管理员指南

Sun™ ONE Web Server

版本 6.1

817-7511
2004 年 4 月

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

目录

关于本指南

本指南介绍了如何配置和管理 Sun™ Open Net Environment (Sun ONE) Web Server 6.1。适用于公司企业中希望通过万维网将客户机服务器应用程序扩展到更大范围的信息技术管理员。

本前言包括以下部分：

本指南的内容

本指南介绍了如何配置和管理 Sun ONE Web Server。配置服务器后，可以通过本指南学习如何维护服务器。

安装服务器后，可以在服务器根目录下的 `/manual/https/ag` 中获得本指南的 HTML 版本。缺省情况下，服务器根目录为 `C:\Sun\WebServer6.1\` 或 `/opt/SunWwbsvr`。

本指南的组织结构

本指南包含五部分、一个词汇表和一个综合索引。如果您不熟悉 Sun ONE Web Server 6.1，请先阅读第一部分 “服务器基础知识”，概要了解该产品。如果您已经熟悉此版本的 Sun ONE Web Server，请快速浏览第一部分 “服务器基础知识”的内容，然后再进入第二部分 “使用 Administration Server”。

熟悉 Administration Server 的基本操作后，可以阅读第三部分 “配置、监视和性能优化”，该部分包括如何配置和监视 Sun ONE Web Server 的实例。第四部分 “管理虚拟服务器和服务”介绍了有关使用程序和配置式样的信息。

最后一部分附录，介绍了有关各种主题的特定参考主题，其中包括：超文本传输协议 (HTTP)、服务器配置文件、ACL 文件、国际化问题、服务器扩展以及 Sun ONE Web Server 用户界面参考，您可能需要查看这些内容。请注意，用户界面附录只能从联机版本中获得。

第一部分：服务器基础知识

本部分概述了 Sun ONE Web Server。其中包括以下各章：

- 第 1 章 “Sun ONE Web Server 简介”概述了 Sun ONE Web Server。
- 第 2 章 “管理 Sun ONE Web Server”介绍了如何通过 Administration Server 管理 Sun ONE Web Server。

第二部分：使用 Administration Server

本部分详细介绍了有关使用 Administration Server 管理 Sun ONE Web Server 的概念和过程。其中包括以下各章：

- 第 3 章 “管理用户和组”介绍了如何使用 “Administration Server Users”和 “Groups”表单配置 Sun ONE Web Server。
- 第 4 章 “用于 Web 容器和 Web 应用程序的 基于 J2EE 的安全性”介绍了如何对 Sun ONE Web Server 进行安全配置，并讨论了以下两种安全模式：基于 ACL 的访问控制和基于 Java™ 2 Platform, Enterprise Edition (J2EE™)/Servlet 的验证和授权。
- 第 5 章 “设置管理首选项”介绍了如何使用 “Administration Server Preferences”和 “Global Settings”表单配置 Sun ONE Web Server。

- 第 6 章 “使用证书和密钥”介绍了如何使用证书和公共密钥提高安全性。请注意，在阅读本章内容之前，应熟悉公共密钥加密和安全套接字层 (SSL) 协议的基本概念。这些概念包括加密和解密；密钥；数字证书和签名；以及 SSL 加密、加密算法和 SSL 握手的主要步骤。
- 第 7 章 “管理服务器群集”介绍了群集服务器的概念，并说明如何使用群集服务器在服务器之间共享配置。

第三部分：配置和监视

本部分包括如何使用 Server Manager 配置和监视 Sun ONE Web Server 的示例。其中包括以下各章：

- 第 9 章 “配置服务器首选项”介绍了如何为 Sun ONE Web Server 配置服务器首选项。
- 第 8 章 “控制对服务器的访问”介绍了如何指定能够访问服务器部件的用户。
- 第 10 章 “使用日志文件”介绍了如何使用超文本传输协议 (HTTP) 监视 Sun ONE Web Server（通过记录和查看日志文件或使用操作系统提供的性能监视工具）。
- 第 11 章 “监视服务器”介绍了如何使用 SNMP （简单网络管理协议）监视 Sun ONE Web Server。
- 第 12 章 “配置命名和资源”介绍了如何配置 Java 命名和描述接口 (JNDI) 资源以及如何在服务器中包括数据库连接。

第四部分：管理虚拟服务器和服务

本部分提供了在 Server Manager 上使用程序和配置式样的相关信息。其中包括以下各章：

- 第 13 章 “使用虚拟服务器”介绍了如何使用 Sun ONE Web Server 设置和管理虚拟服务器。
- 第 14 章 “创建和配置虚拟服务器”介绍了如何创建和配置单个虚拟服务器。
- 第 16 章 “使用程序扩展服务器”介绍了如何在服务器上安装 Java 小程序、CGI 程序、 JavaScript 应用程序及其他插件。
- 第 15 章 “内容管理”介绍了如何配置和管理服务器的内容。
- 第 17 章 “应用配置式样”介绍了如何在 Sun ONE Web Server 中使用配置式样。

- 第 18 章 “使用搜索”介绍了如何在服务器上搜索文档的内容和属性。此外，本章还介绍了如何创建自定义的文本搜索界面，以满足特定用户团体的需要。
- 第 19 章 “使用 WebDAV 进行 Web 发布”介绍如何配置虚拟服务器，以使用 WebDAV 协议进行 Web 发布和在位协作性网页制作。

第五部分：附录

本部分包含多个附录，提供了用户可能需要查看的参考资料。本部分包括以下附录：

- 附录 A “命令行实用程序”提供了使用命令行实用程序代替用户界面屏幕的说明。
- 附录 B “超文本传输协议”简要介绍了 HTTP 的几个基本概念。
- 附录 C “ACL 文件语法”介绍了访问控制列表 (ACL) 文件及其语法。
- 附录 D “国际化和本地化支持”介绍了 Sun ONE Web Server 的国际化版本。

此外，还包括一个词汇表，定义了 Sun ONE Web Server 管理员可能不熟悉的常用术语。

使用 Sun ONE Web Server 文档

可以从以下位置获得 PDF 和 HTML 格式的 Sun ONE Web Server 手册联机文件：

http://docs.sun.com/db/prod/s1websrv#hic

下表列出了 Sun ONE Web Server 各手册中所介绍的任务和概念。

表 1 Sun ONE Web Server 文档参考

要了解有关以下内容的信息	请参见以下文档
软件和文档的最新信息	**发行说明**
Sun ONE Web Server 入门，包括介绍服务器基础知识和功能的实践操作 （建议新用户先阅读此部分内容）	**入门指南**

表 1 Sun ONE Web Server 文档参考

要了解有关以下内容的信息	请参见以下文档
执行安装和移植任务： • 安装 Sun ONE Web Server 及其各种组件、支持的平台和环境 • 从 Sun ONE Web Server 4.1 或 6.0 移植到 Sun ONE Web Server 6.1	*Installation and Migration Guide*
执行以下管理任务： • 使用管理界面和命令行界面 • 配置服务器首选项 • 使用服务器实例 • 监视和记录服务器活动 • 使用证书和公共密钥加密以确保服务器的安全 • 配置访问控制以确保服务器的安全 • 使用 Java™ 2 Platform, Enterprise Edition (J2EE™ Platform) 安全功能 • 部署应用程序 • 管理虚拟服务器 • 定义服务器工作负载和调整系统大小以满足性能需求 • 搜索服务器文档的内容和属性，以及创建文本搜索界面 • 配置服务器以进行内容压缩 • 配置服务器以使用 WebDAV 进行 Web 发布和内容制作	管理员指南
使用编程技术和 API 执行以下操作： • 扩展和修改 Sun ONE Web Server • 动态生成内容以响应客户请求 • 修改服务器的内容	*Programmer's Guide*
创建自定义的 Netscape 服务器应用程序编程接口 (NSAPI) 插件	*NSAPI Programmer's Guide*
在 Sun ONE Web Server 中实现 Servlet 和 JavaServer Pages™ (JSP™) 技术	*Programmer's Guide to Web Applications*

表 1 Sun ONE Web Server 文档参考

要了解有关以下内容的信息	请参见以下文档
编辑配置文件	*Administrator's Configuration File Reference Guide*
调整 Sun ONE Web Server 以优化性能	*Performance Tuning, Sizing, and Scaling Guide*

文档惯例

本节介绍本指南使用的各种惯例：

- **文件和目录路径**采用 UNIX® 格式 （使用正斜杠分隔目录名称）。对于 Windows 版本，目录路径相同，但使用反斜杠分隔目录。
- **URL** 的格式如下：

  `http://server.domain/path/file.html`

  其中，**server** 是运行应用程序的服务器的名称； **domain** 是您的 Internet 域名； **path** 是服务器的目录结构； **file** 是单个文件名。 URL 中的斜体项为占位符。
- **字体惯例**包括：
  - `monospace` 字体用于样例代码和代码列表、 API 和语言元素 （例如，函数名和类名）、文件名、路径名、目录名以及 HTML 标记。
  - *`Italic`* 用于代码变量。
  - *Italic* 还用于书名、强调、变量、占位符以及斜体文字。
  - **Bold** 用于段落标题或粗体文字。
- 本文档中的**安装根目录**都用 *install_dir* 表示。

缺省情况下，基于 UNIX 的平台上的 *install_dir* 的位置为：

```
/opt/SUNWwbsvr/
```

Windows 平台上的位置为：

```
C:\Sun\WebServer6.1
```

产品支持

如果您的系统出现问题，请通过以下方式与用户支持中心联系：

- 访问联机支持 Web 站点：

  `http://www.sun.com/supportraining/`

第 1 部分

服务器基础知识

第 1 章

Sun ONE Web Server 简介

本章介绍 Sun ONE Web Server 以及一些基本的服务器概念。阅读本章可以大致了解 Sun ONE Web Server 的工作原理。

本章包括以下部分：

Sun ONE Web Server

Sun ONE Web Server 6.1 是一种建立在开放标准基础上的多进程、多线程、安全的 Web 服务器。它具备高性能、可靠性、可升级性和可管理性，适用于任何规模的企业。

本节介绍 Sun ONE Web Server 的功能以及您可以执行的一些基本管理任务，其中包括以下主题：

Sun ONE Web Server 6.1 的新增功能

Sun ONE Web Server 6.1 具有以下新功能：

Java Servlet 2.3 和 JavaServer Pages (JSP) 1.2 支持

Sun ONE Web Server 6.1 具有 Java™ 2 Platform, Enterprise Edition (J2EE™) 兼容的 Java™ Servlet 2.3 和 JavaServer Pages™ (JSP™) 1.2 规范的实现。 J2EE 兼容的 Web 容器提供了设计和部署符合 Java™ 技术标准的 Web 应用程序所需的灵活性和可靠性。可以基于每台虚拟服务器来部署 Web 应用程序。

有关这些技术的信息，请访问以下资源：

Java Servlet
http://java.sun.com/products/servlet/index.jsp

Java Servlet 2.3 规范
http://java.sun.com/products/servlet/download.html

JavaServer Pages
http://java.sun.com/products/jsp/index.jsp

有关在 Sun ONE Web Server 中开发 Servlet 和 JSP 的信息，请参见 Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications*。

JDK 1.4.1_03 支持

Sun ONE Web Server 6.1 支持 Java 开发者工具包 (JDK™) 1.4.1_03。此 JDK 与 Web Server 捆绑在一起并可在安装过程中进行安装 （如果选择安装它）。您也可以在安装 Web 服务器之后安装您自己的 JDK。如果准备使用 Administration Server 以及 Java 和 Servlet 支持，则必须安装 JDK。

WebDAV 支持

Sun ONE Web Server 6.1 支持基于 Web 的分布式制作和版本发布 (WebDAV) 协议，该协议通过以下功能实现了协作式 Web 发布：

与 RFC 2518 的兼容性以及与 RFC 2518 客户机的互操作性

- Web 发布的安全性和访问控制
- 对基于文件系统的 WebDAV 集合和资源的基本发布操作

WebDAV 为内容元数据、名称空间管理和覆盖保护提供了集成的支持。这些技术与许多支持 WebDAV 的设计工具的结合为协作式环境提供了一个理想的开发平台。

NSAPI 过滤器支持

Sun ONE Web Server 6.1 扩展了 Netscape 服务器应用程序编程接口 (NSAPI)，支持 NSAPI 过滤器。

使用过滤器可以自定义 HTTP 请求和响应流的处理，使一个函数可以截取并有可能修改另一个函数提供或生成的内容。例如，某个插件可以安装 NSAPI 过滤器以截取由另一个插件的服务器应用程序函数 (SAF) 生成的 XML 页面，然后将该 XML 页面转换成适用于客户机的 HTML、XHTML 或 WAP 页面。或者，在将从客户机接收到的数据提供给另一个插件之前， NSAPI 过滤器可以对这些数据进行解压缩。

有关详细信息，请参见 Sun ONE Web Server 6.1 *NSAPI Programmer's Guide*。

HTTP 压缩支持

Sun ONE Web Server 6.1 支持内容压缩，从而可以提高向客户机提供内容的速度，并且可以提供更多内容，而不会相应地增加硬件的消耗。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。

有关详细信息，请参见 《Sun ONE Web Server 6.1 **管理员指南**》。

新搜索引擎支持

Sun ONE Web Server 6.1 支持一个基于 Java 的新搜索引擎，它提供了全文搜索索引和检索功能。该搜索功能允许用户在服务器上搜索文档并在 Web 页面上显示搜索结果。服务器管理员可以根据用户要搜索的文档来创建文档索引，并且可以自定义搜索界面以满足用户的特定需要。

有关详细信息，请参见 《Sun ONE Web Server 6.1 **管理员指南**》。

增强的安全性

Sun ONE Web Server 6.1 的新功能允许您使用中间文件验证来限制访问。与以前的 Web 服务器版本不同， Sun ONE Web Server 6.1 现在还支持 Java Security Manager。安装本产品时，默认情况下将禁用 Java Security Manager。有关 `server.xml` 的详细信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference Guide*。

JNDI 支持

Sun ONE Web Server 6.1 支持 Java Naming and Directory Interface™(JNDI)，它可以为各种不同的企业命名和目录服务提供无缝的连接。

JDBC 支持

Sun ONE Web Server 的出厂配置提供了立即可用的、无缝 Java™ 数据库连接 (JDBC™)，同时支持广泛的行业标准 JDBC 驱动程序和自定义 JDBC 驱动程序。

Sun ONE Studio 5 支持

Sun ONE Web Server 6.1 支持 Sun™ ONE Studio 5, Standard Edition。 Sun ONE Studio 技术是 Sun 的一种功能强大的、可扩展的集成开发环境 (IDE)，适用于 Java 技术开发者。Sun ONE Studio 5 基于 NetBeans™ 软件并与 Sun ONE 平台集成在一起。（Sun ONE Web Server 6.1 也支持 NetBeans 3.5 和 3.5.1。）

在 Sun ONE Web Server 6.1 支持的所有平台上都可以获得 Sun ONE Studio 支持。用于 Web 服务器的这一插件可以通过以下方式获得：

- Sun ONE Web Server 6.1 媒体包中的 Companion CD
- 使用 Sun ONE Studio 的 AutoUpdate 功能
- 从以下 Sun ONE Web Server 6.1 下载中心获得：
  http://www.sun.com/software/download/inter_ecom.html

有一点需要注意，即 Sun ONE Web Server 6.1 的 Sun ONE Studio 5 插件只能与本地 Web 服务器一起使用 （即与同一台计算机上的 IDE 和 Web 服务器一起使用）。

Sun ONE Web Server 6.1 的 Sun ONE Studio 5 插件的行为与 Sun™ ONE Application Server 7 的插件的行为相同。有关在 Sun ONE Studio 5 中使用 Web 应用程序功能的信息，请参见位于以下位置的教程：
http://developers.sun.com/tools/javatools/documentation/s1s5/cdshop.pdf

请将 Sun ONE Web Server 6.1 实例设置为缺省设置，然后执行教程中所述的操作。

另请参见位于以下位置的 NetBeans 教程：
http://usersguide.netbeans.org/tutorials/webapps/index.html

有关 Sun ONE Studio 5 的详细信息，请访问
http://www.sun.com/software/sundev/jde/

NSS 3.3.5 和 NSPR 4.1.5 支持

Sun ONE Web Server 6.1 支持 Network Security Services (NSS) 3.3.5 和 Netscape Portable Runtime (NSPR) 4.1.5。

PHP 兼容性

Sun ONE Web Server 6.1 与 PHP （一种应用广泛的多功能开放源代码 Web 脚本语言）兼容。 PHP （Hypertext Preprocessor [超文本预处理器] 的循环首字母缩略词）可在所有主要的操作系统中运行。

建议为 Sun ONE Web Server 6.1 使用 PHP 4.3.2 版。有关 Sun ONE Web Server 特定的 PHP 相关安装和配置信息，请访问 http://www.php.net/manual/en/install.netscape-enterprise.php

增强的硬件加速器加密支持

Sun ONE Web Server 6.1 可为 Sun™ Crypto Accelerator 1000 （一种加密加速器板，可增强 Web Server 上的 SSL 的性能）提供硬件加速器支持。

“Start on Boot”选项

在 UNIX 平台上， Sun ONE Web Server 6.1 引入了 “Start on Boot”选项，使您可以将 Web 服务器配置为在系统引导时自动启动。有关详细信息，请参见 Sun ONE Web Server 6.1 *Installation and Migration Guide*。

其他功能

支持多进程和进程监视器、故障转移、自动恢复和动态日志轮转。

管理 Sun ONE Web Server

您可以通过以下用户界面管理 Sun ONE Web Server：

- Sun ONE Web Server Administration Server
- Server Manager
- Class Manager
- Virtual Server Manager

在以前的版本中， Web 服务器和其他 Netscape 服务器都是由称为 Administration Server 的单个服务器进行管理的。在 4.x 版中，该 “Administration Server” 只是 Sun ONE Web Server 的一个附加实例，称为 Sun ONE Web Server Administration Server 或 Administration Server。您可以使用 Administration Server 管理所有 Sun ONE Web Server 实例。有关详细信息，请参见第 36 页上的 “Administration Server”。

注	此外，您还可以通过编辑配置文件或使用命令行实用程序手动执行管理任务。

要管理 Sun ONE Web Server 的单个实例，请使用 Server Manager。有关详细信息，请参见第 38 页上的 “Server Manager”。

要管理虚拟服务器，请使用 Class Manager。有关详细信息，请参见 “第 38 页上的 “Class Manager””。

Sun ONE Web Server 配置

您可以配置 Sun ONE Web Server 以打开或关闭各种功能、决定如何响应单个客户机请求以及编写基于服务器的操作并与操作进行交互的程序。标识这些选项的指令都存储在配置文件中。 Sun ONE Web Server 在启动时或在处理客户机请求期间读取这些配置文件并根据您的选择执行所需的服务器活动。

有关这些文件的详细信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference*。

Administration Server

Administration Server 是基于 Web 的服务器，包含用于配置所有 Sun ONE Web Server 的 Java 表单。

安装 Sun ONE Web Server 后，您可以使用浏览器导航至 “Administration Server” 并使用其中的表单配置 Sun ONE Web Server。提交表单时，Administration Server 将修改您所管理的服务器的配置。

用于导航至 “Administration Server”页面的 URL 取决于计算机的主机名和安装 Sun ONE Web Server 时为该 Administration Server 选择的端口号。例如，如果您将 Administration Server 安装在端口 1234 上，则相应的 URL 为：

```
http://myserver.sun.com:1234/
```

