用代理阵列的更多信息，请参见第 252 页中的 “通过代理服务器阵列进行路由选择”。
- **Parent Array**。父阵列是代理或代理阵列成员路由经过的代理阵列。因此，如果代理在访问远程服务器之前路由经过某个上游代理阵列，则该上游代理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，请参见第 263 页中的 “通过父阵列进行路由选择”。
- **Proxy Timeout**。代理超时是指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之间的最大时间间隔。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，向代理发送多个请求。

▼ 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。**
   此时将显示 "Configure System Preferences" 页面。
3. **根据需要更改选项，然后单击 "OK"。**
4. **单击 "Restart Required"。**
   此时将显示 "Apply Changes" 页面。

5 **单击 "Restart Proxy Server" 按钮应用更改。**

调节 Proxy Server

通过 "Tune Proxy" 页面，可以更改默认参数以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。**
此时将显示 "Tune Proxy" 页面。

3 **（可选）修改 FTP 列表的宽度以允许更长的文件名，从而减少文件名截断。**
默认宽度为 80 个字符。

4 **单击 "OK"。**

5 **单击 "Restart Required"。**
此时将显示 "Apply Changes" 页面。

6 **单击 "Restart Proxy Server" 按钮应用更改。**

添加和编辑侦听套接字

服务器在处理请求之前，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`，以及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。

- **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。此地址可以采用点分对或 IPv6 表示法来表示。此外，也可以是 `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。允许的值为 1-65535。在 UNIX 上，创建在端口 1-1024 上侦听的套接字需要超级用户权限。请将 SSL 侦听套接字配置为在端口 443 上侦听。
  - **Server Name**。此侦听套接字的默认服务器。

  Security

如果禁用安全性，将仅显示以下参数：

- **Security**。启用或禁用选定侦听套接字的安全性。

如果启用安全性，则显示以下参数：

- **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要用于此侦听套接字的已安装证书。
  - **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，此设置为 "Optional"。
  - **SSL Version 2**。启用或禁用 SSL 版本 2。默认情况下禁用此设置。
  - **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**。Enables or disables SSL Version 3. This setting is enabled by default.
  - **TLS**。启用或禁用 TLS，即用于加密通信的传输层安全协议。默认情况下启用此设置。
  - **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。默认情况下启用此设置。
  - **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。该值范围是 1-1024。

    Protocol Family。套接字系列类型。允许的值为 `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。

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

只有安装所需证书后，侦听套接字的安全性才会将 "Enabled" 作为选项，而在此之前该下拉框中仅显示 "Disabled" 选项。

本节包含以下主题：

- 第 93 页中的 “配置“代理服务器验证客户机”方案”
- 第 94 页中的 “配置“内容服务器验证代理服务器”方案”
- 第 95 页中的 “配置“代理验证客户机且内容服务器验证代理”方案”

▼ 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。**
   此时将显示 "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 地址可以采用点分对或 IPv6 表示法来表示。此外，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。允许的值为 `1 - 65535`。**
   在 UNIX 上，创建在端口 1 - 1024 上侦听的套接字需要超级用户权限。请将 SSL 侦听套接字配置为在端口 443 上侦听。
6. **指定要在由服务器发送至客户机的任何 URL 的主机名部分中使用的服务器名称。**
   此设置将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，指定是否应为侦听套接字启用或禁用安全性。**
8. **单击 "OK"。**
9. **单击 "Restart Required"。**
   此时将显示 "Apply Changes" 页面。
10. **单击 "Restart Proxy Server" 按钮应用更改。**

▼ 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。**
   此时将显示 "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。**
   此时将显示 "Edit Listen Sockets" 页面。

4. **对各选项进行所需更改。**
   有关各选项的说明，请参见本节开始部分。
5. **单击 "OK"。**
6. **单击 "Restart Required"。**
   此时将显示 "Apply Changes" 页面。
7. **单击 "Restart Proxy Server" 按钮应用更改。**

▼ 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. **选中要删除的侦听套接字旁边的复选框，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"。**
   此时将显示 "Apply Changes" 页面。
5. **单击 "Restart Proxy Server" 按钮应用更改。**

选择目录服务

"Select Directory Services" 页面列出了指定代理服务器实例的所有目录服务。通过该页面，可以选择要用于特定代理服务器实例的目录服务。有关更多信息，请参见第 45 页中的 “配置目录服务”。

▼ 选择目录服务

1. **访问 Server Manager 并单击 "Preferences" 选项卡。**
2. **单击 "Select Directory Services" 链接。**
   此时将显示 "Select Directory Services" 页面，其中列出了指定代理服务器实例的所有目录服务。
3. **从列表中选择目录服务。**

4. **单击 "OK"。**

5. **单击 "Restart Required"。**
   此时将显示 "Apply Changes" 页面。

MIME 类型

多用途 Internet 邮件扩展 (Multi-purpose Internet Mail Extension, MIME) 类型是多媒体电子邮件和消息传递的一种标准。为了能够根据文件的 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。代理会将新类型添加到 `mime.types` 文件中。有关根据 MIME 类型阻止文件的更多信息，请参见第 273 页中的 “按 MIME 类型过滤” 。

本节介绍如何创建、编辑或删除 MIME 类型。

创建 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。**
   此时将显示 "Create/Edit MIME Types" 页面，其中列出了代理的 `mime.types` 文件中所列的所有 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`。`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，请参见联机帮助。

4. **指定将出现在 HTTP 标头中的内容类型。**

5. **指定文件后缀。**
   “文件后缀” 是指映射到 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

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" 页面将显示代理的 `mime.types` 文件中列出的所有 MIME 类型。
3. **单击要编辑的 MIME 类型的 "Edit" 链接。**
4. **进行所需的更改。单击 "Change MIME Type" 按钮。**

▼ 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" 页面将显示代理的 `mime.types` 文件中列出的所有 MIME 类型。
3. **单击要删除的 MIME 类型的 "Remove" 链接。**

管理访问控制

"Administer Access Control" 页面用于管理访问控制列表 (access control list, ACL)。ACL 使您可以控制哪些客户机可以访问您的服务器。ACL 可以筛选出某些用户、组或主机，以允许或拒绝对服务器部分内容的访问。ACL 还可以设置验证，以便仅有效用户和组才能访问服务器的部分内容。有关访问控制的更多信息，请参见第 8 章。

▼ 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。**
   此时将显示 "Administer Access Control" 页面。
3. **选择一个资源或现有 ACL，或者键入 ACL 名称，然后单击 "Edit" 按钮。**
   此时将显示 "Access Control Rules for" 页面。

4 **进行所需的更改并单击 "Submit"。**

有关访问控制的更多信息，请参见第 8 章中的“设置服务器实例的访问控制”。

配置 ACL 高速缓存

"Configure ACL Cach" 页面用于启用或禁用代理验证高速缓存、设置代理验证高速缓存目录、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。**

此时将显示 "Configure ACL Cache" 页面。

3 **启用或禁用代理验证高速缓存。**

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，都将对照此值计算并检查其期限。如果其期限大于或等于 "Proxy Auth Cache Expiration" 值，则不使用该条目。如果将此值设置为 0，将会关闭高速缓存。

如果将其设置为一个较大的值，则更改 LDAP 条目后，可能需要重新启动 Proxy Server。例如，如果将此值设置为 120 秒，则在长达 2 分钟的时间内，Proxy Server 可能会与 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。默认到期值为 2 分钟。

7 **单击 "OK"。**

8 **单击 "Restart Required"。**

此时将显示 "Apply Changes" 页面。

9 **单击 "Restart Proxy Server" 按钮应用更改。**

了解 DNS 高速缓存

Proxy Server 支持 DNS 高速缓存，以减少代理在将 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。**
   此时将显示 "Configure DNS Cache" 页面。
3. **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. **设置 DNS 高速缓存到期时间。**
   在 DNS 高速缓存条目到达预设的到期时间后，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. **启用或禁用在未找到主机名时对错误进行高速缓存。**
7. **单击 "OK"。**
8. **单击 "Restart Required"。**
   此时将显示 "Apply Changes" 页面。
9. **单击 "Restart Proxy Server" 按钮应用更改。**

配置 DNS 子域

某些 URL 包含的主机名带有多级子域。如果第一个 DNS 服务器无法解析主机名，代理服务器可能需要很长时间来进行 DNS 检查。您可以设置 Proxy Server 在将 "host not found" 消息返回客户机之前要检查的级别数。

例如，如果客户机请求 `http://www.sj.ca.example.com/index.html`，代理将需要很长时间将该主机解析为 IP 地址，因为代理可能必须经过四个 DNS 服务器，才能获取主机的 IP 地址。由于这些查找可能需要很长时间，因此可以配置代理服务器，使其在必须使用某个数量以上的 DNS 服务器时，放弃查找 IP 地址。

▼ 设置代理查找的子域级别

1. **访问 Server Manager 并单击 "Preferences" 选项卡。**
2. **单击 "Configure DNS Subdomains" 链接。**
   此时将显示 "Configure DNS Subdomains" 页面。
3. **从下拉式列表中选择资源，或指定正则表达式。**
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"。**
   此时将显示 "Apply Changes" 页面。
7. **单击 "Restart Proxy Server" 按钮应用更改。**

配置 HTTP 保持活动功能

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

保持活动功能是一种 TCP/IP 功能，用于使连接在完成请求后保持打开状态，以便客户机可以快速重新使用打开的连接。默认情况下，代理不会使用保持活动连接。但对于某些系统，使用保持活动功能可以提高代理的性能。

在标准的基于 Web 的客户机/服务器事务中，客户机可与服务器建立若干连接以请求多个文档。例如，如果客户机请求的 Web 页中包含多个图形图像，则客户机需要针对每个图形文件分别发出请求。重新建立连接是很费时的。因此，保持活动包可能很有用。

▼ 配置 HTTP 保持活动功能

1. **访问 Server Manager 并单击 "Preferences" 选项卡。**
2. **单击 "Configure HTTP Client" 链接。**
   此时将显示 "Configure HTTP Client" 页面。
3. **从下拉式列表中选择资源。**
   选择 HTTP 或 HTTPS 资源以在 Proxy Server 上配置保持活动功能，或指定正则表达式。
4. **选择相应的 "Keep Alive" 选项，以指定 HTTP 客户机是否应使用持久性连接。**
5. **在 "Keep Alive Timeout" 字段中，指定使持久性连接保持打开状态的最大秒数。**
   默认值为 29。
6. **选择相应的 "Persistent Connection Reuse" 选项，以指定 HTTP 客户机是否可对所有类型的请求重新使用现有持久性连接。**
   默认值为 "off"，即不允许对非 GET 请求和含有主体的请求重新使用持久性连接。
7. **在 "HTTP Version String" 字段中，指定 HTTP 协议版本字符串。**
   除非遇到特定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 产品名称和版本。**
9. **在 "SSL Client Certificate Nickname" 字段中，指定要提供给远程服务器的客户机证书昵称。**
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"。**
    此时将显示 "Apply Changes" 页面。
13. **单击 "Restart Proxy Server" 按钮应用更改。**

◆ ◆ ◆ 第 8 章

8 控制对服务器的访问

本章介绍如何控制对 Administration Server 以及 Proxy Server 所处理数据的访问。可以限制对服务器使用的所有数据或其使用的特定 URL 的访问。例如，可以指定只有特定用户可访问特定的 URL，或者指定除这些用户之外的任何用户均可查看文件。您可以允许所有客户机均可访问 HTTP 的 URL，但是只允许对 FTP 进行受限访问。您还可以基于主机名或域名来限制访问 URL，例如您有一个为许多内部 Web 服务器提供服务的 Proxy Server，但是仅希望特定的人员访问其中一台服务器中存储的保密性研究项目。

对 Administration Server 使用访问控制之前，必须启用分布式管理并在 LDAP 数据库中配置一个管理组。本章中的信息是在假设这些任务均已执行的情况下提供的。

本章包含以下各节：

什么是访问控制？

通过访问控制，可以确定何人可访问 Proxy Server 以及他们可访问服务器的哪些部分。您可以控制对整个服务器或仅对服务器各部分（例如目录、文件、文件类型等）的访问。评估传入的请求时，将根据称为访问控制条目 (Access Control Entries, ACE) 的分层结构规则确定访问权限。Proxy Server 将查找匹配的条目以确定应当授予还是拒绝访问权限。每个 ACE 都指定了服务器是否应当继续检查分层结构中的下一个条目。该 ACE 集合称为访问控制列表 (Access Control List, ACL)。收到请求时，将检查 `obj.conf` 文件以查看是否引用了随后用于确定访问权限的 ACL。默认情况下，服务器具有一个 ACL 文件，其中包含多个 ACL。

根据以下各项来允许或拒绝访问：

- 谁在进行请求（用户/组）
- 请求来自何处（主机/IP）
- 请求发生的时间（例如一天中的某个时间）
- 使用的连接类型 (SSL)

本节包含以下主题：

- 第 130 页中的 “用户/组的访问控制”
- 第 136 页中的 “主机/IP 的访问控制”
- 第 136 页中的 “使用访问控制文件”
- 第 137 页中的 “配置 ACL 用户高速缓存”
- 第 137 页中的 “使用客户机证书控制访问”

用户/组的访问控制

您可以仅允许特定的用户或组访问您的服务器。用户/组访问控制要求用户提供用户名和密码，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一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，请参见第 45 页中的 “配置目录服务”。

目录服务用来实现访问控制的信息可能来自以下来源之一：

- 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，对于服务器实例而言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，服务器实例支持以下用户/组验证方法：

- Default
- Basic
- Digest

用户/组验证要求用户进行自我验证，然后才能获取访问权限。进行验证时，用户通过以下方法验证其身份：提供用户名和密码、使用客户机证书或使用摘要验证插件。使用客户机证书时需要进行加密。

默认验证

默认验证是首选方法。默认设置使用 obj.conf 文件中的默认方法；如果 obj.conf 中没有设置，则使用基本验证。如果选择 "Default"，则 ACL 规则不会在 ACL 文件中指定方法。如果选择 "Default"，您只需编辑 obj.conf 文件中的一行文本即可方便地更改所有 ACL 的方法。

基本验证

基本验证要求用户提供用户名和密码，才能访问服务器。基本验证是默认设置。您必须在 LDAP 数据库（例如 Sun Java System Directory Server）或文件中创建和存储用户和组的列表。您使用的目录服务器不能与您的 Proxy Server 安装在相同的服务器根目录下；您也可以使用安装在远程计算机上的目录服务器。

当用户尝试访问具有用户/组验证的资源时，系统会提示用户提供用户名和密码。根据您的服务器是否启用了加密（是否启用 SSL），服务器将收到加密或未加密的信息。

注 – 在不进行 SSL 加密的情况下使用基本验证时，会通过网络以未加密文本形式发送用户名和密码。网络包可能会被截取，并且用户名和密码可能会被盗用。当与 SSL 加密、主机/IP 验证或同时与这两者结合使用时，基本验证是最有效的验证方法。使用摘要验证可以消除此问题。

如果验证成功，用户便可查看请求的资源。如果用户名或密码无效，系统会发出拒绝访问的消息。

您可以自定义未经授权的用户所接收的消息。有关更多信息，请参见第 148 页中的 “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）

如果将服务器配置为使用证书信息进行客户机验证，服务器会执行以下操作：

- 进行检查以确定证书是否来自信任的 CA（Certificate Authority，证书授权机构）。如果不是，验证将失败，事务也将结束。要了解如何启用客户机验证，请参见第 80 页中的 “设置安全性首选项”。
- 如果证书来自信任的 CA，则使用 certmap.conf 文件将证书映射到用户的条目中。要了解如何配置证书映射文件，请参见第 96 页中的 “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。即使证书正确进行了映射，ACL 规则也可能会拒绝该用户的访问。

要求对特定资源的访问控制进行客户机验证与要求对服务器的所有连接进行客户机验证不同。如果将服务器配置为要求对所有连接进行客户机验证，则客户机只需要提供由信任的 CA 颁发的有效证书。如果将服务器配置为使用 SSL 方法进行用户和组验证，则必须执行以下操作：

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

如果需要对访问控制进行客户机验证，必须针对 Proxy Server 启用 SSL 加密。有关启用 SSL 的更多信息，请参见第 5 章。

要成功访问经过 SSL 验证的资源，客户机证书必须来自 Proxy Server 所信任的 CA。如果 Proxy Server 的 `certmap.conf` 文件被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相比较，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，您可以将 `certmap.conf` 配置为仅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，请参见第 5 章。另请参见《Sun Java System Web Proxy Server 4.0.4 Configuration File Reference》。

摘要验证

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

通过摘要验证，用户可以基于用户名和密码进行验证，而无需以明文形式发送用户名和密码。浏览器使用用户密码和 Proxy Server 提供的某些信息，利用 MD5 算法来创建摘要值。

当服务器使用基于 LDAP 的目录服务来执行摘要验证时，服务器端也将使用摘要验证插件来计算该摘要值，并且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，您的目录服务器必须有权访问明文形式的用户密码。Sun Java System Directory Server 具有一个可逆的密码插件，它使用对称的加密算法以加密形式存储数据，这些数据可在稍后被解密成原来的形式。只有目录服务器保存了数据的密钥。

对于基于 LDAP 的摘要验证，您必须启用 Proxy Server 附带的可逆密码插件和特定的摘要验证插件。要将 Proxy Server 配置为处理摘要验证，请在 `dbswitch.conf` 文件（位于 *server-root*`/userdb/` 中）中设置数据库定义的 `digestauth` 属性。

以下为 dbswitch.conf 文件样例。

```
directory default ldap://<host_name>:<port>
default:binddn cn=Directory Manager
default:encoded bindpw ***********
default:digestauth on
```

或者

```
directory default ldap://<host_name>:<port>/
default:binddn cn=Directory Manager
default:encoded bindpw ***********
default:digestauthstate on
```

服务器将尝试基于指定的 ACL 方法验证 LDAP 数据库，如第 132 页中的 “摘要验证”所示。如果未指定 ACL 方法，当要求进行验证时，服务器将使用摘要验证或基本验证；当不要求进行验证时，服务器将使用基本验证。

下表列出了验证数据库支持以及不支持的摘要验证。

表 8–1 摘要验证的不同情况

ACL 方法	验证数据库支持	验证数据库不支持
Default 未指定	Digest 和 Basic	Basic
Basic	Basic	Basic
Digest	Digest	ERROR

处理具有 `method=digest` 的 ACL 时，服务器将尝试通过执行以下操作进行验证：

- 检查 Authorization 请求标头。如果未找到标头，将生成要求进行摘要验证的 401 响应，并且进程将停止。
- 检查 Authorization 类型。如果验证类型为 "Digest"，服务器将执行以下操作：
  - 检查 nonce。如果 nonce 不是此服务器生成的最新有效 nonce，将生成 401 响应，并且进程将停止。如果 nonce 过时，将生成包含 `stale=true` 的 401 响应，并且进程将停止。

    通过更改 `magnus.conf` 文件（位于 *server-root*`/proxy-server_name/config/` 中）中参数 `DigestStaleTimeout` 的值，可以配置 nonce 被保留的时间。要设置该值，请将下面一行添加到 `magnus.conf` 中：

    `DigestStaleTimeout` *seconds*

    其中 *seconds* 表示 nonce 被保留的秒数。指定的秒数过后，nonce 将过期并要求用户进行新的验证。
  - 检查领域。如果领域不匹配，将生成 401 响应，并且进程将停止。
  - 如果验证目录是基于 LDAP 的，则检查 LDAP 目录中的用户是否存在；如果验证目录是基于文件的，则检查文件数据库中的用户是否存在。如果未找到用户，将生成 401 响应，并且进程将停止。
  - 从目录服务器或文件数据库中获取 `request-digest` 值，并检查该值是否与客户机的 `request-digest` 相匹配。如果不匹配，将生成 401 响应，并且进程将停止。
  - 构造 `Authorization-Info` 标头并将其插入服务器标头中。

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。此插件会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。

如果您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和一个 ldif 文件：

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

▼ 在 UNIX 上安装摘要验证插件

开始之前

- 确保此共享库与 Sun Java System Directory Server 位于相同的服务器计算机上。
- 确保知道 Directory Manager 的密码。
- 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。

● **要安装插件，请键入以下命令：**

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

在 Windows 上安装摘要验证插件

为了使具有摘要验证插件的 Directory Server 能够正常启动，必须将 Proxy Server 安装中的多个 `.dll` 文件复制到 Sun Java System Directory Server 服务器计算机中。

▼ 在 Windows 上安装摘要验证插件

1. **访问位于 Proxy Server 内 *server-root*`\bin\proxy\bin` 中的共享库。**
2. **将文件 `nsldap32v50.dll`、`libspnr4.dll` 和 `libplds4.dll` 复制到相应的目录中：**
3. **将这些文件粘贴到以下任一位置：**
   - `\Winnt\system32`
   - Sun Java System Directory Server 安装目录：*server-root*`\bin\sldap\server`

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

加密存储摘要密码的属性时，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 控制台。
2. 打开 Sun ONE Directory Server 5.1 SP1（或更高版本）的实例。
3. 选择 "Configuration" 选项卡。
4. 单击插件旁边的 + 号。
5. 选择 DES 插件。
6. 选择 "Add" 添加一个新属性。
7. 键入 `iplanetReversiblePassword`。
8. 单击 "Save"。
9. 设置摘要验证密码。

注 – 服务器使用位于对象类 iplanetReversiblePassword 中的 iplanetReversiblePassword 属性。要在用户的 `iplanetReversiblePassword` 属性中使用摘要验证密码，您的条目中必须包括 `iplanetReversiblePasswordobject` 对象。

可以使用 `ldapmodify` 或 Directory Server 管理界面实现此操作。

使用 `ldapmodify` —

创建文件 `digest.ldif` 以存储 LDAP 命令。添加密码通过两个步骤完成。

a. **将对象类添加到** `digest.ldif`。

   此文件包含以下内容（可以根据 Directory Server 用户和 ACL 创建多个 `ldif` 文件）：

```
dn:uid=user1,dc=india,dc=sun,dc=com
changetype:modify
add:objectclass
objectclass:iplanetReversiblePasswordobject

dn:uid=user1,dc=india,dc=india,dc=sun,dc=com
changetype:modify
add:iplanetReversiblePassword
iplanetReversiblePassword:user1
```

b. `# ldapmodify -D "cn={CN_Value}" -w <password> -a <ldif_file_name>`

10 **重新启动 Sun Java System Directory Server 实例，并检验是否已将用户属性添加到 Directory Server 数据库中。**

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

您可以通过将 Administration Server 及其文件和目录仅限于使用特定计算机的客户机使用来限制对它们的访问。您可以指定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。用户可以立即访问文件和目录，而无需输入用户名或密码。

由于某台特定的计算机可能由多个用户使用，因此，主机/IP 验证与用户/组验证结合使用时会更加有效。如果同时使用这两种验证方法，访问时将要求提供用户名和密码。

主机/IP 验证不要求在服务器上配置 DNS（Domain Name Service，域名服务）。如果选择使用主机/IP 验证，您必须在网络中运行 DNS 并将您的服务器配置为使用该 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"。您将看到 DNS 设置。

启用 DNS 会降低 Proxy Server 的性能，因为服务器将不得不执行 DNS 查找。要减小 DNS 查找对服务器性能的影响，请仅针对访问控制和 CGI 解析 IP 地址，而不是针对每个请求解析 IP 地址。要设置此限制，请在 `obj.conf` 中指定以下内容：

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

使用访问控制文件

对 Administration Server 或服务器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* 是安装服务器的位置。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 来配置访问，您将拥有这两个文件。但是，如果需要更为复杂的限制，可以创建多个文件并在 `server.xml` 文件中加以引用。还有几个功能只能通过编辑这些文件才能获得，例如，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，请参见第 18 章。有关 `server.xml` 的更多信息，请参见 《Sun Java System Web Proxy Server 4.0.4 Configuration File Reference》 。

配置 ACL 用户高速缓存

默认情况下，Proxy Server 将用户和组验证结果高速缓存在 ACL 用户高速缓存中。通过使用 magnus.conf 文件中的 ACLCacheLifetime 指令，可以控制 ACL 用户高速缓存保持有效的时间。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，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 参数 ACLUserCacheSize，可以配置高速缓存中保存的最大条目数。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。

此外，还可以使用 magnus.conf 参数 ACLGroupCacheSize 来设置为每个用户条目高速缓存的最大组成员数。此参数的默认值为 4。组中非成员关系的用户不会被高速缓存，这将导致每个请求都要进行多个 LDAP 目录访问。

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结合使用。您必须指定访问特定资源时需要使用客户机证书。如果在服务器上启用了此功能，则拥有证书的用户只需在首次尝试访问受限资源时输入其名称和密码。建立用户的身份之后，服务器便会将其登录名和密码映射到此特定的证书。此后，当用户访问要求进行客户机验证的资源时，不再需要输入其登录名或密码。

当用户尝试访问受限资源时，其客户机会向服务器发送客户机证书，然后服务器将检查此证书是否位于其映射列表中。如果此证书属于已被授予访问权限的用户，则此用户便可使用资源。

要求对特定资源的访问控制进行客户机验证与要求对服务器的所有连接进行客户机验证不同。另请注意，如果要求对所有 SSL 连接使用客户机证书，则不会自动将证书映射到数据库中的用户。要设置此映射，必须指定访问指定资源时需要使用客户机证书。

访问控制的工作原理

当服务器收到页面请求时，它会使用 ACL 文件中的规则来确定是否应当授予访问权限。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。

以下示例显示了 ACL 文件可能包含的内容，并提供了访问控制规则示例。

```
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，如果用户请求 URL `http://server_name/my_stuff/web/presentation.html`，Proxy Server 首先将检查整个服务器的访问控制。如果整个服务器的 ACL 被设置为 "Continue"，服务器将检查目录 `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`）的最后的 ACL。

要使用 Server Manager 设置本例的访问控制，可以仅为此文件创建一个 ACL，也可以为此文件中引用的每个资源创建一个 ACL（即，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，一个用于此文件）。

如果有多个匹配的 ACL，服务器将使用最后一个匹配的 ACL 语句。

设置访问控制

本节介绍限制访问的过程。您可以针对所有服务器设置全局访问控制规则，也可以针对特定服务器进行单独设置。例如，人力资源部门可以创建 ACL，允许所有通过验证的用户查看他们自己的工资单数据，但限制访问以只允许负责工资单的人员更新数据。

本节包含以下主题：

- 第 140 页中的 “设置全局访问控制”
- 第 141 页中的 “设置服务器实例的访问控制”

注 – 在设置全局访问控制之前，必须先配置并激活分布式管理。

设置全局访问控制

▼ 为所有服务器设置访问控制

1. **访问 Administration Server 并单击 "Global Settings" 选项卡。**
2. **单 "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" 以装入数据，然后单击 "New ACL"（或 "Edit ACL"）。**
4. **如果系统提示，请进行验证。**
   将显示 "Access Control Rules For" 页面。Administration Server 具有两行不能编辑的默认访问控制规则。
5. **选择 "Access Control Is On"（如果尚未选中）。**
6. **要将一个默认 ACL 规则添加到该表的底部一行，请单击 "New Line" 按钮。**
   要更改访问控制限制的位置，请单击向上或向下箭头。
7. **单击 "Users/Groups" 列中的 "Anyone"。**
   "User/Group" 页面将显示在下面的框架中。
8. **选择您要允许其访问的用户和组，然后单击 "Update"。**
   单击 "Group" 或 "User" 的 "List" 按钮，即可显示从中进行选择的列表。有关这些设置的更多信息，请参见联机帮助。另请参见第 144 页中的 “指定用户和组”。
9. **单击 "From Host " 列中的 "Anyplace"。**
   "From Host" 页面将显示在下面的框架中。
10. **指定允许其访问的主机名和 IP 地址，然后单击 "Update"。**
    有关这些设置的更多信息，请参见联机帮助。另请参见第 145 页中的 “指定 "From Host"”。
11. **单击 "Programs" 列中的 "All"。**
    "Programs" 页面将显示在下面的框架中。
12. **选择 "Program Groups"，或在 "Program Items" 字段中键入您要允许其访问的特定文件名，然后单击 "Update"。**
    有关这些设置的更多信息，请参见联机帮助。另请参见第 146 页中的 “限制对程序的访问”。

13 **（可选）单击 "Extra" 列中的 X 符号可以添加一个自定义的 ACL 表达式。**

"Customized Expressions" 页面将显示在下面的框架中。有关更多信息，请参见第 147 页中的 “编写自定义表达式”。

14 **选中 "Continue" 列中的复选框（如果尚未选中）。**

服务器将评估下一行限制，然后才确定是否允许该用户进行访问。创建多行限制时，请将限制按照由粗到细的顺序排列。

15 **（可选）单击垃圾箱图标可以从访问控制规则中删除相应的行。**

16 **（可选）单击 "Response When Denied" 链接可以指定访问被拒绝时用户收到的响应。**

"Access Deny Response" 页面将显示在下面的框架中。

a. **选择所需的响应。**

b. **指定其他信息（如果适用）。**

c. **单击 "Update"。**

有关这些设置的更多信息，请参见第 148 页中的 “访问被拒绝时的响应”。

17 **单击 "Submit" 可以将新访问控制规则存储在 ACL 文件中；单击 "Revert" 可以将页面中的元素重置为更改前它们所包含的值。**

设置服务器实例的访问控制

使用 Server Manager，您可以创建、编辑或删除特定服务器实例的访问控制。如果要删除，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。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 并单击 "Preferences" 选项卡。**

2 **单击 "Administer Access Control" 链接。**

3 **使用以下方法之一选择 ACL：**

- 从 "Select A Resource" 下拉式列表中选择一个使用 ACL 限制访问的资源，或单击 "Regular Expression" 指定一个正则表达式。有关更多信息，请参见 Proxy Server **管理指南**中的第 16 章。
- 选择现有 ACL 将列出所有启用的 ACL。

尚未启用的现有 ACL 不会显示在此列表中。从下拉式列表中选择 ACL。

- 键入 ACL 名称。可以通过此选项创建命名 ACL。仅当您熟悉 ACL 文件时，才能使用此选项。如果要将命名 ACL 应用到资源，您必须手动编辑 `obj.conf`。有关更多信息，请参见第 18 章。

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"（如果尚未选中）。**

6. **要将一个默认 ACL 规则添加到该表的底部一行，请单击 "New Line" 按钮。**
   要更改访问控制限制的位置，请单击向上或向下箭头。

7. **要编辑此服务器实例的 ACL，请单击 "Action" 列中的操作。**
   "Allow/Deny" 页面将显示在下面的框架中。

8. **选择 "Allow"（如果默认情况下没有选中），然后单击 "Update"。**
   有关 "Allow" 或 "Deny" 的更多信息，请参见第 143 页中的 “设置操作”。

9. **单击 "Users/Groups" 列中的 "Anyone"。"User/Group" 页面将显示在下面的框架中。**

10. **选择您要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，可以显示从中进行选择的列表。有关这些设置的更多信息，请参见联机帮助。另请参见第 144 页中的 “指定用户和组”。

11. **单击 "From Host" 列中的 "Anyplace"。**
    "From Host" 页面将显示在下面的框架中。

12. **指定允许其访问的主机名和 IP 地址，然后单击 "Update"。**
    有关这些设置的更多信息，请参见联机帮助。另请参见第 145 页中的 “指定 "From Host"”。

13. **单击 "Rights" 列中的 "All"。**
    "Access Rights" 页面将显示在下面的框架中。

14. **指定此用户的访问权限，然后单击 "Update"。**
    有关更多信息，请参见第 146 页中的 “限制对程序的访问”。

15. **（可选）单击 "Extra" 列下的 X 符号可以添加一个自定义的 ACL 表达式。**
    "Customized Expressions" 页面将显示在下面的框架中。有关更多信息，请参见第 147 页中的 “编写自定义表达式”。

16 **选中 "Continue" 列中的复选框（如果尚未选中）。**

服务器将评估下一行限制，然后才能确定是否允许该用户进行访问。创建多行限制时，请将限制按照由粗到细的顺序排列。

17 **（可选）单击垃圾箱图标可以从访问控制规则中删除相应的行。**

请勿删除 ACL 文件中的所有 ACL 规则。要启动服务器，至少需要一个 ACL 文件，该文件至少包含一条 ACL 规则。如果删除了 ACL 文件中的所有 ACL 规则，并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" 链接可以指定访问被拒绝时用户收到的响应。**

"Access Deny Response" 页面将显示在下面的框架中。选择所需的响应，指定其他信息（如果适用），然后单击 "Update"。有关这些设置的更多信息，请参见第 148 页中的 “访问被拒绝时的响应”。

19 **单击 "Submit" 可以将新访问控制规则存储在 ACL 文件中；单击 "Revert" 可以将页面中的元素重置为更改前它们所包含的值。**

选择访问控制选项

以下主题介绍了可以在设置访问控制时选择的各种选项。对于 Administration Server，头两行为默认设置，且不能编辑。

本节包含以下主题：

设置操作

您可以指定当请求符合访问控制规则时服务器要执行的操作。

- **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

服务器将检查整个控制访问条目 (Access Control Entries, ACE) 列表以确定访问权限。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"，服务器将检查列表中的第二个 ACE。如果该 ACE 匹配，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。服务器将继续检查列表，直至找到某个不匹配的 ACE，或匹配但不会继续执行的 ACE。最后一个匹配的 ACE 将确定允许访问还是拒绝访问。

指定用户和组

使用用户和组验证时，将提示用户提供用户名和密码，然后才能访问在访问控制规则中指定的资源。

Proxy Server 将检查在 LDAP 服务器（例如 Sun Java System Directory Server）或基于内部文件的验证数据库中存储的用户和组的列表。

您可以允许或拒绝数据库中的任何用户进行访问，也可以使用通配符模式允许或拒绝特定用户进行访问，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。

在用户界面内 "Access Control Rules" 页面的 "Users/Groups" 中，将显示以下元素。

- **Anyone (No Authentication)** 是默认设置，意味着任何用户都可以访问该资源而不必提供用户名或密码。但是，根据其他设置（例如主机名或 IP 地址）的不同，该用户也可能被拒绝访问。对于 Administration Server，此设置意味着您为分布式管理指定的管理员组中的任何用户都可以访问各个页面。
- **Authenticated People Only**
  - **All In The Authentication Database** 将匹配在数据库中具有用户条目的任何用户。
  - **Only The following People** 将指定要匹配的用户和组。您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** 将匹配您指定的组中的所有用户。**User** 将匹配您指定的单个用户。对于 Administration Server，用户还必须位于您为分布式管理指定的管理员组中。

  Prompt For Authentication 将指定在验证对话框中显示的消息文本。您可以使用此文本来说明用户需要键入的内容。基于不同的操作系统，用户大约会看到该提示的前 40 个字符。大多数浏览器会缓存用户名和密码，并将它们与提示文本关联。如果用户访问的服务器文件和目录区域具有相同的提示，则该用户不需要重新键入用户名和密码。反过来，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* 将指定服务器用于从客户机获取验证信息的方法。Administration Server 仅提供了基本验证方法。Server Manager 提供了以下验证方法：
  - *Default* 将使用在 `obj.conf` 文件中指定的默认方法；如果 `obj.conf` 中没有设置，则使用基本验证。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"，您只需编辑 `obj.conf` 文件中的一行文本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 SSL）后才对用户名和密码加密。否则，用户名和密码将以明文形式发送，在受到拦截时可被读取。
- *SSL* 将使用客户机证书验证用户。要使用此方法，必须为服务器启用 SSL。如果启用了加密，可以组合使用基本方法和 SSL 方法。

注 – 只能以反向代理模式而不是正向代理模式启用安全性。

- *Digest* 将使用这样一种验证机制：通过该机制，浏览器可以基于用户名和密码来验证用户，而不必以明文形式发送用户名和密码。浏览器使用用户的密码和 Proxy Server 提供的某些信息，利用 MD5 算法来创建摘要值。服务器端也可以计算此摘要值（使用摘要验证插件）并与客户机提供的摘要值进行比较。

注 – "Prompt For Authentication" 是摘要验证中的一个必需参数。请将此值更改为与领域相匹配（摘要文件所要求的）。例如，如果在摘要文件中，您已经将所有用户配置为位于领域 *test* 中，则 "Prompt For Authentication" 字段中应当包含文本 *test*。

- *Other* 将使用一种自定义方法，您可以使用访问控制 API 来创建此方法。

Authentication Database 指定服务器用于验证用户的数据库。此选项仅在 Server Manager 中可用。如果选择 "Default"，服务器将查找配置为默认的目录服务中的用户和组。如果要将各个 ACL 配置为使用不同的数据库，请选 "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。如果要针对自定义数据库使用访问控制 API，请选择 "Other"，然后键入数据库名称。

指定 "From Host"

您可以基于请求来自哪台计算机限制对 Administration Server 的访问。

在用户界面内 "Access Control Rules For" 页面的 "From Host" 中，将显示以下元素：

- "Anyplace" 允许对所有用户和系统进行访问
- "Only From" 仅允许特定主机名或 IP 地址进行访问

如果选择 "Only From" 选项，请在 "Host Names" 或 "IP Addresses" 字段中键入通配符模式或逗号分隔的列表。按主机名进行限制要比按 IP 地址进行限制更为灵活。如果用户的 IP 地址发生更改，您也不需要更新此列表。但是，按 IP 地址进行限制更可靠。如果某个连接的客户机的 DNS 查找失败，将无法使用主机名限制。

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

对于主机名，* 必须替换名称完整的一部分，即，`*.example.com` 有效，但 `*users.example.com` 无效。当 * 出现在主机名中时，它必须是最左侧的字符。例如，`*.example.com` 有效，但 `users.*.com` 无效。

对于 IP 地址，* 必须替换地址中的整个字节，例如，`198.95.251.*` 有效，但 `198.95.251.3*` 无效。当 * 出现在 IP 地址中时，它必须是最右侧的字符。例如，`198.*` 有效，但 `198.*.251.30` 无效。

限制对程序的访问

对程序的访问只能由 Administration Server 来限制。通过限制对程序的访问，可以仅允许指定的用户查看 Server Manager 页面，并确定这些用户是否能够配置该服务器。例如，您可能允许某些管理员配置 Administration Server 的 "Users and Groups" 部分，但是拒绝他们访问 "Global Settings" 部分。

您可以配置不同的用户访问不同的功能域。为某个用户授予了对若干选定功能域的访问权限后，该用户登录后只能访问这些功能域的 Administration Server 页面。

在用户界面内 "Access Control Rules For" 页面的 "Programs" 中，将显示以下元素：

- "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。
- "Only The Following" 用于指定用户可以访问的程序。
  - **Program Groups** 反映了 Administration Server 的各个选项卡（例如 "Preferences" 和 "Global Settings"），代表了对这些页面的访问。当管理员访问 Administration Server 时，服务器将使用他们的用户名、主机和 IP 地址来确定他们可以查看哪些页面。
  - "Program Items" 用于通过在字段中键入页面名称来控制对某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。访问权限限制了对您服务器上的文件和目录的访问。除了允许或拒绝所有访问权限外，您还可以指定一个规则以允许或拒绝部分访问权限。例如，您可以授予用户对您文件的只读访问权限，这样他们可以查看信息，但不能更改文件。

在用户界面内 "Access Control Rules For" 页面的 "Rights" 中，将显示以下元素。

- "All Access Rights" 是默认设置，将允许或拒绝所有权限。
- **Only The following Rights** 使您可以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，包括 HTTP 方法 PUT、DELETE、MKDIR、RMDIR 和 MOVE。要删除文件，用户必须同时具有写入权限和删除权限。
  - *Execute* 允许用户执行服务器端应用程序，例如 CGI 程序、Java applet 和代理。
  - *Delete* 允许同时还具有写入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

您可以为 ACL 输入自定义表达式。仅当您熟悉 ACL 文件的语法和结构时，才能选择此选项。有若干功能只有通过编辑 ACL 文件或创建自定义表达式才能实现。例如，您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和一周中的某一天来限制访问。本例假设您的 LDAP 目录中有两个组。"Regular" 组可以在星期一到星期五的 8:00 am 到 5:00 pm 进行访问。"Critical" 组在任何时间均可进行访问。