在访问任何表单之前， Administration Server 将提示您进行身份验证。即需要键入用户名和密码。您在计算机上安装 Sun ONE Web Server 时设置了 “superuser”用户名和口令。下图显示了典型的验证屏幕：

安装后，您可以使用分布式管理授予多个用户访问 Administration Server 中的不同表单的权限。有关分布式管理的详细信息，请参见第 96 页上的 “允许多个管理员”中的第 5 章 “设置管理首选项”。

Administration Server 的设置显示在右窗格中，按选项卡组的形式组织。

访问 Administration Server 时首先看到的页面称为 “Servers”。您可以使用此页面上的按钮来管理、添加、删除和迁移 Sun ONE Web Server。Administration Server 提供了以下用于执行管理级任务的选项卡：

- Servers
- Preferences
- Global Settings
- Users & Groups
- Security
- Cluster Mgmt （群集管理）

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。

有关使用 Administration Server 的详细信息，包括这些管理级任务的信息，请参见第 43 页上的 “管理 Sun ONE Web Server”

Server Manager

Server Manager 是基于 Web 的界面，包含用于配置 Sun ONE Web Server 的单个实例的 Java 表单。

您可以通过执行以下步骤访问 Sun ONE Web Server 的 Server Manager：

1. 安装并启动 Sun ONE Web Server。

   Administration Server 将显示 “Servers”。

2. 在 “Manage Servers”区域中，选择所需的服务器并单击 “Manage”。

   Sun ONE Web Server 将显示 “Server Manager Preferences”。

注 请注意，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。

您可以使用 “Preferences”上的链接来管理选项 （例如线程池设置）以及打开和关闭 Web 服务器。

此外， Server Manager 还提供了以下选项卡，用于执行其他 Sun ONE Web Server 管理任务：

- Security
- Logs
- Monitor
- Virtual Server Class
- Java

有关详细信息，请参见联机帮助中的 “Server Manager”。

Class Manager

Class Manager 是基于 Web 的界面，包含用于配置虚拟 Sun ONE Web Server 的 Java 表单。用于虚拟服务器的用户界面包含两部分，即 Server Manager 和 Class Manager。 Class Manager 包含影响单个类或单个虚拟服务器的设置。您可以为 Class Manager 中的类设置服务、添加虚拟服务器 （类的成员）以及配置单个虚拟服务器的设置。

您可以通过执行以下步骤访问 Sun ONE Web Server 的 Class Manager：

1. 在 Server Manager 中，单击 “Virtual Server Class”选项卡。

   Server Manager 将显示 “Manage a Class of Virtual Server”。

2. 从下拉列表中选择一个虚拟服务器类并单击 “Manage”。

   Sun ONE Web Server 将显示 Class Manager 的 “Select a Virtual Server”页面。

   您也可以通过单击屏幕右上角的 “Class Manager”链接来访问 Class Manager。

Class Manager 提供了以下选项卡，用于管理 Sun ONE Web Server 虚拟服务器：

- Virtual Servers
- Programs
- Content Management
- Styles

有关详细信息，请参见联机帮助中的 “Class Manager”。

Virtual Server Manager

要访问 Virtual Server Manager，请转至 Class Manager 中的 “Virtual Servers”选项卡，然后从 “Manager Virtual Servers”上的列表中选择虚拟服务器并单击 “Manage”，或单击树视图中指向某个虚拟服务器的链接。

使用 Virtual Server Manager 中的页面可以检查状态和设置、将 Java Web 应用程序的状态设置为打开以及为选定的虚拟服务器生成报告。

Virtual Server Manager 提供了以下选项卡，用于管理 Sun ONE Web Server 虚拟服务器：

- Preferences
- Logs
- Web Applications
- WebDAV
- Search

使用 Resource Picker

大多数 Server Manager 和 Class Manager 页面都是用于配置整个 Sun ONE Web Server 或整个类。然而，某些页面既可以配置整个服务器 （或类），也可以配置服务器 （或类）维护的文件和目录。这些页面的顶部都显示有 Resource Picker。

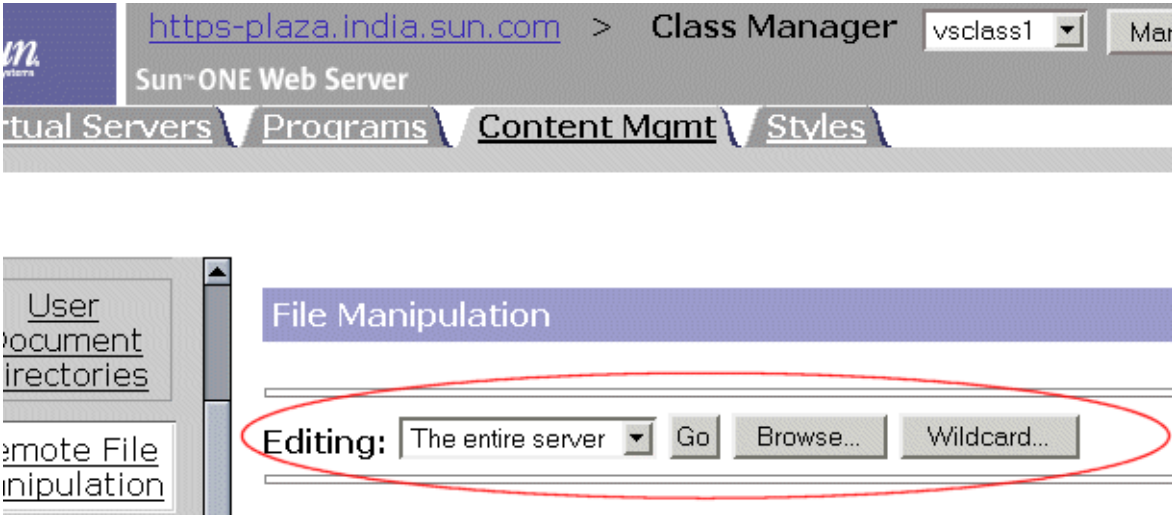


图 1-1 Resource Picker

许多页面上都显示有 Resource Picker，包括 Server Manager 的 “Log Preferences”页面以及可从 Class Manager 的 “Content Management”选项卡访问的大多数屏幕。

要使用 Resource Picker，请从下拉列表中选择要配置的资源。单击 “Browse”可以直接浏览主文档；单击 “Wildcard”可以配置具有特定扩展名的文件。

Resource Picker 中使用的通配符

在服务器配置的许多部分中，您可以指定通配符模式以表示一个或多个要配置的项。请注意，用于访问控制的通配符可能与本节中介绍的这些通配符不同。

通配符模式使用特殊字符。如果要使用其中某个字符本身而不是其特殊意义，请在其前面加上反斜杠 (\)。

通配符模式可以应用于目录路径，而不仅仅应用于文件名。因此，通配符模式可以仅应用于特定目录中的文件。例如，要向目录 /tmp 中添加文件，可以指定通配符模式 tmp/*.html。要添加所有子目录中的 index.html，通配符模式可以是 */index.html。

表 1-1 Resource Picker 通配符模式

模式	用途
*	匹配零个或多个字符。
?	精确匹配一个字符。
|	“or”表达式。与此运算符一起使用的子串可以包含其他特殊字符，例如 * 或 $。子串必须放在括号内，例如 (a|b|c)，但是不能嵌套括号。
$	匹配字符串的结尾。这在 “or”表达式中很有用。
[abc]	匹配 a、b 或 c 中的一个字符。在这些表达式中，唯一需要作为特殊字符处理的字符是]，其他都不是特殊字符。
[a-z]	匹配 a 到 z 之间的某个字符。
[^az]	匹配除 a 和 z 以外的任何字符。
*~	此表达式 （后跟另一个表达式）将删除与第二个表达式匹配的任何模式。

表 1-2 Resource Picker 通配符实例

模式	用途
*.sun.com	匹配以字符 .sun.com 结尾的任何字符串。
(products|docs).sun.com	匹配 products.sun.com 或 docs.sun.com。
198.93.9[23].???	匹配以 198.93.92 或 198.93.93 开始且以任意 3 个字符结尾的数字字符串。
.	匹配包含句点的任何字符串。
~sun-	匹配不以 sun- 开头的任何字符串。
*.sun.com~docs.sun.com	匹配域 sun.com 中除 docs.sun.com 以外的任何主机。
*.sun.com~(products|docs|software).sun.com	匹配域 sun.com 中除主机 products.sun.com、docs.sun.com 和 software.sun.com 以外的任何主机。
.com~.sun.com	匹配域 com 中除子域 sun.com 中的主机以外的任何主机。

第 2 章

管理 Sun ONE Web Server

本章介绍如何使用 Sun ONE Web Server Administration Server 管理 Sun ONE Web Server 6.1。使用 Administration Server，您可以管理服务器、添加和删除服务器以及从以前的版本迁移服务器。

本章包括以下部分：

启动 Administration Server

本节介绍如何访问 UNIX/Linux 和 Windows 平台上的 Administration Server。

UNIX/Linux 平台

要访问 UNIX 或 Linux 平台上的 Administration Server，请执行以下步骤：

1. 转至 *server_root*/https-admserv/ 目录 （例如，/usr/s1ws61/servers/https-admserv/）。
2. 键入 ./start。

   此命令将使用您在安装过程中指定的端口号启动 Administration Server。

Windows 平台

Sun ONE Web Server 安装程序可以创建一个包含若干 Windows 平台图标的程序组。该程序组包含以下图标：

- 发行说明
- 启动 Web Server Administration Server
- 卸载 Web Server
- 管理 Web Server

请注意， Administration Server 是作为一个服务小应用程序运行的，因此您也可以使用 “控制面板”直接启动它。

要访问 Windows 平台上的 Administration Server，请执行以下步骤：

1. 双击 “Start Web Server Administration Server”图标，或在您的浏览器中键入以下 URL 以启动 Administration Server：

   `http://`*`hostname.domain-name:administration_port`*

   Sun ONE Web Server 随后会显示一个窗口，提示您输入用户名和密码。

2. 键入您在安装过程中指定的管理用户名和密码。

   Sun ONE Web Server 将显示 “Administration Server”。

有关详细信息，请参见联机帮助中的 “Administration Server”。

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。

您还可以从远程位置访问 Administration Server，只要您能够访问客户机软件 （例如 Netscape Navigator）。由于 Administrator Server 是通过浏览器访问的，因此您可以从任何一台可以通过网络访问服务器的计算机进行访问。

运行多台服务器

您可以通过两种方式在系统上运行多台服务器：

- 使用虚拟服务器
- 安装多个服务器实例

虚拟服务器

使用虚拟服务器，您只需安装一台服务器便可以为多个公司或个人提供域名、 IP 地址以及某些服务器管理功能。对于用户来说，他们就像拥有了自己的 Web 服务器，只不过是由您提供硬件并进行基本的 Web 服务器维护。

虚拟服务器的设置存储在 *server_root/server_id*/`config` 目录下的 `server.xml` 文件中。使用虚拟服务器无需编辑此文件。有关此文件的详细信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference*。

有关虚拟服务器的详细信息，请参见第 13 章 “使用虚拟服务器”。

安装多个服务器实例

在以前的 Sun ONE Web Server 版本中，虚拟服务器不具有唯一的配置信息。使服务器具有单独配置信息的唯一方法是创建新的服务器实例。但是，在 Sun ONE Web Server 6.1 中，虚拟服务器具有单独的配置信息，因此不再需要使用多个服务器实例。虽然仍然支持多个实例，但是要安装多台服务器，最好还是使用虚拟服务器。

如果选择安装多个 Web 服务器实例，可以使用 Administration Server 进行以下操作：

- 在 Windows 上安装服务器的多个副本作为单独的实例，每个实例具有不同的 IP 地址。
- 配置一组使用相同 IP 地址但不同端口号的服务器。

如果您的系统被配置为侦听多个 IP 地址，请输入系统为安装的每台服务器保留的 IP 地址之一。

如果您在将系统配置为支持多个 IP 地址之前安装了服务器，请将系统配置为响应不同的 IP 地址。然后，您可以安装硬件虚拟服务器，也可以使用 Server Manager 更改服务器的绑定地址并分别为每个 IP 地址安装服务器实例。

要添加服务器实例，请执行以下步骤：

1. 访问 Administration Server 并选择 “Servers”选项卡。
2. 单击 “Add Server”链接。
3. 在指定字段中输入所需信息。

   请注意，服务器标识符不能以数字开头，并且只能在实例名称中使用 Latin-1 字符。
4. 单击 “OK”。

有关详细信息，请参见联机帮助中的 “Add Server”。

删除服务器

您可以使用 Administration Server 从系统中删除服务器。在删除之前，请确保不再需要该服务器，因为此操作将无法撤消。

注 某些 Windows 服务器具有卸载程序，可用于删除服务器及其关联的 Administration Server。有关详细信息，请参见相应的产品文档。

要从计算机中删除服务器，请执行以下步骤：

1. 访问 Administration Server 并选择 “Servers”选项卡。
2. 单击 “Remove Server”。
3. 选择要删除的服务器并单击 “Yes”。
4. 单击 “OK”。

Administration Server 随后将删除该服务器的配置文件、Server Manager 表单和以下目录 （及其所有子目录）：

server_root/https-*server-id*

有关详细信息，请参见联机帮助中的 “Remove Server”。

从以前的版本迁移服务器

您可以将 Sun ONE Web Server 从 4.1 版或 6.0 版迁移到 6.1 版。迁移时将保留 4.1 版或 6.0 版服务器，同时创建使用相同设置的新的 6.1 版服务器。

在迁移设置之前，应当停止运行 4.1 版或 6.0 版服务器，同时要确保计算机上安装了兼容的 Web 浏览器版本。

有关将服务器从以前的版本迁移到 Sun ONE Web Server 6.1 的完整说明，请参见 *Installation and Migration Guide*。

有关详细信息，请参见联机帮助中的 “Migrate Server”。

第 2 部分

使用 Administration Server

第 3 章

管理用户和组

本章介绍如何添加、删除和编辑可以访问 Sun ONE Web Server 的用户和组。

本章包括以下部分：

访问用户和组的信息

使用 Administration Server 可以访问您的应用程序数据，例如用户帐号、组列表、访问权限、组织单位以及用户和组的其他特定信息。

用户和组信息存储在文本格式的文本文件或支持轻量目录访问协议 (LDAP) 的目录服务器 （如 Sun ONE Directory Server）中。 LDAP 是一种开放的目录访问协议，它通过 TCP/IP 运行，可以缩放到全局大小，甚至上百万个条目。

由于 Sun ONE Web Server 不支持本地 LDAP，因而必须先安装一个目录服务器，然后才能够添加用户和组。

关于目录服务

目录服务器 （如 Sun ONE Directory Server）使您可以从一个源管理所有的用户信息。您还可以配置目录服务器，允许您的用户从多个易于访问的网络位置检索目录信息。

在 Sun ONE Web Server 6.1 中，可以配置三种不同类型的目录服务来验证并授权用户和组。如果没有配置其他目录服务，新创建的目录服务的值将被设置为 `default`，而不管其类型为何。

创建目录服务时，将使用该目录服务的详细资料更新 *server-root*`/userdb/dbswitch.conf` 文件。

目录服务的类型

Sun ONE Web Server 6.1 支持的各种目录服务类型包括：

- **LDAP**。在基于 LDAP 的目录服务器上存储用户和组信息。

  如果 LDAP 服务是缺省服务，将按照下面的示例更新 `dbswitch.conf` 文件：

  ```
  directory default
  ldap://draco.india.sun.com:589/dc%3Dindia%2Cdc%3Dsun%2Cdc%3Dcom

  default:binddn cn=Directory Manager

  default:encoded bindpw YWRtaW5hZG1pbg==
  ```

  如果 LDAP 服务不是缺省服务，将按照下面的示例更新 `dbswitch.conf` 文件：

  ```
  directory ldap
  ldap://draco.india.sun.com:589/dc%3Dindia%2Cdc%3Dsun%2Cdc%3Dcom

  ldap:binddn cn=Directory Manager

  ldap:encoded bindpw YWRtaW5hZG1pbg==
  ```

- **密钥文件**。密钥文件是一个文本文件，其中包含散列格式的用户口令以及该用户所属的组的列表。存储在密钥文件中的用户和组仅供 `file` 区域用来进行验证和授权，与系统用户和组无关。有关 `file` 区域的详细信息，请参见 “File 区域”。。

  创建基于密钥文件的数据库时，将按照下面的示例更新 `dbswitch.conf` 文件：

  ```
  directory keyfile file

  keyfile:syntax keyfile

  keyfile:keyfile D:\draco\keyfile\keyfiledb
  ```

- **摘要文件**。基于加密的用户名和密码存储用户和组信息。

  创建基于密钥文件的数据库时，将按照下面的示例更新 `dbswitch.conf` 文件：

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

注 如果要设置分布式管理，缺省的目录服务必须是基于 LDAP 的目录服务。

配置目录服务

要配置目录服务首选项，请执行以下步骤：

1. 访问 Administration Server 并选择 “Global Settings”选项卡。
2. 单击 “Configure Directory Service”链接。
3. 从 “Create New Service of Type”下拉列表中选择您要创建的目录服务类型。
4. 单击 “New”。

   现在，您可以在与选定的目录服务类型相对应的页面中配置目录服务信息。

注 如果没有配置其他目录服务，新创建的目录服务的值将被设置为 `default`，而不管其类型为何。

5. 单击 “Save Changes”保存所做的更改。

创建并配置目录服务后，您可以基于每个虚拟服务器来指定目录服务。以后，服务器将使用与目录服务相关联的权限来评估并强制执行访问控制规则。有关详细信息，请参见 “选择虚拟服务器的目录服务”。

理解独特的名称 （Distinguished Name， DN）

使用 Administration Server 的 “Users & Groups”选项卡来创建或修改用户、组和组织单位。用户是您 LDAP 数据库中的个人，例如您公司的雇员。组是共享某个常用属性的两个或多个用户。组织单位是您公司内的部门，它使用 `organizationalUnit` 对象类。用户、组和组织单位将在本章后面进行详述。

您公司中的每个用户和组都由一个识别名 (DN) 属性来表示。DN 属性是一个文本字符串，它包含关联的用户、组或对象的标识信息。每当您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、设置访问控制以及设置用户帐户时，均需要指定 DN 信息。 Sun ONE Web Server 管理控制台的用户和组界面可帮助您创建或修改 DN。

以下示例显示了 Sun Microsystems 公司某个雇员的典型 DN：

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

该示例中每个等号前面的缩写的含义如下：

- `uid`：用户 ID
- `e`：Email 地址
- `cn`：用户的通用名称
- `o`：组织
- `c`：国家 / 地区

DN 可能包括多种名称 / 值对。它们用于在支持 LDAP 的目录中标识证书主题和条目。

使用 LDIF

如果您目前还没有目录，或者您要向现有目录中添加一个子树，则可以使用目录服务器的 Administration Server LDIF 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。您还可以使用目录服务器的 LDIF 导出功能将您的当前目录导出到 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，请先在某个 `LDIF` 文件中定义条目，然后从目录服务器中导入该 `LDIF` 文件。

创建用户

使用 Administration Server 中的 “Users & Groups” 选项卡来创建或修改用户条目。用户条目包含有关数据库中的单个用户或对象的信息。

创建用户时，必须确保用户对资源不具有未经授权的访问权限，以保护服务器的安全。 Sun ONE Web server 6.1 提供了多种选择来增强安全性：

- 有关如何使用基于 J2EE/Servlet 的区域验证来验证和授权用户的信息，请参见第 83 页上的 “基于区域的安全性”。
- 有关如何使用基于访问控制列表 (ACL) 的验证和授权技术的信息，请参见第 165 页上的 “访问控制的工作原理”。
- 有关使用本地区域 (Native Realm) 功能 （用于在基于 Java 的安全模式和基于 ACL 的安全模式之间建立连接）的信息，请参见第 88 页上的 “配置 Native 区域”。

本部分包括以下主题：

- 在基于 LDAP 的验证数据库中创建新用户
- 在基于文件的验证数据库中创建新用户
- 在基于摘要的验证数据库中创建新用户

在基于 LDAP 的验证数据库中创建新用户

向基于 LDAP 的目录服务添加用户条目时，将使用一个基于 LDAP 的目录服务器的服务来验证和授权用户。本节提供了某些使用基于 LDAP 的验证数据库时需要考虑的指导原则，并说明如何通过 Administration Server 来添加用户。

- 创建基于 LDAP 的用户条目的指导原则
- 如何创建新用户条目
- 目录服务器用户条目

创建基于 LDAP 的用户条目的指导原则

使用管理员表单在基于 LDAP 的目录服务中创建新用户条目时，请考虑以下指导原则：

- 如果输入名和姓，表单将自动为您填写用户的全名和用户 ID。用户 ID 由用户名字的第一个字母后跟姓组成。例如，如果用户的姓名为 Billie Holiday，则用户 ID 将自动设置为 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 通过从搜索基础 （基本 DN）开始向下搜索整个目录来查看该用户 ID 是否已被使用，以确保用户 ID 的唯一性。但是，请注意，如果使用目录服务器的 ldapmodify 命令行实用程序 （如果可用）创建用户，将不能确保用户 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。
- 请注意，基本 DN 指定的识别名是缺省情况下由其开始查找目录的位置，也是您的目录树中放置所有 Sun ONE Web Administration Server 条目的位置。“DN”是表示目录服务器中的条目名称的字符串。
- 请注意，创建新用户条目时，必须至少指定以下用户信息：
  - 名或姓
  - 全名
  - 用户 ID
- 如果您的目录定义了任何组织单位，则可以使用 “Add New User To list”指定要放置新用户的位置。缺省位置是您的目录的基本 DN （或根节点）。

注 Administration Server 和 Sun ONE Web Server 管理控制台之间的用户编辑国际信息文本字段有所不同。在 Sun ONE Web Server 管理控制台中，除了无标记的 cn 字段外，还有一个首选语言 cn 字段，而 Administration Server 中没有该字段。

如何创建新用户条目

要创建用户条目，请阅读第 56 页上的 “创建基于 LDAP 的用户条目的指导原则”中的指导原则，然后执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “New User”链接。
3. 从 “Select Directory Service”下拉列表中选择 “LDAP Directory Service”并单击 “Select”。

4. 在随后显示的页面中添加所需的信息。

   有关详细信息，请参见目录服务器用户条目。

5. 单击 “OK”。

有关详细信息，请参见联机帮助中的 “New User”页面。

目录服务器用户条目

目录管理员可能需要注意以下有关用户条目的提示：

- 用户条目使用 `inetOrgPerson`、`organizationalPerson` 和 `person` 对象类。
- 缺省情况下，用户的识别名具有如下格式：

  ```
  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，并且目录的基本 DN 是 o=Ace Industry, c=US，则该用户的 DN 为：

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

  但是，请注意，您可以将此格式更改为一个基于 uid 的独特名称。

- 用户表单字段中的值被存储为以下 LDAP 属性 （请注意，除 “user”和 “group”以外，存储的任何信息均需要完全的目录服务器许可证）：

表 3-1 LDAP 属性

用户字段	对应的 LDAP 属性
Given Name	`givenName`
Surname	`sn`
Full Name	`cn`
User ID	`uid`
Password	`userPassword`
Email Address	`mail`

编辑用户条目时，还可以使用以下字段：

表 3-2 用户条目 LDAP 属性

用户字段	对应的 LDAP 属性
Title	`title`
Telephone	`telephoneNumber`

- 有时，用某种语言的字符表示用户姓名可能比使用缺省语言更精确。您可以为用户选择一种首选语言，以便用该语言的字符显示用户姓名，即使缺省语言是英语。有关设置用户首选语言的详细信息，请参见联机帮助中的 “Manage Users”页面。

在基于文件的验证数据库中创建新用户

Sun ONE Web Server 6.1 引入了对本地验证数据库的支持，该数据库将用户信息以文本格式存储在中间文件中。基于文件的验证数据库与以下文件类型兼容：

- 密钥文件式样文件
- 摘要式样文件
- .htaccess 式样文件

创建新用户条目

要在基于文件的验证数据库中创建用户条目，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “New User”链接。
3. 从 “Select Directory Service”下拉列表中选择基于文件的目录服务 ID 并单击 “Select”。
4. 输入以下信息：
   - **User ID。**（必需）指定用户的唯一用户名。
   - **Password。**指定用户的密码。
   - **Password (again)。**确认在 “Password”字段中输入的密码。
   - **Groups。**指定该用户所属的组的列表，组之间用逗号分隔。

5. 单击 “Create User”。

在基于摘要的验证数据库中创建新用户

要在基于摘要的验证数据库 （以加密形式存储用户和组信息）中创建用户条目，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “New User”链接。
3. 从 “Select Directory Service”下拉列表中选择基于摘要的目录服务 ID 并单击 “Select”。
4. 输入以下信息：
   - **User ID。**（必需）指定用户的唯一用户名。
   - **Realm。**指定将验证此用户的区域。
   - **Password。**指定用户的密码。
   - **Password (again)。**确认在 “Password”字段中输入的密码。
   - **Groups。**指定该用户所属的组的列表，组之间用逗号分隔。
5. 单击 “OK”。

管理用户

您可以通过 Administration Server 的 “Manage Users”表单编辑用户属性。在该表单中，您可以查找、更改、重命名或删除用户条目，管理用户许可证，或许还可以更改产品的特定信息。

有些 （但不是全部） Sun ONE 服务器在此区域中添加了其他表单，使您可以管理产品的特定信息。例如，如果您的 Administration Server 下安装了一个消息服务器，则会添加一个附加表单，使您可以编辑消息服务器的特定信息。有关这些附加管理功能的详细信息，请参见服务器文档。

本部分包括以下主题：

- 管理用户许可证
- 重新命名用户
- 删除用户

查找用户信息

在编辑用户条目之前，您必须先显示关联的信息。要查找特定用户信息，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “Manage Users”链接。
3. 在 “Find User”字段中，为您要编辑的条目输入一些描述性的值。您可以在搜索字段中输入以下任何值：
   - 名称。输入全名或部分名称。将返回与搜索字符串完全匹配的所有条目。如果未找到这样的条目，将返回包含该搜索字符串的所有条目。如果仍未找到这样的条目，将返回与该搜索字符串类似的所有条目。
   - 用户 ID。
   - 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。
   - Email 地址。包含 @ 符号的任何搜索字符串均被认为是 Email 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 Email 地址。
   - 使用星号 (*) 可以查看当前目录中的所有条目。保留该字段为空白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 users whose”字段中的下拉菜单来缩小搜索结果的范围。
4. 在 “Look Within”字段中，选择您要在其中搜索条目的组织单位。

   缺省为目录的根节点 （最顶层条目）。
5. 在 “Format”字段中，选择 “On-Screen”或 “Printer”。
6. 单击 “Find”。

   将显示选定组织单位中的所有用户。

7. 在显示的结果表中，单击您要编辑的条目名称。

   将显示用户编辑表单。

8. 根据需要更改显示的字段，然后单击 “Save Changes”。

   将立即进行更改。

生成自定义搜索查询

“Find all users whose”字段允许您生成自定义搜索过滤器。使用此字段可以缩小使用 “Find User”搜索的搜索结果。

“Find all users whose”字段提供了以下搜索条件：

- 最左侧的下拉列表允许您指定搜索所基于的属性。

下表说明了可用的搜索属性选项：

表 3-3 搜索属性选项

选项名	说明
full name	搜索每个条目的全名以查找匹配条目。
last name	搜索每个条目的姓以查找匹配条目。
user id	搜索每个条目的用户 ID 以查找匹配条目。
phone number	搜索每个条目的电话号码以查找匹配条目。
email address	搜索每个条目的 Email 地址以查找匹配条目。
unit name	搜索每个条目的单位名称以查找匹配条目。
description	搜索每个组织单位条目的说明以查找匹配条目。

- 在中间的下拉列表中，选择您要执行的搜索类型。

下表说明了可用的搜索类型选项：

表 3-4 搜索类型选项

选项名	说明
`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，如果您知道某个用户的姓名可能包含单词 Dylan，则可以通过此选项使用搜索字符串 Dylan 来查找该用户的条目。

表 3-4 搜索类型选项

选项名	说明
`is`	找到精确匹配的条目。也就是说，此选项将指定一个等价搜索。如果您知道某用户属性的确切值，请使用此选项。例如，如果您知道用户姓名的准确拼写，则可以使用此选项。
`isn't`	返回属性值与搜索字符串不精确匹配的所有条目。也就是说，如果您要查找目录中姓名不是 John Smith 的所有用户，请使用此选项。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，请使用此选项。例如，如果您不能确定用户姓名的拼写是 Sarret、 Sarette 还是 Sarett，请使用此选项。
`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，如果您知道用户姓名以 Miles 开头，但是不知道姓名的其余部分，请使用此选项。
`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，如果您知道用户姓名以 Dimaggio 结尾，但是不知道姓名的其余部分，请使用此选项。

- 在最右侧的文本字段中，输入您的搜索字符串。

要显示 “Look Within”目录中包含的所有用户条目，请输入星号 (*) 或保留该文本字段为空。

编辑用户信息

要更改用户的条目，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 如第 60 页上的 “查找用户信息”中所述显示用户条目。
3. 编辑与您要更改的属性对应的字段。

有关详细信息，请参见联机帮助中的 “Edit Users”页面。

注 有时，您可能要更改用户编辑表单中未显示的属性值。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）。

此外还要注意，虽然您可以在此表单中更改用户的名、姓及全名，但是要完全重命名该条目（包括条目的识别名），则需要使用“Rename User”表单。有关如何重命名条目的详细信息，请参见第 64 页上的“重新命名用户”。

管理用户口令

您为用户条目设置的密码将被各种服务器用来进行用户验证。

要更改或创建用户口令，请执行以下步骤：

1. 访问 Administration Server 并选择“Users & Groups”选项卡。
2. 如第 60 页上的“查找用户信息”中所述显示用户条目。
3. 进行所需的更改并单击“OK”。

有关详细信息，请参见联机帮助中的“Manage Users”页面。

注 您可以将根位置处的 Administration Server 用户更改为操作系统上的另一个用户，以使多个用户（属于同一组）能够编辑 / 管理配置文件。但是，请注意，在 UNIX/Linux 平台上，安装程序可以授予某个组对配置文件的“rw（读写）”权限，而在 Windows 平台上，用户必须属于“Administrators”组。

您还可以通过单击“Disable Password”按钮来禁用用户的口令。这样可以禁止该用户登录服务器而不必删除其目录条目。您可以使用“Password Management”表单输入新密码，从而再次授予该用户访问权限。

管理用户许可证

使用 Administration Server 可以跟踪您的用户被许可使用的 Sun ONE 服务器产品。

要管理可供用户使用的许可证，请执行以下步骤：

1. 访问 Administration Server 并选择“Users & Groups”选项卡。
2. 如第 60 页上的“查找用户信息”中所述显示用户条目。
3. 单击“User Edit”表单顶部的“Licenses”链接。
4. 进行所需的更改并单击“OK”。

有关详细信息，请参见联机帮助中的 “Manage Users”页面。

重新命名用户

重新命名功能只更改用户的姓名而不影响任何其他字段。此外，用户的旧名称仍被保留，因此按旧名称进行搜索仍会找到新条目。

当您重命名某个用户条目时，只能更改该用户的姓名；您不能使用重命名功能将条目从一个组织单位移动到另一个组织单位。例如，假设有两个组织单位，分别为 Marketing 和 Accounting，并且 Marketing 组织单位下有一个名为 Billie Holiday 的条目。您可以将该条目从 Billie Holiday 重命名为 Doc Holiday，但是不能通过重命名条目使 Marketing 组织单位下的 Billie Holiday 变成 Accounting 组织单位下的 Billie Holiday。

要重命名用户条目，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 如第 60 页上的 “查找用户信息”中所述显示用户条目。

   请注意，如果您使用的是基于公共名称的 DN，请指定用户的全名。如果您使用的是基于 uid 的 DN，请输入要用于该条目的新 uid 值。
3. 单击 “Rename User”按钮。
4. 相应更改 “Given Name”、“Surname”、“Full Name”或 “UID”字段以匹配该条目的新 DN。
5. 重命名条目时，您可以通过将 keepOldValueWhenRenaming 参数设置为 false 来指定 Administration Server 不再保留旧的全名或 uid 值。您可以在以下文件中找到此参数：

   server_root/admin-serv/config/dsgw-orgperson.conf

有关详细信息，请参见联机帮助中的 “Manage Users”页面。

删除用户

要删除用户条目，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 如第 60 页上的 “查找用户信息”中所述显示用户条目。
3. 单击 “Delete User”。

有关详细信息，请参见联机帮助中的 “Manage Users”页面。

创建组

组是 LDAP 数据库中用来描述一组对象的对象。 Sun ONE Web Server 组由共享某个通用属性的用户组成。例如，对象集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。

定义组成员的方法有两种：静态和动态。静态组可明确枚举出其成员对象。静态组是一个 CN，包含 `uniqueMembers` 和 / 或 `memberURLs` 和 / 或 `memberCertDescriptions`。对于静态组，其成员并不共享某个通用属性，但 `CN=<Groupname>` 属性除外。

动态组允许您使用一个 LDAP URL 来定义一组仅适用于组成员的规则。动态组的成员共享某个或一组在 `memberURL` 过滤器中定义的通用属性。例如，如果您需要一个包含 Sales 中的所有雇员的组，并且这些雇员已经位于 LDAP 数据库中的

“`ou=Sales,o=Airius.com`”之下，则可以使用以下 `memberurl` 定义一个动态组：

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

随后，该组将包含 “`ou=Sales,o=sun`”点下的树中具有 `uid` 属性的所有对象，即所有 Sales 成员。

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

创建新组后，您可以向其中添加用户或成员。

本部分包括以下主题：

- 静态组
- 动态组

静态组

使用 Administration Server，您可以通过在任意数量的用户的 DN 中指定相同的组属性来创建静态组。静态组不会改变，除非您向其中添加用户或从中删除用户。

创建静态组的指导原则

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

- 静态组可以包含其他静态或动态组。
- 可以选择为新组添加说明。
- 如果您的目录定义了任何组织单位，则可以使用 “Add New Group To”列表指定要放置新组的位置。缺省位置为目录的根节点 （最顶层条目）。
- 输入所需的信息后，单击 “Create Group”添加该组，将立即返回到 “New Group”表单。也可以单击 “Create and Edit Group”来添加组，然后继续为刚刚添加的组执行 “Edit Group”表单中的操作。有关编辑组的详细信息，请参见第 71 页上的 “编辑组属性”。

创建静态组

要创建静态组条目，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “New Group”链接。
3. 输入所需信息并单击 “OK”。

有关详细信息，请参见联机帮助中的 “New Group”。

动态组

动态组具有一个 `groupOfURLs` 对象类 (`objectclass`)，可以没有也可以具有多个 `memberURL` 属性，每个属性都是一个描述一组对象的 LDAP URL。

如果您希望基于任何属性自动将用户分组，或者希望将 ACL 应用到包含匹配 DN 的特定组，则 Sun ONE Web Server 允许您创建动态组。例如，您可以创建一个组，该组将自动包括任何包含属性 `department=marketing` 的 DN。如果您为 department=marketing 应用一个搜索过滤器，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。

本部分包括以下主题：

- Sun ONE Web Server 如何实现动态组
- 组可以同时为动态和静态
- 动态组对服务器性能的影响

- 创建动态组的指导原则
- 创建动态组

Sun ONE Web Server 如何实现动态组

Sun ONE Web Server 在 LDAP 服务器模式中以 `objectclass = groupOfURLs` 的方式实现动态组。`groupOfURLS` 类可以有多个 `memberURL` 属性，每个属性都包含一个 LDAP URL，用于枚举出目录中的一组对象。组的成员是这些对象集的总和。例如，下面的组只包含一个成员 URL：

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

该示例描述了一个包含 “`o=mcom.com`”下的所有对象的集合，属于 Marketing 部门。 LDAP URL 可以包含一个搜索基本 DN，一个范围和一个过滤器；但是，不包含主机名和端口。这意味着您只能引用同一个 LDAP 服务器上的对象。LDAP URL 支持所有范围。

DN 会自动包含在内，因而不需要您向组中添加每个 DN。组是动态变化的，因为每次 ACL 验证需要查找组时，Sun ONE Web Server 都将执行一个 LDAP 服务器搜索。 ACL 文件中使用的用户和组名称与 LDAP 数据库中的对象的 cn 属性相对应。

注	Sun ONE Web Server 使用 `cn （commonName）`属性作为 ACL 的组名称。

从 ACL 到 LDAP 数据库的映射同时在 `dbswitch.conf` 配置文件 （将 ACL 数据库名称与实际的 LDAP 数据库 URL 相关联）和 ACL 文件 （定义要为每个 ACL 使用的数据库）中定义。例如，如果您想让名为 “staff”的组中的成员具有基本访问权限， ACL 代码将查找对象类为 `groupOf<anything>` 且 CN 被设置为 “`staff`”的对象。该对象可通过两种方法来定义组的成员，即明确枚举出成员 DN （与静态组的 `groupOfUniqueNames` 的操作相同），或指定 LDAP URL （例如，`groupOfURLs`）。

组可以同时为动态和静态

组对象可以同时包含 `objectclass = groupOfUniqueMembers` 和 `objectclass = groupOfURLs`；因此，“`uniqueMember`”和 “`memberURL`”属性都是有效的。组成员是其静态和动态成员的总和。

动态组对服务器性能的影响

使用动态组对服务器的性能有所影响。如果您正在测试组成员资格，而该 DN 不是静态组的成员，则 Sun ONE Web Server 将检查数据库基本 DN 中的所有动态组。要完成此任务， Sun ONE Web Server 需要检查每个 memberURL 是否匹配，方法是检查每个 memberURL 的 baseDN 并与用户的 DN 相比较，然后使用用户的 DN 作为 baseDN 并使用 memberURL 作为过滤器来执行一个基本搜索。这一过程将产生大量的单个搜索操作。

创建动态组的指导原则

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

- 动态组不能包含其他组。
- 使用以下格式输入组的 LDAP URL （没有主机名和端口信息，因为这些参数将被忽略）：