```
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，请参见第 18 章。

禁用访问控制

如果在 "Access Control Rules For" 页面中取消选中标记为 "Access Control Is On" 的选项，将会收到提示，询问您是否要删除 ACL 中的记录。单击 "OK" 后，便会从 ACL 文件中删除该资源的 ACL 条目。

如果要取消激活 ACL，请在文件 `generated-proxy-`*`serverid`*`.acl` 中注释掉 ACL 行，通过在每行的开头使用 # 符号实现此操作。

在 Administration Server 中，您可以为特定服务器实例创建并启用访问控制，而为其他服务器禁用访问控制（默认设置为禁用）。例如，您可以通过 Administration Server 页面拒绝对 Server Manager 的任何访问。对于默认情况下启用了分布式管理且禁用了访问控制的任何其他服务器，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显示的默认消息，您可以根据需要自定义响应。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，用户会收到 *server-root*`/httpacl/admin-denymsg.html` 中的 "Permission Denied" 消息。

▼ 更改访问被拒绝消息

1. **单击 "Access Control Rules For" 页面上的 "Response When Denied" 链接。**
2. **选择所需的响应，提供其他信息（如果适用），然后单击 "Update"。确保用户可以访问将他们重定向到的响应。**
3. **单击 "Submit" 保存更改，或者单击 "Revert" 将页面中的元素重置为更改前它们所包含的值。**

限制对服务器中的区域的访问

本节介绍一些常用的对服务器及其内容的限制。每个过程中包含的步骤详细介绍了您必须执行的特定操作。但是，您仍必须完成第 141 页中的 “设置服务器实例的访问控制”中所述的步骤。

本节包含以下主题：

限制对整个服务器的访问

您可能希望为某个组中的用户授予访问权限，以便允许他们从某个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

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. **添加一个规则以拒绝所有用户的访问。**
5. **添加另一个规则以允许特定组的访问。**
6. **使用 "From Host" 指定要限制的主机名和 IP 地址。**
7. **单击 "Submit" 保存更改。**

限制对目录的访问

您可以允许某个组中的用户读取或运行目录及其子目录中的应用程序和文件（这些内容由该组的所有者控制）。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

使用设置对服务器实例的访问控制时介绍的步骤（请参见第 141 页中的 “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. **创建一个规则，其默认值为拒绝任何用户从任何位置进行访问。**
5. **创建另一个规则，允许某个特定组中的用户仅具有读取权限和执行权限。**
6. **创建第三个规则，允许某个特定用户具有所有权限。**
7. **对于最后两个规则，取消选中 "Continue"。**
8. **单击 "Submit" 保存更改。**

限制对文件类型的访问

您可以限制对文件类型的访问。例如，您可能希望仅允许特定用户创建在您的服务器上运行的程序。任何用户都可以运行程序，但只有组中的特定用户可以创建或删除程序。

▼ 限制对文件类型的访问

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. **创建一个规则，为所有用户授予读取权限。**
6. **创建另一个规则，仅为某个特定组授予写入权限和删除权限。**
7. **单击 "Submit" 保存更改。**

   对于文件类型限制，您应当保留选中两个 "Continue" 复选框。当传入某个文件的请求时，服务器将首先检查该文件类型的 ACL。

   在 `obj.conf` 文件中将创建一个 `Pathcheck` 函数，它可能包含了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

您可以将对服务器的写入访问和删除访问限制为仅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

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" 部分的下拉式列表中选择整个服务器，然后单击 "Edit"。**

4. **创建一个规则，为所有用户授予读取权限和执行权限。**
   如果某个用户要添加、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. **创建另一个规则，拒绝所有用户的写入权限和删除权限。**
6. **单击 X 链接，创建一个自定义表达式。**
7. **键入允许的一周中的某些天和一天中的某些时间，例如：**

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

8. **单击 "Submit" 保存更改。**
   自定义表达式中的任何错误都将生成一条错误消息。请进行更正并再次提交。

基于安全性限制访问

您可以为同一服务器实例同时配置 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

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" 部分的下拉式列表中选择整个服务器，然后单击 "Edit"。**
4. **创建一个规则，为所有用户授予读取权限和执行权限。**
   如果某个用户要添加、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. **创建另一个规则，拒绝所有用户的写入权限和删除权限。**
6. **单击 X 链接，创建一个自定义表达式。**
7. **键入 `ssl="on"`。例如：**

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

8. **单击 "Submit" 保存更改。**
   自定义表达式中的任何错误都将生成一条错误消息。请进行更正并再次提交。

保护对资源的访问

本节介绍了在启用分布式管理后，为在 Proxy Server 中保证访问控制的安全性而必须执行的其他任务。

保护对服务器实例的访问

要配置 Proxy Server 以控制对服务器实例的访问，请编辑 *server-root*/httpacl/*.proxy-admserv.acl 文件并指定要授予其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 相关的 ACL 文件 (gen*.proxy-admserv.acl) 中，请完成下面的步骤 1 和 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相关的 ACL 文件中，请仅为该特定 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 user 和 group 之外，再将 ip 添加到验证列表中，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";
   ```

为基于文件的验证创建 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形式存储了用户和组信息。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。

本节介绍如何基于文件验证和摘要验证来为目录服务创建 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` 文件包含一个用于定义文件验证数据库及其配置的条目。例如：

```
directory myfiledb filemyfiledb:syntax keyfilemyfiledb: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，则默认为 `keyfile`。
`keyfile`	（`syntax=keyfile` 时需要）包含用户数据的文件的路径。
`digestfile`	（`syntax=digest` 时需要）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每行的最大长度为 255。如果任一行超出了此限制，服务器将无法启动，并在日志文件中记录错误。

请确保在尝试使用基于文件的验证数据库设置 ACL 之前，已经配置了基于文件的验证目录服务。有关更多信息，请参见第 45 页中的 “配置目录服务”。

为基于文件验证的目录服务创建 ACL

▼ 为基于文件验证的目录服务创建 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，单击要编辑的 ACL 条目的 "Users/Groups" 链接。**
   "User/Group" 页面将显示在下面的框架中。
5. **从 "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" 保存更改。**
   当您按照基于密钥文件的文件验证数据库设置 ACL 时，`dbswitch.conf` 文件使用相应的 ACL 条目进行更新，如下面给出的样例条目所示：

```
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";
```

为基于摘要验证的目录服务创建 ACL

文件验证数据库也支持适用于摘要验证的文件格式（根据 RFC 2617）。将存储基于密码和领域的散列。不会保留明文密码。

▼ 为基于摘要验证的目录创建 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，单击要编辑的 ACL 的 "Users/Groups" 链接。**
   "Users/Groups" 页面将显示在下面的框架中。
5. **从 "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" 保存更改。

当您按照基于摘要验证的文件验证数据库设置 ACL 时，`dbswitch.conf` 文件使用相应的 ACL 条目进行更新，如下面给出的样例条目所示。

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

◆ ◆ ◆ 第 9 章

9 使用日志文件

可以使用多种不同的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。有关使用内置的性能监视服务或 SNMP 的信息，请参见第 10 章。

本章包含以下各节：

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，并在诊断错误时为您提供帮助。位于服务器根目录的 `proxy-server_name/logs/errors` 中的错误日志文件列出了服务器遇到的所有错误。位于服务器根目录下的 `proxy-server_name/logs/access` 中的访问日志记录了有关向服务器提交的请求以及服务器的响应的信息。您可以配置 Proxy Server access 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 – 由于操作系统的限制，在 Linux 上 Proxy Server 不能使用大于 2 GB 的日志文件。达到最大日志大小后，日志记录就会停止。

登录 UNIX 和 Windows 平台

本节介绍如何创建日志文件。此外，还包括以下主题：

- 第 158 页中的 “默认错误日志”
- 第 158 页中的 “使用 syslog 记录日志”

注 – 有关 Windows 操作环境所使用的事件日志机制的更多信息，请在 Windows 帮助系统索引中查找关键字 "Event Logging"。

默认错误日志

在 UNIX 和 Windows 平台上，Administration Server 的日志存储在管理 `proxy-admserv/logs/` 目录下。服务器实例的日志存储在 `proxy-server_name/logs/` 目录中。

可以设置整个服务器的默认日志级别。可以将 `stdout` 和 `stderr` 重定向到服务器的事件日志，将日志输出定向到操作系统的系统日志。此外，还可以将 stdout 和 stderr 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外，还将发送到 stderr。

使用 `syslog` 记录日志

`syslog` 适用于要求集中记录日志的稳定的操作环境。在需要经常查看日志输出以进行诊断和调试的环境中，设置一个服务器实例日志可能比较容易管理。

由于将服务器实例和 Administration Server 的日志数据都存储在一个文件中可能会使读取和调试困难，因此应仅对运行正常的、已部署的应用程序使用 `syslog` 主日志文件。

日志消息与 Solaris 守护进程应用程序中的所有其他日志混合在一起。

将 `syslog` 日志文件与 `syslogd` 和系统日志守护进程一起使用，可以配置 `syslog.conf` 文件执行以下操作：

- 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`

因为将日志记录到 syslog 意味着 Proxy Server 以及其他守护进程应用程序的日志都存储在同一个文件中，所以日志消息中增加了以下信息，以便标识来自特定服务器实例中专用于 Proxy Server 的消息：

- 唯一消息 ID
- 时间标记
- 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 文件中同时为 Administration Server 和服务器实例配置 LOG 元素。

要获得有关 UNIX 操作环境所使用的 syslog 记录机制的更多信息，请在出现终端提示后使用以下 man 命令：

```
man syslog
man syslogd
man syslog.conf
```

日志级别

下表按照严重性递增的顺序定义了 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	表明调试消息详细程度的消息。finest 指定最大详细程度。
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。

将日志文件归档

可以设置将自动归档的访问日志文件和错误日志文件。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 将保存旧的日志文件并用含有保存日期和时间的名称标记所保存的文件。

例如，可以设置每小时轮转访问日志文件一次。Proxy Server 将保存该文件并将其命名为 "access.200505160000"，其中日志文件的名称、年、月、日和 24 小时时间被串联到一起，形成一个字符串。根据所设置的日志轮转类型，日志归档文件的格式会有所不同。

Proxy Server 为归档文件提供了两种日志轮转类型：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

内部守护进程日志轮转发生在 HTTP 守护进程内，且只能在启动时进行配置。服务器在内部轮转日志，不要求重新启动服务器。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 12:00 a.m.，并且轮转间隔为 1440 分钟（一天），那么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。日志文件在每天的 12:00 a.m. 进行轮转，而访问日志将被标记为 12:00 a.m.，并保存为 `access.200505172400`。同样，如果将间隔设置为 240 分钟（4 小时），开始时间为 12:00 a.m.，访问日志文件将包含从 12:00 a.m. 到 4:00 a.m.，从 4:00 a.m. 到 8:00 a.m. 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 12:00 a.m.，并将轮转间隔设置为 240 分钟，而当前的时间为 4:00 a.m.，则第一个要轮转的日志文件将包含从 4:00 a.m. 至 8:00 a.m 之间收集到的信息，下一个日志文件将包含 8:00 a.m. 至 12:00 p.m.（中午）的信息，并依此类推。

基于调度程序的日志轮转

基于调度程序的日志轮转以 *server-root*`/proxy-` *server_name*`/config/` 目录的 `server.xml` 文件中存储的时间和日期为基准。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 4:30 p.m 轮转文件时，access 将变为 access.200505171630。

日志轮转在服务器启动时进行初始化。如果启用了轮转，Proxy Server 将创建一个带有时间标记的访问日志文件并在服务器启动时开始进行轮转。

开始进行轮转后，如果在需要记录到访问日志文件或错误日志文件的、先前调度的 "next rotate time" 之后，发生请求或错误，Proxy Server 将创建一个新的带有时间标记的日志文件。

注 – 应在运行日志分析程序之前将服务器日志归档。

要将日志文件归档以及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，用于日志的格式，以及在客户机访问资源时服务器是否应花时间查找客户机的域名，可以为任何资源自定义访问日志。

您可以使用 Server Manager 中的 "Set Access Log Preferences" 页面来指定日志首选项，也可以手动配置 obj.conf 文件中的指令。在 obj.conf 中，服务器调用函数 flex-init 来初始化灵活日志系统，调用函数 flex-log 按照灵活日志格式记录特定于请求的数据。要使用通用日志文件格式记录请求，服务器调用 init-clf 来初始化 obj.conf 中使用的通用日志子系统，使用 common-log 按照大多数 HTTP 服务器使用的通用日志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。

表 9–2 Administration Server 的日志文件格式

日志格式项	描述
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。

表 9–2 Administration Server 的日志文件格式 （续）

日志格式项	描述
Full Request	客户机所作的完整请求。
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（以字节为单位）。
HTTP Header, "referer"	referer（引用站点）可以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，引用站点将是用户从中访问文本搜索引擎的页面。引用站点使服务器可创建回溯链接的列表。
HTTP Header, "user-agent"	user-agent 信息包括客户机正在使用的浏览器的类型、浏览器版本，以及正在运行的操作系统。这些信息来自客户机发送到服务器的 HTTP 标头信息的 User-agent 字段。
Method	使用的 HTTP 请求方法，如 GET、PUT 或 POST。
URI	Universal Resource Identifier（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 中问号之后的任何文本。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。

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。**
   此时将显示 "Set Access Log Preferences" 页面。
3. **选择下拉式列表中的资源，或者单击 "Edit" 按钮，键入一个正则表达式，然后单击 "OK"。**

4. **指定是否记录客户机类。**

   此设置要求启用域名服务 (Domain Name Service, DNS)。

5. **指定访问日志文件的绝对路径。**

   默认情况下，日志文件存储在服务器根目录下的 `logs` 目录中。如果指定了部分路径，服务器将假设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，此字段的默认值为 `$accesslog`，它是配置文件中表示服务器的访问日志文件的变量。

6. **选择是否应在访问日志中记录访问服务器的系统的域名或 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。**

   可以使用以下选项：

   - **Use Common** *LogFile Format*。包括客户机的主机名、经过验证的用户名、请求的日期和时间、HTTP 标头、返回到客户机的状态码，以及发送到客户机的文档的内容长度。
   - **Only Log**。使您可以确定将记录的信息。可以从表 9–2 中列出的灵活日志格式项进行选择。
   - 如果选择一种自定义格式，请在 "Custom Format" 字段中键入该格式。

8. **单击 "OK"。**

9. **单击 "Restart Required"。**

   此时将显示 "Apply Changes" 页面。

10. **单击 "Restart Proxy Server" 按钮应用更改。**

设置服务器实例的访问日志首选项

下表中列出了可用于设置服务器实例的访问日志首选项的灵活日志格式。

表 9–3 服务器实例的日志文件格式

日志格式项	描述
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。

表 9–3 服务器实例的日志文件格式 （续）

日志格式项	描述
System Date	客户机请求的日期和时间。
Full Request	客户机所作的完整请求。
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（以字节为单位）。
HTTP Header, "referer"	referer（引用站点）可以指定客户机从中访问当前页面的页面。例如，如果用户要查看文本搜索查询的结果，引用站点将是用户从中访问文本搜索引擎的页面。引用站点使服务器可创建回溯链接的列表。
HTTP Header, "user-agent"	user-agent 信息包括客户机正在使用的浏览器的类型、浏览器版本，以及正在运行的操作系统。这些信息来自客户机发送到服务器的 HTTP 标头信息的 User-agent 字段。
Method	使用的 HTTP 请求方法，如 GET、PUT 或 POST。
URI	Universal Resource Identifier（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 中问号之后的任何文本。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	此字段指定高速缓存文件是被写入、刷新还是由最新版本检查返回。
Remote Server Finish Status	此字段指定向远程服务器提交的请求是已成功执行完成，单击浏览器中的“停止”按钮时由客户机中断，还是由错误条件终止。
Status Code From Server	从服务器返回的状态码。
Route To Proxy (PROXY, SOCKS, DIRECT)	用于检索资源的路由。可以直接检索文档，也可以通过代理或 SOCKS 服务器检索文档。
Transfer Time	传送的时间长度（以秒或毫秒为单位）
Header-length From Server Response	服务器响应的标头的长度。
Request Header Size From Proxy To Server	从代理到服务器的请求标头的大小。

表 9–3 服务器实例的日志文件格式 （续）

日志格式项	描述
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	从客户机接收的请求标头的大小。
Content-length From Proxy To Server Request	从代理发送到服务器的文档的长度（以字节为单位）。
Content-length Received From Client	来自客户机的文档的长度（以字节为单位）。
Content-length From Server Response	来自服务器的文档的长度（以字节为单位）。
Unverified User From Client	验证期间提供给远程服务器的用户名。

▼ 设置服务器实例的访问日志首选项

1 **访问 Server Manager 并单击 "Server Status" 选项卡。**

2 **单击 "Set Access Log Preferences" 链接。**

此时将显示 "Set Access Log Preferences" 页面。

3 **选择下拉式列表中的资源，或者单击 "Edit" 按钮，键入一个正则表达式，然后单击 "OK"。**

4 **指定是否记录客户机类。**

此设置要求启用域名服务 (Domain Name Service, DNS)。

5 **指定访问日志文件的绝对路径。**

默认情况下，日志文件存储在服务器根目录下的 `logs` 目录中。如果指定了部分路径，服务器将假设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，此字段的默认值为 `$accesslog`，它是配置文件中表示服务器的访问日志文件的变量。

6 **选择是否应在访问日志中记录访问服务器的系统的域名或 IP 地址。**

7 **选择日志文件的格式：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"，将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。**

服务器访问日志格式可以为通用日志文件格式、扩展日志文件格式、扩展 2 日志文件格式、灵活日志格式或单独的可自定义格式。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。灵活日志格式使您可以从 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、请求的日期和时间、HTTP 标头、返回到客户机的状态码，以及发送到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和一些其他字段，如远程状态、代理到客户机的内容长度、远程到代理的内容长度、代理到远程的内容长度、客户机到代理的标头长度、代理到客户机的标头长度、代理到远程的标头长度、远程到代理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和一些其他字段，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。可以从表 9–3 中列出的灵活日志格式项进行选择。
- 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" 字段中键入它们。

键入服务器不应记录其访问的主机的通配符模式。例如，`*.example.com` 将不记录域为 example.com 的用户的访问。可以为主机名、IP 地址，或同时为二者键入通配符模式。

10 选择是否在日志文件中包括格式字符串。

如果使用的是 Proxy Server 的日志分析程序，应包括格式字符串。如果使用的是第三方的分析程序，可能不需要在日志文件中包括格式字符串。

11 单击 "OK"。

12 单击 "Restart Required"。

此时将显示 "Apply Changes" 页面。

13 单击 "Restart Proxy Server" 按钮应用更改。

简易 Cookie 日志

使用 flexlog 功能，Proxy Server 可以很容易地记录特定的 cookie。将 `Req->headers.cookie.cookie_name` 添加到配置文件 `obj.conf` 中用于初始化 `flex-log` 子系统的行。如果 cookie 变量存在于请求标头中，此指令将记录 cookie 变量 `cookie_name` 的值，如果变量不存在，将记录 "-"。

设置错误日志选项

可以配置在服务器的错误日志中记录信息。

▼ 设置错误记录选项

1. **要从 Administration Server 设置错误日志选项，请选择 "Preferences" 选项卡，然后单击 "Set Error Log Preferences" 链接。**
   要从 Server Manager 为服务器实例设置错误日志选项，请选择 "Server Status" 选项卡，然后单击 "Set Error Log Preferences" 链接。
2. **在 "Error Log File Name" 字段中指定将存储来自服务器的消息的文件。**
3. **从 "Log Level" 下拉式列表中，指定错误日志中应记录的信息量。可以使用以下选项：**
4. **要将 stdout 输出重定向到错误日志，请选择 "Log Stdout"。**
5. **要将 stderr 输出重定向到错误日志，请选择 "Log Stderr"。**
6. **要将日志消息重定向到控制台，请选择 "Log To Console"。**
7. **要使用 UNIX 系统日志服务或 Windows 事件日志来生成和管理日志，请选择 "Use System Logging"。**
8. **单击 "OK"。**
9. **单击 "Restart Required"。**
   此时将显示 "Apply Changes" 页面。
10. **单击 "Restart Proxy Server" 按钮应用更改。**

配置 LOG 元素

下表介绍了可以在 `server.xml` 文件中配置的 LOG 元素的属性。

表 9–4 LOG 属性

属性	默认值	描述
`file`	`errors`	指定将存储来自服务器的消息的文件。

表 9–4 LOG 属性 （续）

属性	默认值	描述
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。
logstdout	true	（可选）如果为 true，将重定向 stdout 输出到错误日志。有效值为 on、off、yes、no、1、0、true 和 false。
logstderr	true	（可选）如果为 true，将重定向 stderr 输出到错误日志。有效值为 on、off、yes、no、1、0、true 和 false。
logtoconsole	true	（可选，仅限于 UNIX）如果为 true，将重定向日志消息到控制台。
createconsole	false	（可选，仅限于 Windows）如果为 true，将为 stderr 输出创建一个 Windows 控制台。有效值为 on、off、yes、no、1、0、true 和 false。
usesyslog	false	（可选）如果为 true，将使用 UNIX syslog 服务或 Windows 事件日志来生成和管理日志。有效值为 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和归档的访问日志文件。

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

要从 Server Manager 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。

以下示例显示了通用日志文件格式的访问日志。

```
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
```

下表描述了此访问日志样例的最后一行。

访问日志字段	示例
客户机的主机名或 IP 地址	`198.18.17.222`（此例中，由于禁用了代理服务器的 DNS 查找设置，因此显示客户机的 IP 地址；如果启用了 DNS 查找，将显示客户机的主机名。）
RFC 931 信息	-（RFC 931 标识未实现）
用户名	*abc*（客户输入的用于验证的用户名）
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

错误日志文件包含自创建该日志文件以来服务器遇到的错误。该文件还包含有关服务器的信息消息，如启动服务器的时间。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中断的 URL 路径或缺少的文件。

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

要从 Server Manager 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。

以下错误日志示例包含三个条目。

```
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 目录包含通过 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 目录中的 HTML 文档介绍了此工具的参数。server-install/extras/flexanlg 目录包含灵活日志文件格式的命令行日志分析程序。但是默认情况下，Server Manager 使用灵活日志文件报告工具，无论选择了哪种日志文件格式，都是如此。

使用日志分析程序可以生成有关默认服务器的统计信息，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，应归档服务器日志。有关归档服务器日志的更多信息，请参见第 160 页中的 “将日志文件归档”。

还可以在转到 server-root/proxy-server*id* 目录后，在命令提示符上键入 ./start -shell，这样就不必设置库路径。

如果使用扩展日志格式或扩展 2 日志格式，日志分析程序将在输出文件中生成除了所指定要报告的信息外，还会生成多个报告。以下部分介绍了这些报告。

传送时间分布报告

传送时间分布报告说明了代理服务器用于传送请求的时间。此报告显示按服务时间和完成的百分比分类的信息。以下示例是一个传送时间分布报告样例。

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%]..........................................
```

数据流报告

数据流报告说明了从客户机到代理、代理到客户机、代理到远程服务器和远程服务器到代理的数据流（已传送的字节数）。对于这每一种情况，报告都将以标头和内容的形式说明已传送的数据量。数据流报告还说明了从高速缓存到客户机的数据流。以下是一个数据流报告样例。

	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:

	Headers	Content	Total
- Cache -> Client.....	0 MB	0 MB	0 MB

状态码报告

状态码报告说明了代理服务器从远程服务器接收和发送到客户机的状态码以及数量。状态码报告还提供了所有这些状态码的解释。以下示例是一个状态码报告样例。

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

请求和连接报告

请求和连接报告说明了代理服务器从客户机接收的请求数，代理向远程服务器请求的连接数（初始检索、最新版本检查和刷新），以及代理服务器使用高速缓存的文档而避免的远程连接数。以下示例是一个请求和连接报告样例。

```
- Total requests.............     478
- Remote connections.........     439
- Avoided remote connects....      39 [ 8.2%]
```

高速缓存性能报告

高速缓存性能报告说明了客户机的高速缓存、代理服务器的高速缓存以及直接连接的性能。

客户机高速缓存

当客户机对文档执行最新版本检查，而远程服务器将返回一条 304 消息，通知客户机文档未修改时，即发生了客户机高速缓存命中。客户机启动的最新版本检查表明，客户机的高速缓存中包含文档的独立副本。

对于客户机的高速缓存，报告将说明：

- **Client and proxy cache hits**：代理服务器和客户机都具有所请求文档的副本，查询远程服务器进行关于代理副本的最新版本检查，然后对客户机的请求进行关于代理副本的评估时的高速缓存命中。高速缓存性能报告说明了代理提供服务的此类型的请求数，以及代理为这些请求提供服务花费的平均时间数。
- **Proxy shortcut no-check**：代理服务器和客户机都具有所请求文档的副本，代理服务器在未检查远程服务器的情况下，通知客户机其高速缓存中的文档为最新版本时的客户机高速缓存命中。高速缓存性能报告说明了代理提供服务的此类型的请求数，以及用于为这些请求提供服务的平均时间。
- **Client cache hits only**：仅客户机具有所请求文档的高速缓存副本时的客户机高速缓存命中。在此类型的请求中，代理服务器直接对客户机的 If-modified-since GET 标头进行通道操作。高速缓存性能报告说明了代理提供服务的此类型的请求数，以及用于为这些请求提供服务的平均时间。
- **Total client cache hits**：客户机高速缓存命中的总次数，以及用于为这些请求提供服务的平均时间。

代理高速缓存

客户机从代理服务器请求文档，而代理服务器的高速缓存中已包含该文档时，将发生代理高速缓存命中。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**：代理服务器查询远程服务器，从而对文档进行最新版本检查时的高速缓存命中。高速缓存性能报告说明了代理提供服务的此类型的请求数，以及用于为这些请求提供服务的平均时间。
- **Proxy cache hits without check**：代理服务器**未**查询远程服务器以进行文档的最新版本检查情况下的高速缓存命中。高速缓存性能报告说明了代理提供服务的此类型的请求数，以及用于为这些请求提供服务的平均时间。
- **pure proxy cache hits**：客户机没有所请求文档的高速缓存副本时的代理高速缓存命中。高速缓存性能报告说明了代理提供服务的此类型的请求数，以及用于为这些请求提供服务的平均时间。

组合的代理高速缓存命中次数

对于组合的代理高速缓存命中次数，报告说明了命中代理服务器的高速缓存的总次数，以及为这些请求提供服务花费的平均时间。

直接事务

直接事务是指直接从远程服务器进入代理服务器，然后到客户机，而没有发生任何高速缓存命中的事务。对于直接事务，报告将显示：

- **Retrieved documents**：直接从远程服务器检索的文档数。高速缓存性能报告说明了代理提供服务的此类型的请求数，为这些请求提供服务花费的平均时间，以及总事务的百分比。
- **Other transactions**：返回的状态码不是 200 或 304 的事务。高速缓存性能报告说明了代理提供服务的此类型的请求数，以及为这些请求提供服务花费的平均时间。
- **Total direct traffic**：请求数，包括失败的请求和成功检索的文档（直接从客户机进入远程服务器的文档）。高速缓存性能报告说明了代理提供服务的此类型的请求数，用于为这些请求提供服务的平均时间，以及总事务的百分比。

以下示例是一个高速缓存性能报告样例。

```
                    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

传送时间报告说明了有关代理服务器用于处理事务的时间的信息。此报告说明了以下分类的值：

Average transaction time：记录的所有传送时间的平均值。

Average transfer time without caching：不是从高速缓存返回的事务（即导致远程服务器作出 200 响应的那些事务）的平均传送时间。

Average with caching, without errors：所有非错误事务（即那些状态码为 2xx 和 3xx 的事务）的平均传送时间。

Average transfer time improvement：平均事务时间与进行高速缓存且没有错误时平均传送时间之差。

以下示例是一个传送时间报告样例。

```
- 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

对于进行了分析的每一小时，每小时活动报告将说明：

- 平均加载次数
- 未对远程服务器进行最新版本检查时的高速缓存命中次数
- 对远程服务器进行最新版本检查，证明文档为最新版本且在客户机高速缓存中存在时，命中代理服务器的高速缓存的次数
- 对远程服务器进行最新版本检查，证明文档为最新版本但**不**存在于客户机高速缓存中时，命中代理服务器的高速缓存的次数
- 对远程服务器进行最新版本检查，导致更新了部分文档时，命中代理服务器的高速缓存的次数
- 对远程服务器进行最新版本检查，返回了状态码为 200 的所请求文档的新副本时，命中代理服务器的高速缓存的次数
- 直接从远程服务器检索文档，没有发生代理服务器的任何高速缓存命中的请求数

▼ 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。**
   此时将显示 "Generate Report" 页面。
3. **键入服务器的名称。此名称将显示在生成的报告中。**
4. **选择报告将以 HTML 格式还是 ASCII 格式显示。**
5. **选择要分析的日志文件。**

6 **如果要将结果保存到文件中，请在 "Output File" 字段中键入一个输出文件名。**

如果保留该字段为空，报告结果将会列显到屏幕上。对于较大的日志文件，应将结果保存到文件中，因为将输出列显到屏幕上可能需要较长时间。

7 **选择是否为某些服务器统计信息生成总计。**

可以生成以下总计：

- **Total Hits**- 启用访问日志后，服务器收到的命中总数。
- **304 (Not Modified) Status Codes**- 使用所请求文档的本地副本而不是服务器返回页面的次数。
- **302 (Redirects) Status Codes**- 由于原始 URL 被转移，服务器重定向到新 URL 的次数。
- **404 (Not Found) Status Codes**- 服务器找不到所请求的文档，或者由于客户机不是授权用户，服务器未对文档提供服务的次数。
- **500 (Server Error) Status Codes**- 发生服务器相关错误的次数。
- **Total Unique URLs**- 启用访问日志后访问的唯一 URL 的数量。
- **Total Unique Hosts**- 启用访问日志后，访问了服务器的唯一主机的数量。
- **Total Kilobytes Transferred**- 启用了访问日志后，服务器传送的字节数（以 KB 为单位）。

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：**

- **Find Top** *Number* **Seconds Of Log**- 基于最近几秒钟内的信息生成统计信息。
- **Find Top** *Number* **Minutes Of Log**-
- 基于最近几分钟内的信息生成统计信息。
- **Find Top** *Number* **Hours Of Log**- 基于最近几小时内的信息生成统计信息。
- **Find** *Number* **Users (If Logged)**- 基于用户数信息生成统计信息。
- **Find Top** *Number* **Referers (If Logged)**- 基于引用站点数量信息生成统计信息。
- **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、浏览器版本以及操作系统）生成统计信息。
- **Find Top** *Number* **Miscellaneous Logged Items (If Logged)**- 基于用户数信息生成统计信息。

9 **选择是否生成列表。**

如果选择了生成列表，请指定要生成列表的项：

- **URLs Accessed**- 显示访问的 URL
- *Number* **Most Commonly Accessed URL**- 显示最常访问的 URL 或访问超过指定次数的 URL
- **URLs That Were Accessed More Than** *Number* **Times**- 显示访问超过指定次数的 URL

- **Hosts Accessing Your Server**- 显示访问了 Proxy Server 的主机
- *Number* **Hosts Most Often Accessing Your Server**- 显示访问服务器最频繁的主机，或者已访问服务器超过指定次数的主机
- **Hosts That Accessed Your Server More Than** *Number* **Times**- 显示访问服务器超过指定次数的主机

10 指定要查看结果的顺序

按照希望各部分在报告中的顺序，赋予从 1 至 3 的优先级。如果选择不生成其中的任一项的优先级，该部分将自动被忽略。这些部分包括：

- 查找总计
- 常规统计信息
- 生成列表

11 单击 "OK"。

报告将显示在新窗口中。

通过命令行运行日志分析程序

要通过命令行分析访问日志文件，请运行目录 `server-install/extras/flexanlg` 中的 `flexanlg` 工具。

要运行 `flexanlg`，请在命令提示符位置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]
```

标记了 * 的选项可以重复。

```
You can display this information online by
typing ./flexanlg -h.