  ```
  ldap:///<basedn>?<attributes>?<scope>?<(filter)>
  ```

  下表说明了必需的参数：

表 3-5 动态组：必需的参数

参数名	说明
<base_dn>	搜索基础的独特名称 (DN)，或 LDAP 目录中开始执行搜索的起点。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，请使用逗号来分隔属性 （例如 cn,mail,telephoneNumber），如果不指定属性，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>	搜索范围，其值可以是： • **base** 只检索有关 URL 中指定的独特名称 (<base_dn>) 的信息。 • **one** 检索有关 URL 中指定的独特名称 (<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 中指定的独特名称 (<base_dn>) 之下所有级别的条目信息。此范围包括基本条目。 此参数是必需的。

表 3-5 动态组：必需的参数

参数名	说明
`<(filter)>`	应用于指定搜索范围内的条目的搜索过滤器。如果您使用的是 Administration Server 表单，则必须指定此属性。请注意，必须带有括号。 此参数是必需的。

请注意，`<attributes>`、`<scope>` 和 `<(filter)>` 参数是根据它们在 URL 中的位置来标识的。因此，即使不想指定任何属性，也需要使用问号来分隔该字段。

- 可以选择为新组添加说明。
- 如果您的目录定义了任何组织单位，则可以使用 “Add New Group To”列表指定要放置新组的位置。缺省位置为目录的根节点 （最顶层条目）。
- 输入所需的信息后，单击 “Create Group”添加该组，将立即返回到 “New Group”表单。也可以单击 “Create and Edit Group”来添加组，然后继续为刚刚添加的组执行 “Edit Group”表单中的操作。有关编辑组的信息，请参见第 71 页上的 “编辑组属性”。

创建动态组

要在目录中创建动态组条目，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “New Group”链接。
3. 从 “Type of Group”下拉列表中选择 “Dynamic Group”。
4. 输入所需信息并单击 “OK”。

有关详细信息，请参见联机帮助中的 “New Group”。

管理组

使用 Administration Server，您可以通过 “Manage Group”表单来编辑组及管理组全体成员。本部分包括以下主题：

- 查找组条目
- 编辑组属性
- 添加组成员
- 向组成员列表中添加组
- 从组成员列表中删除条目
- 管理所有者
- 管理 “See Alsos”
- 删除组
- 重命名组

查找组条目

在编辑组条目之前，您必须先查找并显示条目。

要查找组条目，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “Manage Groups”链接。
3. 在 “Find Group”字段中输入您要查找的组的名称。

   您可以在搜索字段中输入以下任何值：

   - 名称。输入全名或部分名称。将返回与搜索字符串完全匹配的所有条目。如果未找到这样的条目，将返回包含该搜索字符串的所有条目。如果仍未找到这样的条目，将返回与该搜索字符串类似的所有条目。
   - 使用星号 (*) 可以查看当前驻留在您目录中的所有组。保留该字段为空白也可以实现这一目的。
   - 任意 LDAP 搜索过滤器。包含等号 (=) 的任何字符串均被认为是搜索过滤器。

   还可以使用 “Find all groups whose”中的下拉菜单来缩小搜索结果的范围。

4. 在 “Look Within”字段中，选择您要在其中搜索条目的组织单位。

   缺省为目录的根节点 （最顶层条目）。

5. 在 “Format”字段中，选择 “On-Screen”或 “Printer”。

6. 单击 “Find”。

   将显示与搜索条件相匹配的所有组。

7. 在显示的结果表中，单击您要编辑的条目名称。

“Find all groups whose”字段

“Find all groups whose”字段允许您生成自定义的搜索过滤器。使用此字段可以缩小由 “Find Group”返回的搜索结果。

要显示 “Look Within”目录中包含的所有组条目，请输入星号 (*) 或保留该字段为空。

有关如何生成自定义搜索过滤器的详细信息，请参见第 61 页上的 “生成自定义搜索查询”。

编辑组属性

要编辑组条目，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。

2. 单击 “Manage Groups”链接。

3. 找到您要编辑的组，键入所需的更改。

   有关如何查找特定条目的详细信息，请参见第 70 页上的 “查找组条目”中介绍的概念。

注	您可以将根位置处的 Administration Server 用户更改为操作系统上的另一个用户，以使多个用户 （属于同一组）能够编辑 / 管理配置文件。但是，请注意，在 UNIX/Linux 平台上，安装程序可以授予某个组对配置文件的 “rw （读写）”权限，而在 Windows 平台上，用户必须属于 “Administrators”组。

有关编辑组属性的详细信息，请参见联机帮助中的 “Manage Groups”。

注 有时，您可能要更改组编辑表单中未显示的属性值。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

要向组中添加成员，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “Manage Groups”链接。
3. 如第 70 页 “查找组条目”中所述找到您要管理的组，然后单击 “Group Members”下的 “Edit”按钮。

   Sun ONE Web Server 将显示一个新表单，从中可以搜索条目。如果您要向列表中添加用户条目，请确保 “Find”下拉列表中显示 “Users”。如果您要向组中添加组条目，请确保显示 “Group”。
4. 在最右侧的文本字段中，输入搜索字符串。请输入以下选项之一：
   - 名称。输入全名或部分名称。将返回其名称与搜索字符串完全匹配的所有条目。如果未找到这样的条目，将返回包含该搜索字符串的所有条目。如果仍未找到这样的条目，将返回与该搜索字符串类似的所有条目。
   - 用户 ID，如果您正在搜索用户条目。
   - 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。
   - Email 地址。包含 @ 符号的任何搜索字符串均被认为是 Email 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 Email 地址。
   - 输入星号 (*) 或保留该文本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 “Find and Add”查找所有匹配的条目并将其添加到组中。

   如果您不希望将搜索返回的某些条目添加到组中，请单击 “Remove from list?”列中的相应的框。您还可以构建一个搜索过滤器以匹配要删除的条目，然后单击 “Find and Remove”。

6. 完成组成员列表后，单击 “Save Changes”。

   现在，当前显示的条目即成为组的成员。

有关添加组成员的详细信息，请参见联机帮助中的 “Edit Members”页面。

向组成员列表中添加组

您可以向组成员列表中添加组 （而不是单个成员）。这样，所添加的组的成员将成为该接收组的成员。例如，如果 Neil Armstrong 是 Engineering Managers 组的成员，而您使 Engineering Managers 组成为 Engineering Personnel 组的成员，则 Neil Armstrong 也将成为 Engineering Personnel 组的成员。

要将组添加到另一个组的组成员列表中，可以像添加用户条目一样添加该组。有关详细信息，请参见第 72 页上的 “添加组成员”。

从组成员列表中删除条目

要从组成员列表中删除条目，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “Manage Groups”链接，找到您要管理的组 （如第 70 页 “查找组条目”中所述），然后单击 “Group Members”下的 “Edit”按钮。
3. 对于要从列表中删除的每个成员，单击 “Remove from list?”列中的相应的框。

   您还可以构建一个过滤器来查找要删除的条目，然后单击 “Find”和 “Remove”按钮。有关创建搜索过滤器的详细信息，请参见第 72 页上的 “添加组成员”。
4. 单击 “Save Changes”。条目将从组成员列表中删除。

管理所有者

您可以像管理组成员列表一样管理组的所有者列表。下表列出了有关详细信息所对应的小节：

表 3-6 其他信息

要完成的任务	参阅章节
向组中添加所有者	第 72 页上的 “添加组成员”。
向所有者列表中添加组	第 73 页上的 “向组成员列表中添加组”。
从所有者列表中删除条目	第 73 页上的 “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。这使用户可以很容易地找到与当前组相关的人员和组。

管理 “See Alsos”的方法与管理组成员列表相同。下表列出了有关详细信息所对应的章节：

表 3-7 其他信息

要完成的任务	参阅章节
向 “See Alsos”中添加其他用户	第 72 页上的 “添加组成员”。
向 “See Alsos”中添加组	第 73 页上的 “向组成员列表中添加组”。
从 “See Alsos”中删除条目	第 73 页上的 “从组成员列表中删除条目”。

删除组

要删除组，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “Manage Groups”链接，找到您要管理的组 （如第 70 页上的 “查找组条目”中所述），然后单击 “Delete Group”。

注 Administration Server 不会删除所删除组中的单个成员，而只是删除该组条目。

重命名组

要重命名组，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “Manage Groups”链接，找到您要管理的组 （如第 70 页上的 “查找组条目”中所述）。
3. 单击 “Rename Group”按钮，在出现的对话框中键入新的组名称。

当您重命名某个组条目时，只能更改该组的名称；不能使用 “Rename Group”功能将条目从一个组织单位移动到另一个组织单位。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。

创建组织单位

组织单位可以包含许多组，通常代表一个科室、部门或其他零散的业务组。 DN 可以存在于多个组织单位中。

要创建组织单位，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “New Organizational Unit”链接并输入所需的信息。

有关详细信息，请参见联机帮助中的 “New Organizational Unit”页面。

目录管理员可能需要注意以下提示：

- 使用 `organizationalUnit` 对象类创建新的组织单位。
- 新组织单位的 DN 具有如下格式：

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

例如，如果您在组织单位 West Coast 中创建一个名为 Accounting 的新组织单位，并且您的基本 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

您可以通过 “Organizational Unit Edit”表单编辑和管理组织单位。本部分包括以下主题：

- 查找组织单位
- 编辑组织单位属性
- 重命名组织单位
- 删除组织单位

查找组织单位

要查找组织单位，请执行以下步骤：

1. 访问 Administration Server 并选择 “Users & Groups”选项卡。
2. 单击 “Manage Organizational Units”链接。
3. 在 “Find organizational unit”字段中键入您要查找的单位的名称。您可以在搜索字段中输入以下任何值：
   - 名称。输入全名或部分名称。将返回与搜索字符串完全匹配的所有条目。如果未找到这样的条目，将返回包含该搜索字符串的所有条目。如果仍未找到这样的条目，将返回与该搜索字符串类似的所有条目。
   - 使用星号 (*) 可以查看当前驻留在您目录中的所有组。保留该字段为空白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”字段中的下拉菜单来缩小搜索结果的范围。
4. 在 “Look Within”字段中，选择您要在其中搜索条目的组织单位。

   缺省为目录的根点。

5. 在 “Format”字段中，选择 “On-Screen”或 “Printer”。
6. 单击 “Find”。

   将显示与搜索条件相匹配的所有组织单位。
7. 在显示的结果表中，单击您要查找的组织单位名称。

“Find all units whose”字段

“Find all units whose”字段允许您生成自定义的搜索过滤器。使用此字段可以缩小由 “Find organizational unit”返回的搜索结果。

要显示 “Look Within”目录中包含的所有组条目，请输入星号 (*) 或保留该字段为空。

有关如何生成自定义搜索过滤器的详细信息，请参见第 61 页上的 “生成自定义搜索查询”。

编辑组织单位属性

要更改某个组织单位条目，请访问 Administration Server 并执行以下步骤：

1. 如第 76 页上的 “查找组织单位”中所述找到您要编辑的组织单位。

   将显示组织单位编辑表单。
2. 根据需要更改显示的字段，然后单击 “Save Changes”。

   将立即进行更改。

注 有时，您可能希望更改组织单位编辑表单中未显示的属性值。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）。

重命名组织单位

要重命名组织单位条目，请访问 Administration Server 并执行以下步骤：

1. 确保在目录中您要删除的组织单位下没有任何其他条目。
2. 如第 76 页上的 “查找组织单位”中所述找到您要编辑的组织单位。
3. 单击 “Rename”按钮。
4. 在显示的对话框中输入新的组织单位名称。

注 当您重命名某个组织单位条目时，只能更改该组织单位的名称；不能使用重命名功能将条目从一个组织单位移动到另一个组织单位。有关详细信息，请参见第 77 页上的 “重命名组织单位”。

删除组织单位

要删除组织单位条目，请访问 Administration Server 并执行以下步骤：

1. 确保在目录中您要删除的组织单位下没有任何其他条目。
2. 如第 76 页上的 “查找组织单位”中所述找到您要编辑的组织单位。
3. 单击 “Delete”按钮。
4. 在显示的确认框中，单击 “OK”。

   组织单位将被立即删除。

第 4 章

用于 Web 容器和 Web 应用程序的基于 J2EE 的安全性

本章介绍了 Sun ONE Web Server 6.1 Web 容器和 Web 应用程序的基于 J2EE 安全性的基本功能。首先介绍 Web 服务器支持的两种主要验证和授权模式：基于访问控制列表 (ACL) 的安全模式和基于 J2EE/Servlet 的安全模式。本章还介绍了 Sun ONE Web Server 6.1 中的新增功能，您可以通过该功能部署 Java Web 应用程序，从而可以利用这两种安全系统的优点。

本章的其余部分将说明 J2EE/Servlet 的配置问题，相关的安全问题在以下各章中进行了介绍：

- 证书和公共密钥加密 （第 6 章 “使用证书和密钥”）。
- 基于 ACL 的安全性 （第 8 章 “控制对服务器的访问”）。

本章包括以下部分：

关于 Sun ONE Web Server 安全性

您可以通过多种安全服务和机制（包括验证、授权和访问控制）来保护驻留在 Web 服务器上的资源。

验证是确认身份的过程。授权意味着将对受限制资源的访问权限授予某个用户身份，而访问控制机制则强制这些限制。验证和授权可以通过多种安全模式和服务来强制。

Sun ONE Web Server 6.1 支持两种安全模式：由 HTTP 引擎提供的基于 ACL 的安全模式和由 Web 容器提供的基于 J2EE Servlet 2.3 版规范的安全模式。

两种模式在 Sun ONE Web Server 6.1 进程的生命周期中共存。每种模式都支持客户机验证和授权安全服务。

Sun ONE Web Server 6.1 Web 容器提供了通过基于 Java 验证和授权服务 (JAAS) 区域机制的验证，以及通过基于 J2EE 角色机制的授权。 Sun ONE Web Server 6.1 提供的一种区域是 Native 区域，它在这两种安全模式之间架起了一座桥梁。

Sun ONE Web Server 6.1 支持声明的安全性和程序化安全性。

Sun ONE Web Server 6.1 利用 J2EE 平台的各种功能来定义开发和装配应用程序组件的人员与在操作环境中配置应用程序的人员之间的声明合同。在应用程序安全性上下文中，应用程序供应商需要以某种方式声明应用程序的安全要求，以便这些要求可以在应用程序配置过程中得到满足。应用程序中使用的声明安全机制在**部署描述符**文件中以声明的语法来表示。然后，应用程序部署者将使用容器专用的工具，将部署描述符中的应用程序要求映射到由 J2EE 容器实现的安全机制中。 Sun ONE Web Server 6.1 中 Web 应用程序的部署描述符文件为 `web.xml` 和 `sun-web.xml` 文件。

程序安全性是指由具有安全意识的应用程序做出的安全决定。当单个声明的安全性不足以表示某个应用程序的安全模式时，程序化安全性将非常有用。例如，一个应用程序可能基于一天的某个时间、某个调用的参数或某个 Web 组件的内部状态进行授权决定。另一个应用程序可能基于存储在数据库中的用户信息来限制访问。

本章的其余部分将为您介绍以下由 Sun ONE Web Server 6.1 支持的验证和授权中的关键概念：

- 基于 ACL 的访问控制 （在 “基于 ACL 的访问控制概述”部分中介绍）。
- 基于 J2EE 的访问控制 （在 “基于 J2EE/Servlet 的访问控制概述”部分中介绍）。
- Native 区域支持 （在 “Native 区域”部分中介绍）。
- 程序化安全性 （在 “如何配置区域”部分中介绍）。

基于 ACL 的访问控制概述

基于 ACL 的访问控制将在第 8 章 “控制对服务器的访问”部分中详细介绍。下面只简单介绍其中的关键概念。

Sun ONE Web Server 6.1 通过使用本地存储的访问控制列表 (ACL) 来支持验证和授权，该列表用于说明用户对资源所具有的访问权限。例如， ACL 中的一项内容可以为名为 John 的用户授予对特定文件夹 `misc` 的读权限。

```
acl "path=/export/user/990628.1/docs/misc/";
  authenticate (user,group) {
     database = "default";
     method = "basic";
  };
  deny (all) (user="anyone");
  allow (read) (user = "John");
```

Sun ONE Web Server 6.1 中的核心 ACL 支持以下三种类型的验证：基本验证、SSL 验证和摘要验证。

基本验证基于以明文形式传输的用户名和密码列表。 SSL 方法要求浏览器具有用户证书，证书中包含该用户的公共密钥和其他用户信息 （例如名称、 Email 等）。摘要验证使用加密技术对用户证书进行加密。

下面介绍基于 ACL 的访问控制模式的主要功能：

- 基于 ACL 的验证和授权使用以下配置文件：
  - *server-install*`/httpacl/*.acl` 文件
  - *server-install*`/userdb/dbswitch.conf`
  - *server-install*`/`*server-instance*`/config/server.xml`
- 验证数据库由 `dbswitch.conf` 文件中配置的 `auth-db` 模块提供。
- 如果配置了 ACL，验证和授权将通过 *server-install*`/httpacl/*.acl` 文件中设置的访问控制规则来执行。应用的授权规则是在与处理请求的虚拟服务器相对应的 ACL 文件中定义的规则 （在 `server.xml` 中相应的 `VS` 项中配置），请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference* 中的 `ACLFILE` 元素和 `VS` 元素的 `aclids` 特性。这些文件通常位于 `/httpacl/` 目录中，但如果您更改了 `server.xml` 配置，也可以将这些文件置于其他目录中。

此外， Sun ONE Web Server 6.1 SSL 引擎还支持外部加密硬件，以卸载 SSL 处理和提供可选的防篡改密钥存储。

有关访问控制和使用外部加密硬件的详细信息，请参见第 8 章 “控制对服务器的访问”。

基于 J2EE/Servlet 的访问控制概述

基于 J2EE/Servlet 的访问控制将在 Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications* 中详细介绍。下面只简单介绍其中的关键概念。

Sun ONE Web Server 6.1 除了提供基于 ACL 的验证以外，还利用 J2EE 1.3 规范中定义的安全模式提供几种功能，以帮助您开发和部署安全 Java Web 应用程序。

典型的基于 J2EE 的 Web 应用程序包括以下部分 （可以限制对其中任何部分或所有部分的访问）：

- Servlet
- JavaServer Pages (JSP) 组件
- HTML 文档
- 其他资源 （例如，图像文件和压缩的归档文件）

基于 J2EE/Servlet 的访问控制基础结构将基于安全区域的使用。当用户尝试通过 Web 浏览器访问应用程序中受保护的部分时，Web 容器将提示输入该用户的证书信息，然后将其传输到当前在该特定应用程序的安全服务中活动的区域中进行验证。

下面介绍基于 J2EE/Servlet 的访问控制模式的主要功能：

- 基于 J2EE/Servlet 的验证使用以下配置文件：
  - Web 应用程序部署描述符文件 `web.xml` 和 `sun-web.xml`
  - *server-install*`/`*server-instance*`/config/server.xml`
- 验证由 Java 安全性区域执行，这些区域通过 `server.xml` 文件中的 `AUTHREALM` 各项进行配置。
- 如果已经设置了此类规则，授权将由部署描述符文件 (`web.xml`) 中的访问控制规则来执行。

下面简单介绍安全性区域的概念。有关 J2EE 安全模式和基于区域的验证的详细介绍，请参见 Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications*。

基于区域的安全性

基于 J2EE 的安全性模式提供了识别和验证用户的安全性区域。用户信息可以从基础安全性区域获得。基于区域的安全性包括两个方面：

- 基于区域的用户验证。它通过基础区域验证用户。
- 基于角色的授权。它为用户指派角色，而用户又将被授予或限制对资源的访问权限。

基于区域的用户验证

验证进程通过一个基础区域（也称为安全域）来验证用户。区域包括一组用户、可选的组映射和可以用来验证验证请求的验证逻辑。通过配置的区域验证验证请求并建立安全性上下文之后，此身份将应用于所有后续的授权决定，除非被 `run-as` 条件否决。

服务器实例可能具有多种配置区域。 `server.xml` 文件的 `AUTHREALM` 元素中提供了配置信息。

在 Sun ONE Web Server 中，验证服务是通过 JAAS 建立的，JAAS 用于提供可插接式安全域。 Sun ONE Web Server 6.1 中的 Java 验证区域与 Sun ONE Application Server 7.0 中的区域一致。

Sun ONE Web Server 6.1 提供了以下区域：

- LDAP 区域
- File 区域
- Solaris 区域
- Certificate 区域
- Certificate 区域
- Native 区域

LDAP 区域

通过 `ldap` 区域可以将 LDAP 数据库用于用户安全性信息。 LDAP 目录服务是带有唯一标识符的属性的集合。 `ldap` 区域非常适合部署到生产系统中。

要使用 ldap 区域验证用户，必须在 LDAP 目录中创建所需的用户。您可以通过 Administration Server 的 “Users & Groups”选项卡或 LDAP 目录产品的用户管理控制台执行此操作。有关详细信息，请参见 “第 55 页上的 “在基于 LDAP 的验证数据库中创建新用户””。

File 区域

file 区域是首次安装 Sun ONE Web Server 时的缺省区域。该区域的设置简单方便，它将为开发者提供了很多方便。

file 区域使用存储在文本文件中的用户数据来验证用户。 file 区域支持以下验证数据库：

- 密钥文件式样数据库
- htaccess 式样数据库
- 摘要式样数据库

有关各种基于文件的验证数据库的更多信息，请参见 < 添加 >。

file 区域所使用的用户信息文件最初是空的，因此您必须在使用 file 区域之前添加用户。有关如何执行此操作的详细信息，请参见第 58 页上的 “在基于文件的验证数据库中创建新用户”。

Solaris 区域

solaris 区域允许通过 Solaris 用户名和密码数据进行验证。只有 Solaris 9 支持此区域，因为此区域使用的是 Solaris 9 操作环境中的用户数据库，它能够减少设置单独数据库的额外步骤。

Certificate 区域

certificate 区域支持 SSL 验证。 certificate 区域在 Sun ONE Web Server 的安全性上下文中设置用户身份，并将其与客户机证书的用户数据总装在一起。然后， J2EE 容器将基于证书中每个用户的 DN 处理授权进程。此区域使用 SSL 或 TLS 客户机验证并通过 X.509 证书来验证用户。

有关如何设置服务器和客户机证书的详细信息，请参见第 6 章 “使用证书和密钥”。

Certificate 区域

您可以通过可插接式 JAAS 登录模块和区域实现为其他数据库 （如 Oracle）建立区域，以满足您的特定需要。请注意，客户端 JAAS 登录模块不适用于 Sun ONE Web Server。

请参见 Sun ONE Web Server 6.1 中的样例区域作为模板。

Native 区域

Native 区域是一个特殊的区域，它为基于 ACL 的核心验证模式和 J2EE/Servlet 验证模式提供了联系桥梁。通过将 Native 区域用于 Java Web 应用程序，可以让 ACL 子系统执行验证 （而不是让 Java Web 容器执行），并且使此身份可以用于 Java Web 应用程序。

当调用验证操作时， Native 区域会将此验证委派给核心验证子系统。从用户的角度来看，这实际上相当于 LDAP 区域将验证委派给已配置的 LDAP 服务器。当 Native 区域处理组成员关系查询时，也被委派给核心验证子系统。对于 Java Web 模块和开发者而言， Native 区域与任何其他可用于 Web 模块的 Java 区域没有什么区别。

因为 Native 区域将验证委派给核心验证子系统，所以需要一些附加的配置。有关详细信息，请参见 “配置 Native 区域”。

Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications* 详细介绍了 J2EE 安全区域和可以用来配置安全区域的配置参数。

基于角色的授权

Java Servlet 2.3 规范定义了如何建立访问控制规则，用以限制对各种 J2EE 应用程序资源的访问。

将角色映射到受限制的区域

J2EE 访问控制建立在角色的基础上。要限制对特定 HTML 页面、 Servlet 和 JSP 等的访问，必须定义以下内容：

- 受限制的区域，在 Web 模块描述符 (`web.xml`) 中列出
- 有权访问每个受限制区域的角色 （在 `web.xml` 中）
- 到角色的用户和组映射，用以确定授权特定用户访问受限制的区域 （在 `sun-web.xml` 中）。

用户可以担任多个角色；在验证至少为他们分配了一个角色后，便允许他们访问相应的区域。

请使用 Sun ONE Web Server 6.1 的 `webapps/security` 目录中带有各种访问限制的样例作为模板。有关基于 Servlet 角色安全性的详细介绍，请参见 Servlet 2.3 规范。

按角色定义访问控制

J2EE 应用程序角色是抽象的角色，适用于特定的应用程序。如果要在实际环境中运行您的应用程序，并且限定只有授权的用户才能对其进行受限访问，必须在 `sun-web.xml` 描述符中将用户名映射到角色。请使用以下一种或两种方式：

主映射 — 在 `sun-web.xml` 中将一个或多个用户名直接映射到一个角色。此方法便于进行测试，但不适用于超出每个角色中用户的限制数目的情况。

组映射 — 在 `sun-web.xml` 中将一个或多个用户名间接映射到一个或多个组。例如，组名称可以是工程师、经理或职员。然后，为属于列出的组且通过验证的用户指派应用程序角色。注意，由处于活动状态的区域实现 （或引用数据库）负责确定哪些用户属于给定的组。

当委托人 （用户）请求访问特定的 Web 资源 （例如 Servlet 或 JSP）时， Web 容器将检查与部署描述符文件中的资源关联的安全限制或权限，以确定委托人是否有权访问该资源。

角色映射项将角色映射到模块描述符中的用户或组。示例：

```
<sun-web-app>
   <security-role-mapping>
   <role-name>manager</role-name>
   <principal-name>jsmith</principal-name>
   <group-name>divmanagers</group-name>
</security-role-mapping>
</sun-web-app>
```

有关部署描述符文件的详细信息，请参见 Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications*。

如何配置区域

您可以使用以下任一方式配置区域：

- 使用管理界面
- 编辑 server.xml 文件

使用管理界面

要使用管理界面配置区域，请执行以下操作：

1. 从 Administration Server 界面访问要管理的服务器实例，然后单击 “Java” 选项卡。
2. 单击 “Security Realms” 链接。

   缺省情况下提供以下区域：

   — file

   — native

   — ldap
3. 要添加区域，请单击 “New” 按钮。要删除区域，请选中区域名称旁边的复选框，然后单击 “OK”。要编辑区域，请单击该区域的名称。
4. 如果要添加或编辑区域，请输入该区域的名称、类名、特性和用户 （仅限于 `file` 区域），然后单击 “OK” 按钮。
5. 单击 “OK”。

编辑 server.xml 文件

缺省区域将在 `server.xml` 文件的 `SECURITY` 元素中进行设置，此设置是在后台进行的。 `SECURITY` 配置如下所示：

```
<SECURITY defaultrealm="file" anonymousrole="ANYONE"
      audit="false">
   <AUTHREALM name="file"
         classname="com.iplanet.ias.security.auth.realm.file.FileRe
alm">
      <property name="file" value="instance_dir/config/keyfile"/>
```

```
      <property name="jaas-context" value="fileRealm"/>
   </AUTHREALM>
   ...
</SECURITY>
```

defaultrealm 属性指向服务器缺省使用的区域。所有未在 web.xml 中提供有效区域的 Web 应用程序都将使用缺省区域。它必须指向一个已配置的 AUTHREALM 名称。缺省情况下是 file 区域。

audit 标志用于确定是否记录审核信息。如果将此标志设置为 true，服务器将记录所有验证和授权事件的审核信息。

如果更改了区域配置，则必须重新启动服务器才能使更改生效。

有关 server.xml 文件的更多信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference*。

配置 Native 区域

与配置所有区域一样，您可以使用 server.xml 的 SECURITY 元素中的 AUTHREALM 元素来配置 Native 区域。示例：

```
<AUTHREALM name="native"
classname="com.sun.enterprise.security.auth.realm.webcore.NativeRea
lm">
   <PROPERTY name="auth-db" value="mykeyfile" />
   <PROPERTY name="jaas-context" value="nativeRealm"/>
</AUTHREALM>
```

auth-db 特性指向核心验证数据库，该 Native 区域实例会将所有验证请求委派给该数据库。在本实例中，该验证数据库名为 “mykeyfile”。此特性可选。如果未指定属性，核心验证引擎将使用 default auth-db 处理来自此 Native 区域的所有请求。在多数区域中， jaas-context 特性是指向要使用的 JAAS 登录上下文的指针 （在 login.conf 中定义）。

Native 区域不需要其他配置。但是，由于将请求委派给了核心验证数据库，因此该特定验证数据库还必须是已配置的特性。下面将举例说明如何配置核心验证数据库。

要配置核心 (native) 验证数据库，server.xml 中的 VS 元素必须包含 USERDB 元素，该元素可将 auth-db 名称映射到数据库名称。例如：

```
<VS id="https-plaza.com"  ....
....
   <USERDB id="mykeyfile" database="myalt"/>
....
</VS>
```

请注意，如果未给定 auth-db 特性 （这种情况下使用 “default”），则 USERDB 项会将 id="default" 映射到某个数据库名称。如果不存在映射，则映射到 default。

其次，文件 *install-root*/userdb/dbswitch.conf 必须包含 myalt 数据库的配置。以下示例将 myalt 定义为基于文件的验证数据库。

```
directory myalt file
myalt:syntax keyfile
myalt:keyfile /local/ws61/https-plaza.com/config/keyfile
```

以上配置并非专用于 Native 区域。任何有效的验证目录配置都可以用作 Native 区域的目标验证数据库。这意味着 Native 区域可以配置为委派给本地 LDAP 验证数据库，甚至是自定义的本地验证数据库。

注 在 Sun ONE Web Server 6.1 中， Web 应用程序有两种将 LDAP 用作验证引擎的不同机制：

- 使用 Java LDAP 区域
- 使用配置为委派给本地 LDAP 验证数据库的 Java 本地区域。

指定缺省区域

缺省区域将用于处理所有在 web.xml 部署描述符文件中未指定有效替代区域的 Web 应用程序中的验证事件。要为服务器实例指定活动的验证区域，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java” 选项卡。
2. 单击 “Java Security” 链接。

3. 设置以下信息：
   - **Default Realm**。为该服务器实例指定活动的验证区域（AUTHREALM 名称属性）。
   - **Anonymous Role**（可选）。用作缺省或匿名角色的名称。
   - **Audit Enabled**（可选）。如果为 true，将执行附加的访问记录以提供审核信息。审核信息包括以下内容：
     - 验证成功或失败的事件
     - 同意或拒绝 Servlet 访问
   - **Log Level**（可选）。控制记录到错误日志的消息类别。
4. 单击“OK”。

如何配置区域

除了由区域提供的容器管理验证以外， Sun ONE Web Server 6.1 还支持通过程序化登录界面访问的管理验证。此界面支持不适用于区域基础结构的自定义验证模式。J2EE 应用程序也可以使用程序化登录直接为自己建立验证上下文。但是，这种方式不便于应用程序的移植和维护，因此建议不要使用。

调用应用程序的程序化登录机制需要 `ProgrammaticLoginPermission` 权限。缺省情况下，此权限不会授予部署的应用程序，因为这不是标准的 J2EE 机制。

Sun ONE Web Server 6.1 支持 Security Manager。首次安装服务器时，将缺省禁用 Security Manager。如果在服务器实例中启用了 Java Security Manager，则需要将此权限授予要使用程序化登录的任何 Web 应用程序。

要为应用程序授予所需的权限，您需要编辑 `server.policy` 文件。

通过在 `server.xml` 文件中指定标准的 Java 策略项，您可以启用策略支持。