-P: proxy log format                                    Default: no
-n servername: The name of the server
-x : Output in HTML                                     Default: no
-r : Resolve IP addresses to hostnames                  Default: no
-p [c,t,l]: Output order (counts, time stats, lists)  Default: ctl
-i filename: Input log file                             Default: none
-o filename: Output log file                            Default: stdout
-m filename: Meta file                                  Default: none
-c [h,n,r,f,e,u,o,k,c,z]: Count these item(s) -       Default: hnreuokc
    h: total hits
    n: 304 Not Modified status codes (Use Local Copy)
    r: 302 Found status codes (Redirects)
    f: 404 Not Found status codes (Document Not Found)
```

```
    e: 500 Server Error status codes (Misconfiguration)
    u: total unique URL's
    o: total unique hosts
    k: total kilobytes transferred
    c: total kilobytes saved by caches
    z: Do not count any items.
-t [sx,mx,hx, xx,z]: Find time stats -      Default:s5m5h10u10a10r10x10
    s(number): Find top (number) seconds of log
    m(number): Find top (number) minutes of log
    h(number): Find top (number) hours of log
    u(number): Find top (number) users of log
    a(number): Find top (number) user agents of log
    r(number): Find top (number) referers of log
    x(number): Find top (number) for miscellaneous keywords
    z: Do not find any time stats.
-l [cx,hx]: Make a list of -                          Default: c+3h5
    c(x,+x): Most commonly accessed URL's
             (x: Only list x entries)
             (+x: Only list if accessed more than x times)
    h(x,+x): Hosts (or IP addresses) most often accessing your server
             (x: Only list x entries)
             (+x: Only list if accessed more than x times)
    z: Do not make any lists.
```

查看事件 (Windows)

除了将错误记录到服务器错误日志，Proxy Server 还将严重的系统错误记录到事件查看器。事件查看器使您可以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。Proxy Server 错误包含源标签 `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，请参见系统文档。

◆ ◆ ◆ 第 10 章

10 监视服务器

本章介绍有关监视服务器的方法的信息，其中包括内置监视工具和简单网络管理协议 (Simple Network Management Protocol, SNMP)。

正如监视网络中的其他设备一样，您可以将 SNMP 与 Sun Java System 管理信息库 (management information base, MIB) 及 HP OpenView 等网络管理软件结合使用来实时监视服务器。

注 – 在 Windows 上，在安装 Proxy Server 4 之前，请确保系统中已经安装了 Windows SNMP 组件。

可以使用统计信息功能或 SNMP 来实时查看服务器的状态。如果使用的是 UNIX 或 Linux，必须配置 Proxy Server 以使用 SNMP（如果计划使用它）。

本章包含以下各节：

使用统计信息监视服务器

您可以使用统计信息功能监视服务器的当前活动。统计信息显示了服务器正在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。由于收集统计信息会增加 Proxy Server 开销，因此默认情况下禁用统计信息。如果启用统计信息，服务器将开始收集并保存统计信息。

启用统计信息后，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总计。有关这些统计信息的说明，请参见联机帮助中的 "Monitor Current Activity" 页。

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。必须启用此函数才能从 Server Manager 中查看统计信息，或使用 `perfdump` 函数生成报告。此外，还可使用 `stats-xml` 函数来启用概要分析，后者是通过使用自定义的 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概要分析后，将会对 `obj.conf` 文件中一个称为 `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"
```

此说明还会创建一条 `NameTrans` 指令，以便您从浏览器窗口访问统计信息。

```
NameTrans fn="assign-name" name="stats-xml" from="(/stats-xml|/stats-xml/.*)
```

最后，启用统计信息还会添加一条 `Service` 指令，用于在选择 `NameTrans` 指令时处理 `stats-xml` 函数。

```
<Object name="stats-xml">

Service fn="stats-xml"

</Object>
```

收集统计信息时将会更新 `obj.conf` 中的 Init 函数。因此，为使这些更改生效，必须停止并启动服务器。

下例显示了 `obj.conf` 文件中的 `stats-init`：

```
Init profiling="on" fn="stats-init" update-interval="5"
```

此外，还可以指定以下值：

- **update-interval**。统计信息的更新周期（以秒为单位）。设置越高（频率越低），性能越好。最小值为 1；默认值为 5。
- **profiling**。是否激活 NSAPI 性能概要分析。默认值为 *no*，该值可略微改善服务器性能。但是，如果通过用户界面激活统计信息，默认情况下将会启用概要分析。

可以使用以下 URL 检索 `stats-xml` 输出：

`http://`*computer_name:proxyport* `/stats-xml/proxystats.xml`

此请求将返回一个包含 Proxy Server 统计信息的 XML 页面。某些浏览器允许您在浏览器窗口中查看数据，而另外一些浏览器则要求将数据保存至外部文件，然后使用外部查看器进行查看。如果不能解析所分析数据的不同视图的统计信息，此信息的用途将不十分明显。借助第三方工具可帮助完成此过程。如果没有解析工具，最好通过 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的 `stats-xml` 统计信息的用户进行限制，应为 `/stats-xml` URI 创建一个 ACL。

此外，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 创建了一个命名的 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。您可以通过 Server Manager 或通过编辑 `obj.conf` 和 `magnus.conf` 文件来激活统计信息。为监视和性能调优目的而开发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/概要分析后，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 并单击 "Server Status" 选项卡。**
2. **单击 "Monitor Current Activity" 链接。**
   此时将显示 "Monitor Current Activity" 页面。
3. **对于 "Activate Statistics/Profiling"，选择 "Yes" 选项以启用统计信息。**
4. **单击 "OK"。**
5. **单击 "Restart Required"。**
   此时将显示 "Apply Changes" 页面。
6. **单击 "Restart Proxy Server" 按钮应用更改。**

▼ 使用 stats-xml 启用统计信息

1. **在 obj.conf 文件的默认对象下添加下行：**

```
NameTrans fn="assign-name" name="stats-xml" from="
(/stats-xml|/stats-xml/.*)"
```

2. **在 obj.conf 中添加以下 Service 函数：**

```
<Object name="stats-xml">

Service fn="stats-xml"

</Object>
```

3. **在 obj.conf 中添加 stats-init SAF。**

使用统计信息

启用统计信息后，便可获取有关服务器实例运行状况的各种信息。统计信息按功能被划分为若干方面。

在 Server Manager 中显示统计信息

本节介绍如何在 Server Manager 中查看 proxystats.xml 数据的子集。

可以采用总计图、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。

以下部分将介绍可获取的上述各项的信息类型。

连接统计信息

可从 Server Manager 获取以下连接统计信息：

- 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 获取以下 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 获取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）

服务器请求统计信息

可从 Server Manager 获取以下服务器统计信息：

- 请求总数
- 接收字节数
- 发送字节数
- 进程数
- 按 HTTP 服务器代码对请求的划分情况（还会以条形图形式显示）。例如，HTTP 服务器代码 200 表示已完成的请求

▼ 访问统计信息

1. **访问 Server Manager 并单击 "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的统计信息的间隔秒数。
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，请参见第 184 页中的 “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，并且已启用了统计信息/概要分析，将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，具体依刷新间隔的值而定。
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。有关更多信息，请参见下一节。

使用 perfdump 实用程序监视当前活动

`perfdump` 实用程序是 Proxy Server 中内置的一个服务器应用函数 (Server Application Function, SAF)，用于从 Proxy Server 内部统计信息中收集各种性能数据片断并以 ASCII 文本形式进行显示。与通过 Server Manager 获得的统计信息种类相比，使用 `perfdump` 实用程序可监视更多种统计信息。

利用 `perfdump` 可将统计信息整合起来。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准确地了解服务器的情况。

启用 perfdump 实用程序

只有在启用 `stats-xml` 函数之后，才能启用 `perfdump` SAF。

▼ 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 **将下行添加到默认对象：**

```
NameTrans fn=assign-name from="/.perf" name="perf"
```

3 **重新启动服务器软件。**

4 **通过转到** `http://` *computer_name:proxyport*`/.perf` **访问** `perfdump`。

您可以请求 `perfdump` 统计信息，并指定浏览器的自动刷新频率（以秒为单位）。以下示例将刷新频率设置为每隔 5 秒一次：

```
http:// computer_name:proxyport/.perf?refresh=5
```

`perfdump` 输出样例

以下显示了 `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

DiskCacheInfo:
------------------
Hit Ratio               0/0 (  0.00%)
Misses                  0
Cache files at startup  0
Cache files created     0
Cache files cleaned up  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，请参见《Sun ONE Web Server 6.1 Performance Tuning, Sizing, and Scaling Guide》的第 2 章中的 "Using Statistics to Tune Your Server"。

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的 perfdump 统计信息的用户进行限制，需要为 /.perf URI 创建一个 ACL。

此外，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 创建了一个命名的 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

通过性能存储桶，可以定义存储桶并将其链接到各种服务器函数。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。您可以定义两个存储桶来维护 CGI 请求和 servlet 请求各自的计数器，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 实用程序访问此信息。

存储桶中存储的信息如下：

- **存储桶名称**－此名称用于将存储桶与函数进行关联
- **说明**－对存储桶所关联的函数的描述
- **此函数的请求数**－导致此函数被调用的请求总数
- **函数的调用次数**－此数目可能与函数的请求数不一致，因为对于单个请求，某些函数可能会执行多次
- **函数延迟或分发时间**－服务器调用函数所花费的时间
- **函数时间**－函数本身所花费的时间

default-bucket 由服务器预定义，用于记录未与任何用户定义的存储桶关联的函数的统计信息。

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 186 页中的 “使用 perfdump 实用程序监视当前活动”中所述启用性能测量。

以下示例说明了如何在 magnus.conf 文件中定义新的存储桶：

```
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"
```

此示例将创建三个存储桶：acl-bucket、file-bucket 和 cgi-bucket。要将这些存储桶与函数关联，请在要测量性能的 obj.conf 函数中添加 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。

该报告包含以下信息：

- "Average"、"Total" 和 "Percent" 列给出每一个所请求的统计信息的数据。
- "Request Processing Time" 是服务器处理迄今已收到的所有请求需要的总时间。
- "Number of Requests" 是函数的请求总数。
- "Number of Invocations" 是函数的总调用次数。该值与请求数不同，因为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调用总数计算得出的。
- "Latency" 是 Proxy Server 为调用函数进行准备所花费的时间（以秒为单位）。
- "Function Processing Time" 是 Proxy Server 在函数内部花费的时间（以秒为单位）。"Function Processing Time" 和 "Total Response Time" 的百分比是参照总的 "Request Processing Time" 计算得出的。

- "Total Response Time" 为 "Function Processing Time" 和 "Latency" 之和。

以下显示了可通过 `perfdump` 获取的性能存储桶信息样例：

```
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 是一种用于交换有关网络活动的数据的协议。利用 SNMP，可在被管理的设备和网络管理站 (network management station, 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、代理服务器和网络上的其他服务器。NMS 是一种用于远程管理网络的系统。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 通常是一个具有强大功能的工作站，其中安装了一个或多个网络管理应用程序。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。此信息可能包括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。将 SNMP 与代理服务器一起使用时，此信息将通过两种代理（子代理和主代理）在 NMS 和服务器之间传输。

子代理收集有关服务器的信息，并将这些信息传送给服务器的主代理。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 可存储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。这些对象是在称为管理信息库 (management information base, MIB) 的树状结构中定义的。MIB 提供了对 Proxy Server 网络配置、状态和统计信息的访问。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、mgmt、experimental 和 private。private 子树包含 enterprises 节点。enterprises 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 节点下。Sun Java System 服务器 MIB 也位于 enterprises 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，将重要事件向 NMS 报告。NMS 也可以查询服务器的 MIB 以获取数据，或以远程方式更改 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。您可以使用 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

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（操作系统的本地代理）
- 如果是，该本地 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说明，请参见您的系统文档。

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 10–1 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部分中详细讨论。
■ 当前没有运行本地代理	1. 启动主代理。 2. 为系统上安装的每个服务器启用子代理。
■ 本地代理当前正在运行 ■ 无 SMUX ■ 不需要继续使用本地代理	1. 为 Administration Server 安装主代理时，停止本地代理。 2. 启动主代理。 3. 为系统上安装的每个服务器启用子代理。
■ 本地代理当前正在运行 ■ 无 SMUX ■ 需要继续使用本地代理	1. 安装 SNMP 代理的代理程序。 2. 启动主代理。 3. 启动 SNMP 代理的代理程序。 4. 使用主代理端口号以外的其他端口号重新启动本地代理。 5. 为系统上安装的每个服务器启用子代理。
■ 本地代理当前正在运行 ■ 支持 SMUX	1. 重新配置 SNMP 本地代理。 2. 为系统上安装的每个服务器启用子代理。

使用 SNMP 代理的代理程序 (UNIX)

如果已有一个本地代理正在运行，并且想要继续与 Proxy Server 主代理一起同时使用它，则需要使用 SNMP 代理的代理程序。在启动之前，请确保停止本地主代理。有关更多信息，请参见您的系统文档。

注 – 要使用代理的代理程序，必须先安装它然后再启动。此外，还必须使用 Proxy Server 主代理所运行端口号以外的其他端口号，重新启动本地 SNMP 主代理。

本节包括以下主题：

安装 SNMP 代理的代理程序

如果某个 SNMP 代理正在系统上运行，并且您希望继续使用本地 SNMP 守护程序，请执行以下各节中的步骤：

▼ 安装 SNMP 代理的代理程序

1. **安装 SNMP 主代理。**
   参见第 195 页中的 “安装 SNMP 主代理”。

2. **安装并启动 SNMP 代理的代理程序，然后重新启动本地 SNMP 守护程序。**
   参见第 193 页中的 “使用 SNMP 代理的代理程序 (UNIX)”。

3. **启动 SNMP 主代理。**
   参见第 196 页中的 “启用和启动 SNMP 主代理”。

4. **启用子代理。**
   参见第 201 页中的 “启用子代理”。

   要安装 SNMP 代理的代理程序，请编辑 `CONFIG` 文件，该文件位于服务器根目录的 `plugins/snmp/sagt` 中。添加 SNMP 守护程序将要侦听的端口。此文件还应包括 SNMP 代理的代理程序将要转发的 MIB 树和陷阱。

   以下示例显示了一个 `CONFIG` 文件。

```
AGENT AT PORT 1161 WITH COMMUNITY public
SUBTREES       1.3.6.1.2.1.1,
               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 SNMP 代理的代理程序

要启动 SNMP 代理的代理程序，请在命令提示符下键入：

```
# sagt -c CONFIG&
```

重新启动本地 SNMP 守护程序

启动 SNMP 代理的代理程序后，需要在 CONFIG 文件中指定的端口重新启动本地 SNMP 守护程序。要重新启动本地 SNMP 守护程序，请在命令提示符下键入：

```
# 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 本地代理

如果 SNMP 守护程序在 AIX 上运行，则它支持 SMUX。因此，无需安装主代理。但是，您必须更改 AIX SNMP 守护程序配置。

AIX 使用多个配置文件来筛选其通信。您必须编辑 snmpd.conf 文件，以便 SNMP 守护程序接受 SMUX 子代理的传入消息。有关更多信息，请参见 snmpd.conf 的联机手册页。在此文件中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 root 用户身份安装 Administration Server 实例。但是，即使是非 root 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的 SNMP 任务（例如 MIB 浏览）。

▼ 安装 SNMP 主代理

1. **以 root 用户身份登录。**
2. **检查端口 161 上是否运行有 SNMP 守护程序 (snmpd)。**
   - **如果没有运行 SNMP 守护程序，请转到第 195 页中的 " 安装 SNMP 主代理 "。**

- 如果运行有 SNMP 守护程序，请确保知道如何重新启动它以及它支持哪些 MIB 树。然后结束其进程。

3. 在 Administration Server 的 "Global Settings" 选项卡中，单击 "Set SNMP Master Agent Trap" 链接。
4. 键入正在运行网络管理软件的系统的名称。
5. 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，请参见第 200 页中的 “配置陷阱目标”。
6. 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，请参见第 200 页中的 “配置团体字符串”。
7. 单击 "OK"。
8. 在 Administration Server 的 "Global Settings" 选项卡中，单击 "Set SNMP Master Agent Community" 链接。
9. 键入主代理的团体字符串。
10. 选择团体的操作。
11. 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` 的绑定错误消息，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. 在 /*server-root* /plugins/snmp/magt/CONFIG 文件中指定所需端口。
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，主代理将在所需端口上启动。用户界面将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 守护程序 (snmpd)。

   如果运行有 SNMP 守护程序，请确保知道如何重新启动它以及它支持哪些 MIB 树。然后结束其进程。
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 守护程序 (snmpd)。

   如果运行有 SNMP 守护程序，请确保知道如何重新启动它以及它支持哪些 MIB 树。然后结束其进程。

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

`CONFIG` 文件中的 `sysContact` 和 `sysLocation` 条目用于指定 `sysContact` 和 `sysLocation` MIB-II 变量。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。

以下示例显示了一个 `CONFIG` 文件，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 RoadMountain 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 并单击 "Server Status" 选项卡。**
2. **单击 "Configure SNMP Subagent" 链接。**
   此时将显示 "Configure SNMP Subagent" 页面。
3. **在 "Master Host" 字段中，键入服务器的名称和域。**
4. **键入服务器的说明，包括操作系统信息。**
5. **键入负责该服务器的组织。**

6. **在 "Location" 字段中，键入服务器的绝对路径。**
7. **在 "Contact" 字段中，键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"。**
    此时将显示 "Apply Changes" 页面。
11. **单击 "Restart Proxy Server" 按钮应用更改。**

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，请在命令提示符下键入以下命令：

```
# magt CONFIG INIT&
```

`INIT` 文件是一个非易失性文件，其中包含 MIB-II 系统组信息（包括系统位置和联系信息）。如果 `INIT` 尚不存在，首次启动主代理时将会创建该文件。如果 `CONFIG` 文件中的管理器名称无效，将导致主代理启动进程失败。

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。并行 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。以下示例显示了一个传输映射条目：

```
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下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

1. **登录 Administration Server。**
2. **在 Administration Server 的 "Global Settings" 选项卡中，单击 "Control SNMP Master Agent" 链接。**
3. **单击 "Start"。**
   您还可以通过 "Control SNMP Master Agent" 页面来停止和重新启动 SNMP 主代理。

配置 SNMP 主代理

在主机上启用了主代理和子代理后，需要配置主机的 Administration Server。在此配置中，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 代理用于授权的一个文本字符串。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。

通过 Administration Server 中的 "Set SNMP Master Agent Community" 页面，可为 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一类消息。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。您可以通过 Proxy Server 为 SNMP 主代理配置此陷阱目标。此外，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，实际上是在编辑 `CONFIG` 文件。

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。有关更多信息，请参见第 195 页中的 “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" 页面启动子代理。有关更多信息，请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 (network management station, NMS) 发送给主代理。您可以通过 Administration Server 使用这些消息。

SNMP 以协议数据单元 (protocol data unit, PDU) 的形式交换网络信息。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）具有在需要时将报告给 NMS 的值和标题。由服务器发送给 NMS 的协议数据单元称为陷阱。以下示例说明了 GET、SET 和陷阱消息在 NMS 或服务器启动的通信中的用法。

NMS 启动的通信。NMS 可从服务器请求信息，也可更改存储在服务器 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 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：

6. 子代理通知主代理服务器已停止。
7. 主代理发送一条消息或陷阱，将该事件报告给 NMS。
8. 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 11 章

11 代理和路由 URL

本章介绍代理服务器如何处理请求，并说明如何为特定资源启用代理。本章还介绍如何配置代理服务器，以将 URL 路由至不同的 URL 或服务器。

本章包含以下各节：

为资源启用/禁用代理

您可以为资源打开或关闭代理。资源可以是单个 URL、具有某些共同特征的 URL 组或整个协议。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。通过针对该资源关闭代理，可以拒绝对一个或多个 URL 的访问。此设置可作为一种全局方式，以拒绝或允许对资源的所有访问。此外，也可以通过使用 URL 过滤器来允许或拒绝对资源的访问。有关 URL 过滤器的更多信息，请参见第 267 页中的 “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。**
   此时将显示 "Enable/Disable Proxying" 页面。
3. **选择下拉式列表中的资源，或者单击 "Regular Expression" 按钮，键入一个正则表达式，然后单击 "OK"。**
4. **可以为指定的资源选择默认设置。**
   - **Use Default Setting Derived From A More General Resource**。此资源将使用更通用资源的设置（包括此设置）。
   - **Do Not Proxy This Resource**。无法通过代理访问此资源。
   - **Enable Proxying Of This Resource**。代理允许客户机访问此资源（前提是客户机通过其他安全性和授权检查）。为资源启用代理时，将启用所有方法。系统会为该资源启用所有读取方法（包括用于 SSL 通道的 GET、HEAD、INDEX、POST 和 CONNECT 方法）和写入方法（包括 PUT、MKDIR、RMDIR、MOVE 和 DELETE 方法）。除非有任何其他安全性检查，否则所有客户机都将拥有读写访问权限。
5. **单击 "OK"。**
6. **单击 "Restart Required"。**
   此时将显示 " Apply Changes" 页面。
7. **单击 "Restart Proxy Server" 按钮应用更改。**

通过其他代理进行路由

"Set Routing Preferences" 页面用于配置代理服务器，使其使用派生默认配置或直接连接，或者通过代理阵列、ICP 邻域、其他代理服务器或 SOCKS 服务器来路由某些资源。

为资源配置路由

▼ 为资源配置路由

1 **访问 Server Manager 并单击 "Routing" 选项卡。**

2 **单击 "Set Routing Preferences" 链接。**
此时将显示 "Set Routing Preferences" 页面。

3 **选择下拉式列表中的资源，或者单击 "Regular Expression" 按钮，键入一个正则表达式，然后单击 "OK"。**

4 **为配置的资源选择所需的路由类型。**
可用选项包括：

- **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）来确定是应使用远程服务器，还是应使用其他代理。例如，如果代理将所有 `http://.*` 请求路由到另一个代理服务器，将所有 `http://www.*` 请求路由到远程服务器，则可以为 `http://www.example.*` 请求创建一个派生默认配置路由，然后这些请求将会因 `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，而不通过代理。
- **Route Through A SOCKS Server**。对指定资源的请求将通过 SOCKS 服务器进行路由。如果选择此选项，请指定代理服务器将路由经过的 SOCKS 服务器的名称（或 IP 地址）和端口号。
- **Route Through**。用于指定是否要通过代理阵列、ICP 邻域、父阵列或代理服务器进行路由。如果选择多种路由方法，代理将遵循表单上显示的分层结构：代理阵列、重定向、ICP、父阵列或其他代理。有关通过代理服务器进行路由的更多信息，请参见第 206 页中的 “链接 Proxy Server”。

  有关通过 SOCKS 服务器进行路由的信息，请参见第 206 页中的 “通过 SOCKS 服务器进行路由”。有关通过代理阵列、父阵列或 ICP 邻域进行路由的信息，请参见第 12 章。

注 – 要在 443 以外的端口上启用连接请求的路由，请在 `obj.conf` 文件中将 `ppath` 参数更改为 `connect://.*`。

---

5 **单击 "OK"。**

6 **单击 "Restart Required"。**
此时将显示 "Apply Changes" 页面。

7 **单击 "Restart Proxy Server" 按钮应用更改。**

链接 Proxy Server

可以使代理通过访问其他代理来获得某些资源，而不是访问远程服务器。链接是一种在防火墙后组织多个代理的有效方式。利用链接还可以建立分层结构的高速缓存。

▼ 通过其他 Proxy Server 进行路由

1. **访问 Server Manager 并单击 "Routing" 选项卡。**
2. **单击 "Set Routing Preferences" 链接。**
   此时将显示 "Set Routing Preferences" 页面。
3. **选择下拉式列表中的资源，或者单击 "Regular Expression" 按钮，键入一个正则表达式，然后单击 "OK"。**
4. **在该页面的 "Routing Through Another Proxy" 部分中，选择 "Route Through" 选项。**
5. **选中 "Another Proxy" 复选框。**
6. **在 "Another Proxy" 字段中，可以键入要路由经过的代理服务器的服务器名和端口号。**
   请按“服务器名:端口”方式键入服务器名和端口号。
7. **单击 "OK"。**
8. **单击 "Restart Required"。**
   此时将显示 " Apply Changes" 页面。
9. **单击 "Restart Proxy Server" 按钮应用更改。**

通过 SOCKS 服务器进行路由

如果网络上已有远程 SOCKS 服务器在运行，则可以将代理配置为与该 SOCKS 服务器连接以获得特定资源。

▼ 通过 SOCKS 服务器进行路由

1. **访问 Server Manager 并单击 "Routing" 选项卡。**
2. **单击 "Set Routing Preferences" 链接。**
   此时将显示 "Set Routing Preferences" 页面。

3 选择下拉式列表中的资源，或者单击 "Regular Expression" 按钮，键入一个正则表达式，然后单击 "OK"。

4 在该页面的 "Routing Through Another Proxy" 部分中，选择 "Route Through" 选项。

5 选择 "Route Through SOCKS Server" 选项。

6 指定代理服务器将路由经过的 SOCKS 服务器的名称（或 IP 地址）和端口号。

7 单击 "OK"。

8 单击 "Restart Required"。
此时将显示 "Apply Changes" 页面。

9 单击 "Restart Proxy Server" 按钮应用更改。

后续步骤

启用通过 SOCKS 服务器进行路由后，应使用 "SOCKS v5 Routing" 页面创建代理路由。代理路由用于确定可通过代理路由经过的 SOCKS 服务器访问的 IP 地址。代理路由还可指定该 SOCKS 服务器是否与主机直接相连。

将客户机 IP 地址转发到服务器

"Forward Client Credentials" 页面用于配置代理，使其将客户机凭证发送到远程服务器。

▼ 配置代理以发送客户机 IP 地址

1 访问 Server Manager 并单击 "Routing" 选项卡。

2 单击 "Forward Client Credentials" 链接。
此时将显示 "Forward Client Credentials" 页面。

3 选择下拉式列表中的资源，或者单击 "Regular Expression" 按钮，键入一个正则表达式，然后单击 "OK"。

4 设置以下转发选项：

- **Client IP Addressing Forwarding**。请求文档时，Proxy Server 不会将客户机的 IP 地址发送到远程服务器，而是充当客户机，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：
  - 如果代理位于内部代理链中。

- 如果客户机需访问要求知道客户机 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。

设置该选项可配置代理，使其发送客户机 IP 地址：

- **Default**。允许 Proxy Server 转发客户机的 IP 地址。
- **Blocked**。不允许代理转发客户机的 IP 地址。
- **Enabled Using HTTP Header**。您可以指定代理转发 IP 地址时使用的 HTTP 标头。默认 HTTP 标头的名称为 `Client-ip`，但您可以使用所选择的任何标头发送 IP 地址。

- **Client Proxy Authentication Forwarding**。设置该选项可配置代理，使其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**。不允许代理转发客户机的验证详细信息。
  - **Enabled Using HTTP Header**。您可以指定代理转发验证详细信息时使用的 HTTP 标头。
- **Client Cipher Forwarding**。设置该选项可配置代理，使其将客户机的 SSL/TLS 加密算法套件的名称发送到远程服务器。
  - **Default**。允许 Proxy Server 将客户机的 SSL/TLS 加密算法套件的名称转发到远程服务器。
  - **Blocked**。不允许代理将客户机的 SSL/TLS 加密算法套件的名称转发到远程服务器。
  - **Enabled Using HTTP Header**。您可以指定代理在将客户机的 SSL/TLS 加密算法套件的名称转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头的名称为 `Proxy-cipher`，但您可以使用所选择的任何标头发送客户机的 SSL/TLS 加密算法套件的名称。
- **Client Keysize Forwarding**。设置该选项可配置代理，使其将客户机的 SSL/TLS 密钥的大小发送到远程服务器。
  - **Default**。允许 Proxy Server 将客户机的 SSL/TLS 密钥的大小转发到远程服务器。
  - **Blocked**。不允许代理将客户机的 SSL/TLS 密钥的大小转发到远程服务器。
  - **Enabled Using HTTP Header**。您可以指定代理在将客户机的 SSL/TLS 密钥的大小转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头的名称为 `Proxy-keysize`，但您可以使用所选择的任何标头发送客户机的 SSL/TLS 密钥的大小。
- **Client Secret Keysize Forwarding**。设置该选项可配置代理，使其将客户机的 SSL/TLS 私钥的大小发送到远程服务器：
  - **Default**。允许 Proxy Server 将客户机的 SSL/TLS 私钥的大小转发到远程服务器。
  - **Blocked**。不允许代理将客户机的 SSL/TLS 私钥的大小转发到远程服务器。

- **Enabled Using HTTP Header**。您可以指定代理在将客户机的 SSL/TLS 私钥的大小转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头的名称为 `Proxy-secret-keysize`，但您可以使用所选择的任何标头发送客户机的 SSL/TLS 私钥的大小。