```
<JVMOPTIONS>-Djava.security.manager</JVMOPTIONS>

<JVMOPTIONS>-Djava.security.policy=install-root/https-servername/config/server.policy</JVMOPTIONS>
```

有关 `server.policy` 文件的详细信息，请参见 Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications*。

决定何时使用 J2EE/Servlet 验证模式

本部分介绍应在哪些情况下使用基于 J2EE/Servlet 的验证模式。

在以下情况下，请使用 J2EE/Servlet 验证模式：

- 一般而言，对于大多数新的基于 J2EE/Servlet 的 Web 应用程序。
- 对于您不希望修改的现有 `.war` 文件。
- 对于创建现在或将来 J2EE/Servlet 的完全兼容性都很重要的 Web 应用程序。
- 如果希望使用基于表单的验证 （因为 ACL 不支持基于表单的验证）。

请记住，即使使用基于 ACL 的基础结构，您仍可以使用 Native 区域 Java 区域传输用户标识，使其可用于 Servlet。

第 5 章

设置管理首选项

您可以使用 “Preferences”和 “Global Settings”选项卡中的页面来配置 Administration Server。请注意，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。

本章包括以下部分：

关闭 Administration Server

服务器将在安装后持续运行，侦听并接受 HTTP 请求。有时您可能要停止并重新启动服务器，例如，如果刚刚安装了 Java 开发工具 (JDK) 或 Directory Server，或者更改了侦听套接字设置。

您可以使用以下方法之一停止服务器：

- 访问 Administration Server，请依次选择 “Preferences”选项卡和 “Shut Down”链接，然后单击 “Shut down the administration server！”按钮。

  有关详细信息，请参见联机帮助中的 “Shut Down”。

- 使用 “控制面板”中的 “服务”窗口 (Windows)。
- 使用 `stop` 来完全关闭服务器。这将中断服务，直至重新启动。

关闭服务器后，服务器可能需要几秒钟时间完成关闭进程并将状态更改为 “Off”。

编辑侦听套接字设置

在服务器能够处理请求之前，必须先通过侦听套接字接受请求，然后将请求发送给正确的虚拟服务器。安装 Sun ONE Web Server 时将自动创建一个侦听套接字 (ls1)。此侦听套接字使用 IP 地址 0.0.0.0 和在安装过程中指定为 HTTP 服务器端口号的端口号 （缺省为 8888）。不能删除缺省侦听套接字。

您可以使用 Administration Server 的侦听套接字表来编辑服务器的侦听套接字设置。要访问该表，请执行以下步骤：

1. 访问 Administration Server 并单击 “Preferences”选项卡。
2. 单击 “Edit Listen Sockets”链接。
3. 进行所需的更改并单击 “OK”。

有关详细信息，请参见第 13 章 “使用虚拟服务器”以及联机帮助中的 “Edit Listen Sockets”页面。

更改用户帐户 (UNIX/Linux)

在 UNIX 和 Linux 计算机上，使用 “Server Settings”页面可以更改 Web 服务器的用户帐户。服务器的所有进程都将使用此用户帐户运行。

对于以下情况，您不必指定服务器用户：如果选择的端口号大于 1024 且没有使用 `root` 用户帐户运行服务器 （在这种情况下，您不必使用 `root` 用户帐户登录来启动服务器）。如果您未在此处指定用户帐户，服务器将使用启动时的用户帐户运行。请确保启动服务器时使用的是正确的用户帐户。

注	如果您不知道如何在系统上创建新用户，请与系统管理员联系或查阅系统文档。

即使使用 root 用户帐户启动了服务器，您也不应始终使用该帐户来运行服务器。您需要限制服务器对系统资源的访问并作为非特权用户运行。您输入的作为服务器用户的用户名应当已经存在，并且是一个标准的 UNIX/Linux 用户帐户。服务器启动后将使用此用户帐户运行。

如果希望避免创建新用户帐户，可以选择用户 `nobody` 或相同主机上运行的另一个 HTTP 服务器使用的帐户。但是，在某些系统上，用户 `nobody` 可以拥有文件，但不能运行程序。

要访问 “Server Settings”页面，请执行以下步骤：

1. 访问 Administration Server 并选择 “Preferences”选项卡。
2. 单击 “Server Settings”链接。
3. 进行所需的更改并单击 “OK”。

更改超级用户设置

您可以配置 Administration Server 的超级用户访问。这些设置只影响超级用户帐户。也就是说，如果 Administration Server 使用分布式管理，则需要为您允许的管理员设置其他访问控制。

注意 如果使用 Sun ONE Directory Server 管理用户和组，则需要在更改超级用户名或口令**之前**先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 中的各个 “Users & Groups”表单。要解决此问题，您需要使用确实对目录具有访问权限的管理员帐户来访问 Administration Server，或者使用 Sun ONE Directory Server 的控制台或配置文件来更新目录。

要更改 Administration Server 的超级用户设置，请执行以下步骤：

1. 访问 Administration Server 并选择 “Preferences”选项卡。
2. 单击 “Superuser Access Control”链接。
3. 进行所需的更改并单击 “OK”。

注 您可以将根位置处的 Administration Server 用户更改为操作系统上的另一个用户，以使多个用户 （属于同一组）能够编辑 / 管理配置文件。但请注意，在 UNIX/Linux 平台上，安装程序可以授予某个组对配置文件的 “rw（读 / 写）”权限，而在 Windows 平台上，用户必须属于“Administrators”组。

超级用户的用户名和口令保存在一个名为 *server_root*/https-admserv/config/admpw 的文件中。如果忘记了用户名，可以查看此文件以获取实际的名称；但是，请注意，密码是加密且不可读的。该文件的格式为 username:password。如果忘记了密码，可以编辑 admpw 文件，只需删除加密的密码即可。然后，您可以转至 Server Manager 的各个表单并指定一个新密码。

注意 因为可以编辑 admpw 文件，所以将服务器计算机放在一个安全的地方并限制对其文件系统的访问是非常重要的：

- 在 UNIX/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 守护程序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为 Administration Server 使用的用户帐户。

允许多个管理员

通过分布式管理，多个管理员可以更改服务器的特定部分。

注 缺省目录服务必须是基于 LDAP 的目录服务，以便能够进行分布式管理。

使用分布式管理时，有两个级别的用户：

- **超级用户**是列在 server_root/https-admserv/config/admpw 文件中的用户。这是在安装过程中指定的用户名 （和密码）。此用户对 Administration Server 中的所有表单具有完全访问权限，但 “Users & Groups” 表单除外，这取决于超级用户是否在 LDAP 服务器 （如 Sun ONE Directory Server）中有一个有效帐户。
- **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设置的访问控制规则 （通常由超级用户设置）。管理员可以执行有限的管理任务，并且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）。

有关访问控制的详细信息，请参见第 8 章 “控制对服务器的访问” 中第 156 页上的 “什么是访问控制？ ,”。

注 在启用分布式管理之前，必须先安装 Directory Server。有关详细信息，请参见《Sun ONE Web Server **安装和迁移指南**》和 Sun ONE Directory Server *Administrator's Guide*。

要启用分布式管理，请执行以下步骤：

1. 确认已安装了 Directory Server。
2. 访问 Administration Server。
3. 安装 Directory Server 之后，可能还需要创建一个管理组 （如果以前未创建）。

   要创建组，请执行以下步骤：

   a. 选择 “Users & Groups”选项卡。

   b. 单击 “New Group”链接。

   c. 在 LDAP 目录中创建一个 “administrators”组并添加用户的名称（您希望允许这些用户配置 Administration Server 或在其服务器根目录中安装的任何服务器）。“administrators”组中的所有用户都具有对 Administration Server 的完全访问权限，但是您可以使用访问控制来限制他们能够配置的服务器和表单。

注意 创建访问控制列表后，分布式管理组将添加到该列表中。如果更改 “administrators”组的名称，必须手动编辑访问控制表以更改其引用的组。

4. 选择 “Preferences”选项卡。
5. 单击 “Distributed Admin”链接。
6. 进行所需的更改并单击 “OK”。

有关详细信息，请参见联机帮助中的 “Distributed Administration”。

指定日志文件选项

Administration Server 日志文件记录了有关服务器的数据，包括遇到的错误类型以及有关服务器访问的信息。这些日志提供了遇到的错误类型以及特定文件被访问的时间等数据，通过查看这些日志可以监视服务器的活动并排除故障。

您可以使用 “Log Preferences” 指定 Administration Server 日志中记录的数据类型和格式。例如，可以选择记录访问 Administration Server 的每个客户机的有关数据，也可以忽略某些客户机。此外，您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”，请选择 “Preferences” 选项卡，然后单击 “Logging Options” 链接。

有关详细信息，请参见联机帮助中的 “Logging Options” 页面和第 10 章 “使用日志文件”。

查看日志文件

Administration Server 日志文件位于服务器根目录下的 `admin/logs` 中。例如，在 Windows 上，日志文件的路径可能为 `c:\Sun\server6\https-admserv\logs`。您可以通过 Sun ONE Web Server 的控制台或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

访问日志记录了有关对服务器的请求以及服务器的响应的信息。

要查看访问日志文件，请执行以下步骤：

1. 访问 Administration Server 并选择 “Preferences” 选项卡。
2. 单击 “View Access Log” 链接并单击 “OK”。

有关详细信息，请参见联机帮助中的 “View Access Log” 页面和第 10 章 “使用日志文件”。

错误日志文件

错误日志列出了自日志文件创建后服务器遇到的所有错误。它还包含有关服务器的信息消息，如服务器何时启动、谁试图登录服务器但未成功等。

要查看错误日志文件，请执行以下步骤：

1. 访问 Administration Server 并选择 “Preferences”选项卡。
2. 单击 “View Error Log”链接并单击 “OK”。

有关详细信息，请参见联机帮助中的 “View Access Log”页面和第 10 章 “使用日志文件”。

将日志文件归档

您可以设置日志文件以便将其自动归档。在某个特定时间或指定的间隔后， Sun ONE Web Server 将轮转您的访问日志。Sun ONE Web 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，您可以将文件设置为每小时旋转一次， Sun ONE Web Server 将保存文件并将其命名为 `access.199907152400`，其中名称、年月日以及 24 小时制时间被连接在一起构成一个字符串。根据所设置的日志轮转类型，访问日志归档文件的实际格式会有所不同。

访问日志的轮转在服务器启动时进行初始化。如果启用了轮转， Sun ONE Web 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。

轮转开始后，当发生需要记录到访问日志文件的请求且该请求发生在之前安排的 “下次旋转时间”之后时， Sun ONE Web Server 将创建一个带有新的时间标记的访问日志文件。

使用基于 schedulerd 控制的日志轮转 (UNIX/Linux)

您可以配置 Sun ONE Web Server 的若干功能，使它们自动运行并设置为在指定的时间开始。 `schedulerd` 控制守护程序将检查计算机的时钟，然后在特定的时间开始执行进程。（这些设置存储在 `schedulerd` 文件中。）

此 `schedulerd` 控制守护程序用于控制 Sun ONE Web Server 的 cron 任务，可以通过 Administration Server 将其激活和取消激活。cron 进程执行的任务根据不同的服务器而不同。（请注意，在 Windows 平台上，调度任务发生在单个服务器中。）

`schedulerd` 控制守护程序可以控制的某些任务包括调度内存回收的维护和日志文件的归档。如果更改了所调度任务的设置，则需要重新启动 `schedulerd` 控制守护程序。

要重新启动、启动或停止 `schedulerd` 控制守护程序，请执行以下步骤：

1. 访问 Administration Server 并选择 “Global Settings”选项卡。
2. 单击 “Cron Control”链接。
3. 单击 “Start”、“Stop”或 “Restart”以更改 `schedulerd` 控制。

请注意，任何时候向 schedulerd 添加任务时，都需要重新启动该守护程序。

配置目录服务

您可以使用称为 “轻型目录访问协议” (LDAP) 的开放系统服务器协议在单个 Directory Server 中存储和管理诸如用户名和口令等信息。您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。

要配置目录服务首选项，请执行以下步骤：

1. 访问 Administration Server 并选择 “Global Settings”选项卡。
2. 单击 “Configure Directory Service”链接。
3. 进行所需的更改并单击 “OK”。

有关详细信息，请参见联机帮助中的 “Configure Directory Service”页面。

限制服务器访问

您可以控制对整个服务器或服务器各部分 （即目录、文件、文件类型）的访问。当服务器评估传入的请求时，它将根据一个称为访问控制条目 (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 集合称为访问控制表 (ACL)。当一个请求传入服务器时，服务器将在 *vsclass*`.obj.conf` 文件 （其中 *vsclass* 是虚拟服务器类的名称）中查找对某个 ACL 的引用，然后用该 ACL 确定访问权限。缺省情况下，服务器具有一个 ACL 文件，其中包含多个 ACL。

您可以通过 Administration Server 为所有服务器设置全局访问控制，或通过 Server Manager 为特定服务器实例中的资源设置访问控制。有关设置资源访问控制的详细信息，请参见第 8 章 “控制对服务器的访问”中第 167 页上的 “设置访问控制 ,”。

注 必须先启用分布式管理，然后才能限制服务器访问。

要限制对 Sun ONE Web Server 的访问，请执行以下步骤：

1. 访问 Administration Server 并选择 “Global Settings”选项卡。
2. 单击 “Restrict Access”链接。
3. 选择所需的服务器并单击 “Edit ACL”。

   Administration Server 将显示指定服务器的访问控制规则。
4. 进行所需的访问控制更改并单击 “OK”。有关详细信息，请参见联机帮助中的 “Restrict Access”页面。

第 6 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 ONE Web Server 6.1 的安全性。还介绍了如何激活用于保护您的数据、拒绝入侵者访问和允许所需的访问的各种安全功能。 Sun ONE Web Server 6.1 集成了所有 Sun ONE 服务器的安全体系结构：它建立在行业标准和公共协议基础之上，以获取最大的互操作性和一致性。

在阅读本章之前，您应该已经熟悉公共密钥加密的基本概念。这些概念包括加密和解密、公共密钥和专用密钥、数字证书以及加密协议。有关详细信息，请参阅 *Introduction to SSL*。

以下各节详细介绍了确保 Web 服务器安全的过程：

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身份确认的过程。证书是支持验证的一种方法。

使用证书进行验证

证书中包含的数字数据用于指定个人、公司或其他实体的名称，并证明证书中包含的公共密钥属于该实体。客户机和服务器都可以拥有证书。

证书由证书授权机构 （即 CA）颁发并进行数字签名。 CA 可以是通过 Internet 销售证书的公司，也可以是负责为贵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验证器。

除了公共密钥和由证书标识的实体名称之外，证书还包括到期日期、颁发该证书的 CA 的名称和颁发该证书的 CA 的 “数字签名”。有关证书内容和格式的详细信息，请参见 *Introduction to SSL*。

注 在激活加密之前必须安装服务器证书。

服务器验证

服务器验证指客户机对服务器进行的信任识别；即对被认为要对位于特定网络地址的服务器负责的组织进行识别。

客户机验证

客户机验证指服务器对客户机进行的信任识别；即对被认为使用客户端软件的人员进行识别。客户机可以有多个证书，如同一个人可以有几个不同的身份一样。

虚拟服务器证书

每台虚拟服务器可以拥有不同的证书数据库。每个虚拟服务器数据库可以包含多个证书。虚拟服务器的每个实例也可以拥有不同的证书。

创建信任数据库

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

创建信任数据库时，您需要指定将用于密钥对文件的密码。您还需要此密码来启动使用加密通信的服务器。有关更该口令时的注意事项列表，请参见第 140 页上的“更改密码或 PIN”。

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

server_root/alias/<serverid-hostname>-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。虚拟服务器将采用为其服务器实例创建的信任数据库。

创建信任数据库

要创建信任数据库，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager，然后选择“Security”选项卡。

   对于 Server Manager，必须先从下拉列表中选择服务器实例。

2. 单击“Create Database”链接。
3. 输入数据库的密码。
4. 重复以上步骤。
5. 单击“OK”。
6. 对于 Server Manager，单击“Apply”，然后单击“Restart”使更改生效。

使用 password.conf

缺省情况下， Web 服务器会在启动之前提示管理员输入密钥数据库口令。如果希望重新启动一个无人参与的 Web 服务器，则需要将该密码保存在 `password.conf` 文件中。仅当系统受到充分的保护时才可以执行此操作，只有这样文件和密钥数据库才不会被损坏。

正常情况下，无法使用 /etc/rc.local 或 /etc/inittab 文件启动已启用 SSL 的 UNIX 服务器，因为该服务器在启动之前要求输入口令。尽管可以通过将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，但建议不要使用这种方法。服务器的 password.conf 文件应归超级用户或安装服务器的用户所有，并且只有所有者对其具有读写权限。

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 的服务器的口令。将启用了 SSL 的服务器的口令保存在 password.conf 文件中之前，请考虑可能带来的安全风险。

在 Windows 上，如果安装了 NTFS 文件系统，则应该限制对包含 password.conf 文件 （即使不使用该文件）的目录的访问权限，从而保护包含该文件的目录。管理服务器用户和 Web 服务器用户应该对该目录具有读 / 写权限。保护该目录可以防止其他用户创建伪 password.conf 文件。您无法通过限制对 FAT 文件系统上的目录或文件的访问权限来保护它们。

自动启动启用了 SSL 的服务器

如果您不担心会带来安全风险，请执行以下步骤自动启动启用了 SSL 的服务器：

1. 确保已启用 SSL。
2. 在服务器实例的 config 子目录中创建新的 password.conf 文件。
   - 如果使用的是服务器附带的内部 PKCS#11 软件加密模块，请输入以下信息：

     internal:*your_password*
   - 如果使用的是其他 PKCS#11 模块 （用于硬件加密或硬件加速器），请指定 PKCS#11 模块的名称，后面跟着密码。例如：

     nFast:*your_password*
3. 停止并重新启动服务器，以使新设置生效。

即使创建了 password.conf 文件之后，您在启动 Web 服务器时始终会收到输入密码的提示。

申请和安装 VeriSign 证书

VeriSign 是 Sun ONE Web Server 的首选证书授权机构。 VeriSign 的 VICE 协议可以简化证书的请求过程。 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认证机构 (CA)。如果公司有自己的内部 CA，则可以向其申请证书。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。包括指向其站点链接的可用认证机构列表可以从 “Request a Certificate”中获得。有关 CA 所需内容的详细信息，请参阅通过 “Server Administrator”和 “Request a Certificate”下的 “Server Manager Security Pages”所获得的认证机构列表。

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。您可以为每台虚拟服务器选择一个服务器实例证书。

申请 VeriSign 证书

要请求 VeriSign 证书，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager，然后选择 “Security”选项卡。

   对于 Server Manager，必须先从下拉列表中选择服务器实例。
2. 单击 “Request VeriSign Certificate”链接。
3. 查看所需的步骤。
4. 单击 “OK”。
5. 按照 VeriSign 中的步骤进行操作。

安装 VeriSign 证书

如果您申请了 VeriSign 证书并获得了批准，该证书会于一到三天内显示在 “Install VeriSign Certificate”页面的下拉列表中。要安装 VeriSign 证书，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager，然后选择 “Security”选项卡。

   对于 Server Manager，必须先从下拉列表中选择服务器实例。
2. 单击 “Install VeriSign Certificate”链接。

3. 除非您将使用外部加密模块，否则从加密模块的下拉列表中选择内部 （软件）模块。
4. 输入密钥对文件密码或 PIN。
5. 从下拉列表中选择要检索的事务 ID。

   通常选择最后一个。
6. 单击 “OK”。
7. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

申请和安装其他服务器证书

除了 VeriSign，还可以从其他认证机构申请和安装证书。可以通过服务器管理员 (Server Administrator) 和 “Request a Certificate”下的 “Server Manager Security”获得 CA 列表。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这些其他类型的服务器证书。

所需的 CA 信息

开始请求过程之前，请确保您了解 CA 所需的信息。无论从商业 CA 还是内部 CA 申请服务器证书，都需要提供以下信息：

- **“Common Name”**必须是在 DNS 查找中使用的全限定主机名 （例如，*www.sun.com*）。这是浏览器用于连接到您站点的 URL 中的主机名。如果这两个名称不匹配，客户机将收到证书名称与站点名称不匹配的通知，并怀疑您的证书的真实性。某些 CA 可能会有其他要求，因此对其进行检查很重要。

  如果从内部 CA 申请证书，也可以在此字段中输入通配符或正则表达式。多数供应商都不会批准在通用名称中输入通配符或正则表达式来申请的证书。
- “**Email Address**”是您的商业 Email 地址。该地址用于您与 CA 之间的通信。
- “**Organization**”是公司、教育机构、合作伙伴等的正式而合法的名称。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。
- “**Organizational Unit**”是用于说明公司中组织的可选字段。也可以用于标注不太正式的公司名称 （不带 *Inc.*、 *Corp.* 等等）。
- “**Locality**”是通常用于描述组织所在的城市、公国或国家 （地区）的可选字段。

- “**State or Province**”通常是必需的，但对于某些 CA 是可选的。请注意，多数 CA 不接受缩写，但会检查这些缩写进行确认。
- “**Country**”是必需的，即您所在国家 （地区）名称的两个字符的缩写 （ISO 格式）。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 （称为独特的名称 [DN]），用于唯一标识证书的主题。

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

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.sun.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重大客户诉讼案件的公司。

申请其他服务器证书

要请求证书，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager，然后选择 “Security”选项卡。

   对于 Server Manager，必须先从下拉列表中选择服务器实例。

2. 单击 “Request a Certificate”链接。
3. 选择这是一个新证书，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. 要指定提交证书申请的方式，请执行以下步骤：

   - 如果 CA 期望以 Email 的形式收到申请，请选中 “CA Email”并输入该 CA 的 Email 地址。要获得 CA 的列表，请单击 “List of available certificate authorities”。
   - 如果要从使用 Netscape 证书服务器 (Certificate Server) 的内部 CA 申请证书，请单击 “CA URL”并输入该证书服务器的 URL。此 URL 应指向处理证书请求的证书服务器的程序。样例 URL 如下所示：
     `https://CA.mozilla.com:444/cms`。

5. 从下拉列表中选择申请证书时要使用的密钥对文件的加密模块。

6. 输入密钥对文件的密码。

   除非您选择内部模块以外的加密模块，否则该密码是您创建信任数据库时指定的密码。服务器将使用该密码获取专用密钥并加密发送给 CA 的信息，然后将您的**公共密钥**和加密的信息发送给 CA。 CA 使用公共密钥来解密您的信息。

7. 输入您的标识信息。

   此信息的格式因 CA 而异。有关这些字段的常规说明，请参阅通过服务器管理员 (Server Administrator) 和 “Request a Certificate”下的 “Server Manager Security”中所获得的认证机构的列表。请注意，证书更新通常不需要此信息中的大部分内容。

8. 仔细检查这些内容以确保其准确性。

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

9. 单击 “OK”。

10. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

服务器将生成包含您的信息的证书申请。该申请中包含使用专用密钥创建的数字签名。CA 使用数字签名来验证在从服务器计算机向 CA 的路由过程中请求未被更改。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 Email 发送申请，服务器将撰写包含申请的 Email 并将其发送给 CA。通常，证书会通过 Email 返回。如果您指定了指向证书服务器的 URL，服务器将使用 URL 向证书服务器提交申请。您可以通过 Email 或其他方式获得回应，这取决于 CA。

如果 CA 同意向您颁发证书，则会通知您。多数情况下， CA 会通过 Email 向您发送证书。如果您的组织使用证书服务器，则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 在向您颁发证书之前都需要您提供身份证明。而且，要获得批准可能需要一天到两个月的时间。您负责及时向 CA 提供所有必需的信息。

收到证书后，即可进行安装。在此期间，您仍然可以使用未安装 SSL 的服务器。

安装其他服务器证书

当您收到从 CA 发回的证书时，该证书将通过公共密钥加密，因此只有您可以将其解密。只有输入正确的信任数据库密码，才能解密和安装证书。

证书有三种类型：

- 提供给客户机的您自己的服务器证书
- 在证书链中使用的 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 证书用于标识认证机构 (CA) 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 未向您自动发送其证书，则您应该请求证书。很多 CA 在 Email 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。

当您从 CA 收到证书时，该证书将通过公共密钥加密，因此只有您可以将其解密。安装证书时，服务器将使用您指定的密钥对文件密码将其解密。如下所述，您可以将 Email 保存在服务器可以访问的位置中，也可以复制 Email 的文本并准备将其粘贴到 “Install Certificate”表单中。

安装证书

要安装证书，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager，然后选择 “Security”选项卡。

   对于 Server Manager，必须先从下拉列表中选择服务器实例。

2. 单击 “Install Certificate”链接。
3. 选中要安装的证书类型：
   - “This Server”用于仅与您的服务器关联的单个证书。
   - “Server Certificate Chain”用于要包含在证书链中的 CA 证书。
   - “Trusted Certificate Authority (CA)”用于某个信任 CA 的证书，该 CA 将作为客户机验证的信任 CA 使用。

4. 从下拉列表中选择加密模块。
5. 输入密钥对文件密码。
6. 如果该证书的名称是此服务器实例中使用的唯一名称，请保留 “a name for the certificate”（该证书的名称）字段为空，除非出现以下情况：

   - 多个证书将用于虚拟服务器

     输入服务器实例中唯一的证书名称

   - 使用了内部模块以外的加密模块

     在单个加密模块中，输入所有服务器实例中唯一的证书名称

   如果输入了名称，该名称将显示在 “Manage Certificates”列表中，并且应为说明性名称。例如，“United States Postal Service CA”是某个 CA 的名称，而 “VeriSign Class 2 Primary CA”则同时说明了 CA 和证书的类型。如果未输入证书名称，则应用缺省值。
7. 选择以下任一选项：

   - “Message is in this file”（消息包含在此文件中），并输入已保存的 Email 的完整路径名
   - “Message text”（消息文本）（带标头），并粘贴 Email 文本

     如果复制并粘贴文本，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. 选择以下任一选项：

   - “Add Certificate”（如果要安装新的证书）。
   - “Replace Certificate”（如果要安装证书更新）。
10. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

证书将存储在服务器的证书数据库中。文件名为 `<alias>-cert8.db`。例如：

```
https-serverid-hostname-cert8.db
```

升级时迁移证书

如果要从 iPlanet Web Server 4.1 或 6.0 进行移植，您的文件 （包括信任数据库和证书数据库）将被自动更新。

密钥对文件和证书只有在服务器启用了安全性时才能被迁移。也可以使用“Administration Server”和 “Server Manager”中的 “Security”选项卡自行迁移密钥和证书。

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 ONE Web Server 6.1 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。

您可以通过 Administration Server （为其自身）或 Server Manager （为服务器实例）管理信任数据库及其委托证书，其中包括服务器证书和所有包含的认证机构。证书和密钥对数据库文件现在按使用它们的服务器实例命名。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。以前的数据库中列出的所有认证机构都将迁移到 Sun ONE Web Server 6.1 数据库中。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。

使用内置根证书模块

Sun ONE Web Server 6.1 附带的动态可装入根证书模块包括了许多 CA （其中包括 VeriSign）的根证书。通过根证书模块，您可以将根证书升级到更高的版本，且方法比以前容易的多。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 Sun ONE Web Server 或 Service Packs 中将可用。

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

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

如果以后要恢复根证书模块，则可以将扩展程序从 `bin/https/lib` （UNIX 和 HP）或 `bin\https\bin` (Windows) 复制回 `alias` 子目录。

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

管理证书

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

要管理证书列表，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager，然后选择 “Security”选项卡。

   对于 Server Manager，必须先从下拉列表中选择服务器实例。

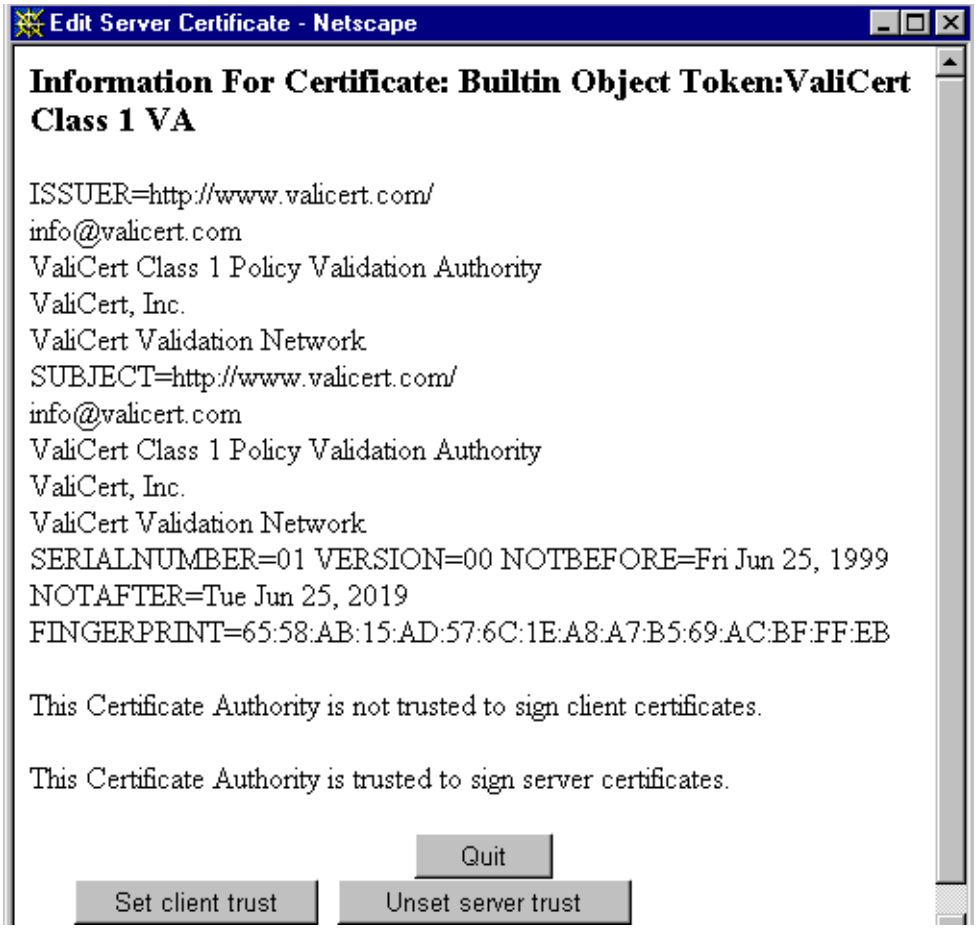
2. 单击 “Manage Certificates”链接。

   - 如果要使用内部加密模块管理缺省配置的证书，将显示所有已安装证书的列表，其中包括证书的类型和截止日期。所有证书都存储在 *server_root*/alias 目录中。
   - 如果要使用外部加密模块 （例如硬件加速器），则需要先为每个特定模块输入密码，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 “Certificate Name”（证书名称）。

   将显示 “Edit Server Certificate”，其中包含该证书类型的管理选项。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。

   编辑服务器证书



4. 在 “Edit Server Certificate”窗口中，您可以选择以下选项：
   - “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）
5. 单击 “OK”。
6. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

证书信息中包含所有者和颁发证书的机构。

通过信任设置，您可以设置客户机信任或取消设置服务器信任。对于 LDAP 服务器证书，服务器必须被信任。

安装和管理 CRL 和 CKL

证书撤销列表 (CRL) 和损坏的密钥列表 (CKL) 能够清楚地列出客户机或服务器用户应不再信任的所有证书和密钥。如果证书中的数据发生变化 （例如，某位用户在证书到期之前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 都由 CA 生成并定期更新。

安装 CRL 或 CKL

要从 CA 获得 CRL 或 CKL，请执行以下步骤：

1. 获取 CA 的 URL，以下载 CRL 或 CKL。
2. 在浏览器中输入 URL，访问该站点。
3. 按照 CA 的说明将 CRL 或 CKL 下载到本地目录中。
4. 访问 Administration Server 或 Server Manager，然后选择 “Security”选项卡。

   对于 Server Manager，必须先从下拉列表中选择服务器实例。
5. 单击 “Install CRL/CKLs”链接。
6. 选择以下任一选项：
   - “Certificate Revocation List”（证书撤回列表）
   - “Compromised Key List”（损坏的密钥列表）
7. 输入关联文件的完整路径名。

8. 单击 “OK”。
   - 如果选择 “Certificate Revocation List”，将显示 “Add Certificate Revocation List”，其中列出了 CRL 信息。
   - 如果选择 “Compromised Key List”，将显示 “Add Compromised Key List”，其中列出了 CKL 信息。

注 如果数据库中已存在 CRL 或 CKL 列表，将显示 “Replace Certificate Revocation List”或 “Replace Compromised Key List”。

9. 单击 “Add”。
10. 单击 “OK”。
11. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

管理 CRL 和 CKL

要管理 CRL 和 CKL，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager，然后选择 “Security”选项卡。

   对于 Server Manager，必须先从下拉列表中选择服务器实例。
2. 单击 “Manage CRL/CKLs”链接。

   将显示 “Manage Certificate Revocation Lists /Compromised Key Lists”，其中列出了所有已安装的服务器 CRL 和 CKL 及其截止日期。
3. 从 “Server CRLs”或 “Server CKLs”列表中选择 “Certificate Name”。
4. 选择以下选项：
   - “Delete CRL”
   - “Delete CKL”
5. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

设置安全首选项

获得证书后，就可以开始保护您的服务器。 Sun ONE Web Server 提供了多个安全元素。

加密是转换信息、使除预期接收者以外的任何人都无法识别信息的过程。解密是变换加密信息、使其重新可被识别的过程。Sun ONE Web Server 6.1 支持 SSL 和 TLS 加密协议。

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

在任何双向加密过程中，双方都必须使用相同的加密算法。由于可以使用多种加密算法，因此需要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。您可以从 SSL2、 SSL3 和 TLS 协议中选择加密算法。

注 因为在 SSL 2.0 版本之后对 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，否则不要使用 SSL 2。使用 SSL 2 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。使用加密算法的同时还必须使用密钥，以便生成真正的加密结果，或解密以前加密的信息。加密过程使用以下两种密钥获得此结果：公共密钥和专用密钥。使用公共密钥加密的信息只能使用关联的专用密钥进行解密。公共密钥作为证书的一部分发布，因此只有关联的专用密钥受到保护。

有关各种加密算法套件的说明以及密钥和证书的详细信息，请参见 *Introduction to SSL*。

要指定服务器可以使用的加密算法，请在列表中选中这些算法。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。但是，您可能不希望启用非最优加密的加密算法。

注意 请不要选择 “No Encryption, only MD5 message 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。

SSL 和 TLS 协议

Sun ONE Web Server 6.1 支持用于加密通信的安全套接字层 (SSL) 协议和传输层安全性 (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。要启用 Administration Server 上的 SSL，请执行以下步骤：

1. 访问 Administration Server 并选择 “Global Settings”选项卡。
2. 单击 “Configure Directory Service”链接。
3. 选择 “Yes”使用安全套接字层 (SSL) 进行连接。
4. 单击 “Save Changes”。
5. 单击 “OK”将您的端口更改为使用 SSL 的 LDAP 标准端口。

为侦听套接字启用安全性

您可以通过以下方式确保服务器侦听套接字的安全：

- 打开安全性
- 为侦听套接字选择服务器证书
- 选择加密算法

打开安全性

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

创建侦听套接字时打开安全性

要在创建新的侦听套接字时打开安全性，请执行以下步骤：

1. 访问 Server Manager 并从下拉列表中选择要在其中创建侦听套接字的服务器实例。
2. 选择 “Preferences”选项卡 （如果尚未显示）。
3. 选择 “Edit Listen Sockets”链接。

   将显示 “Edit Listen Sockets”。
4. 单击 “New”按钮。

   将显示 “Add Listen Socket”。
5. 输入所需信息并选择缺省的虚拟服务器。
6. 要打开安全性，请从 “Security”下拉列表中选择 “Enabled”。
7. 单击 “OK”。
8. 单击 “Apply”，然后单击 “Restart”使更改生效。

注 您需要在创建侦听套接字后，使用 “Edit Listen Sockets”链接来配置安全设置。

编辑侦听套接字时打开安全性

您也可以在通过 Administration Server 或 Server Manager 编辑侦听套接字时打开安全性。要在编辑侦听套接字时打开安全性，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager，然后选择 “Security”选项卡。

   对于 Server Manager，必须先从下拉列表中选择服务器实例。
2. 选择 “Preferences”选项卡 （如果尚未显示）。
3. 选择 “Edit Listen Sockets”链接。

   将显示 “Edit Listen Sockets”。
4. 要编辑侦听套接字，请单击要编辑的侦听套接字的 “Listen Socket ID”。

   将显示 “Edit Listen Socket”。
5. 要为侦听套接字打开安全性，请从 “Security”下拉列表中选择 “Enabled”。
6. 单击 “OK”。

7. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

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 必须至少安装了一个证书。

要为侦听套接字选择服务器证书以便使用，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager，然后选择 “Preferences”选项卡。

   对于 Server Manager，必须先从下拉列表中选择服务器实例。

2. 选择 “Edit Listen Sockets”链接。

   将显示 “Edit Listen Sockets”。

3. 要编辑侦听套接字，请单击要编辑的侦听套接字的 “Listen Socket ID”。

   将显示 “Edit Listen Socket”。

4. 要为侦听套接字打开安全性，请从 “Security”下拉列表中选择 “Enabled”。

注 如果安装了外部模块，将显示 “Manage Server Certificates”页面，并要求在继续操作之前输入外部模块的口令。

5. 从 “Server Certificate Name”下拉列表中为侦听套接字选择服务器证书。

   该列表中包含了所有已安装的内部和外部证书。

注 如果未安装服务器证书，将显示警告消息而不是 “Server Certificate Name”下拉列表。

6. 单击 “OK”。
7. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

选择加密算法

要保护 Web 服务器的安全性，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。在侦听套接字上为 Server Manager 启用 SSL 和 TLS 将为所有与该侦听套接字关联的虚拟服务器设置安全首选项。

如果希望使用非加密的虚拟服务器，则必须将其配置为使用相同的侦听套接字，并且关闭安全性。

缺省设置允许使用最常用的加密算法。除非有充分的理由不使用特定的加密算法套件，否则应全部启用。有关特定密码的详细信息，请参见 *Introduction to SSL*。

注 必须至少安装了一个证书。

推荐使用的 `tlsrollback` 参数的缺省设置为 `True`。这会将服务器配置为检测人为版本回滚攻击。将此值设置为 `False` 可能需要与某些未正确实现 TLS 规范的客户机之间的互操作性。

请注意，将 `tlsrollback` 设置为 `False` 会降低连接对版本回滚攻击的防护能力。版本回滚攻击是一种机制，第三方可以通过这种机制强制客户机和服务器使用安全性较低的早期协议（例如 SSLv2）进行通信。由于 SSLv2 协议中存在已知的不足之处，因此无法检测到版本回滚攻击将使第三方更容易截取和解密加密的连接。

要启用 SSL 和 TLS，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager，然后选择 “Preferences”选项卡。

   对于 Server Manager，您必须先从下拉列表中选择服务器实例。

2. 单击 “Edit Listen Sockets”链接。

   将显示 “Edit Listen Sockets”。对于安全侦听套接字，“Edit Listen Socket”中显示可用的加密算法设置。

注 如果未在侦听套接字上启用 “Security”，则不会列出任何 SSL 和 TLS 信息。要使用加密算法，请确保已在选定侦听套接字上启用了该安全性。有关更多信息，请参见 “为侦听套接字启用安全性”。

3. 选中所需加密设置对应的复选框。

注 对于 Netscape Navigator 6.0，请选中 TLS 和 SSL3。对于 TLS 回滚也要选中 TLS，并确保禁用了 SSL3 和 SSL2。

4. 单击 “OK”。

5. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

注 打开侦听套接字的安全性后应用更改时，系统将自动修改 `magnus.conf` 文件以显示安全性已打开，并且自动指定所有与该侦听套接字关联的虚拟服务器的缺省安全参数。

在服务器上启用 SSL 后，它的 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#`*`]`

例如， `https://admin.sun.com:443`。

如果使用缺省的安全 http 端口号 (443)，则无需在 URL 中输入该端口号。

全局配置安全性

安装启用了 SSL 的服务器将在 `magnus.conf` 文件 （服务器的主配置文件）中为全局安全参数创建指令条目。安全性必须设置为 “on”，虚拟服务器安全设置才能正常运行。虚拟服务器的 SSL 特性可以以服务器为单位在 `server.xml` 文件的 `SSLPARAMS` 元素中查找。

要设置 SSL 配置文件指令的值，请执行以下步骤：

1. 访问 Server Manager 并从下拉列表中选择虚拟服务器的服务器实例。
2. 确保为要配置的侦听套接字启用了安全性。要进行此操作，请执行以下步骤：
   a. 单击 “Edit Listen Sockets”链接。
   b. 单击要启用其安全性的侦听套接字所对应的 “Listen Socket ID”。

      将转至 “Edit Listen Socket”。
   c. 从 “Security”下拉列表中选择 “Enabled”。
   d. 单击 “OK”。

3. 单击 “Magnus Editor” 链接。
4. 从下拉列表中选择 “SSL Settings” 并单击 “Manage”。
5. 输入以下各参数的值：
   - SSLSessionTimeout
   - SSLCacheEntries
   - SSL3SessionTimeout
6. 单击 “OK”。
7. 单击 “Apply”，然后单击 “Restart” 使更改生效。

这些 SSL 配置文件指令如下所述：

SSLSessionTimeout

`SSLSessionTimeout` 指令用于控制 SSL2 会话缓存。

语法

`SSLSessionTimeout` seconds

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

SSLCacheEntries

指定可以缓存的 SSL 会话的数量。

SSL3SessionTimeout

SSL3SessionTimeout 指令用于控制 SSL3 和 TLS 会话缓存。

语法

`SSL3SessionTimeout` seconds

其中 `seconds` 是缓存的 SSL3 会话保持有效的秒数。缺省值为 86400 秒 （24 小时）。如果指定了 `SSL3SessionTimeout` 指令，秒数的值将自动限定为 5 到 86400 之间。

使用外部加密模块

Sun ONE Web Server 6.1 支持以下使用外部加密模块 （例如智慧卡或令牌环）的方法：

- PKCS#11
- FIPS-140

激活 FIPS-140 加密标准之前，您需要添加 PKCS #11 模块。

安装 PKCS#11 模块

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

使用 modutil 工具安装 PKCS#11 模块

可以使用 `modutil` 工具并通过 `.jar` 文件或对象文件的形式安装 PKCS#11 模块。

要使用 `modutil` 安装 PKCS#11 模块，请执行以下步骤：

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/https/admin/bin` 添加到您的 PATH 中。
4. 在 `server_root/bin/https/admin/bin` 中找到 `modutil`。
5. 设置环境。例如：
   - 在 UNIX 上：`setenv`

     `LD_LIBRARY_PATH server_root/bin/https/lib:${LD_LIBRARY_PATH}`
   - 在 IBM-AIX 上：`LIBPATH`
   - 在 HP-UX 上：`SHLIB_PATH`
   - 在 Windows 上，将以下内容添加到 `PATH`

     `LD_LIBRARY_PATH server_root/bin/https/bin`

     您可以在以下目录中找到您计算机的 PATH：
     `server_root/https-admin/start`。

6. 输入命令：modutil。

   将列出各种选项。

7. 执行所需的操作。

   例如，要在 UNIX 中添加 PCKS#11 模块，您需要输入：

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

使用 pk12util

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

使用 *pk12util* 导出

要从内部数据库中导出证书和密钥，请执行以下步骤：

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

     LD_LIBRARY_PATH/server_root/bin/https/lib:${LD_LIBRARY_PATH}
   - 在 IBM-AIX 上：LIBPATH
   - 在 HP-UX 上：SHLIB_PATH
   - 在 Windows 上，将以下内容添加到 PATH

     LD_LIBRARY_PATH server_root/bin/https/bin

     您可以在以下目录中找到您计算机的 PATH：server_root/https-admin/start。
5. 输入命令：pk12util。

   将列出各种选项。

6. 执行所需的操作。

   例如，在 UNIX 中，您需要输入：

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

7. 输入数据库密码。

8. 输入 pkcs12 密码。

使用 *pk12util* 导入

要将证书和密钥导入内部或外部 PKCS#11 模块，请执行以下步骤：

1. 转至包含数据库的 server_root/alias 目录。

2. 将 server_root/bin/https/admin/bin 添加到您的 PATH 中。

3. 在 server_root/bin/https/admin/bin 中找到 pk12util。

4. 设置环境。例如：

   - 在 UNIX 上：setenv

     ```
     LD_LIBRARY_PATH/server_root/bin/https/lib:${LD_LIBRARY_PATH}
     ```

   - 在 IBM-AIX 上：LIBPATH

   - 在 HP-UX 上：SHLIB_PATH

   - 在 Windows 上，将以下内容添加到 PATH

     ```
     LD_LIBRARY_PATH server_root/bin/https/bin
     ```

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

5. 输入命令：pk12util。

   将列出各种选项。

6. 执行所需的操作。

   例如，在 UNIX 中，您需要输入：

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

   -P 必须跟在 -h 之后，并且必须是最后一个参数。

   输入正确的令牌名，包括大写字母和引号之间的空格。

7. 输入数据库密码。

8. 输入 pkcs12 密码。使用某个外部证书启动服务器。

如果服务器的证书安装在外部 PKCS#11 模块 （例如，硬件加速器）中，服务器将无法使用该证书启动，除非您对 server.xml 进行编辑，或如下所述指定证书的名称。

服务器始终尝试使用名为 “Server-Cert”的证书启动。但外部 PKCS#11 模块中的证书将在其标识符中包含该模块的某个令牌名。例如，名为 “smartcard0”的外部智慧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，需要为在其上运行的侦听套接字指定证书名称。

为侦听套接字选择证书名称

要为侦听套接字选择证书名称，请执行以下步骤：

注 如果未在侦听套接字上启用 “Security”，则不会列出证书的信息。要为侦听套接字选择证书名称，首先必须确保已启用了其上的安全性。有关更多信息，请参见 “为侦听套接字启用安全性”。

1. 访问 Administration Server 或 Server Manager，然后选择 “Preferences”选项卡。

   对于 Server Manager，您必须先从下拉列表中选择服务器实例。

2. 选择 “Preferences”选项卡 （如果尚未选定）。
3. 单击 “Edit Listen Sockets”链接。

   将显示 “Edit Listen Sockets”。

4. 单击要与证书关联的侦听套接字所对应的 “Listen Socket Id”链接。

   将显示 “Edit Listen Socket”。

5. 从 “Server Certificate Name”下拉列表中为侦听套接字选择服务器证书。

   该列表中包含了所有已安装的内部和外部证书。

注 如果未安装服务器证书，将显示警告消息而不是 “Server Certificate Name”下拉列表。

6. 单击 “OK”。
7. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

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

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

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

注 如果尚未创建信任数据库，您为外部 PKCS#11 模块请求或安装证书时将创建一个信任数据库。创建的缺省数据库没有密码，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。如果创建的缺省数据库没有密码，请使用 “Security”选项卡和 “Create Database”来设置密码。

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。在服务器上安装 PKCS#11 之后，您可以对 Sun ONE Web Server 进行配置，使其与联邦信息处理标准 (FIPS)-140 兼容。这些库仅包含在 SSL 3.0 版本中。

要启用 FIPS-140，请执行以下步骤：

1. 按照 FIPS-140 中的说明安装该插件。
2. 访问 Administration Server 或 Server Manager，然后选择 “Preferences”选项卡。

   对于 Server Manager，您必须先从下拉列表中选择服务器实例。
3. 单击 “Edit Listen Sockets”链接。

   将显示 “Edit Listen Sockets”。对于安全侦听套接字，“Edit Listen Socket”中将显示可用的安全设置。

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

4. 从 SSL 3 版本的下拉列表中选择 “Enabled”（如果尚未选定）。

5. 选中适当的 FIPS-140 加密算法套件：
   - (FIPS) 56 位加密 DES 和 SHA 消息验证
   - (FIPS) 168 位加密 Triple DES 和 SHA 消息验证
6. 单击 “OK”。
7. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

设置客户机安全要求

执行可确保服务器安全的所有步骤后，可以为客户机设置其他安全要求。

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。

Sun ONE Web 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。您可以在 Administration Server 的 “Security”下的 “Manage Certificates”中查看签名客户机证书时信任的 CA 列表。 CA 有四种类型：

- 不可信 CA （不匹配）
- 信任的服务器 CA （不匹配）
- 信任的客户机 CA （匹配）
- 信任的客户机 / 服务器 CA （匹配）

您可以对 Web 服务器进行配置，以拒绝不具有来自信任 CA 的客户机证书的任何客户机。要接受或拒绝信任的 CA，必须为 CA 设置了客户机信任。有关更多信息，请参见 “第 114 页上的 “管理证书””。

如果证书已过期， Sun ONE Web 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 Administration Server 的 “Manage Certificates”中查看已过期的证书。

您可以对服务器进行配置，以便从客户机证书收集信息并将其与 LDAP 目录中的用户项相匹配。这样可以确保客户机具有有效的证书和 LDAP 目录中的项。而且还可以确保客户机证书与 LDAP 目录中的证书相匹配。要了解如何进行此操作，请参见 第 131 页上的 “将客户机证书映射到 LDAP”。

您可以将客户机证书和访问控制结合使用，以便除了来自信任的 CA 以外，与证书关联的用户还必须与访问控制规则 (ACL) 相匹配。有关更多信息，请参见 “第 164 页上的 “使用访问控制文件””。

您也可以处理客户机证书的信息。有关详细信息，请参见 Sun ONE Web Server 6.1 *NSAPI Programmer's Guide*。

申请客户机验证

要请求客户机验证，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager，然后选择 “Preferences”选项卡。

   对于 Server Manager，必须先从下拉列表中选择服务器实例。

2. 单击 “Edit Listen Sockets”链接。

   将显示 “Edit Listen Sockets”。

3. 单击要为其申请客户机验证的侦听套接字所对应的 “Listen Socket Id”链接。

   将显示 “Edit Listen Socket”。

4. 要为侦听套接字申请客户机验证，请从 “Client Authentication”下拉列表中选择 “Required”。

5. 单击 “OK”。

6. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

注 目前，每个 Web 服务器实例只有一个证书信任数据库。在该服务器实例下运行的所有安全虚拟服务器都共享同一个信任的客户机 CA 列表。如果两台虚拟服务器需要不同的信任 CA，则这些虚拟服务器应该在具有单独信任数据库的不同的服务器实例中运行。

将客户机证书映射到 LDAP

本节介绍 Sun ONE Web Server 用来将客户机证书映射到 LDAP 目录中的项的过程。

服务器获得客户机的请求后，将在处理请求之前索要客户机的证书。某些客户机会在向服务器发送请求的同时发送客户机证书。

注 将客户机证书映射到 LDAP 之前，还需要设置所需的 ACL；有关详细信息，请参阅第 8 章 “控制对服务器的访问”。

服务器将尝试查看该 CA 是否与 Administration Server 中的某个信任 CA 相匹配。如果找不到匹配的 CA， Sun ONE Web Server 将终止连接。如果能够找到匹配的 CA，服务器将继续处理请求。

验证证书是来自信任的 CA 之后，服务器会通过以下方式将证书映射到 LDAP 项：

- 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）相关信息相匹配的项。
- （可选）验证客户机证书是否与对应于 DN 的 LDAP 项中的证书相匹配。

服务器使用名为 `certmap.conf` 的证书映射文件来确定如何进行 LDAP 搜索。映射文件将告诉服务器要使用客户机证书中的哪些值 （例如最终用户的名称、 Email 地址等）。服务器将使用这些值搜索 LDAP 目录中的用户项，但服务器首先需要确定从 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需要搜索的内容 （步骤 1）之后，将在 LDAP 目录中执行搜索 （步骤 2）。如果未找到匹配项或找到多个匹配项，并且映射**未**设置为验证证书，搜索将失败。有关预期搜索结果行为的完整列表，请参见下表 “表 5-1”。请注意，您可以在 ACL 中指定预期的行为，例如，您可以指定 Sun ONE Web Server 在证书匹配失败时仅接受您。有关如何设置 ACL 首选项的详细信息，请参阅第 164 页上的 “使用访问控制文件”。

表 6-1 LDAP 搜索结果

LDAP 搜索结果	证书验证打开	证书验证关闭
未找到项	验证失败	验证失败
恰好找到一个项	验证失败	验证成功
找到多个项	验证失败	授权失败

服务器在 LDAP 目录中找到匹配项和证书后，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 目录中查找用户项的方式。您可以使用 certmap.conf 配置证书 （按名称指定）映射到 LDAP 项的方式。您可以编辑此文件并添加项，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、Email 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其搜索
- 在 LDAP 目录中进行搜索时，服务器应用作搜索条件的证书属性
- 服务器是否要进行其他验证过程

证书映射文件位于以下位置：

server_root/userdb/certmap.conf

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