- **Client SSL Session ID Forwarding**。设置该选项可配置代理，使其将客户机的 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**。不允许代理将客户机的 SSL/TLS 会话 ID 转发到远程服务器。
  - **Enabled Using HTTP Header**。您可以指定代理在将客户机的 SSL/TLS 会话 ID 转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头的名称为 `Proxy-ssl-id`，但您可以使用所选择的任何标头发送客户机的 SSL/TLS 会话 ID。
- **Client Issuer DN Forwarding**。设置该选项可配置代理，使其将客户机的 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 证书颁发者的标识名转发到远程服务器。
  - **Blocked**。不允许代理将客户机的 SSL/TLS 证书颁发者的标识名转发到远程服务器。
  - **Enabled Using HTTP Header**。您可以指定代理在将客户机的 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 标头的名称为 `Proxy-issuer-dn`，但您可以使用所选择的任何标头发送客户机的 SSL/TLS 证书颁发者的名称。
- **Client User DN Forwarding**。设置该选项可配置代理，使其将客户机的 SSL/TLS 证书主题的标识名发送到远程服务器。
  - **Default**。允许 Proxy Server 将客户机的 SSL/TLS 证书主题的标识名转发到远程服务器。
  - **Blocked**。不允许代理将客户机的 SSL/TLS 证书主题的标识名转发到远程服务器。
  - **Enabled Using HTTP Header**。您可以指定代理在将客户机的 SSL/TLS 证书主题的标识名转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头的名称为 `Proxy-user-dn`，但您可以使用所选择的任何标头发送客户机的 SSL/TLS 证书主题的名称。
- **Client SSL/TLS Certificate Forwarding**。设置该选项可配置代理，使其将客户机的 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**。不允许代理将客户机的 SSL/TLS 证书转发到远程服务器。
  - **Enabled Using HTTP Header**。您可以指定代理在将客户机的 SSL/TLS 证书转发到远程服务器时使用的 HTTP 标头。默认 HTTP 标头的名称为 `Proxy-auth-cert`，但您可以使用所选择的任何标头发送客户机的 SSL/TLS 证书。

- **Client Cache Information Forwarding**。选择以下选项之一可配置代理，使其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**。您可以指定代理在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 标头的名称为 `Cache-info`，但您可以使用所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**。设置该选项可配置代理，使其发送 HTTP 请求。
  - **User**。指定要验证的用户。
  - **Password**。指定用户密码。
  - **Using HTTP Header**。您可以指定代理在传送凭证时使用的 HTTP 标头。

5 **单击 "OK"。**

6 **单击 "Restart Required"。此时将显示 "Apply Changes" 页面。**

7 **单击 "Restart Proxy Server" 按钮应用更改。**

允许客户机检查 IP 地址

为了维护网络安全，客户机可能具有将访问权限仅限于某些 IP 地址的功能。为使客户机使用此功能，代理服务器提供了对检查 Java IP 地址的支持。此支持允许客户机向代理服务器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原始服务器的 IP 地址。代理服务器会将该 IP 地址附加在标头中。当客户机知道原始服务器的 IP 地址后，即可显式指定对以后的连接使用同一 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。**
此时将显示 "Check Java IP Address" 页面。

3 **选择下拉式列表中的资源，或者单击 "Regular Expression" 按钮，键入一个正则表达式，然后单击 "OK"。**

4 **启用或禁用 Java IP 地址检查，或者使用其默认配置。**

注 – 默认选项使用更通用模板派生的默认配置。通用模板使用一个较短且匹配的正则表达式来确定是应启用，还是应禁用 Java IP 地址检查。

5 **单击 "OK"。**

6 **单击 "Restart Required"。**
此时将显示 "Apply Changes" 页面。

7 **单击 "Restart Proxy Server" 按钮应用更改。**

客户机自动配置

如果代理服务器支持多个客户机，则可能需要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，用于确定访问各种 URL 时浏览器所使用的代理（如果有）。有关此功能的更多信息，请参见第 17 章。

设置网络连通性模式

您可以将代理服务器计算机连接到网络，也可以将其与网络断开连接。利用此功能，可轻松将代理安装在可用于演示的便携式计算机上。

当代理与网络断开连接时，文档将直接从高速缓存返回。代理不会执行最新性检查，因此文档检索速度相当快。但是，文档可能不是最新的。有关高速缓存的更多信息，请参见第 12 章。

如果未连接到网络，连接将始终不会挂起，这是因为代理服务器知道不存在网络连接，因此也就决不会尝试连接远程服务器。在网络关闭但代理服务器计算机仍在运行时，可以使用此无网络设置。如果运行与网络断开连接的代理，则意味着最终将从高速缓存访问过时的数据。而且，在无网络条件下运行也消除了使用代理安全性功能的必要性。

Proxy Server 提供了以下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。
- 正常模式是代理的正常操作模式。如果文档不在高速缓存中，代理将从内容服务器检索文档。如果文档在高速缓存中，则可能会对照内容服务器对其进行检查，以确定其是否为最新文档。如果高速缓存的文件已更改，将使用当前副本进行替换。
- 快速演示模式用于在网络可用时提供流畅的演示。如果在高速缓存中找到文档，将不会与内容服务器联系，甚至不会去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延迟。如果文档不在高速缓存中，则会从内容服务器检索并将其高速缓存。与正常模式相比，快速演示模式的延迟更少，但由于服务器在具有文档副本后不会对文档执行最新性检查，因此有时可能会返回过时的数据。

- 无网络模式是专为便携式计算机未连接网络时而设计的。如果文档在高速缓存中，代理将返回文档；如果文档不在高速缓存中，代理将返回错误。代理始终不会尝试与内容服务器联系，这样可以防止代理在试图获取不存在的连接时超时。

▼ 更改 Proxy Server 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。此时将显示 "Set Connectivity Mode" 页面。**
3. **选择下拉式列表中的资源，或者单击 "Regular Expression" 按钮，键入一个正则表达式，然后单击 "OK"。**
4. **选择所需模式。**
5. **单击 "OK"。**
6. **单击 "Restart Required"。此时将显示 "Apply Changes" 页面。**
7. **单击 "Restart Proxy Server" 按钮应用更改。**

更改默认的 FTP 传输模式

FTP 提供两种不同的方式在 FTP 服务器与客户机（充当客户机的代理）之间建立数据连接。这两种模式分别称为 PASV 和 PORT 模式 FTP。

- *Passive Mode (PASV)*。从代理服务器启动数据连接，然后 FTP 服务器接受连接。这对于运行代理服务器的站点更安全，因为服务器不必接受传入连接。
- *Active Mode (PORT)*。由远程 FTP 服务器启动数据连接，然后代理接受传入连接。如果代理服务器位于防火墙内，防火墙可能会禁止从 FTP 服务器传入的 FTP 数据连接，这意味着 PORT 模式可能无效。

某些 FTP 站点会运行防火墙，从而使 PASV 模式对代理服务器不起作用。因此，可将代理服务器配置为使用 PORT 模式 FTP。您可以对整个服务器启用 PORT 模式，也可以仅对特定 FTP 服务器启用此模式。

如果远程 FTP 服务器不支持 PASV 模式，则即使启用了 PASV 模式，代理服务器也将使用 PORT 模式。

如果代理服务器位于防火墙之后，使 PORT 模式 FTP 不起作用，则无法启用 PORT 模式。如果为资源选择默认模式，代理服务器将使用更通用资源的模式。如果未指定任何模式，则会使用 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。此时将显示 "Set FTP Mode" 页面。
3. 选择下拉式列表中的资源，或者单击 "Regular Expression" 按钮，键入一个正则表达式，然后单击 "OK"。
4. 选择 FTP 传输模式。
5. 单击 "OK"。
6. 单击 "Restart Required"。此时将显示 "Apply Changes" 页面。
7. 单击 "Restart Proxy Server" 按钮应用更改。

指定 SOCKS 名称服务器 IP 地址

如果将代理配置为通过 SOCKS 服务器建立外发连接，可能需要显式指定要用于 SOCKS 的名称服务器的 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。
   此时将显示 "Set SOCKS Name Server" 页面。
3. 在相应字段中键入 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 IP 地址的功能以前只能通过 SOCKS_NS 环境变量访问。如果设置该环境变量并使用 "SOCKS Name Server Setting" 表单来指定名称服务器 IP 地址，代理将使用表单中指定的 IP 地址，而不会使用该环境变量。

---

5 **单击 "Restart Required"。**
此时将显示 "Apply Changes" 页面。

6 **单击 "Restart Proxy Server" 按钮应用更改。**

配置 HTTP 请求负载平衡

"Configure HTTP Request Load Balancing" 页面用于在指定的原始服务器中分配负载。

▼ 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。**
此时将显示 "Configure HTTP Request Load Balancing" 页面。

3 **选择下拉式列表中的资源，或者单击 "Regular Expression" 按钮，键入一个正则表达式，然后单击 " OK"。**

4 **在 "Server" 字段中指定原始服务器的 URL。如果给定多个服务器参数，Proxy Server 将在指定的原始服务器中分配负载。**

5 **在 "Sticky Cookie" 字段中指定 cookie 的名称，当其出现在响应中时，将导致后续请求停留在该原始服务器中。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，且其值中包含冒号并后接路由 ID，则请求将始终发送到由该路由 ID 标识的原始服务器中。默认值为** `jsessionid`**。**

7 **在 "Route Header" 字段中，指定用于将路由 ID 传送至原始服务器的 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 在响应中遇到粘性 cookie 时生成的 cookie 的名称。**
默认值为 `JROUTE`。

9 **设置 "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 **设置 "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 **设置 "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 **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"。**
此时将显示 "Apply Changes" 页面。

15 **单击 "Restart Proxy Server" 按钮应用更改。**

管理 URL 和 URL 映射

使用 Server Manager 可将 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 访问代理时，代理将从镜像服务器（而非 URL 中指定的服务器）检索请求的文档。客户机绝不会知道请求将转到其他服务器。您也可以重定向 URL。在这种情况下，代理仅将重定向的 URL 返回客户机，而不返回文档，因此客户机随后可以请求新文档。使用映射还可以将 URL 映射到文件，如 PAC 和 PAT 映射。

创建和修改 URL 映射

要映射 URL，需指定 URL 前缀以及映射目标位置。以下部分介绍了各种类型的 URL 映射。您可以创建以下类型的 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发送重定向的响应而非文档时，反向代理将使用这些映射。有关更多信息，请参见第 14 章。
- 正则表达式将与表达式匹配的所有 URL 都映射到单个 URL。例如，可以将与 .*job.* 匹配的所有 URL 映射到一个特定 URL（此 URL 可能会解释代理服务器为何不允许用户转到特定 URL）。
- 客户机自动配置将 URL 映射到代理服务器上存储的特定 `.pac` 文件。有关自动配置文件的更多信息，请参见第 17 章。
- 代理阵列表 (Proxy array table, PAT) 将 URL 映射到代理服务器上存储的特定 `.pat` 文件。只应从主代理创建此类映射。有关 PAT 文件和代理阵列的更多信息，请参见第 252 页中的 “通过代理服务器阵列进行路由选择”。

访问 URL 的客户机将被发送到同一服务器或不同服务器的不同位置。当资源已移动，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时，此功能会很有用。

例如，假定您有一个称为 hi.load.com 的高负载 Web 服务器，您想要将其镜像到另一个称为 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 HTTP 请求中非法的字符。

请勿在前缀中使用结尾斜杠！

▼ 创建 URL 映射

1. **访问 Server Manager 并单击 "URL" 选项卡。**
2. **单击 "Create Mapping" 链接。**
   此时将显示 "Create Mapping" 页面。
3. **选择要创建的映射类型。**
   - **Regular Mappings**。如果选择此选项，该页面的下部将显示以下选项：
     - *Rewrite Host*。指示是否重写 Host HTTP 标头，以匹配 to 参数指定的主机。
     - **Reverse Mappings**。将一个重定向的 URL 前缀映射到另一个 URL 前缀。如果选择此选项，该页面的下部将显示以下选项：
       - *Rewrite Location*。指示是否应重写 Location HTTP 响应标头。
       - *Rewrite Content Location*。指示是否应重写 Content-location HTTP 响应标头。
       - *Rewrite Headername*。选中该复选框以指示是否应重写 *headername* HTTP 响应标头，其中 *headername* 是用户定义的标头名称。

     Regular Expressions。将与表达式匹配的所有 URL 都映射到单个 URL。有关正则表达式的更多信息，请参见第 16 章。
   - **Client Autoconfiguration**。将 URL 映射到 Proxy Server 上存储的特定 .pac 文件。有关自动配置文件的更多信息，请参见第 17 章。
   - **Proxy Array Table (PAT)**。将 URL 映射到 Proxy Server 上存储的特定 .pat 文件。只应从主代理创建此类映射。有关 PAT 文件和代理阵列的更多信息，请参见第 12 章中的“通过代理阵列进行路由”。
4. **键入映射源前缀。**
   对于正则映射和反向映射，此前缀应是要替代的 URL 的一部分。

   对于正则表达式映射，该 URL 前缀应是要匹配的所有 URL 的正则表达式。如果还为映射选择了模板，则该正则表达式将仅适用于模板的正则表达式中的 URL。

   对于客户机自动配置映射和代理阵列表映射，该 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，此值应是指向代理服务器硬盘中的 `.pac` 文件的绝对路径。对于代理阵列表映射，此值应是指向主代理本地磁盘中的 `.pat` 文件的绝对路径。
6. **从下拉式列表中选择模板名称，或者如果不想应用模板，则将该值保留为 "NONE"。**
7. **单击 "OK" 创建映射。**
8. **单击 "Restart Required"。**
   此时将显示 "Apply Changes" 页面。
9. **单击 "Restart Proxy Server" 按钮应用更改。**

▼ 更改现有映射

1. **访问 Server Manager 并单击 "URL" 选项卡。**
2. **单击 "View/Edit Mappings" 链接。**
   此时将显示 "View/Edit Mappings" 页面。
3. **单击要修改的映射旁边的 "Edit" 链接。可以编辑受该映射影响的前缀、映射的 URL 和模板。单击 "OK" 确认所做更改。**
4. **单击 "Restart Required"。此时将显示 "Apply Changes" 页面。**
5. **单击 "Restart Proxy Server" 按钮应用更改。**

▼ 删除映射

1. **访问 Server Manager 并单击 "URL" 选项卡。**
2. **单击 "View/Edit Mappings" 链接。**
   此时将显示 "View/Edit Mappings" 页面。
3. **选择要删除的映射，然后单击该映射旁边的 "Remove" 链接。**
4. **单击 "Restart Required"。此时将显示 "Apply Changes" 页面。**
5. **单击 "Restart Proxy Server" 按钮应用更改。**

重定向 URL

可以配置代理服务器，使其向客户机返回重定向的 URL，而不是获取并返回文档。利用重定向，客户机可得知初始请求的 URL 已被重定向到其他 URL。通常，客户机会立即请求重定向的 URL。Netscape Navigator 会自动请求重定向的 URL。用户不必再次显式请求相应文档。

在要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 并单击 "URL" 选项卡。**
2. **单击 "Redirect URLs" 链接。此时将显示 "Redirect URLs" 页面。**
3. **键入作为 URL 前缀的源 URL。**
4. **键入要重定向到的 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" 字段旁边的单选按钮，然后键入一个 URL 前缀。
   - 如果选择使用固定的 URL，请选择 "Fixed UR" 字段旁边的单选按钮，然后键入一个固定的 URL。
5. **单击 "OK"。**
6. **单击 "Restart Required"。**
   此时将显示 "Apply Changes" 页面。
7. **单击 "Restart Proxy Server" 按钮应用更改。**

◆ ◆ ◆ 第 12 章

12 高速缓存

本章介绍了 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。

本章包含以下各节：

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，代理服务器会将文档从远程服务器复制到其本地高速缓存目录结构中，同时会将该文档发送给客户机。

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该文档，如下图所示。如果代理服务器确定文件不是最新的，则代理服务器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。

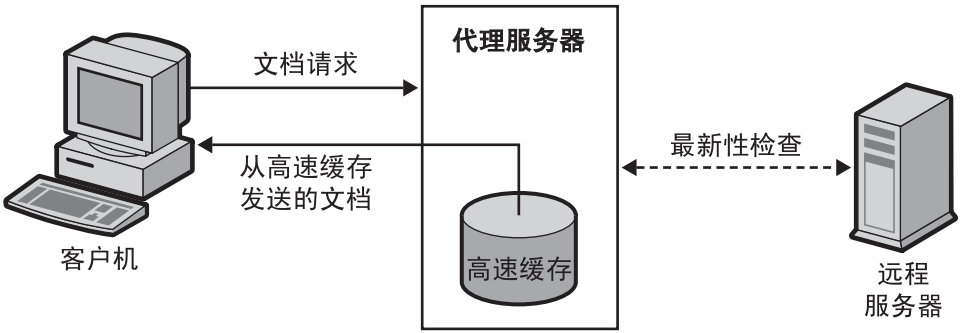

图 12–1 代理服务器文档检索

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 会定期自动清理高速缓存，以确保高速缓存不会混乱地堆积过时的文档。

了解高速缓存结构

高速缓存由一个或多个分区组成。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，请至少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，您可以独立于其他所有分区来启用、禁用和配置某个分区。

在一个位置存储大量高速缓存的文件会降低性能，因此，请在每个分区中创建若干个目录或段。段是高速缓存结构中位于分区下的下一个级别。高速缓存跨所有分区最多可以有 256 个段。高速缓存段的数量必须为 2 的幂（例如，1、2、4、8、16、...、256）。

高速缓存分层结构中的最低级别是子段。子段是指段内的目录。每个段有 64 个子段。高速缓存的文件存储在子段，即高速缓存的最低级别中。

下图显示了一个含有分区和段的高速缓存结构示例。在此图中，高速缓存目录结构将整个高速缓存划分为三个分区。第一个分区包含四个高速缓存段，后两个分区各包含两个段。

每个高速缓存段的表示方法是：以 "s" 代表段，其后是段号。对于显示为 s3.4 的段，3 表示高速缓存段数 ($2^3 = 8$) 中 2 的幂次，4 表示段号（共 8 个段，分别标记为 0 到 7）。因此，s3.4 代表 8 个段中的第 5 个段。

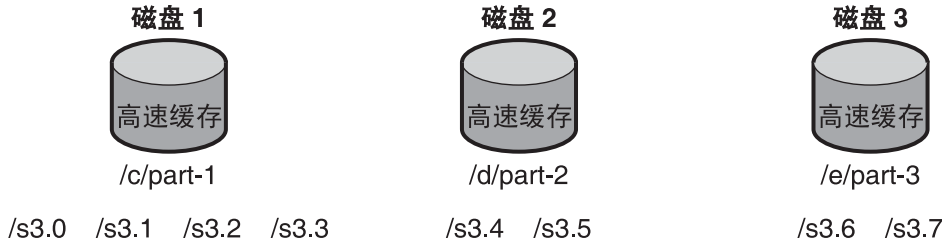

图 12–2 高速缓存结构示例

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。该算法可以确保在各个目录中均匀分布文档。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 算法（信息-摘要算法 5）将 URL 简化为 16 字节的二进制数据，并使用此数据的 8 个字节来计算用于在高速缓存中存储文档的 16 字符十六进制文件名。

设置高速缓存细节

通过设置高速缓存细节，您可以启用高速缓存并控制 Proxy Server 将要高速缓存的协议类型。高速缓存细节包括以下各项：

- 是启用还是禁用高速缓存
- 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报告回给远程服务器

注 – 设置大型高速缓存的细节很耗时，并且可能会导致管理界面超时。因此，如果您要创建大型高速缓存，请使用命令行实用程序来设置高速缓存细节。有关高速缓存命令行实用程序的更多信息，请参见第 239 页中的 “使用高速缓存命令行界面”。

▼ 设置高速缓存细节

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**

2. **单击 "Set Cache Specifics" 链接。**
   将会显示 "Set Cache Specifics" 页面。

3. **通过选择相应的选项，可以启用或禁用高速缓存。**
   默认情况下，将启用高速缓存。

4. **提供工作目录。**
   默认情况下，工作目录位于服务器实例下。此位置可以更改。有关更多信息，请参见第 223 页中的 “创建高速缓存工作目录”。

5. **单击分区配置链接。**
   将会显示 "Add/Edit Cache Partitions" 页面。您可以添加新的高速缓存分区或编辑现有高速缓存分区。高速缓存大小是指允许高速缓存增长到的最大大小。高速缓存的最大大小为 32 GB。有关更多信息，请参见第 223 页中的 “设置高速缓存大小”。

6. **单击高速缓存容量配置链接。**
   将会显示 "Set Cache Capacity" 页面。您可以在 "Set Cache Capacity" 页面上设置高速缓存容量。

7. **选择 "Cache HTTP" 以启用对 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，请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，请参见第 224 页中的 “高速缓存 HTTP 文档”。可用选项包括：

   - 选择 "Always Check That The Document Is Up To Date" 选项可以确保 HTTP 文档总是最新的。
     - 从 "Check Only If Last Check More Than" 下拉式列表中选择小时数，可以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**。它是由原始服务器随文档一同发送的上次修改标头。
       - **Use Only Explicit Expiration Information**。代理服务器使用到期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" 选项可防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报告回给远程服务器。

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相应的值来设置时间间隔。有关更多信息，请参见第 225 页中的“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相应的值来设置时间间隔。有关更多信息，请参见第 225 页中的“高速缓存 FTP 和 Gopher 文档”。

10 单击 "OK"。

11 单击 "Restart required"。将会显示 "Apply Changes" 页面。

12 单击 "Restart Proxy Server" 按钮以应用更改。

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" 页面中指定的工作目录通常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。如果更改高速缓存目录名称或将其移动到其他位置，必须为代理服务器提供新位置。

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分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，因为它是高速缓存可以增长到的最大大小。所有分区大小的总和必须小于或者等于高速缓存大小。

可供代理服务器高速缓存使用的磁盘空间量对高速缓存性能具有相当大的影响。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。这些活动会降低性能。

高速缓存大小较大时效率会更高，因为高速缓存的文档越多，网络通信流量负载就越小，代理服务器提供的响应速度就越快。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使用而已。

还可以将高速缓存分割到多个磁盘分区中。

高速缓存 HTTP 文档

HTTP 文档提供了其他协议的文档所不具备的高速缓存特性。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。

注 – Proxy Server 4 不支持对 HTTPS 文档进行高速缓存。

所有 HTTP 文档都有一个描述性标头部分，Proxy Server 使用它来比较和评估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 文档执行最新版本检查时，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一个请求，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，可以使用 Proxy Server 为 HTTP 文档设置 "Cache Expiration" 设置。"Cache Expiration" 设置为代理服务器提供相关信息，以便评估在向服务器发送请求之前是否需要对 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 文档上次修改日期进行此评估。

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执行最新性检查（这会覆盖失效期设置），还是等待特定时间段后再进行检查。下表显示了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并节约带宽。

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“到期”标头	时间间隔到期时执行最新性检查
	使用文档的上次修改标头进行估计	估计值和到期标头中的较小值*

注 – * 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过时数据。

设置 HTTP 高速缓存刷新间隔

如果您决定要让 Proxy Server 对 HTTP 文档进行高速缓存，请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，合理的刷新间隔为四到八小时。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机中单击 "Reload" 按钮来强制刷新。此操作使代理服务器强制对远程服务器执行最新性检查。

可以在 "Set Cache Specifics" 页面或 "Set Caching Configuration" 页面中为 HTTP 文档设置刷新间隔。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上次修改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。使用显式到期标头的 HTTP 文档并不很多，因此应根据上次修改标头进行估计。

如果决定根据上次修改标头对 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，然后将生成的数值与上次执行最新性检查到现在为止的时间进行比较。如果此数值小于这段时间间隔，则表明文档尚未过期。小数越小，将会使代理服务器更为频繁地检查文档。

例如，假设有一个文档，其上次更改时间是十天以前。如果将上次修改因子设置为 0.1，代理服务器将把该因子理解为文档可能会在一天 (10 * 0.1 = 1) 内保持不变。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更频繁地执行更新的那个值（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" 页面中设置 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”）。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 不包含用于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高速缓存刷新间隔。高速缓存刷新间隔是指 Proxy Server 从远程服务器检索文档最新版本前等待的时间长度。如果不设置高速缓存刷新间隔，即使高速缓存中的文档版本是最新的，代理服务器也将检索这些文档。

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。如果该时间间隔足够短（例如，几个小时），则会在显著提高响应速度的同时，也会消除大部分此类风险。

可以在 "Set Cache Specifics" 页面或 "Set Caching Configuration" 页面中设置 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，请参见第 221 页中的 “设置高速缓存细节”。有关使用 "Set Caching Configuration" 页面的更多信息，请参见第 229 页中的 “配置高速缓存”。

注 – 如果 FTP 和 Gopher 文档差异很大（有些经常发生变化，有些则很少发生变化），请使用 "Set Caching Configuration" 页面为每种文档创建单独的模板（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，则可能需要更改或添加分区。

▼ 添加高速缓存分区

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**
2. **单击 "Add/Edit Cache Partitions" 链接。**
   将会显示 "Add/Edit Cache Partitions" 页面。
3. **单击 "Add Cache Partition" 按钮。**
   将会显示 "Cache Partition Configuration" 页面。
4. **为新分区提供适当的值。**
5. **单击 "OK"。**
6. **单击 "Restart required"。**
   将会显示 "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，然后单击 "Caching" 选项卡。**
2. **单击 "Add/Edit Cache Partitions" 链接。**
   将会显示 "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"。**
   将会显示 "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直接相关。容量越大，分层结构就越大。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，将会创建 256 个段。

▼ 设置高速缓存容量

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**
2. **单击 "Set Cache Capacity" 链接。**
   将会显示 "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"。**
   将会显示 "Apply Changes" 页面。

6 **单击 "Restart Proxy Server" 按钮以应用更改。**

管理高速缓存段

代理服务器高速缓存被分为一个或多个高速缓存段。最多可以有 256 个段。高速缓存段数必须是 2 的乘方（例如，1、2、4、8、16、...、256）。最大容量为 32 GB（最优），具有 256 个高速缓存段。

如果选用容量为 500 MB 的高速缓存，安装程序将创建 4 个高速缓存段 (500 d6 125 = 4)；如果选择容量为 2 GB 的高速缓存，安装程序将创建 16 个段 (2000 d6 125 = 16)。为便于获得段数，选择 125 MB 作为每个段的最优值。段数越多，存储和分布的 URL 数就越大。

▼ 管理高速缓存段

1 **访问 Server Manager，然后单击 "Caching" 选项卡。**

2 **单击 "Manage Sections" 链接。**
将会显示 "Manage Sections" 页面。

3 **更改表中的信息。**
可以在现有分区之间移动段。

4 **单击 "OK"。**

5 **单击 "Restart required"。**
将会显示 "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

可以使用高速缓存垃圾收集器来删除高速缓存中的文件。可以在自动模式或显式模式下进行垃圾收集。显式模式由管理员在外部进行调度。选择其中一种模式，然后单击 "OK"。单击 "Restart required"。将会显示 "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。

▼ 设置垃圾收集

1 **访问 Server Manager，然后单击 "Caching" 选项卡。**

2 **单击 "Schedule Garbage Collection" 链接。**
将会显示 "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"。**
将会显示 "Apply Changes" 页面。

7 **单击 "Restart Proxy Server" 按钮以应用更改。**

配置高速缓存

可以为与您指定的正则表达式模式匹配的 URL 指定若干个配置参数值。此功能使您能够基于高速缓存的文档类型对代理服务器高速缓存进行精细控制。配置高速缓存时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
- 客户机中断的高速缓存行为
- 与原始服务器之间的失败连接的高速缓存行为

注 – 如果将某个特定资源的高速缓存默认值设置为 "Derived configuration" 或 "Don't cache"，则 "Set Caching Configuration" 页面中不会显示高速缓存配置选项。不过，如果为某个资源选择了高速缓存默认值 "Cache"，则可以指定若干个其他配置项。

▼ 配置高速缓存

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**
2. **单击 "Set Caching Configuration" 页面。**
   将会显示 "Set Caching Configuration" 页面。
3. **从下拉式列表中选择资源，或单击 "Regular Expression" 按钮，键入正则表达式，然后单击 "OK"。**
4. **更改配置信息。**
5. **单击 "OK"。**
6. **单击 "Restart required"。**
   将会显示 "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

以下各节包含的信息将帮助您确定最适合需要的配置。

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，要让服务器自动高速缓存域 `company.com` 中的所有文档，可以创建以下正则表达式

`[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。

注 – 如果将某个特定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，如果为某个资源选择了高速缓存默认值 "Cache"，则可以指定若干个其他配置项。有关这些项的列表，请参见第 229 页中的 “配置高速缓存”。

也可以设置 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。Proxy Server 可对高速缓存中的文件进行标记，以便它可以在用户请求这些文件时要求从远程服务器进行验证。

因为 Proxy Server 无法确定远程服务器如何进行验证，而且它没有用户 ID 或密码列表，所以它只会在每次收到对要求进行验证的文档的请求时，强制对远程服务器进行最新性检查。因此，用户必须键入 ID 和密码以获得对文件的访问权限。如果用户先前已在浏览器会话中访问过该服务器，则浏览器会自动发送验证信息，而不提示用户。

如果不启用对要求进行验证的页面进行高速缓存，代理服务器将不会高速缓存这些页面（这是默认行为）。

高速缓存查询

高速缓存的查询仅适用于 HTTP 文档。您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，其重复的可能性越小，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），响应必须至少有上次修改标头。这就要求查询引擎指出可以高速缓存查询结果文档。
- 如果存在上次修改标头，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，它应返回到期标头。

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，则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。在这种情况下，您可能只需高速缓存较大的文件。您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

最新性检查策略可以确保 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

可以使用上次修改因子或显式失效期信息来设置失效期策略。

设置客户机中断的高速缓存行为

如果在仅检索了部分文档时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，代理服务器将终止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

如果由于原始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。此行为避免了重复高速缓存。例如，如果用户从本地服务器请求了 `http://machine/filename.html` 和 `http://machine.example.com/filename.html`，则这两个 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很快，从而没有必要高速缓存它们。

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，然后单击 "Caching" 选项卡。**
2. **单击 "Cache Local Hosts" 链接。**
   将会显示 "Cache Local Hosts" 页面。
3. **从下拉式列表中选择资源，或单击 "Regular Expression" 按钮，键入正则表达式，然后单击 "OK"。**
   有关正则表达式的更多信息，请参见第 16 章。
4. **单击 "enabled" 按钮。**
5. **单击 "OK"。**

6 **单击 "Restart required"。**
将会显示 "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，启用文件高速缓存。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 发行版并未实现该功能

▼ 配置文件高速缓存

1 **在 Server Manager 中，单击 "Caching" 选项卡。**

2 **单击 "File Cache Configuration" 链接。**
将会显示 "File Cache Configuration" 页面。

3 **选择 "Enable File Cache"（如果尚未选择）。**

4 **选择是否传送文件。**
启用 "Transmit File" 后，服务器将在文件高速缓存中高速缓存文件的已打开文件描述符，而不是文件内容。`PR_TransmitFile` 用于将文件内容发送到客户机。启用 "Transmit File" 后，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 中启用 "Transmit File"，而在 UNIX 中则将其禁用。在 UNIX 中，应该只为对 PR_TransmitFile 具有本机 OS 支持的平台启用 "Transmit File"，此类平台目前包括 HP-UX 和 AIX。建议不要在 UNIX/Linux 平台上使用此选项。

5 **键入散列表的大小。**
默认大小为最大文件数的两倍加 1。例如，如果最大文件数设置为 1024，则默认的散列表大小为 2049。

6 **键入有效高速缓存条目的最长生存期（以秒为单位）。**
默认设置为 30。此设置用于控制高速缓存文件后，可以继续使用高速缓存的信息的时间长度。存在时间久于 MaxAge 的条目将由同一文件的新条目替换（如果在高速缓存中引用同一文件）。请根据内容是否会定期更新来设置最长生存期。例如，如果内容一

天定期更新四次，您可以将最长生存期设置为 21600 秒（6 小时）。否则，可考虑将最长生存期设置为修改文件之后希望处理以前版本的内容文件的最长时间。

7 **键入要高速缓存的最大文件数。**

默认设置为 1024。

8 **键入中等和小文件大小限制（以字节为单位）。**

默认情况下，将 "Medium File Size Limit" 设置为 537600，将 "Small File Size Limit" 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。中等文件的内容通过将文件映射到虚拟内存（仅限于 UNIX/Linux 平台）来进行高速缓存。小文件的内容通过分配堆空间并将文件读入其中来进行高速缓存。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（以字节为单位）。默认情况下，将此大小设置为 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（以字节为单位）。对于 UNIX/Linux，默认情况下将此大小设置为 1048576。

10 **单击 "OK"。**

11 **单击 "Restart required"。**

将会显示 "Apply Changes" 页面。

12 **单击 "Restart Proxy Server" 按钮以应用更改。**

查看 URL 数据库

您可以查看所有已记录并按照访问协议和站点名称分组的高速缓存 URL 的名称和属性。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，然后单击 "Caching" 选项卡。
2. 单击 "View URL Database" 链接。
   将会显示 "View URL Database" 页面。
3. 单击 "Regenerate" 按钮以生成最新的高速缓存的 URL 列表。
4. （可选）要查看特定 URL 的信息，请在 "Search" 字段中键入 URL 或正则表达式，然后单击 "Search" 按钮。
5. 要查看按域名和主机分组的高速缓存数据库信息：
   a. 从列表中选择域名。
      将会显示该域中主机的列表。单击某个主机的名称，将会显示 URL 列表。
   b. 单击某个 URL 的名称。
      将会显示有关该 URL 的详细信息。
   c. 单击某个 URL 的名称以查看有关该 URL 的详细信息。

▼ 废止效或删除高速缓存的 URL

1. 访问 Server Manager，然后单击 "Caching" 选项卡。
2. 单击 "View URL Database" 链接。
   将会显示 "View URL Database" 页面。
3. 单击 "Regenerate" 按钮以生成高速缓存数据库的快照。
   此快照构成了执行其余步骤的基础。
4. 如果您知道要废止或删除的特定 URL，请在 "Search" 字段中键入该 URL 或与该 URL 匹配的正则表达式，然后单击 "Search" 按钮。
5. 如果您要处理按域名和主机分组的 URL：
   a. 从列表中选择域名。
      将会显示该域中主机的列表。
   b. 单击某个主机的名称，将会显示 URL 列表。

6 **要废止单个文件：**

   a. **选择这些文件的 URL 旁边的 "Ex" 选项。**

   b. **单击 "Exp/Rem Marked" 按钮。**

7 **要废止列表中的所有文件，请单击表单底部的 "Exp All" 按钮。**

8 **要删除高速缓存中的单个文件：**

   a. **选择要删除的那些文件的 URL 旁边的 "Rm" 选项。**

   b. **单击 "Exp/Rem Marked" 按钮。**

9 **要删除列表中的所有文件，请单击 "Rem All" 按钮。**

10 **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

只要代理服务器不繁忙，您就可以将文件预先装入指定 Web 站点，或对高速缓存中已有的文档进行最新性检查。您可以创建、编辑和删除成批的 URL，还可以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，可以主动对文件进行高速缓存。可以对当前位于高速缓存中的若干个文件执行最新版本检查，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，然后单击 "Caching" 选项卡。**

2 **单击 "Set Cache Batch Updates" 链接。**
将会显示 "Set Cache Batch Updates" 页面。

3 **从 "Create/Select a Batch Update Configuration" 旁边的下拉式列表中选择 "New and Create"。**

4. **单击 "OK"。将会显示 "Set Cache Batch Updates" 页面。**

5. **在 "Name" 部分中，键入新批量更新条目的名称。**

6. **在该页面的 "Source" 部分中，选择要创建的批量更新的类型。**
   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" 部分的字段中，标识要在批量更新中使用的文档。**

8. **在 "Exceptions" 部分中，标识要排除在批量更新之外的任何文件。**

9. **在 "Resources" 部分中，键入最大并发连接数以及要遍历的最大文档数。**

10. **单击 "OK"。**
    从 "Create/Select a Batch Update Configuration" 旁边的下拉式列表中，选择新添加的批次名称和日程表。

11. **单击 "OK"。**

注 – 您可以在不启用批量更新的情况下创建、编辑和删除批量更新配置。但是，如果您希望按照在 "Set Cache Batch Updates" 页面中设置的时间来更新批量更新，则必须启用更新。

---

12. **将会显示 "Schedule Batch Updates" 页面。**

13. **选择 "Update On" 或 "Update Off" 选项。**

14. **在下拉式列表中选择一个时间，然后选择您希望运行更新的日期。**

15. **单击 "OK"。**

16. **单击 "Restart required"。**
    将会显示 "Apply Changes" 页面。

17. **单击 "Restart Proxy Server" 按钮以应用更改。**

编辑或删除批量更新配置

如果要排除某些文件或者要更频繁地更新批次，则可以编辑批量更新。您可能还希望完全删除某个批量更新配置。

▼ 编辑或删除批量更新配置

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**
2. **单击 "Set Cache Batch Updates" 链接。**
   将会显示 "Set Cache Batch Updates" 页面。
3. **要编辑某个批次，请选择该批次的名称，然后从 "Create/Select a Batch Update Configuration" 旁边的下拉式列表中选择 "Edit"。**
4. **单击 "OK"。**
   将会显示 "Set Cache Batch Updates" 页面。
5. **根据需要修改信息。**
6. **单击 "OK"。**
7. **单击 "Restart required"。**
   将会显示 "Apply Changes" 页面。
8. **单击 "Restart Proxy Server" 按钮以应用更改。**

▼ 删除批量更新配置

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**
2. **单击 "Set Cache Batch Updates" 链接。**
3. **要删除某个批次，请选择该批次的名称，然后从 "Create/Select a Batch Update Configuration" 旁边的下拉式列表中选择 "Delete"。**
4. **单击 "OK"。**
5. **单击 "Restart required"。**
   将会显示 "Apply Changes" 页面。
6. **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。这些实用程序中的大多数都与 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）。所有这些实用程序都位于 `extras` 目录中。

▼ 运行命令行实用程序

1 **从命令行提示符下，转到** *server_root*`/proxy-server`*id* **目录。**

2 **键入** **`./start -shell`**。

以下各节介绍了各种实用程序。

生成高速缓存目录结构

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。

注 – 该实用程序不更新 `server.xml` 文件。`cbuild` 不能调整具有多个分区的高速缓存的大小。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。第一种模式为：

```
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 *server_root*/proxy-server*id*/config 目录中。
- *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。此选项不能与 *cache-dim* 参数一起使用。最大大小为 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。

第二种模式为：

```
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 *server_root*/proxy-server*id*/config 目录中。
- *cache-dir* 是高速缓存结构的目录。
- *cache-dim* 用于确定段数。例如，在图 12–2 中，段显示为 s3.4，3 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

代理服务器实用程序 `urldb` 用于管理高速缓存中的 URL 列表。可以使用此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，请在命令行中键入以下命令：

  ```
  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* 列出与正则表达式匹配的域
- *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 *server-root*/proxy-server*id*/config 目录中。

- 要列出域中的所有匹配站点，请在命令行中键入以下命令：

```
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 列出域中所有与正则表达式匹配的站点
- *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 *server-root*/proxy-server*id*/config 目录中。

- 要列出所有匹配站点，请在命令行中键入以下命令：

```
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 列出所有与正则表达式匹配的站点
- *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 *server-root*/proxy-server*id*/config 目录中。

- 要列出站点中的匹配 URL，请在命令行中键入以下命令：

```
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` 列出站点中所有与正则表达式匹配的 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 *server-root*`/proxy-server`*id*`/config` 目录中。

  directory.

- 要废止或删除站点中的匹配 URL，请在命令行中键入以下命令：

```
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 server-root/proxy-serverid/config
```

其中，

- `matching_urls_from_site` 列出站点中所有与正则表达式匹配的 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。此选项不能用于域模式和站点模式
- `-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 *server-root*`/proxy-server`*id*`/config` 目录中。

- 要列出所有匹配的 URL，请在命令行中键入以下命令：

```
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` 列出所有与正则表达式匹配的 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 *server-root*/proxy-server*id*/config 目录中。

- 要废止或删除所有匹配的 URL，请在命令行中键入以下命令：

```
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 列出所有与正则表达式匹配的 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 *server-root*/proxy-server*id*/config 目录中。

- 要废止或删除 URL 列表，请在命令行中键入以下命令：

```
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。此选项可用于提供 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 *server-root*/proxy-server*id*/config 目录中。

管理高速缓存垃圾收集

通过 cachegc 实用程序，您可以将可能已过期或存在时间过久而不能高速缓存（由于受到高速缓存大小约束）的对象从高速缓存数据库删除。

注 – 请确保在使用 cachegc 实用程序时，代理服务器实例中没有运行 CacheGC。

可以按以下方式使用 cachegc 实用程序：

```
cachegc -f leave-fs-full-percent -u gc-high-margin-percent -l gc-low-margin-percent -e
    extra-margin-percent -d conf-dir
```

例如：

```
cachegc -f 50 -u 80 -l 60 -e 5 -d server-root/proxy-serverid/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，达到此百分比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* 由垃圾收集器用于确定要删除高速缓存的百分比。
- *conf-dir* 是代理服务器实例的配置目录，它位于 *server-root*/proxy-server*id*/config 目录中。

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。在第二种模式下，它从给定 URL 开始，对从该 URL 到您指定的深度的 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 是符合 RFC 标准的爬虫程序 (robot)。

```
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-serverid/config
```

其中，

- *hostname* 是运行代理服务器的计算机的主机名。默认值为 localhost。
- *port* 是运行代理服务器的端口。默认端口为 8080。
- *time-lmt* 是实用程序运行的时间限制
- *contact-address* 确定将在从 bu 发送来的 HTTP 请求中发送的联系地址。默认值为 worm@proxy-name。

- *sleep-time* 是两次连续请求之间的休眠时间。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 *server-root*`/proxy-server`*id*`/config` 目录中。

使用 Internet 高速缓存协议 (Internet Cache Protocol, ICP)

Internet 高速缓存协议 (Internet Cache Protocol, 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。高速缓存可以使用 ICP 就是否存在高速缓存的 URL 及这些 URL 的最佳检索位置发送查询和回复。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，这些高速缓存将发回 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，则会发回未命中消息 (miss)。如果它们确实包含该 URL，则会发回命中消息 (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。它使一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要进行通信，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），对于这种情况，使用 ICP 进行通信会很有效。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 相互通信的代理服务器称为**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：**父级代理服务器**和**同级代理服务器**。如果其他近邻都没有请求的 URL，则只有父级代理服务器可以访问远程服务器。ICP 邻域可以没有父级代理服务器，也可以有多个父级代理服务器。ICP 邻域中的任何**非**父级代理服务器均被视为同级代理服务器。除非将同级代理服务器标记为 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。必须为每个近邻指定一个轮询轮次。如果将所有近邻都配置在轮询轮次一中，则会在一个循环中同时查询所有近邻。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，如果没有近邻返回命中信息 (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。

由于 ICP 父级代理服务器可能会成为网络瓶颈，因此可以使用轮询轮次来减轻其负载。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，将所有父级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某个 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，将把请求转给父级代理服务器。如果父级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，将无法应答来自其近邻的 ICP 请求。在代理服务器上启用 ICP 时会启动 ICP 服务器（如果它尚未运行）。

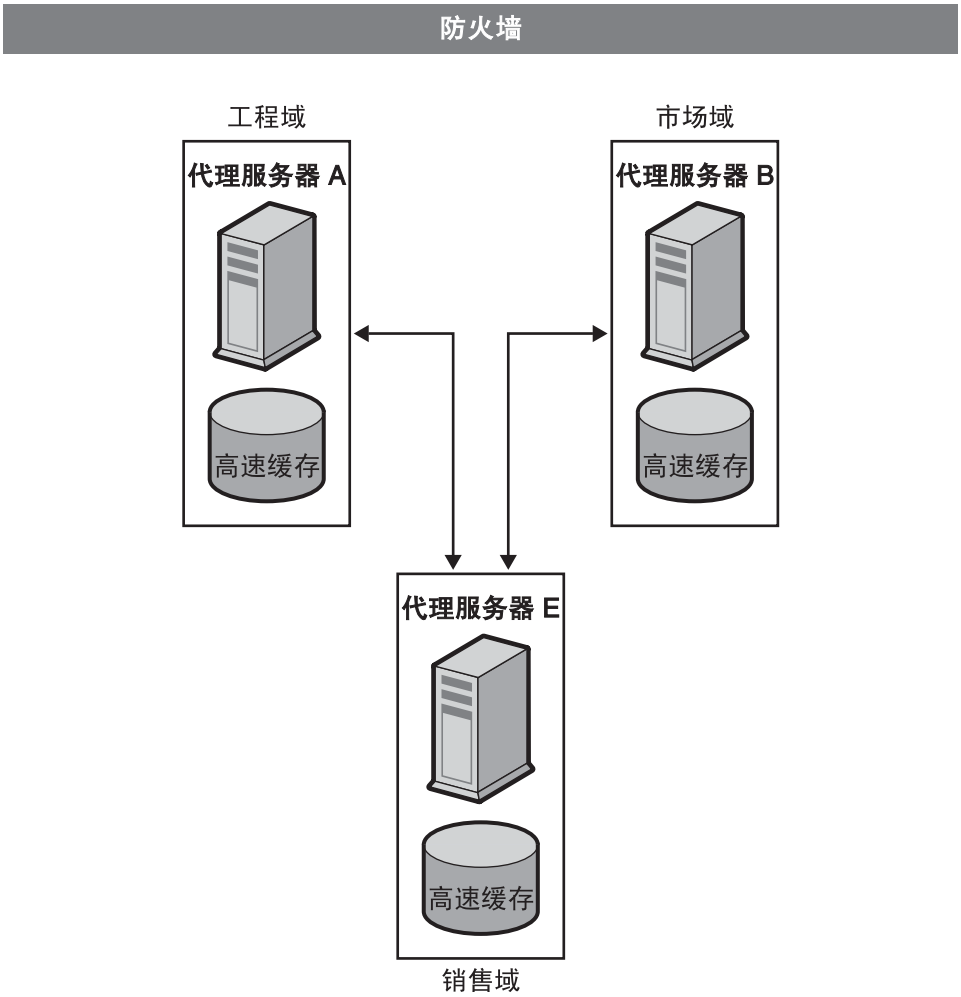

图 12–3 ICP 交换

设置 ICP

本节提供有关设置 ICP 的详细信息。设置 ICP 所需执行的常规步骤如下：

1. （可选）向 ICP 邻域中添加父级代理服务器。

   有关更多信息，请参见第 247 页中的 “向 ICP 邻域添加父级代理服务器或同级代理服务器”。

2. 向 ICP 邻域中添加同级代理服务器。

   有关更多信息，请参见第 247 页中的 “向 ICP 邻域添加父级代理服务器或同级代理服务器” 。

3. 配置 ICP 邻域中的每个近邻。

   有关更多信息，请参见第 248 页中的 “在 ICP 邻域中编辑配置” 。

4. 启用 ICP。

   有关信息，请参见第 250 页中的 “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级代理服务器，请启用通过 ICP 邻域进行路由选择。

   有关更多信息，请参见第 251 页中的 “启用通过 ICP 邻域进行路由选择” 。

▼ 向 ICP 邻域添加父级代理服务器或同级代理服务器

1 **访问 Server Manager，然后单击 "Caching" 选项卡。**

2 **单击 "Configure ICP" 链接。**

将会显示 "Configure ICP" 页面。

3 **在该页面的 "Parent List" 部分中，单击 "Add" 按钮。**

将会显示 "ICP Parent" 页面。

- 要添加父级代理服务器，请在该页面的 "Parent List" 部分中单击 "Add"。

  将会显示 "ICP Parent" 页面。
- 要添加同级代理服务器，请在该页面的 "Sibling List" 部分中单击 "Add"。

  将会显示 "ICP Sibling" 页面。

4 **在 "Machine Address" 字段中，键入要添加到 ICP 邻域的代理服务器的 IP 地址或主机名。**

5 **在 "ICP Port" 字段中，键入代理服务器将在其上侦听 ICP 消息的端口号。**

6 **（可选）在 "Multicast Address" 字段中，键入父级代理服务器要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。**

使用多址广播地址时，代理服务器能够向网络发送一个可被正在侦听该多址广播地址的所有近邻看到的查询。如果采用此技术，则可不必分别向每个近邻发送查询。多址广播的使用是可选的。

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，键入要将多址广播消息转发到的子网的数量。**

如果将 TTL 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，则将该消息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，为了防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，请在 "TTL" 字段中设置较低的 TTL 值。

---

8 **在 "Proxy Port" 字段中，键入父级代理服务器上的代理服务器端口。**

9 **在 "Polling Round" 下拉式列表中，选择希望父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"。**

将会显示 "Apply Changes" 页面。

12 **单击 "Restart Proxy Server" 按钮以应用更改。**

▼ 在 ICP 邻域中编辑配置

1 **访问 Server Manager，然后单击 "Caching" 选项卡。**

2 **选择 "Configure ICP" 链接。将会显示 "Configure ICP" 页面。**

3 **选中要编辑的代理服务器旁边的单选按钮。**

4 **单击 "Edit" 按钮。**

5 **修改相应的信息。**

6 **单击 "OK"。**

7 **单击 "Restart required"。**

将会显示 "Apply Changes" 页面。

8 **单击 "Restart Proxy Server" 按钮以应用更改。**

▼ 从 ICP 邻域中删除代理服务器

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**
2. **选择 "Configure ICP" 链接。将会显示 "Configure ICP" 页面。**
3. **选中要删除的代理服务器旁边的单选按钮。**
4. **单击 "Delete" 按钮。**
5. **单击 "Restart required"。**
   将会显示 "Apply Changes" 页面。
6. **单击 "Restart Proxy Server" 按钮以应用更改。**

▼ 在 ICP 邻域中配置本地代理服务器

您需要在 ICP 邻域中配置每个近邻或本地代理服务器。

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**
2. **选择 "Configure ICP" 链接。**
   将会显示 "Configure ICP" 页面。
3. **在 "Binding Address" 字段中，键入近邻服务器将绑定到的 IP 地址。**
4. **在 "Port" 字段中，键入近邻服务器将在其上侦听 ICP 的端口号。**
5. **在 "Multicast Address" 字段中，键入近邻要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。使用多址广播地址时，代理服务器能够向网络发送一个可被正在侦听该多址广播地址的所有近邻看到的查询。如果采用此技术，则可不必分别向每个近邻发送查询。

   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，键入代理服务器的名称或 IP 地址，当邻近代理服务器均未做出“ 命中 ”响应时，近邻应将请求路由到此代理服务器。**
   如果您在此字段中键入文字 "origin"，或将该字段留空，则默认情况下会路由至原始服务器。

如果您从 "No Hit Behavior" 下拉式列表中选择 "first responding parent"，则您在 "Default Route" 字段中键入的路由将不起作用。如果您选择默认的 "no hit" 行为，则代理服务器将只使用此路由。

7. **在第二个 "Port" 字段中，键入您在 "Default Route" 字段中键入的默认路由机器的端口号。**

8. **从 "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。**
   可用的选项如下：
   - **first responding parent**。近邻将通过最先做出“未命中”响应的父级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，键入将要服务于 ICP 请求的进程数。**

10. **在 "Timeout" 字段中，键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"。**
    将会显示 "Apply Changes" 页面。

13. **单击 "Restart Proxy Server" 按钮以应用更改。**

▼ 启用 ICP

1. **访问 Server Manager，然后单击 "Preferences" 选项卡。**

2. **单击 "Configure System Preferences" 链接。**
   将会显示 "Configure System Preferences" 页面。

3. **选中对应于 ICP 的 "Yes" 单选按钮，然后单击 "OK"。**

4. **单击 "Restart required"。**
   将会显示 "Apply Changes" 页面。

5. **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

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级代理服务器时，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级代理服务器，并且它本身没有任何同级代理服务器或父级代理服务器，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。

1. **访问 Server Manager，然后单击 "Routing" 选项卡。**
2. **单击 "Set Routing Preferences" 链接。**
   将会显示 "Set Routing Preferences" 页面。
3. **从下拉式列表中选择资源，或单击 "Regular Expression" 按钮，键入正则表达式，然后单击 "OK"。**
4. **选中 "Route Through" 选项旁边的单选按钮。**
5. **选中 ICP 旁边的复选框。**
6. **（可选）要使客户机直接从拥有文档的 ICP 近邻检索文档，而不是通过其他近邻获取文档，请选中 "Text Redirect" 选项旁边的复选框。**
7. **单击 "OK"。**

注意 – 当前任何客户机都不支持重定向，所以目前请不要使用该功能。

8. **单击 "Restart required"。**
   将会显示 "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

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。阵列中的每个代理服务器都将包含不同的高速缓存 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。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。只会将每个成员的高速缓存中 URL 的 1/*n*（其中 *n* 是阵列中的代理服务器数）重新指定给其他成员。

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指定一个分数，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 (Proxy Auto Configuration, PAC) 机制确定要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 文件来计算散列算法，以便为请求的 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。在此图中，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您使用管理界面确定的代理服务器阵列成员资格表 (Proxy Array Membership Table, PAT) 规范自动生成特殊 PAC 文件。

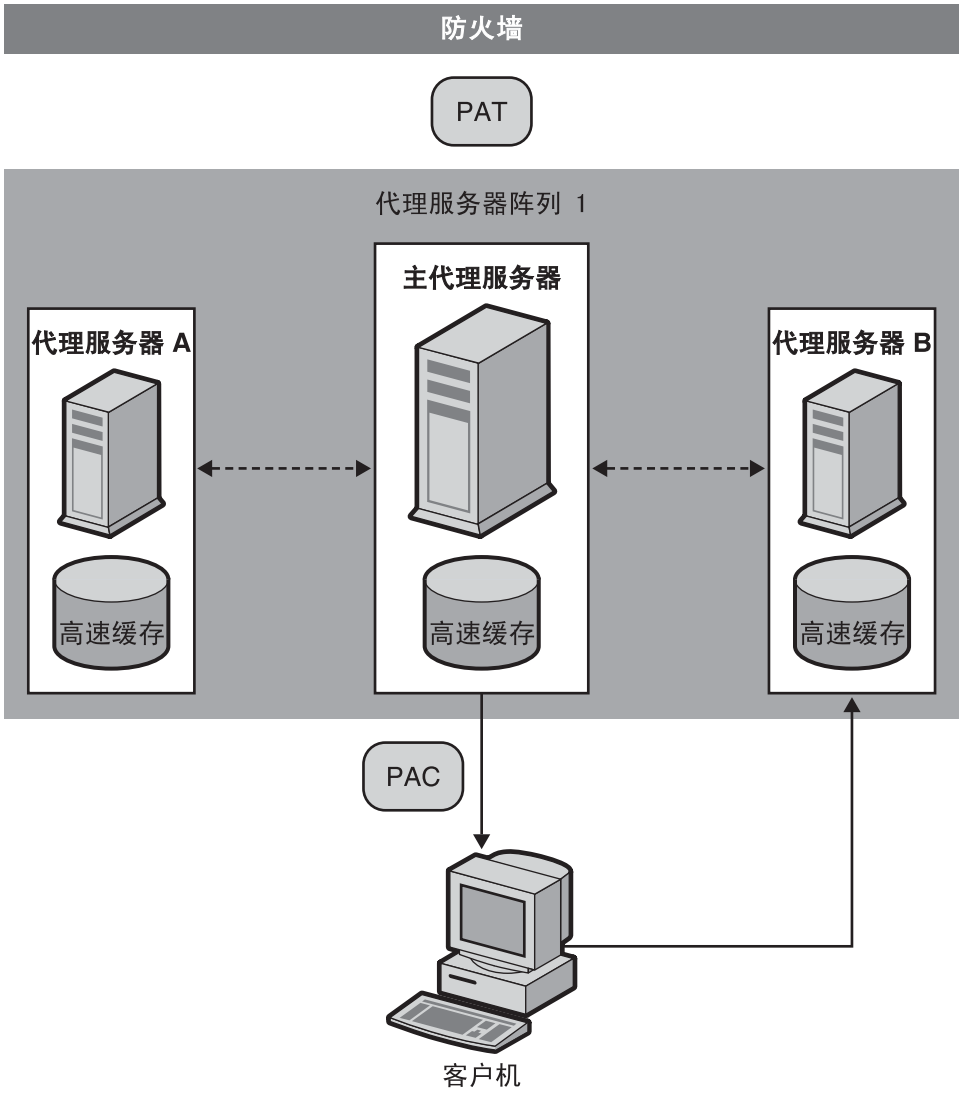

图 12–4 客户机到代理服务器路由选择

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（Proxy Array Table，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释）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。

PAT 文件是在代理服务器阵列中的主代理服务器上创建的。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。您可以将每个成员都配置为根据这些更改自动生成 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。如果代理服务器通过上游代理服务器阵列路由传入的请求，则该上游代理服务器阵列被称为父阵列。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 是父阵列。

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，以确定是否有对父阵列 PAT 文件的更新。通常，该成员轮询父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。在此图中，对于客户机请求的 URL，代理服务器 B 的分数最高。

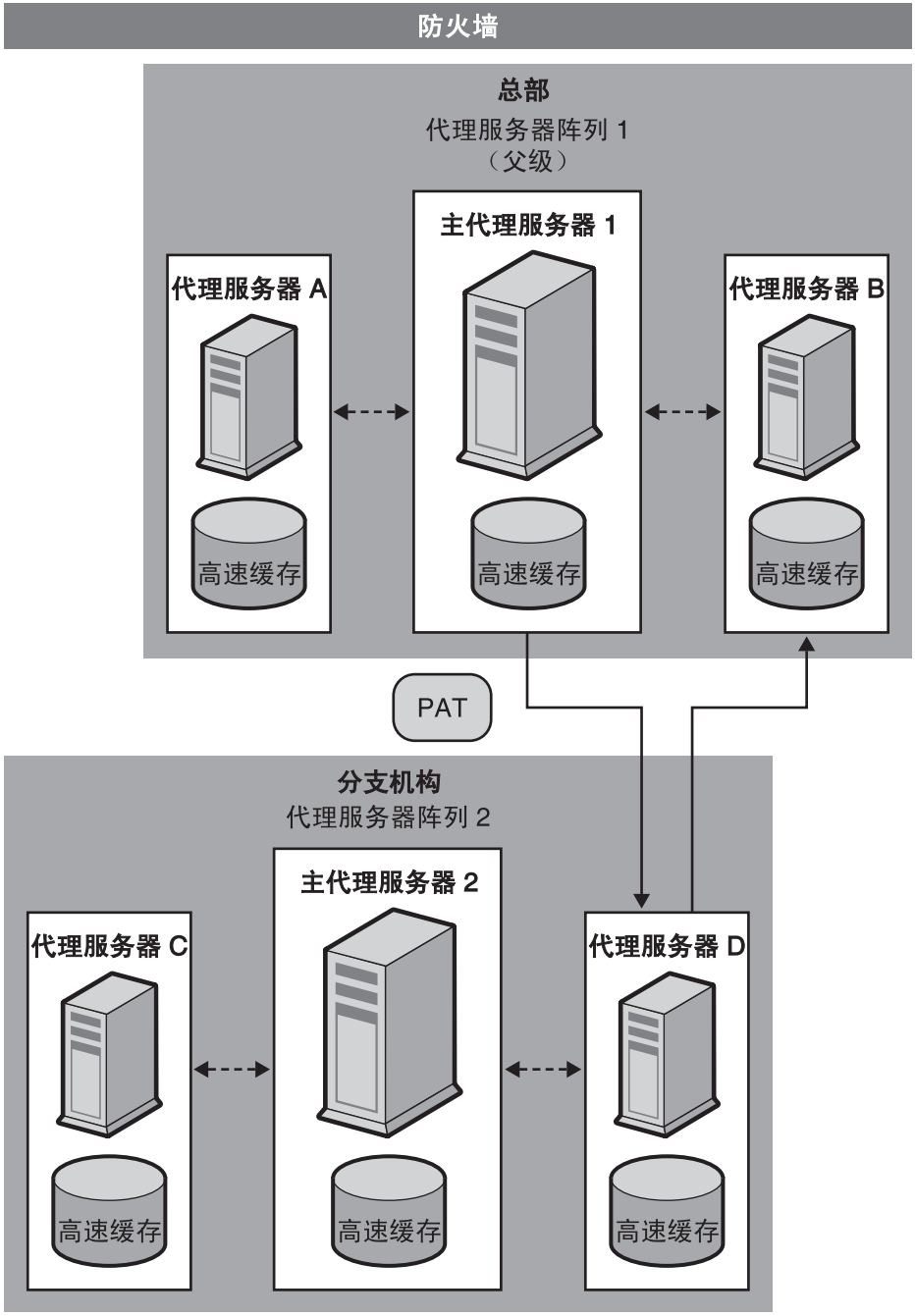

图 12–5 代理服务器到代理服务器路由选择

设置代理服务器阵列的常规步骤如下所示。

从主代理服务器中，执行以下步骤：

1. 创建代理服务器阵列。

   有关创建成员列表的更多信息，请参见第 256 页中的 “创建代理服务器阵列成员列表”。

2. 根据 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。有关更多信息，请参见第 262 页中的 “根据 PAT 文件生成 PAC 文件”。

3. 配置阵列的主成员。有关更多信息，请参见第 259 页中的 “配置代理服务器阵列成员”。

4. 启用通过代理服务器阵列进行路由选择。有关更多信息，请参见第 260 页中的 “启用通过代理服务器阵列进行路由选择”。

5. 创建 PAT 映射以将 URL `/pat` 映射到 PAT 文件。

6. 启用代理服务器阵列。

   有关更多信息，请参见第 261 页中的 “启用或禁用代理服务器阵列”。

从每个非主代理服务器中，执行以下步骤：

1. 配置阵列的非主成员。

   有关更多信息，请参见第 259 页中的 “配置代理服务器阵列成员”。

2. 启用通过代理服务器阵列进行路由选择。

   有关更多信息，请参见第 260 页中的 “启用通过代理服务器阵列进行路由选择”。

3. 启用代理服务器阵列。

   有关更多信息，请参见第 261 页中的 “启用或禁用代理服务器阵列”。

注 – 如果代理服务器阵列要通过父阵列进行路由，则还需要启用父阵列并将每个成员配置为通过父阵列进行路由以获得所需的 URL。有关更多信息，请参见第 263 页中的 “通过父阵列进行路由选择”。

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 – 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。

▼ 创建代理服务器阵列成员列表

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**
2. **单击 "Configure Proxy Array" 链接。**
   将会显示 "Configure Proxy Array" 页面。
3. **在 "Array name" 字段中，键入阵列的名称。**
4. **在 "Reload Configuration Every" 字段中，键入针对 PAT 文件执行轮询的时间间隔（以分钟为单位）。**
5. **单击 "Array Enabled" 复选框。**
6. **单击 "Create" 按钮。**
   创建代理服务器阵列后，"Create" 按钮将更改为 "OK" 按钮。

   注 – 一定要在开始向成员列表中添加成员之前单击 "OK"。
7. **单击 "OK"。**
8. **单击 "Restart required"。**
   将会显示 "Apply Changes" 页面。
9. **为代理服务器阵列中的每个成员提供以下信息，然后单击 "OK"。**
   应先添加主成员，然后再添加其他成员。
   - **Name**。要添加到成员列表的代理服务器的名称。
   - **IP Address**。要添加到成员列表的代理服务器的 IP 地址。
   - **Port**。此为成员针对 PAT 文件进行轮询时所使用的端口。
   - **Load Factor**。一个整数，它反映应该通过成员进行路由的相对负载。
   - **Status**。成员的状态。此值可以为 "on" 或 "off"。如果禁用某个代理服务器阵列成员，将会通过其他成员重新路由该成员的请求。

   注 – 键入要添加的每个代理服务器阵列成员的信息之后，一定要单击 "OK"。

10 **单击 "Restart required"。**
将会显示 "Apply Changes" 页面。

11 **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 – 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。

▼ 编辑成员列表信息

1 **访问 Server Manager，然后单击 "Caching" 选项卡。**

2 **单击 "Configure Proxy Array" 链接。**
将会显示 "Configure Proxy Array" 页面。

3 **在 "Member List" 中，选中要编辑的成员旁边的单选按钮。**

4 **单击 "Edit" 按钮。**
将会显示 "Configure Proxy Array Member" 页面。

5 **编辑相应的信息。**

6 **单击 "OK"。**

7 **单击 "Restart required"。**
将会显示 "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，请更新 "Configure Proxy Array" 页面上的配置 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

删除代理服务器阵列成员时，会将它们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。

▼ 删除代理服务器阵列的成员

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**
2. **单击 "Configure Proxy Array" 链接。**
   将会显示 "Configure Proxy Array" 页面。
3. **在 "Member List" 中，选中要删除的成员旁边的单选按钮。**
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，请更新 "Configure Proxy Array" 页面上的配置 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"。**
   将会显示 "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

必须通过代理服务器阵列中的每个成员本身配置该成员一次。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，然后单击 "Caching" 选项卡。**
2. **单击 "Configure Proxy Array Member" 链接。**
   将会显示 "Configure Proxy Array Member" 页面。
3. **在 "Proxy Array" 部分中，通过选中相应的单选按钮指示成员是否需要针对 PAT 文件进行轮询。**

- **Non-Master Member**。如果您配置的成员**不是**主代理服务器，请选择此选项。任何不是主代理服务器的代理服务器阵列成员都必须针对 PAT 文件执行轮询，以便从主代理服务器检索该文件。
- **Master Member**。如果配置的是主代理服务器，请选择此选项。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，键入将要针对 PAT 文件进行轮询的主代理服务器的名称。**
5. **在 "Port" 字段中，键入主代理服务器接受 HTTP 请求的端口。**
6. **在 "URL" 字段中，键入主代理服务器上 PAT 文件的 URL。如果您已经在主代理服务器上创建了一个 PAT 映射，要将该 PAT 文件映射到 URL `/pat`，应在 "URL" 字段中键入 `/pat`。**
7. **（可选）在 "Headers File" 字段中，键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。**
8. **单击 "OK"。**
9. **单击 "Restart required"。**
   将会显示 "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，然后单击 "Routing" 选项卡。**
2. **单击 "Set Routing Preference" 链接。**
   将会显示 "Set Routing Preferences" 页面。
3. **从下拉式列表中选择资源，或单击 "Regular Expression" 按钮，键入正则表达式，然后单击 "OK"。**
4. **选择 "Route Through" 选项。**
5. **选中代理服务器阵列或父阵列的复选框。**
   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。如果存在父阵列，则只能启用父阵列路由选择。这两个路由选择选项相互独立。

6. **如果选择通过代理服务器阵列进行路由，并且要将请求重定向到其他 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处理的请求，它会告知客户机与哪个代理服务器联系以处理该请求。

7. **单击 "OK"。**

8. **单击 "Restart required"。**

   将会显示 "Apply Changes" 页面。

9. **单击 "Restart Proxy Server" 按钮以应用更改。**

启用或禁用代理服务器阵列

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。如果您禁用了父阵列选项，则应在 "Set Routing Preferences" 页面中设置有效的替代路由选择选项，如显式代理服务器或直接连接。

▼ 启用或禁用代理服务器阵列

1. **访问 Server Manager，然后单击 "Preferences" 选项卡。**

2. **单击 "Configure System Preferences" 链接。**

   将会显示 "Configure System Preferences" 页面。

3. **启用或禁用代理服务器阵列。**

   - 要启用代理服务器阵列，请单击与要启用的阵列（普通代理服务器阵列或父阵列）类型对应的 "Yes" 选项。
   - 要禁用代理服务器阵列，请单击 "No"。

4. **单击 "OK"。**

5. **单击 "Restart required"。**

   将会显示 "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，则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处理的请求，它会告知客户机与哪个代理服务器联系以处理该请求。

根据 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，客户机使用代理自动配置 (Proxy Auto Configuration, PAC) 机制接收有关要通过哪个代理服务器的信息。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。

可以根据 PAT 文件手动或自动生成 PAC 文件。如果通过代理服务器阵列的某个特定成员手动生成 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。如果您将某个代理服务器阵列成员配置为自动生成 PAC 文件，则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 – 如果您没有为代理服务器使用代理服务器阵列功能，请使用 "Create/Edit Autoconfiguration File" 页面生成 PAC 文件。有关更多信息，请参见第 17 章。

▼ 根据 PAT 文件手动生成 PAC 文件

只能通过主代理服务器生成 PAC 文件。

1. **访问主代理服务器的 Server Manager，然后单击 "Caching" 选项卡。**
2. **单击 "Configure Proxy Array" 链接。**

   将会显示 "Configure Proxy Array" 页面。
3. **单击 "Generate PAC" 按钮。**

   将会显示 "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" 字段中键入文件名称，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` 函数中的代理服务器阵列选择逻辑前。此函数通常用于不需要通过代理服务器阵列的本地请求。

   如果您已在配置代理服务器阵列成员时提供了该自定义逻辑文件，将会用该信息填充此字段。您可以在这里编辑自定义逻辑文件名。

5. **在 "Default Route" 字段中，键入当阵列中的代理服务器不可用时客户机应采用的路由。**
   如果您已在配置代理服务器阵列成员时提供了默认路由，将会用该信息填充此字段。您可以在这里编辑默认路由。

6. **单击 "OK"。**

7. **单击 "Restart required"。**
   将会显示 "Apply Changes" 页面。

8. **单击 "Restart Proxy Server" 按钮以应用更改。**

▼ 自动生成 PAC 文件

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**

2. **单击 "Configure Proxy Array Member" 链接。**
   将会显示 "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" 字段中键文件名称，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` 函数中的代理服务器阵列选择逻辑前。
   如果您已在配置代理服务器阵列时提供并保存了该自定义逻辑文件，将会用该信息填充此字段。您可以在这里编辑自定义逻辑文件名。

5. **在 "Default Route" 字段中，键入当阵列中的代理服务器不可用时客户机应采用的路由。**
   如果您已在配置代理服务器阵列时提供了默认路由，将会用该信息填充此字段。您可以编辑默认路由。

6. **单击 "OK"。**

7. **单击 "Restart required"。**
   将会显示 "Apply Changes" 页面。

8. **单击 "Restart Proxy Server" 按钮以应用更改。**

通过父阵列进行路由选择

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阵列进行路由，而不是直接转至远程服务器。

▼ 通过父阵列进行路由选择

1. **启用父阵列。**
   有关更多信息，请参见第 261 页中的 “启用或禁用代理服务器阵列” 。
2. **启用通过父阵列进行路由选择。**
   有关更多信息，请参见第 260 页中的 “启用通过代理服务器阵列进行路由选择” 。
3. **访问 Server Manager，然后单击 "Caching" 选项卡。**
4. **单击 "Configure Proxy Array Member" 链接。**
   将会显示 "Configure Proxy Array Member" 页面。
5. **在该页面的 "Parent Array" 部分的 "Poll Host" 字段中，键入父阵列中将针对 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阵列的主代理服务器。
6. **在该页面的 "Parent Array" 部分的 "Port" 字段中，键入父阵列中将针对 PAT 文件对其进行轮询的代理服务器的端口号。**
7. **在 "URL" 字段中，键入主代理服务器上 PAT 文件的 URL。**
   如果您已在主代理服务器中创建了 PAT 映射，请在此 "URL" 字段中键入该映射。
8. **（可选）在该表单的 "Parent Array" 部分的 "Headers File" 字段中，键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"。**
    将会显示 "Apply Changes" 页面。
11. **单击 "Restart Proxy Server" 按钮以应用更改。**

查看父阵列信息

如果代理服务器阵列要通过父阵列进行路由选择，则需要有关该父阵列的成员的信息。此信息以 PAT 文件形式从父阵列发出。

▼ 查看父阵列信息

1. **访问 Server Manager，然后单击 "Caching" 选项卡。**
2. **单击 "View Parent Array Configuration" 链接。**
   将会显示 "View Parent Array Configuration" 页面。
3. **查看信息。**

◆ ◆ ◆ 第 13 章

13 通过代理服务器过滤内容

本章介绍如何过滤 URL，以使代理服务器禁止访问 URL 或修改它返回到客户机的 HTML 和 JavaScript 内容。此外，本章还介绍如何基于客户机使用的 Web 浏览器（用户代理）通过代理服务器限制访问。

您可以使用 URL 过滤器文件来确定服务器支持哪些 URL。例如，可以创建或购买一个包含要限制的 URL 的文本文件，而不是手动键入要支持的 URL 的通配符模式。通过此功能，可以创建一个包含 URL 的文件，该文件可用在许多不同的代理服务器上。

您还可以基于 URL 的 MIME 类型对 URL 进行过滤。例如，您可能允许代理服务器高速缓存和发送 HTML 和 GIF 文件，但不允许它获取二进制文件或可执行文件（因为这些文件可能带来计算机病毒）。

本章包含以下各节：

过滤 URL

您可以使用包含 URL 的文件来配置代理服务器检索哪些内容。可以设置一个代理服务器始终支持的 URL 列表以及一个代理服务器从不支持的 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适合儿童的内容，则可以设置一个准许儿童查看的 URL 列表。然后，可以使代理服务器仅检索批准的 URL。如果客户机尝试访问不支持的 URL，则可以让代理服务器返回默认的 "Forbidden" 消息，也可以创建一条解释客户机为何无法访问此 URL 的自定义消息。

要基于 URL 限制访问，请创建一个包含允许或限制的 URL 的文件。可以通过 Server Manager 实现此操作。创建此文件后，可以设置限制。这些过程将在以下各节中进行介绍。

创建包含 URL 的过滤器文件

过滤器文件是包含 URL 列表的文件。代理服务器使用的过滤器文件为纯文本文件，其中的 URL 行采用以下模式：

```
protocol://host:port/path/filename
```

可以分别在以下三部分中使用正则表达式：`protocol` 、`host:port` 和 `path/filename`。例如，如果要针对所有协议创建链接到 `netscape.com` 域的 URL 模式，应在文件中包含以下行：

```
.*://.*\\.example\\.com/.*
```

仅当未指定端口号时此行才起作用。有关正则表达式的更多信息，请参第 16 章中的“了解正则表达式”。

如果您要创建自己的文件，但不使用 Server Manager，请使用 Server Manager 页面创建一个空文件，然后在此文件中添加自己的文本或使用包含正则表达式的文件替换此文件。

▼ 创建过滤器文件

1. **访问 Server Manager 并单击 "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" 按钮旁边的下拉式列表中选择 "New Filter"。**
4. **在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" 滚动文本框键入 URL 以及 URL 的正则表达式。**
   使用 "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，请参见第 16 章中的“了解正则表达式”。
6. **单击 "OK"。**
   代理服务器将创建文件并返回到 "Restrict URL Filter Access" 页面。将在 `proxy-server`*id*`/conf_bk` 目录中创建过滤器文件。

为过滤器文件设置默认访问

创建包含要使用的 URL 的过滤器文件后，可以为这些 URL 设置默认访问。

▼ 为过滤器文件设置默认访问

1. **访问 Server Manager 并单击 "Filters" 选项卡。**
2. **单击 "Restrict URL Filter Access" 链接。**
   将显示 "Restrict URL Filter Access" 页面。
3. **选择要用于过滤器的模板。**
   通常，需要为整个代理服务器创建过滤器文件，但是您可能希望为 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" 列表来选择一个包含您希望代理服务器支持的 URL 的过滤器文件。**
5. **使用 "URL Filter To Deny" 列表来选择一个包含您希望代理服务器拒绝对其访问的 URL 的过滤器文件。**
6. **选择您希望代理服务器向请求了拒绝的 URL 的客户机返回的文本。**
   - 发送代理服务器生成的默认 "Forbidden" 响应。
   - 发送包含自定义文本的文本文件或 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 可以检查要返回到客户机的内容，并使用其他字符串替换 URL 之类的模式。可以配置两个参数：来源字符串和目标字符串。Proxy Server 将查找与来源字符串匹配的文本并将其替换为目标字符串中的文本。此功能仅在反向代理模式下有效。

▼ 创建 URL 重写模式

1. **访问 Server Manager 并单击 "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资源或指定正则表达式。**
   有关正则表达式的更多信息，请参见第 16 章中的“了解正则表达式”。
4. **在 "Source Pattern" 文本框中指定来源字符串。**
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 并单击 "Filters" 选项卡。**
2. **单击 "Set Content URL Rewriting" 链接。**
   将显示 "Set Content URL Rewriting" 页面。
3. **单击要编辑的 URL 重写模式旁边的 "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 并单击 "Filters" 选项卡。**
2. **单击 "Set Content URL Rewriting" 链接。**
   将显示 "Set Content URL Rewriting" 页面。
3. **单击要删除的 URL 重写模式旁边的 "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。**

针对特定 Web 浏览器限制访问

可以基于客户机的 Web 浏览器的类型和版本限制对代理服务器的访问。将基于所有 Web 浏览器在发出请求时发送到服务器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 并单击 "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，或键入与您希望 Proxy Server 支持的浏览器的用户代理字符串匹配的正则表达式。**
   如果要指定多个客户机，请将正则表达式括在圆括号中并使用 | 字符隔开多个条目。有关正则表达式的更多信息，请参见第 16 章中的“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阻止文件上载和其他请求。

▼ 基于 MIME 类型阻止请求

1. **访问 Server Manager 并单击 "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，键入正则表达式，然后单击 "OK"。**
4. **选择所需的请求阻止类型。**
   - Disabled－禁用请求阻止
   - Multipart MIME (File Upload)－阻止所有文件上载
   - MIME Types Matching Regular Expression－阻止对与键入的正则表达式匹配的 MIME 类型的请求。有关正则表达式的更多信息，请参见第 16 章中的“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的请求。**
6. **选择针对哪些方法阻止请求。**
   选项包括：
   - Any Method With Request Body－阻止包含请求主体的所有请求（无论请求使用的是何种方法）
   - 仅适用于：
     - 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－阻止所有使用所输入方法的文件上载请求
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。**

抑制外出的标头

通常，为了安全起见，可以将代理服务器配置为从请求中删除外出的标头。例如，您可能要阻止 From 标头传出，因为它会泄露用户的电子邮件地址。或者，您可能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使用的是何种 Web 浏览器。此外，在将请求转发到 Internet 之前，还可能要删除仅在内联网中使用的与日志记录或客户机相关的标头。

此功能不会影响代理服务器本身专门处理或生成的标头，也不会影响协议正常工作所需的标头，例如 If-Modified-Since 和 Forwarded。

代理服务器产生的转发标头不会构成安全问题。远程服务器可以通过连接来检测连接的代理主机。在代理链中，外部代理可抑制来自内部代理的转发标头。如果您不希望向远程服务器泄露内部代理或客户机主机名，建议使用此方法来设置您的服务器。

▼ 抑制外出的标头

1. **访问 Server Manager 并单击 "Filters" 选项卡。**
2. **单击 "Suppress Outgoing Headers" 链接。**
   将显示 "Suppress Outgoing Headers" 页面。
3. **在 "Suppress Headers" 文本框中键入以逗号分隔的要抑制的请求标头列表。**
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

您可以将代理服务器配置为阻止与某个 MIME 类型匹配的特定文件。例如，可以将代理服务器设置为阻止任何可执行文件或二进制文件，这样使用代理服务器的所有客户机便无法下载可能的计算机病毒。

如果您希望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，请参见第 123 页中的 “创建 MIME 类型” 。

可将过滤 MIME 类型与模板进行组合，从而仅针对特定的 URL 阻止特定的 MIME 类型。例如，可以阻止来自 .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 并单击 "Filters" 选项卡。**
2. **单击 "Set MIME Filters" 链接。**
   将显示 "Set MIME Filters" 页面。
3. **选择要用于过滤 MIME 类型的模板，或确保编辑整个服务器。**
4. **在 "Current filter" 文本框中，可以键入与要阻止的 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/.*`**。此方法要快于检查每个应用程序类型的 MIME 类型。正则表达式不区分大小写。有关正则表达式的更多信息，请参见第 16 章中的“了解正则表达式”。
5. **检查要过滤的 MIME 类型。**
   当客户机尝试访问被阻止的文件时，代理服务器将返回 "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

在将文件传递到客户机之前，可以指定要过滤掉的 HTML 标记。通过此方法，可以过滤掉 HTML 文件中嵌入的对象（如 Java applet 和 JavaScript）。要过滤 HTML 标记，应指定 HTML 标记的开始标记和结束标记。然后，代理服务器会使用空格替换这些标记中的所有文本和对象，然后再将文件发送到客户机。

代理服务器会将原始（未编辑的）文件存储在高速缓存中（如果将代理服务器配置为高速缓存此资源）。

▼ 过滤掉 HTML 标记

1. **访问 Server Manager 并单击 "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，也可以选择仅指定特定 URL（例如，来自 .edu 域中主机的 URL）的模板。

4. **选择要过滤的默认 HTML 标记。**

   - APPLET 通常位于 Java applet 的两侧。
   - SCRIPT 表示 JavaScript 代码的开始位置。
   - IMG 指定内置图像文件。

5. **可以键入任何要过滤的 HTML 标记。**

   键入 HTML 标记的开始标记和结束标记。

   例如，要过滤掉表单，可以在 "Start Tag" 框中键入 **FORM**，在 "End Tag" 框中键入 **/FORM**。HTML 标记不区分大小写。如果要过滤的标记没有结束标记（例如 OBJECT 和 IMG），可以将 "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。内容压缩可以提高向客户机传送内容的速度，同时可以提供更多内容，而无需增加硬件的消耗。压缩内容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。

通过内容压缩，Proxy Server 可以发送压缩数据，并指示浏览器对这些数据进行动态解压缩。这种压缩减少了发送的数据量，同时提高了页面的显示速度。

将服务器配置为根据需要压缩内容

您可以将 Proxy Server 配置为动态压缩传输数据。动态生成的 HTML 页面仅在用户提出请求时才存在。

▼ 将服务器配置为根据需要压缩内容

1. **访问 Server Manager 并单击 "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键入正则表达式。**
   有关正则表达式的更多信息，请参见第 16 章中的“了解正则表达式”。
4. **指定以下信息：**
   - **Activate Compress Content on Demand?**选择服务器是否要为选定资源提供预压缩内容。
   - **Vary Header**。指定是否要插入 Vary: Accept-encoding 标头。选择 "yes" 或 "no"。如果设置为 "yes"，当选择文件的压缩版本时将始终插入 Vary: Accept-encoding 标头。

     如果设置为 "no"，当选择文件的压缩版本时将不会插入 Vary: Accept-encoding 标头。

     默认情况下，该值设置为 "yes"。
   - **Fragment Size**。指定压缩库 (`zlib`) 使用的内存段大小（以字节为单位）以控制一次压缩的量。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，是速度和压缩的折中。
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

本章介绍如何将 Proxy Server 用作反向代理。可以在防火墙外部使用反向代理来向外部客户机提供一个安全内容服务器，以防从公司外直接、不受监视地访问服务器数据。此外，还可以使用反向代理进行复制；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。

本章包含以下各节：

反向代理的工作方式

您可以使用两种不同方法进行反向代理。一种方法利用 Proxy Server 的安全性功能来处理事务。另一种方法使用高速缓存在高用量服务器上提供负载平衡。这两种方法均有别于惯用的代理用法，因为它们并不严格在防火墙上运行。

代理充当服务器的替身

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作为内容服务器的替身。当外部客户机试图访问内容服务器时，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路将结果回传给代理。代理将检索到的信息发送给客户机，就像代理是实际的内容服务器一样，如图 14–1 中所示。如果内容服务器返回错误消息，代理服务器可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。这种措施可防止外部客户机获取内部内容服务器的重定向 URL。

通过这种方式，代理就在安全数据库和可能存在的恶意攻击之间提供了另一道屏障。如果侥幸攻击成功，作恶者充其量也仅限于访问单个事务中所涉及的信息，而不至于获得整个数据库的访问权。未经授权的用户无法到达真正的内容服务器，因为防火墙通路仅允许代理服务器有权进行访问。

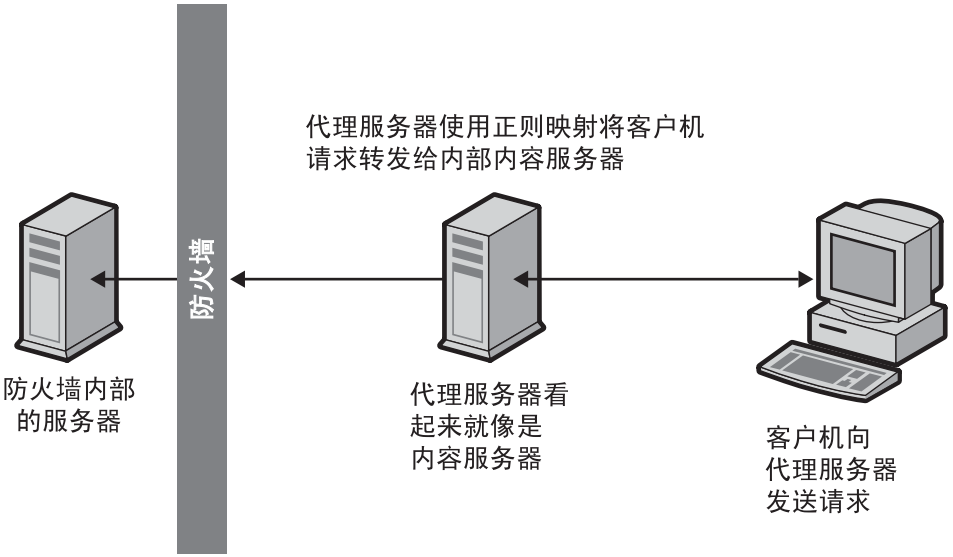

图 14–1 反向代理过程

您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）有权通过防火墙进行访问，而不允许任何其他计算机进出。

安全反向代理

当代理服务器与其他计算机之间的一个或多个连接使用安全套接字层 (Secure Sockets Layer, SSL) 协议加密数据时，将会进行安全反向代理。

安全反向代理具有许多用途：

- 提供从防火墙外部的代理服务器到防火墙内部的安全内容服务器的加密连接
- 允许客户机安全地连接到代理服务器，协助信息（如信用卡号）的安全传输

由于加密数据时占用开销，因此安全反向代理将会降低各安全连接的速度。但是，因为 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性参数，从而大大降低了后续连接的开销。

配置安全反向代理的方法有三种：

- **客户机安全连接到代理**。如果未经授权的用户很少或根本没有机会访问代理与内容服务器之间交换的信息，则此方案很有效，如下图所示。

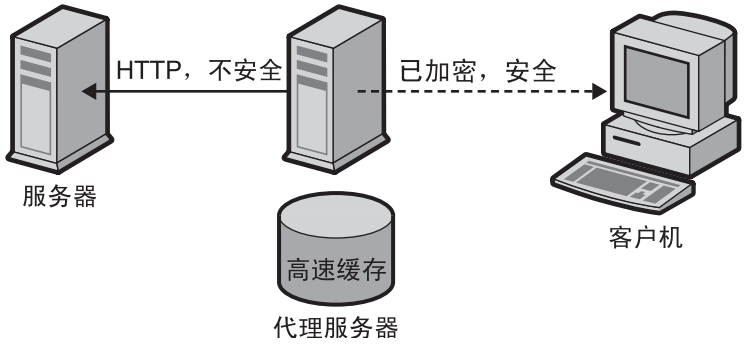

图 14–2　客户机安全连接到代理

- **代理安全连接到内容服务器**。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，如下图所示。

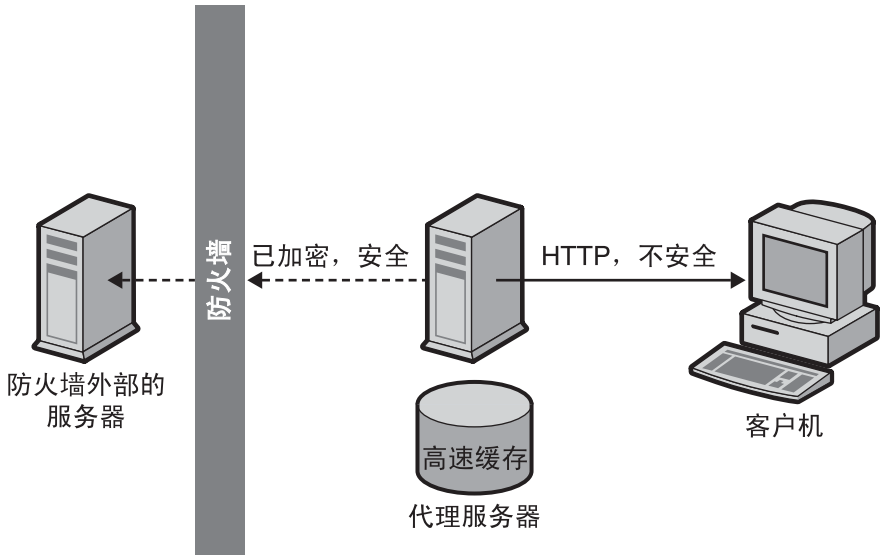

图 14–3　代理安全连接到内容服务器

- **客户机安全连接到代理并且代理安全连接到内容服务器**。如果需要保护服务器、代理和客户机之间交换的信息的安全，则此方案很有效。在此方案中，代理服务器既可充当站点间的安全通道，又可增加客户机验证的安全性，如下图所示。

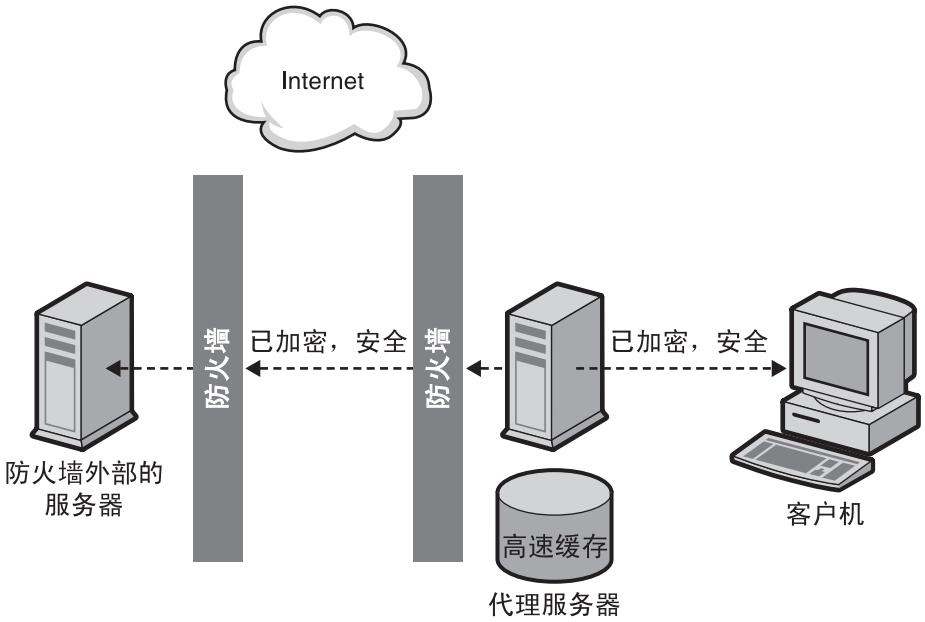

图 14–4 客户机安全连接到代理并且代理安全连接到内容服务器

有关如何设置上述每种配置的信息，请参见第 281 页中的 “设置反向代理”。

除了 SSL 之外，代理还可以使用客户机验证，这种方法要求向代理提出请求的计算机提供证书或其他形式的标识以验证其身份。

负载平衡代理

您可以在组织中使用多个代理服务器来平衡 Web 服务器之间的网络负载。此模型将利用代理服务器的高速缓存功能创建一个用于负载平衡的服务器池。在这种情况下，代理服务器可以位于防火墙的任意一侧。如果 Web 服务器每天都会收到大量请求，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。

代理服务器充当发往真正服务器的客户机请求的媒介。代理服务器会高速缓存所请求的文档。如果有多个代理服务器，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。

使用多个代理来处理对某个高用量内容服务器的请求的优点在于，该服务器可以处理更繁重的负载，并且比其独自处理时的效率更高。在初始启动期间，代理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进行处理。例如，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，并且每个代理每天处理 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% 到达内容服务器，合计约为每个代理每天 200,000 次命中，即总数仅为 600,000 次，从而大大提高效率。命中次数可从约 2 百万次增加到 6 百万次，而内容服务器的负载可相应地从 2 百万次减少到 600,000 次。实际结果依具体情况而定。

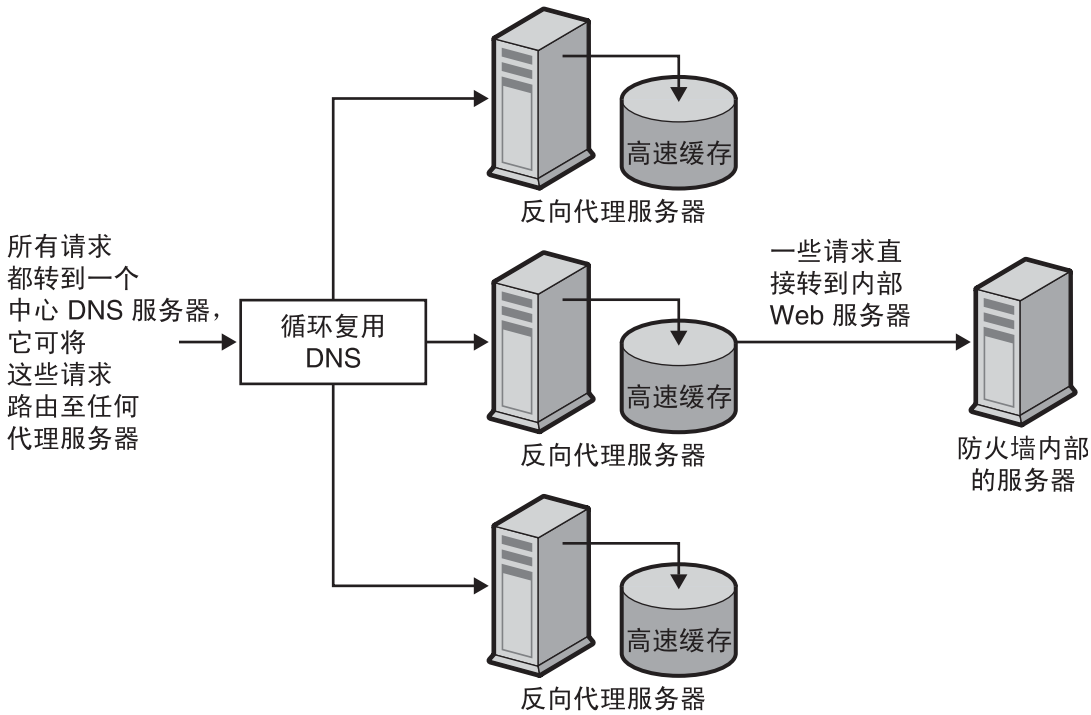

图 14–5 用于负载平衡的代理

设置反向代理

要设置反向代理，需要两个映射：正则映射和反向映射。

- 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 – 请不要将反向代理与提供自动配置文件的代理一起使用，因为该代理可能会返回错误的结果。

- 反向映射用于指示代理服务器为来自内容服务器的重定向设置陷阱。代理将截取重定向，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。在该返回消息中，内容服务器会添加一个 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，并且要为其设置反向代理服务器。可以将该反向代理称为 `http://proxy.site.com/`。

▼ 创建正则映射或反向映射

1 **访问 Server Manager 并单击 "URLs" 选项卡。**

2 **单击 "Create Mapping" 链接。**

此时将显示 "Create Mapping" 页面。

3 **在显示的页面中，为正则映射提供源前缀和源目标。**

例如，

源前缀：`http://proxy.site.com`

源目标：`http://http.site.com/`

4 **单击 "OK"。**

返回该页面并创建反向映射，例如，

反向映射：

源前缀：`http://http.site.com/`

源目标：`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 "View/Edit Mappings" 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的用户。第一个映射用于捕捉以常规代理形式连接到反向代理的用户。仅当用户不更改管理 GUI 自动提供的 "Map Source Prefix" 文本框的内容时，才会添加 "/" 映射。根据具体设置，通常只有第二个映射是必需的，但是附加映射不会导致代理出现问题。

注 – 如果 Web 服务器具有多个 DNS 别名，每个别名都应有一个对应的正则映射。如果 Web 服务器使用自身的多个 DNS 别名生成重定向，则其中每个别名都应有一个对应的反向映射。

CGI 应用程序仍在原始服务器上运行。代理服务器从不自行运行 CGI 应用程序。但是，如果 CGI 脚本指示结果可以进行高速缓存（通过发出上次修改或到期标头暗示生存时间非零），代理将会高速缓存结果。

为 Web 服务器制作内容时，切记反向代理也将为该内容提供服务，因此，指向 Web 服务器上的文件的所有链接都应为相对链接。请不要在 HTML 文件中引用主机名。所有链接都只能由页面组成：

```
/abc/def
```

而不能是全限定主机名，例如：

```
http://http.site.com/abc/def
```

注 – 您可以为反向代理模式下发生的错误提供自定义错误页面。这些错误页面将替代由代理生成的错误。这样可防止客户机了解到已经配置了代理服务器。

设置安全反向代理

设置安全反向代理之前，应熟悉数字证书、证书授权机构和验证。

设置安全反向代理与设置非安全反向代理几乎相同。唯一的区别在于需要将 HTTPS 指定为要加密文件的协议。

客户机安全连接到代理

此过程说明如何根据所选配置方案设置安全反向代理。为了演示如何设置映射，以下说明假定您有一个称为 `http.site.com` 的 Web 服务器，并且要设置一个称为 `proxy.site.com` 的安全反向代理服务器。按所述步骤进行操作时，请使用您的 Web 服务器名称和代理名称替代指示中使用的示例名称。

▼ 设置客户机安全连接到代理映射

1. **访问 Server Manager 并单击 "URLs" 选项卡。**
2. **单击 "Create Mapping" 链接。**
   此时将显示 "Create Mapping" 页面。

3 **在显示的页面中，采用以下方式设置正则映射和反向映射：**
正则映射：

源前缀：`https://proxy.mysite.com`

源目标：`http://http.mysite.com/`

反向映射：

源前缀：`http://http.mysite.com/`

源目标：`https://proxy.mysite.com/`

4 **保存并应用所做的更改。**
要查看刚创建的映射，请单击 "View/Edit Mappings" 链接。

注 – 此配置仅在代理服务器以安全模式运行时才有效。换言之，必须启用加密并且必须从命令行重新启动代理。要从命令行重新启动代理，请转到代理目录，然后键入 **`./start`**。

▼ 设置代理安全连接到内容服务器映射

1 **访问 Server Manager 并单击 "URLs" 选项卡。**

2 **单击 "Create Mapping" 链接。**
此时将显示 "Create Mapping" 页面。

3 **在显示的页面中，采用以下方式设置正则映射和反向映射：**
正则映射：

源前缀：`http://proxy.mysite.com`

源目标：`https://http.mysite.com/`

反向映射：

源前缀：`https://http.mysite.com/`

源目标：`http://proxy.mysite.com/`

4 **保存并应用所做的更改。**
要查看刚创建的映射，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有效。

▼ 设置客户机安全连接到代理和代理安全连接到内容服务器

1 **访问 Server Manager 并单击 "URLs" 选项卡。**

2 **单击 "Create Mapping" 链接。**
此时将显示 "Create Mapping" 页面。

3 **在显示的页面中，采用以下方式设置正则映射和反向映射：**
正则映射：

源前缀：`https://proxy.mysite.com`

源目标：`https://http.mysite.com/`

反向映射：

源前缀：`https://http.mysite.com/`

源目标：`https://proxy.mysite.com/`

4 **保存并应用所做的更改。**
要查看刚创建的映射，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有效。换言之，对于代理，必须启用加密并且必须从命令行重新启动代理。要从命令行重新启动代理，请转到代理目录，然后键入 **`./restart`**。

反向代理中的虚拟多重主机

利用虚拟多重主机功能，原始服务器（如反向代理服务器）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，假定您有以下 DNS 主机名：

- `www`
- `specs`
- `phones`

其中每个主机名都可以映射到同一 IP 地址（反向代理的 IP 地址）。然后，反向代理可以根据访问它时使用的 DNS 名称执行不同操作。

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`

可以将多个本地主机名以及多个域全部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

虚拟多重主机功能详细信息

为运行虚拟多重主机功能，需要先指定 DNS 主机名和域名（或别名），然后指定应将发送给该主机名的请求定向到的目标 URL 前缀。例如，假定您有以下两个映射：

- 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

该方法同样适用于虚拟域映射。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，服务器将不执行映射。找不到任何匹配项时，代理通常会发出 "Proxy denies fulfilling the request" 响应。

▼ 配置虚拟多重主机

1. **访问 Server Manager 并单击 "URLs" 选项卡。**
2. **单击 "Configure Virtual Multihosting" 链接。**
   此时将显示 "Configure Virtual Multihosting" 页面。
3. **在 "Source Hostname (alias)" 字段中，指定此映射将应用到的本地主机名（或 DNS 别名）。**
4. **在 "Source Domain Name" 字段中，键入此映射将应用到的本地域名。**
   通常，此名称为您自己网络的域名，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，键入目标 URL 前缀。如果主机名和域名符合上述规范，则会将请求定向到此 URL。**

6 **如果使用模板，请从 "Use This Template" 下拉式列表中选择模板名称；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"。**
此时将显示 "Apply Changes" 页面。

9 **单击 "Restart Proxy Server" 按钮应用更改。**
对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将显示在 "Configure Virtual Multihosting" 页面的底部。"Source Hostname (alias)" 和 "Source Domain Name" 字段连同代理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` 且端口号为 8080，则会显示以下正则表达式：

```
www(|.example.com)(|:8080)
```

此正则表达式可以保证与用户可能键入或客户机可能发送的以下所有可能组合匹配。即使端口号不是 80，某些客户机软件也可能将其省略，因为服务器正在侦听该端口。

- `www`
- `www:8080`
- `www.example.com`
- `www.example.com:8080`

虚拟多重主机说明

- 配置反向代理映射之前，需要禁用客户机自动配置功能。客户机自动配置功能用于正向代理操作，而不是反向代理。
- 虚拟多重主机功能会建立自动反向映射。请不要为使用 "Virtual Multihosting" 页面提供的映射创建反向映射。
- 虚拟映射是使用 `obj.conf` 文件中的 `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映射、反向映射、正则表达式映射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任何匹配项，则会继续转换 `obj.conf` 中虚拟映射部分之后的下一个映射。

  注 – 按照规范顺序，反向映射位于其他映射之前。

- 如果更改了代理服务器的端口号，则需要根据新端口号重新创建虚拟多重主机映射。

◆ ◆ ◆ 第 15 章

使用 SOCKS

本章介绍如何配置和使用 Sun Java System Web Proxy Server 附带的 SOCKS 服务器。Proxy Server 支持 SOCKS 第 4 版和第 5 版。

本章包含以下各节：

关于 SOCKS

SOCKS 是一种联网代理协议，用于重定向来自 SOCKS 服务器相对侧主机的连接请求，通过该协议，无需直接 IP 连接能力，一侧的主机便能够获得对另一侧主机的完全访问权限。SOCKS 通常用作网络防火墙，以使 SOCKS 服务器后面的主机能够获得对 Internet 的完全访问权限，同时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程序，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、建立代理连接以及转发数据。SOCKS 服务器在网络层而非应用层上运行，因此它不了解用于传输请求的协议或方法。由于 SOCKS 服务器不了解协议，因此可以使用该服务器来传送 Proxy Server 不支持的那些协议（如 Telnet）。

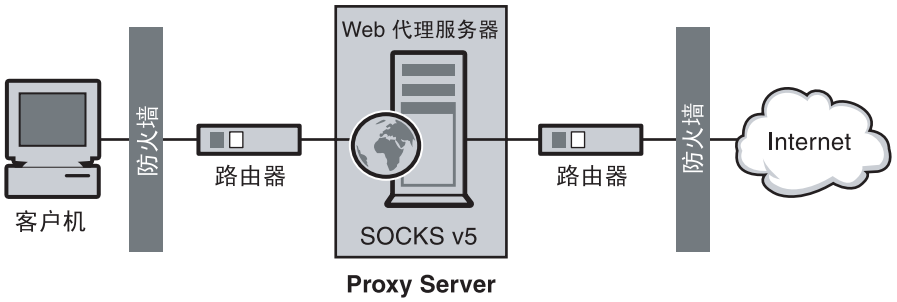

图 15–1 SOCKS 服务器在网络中的位置

使用捆绑的 SOCKS v5 服务器

Sun Java System Web Proxy Server 附带了自己的 SOCKS 守护程序，该守护程序识别其他 SOCKS 守护程序使用的标准 `socks5.conf` 文件格式。此守护程序可以由 Proxy Server 用来为请求选择路由，也可以从 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，请参见第 299 页中的 “配置路由条目”。

默认情况下，禁用 Proxy Server 附带的 SOCKS 守护程序。您可以通过 Server Manager 界面的 "SOCKS" 选项卡或命令行来启用该守护程序。有关更多信息，请参见第 292 页中的 “启动和停止 SOCKS v5 服务器”。

注 – 在 Proxy Server 4 中，SOCKS 守护程序的名称已从 `ns-sockd` 更改为 `sockd`。

使用 Proxy Server 附带的 SOCKS 服务器时必须采取的总体步骤如下：

▼ 使用 SOCKS

1. **配置 SOCKS 服务器。参见第 292 页中的 “ 配置 SOCKS v5 服务器 ”。**
2. **如果 SOCKS 服务器将在具有多个接口的计算机上运行，请创建 SOCKS 路由条目。参见第 299 页中的 “ 配置路由条目 ”。**
3. **创建验证条目。参见第 294 页中的 “ 配置 SOCKS v5 验证条目 ”。**
4. **创建连接条目。参见第 296 页中的 “ 配置 SOCKS v5 连接条目 ”。**
5. **启用 SOCKS 服务器。参见第 292 页中的 “ 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。其中每个条目都定义了在收到与该条目匹配的请求时 Proxy Server 将执行的操作。在 Server Manager 中所做的选择将写入 `socks5.conf`。此外，也可以手动编辑该文件。`socks5.conf` 文件位于安装根目录 *server-root*，如下所示：

server-root`/proxy-`*serverid*`/config` 目录

本节提供了有关 `socks5.conf` 的常规信息。有关该文件及其指令和语法的详细信息，请参见 Proxy Server **配置文件参考**。

验证

可以将 SOCKS 守护程序配置为使用其服务时要求验证。验证基于连接客户机的主机名和端口。如果选择要求用户名和密码，将会根据 `socks5.conf` 文件所引用的用户名和密码文件进行信息验证。如果提供的用户名和密码与密码文件中的列表不匹配，则拒绝访问。密码文件中用户名和密码的格式为 *username password*，其中用户名和密码用空格分隔。.

您还可以禁止用户。若要求进行用户名和密码验证，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，请参见 Proxy Server **配置文件参考**中的 `socks5.conf` 部分。

此外，还可以根据已配置的 LDAP 服务器（而不仅仅是文件）来执行用户名和密码验证。

访问控制

访问控制是使用 `socks5.conf` 文件中的一组有序行来执行的。每一行中都包含一条指令，用于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 守护程序将错误消息和访问消息都记录在 SOCKS 日志文件中。在 `socks5.conf` 中，可以指定日志文件位置和日志记录类型。

SOCKS 守护程序还会每小时生成一个统计条目，用于提供该守护程序的统计信息。

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。这些数目会影响 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，请参见第 292 页中的 “配置 SOCKS v5 服务器”中的相关部分。

启动和停止 SOCKS v5 服务器

可以从 Server Manager 或命令行来启动和停止 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 并单击 "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* 目录中找到的脚本，其中 *server-root* 为安装根目录：

- `start-sockd` 用于启动 SOCKS 守护程序
- `stop-sockd` 用于停止 SOCKS 守护程序
- `restart-sockd` 用于重新启动 SOCKS 守护程序

配置 SOCKS v5 服务器

▼ 配置 SOCKS 服务器

1. **访问服务器实例的 Server Manager 并单击 "SOCKS" 选项卡。**
2. **单击 "Configure SOCKS v5" 链接。**
3. **在 "SOCKS Port" 字段中，键入 SOCKS 服务器将侦听的端口号。默认值为 1080。**
4. **选择要使用的 SOCKS 选项。**
   可以使用以下选项：
   - *Disable Reverse DNS Lookup*。对 SOCKS 服务器禁用反向 DNS 查找。反向 DNS 用于将 IP 地址转换为主机名。禁用反向 DNS 查找可节省网络资源。默认情况下将禁用 DNS 查找。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，服务器将会执行映射，并向 SOCKS 日志文件中添加一个条目，用于列出该 DNS 转换。

- **Use Client-specific Bind Port**。允许客户机在 "BIND" 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。默认情况下禁用此选项。
- **允许***Wildcard As Bind IP Address*。允许客户机在 "BIND" 请求中指定一个全部由零组成的 IP 地址 (0.0.0.0)，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 SOCKS 服务器会拒绝绑定到 0.0.0.0 的请求。默认情况下禁用此选项。
- *Quench Updates*。禁用每小时自动写入一次统计文件。如果禁用，则每次请求时都会进行写入。有关更多信息，请参见第 291 页中的 “日志记录”。

"Quench Updates" 元素显示在用户界面中，但在本 Proxy Server 4 发行版中并未实现。

5 **在 "Log File" 字段中，键入 SOCKS 日志文件的完整路径名。**

默认路径为 *server-root*`/proxy-` *serverid*`/logs/socks5.log`。

6 **从 "Log Level" 下拉式列表中，选择日志文件是应仅包含警告和错误，还是应包含所有请求或调试消息。**

7 **选择 RFC 1413 ident 响应。**

Ident 允许 SOCKS 服务器确定客户机的用户名。通常，仅当客户机运行某些版本的 UNIX 时，此功能才有效。可以使用以下选项：

- **Don't Ask**。从不使用 ident 来确定客户机的用户名。此设置为默认设置，建议使用。
- **Ask But Don't Require**。询问所有客户机的用户名，但并不需要该名称。此选项使用 ident 只是出于日志记录目的。
- **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。这些数目会影响 SOCKS 服务器的性能。单击 "OK"。**

- **Number Of Worker Threads**。默认值为 40。如果 SOCKS 服务器太慢，请增加工作线程数。如果服务器不稳定，则应减少该数值。更改此数目时，请从默认值开始并根据需要进行增减。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，请增加接受线程数。如果服务器不稳定，则应减少该数值。更改此数目时，请从默认值开始并根据需要进行增减。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。如果在 SOCKS 服务器欠载且连接减少时请求失败，请调节此设置。

配置 SOCKS v5 验证条目

SOCKS 验证条目用于确定 SOCKS 守护程序应接受来自哪些主机的连接，以及 SOCKS 守护程序应使用何种类型的验证来验证这些主机。

▼ 创建 SOCKS 验证条目

1 **访问服务器实例的 Server Manager 并单击 "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，键入 SOCKS 服务器将要验证的主机的 IP 地址或主机名。**

如果键入的是 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，以确定其是否为有效主机。请勿在主机掩码条目中使用空格。如果不键入主机掩码，验证条目将适用于所有主机。

例如，可在 "Host Mask" 字段中键入 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此 IP 地址，并确定主机的 IP 地址是否与验证记录所请求的 IP 地址 (155.25.0.0) 匹配。

5 **在 "Port Range" 字段中，键入 SOCKS 服务器将要验证的主机的端口。**

请勿在端口范围条目中使用空格。如果不提供端口范围，验证条目将适用于所有端口。

可以使用方括号 [ ] 包括范围两端的端口，也可使用圆括号 ( ) 将它们排除在外。例如，[1000-1010] 表示 1000 和 1010 之间包括 1000 和 1010 在内的所有端口号，而 (1000-1010) 表示 1000 和 1010 之间不包括 1000 和 1010 在内的所有端口号。另外，也可以混合使用方括号和圆括号。例如，(1000-1010] 表示 1000 和 1010 之间不包括 1000 但包括 1010 在内的所有端口号。

6 **从 "Authentication Type" 下拉式列表中选择验证类型。**

可以使用以下选项：

- **Require user-password**。访问 SOCKS 服务器时需要用户名和密码。
- **User-password, if available**。如果存在用户名和密码，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**。访问 SOCKS 服务器时不需要验证。

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，因此必须指定对这些方法的评估顺序。这样，如果客户机不支持所列的第一种验证方法，便会改用第二种方法。如果客户机不支持所列的任何验证方法，SOCKS 服务器将断开连接而不接受请求。

▼ 编辑验证条目

1 访问服务器实例的 Server Manager 并单击 "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。

5 单击 "OK"。

▼ 删除验证条目

1 访问服务器实例的 Server Manager 并单击 "SOCKS" 选项卡。

2 单击 "Set SOCKS v5 Authentication" 链接。

3 选择要删除的验证条目。

4 单击 "Delete" 按钮。

▼ 移动验证条目

条目按其在 socks5.conf 文件中出现的顺序进行评估。可以通过移动来更改其顺序。

1 访问服务器实例的 Server Manager 并单击 "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。

5 单击 "OK"。

配置 SOCKS v5 连接条目

SOCKS 连接条目用于指定 SOCKS 守护程序是应允许请求，还是应拒绝请求。

▼ 创建连接条目

1. **访问服务器实例的 Server Manager 并单击 "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请求的验证方法。**
5. **从 "Connection Type" 下拉式列表中，选择此行所匹配的命令类型。命令类型可能包括：**
   - **Connect**
     - **Bind**
     - **UDP**
     - **All**
6. **在 "Source Host Mask" 字段中，键入连接控制条目所请求的主机的 IP 地址或主机名。**

   如果键入的是 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，以确定其是否为有效主机。请勿在主机掩码条目中使用空格。如果不键入主机掩码，连接条目将适用于所有主机。

   例如，可在主机掩码字段中键入 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此 IP 地址，并确定主机的 IP 地址是否与连接控制条目所请求的 IP 地址 (155.25.0.0) 匹配。
7. **在 "Port Range" 字段中，键入连接控制条目所请求的源计算机的端口。**

   请勿在端口范围条目中使用空格。如果不指定端口范围，连接条目将适用于所有端口。

   可以使用方括号 [ ] 包括范围两端的端口，也可使用圆括号 ( ) 将它们排除在外。例如，[1000-1010] 表示 1000 和 1010 之间包括 1000 和 1010 在内的所有端口号，而 (1000-1010) 表示 1000 和 1010 之间不包括 1000 和 1010 在内的所有端口号。另外，也可以混合使用方括号和圆括号。例如，(1000-1010] 表示 1000 和 1010 之间不包括 1000 但包括 1010 在内的所有端口号。

8. **在 "Destination Host Mask" 字段中，键入连接条目所请求的 IP 地址或主机名。**

   如果键入的是 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，以确定其是否为有效的目标主机。请勿在主机掩码条目中使用空格。如果不键入目标主机掩码，连接条目将适用于所有主机。

   例如，可在 "Destination Host Mask" 字段中键入 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此 IP 地址，并确定目标主机的 IP 地址是否与代理条目所请求的 IP 地址 (155.25.0.0) 匹配。

9. **在 "Port Range" 字段中，键入连接控制条目所请求的目标主机的端口。**

   请勿在端口范围条目中使用空格。如果不键入端口范围，连接条目将适用于所有端口。

   注 – 大多数 SOCKS 应用程序均会请求端口 0 来执行绑定请求，这表示它们没有端口首选项。因此，用于绑定的目标端口范围应始终包括端口 0。

   可以使用方括号 [ ] 包括范围两端的端口，也可使用圆括号 ( ) 将它们排除在外。例如，[1000-1010] 表示 1000 和 1010 之间包括 1000 和 1010 在内的所有端口号，而 (1000-1010) 表示 1000 和 1010 之间不包括 1000 和 1010 在内的所有端口号。另外，也可以混合使用方括号和圆括号。例如，(1000-1010] 表示 1000 和 1010 之间不包括 1000 但包括 1010 在内的所有端口号。

10. **在 "User Group" 字段中，键入要允许或拒绝访问的组。**

    如果不指定组，连接条目将适用于所有用户。

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"。**

    由于可以采用多个连接指令，因此必须指定对这些指令的评估顺序。

▼ 编辑连接条目

1. **访问服务器实例的 Server Manager 并单击 "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。**
5. **单击 "OK"。**

▼ 删除连接条目

1. 访问服务器实例的 Server Manager 并单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Connections" 链接。
3. 选择要删除的连接条目。
4. 单击 "Delete" 按钮。

▼ 移动连接条目

条目按其在 `socks5.conf` 文件中出现的顺序进行评估。可以通过移动来更改其顺序。

1. 访问服务器实例的 Server Manager 并单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Connections" 链接。
3. 选择要移动的连接条目。
4. 单击 "Move" 按钮。
5. 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 服务器链接

可以采用与 Proxy Server 相同的方式将 SOCKS 服务器链接在一起，这表示一个 SOCKS 服务器可以通过另一个 SOCKS 服务器进行路由。

▼ 配置 SOCKS 服务器链接

1. 访问服务器实例的 Server Manager 并单击 "SOCKS" 选项卡。
2. 单击 "Set SOCKS v5 Routing" 链接。
3. 如果代理链中的下游代理要求验证才能为任何请求提供服务，请在 "Server Chaining" 部分中，键入用于向链接的 Proxy Server 进行验证的用户名和口令。单击 "OK"。

配置路由条目

可以使用路由条目来配置 Proxy Server，使其通过 SOCKS 服务器对请求进行路由。 路由条目有两种类型，即 SOCKS v5 路由和 SOCKS v5 代理路由。

- SOCKS v5 路由用于确定 SOCKS 守护程序应对特定的 IP 地址使用哪个接口。
- SOCKS v5 代理路由用于确定可通过其他 SOCKS 服务器访问的 IP 地址，以及该 SOCKS 服务器是否与主机直接相连。通过 SOCKS 服务器进行路由时，代理路由很重要。

▼ 创建路由条目

1. **访问服务器实例的 Server Manager 并单击 "SOCKS" 选项卡。**
2. **单击 "Set SOCKS v5 Routing" 链接。**
3. **在 "Routing" 部分中，单击 "Add" 按钮。**
4. **在 "Host Mask" 字段中，键入与传入和传出连接必须经过的指定接口相对应的 IP 地址或主机名。**

   如果键入的是 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，以确定其是否为有效主机。请勿在主机掩码条目中使用空格。如果不提供主机掩码，SOCKS v5 条目将适用于所有主机。

   例如，可在主机掩码字段中键入 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此 IP 地址，并确定主机的 IP 地址是否与路由条目所请求的 IP 地址 (155.25.0.0) 匹配。

5. **在 "Port Range" 字段中，键入与传入和传出连接必须经过的指定接口相对应的端口。端口范围中不应包含任何空格。**

   如果不指定端口范围，SOCKS v5 条目将适用于所有端口。

   可以使用方括号 [ ] 包括范围两端的端口，也可使用圆括号 ( ) 将它们排除在外。例如，[1000-1010] 表示 1000 和 1010 之间包括 1000 和 1010 在内的所有端口号，而 (1000-1010) 表示 1000 和 1010 之间不包括 1000 和 1010 在内的所有端口号。另外，也可以混合使用方括号和圆括号。例如，(1000-1010] 表示 1000 和 1010 之间不包括 1000 但包括 1010 在内的所有端口号。

6. **在 "Interface/Address" 字段中，键入传入和传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方法，因此必须指定对这些方法的评估顺序。

注 – 传入和传出连接都应使用指定的接口，否则，传入路由将不同于所配置的接口并会收到错误消息。

▼ 创建代理路由条目

1. **访问服务器实例的 Server Manager 并单击 "SOCKS" 选项卡。**
2. **单击 "Set SOCKS v5 Routing" 链接。**
3. **在 "Proxy Routing" 部分中，单击 "Add" 按钮。**
4. **从 "Proxy Type" 下拉式列表中，选择通过其进行路由的 Proxy Server 的类型。可以使用以下选项：**
   - **SOCKS v5**
     - **SOCKS v4**
     - **Direct connection**
5. **在 "Destination Host Mask" 字段中，键入连接条目所请求的 IP 地址或主机名。**

   如果键入的是 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，以确定其是否为有效的目标主机。请勿在主机掩码条目中使用空格。如果不提供目标主机掩码，连接条目将适用于所有主机。

   例如，可在 "Destination Host Mask" 字段中键入 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此 IP 地址，并确定目标主机的 IP 地址是否与代理条目所请求的 IP 地址 (155.25.0.0) 匹配。
6. **在 "Destination Port Range" 字段中，键入代理条目所请求的目标主机的端口。**

   请勿在端口范围条目中使用空格。如果不指定端口范围，代理条目将适用于所有端口。

   可以使用方括号 [ ] 包括范围两端的端口，也可使用圆括号 ( ) 将它们排除在外。例如，[1000-1010] 表示 1000 和 1010 之间包括 1000 和 1010 在内的所有端口号，而 (1000-1010) 表示 1000 和 1010 之间不包括 1000 和 1010 在内的所有端口号。另外，也可以混合使用方括号和圆括号。例如，(1000-1010] 表示 1000 和 1010 之间不包括 1000 但包括 1010 在内的所有端口号。
7. **在 "Destination Proxy Address" 字段中，键入要使用的 Proxy Server 的主机名或 IP 地址。**
8. **在 "Destination Proxy Port" 字段中，键入 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方法，因此必须指定对这些方法的评估顺序。

▼ 编辑路由条目

1 访问服务器实例的 **Server Manager** 并单击 **"SOCKS"** 选项卡。

2 单击 **"Set SOCKS v5 Routing"** 链接。

3 选择要编辑的条目。

4 单击 **"Edit"** 按钮。

5 根据需要进行更改。

6 单击 **"OK"**。

▼ 删除路由条目

1 访问服务器实例的 **Server Manager** 并单击 **"SOCKS"** 选项卡。

2 单击 **"Set SOCKS v5 Routing"** 链接。

3 选择要删除的条目。

4 单击 **"Delete"** 按钮。

▼ 移动路由条目

条目按其在 `socks5.conf` 文件中出现的顺序进行评估。可以通过移动来更改其顺序。

1 访问服务器实例的 **Server Manager** 并单击 **"SOCKS"** 选项卡。

2 单击 **"Set SOCKS v5 Routing"** 链接。

3 选择要移动的条目。

4 单击 **"Move"** 按钮。

5 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

16 管理模板和资源

可以使用模板将 URL 分组在一起，以便配置代理如何处理这些分组。根据客户机尝试检索的 URL，可以使代理表现不同的行为。例如，在从特定域访问 URL 时，可以要求通过键入用户名和密码的方式进行客户机验证。或者，可以拒绝对指向图像文件的 URL 的访问。根据文件类型可以配置不同的高速缓存刷新设置。

本章包含以下各节：

关于模板

模板是称为资源的 URL 的集合。资源可以是单个 URL、具有共同点的一组 URL 或者整个协议。 您可以命名并创建一个模板，然后使用正则表达式将 URL 指定给该模板。这样，可以配置代理服务器按不同方式处理各种 URL 请求。任何可以使用正则表达式创建的 URL 模式都可以包括在模板中。下表列出了默认资源，并对其他模板提供了一些建议。

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 HTTP 请求
`gopher://.*`	所有 Gopher 请求
`connect://.*:443`	指向 HTTPS 端口的所有安全 SSL 事务。

表 16–1 资源正则表达式通配符模式 （续）

正则表达式模式	配置的内容
`http://home\.example\.com.*`	`home.example.com` Web 站点上的所有文档
`.*\.gif.*`	包括字符串 `.gif` 的任何 URL
`.*\.edu.*`	包括字符串 `.edu` 的任何 URL
`http://.*\.edu.*`	转向 `.edu` 域中的计算机的任何 URL

了解正则表达式

Proxy Server 允许您使用正则表达式标识资源。正则表达式指定字符串的模式。在 Proxy Server 中，正则表达式用于查找 URL 中匹配的模式。

以下示例说明了正则表达式：

```
[a-z]*://[^:/]*\.abc\.com.*
```

此正则表达式将匹配来自 `.abc.com` 域的任何文档。这些文档可以是任何协议，可以具有任何文件扩展名。

下表列出了正则表达式及其对应的含义。

表 16–2 正则表达式及其含义

表达式	含义
.	匹配除换行符之外的任何单个字符。
x?	匹配未出现或出现一次的正则表达式 *x*。
*x**	匹配未出现或出现多次的正则表达式 *x*。
x+	匹配出现一次或多次的正则表达式 *x*。
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* 出现至少 *n* 次。
x{n}	匹配字符 *x*，其中 *x* 正好出现 *n* 次。
[abc]	匹配括号中包含的任何字符。
[^abc]	匹配括号中不包含的任何字符。
[a-z]	匹配括号中范围内的任何字符。
x	匹配字符 *x*，其中 *x* 不是特殊字符。

表 16–2 正则表达式及其含义 （续）

表达式	含义
\x	去除特殊字符 *x* 的含义。
"x"	去除特殊字符 *x* 的含义。
xy	匹配出现的正则表达式 *x*，且紧跟出现正则表达式 *y*。
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。

以下示例说明了可以如何使用第 304 页中的 “了解正则表达式”中的一些正则表达式。

```
[a-z]*://([^.:/]*[:/]|.*\.local\.com).*
```

- `[a-z]*` 匹配任何协议的文档。
- `://` 匹配 (:)，且紧跟 (//)。
- `[^.:/]*[:/]` 匹配不包括 (.)、(:)或 (/) 的任何字符串，且紧跟 (:) 或 (/)。因此，此表达式匹配非全限定的主机名和包括端口号的主机。
- `|.*\.local\.com` 不匹配全限定主机名，如 `local.com`，但匹配 `.local.com` 域中的文档。
- `.*` 匹配具有任何文件扩展名的文档。

如第 304 页中的 “了解正则表达式”中所述，反斜杠可用于转义或去除特殊字符的含义。字符（如句点和问号）具有特殊含义，因此，如果使用它们表示其本身，必须进行转义。特别是，许多 URL 中都可以发现句点。因此，要在正则表达式中去除句点的特殊含义，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的列表，从而允许您指定从您的站点可以访问的 URL。根据具体使用情况，通配符的格式可以为正则表达式或 shell 表达式。通常：

- 对匹配目标 URL 的任何模式使用正则表达式。这包括 <Object ppath=...>、URL 过滤器以及 NameTrans、PathCheck 和 ObjectType 函数。
- 对于匹配传入的客户机或用户 ID 的任何模式，使用 shell 表达式，包括用于进行访问控制的用户名和组，以及传入用户的 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多个 URL。通配符使您可以根据 URL 中包含给定词的域名或任何 URL 进行过滤。例如，您可能需要屏蔽对包含字符串 "careers." 的 URL 的访问。为此，可以指定 `http://.*careers.*` 作为模板的正则表达式。

使用模板

▼ 创建模板

使用正则表达式通配符模式可以创建模板。然后，可以配置仅影响该模板中指定的 URL 的各个方面。例如，可以对 `.GIF` 图像使用一种类型的高速缓存配置，对纯 `.html` 文件使用另一种类型的高速缓存配置。

1. **访问 Server Manager 并单击 "Templates" 选项卡。**
   单击 "Create Template" 链接。此时将显示 "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"。**
   该名称应易于记忆。Server Manager 将提示您保存并应用更改。在为模板创建正则表达式后，可以保存更改，如以下步骤中所述。

▼ 应用模板

1. **访问 Server Manager 并单击 "Templates" 选项卡。**
2. **单击 "Apply Template" 链接。**
   此时将显示 "Apply Template" 页面。
3. **在 "URL Prefix Wildcard" 字段中，键入含有要包括在模板中的所有 URL 的正则表达式通配符模式。**
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"。**
   此时将显示 "Apply Changes" 页面。
7. **单击 "Restart Proxy Server" 按钮应用更改。**

▼ 删除模板

可以删除现有模板。删除模板将删除模板的所有关联配置。例如，如果对模板 TEST 中的所有 URL 设置了访问控制，删除 TEST 模板也将删除对该模板中包含的 URL 的访问控制。

1. **访问 Server Manager 并单击 "Templates" 选项卡。**
2. **单击 "Remove Template" 链接。**
   此时将显示 "Remove Template" 页面。
3. **选择 "Remove" 列表中的模板。**
4. **单击 "OK"。**
5. **单击 "Restart Required"。**
   此时将显示 "Apply Changes" 页面。
6. **单击 "Restart Proxy Server" 按钮应用更改。**

▼ 编辑模板

可以查看并编辑 Server Manager 中创建的模板。

1. **访问 Server Manager 并单击 "Templates" 选项卡。**
2. **单击 "View Template" 链接。**
   此时将显示 "View Template" 页面。模板显示在列出了模板和模板名称的正则表达式的表中。
3. **要编辑现有模板，请单击 "Edit Template Assignment" 链接。此时将显示 "Apply Template" 页面。**

删除资源

使用 "Remove Resource" 页面可以删除整个正则表达式对象及其对应的配置。例如，可以删除 gopher 资源，这样与该资源关联的所有设置将被从代理服务器的配置文件中删除。

▼ 删除资源

1. **访问 Server Manager 并单击 "Templates" 选项卡。**
2. **单击 "Remove Resource" 链接。**
   此时将显示 "Remove Resource" 页面。
3. **通过从 "Remove" 下拉列表中进行选择来选择要删除的资源。**
4. **单击 "OK"。**
5. **单击 "Restart Required"。**
   此时将显示 "Apply Changes" 页面。
6. **单击 "Restart Proxy Server" 按钮应用更改。**

◆ ◆ ◆ 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）。

当浏览器启动时，会装入自动配置文件。每当用户单击链接或键入 URL 时，浏览器都会使用此配置文件来确定是否应使用代理服务器，如果使用，应使用哪个代理服务器。通过此功能，您可以轻松地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。

- 可以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。
- 可以将此文件存储在浏览器可访问的 Web 服务器、FTP 服务器或任何网络目录中。将浏览器配置为通过提供文件的 URL 来查找此文件，因此可接受任何常规 URL。如果需要进行复杂的计算（例如，如果您的组织中具有庞大的代理链），则可以编写一个 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。
- 可以将自动配置文件连同每个浏览器副本一起存储在本地。但是，如果需要更新此文件，必须向每个客户机分发文件的副本。

可以采用以下两种方式之一创建自动配置文件：使用 Server Manager 中的页面或者手动创建。本章的后面部分将提供有关创建此类文件的说明。

本章包含以下各节：

了解自动配置文件

作为管理 Proxy Server 的人员，您还将创建和分发客户机自动配置文件。

自动配置文件的作用

自动配置文件采用 JavaScript 编写，JavaScript 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。浏览器将解释 JavaScript 文件。

首次装入浏览器时，将会下载自动配置文件。可以将此文件保存在浏览器可通过 URL 访问的任意位置。例如，可以将此文件保存在 Web 服务器中。倘若浏览器可以使用 file:// URL 访问到此文件，甚至可以将其保存在网络文件系统上。

代理配置文件采用 JavaScript 编写。JavaScript 文件定义了一个函数（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）。浏览器会向此 JavaScript 函数发送两个参数：运行浏览器的系统的主机名以及浏览器尝试获取的 URL。该 JavaScript 函数会向浏览器返回一个值，告知浏览器如何继续执行。

利用自动配置文件可以针对各种类型的 URL、各种服务器，或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）。换而言之，您可以具有多个专用代理服务器，例如，可使一个用作 .com 域，另一个用作 .edu 域，而再一个则用作其他的域。通过这种方法，可以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存储一个副本，而不是多个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。

您要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，通过在 "Proxies" 选项卡中键入代理自动配置文件的 URL 来进入此文件的 URL。代理服务器的 URL 具有如下格式：

`http://`*proxy.domain:port/URI*

例如，URL 可以为 `http://proxy.example.com`，这是格式为 host:port 组合的 URL 部分。但是，如果确实要使用 URI，则可以使用模板来控制对各个自动配置文件的访

问。例如，如果创建一个名为 /test 的 URI，其中包含一个名为 /proxy.pac 的自动配置文件，则可以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。

您可以创建多个自动配置文件，并通过不同的 URL 访问这些文件。下表列出了一些 URI 示例以及客户机用于访问这些 URI 的 URL。

表 17–1 URI 样例和相应的 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

对反向代理使用 PAC 文件

由于反向代理的工作方式，因此针对 .pac 文件使用代理服务器和服务器会很困难。当代理服务器收到文件请求时，它必须确定此请求是针对本地 .pac 文件还是针对远程文档。

要使代理服务器在除了维护和处理 .pac 文件之外还充当反向代理，请编辑 obj.conf 文件以确保 NameTrans 函数的顺序正确。

通过创建正则映射可使代理服务器用作反向代理。这通常会示意代理将所有请求都路由到远程内容服务器。您可以添加代理自动配置文件并将其映射到特定的目录（例如 /pac）。在这种情况下，任何希望获取 .pac 文件的客户机都将使用如下 URL：

```
http://proxy.mysite.com/pac
```

注意 – 如果进行此映射，请确保远程内容服务器中没有类似的目录。

编辑 obj.conf 文件，以确保用于代理自动配置文件的指令和函数出现在任何其他映射之前。此类指令和函数必须最先出现，因为代理服务器在处理请求之前，通常要先运行所有的 NameTrans 函数。然而，使用自动配置文件，代理可立即识别出此路径并返回 .pac 文件。

以下是一个 obj.conf 文件的示例，它使用了反向代理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 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。**

所显示的页面将列出代理的系统中具有的所有自动配置文件。您可以单击自动配置文件对其进行编辑。其余的步骤将介绍如何创建新文件。

3 **键入一个可选 URI，此为客户机从代理中获取自动配置文件时使用的 URL 的路径部分。**

例如，键入 / 可使客户机以代理的主文档（类似于 Web 服务器的 `index.html` 文件）形式访问该文件；此后，当客户机访问代理以获取自动配置文件时，将只使用域名。您可以使用多个 URI，并为每个 URI 创建单独的自动配置文件。

4 **使用 `.pac` 作为扩展名键入自动配置文件的名称。**

如果只有一个文件，则将其命名为 `proxy.pac` 即可。pac 是 proxy autoconfiguration（代理自动配置）的缩写。所有自动配置文件均为包含单个 JavaScript 函数的 ASCII 文本文件。

5 **单击 "OK"。此时会出现另一个页面。**

使用此页面创建自动配置文件。客户机将按顺序完成此页面中的各项。此页面中的项目包括：

- **Never Go Direct To Remote Server** 示意浏览器始终使用代理。您可以指定第二个代理服务器，以便在您的代理服务器未运行时使用。
- **Go Direct To Remote Server When** 确定何时跳过代理服务器。浏览器将按照选项在页面中的列出顺序确定这些情况：

- **Connecting To Non-fully Qualified Host Names** 在用户仅指定计算机名时使浏览器直接转至服务器。例如，如果内部 Web 服务器名为 `winternal.mysite.com`，则用户可以仅键入 `http://winternal` 而不用键入全限定域名。在这种情况下，浏览器直接转至此 Web 服务器而不是代理。
- **Connecting To A Host In Domain** 允许您指定浏览器可直接访问的域名，最多可以指定三个。指定域时，应以点字符开头。例如，可以键入 `.example.com`。
- **Connecting To A Resolvable Host** 在客户机可以解析主机时使浏览器直接转至服务器。将 DNS 设置为仅解析本地（内部）主机时，通常会使用此选项。连接到本地网络之外的服务器时，客户机将使用代理服务器。

注意 – 此选项会对客户机的性能产生负面影响，因为在每次进行请求时客户机都必须查询 DNS。

- **Connecting To A Host In Subnet** 在客户机访问特定子网中的服务器时使浏览器直接转至服务器。如果组织在某个地理区域中具有许多子网，此选项会很有用。例如，某些公司可能有一个域名，该域名适用于全球范围的各个子网，但是每个子网都专用于某个特定区域。

注意 – 此选项会对客户机的性能产生负面影响，因为在每次进行请求时客户机都必须查询 DNS。

- **Except When Connecting To Hosts** 允许您指定直接转至服务器规则的例外情况。例如，如果键入 `.example.com` 作为要直接转至的域，则可以将转至 `home.example.com` 作为一个例外情况。这样，当浏览器转至 `home.example.com` 时将使用代理，但可以直接转至 `example.com` 域中的任何其他服务器。
- **Secondary Failover Proxy** 指定第二个代理以便在您的代理服务器未运行时使用。
- **Failover Direct** 在代理服务器未运行时使浏览器直接转至服务器。如果指定了辅助故障转移代理，则 Navigator 在直接转至服务器之前，将尝试转至第二个代理服务器。

6 单击 "OK" 以创建自动配置文件。

该文件将存储在 *server-root*`/proxy-server`*id*`/pac` 目录中。

您将看到一条确认消息，说明已正确创建该文件。重复上述步骤，以创建所需数目的自动配置文件。

创建自动配置文件后，请确保告诉所有使用代理服务器的人员指向正确的自动配置文件，或亲自配置浏览器的各个副本。

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使用客户端 JavaScript 编写的。每个文件都包含一个名为 `FindProxyForURL()` 的 JavaScript 函数，用于确定浏览器应针对每个 URL 使用的代理服务器（如果有）。浏览器将向此 JavaScript 函数发送两个参数：目标原始服务器的主机名以及浏览器尝试获取的 URL。JavaScript 函数将向 Navigator 返回一个值，告知它如何继续执行。以下部分将介绍函数语法以及可能的返回值。

`FindProxyForURL()` 函数

`FindProxyFor()` URL 函数的语法如下：

```
function FindProxyForURL(url, host){   ...}
```

对于浏览器访问的每个 URL，浏览器都会发送 *url* 和 *host* 参数，并按如下方式调用此函数：

```
ret = FindProxyForURL(url, host);
```

url 是要在浏览器中访问的完整 URL。

host 是从要访问的 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

自动配置文件包含函数 `FindProxyForURL()`。此函数使用客户机主机名以及所访问的 URL 作为参数。此函数将返回一个字符串，告知浏览器如何继续执行。如果字符串为空，则不应使用任何代理。此字符串可以包含下表所示的任意数目的生成块，其间以分号隔开。

表 17–2 `FindProxyForURL()` 返回值

返回值	引起的浏览器操作
`DIRECT`	不通过任何代理直接与服务器建立连接。
`PROXY` *host:port*	使用指定的代理和端口号。如果存在多个以分号隔开的值，则使用第一个代理。如果此代理失败，则使用下一个代理，依此类推。
`SOCKS` *host:port*	使用指定的 SOCKS 服务器。如果存在多个以分号隔开的值，则使用第一个代理。如果此代理失败，则使用下一个代理，依此类推。

如果浏览器遇到不可用的代理服务器，则浏览器将每隔 30 分钟自动重试一次先前未响应的代理，在 30 分钟之后进行第一次重试，在 1 小时之后进行第二次重试，依此类推。因此，如果您暂时关闭了代理服务器，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。

如果所有代理均出现故障，且未指定 DIRECT 返回值，浏览器将询问用户是否应暂时忽略代理而尝试直接进行连接浏览器将询问是否应在 20 分钟后重试代理，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。

在以下示例中，返回值告知浏览器使用端口 8080 上名为 `w3proxy.example.com` 的代理。如果此代理不可用，则浏览器将使用端口 8080 上名为 `proxy1.example.com` 的代理：

```
PROXY w3proxy.example.com:8080; PROXY proxy1.example.com:8080
```

在下一个示例中，主代理为 `w3proxy.example.com:8080`。如果此代理不可用，则浏览器将使用 `proxy1.example.com:8080`。如果这两个代理都不可用，则浏览器将直接转至服务器。20 分钟之后，浏览器会询问用户是否应重试第一个代理。

```
PROXY w3proxy.example.com:8080; PROXY proxy1.example.com:8080; DIRECT
```

JavaScript 函数和环境

JavaScript 语言具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 true 或 false 值。相关的实用程序函数属于例外情况，因为它们返回 DNS 主机名或 IP 地址。您可以在主 `FindProxyForURL()` 函数中使用这些函数，以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，请参见本章后面的示例。

本节将介绍各个函数或环境条件。适用于浏览器与代理集成的函数和环境条件如下：

- 主机名函数包括：
  - `dnsDomainIs()()`
  - `isInNet()()`
  - `isPlainhost name()()`
  - `isResolvable()()`
  - `localHostOrDomainIs()()`
- 实用程序函数包括：
  - dnsDomainLevels()
  - dnsResolve()
  - myIpAddress()
- 基于 URL/主机名的条件包括：
  - shExpMatch()
- 基于时间的条件包括：

- 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（如果有）。

dnsDomainIs()(host, domain)

dnsDomainIs()() 函数将检测 URL 主机名是否属于给定的 DNS 域。如果要将浏览器配置为不对本地域使用代理，则此函数很有用，如第 323 页中的 “示例 1：代理除本地主机之外的所有服务器”和第 324 页中的 “示例 2：代理防火墙外部的本地服务器”中所示。

在某些情况下会基于 URL 所属的 DNS 域从一组代理中选择接收请求的代理，当您在这些情况下使用多个代理进行负载平衡时，此函数也很有用。例如，如果要通过将包含 .edu 的 URL 定向到一个代理，而将包含 .com 的 URL 定向到另一个代理来进行负载平衡，则可以使用 dnsDomainIs()() 来检查 URL 主机名。

参数

host 是 URL 中的主机名。

domain 是对主机名进行测试所用的域名。

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)

使用 isInNet()() 函数，可以将 URL 主机名解析为 IP 地址，并测试它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。请参见第 325 页中的 “示例 4：直接连接到子网”。

参数：

host 是 DNS 主机名或 IP 地址。如果传递的是主机名，此函数会将其解析为 IP 地址。

pattern 是采用点分隔格式的 IP 地址模式。

mask 是 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；值为 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()()` 函数将检测所请求 URL 中的主机名是普通主机名还是全限定域名。如果希望浏览器直接连接到本地服务器，则此函数会很有用，如第 323 页中的 “示例 1：代理除本地主机之外的所有服务器”和第 324 页中的 “示例 2：代理防火墙外部的本地服务器”中所示。

参数

host 是 URL 中的主机名，仅当主机名中没有域名（无带点的段）时才不包括端口号。

返回值

如果 *host* 为本地的，则返回 true；如果 *host* 为远程的，则返回 false

示例

```
isPlainhost name("host")
```

如果 *host* 为形如 `www` 的字符串，此函数返回 true。如果 host 为形如 `www.example.com` 的字符串，此函数返回 false。

isResolvable()(host)

如果防火墙内的 DNS 仅识别内部主机，则可以使用 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，可以将浏览器配置为对内部服务器使用直接连接，而仅对外部服务器使用代理。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()() 函数通过查询 DNS 尝试将主机名解析为 IP 地址。请参见第 324 页中的 “示例 3：仅代理未解析的主机” 。

参数

host() 是 URL 中的主机名。

返回值

如果此函数可以解析主机名，则返回 true；如果不能解析，则返回 false

示例

```
isResolvable("host")
```

如果 host() 为形如 www 的字符串，并可通过 DNS 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。请参见第 324 页中的 “示例 2：代理防火墙外部的本地服务器” 。

如果主机名与指定的主机名完全匹配，或者主机名中没有与非限定主机名匹配的域名部分，localHostOrDomainIs()() 函数将返回 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")
```

实用程序函数

通过实用程序函数，可以查明域级别、运行浏览器的主机或主机的 IP 地址。

dnsDomainLevels()(host)

`dnsDomainLevels()()` 函数查找 URL 主机名中的 DNS 级别数（圆点数）。

参数

host 是 URL 中的主机名。

返回值

DNS 域级别数（整数）。

示例

`dnsDomainLevels("www")` 将返回 0。

`dnsDomainLevels("www.example.com")` 将返回 2。

dnsResolve()(host)

`dnsResolve()()` 函数解析给定主机（通常来自 URL）的 IP 地址。如果 JavaScript 函数必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。将给定的 DNS 主机名解析为 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：

如果要在计算机 home.example.com 上运行 Navigator，以下示例将返回字符串 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()() 函数将对 URL 主机名或 URL 本身进行匹配。此函数的主要用途是进行负载平衡并将 URL 以智能化方式路由到不同的代理服务器。

参数

str 是要比较的任何字符串（例如，URL 或主机名）。

shexp 是进行比较时所依据的 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。请参见第 326 页中的 “示例 6：使用 shExpMatch()() 平衡代理负载”。

返回值

true 或 false

示例

第一个示例将返回 true。第二个示例将返回 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

您可以使 **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()()` 函数检测某个特定日期或日期范围，例如 1996 年 4 月 19 日到 1996 年 5 月 3 日。如果您希望 `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，代表一个月中的某日。

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 可以是字符串 "GMT"，表示应采用格林尼治标准时间进行时间比较；也可以留空，从而假定时间采用本地时区。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。如果在每个类别 (day, month, year) 中仅指定一个值，则此函数仅在与指定值匹配的日子才会返回 true 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)`

以下语句在格林尼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()` 函数检测一天中的某个特定时间或时间范围，例如 9 p.m. 到 12 a.m.。如果您希望 `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 11:00 p.m.）。

min 为分钟数，范围从 0 到 59。

sec 为秒数，范围从 0 到 59。

gmt 可以是字符串 GMT（表示 GMT 时区），也可以未指定（表示本地时区）。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 1:00 p.m.为 true：`timerange(12, 13)`

以下语句从 GMT 时间正午到 12:59 p.m. 为 true：`timerange(12, "GMT")`

以下语句从 9:00 a.m. 到 5:00 p.m.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() 函数检测某一特定周日或某一周日范围，例如星期一到星期五。如果您希望 *FindProxyForURL* 函数视具体星期几而执行不同的操作，则此函数将很有用。

参数

wd1 和 *wd2* 为以下任意一个周日字符串：`SUN MON TUE WED THU FRI SAT`

gmt 可以是 GMT（表示格林尼治标准时间），也可以留空（表示本地时间）。

只有第一个参数 *wd1* 为强制性参数。*wd2*、*gmt* 可以分别留空或同时留空。

如果只有一个参数，则此函数将在该参数所表示的周日返回 true 值。如果指定字符串 GMT 作为第二个参数，则采用 GMT 时间，否则，采用本地时区的时间。

如果 *wd1* 和 *wd2* 均被定义，则该条件在当前周日介于这两个周日之间时为 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（本地时区）为 true。`weekdayRange("MON", "FRI")`

以下语句从格林尼治标准时间星期一到星期五为 true。`weekdayRange("MON", "FRI", "GMT")`

以下语句在本地时间星期六为 true。`weekdayRange("SAT")`

以下语句在格林尼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")`

函数示例

本节提供详细的 JavaScript 函数示例。

示例 1：代理除本地主机之外的所有服务器

在本例中，浏览器直接连接到非全限定的所有主机以及本地域中的主机。所有其他主机均要经过名为 `w3proxy.example.com:8080` 的代理。

注 – 如果此代理出现故障，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：代理防火墙外部的本地服务器

本例类似于第 323 页中的 “示例 1：代理除本地主机之外的所有服务器”，只是它将对防火墙外部的本地服务器使用代理。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` 域中除本地主机之外的所有主机使用代理。主机 `www.example.com` 和 `merchant.example.com` 也要经过代理。

指定适当的例外情况顺序可以提高效率：`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 *and* 表达式之前的 *or* 表达式两边的括号。

示例 3：仅代理未解析的主机

本例适用于内部 DNS 仅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。

```
function FindProxyForURL(url, host)
{
    if (isResolvable(host))
            return "DIRECT";
        else
            return "PROXY proxy.mydomain.com:8080";
}
```

本例要求每次都查询 DNS。因此，可将本例与其他规则组合在一起使用，以便仅在其他规则无法生成结果时查询 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。

```
function FindProxyForURL(url, host)
{
    if (isInNet(host, "198.95.0.0", "255.255.0.0"))
        return "DIRECT";
    else
        return "PROXY proxy.mydomain.com:8080";
}
```

在本例中，可以通过在开头添加冗余规则来最大程度地减少对 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：使用 dnsDomainIs()() 平衡代理负载

本例较为复杂。它使用四个代理服务器，其中一个充当其他服务器的热备份。如果其余三个代理服务器中的任何一个出现故障，则第四个服务器将进行接管。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服务器上均有一个副本。分配负载如下表所示。

表 17–3 平衡代理负载

代理	用途
#1	.com 域
#2	.edu 域
#3	其他所有域
#4	热备份

所有本地访问均应为直接访问。所有代理服务器都在端口 8080 上运行。您可以使用 + 运算符来串联字符串。

```
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：使用 shExpMatch()() 平衡代理负载

本例与第 325 页中的 “示例 5：使用 dnsDomainIs()() 平衡代理负载”基本相同，但本例使用的是 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，使其用于特定的协议。在 FindProxyForURL()() 函数中，可以使用大多数标准 JavaScript 功能。例如，要根据协议设置不同的代理，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()()` 函数也可以实现此配置；例如：

```
...
if (shExpMatch(url, "http:*")) {
    return "PROXY http-proxy.mydomain.com:8080;
}
...
```

◆ ◆ ◆ 第 18 章

18 ACL 文件语法

访问控制列表 (Access Control List, ACL) 文件是指包含定义何人可以访问 Proxy Server 资源的列表的文本文件。默认情况下，Proxy Server 使用一个包含访问服务器的所有列表的 ACL 文件。此外，还可以在 `obj.conf` 文件中创建和引用多个 ACL 文件。

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。有关控制访问 Proxy Server 及其资源的详细信息，请参见第 8 章。Proxy Server 版本 4 中支持资源模板，如第 16 章中所述。

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 文件都必须以单个语法版本号开头。例如：

```
version 3.0;
```

版本行可以在所有注释行之后显示。Proxy Server 使用语法版本 3.0。可以通过在注释行的开头使用 # 符号将注释包括在文件中。

文件中的每个 ACL 都以定义其类型（路径、资源或命名）的语句开头。

- 路径 ACL 指定它们所影响的资源的绝对路径。
- 资源 ACL 指定它们所影响的模板，例如 `http://`、`https://`、`ftp://` 等。有关这些模板的更多信息，请参见第 16 章。
- 命名 ACL 指定在 `obj.conf` 文件内的资源中引用的名称。服务器带有一个默认命名资源，任何用户都可以对其进行读取访问，但只有 LDAP 目录中的用户可以对其进行写入访问。尽管可以通过 Proxy Server 用户界面创建命名 ACL，但是您必须对 `obj.conf` 文件中的资源手动引用命名 ACL。

路径 ACL 和资源 ACL 可以包括通配符。有关通配符的更多信息，请参见第 16 章。

类型行以字母 acl 开头，然后将类型信息置于双引号中，其后紧跟分号。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，便可以包含一个或多个验证语句，可定义用于 ACL 的方法。此外，还可以包括授权语句，用于定义被允许或拒绝进行访问的用户和计算机。以下各部分将介绍这些语句的语法。

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。这三种常见方法为：

- Basic（默认）
- Digest
- SSL

Basic 和 Digest 方法要求用户提供用户名和密码，然后才能访问资源。

SSL 验证方法要求用户具有客户机证书。要进行验证，必须针对 Proxy Server 启用加密功能，并且用户的证书签发者必须位于信任的 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 Basic 验证方法。服务器的验证数据库必须支持用户发出的 Digest 验证。

每个验证行都必须指定服务器将验证的属性：用户、组或者用户和组。以下验证语句（位于 ACL 类型行之后）将 Basic 验证指定给与数据库或目录中单个用户相匹配的用户：

```
authenticate(user) { method = "basic";};
```

以下实例将 SSL 用作用户和组的验证方法：

```
authenticate(user, group) { method = "ssl";};
```

以下实例允许用户名以 sales 一词开头的所有用户进行访问：

```
allow (all) user = "sales*";
```

如果将最后一行更改为 group = sales，ACL 将失败，因为未对组属性进行验证。

授权语句

每个 ACL 项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。由于规则具有分层结构，因此在第一条规则中拒绝所有用户的访问，然后在接下来的规则中具体指定允许哪些用户、组或计算机进行访问。例如，如果允许所有用户访问名为 /my_files 的目录，而允许少数用户访问子目录 /my_files/personal，则无法实现对该子目录的访问控制，因为有权访问 /my_files 目录的所有用户同时也有权访问 /my_files/personal 目录。要防止出现上述情况，请为子目录创建一条规则，先拒绝任何用户访问，然后允许少数需要访问的用户访问。

但在某些情况下，如果将默认 ACL 设置为拒绝所有用户访问，其他 ACL 规则将不需要 "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 中的分层结构取决于资源。当服务器收到对特定资源的请求时，它会生成一个适用于此资源的 ACL 列表。服务器首先将列出的命名 ACL 添加到其 obj.conf 文件的 check-acl 语句中，然后附加匹配的路径 ACL 和资源 ACL。按照相同的顺序对此列表进行处理。除非出现 "absolute" ACL 语句，否则将依次验证所有语句。如果 "absolute allow" 或 "absolute deny" 语句验证为 "true"，服务器将停止处理并接受此结果。

如果有多个匹配的 ACL，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的用户名、组名、主机名或 IP 地址来定义允许或拒绝哪些用户进行访问。以下行提供的实例显示了如何为不同的用户或计算机授予访问权限：

- `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 小时制指定时间，例如使用 0400 指定 4:00 a.m. 或使用 2230 指定 10:30 p.m.。以下实例将名为 guests 的用户组限制为在 8:00 a.m. 到 4:59 p.m. 这段时间进行访问。

```
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 组的用户在任意一天的任何时间进行访问。discount 组的用户在周末全天以及平日除 8 a.m. 到 4:59 p.m. 这段时间之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。以下运算符可以用于 user、group、dns 和 ip：

- and
- or
- not
- =（等于）
- !=（不等于）

以下运算符可以用于 timeofday 和 dayofweek：

- 大于
- < 小于
- = 大于等于
- <= 小于等于

默认 ACL 文件

安装之后，*server_root*/httpacl/generated.proxy- *serverid*.acl 文件为服务器提供了默认设置。在用户界面中创建设置之前，服务器将使用工作文件 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，必须将字符置于双引号中。

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置于双引号中。

在 obj.conf 文件中引用 ACL 文件

在 obj.conf 文件的 PathCheck 指令中，可以通过使用 check-acl 函数来引用命名 ACL 或单独的 ACL 文件。该行使用以下语法：

```
PathCheck fn="check-acl" acl="aclname "
```

其中，*aclname* 是任何 ACL 文件中出现的 ACL 的唯一名称。

例如，要使用名为 testacl 的 ACL 限制对某个目录的访问，可以将下列各行添加到 obj.conf 文件中：

```
<Object ppath="https://"PathCheck fn="check-acl" acl="testacl"</Object>
```

在此实例中，第一行是对象，用于声明要对其进行访问限制的服务器资源。第二行是 PathCheck 指令，此指令使用 check-acl 函数将命名 ACL (testacl) 绑定到指令所在的对象中。testacl ACL 可以位于 server.xml 内引用的任何 ACL 文件中。

◆ ◆ ◆ 第 19 章

19 调节服务器性能

在 Proxy Server 环境中，许多元素会影响性能，其中包括代理客户机、Proxy Server、原始服务器和网络。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。

本附录包含以下各节：

常规性能注意事项

本节介绍分析 Proxy Server 性能时应考虑的常规问题。

本节包含以下主题：

- 第 337 页中的 “安全性要求”
- 第 337 页中的 “Solaris 文件系统高速缓存”

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在访问 Proxy Server 以及他们请求了哪些页面。

通过在 obj.conf 文件中注释掉以下指令，可以禁用 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高速缓存在 ACL 用户高速缓存中。您可以使用 magnus.conf 文件中的 ACLCacheLifetime 指令来控制 ACL 用户高速缓存保持有效的时间。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。

ACLCacheLifetime 的默认值为 120 秒，这意味着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，此设置将会对 Proxy Server 的性能产生负面影响。如果将 ACLCacheLifetime 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，因为此设置将强制 Proxy Server 查询 LDAP 服务器。只有在 LDAP 目录不经常改变时才设置一个较大的值。

ACLUserCacheSize 是一个 `magnus.conf` 参数，用于配置高速缓存中可以保存的最大条目数。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，此列表末尾的条目将被删除以便容纳新条目。

此外，还可以使用 *ACLGroupCacheSize* 参数来设置每个用户条目可以高速缓存的最大组成员数。默认值为 4。由于组中不属于成员的用户不会被高速缓存，因此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

可以在服务器的套接字中指定发送缓冲区的大小 (SndBufSize) 和接收缓冲区的大小 (RcvBufSize)。这些参数可以在 `magnus.conf` 文件中进行配置。对于不同的 UNIX 和 Linux 操作系统，建议的值会有所不同。请参阅操作系统的文档以正确设置这些参数。

连接超时

可以使用 magnus.conf 文件中的 *AcceptTimeout* 参数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，则会关闭连接。默认情况下，将此参数设置为 30 秒。在大多数情况下，不需要更改此设置。您可以通过将此参数设置为小于默认值来释放线程，但这样做可能会导致断开连接速度较慢的用户的连接。

错误日志级别

增大 server.xml() 文件 LOG 标记中的 loglevel 属性值会导致服务器在错误日志中生成和存储更多信息。然而，将条目写入此文件中会影响性能。请仅在调试问题时增大日志记录级别，而在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 会提高 Proxy Server 的保密性和安全性，但是也会影响性能，因为对数据包进行加密和解密会导致发生系统开销。您可能需要考虑将加密和解密处理工作转移给硬件加速器卡。

Solaris 文件系统高速缓存

Proxy Server 高速缓存并未存储在随机存取存储器中。每次从高速缓存中提取文档时，都会对文件系统进行文件访问操作。您可能需要考虑使用 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，将会从内存而不是从文件系统中提取对高速缓存的文件的引用。

超时值

超时对服务器性能具有显著影响。为 Proxy Server 设置最佳超时值有助于节省网络资源。

在 Proxy Server 中，可以使用两个特定于实例的 SAF（server application function，服务器应用函数）以及一个全局参数来配置超时值：

- 第 338 页中的 “init-proxy() SAF（obj.conf 文件）”
- 第 338 页中的 “http-client-config() SAF（obj.conf 文件）”
- 第 339 页中的 “KeepAliveTimeout() SAF（magnus.conf 文件）”

init-proxy() SAF（obj.conf 文件）

init-proxy() 函数用于初始化 Proxy Server 的内部设置。此函数在 Proxy Server 初始化过程中被调用，但还应在 obj.conf 文件中进行指定以确保正确初始化各值。

此函数的语法如下：

```
Init fn=init-proxy timeout=seconds timeout-2=seconds
```

在上例中，对 Proxy Server 的 init-proxy SAF 超时设置直接应用了以下参数：

- timeout（代理超时）－代理超时参数用于指示服务器等待多长时间后退出闲置连接。如果代理超时值较高，会将重要的代理线程长时间地调配给可能出现故障的客户机使用。如果超时值较低，会退出需要较长时间才产生结果的 CGI 脚本，例如数据库查询网关。

  要确定服务器的最佳代理超时值，请考虑以下问题：

  - Proxy Server 是否要处理许多数据库查询或 CGI 脚本?
  - Proxy Server 所处理的请求数是否少到可以随时腾出进程?

    如果对上述任一问题的回答是肯定的，则可以决定设置较高的代理超时值。建议的最高代理 *timeout* 值为 1 小时。默认值为 300 秒（5 分钟）。

    通过访问 Server Manager 中 "Preferences" 选项卡下的 "Configure System Preferences" 页面，可以查看或修改代理超时值。使用 "Proxy Timeout" 来指代此参数。

  timeout-2（中断后超时）－中断后超时值指示 Proxy Server 在客户机退出事务后继续写入高速缓存文件的时间。换而言之，如果客户机在 Proxy Server 几乎已完成对文档的高速缓存时退出连接，则服务器可以继续对文档进行高速缓存，直至达到中断后超时值为止。

  建议的最高中断后超时值为 5 分钟。默认值为 15 秒。

http-client-config() SAF（obj.conf 文件）

http-client-config 函数用于配置 Proxy Server 的 HTTP 客户机。

此函数的语法如下：

```
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"
```

这些设置包括：

- keep-alive－（可选）布尔值，指示 HTTP 客户机是否应尝试使用持久性连接。默认值为 true。
- keep-alive-timeout－（可选）使持久性连接保持打开状态的最大秒数。默认值为 29。
- always-use-keep-alive－（可选）布尔值，指示 HTTP 客户机是否可以对所有类型的请求重复使用现有持久性连接。默认值为 false，表示对于非 GET 请求或含有主体的请求，将不重复使用持久性连接。
- protocol－（可选）HTTP 协议版本字符串。默认情况下，HTTP 客户机使用 HTTP/1.0 或 HTTP/1.1，具体取决于 HTTP 请求的内容。除非遇到特定的协议互操作性问题，否则不要使用 protocol 参数。
- proxy-agent－（可选）代理服务器代理程序 (Proxy-agent) HTTP 请求标头的值。默认值为包含 Proxy Server 产品名和版本的字符串。

`KeepAliveTimeout()` SAF（`magnus.conf` 文件）

`KeepAliveTimeout()` 参数确定服务器使客户机与 Proxy Server 之间的 HTTP 保持活动连接或持久性连接处于打开状态的最长时间（以秒为单位）。默认值为 30 秒。如果闲置时间超过 30 秒，则连接会超时。最大值为 300 秒（5 分钟）。

注意 – `magnus.conf` 文件中的超时设置适用于客户机与 Proxy Server 之间的连接。`obj.conf` 文件内 `http-client-config` SAF 中的超时设置适用于 Proxy Server 与原始服务器之间的连接。

最新性检查

Proxy Server 通过从本地高速缓存提供文档而不是从原始服务器中获取文档来提高性能。这种方法的一个缺点是可能会提供过时的文档。

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。只应在必要时执行这种最新性检查，因为频繁地检查文档会降低 Proxy Server 的总体性能。

最新性检查在 "Caching" 选项卡的 "Set Cache Specifics" 页面中进行配置。默认设置为每两小时检查一次是否有新文档。可以在 ObjectType 指令中使用 max-uncheck 参数来配置此信息。

为了提高服务器的性能，同时确保文档是最新的，可对最新性检查进行自定义，方法是结合上次修改因子确定合理的文档生命周期。

上次修改因子

上次修改因子有助于根据先前已记录的更改来确定文档发生变化的可能性。

上次修改因子是介于 .02 与 1.0 之间的小数。将其与上次实际修改文档的时间和上次执行文档最新性检查时间之间的间隔相乘，然后将生成的数值与上次执行最新性检查到现在为止的时间进行比较。如果此数值小于这段时间间隔，则表明文档尚未过期。不过，如果此数值大于这段时间间隔，则表明文档已过期，将从原始服务器中获取新版本。

上次修改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。

应将上次修改因子设置为介于 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。如果配置不合理，此系统会独占重要的 Proxy Server 资源。要优化性能，请考虑以下选项：

- 启用 DNS 高速缓存。

  在 Server Manager 的 "Preferences" 选项卡下选择 "Configure DNS Cache" 链接，可以启用 DNS 高速缓存。选择对应于 DNS 高速缓存的 "Enabled" 单选按钮。
- 仅记录客户机 IP 地址而不记录客户机 DNS 名称。

  在 Server Manager 的 "Server Status" 选项卡下选择 "Set Access Log Preferences" 链接，可以禁用客户机 DNS 名称日志记录。选择 "IP Addresses" 单选按钮以记录 IP 地址而不记录客户机主机名。
- 禁用反向 DNS。

  反向 DNS 可将 IP 地址转换为主机名。在 Server Manager 的 "Preferences" 选项卡下选择 "Configure System Preferences" 链接，可以禁用反向 DNS。选择 "No" 单选按钮以禁用反向 DNS。
- 避免基于客户机主机名进行访问控制。

  如果可能，在访问控制语句中使用客户机的 IP 地址而不使用主机名。

线程数

magnus.conf 文件中的 RqThrottle 参数用于指定 Proxy Server 可以处理的最大并发事务数。默认值为 128。更改此值可以调节服务器，从而最大程度地缩短所执行事务的等待时间。

为了计算并发请求数，服务器会对活动请求进行计数。当新请求到达时，服务器会将计数值加一；当服务器完成请求时，会从计数中减一。当新请求到达时，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，则会推迟处理新请求，直至活动的请求数降至最大数量以下。

通过查看由 `perfdump` 生成的 SessionCreationInfo 部分的数据，或查看 `proxystats.xml` 数据，可以监视并发请求数。利用此信息，可以确定与总线程数（限制）相比最大并发请求数（峰值）。以下信息来自 `perfdump` 输出：

```
SessionCreationInfo:
------------------------
Active Sessions          1
Keep-Alive Sessions      0
Total Sessions Created   48/128
```

Active Sessions 显示当前正在处理请求的会话（请求处理线程）数。Keep-Alive Sessions 与 Active Sessions 类似，但是专用于显示保持活动连接数。Total Sessions Created 同时显示创建的会话数以及允许的最大会话数。这些值是 RqThrottle 值的最小值和最大值。

注意 – 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此参数。

达到所配置的最大线程数并非表明情况一定是不理想的。您不必自动增加 RqThrottle 值。达到此限制意味着服务器在峰值负载下需要这么多线程。只要服务器能够及时处理请求，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 `perfdump` 输出有规律地显示创建的会话总数值经常接近 RqThrottle 的最大值，则请考虑增大线程限制。

合适的 RqThrottle 值范围为 100 到 500，具体取决于负载。

入站连接池

可以使用 magnus.conf 中的 KeepAlive* 及相关设置对入站连接池进行调节，其中包括下列设置：

- MaxKeepAliveConnections
- KeepAliveThreads
- KeepAliveTimeout
- KeepAliveQueryMaxSleepTime
- KeepAliveQueryMeanTime
- ConnQueueSize
- RqThrottle
- acceptorthreads

有关这些参数的更多信息，请参见《Sun ONE Web Server 6.1 Performance Tuning, Sizing, and Scaling Guide》的第 2 章，其网址为：

http://docs.sun.com/app/docs/doc/819-6516/

在此版本的 Proxy Server 中无法配置出站连接池设置。

FTP 列表宽度

如果增加 FTP 列表宽度，则允许使用较长的文件名，因而会减少文件名截断现象。默认宽度为 80 个字符。

在 Server Manager 的 "Preferences" 选项卡下选择 "Tune Proxy" 链接，可以修改 FTP 列表宽度。

高速缓存体系结构

合理地配置高速缓存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。

正确设置高速缓存对于 Proxy Server 的性能至关重要。设置代理高速缓存布局时应记住的最重要规则是分配负载。应将高速缓存设置为每个分区大约具有 1 GB 的空间，并且应分布在多个磁盘和多个磁盘控制器中。与采用单个大容量的高速缓存相比，采用这种布置可以更快地创建和检索文件。

高速缓存批量更新

通过高速缓存批量更新功能，可以从指定的 Web 站点预先装入文件，或对高速缓存中已存在的文档执行最新性检查。当 Proxy Server 中的负载最低时，通常会启动此功能。您可以在 "Cache Batch Updates" 页面中批量创建、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，或预先装入某个特定 Web 站点的多个文件。

在具有服务器和代理网络的大型站点中，可能需要使用批量更新来预先装入此 Web 的给定区域。批处理进程可以跨文档中的链接执行递归下降分析，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。`bu.conf` 配置文件中的参数有助于防止该进程无限期地执行递归，可对该进程进行一定程度的控制。

使用 Proxy Server 访问日志可以确定哪些站点使用频率最高，并对这些站点执行批量更新以提高性能。

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。垃圾收集是一个占用大量资源的过程。因此，可能需要调节某些垃圾收集设置以提高性能。

以下参数具有对垃圾收集过程进行微调的能力。可以在 "Tune Garbage Collection" 表单上查看或修改这些参数，在 Server Manager 的 "Caching" 选项卡下选择 "Tune GC" 即可找到此表单。这些参数包括：

- *gc hi margin percent*
- *gc lo margin percent*
- *gc extra margin percent*
- *gc leave fs full percent*

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，达到此百分比时，将触发垃圾收集。

此值必须高于 gc lo margin percent 的值。

gc hi margin percent 的有效范围为 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，垃圾收集器以此百分比作为目标。

此值必须低于 gc hi margin percent 的值。

gc lo margin percent 的有效范围为 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部分。

gc extra margin percent 的有效范围为 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，低于此百分比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 的有效范围为 0（允许全部删除）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 19–1 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。将此参数设置为 0 意味着缓冲区空间不足不会影响性能。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	
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	对于通信流量高的 Web 站点，请降低此值。

表 19–1 Solaris 性能调节参数 （续）

参数	范围	默认值	调节后的值	注释
tcp_rexmit_interval_initial	ndd/dev/tcp	3000	3000	如果重新传输量超过 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	使用此参数可以增大传输缓冲区。
tcp_recv_hiwat	ndd/dev/tcp	8129	32768	使用此参数可以增大接收缓冲区。

有关这些参数的更多信息，请参见《Sun ONE Web Server 6.1 Performance Tuning, Sizing, and Scaling Guide》的第 5 章，网址为：

http://docs.sun.com/app/docs/doc/819-6516/

索引

B

C

D

E

L

M

N

O

废

分

服

父

管

归

过

缓

基

加

语

远

允

运

摘

侦

整

正