```
certmap <name> <issuerDN>

<name>:<property> [<value>]
```

第一行用于指定项的名称以及形成 CA 证书中独特的名称的属性。该名称是任意的，您可以将其定义为所需的任何名称。但是，issuerDN 必须与颁发客户机证书的 CA 的颁发者 DN **完全**匹配。例如，以下两个 issuerDN 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项：

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

提示 如果使用的是 Sun ONE Directory Server 并在匹配 issuerDN 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特性与值相匹配。 certmap.conf 文件中包含六个缺省特性 （可以使用证书 API 自定义特性）：

- DNComps 由一系列以逗号分隔的属性组成，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> 项开始搜索，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 项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项。

- FilterComps 由一系列以逗号分隔的属性组成，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 目录中各项的搜索条件。如果服务器在 LDAP 目录中找到了一个或多个与从证书中收集到的用户信息相匹配的条目，则表示搜索成功并且服务器可以选择执行某个验证。

  例如，如果 FilterComps 设置为使用 Email 和用户 ID 属性 (FilterComps=e,uid)，服务器将在目录中搜索 Email 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。 Email 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。过滤器需要非常具体，以仅仅匹配 LDAP 数据库中的某一项。

  有关 x509v3 证书属性的列表，请参阅下表：

表 6-2 x509v3 证书的属性

属性	说明
c	国家 （地区）
o	组织
cn	通用名称
l	位置
st	状态
ou	组织单位
uid	UNIX/Linux 用户 ID
Email	Email 地址

  过滤器的属性名必须是来自证书 （而不是来自 LDAP 目录）的属性名。例如，某些证书将 e 属性用于用户的 Email 地址，而 LDAP 则称该属性为 mail。

- verifycert 告诉服务器是否需要将客户机的证书与在 LDAP 目录中找到的证书进行比较。它使用两个值：on 和 off。如果 LDAP 目录中包含证书，则只能使用此特性。此功能有助于确保最终用户使用的证书有效且未被撤回。

- `CmapLdapAttr` 是 LDAP 目录中包含该用户所有证书的主题 DN 的属性名称。该特性的缺省值为 `certSubjectDN`。该属性不是标准的 LDAP 属性，因此要使用该属性，需要扩展 LDAP 模式。有关详细信息，请参阅 *Introduction to SSL*。

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

  当使用 `DNComps` 和 `FilterComps` 匹配条目遇到困难时，这种用于将证书与 LDAP 条目相匹配的方法非常有用。

- `Library` 是其值为指向共享库或 DLL 的路径名的特性。只有在使用证书 API 创建自己的特性时才需要使用此特性。有关详细信息，请参见 *NSAPI Programmer's Guide*。

- `InitFn` 是其值为自定义库中 init 函数名称的特性。只有在使用证书 API 创建自己的特性时才需要使用此特性。

有关这些特性的详细信息，请参见第 136 页上的 “映射样例”中介绍的实例。

创建自定义特性

您可以使用客户机证书 API 创建自己的特性。有关程序设计和使用客户机证书 API 的信息，请参见 *NSAPI Programmer's Guide*。

创建自定义映射后，就可以引用以下格式的映射：

```
<name>:library <path_to_shared_library>
<name>:InitFn <name_of_init_function>
```

例如：

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

映射样例

certmap.conf 文件中应至少包含一项。以下示例说明了使用 certmap.conf 文件的不同方式。

示例 1

本示例表示了只有一个 “缺省”映射的 certmap.conf 文件：

```
certmap default default
default:DNComps ou, o, c
default:FilterComps e, uid
default: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 <> 中的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 Email 地址和用户 ID 的值在 LDAP 目录中搜索匹配的项。找到匹配的项时，服务器将比较客户机发送的证书和存储在目录中的证书，以验证该证书。

示例 *2*

以下示例文件中包括两个映射：一个是缺省映射，另一个用于美国邮电业 (US Postal Service)：

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

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

如果服务器获得的证书来自美国邮电业以外的其他用户，则服务器将使用缺省映射，即从 LDAP 树的顶端启动并搜索匹配客户机 Email 和用户 ID 的条目。如果证书来自美国邮电业，服务器将从包含组织单位的 LDAP 分支启动并搜索匹配的 Email 地址。而且，请注意，如果证书来自 USPS，服务器将验证该证书，而不验证其他证书。

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

示例 3

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

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

如果客户机证书主题为：

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

服务器将首先搜索包含以下信息的项：

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

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

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

设置更强大的加密算法

“Stronger Ciphers”选项提供了用于访问的 168 位、128 位或 56 位大小的密钥还提供了无限制密钥。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，Sun ONE Web Server 将返回 “Forbidden”状态。

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

密钥大小限制的实现目前基于 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 （而不是 URI）的名称。

如果未启用 SSL 或未指定 secret-keysize 参数， PathCheck 将返回 REQ_NOACTION。如果当前会话的密钥大小小于指定的 secret-keysize，函数将返回状态为 PROTOCOL_FORBIDDEN 的 REQ_ABORTED （如果未指定 bong-file），否则函数将返回 REQ_PROCEED，并且 “path” 变量被设置为 bong-file <filename>。而且，如果不符合密钥大小限制条件，当前会话的 SSL 会话缓存项将失效，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 当 “Stronger Ciphers” 表单中添加 PathCheck fn=ssl-check 时，它将删除所有在对象中找到的 Service fn=key-toosmall 指令。

要设置更强大的加密算法，请执行以下步骤：

1. 访问 Server Manager 并从下拉列表中选择服务器实例。
2. 单击 “Virtual Server Class” 选项卡。
3. 从下拉列表中选择一个类并单击 “Manage”。

   将显示 “Class Manager”。
4. 选择 “Content Mgmt” 选项卡。
5. 选择 “Stronger Ciphers”。
6. 通过以下方式选择以进行编辑：
   - 从下拉列表中
   - 单击 “Browse”
   - 单击 “Wildcard”
7. 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
8. 输入要拒绝访问的消息所在的文件位置。
9. 单击 “OK”。
10. 单击 “Apply”。
11. 选择冷启动 / 重新启动或动态应用。

有关详细信息，请参阅 *Introduction to SSL*。

考虑其他安全问题

除了某些人会试图破解您的加密以外，还存在其他安全风险。网络面临的风险来自外部和内部的黑客，他们使用各种方法试图访问您的服务器以及服务器上的信息。

因此除了在服务器上启用加密外，还应采取额外的安全预防措施。例如，将服务器计算机放在一个安全的房间内，以及不允许不信任的个人将程序上载到您的服务器中。

以下各节介绍了可以使服务器更安全的重要方法：

- 限制物理访问
- 限制管理访问
- 选择可靠的密码
- 更改密码或 PIN
- 限制服务器上的其他应用程序
- 禁止客户机缓存 SSL 文件
- 限制端口
- 了解服务器的限制
- 进行其他更改以保护服务器

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。这样可以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 (root) 口令 （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。如果希望 Administration Server 为最终用户提供对 LDAP 服务器或本地目录信息的访问，请考虑维护两台 Administration Server 和使用群集管理。这样启用了 SSL 的 Administration Server 可用作主服务器，而另一台 Administration Server 则用于最终用户的访问。

有关群集的详细信息，请参见第 145 页上的 “关于群集”。

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。

选择可靠的密码

您可以在服务器中使用多个密码：管理密码、专用密钥密码、数据库密码等等。管理密码是所有密码中最重要的一个，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。专用密钥密码是下一个最重要的密码。如果有人获取了您的专用密钥和专用密钥密码，则可以创建虚设服务器 （伪装成您的服务器），或截取和更改服务器的通信信息。

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

创建难以破解的密码

以下这些简单的指导可帮助您创建更安全的口令。

不必将以下所有规则都用于一个密码，但使用的规则越多，密码就越难以破解：

- 密码的长度应为 6 到 14 个字符 （Mac 密码不得超过 8 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

最好定期更改您的信任数据库 / 密钥对文件口令或 PIN。如果 Administration Server 中启用了 SSL，则启动服务器时需要此密码。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。有关更改密码时的注意事项列表，请参阅第 140 页上的 “创建难以破解的密码”。

更改密码

要更改 Administration Server 或服务器实例的信任数据库 / 密钥对文件密码，请执行以下步骤：

1. 访问 Administration Server 或 Server Manager。

   对于 Server Manager，您必须先从下拉列表中选择服务器实例。

2. 选择 “Change Password”链接。

3. 从下拉列表中选择要在其中更改密码的安全令牌。

   缺省情况下，内部密钥数据库的安全令牌为 “internal”。如果安装了 PKCS#11 模块，则会看到列出的所有令牌。单击 “Change Password”链接。

4. 输入当前密码。

5. 输入新密码。

6. 再次输入新密码。

7. 单击 “OK”。

8. 对于 Server Manager，单击 “Apply”，然后单击 “Restart”使更改生效。

确保您的密钥对文件受到保护。 Administration Server 将密钥对文件存储在 *server_root*/alias 目录中。使文件和目录只能被您计算机上安装的 Sun ONE 服务器读取。

了解备份磁带上是否存储了该文件以及其他人是否能够截获该文件也很重要。如果存储了该文件，则必须像保护服务器一样尽力保护您的备份。

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。利用服务器上运行的其他程序中的漏洞可以避开服务器的安全保护。请禁用所有不必要的程序和服务。例如， UNIX `sendmail` 守护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。请不要在服务器计算机中运行 telnet 或 rlogin。并且，也不应在服务器计算机中运行 rdist （该命令可以用来分发文件，也可以用于更新服务器计算机中的文件）。

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。

同样，在服务器上安装哪些程序以及是否允许其他用户在服务器上进行安装都要格外小心。其他用户的程序可能会存在安全漏洞。最糟糕的是，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。

禁止客户机缓存 SSL 文件

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

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

限制端口

禁用计算机上未使用的所有端口。使用路由器或防火墙配置可以防止到绝对最小端口集以外的任何端口的传入连接。这意味着获取计算机上 Shell 的唯一方法就是通过物理方式使用服务器计算机，该计算机应该已放置在一个受限制的区域内。

了解服务器的限制

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

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

进行其他更改以保护服务器

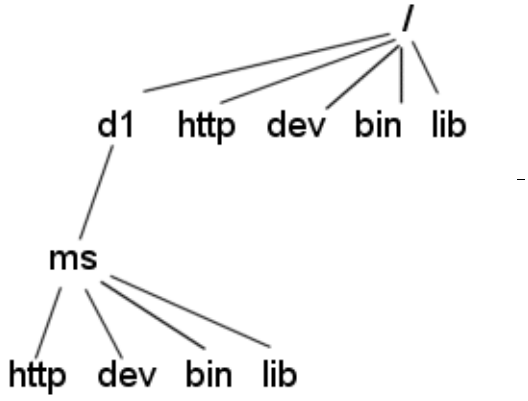
如果要同时使用受保护的和不受保护的服务器，则应该在受保护的服务器以外的其他计算机上操作不受保护的服务器。如果您的资源有限，必须在同一台计算机上运行不受保护的服务器和受保护的服务器，请执行以下操作：

- 指定正确的端口号。确保指定给受保护的服务器和不受保护的服务器的端口号不同。已注册的缺省端口号为：
  - 443（用于受保护的服务器）
  - 80（用于不受保护的服务器）
- 对于 UNIX 或 Linux，请启用文档根目录的 `chroot` 功能。不受保护的服务器应包含对使用 `chroot` 重定向的文档根目录的引用。

`chroot` 允许您创建第二个根目录，以限制服务器使用特定的目录。可以使用此功能来保护不受保护的服务器。例如，您可以设置根目录为 `/d1/ms`。那么 Web 服务器尝试访问根目录时，将会真正获得 `/d1/ms`。如果尝试访问的是 `/dev`，则会获得 `/d1/ms/dev` 等等。这允许您在 UNIX/Linux 系统上运行 Web 服务器，而不必授予它对实际根目录下所有文件的访问权限。

但是，如果使用 `chroot`，则需要在替代根目录下设置 Sun ONE Web Server 所需的完整目录结构，如下图所示：

chroot 目录结构示例



为虚拟服务器类指定 chroot

通过执行以下步骤可以为虚拟服务器类指定 `chroot` 目录：

1. 访问 Server Manager 并从下拉列表中选择服务器实例。
2. 选择 “Virtual Server Class”选项卡。
3. 单击 “Edit Classes”链接。
4. 确保将要指定 `chroot` 目录的类的 “Option”设置为 “Edit”。
5. 单击该类的 “Advanced”按钮。

   将显示 “Virtual Servers CGI Settings”。
6. 在 “Chroot”字段中输入完整的路径名。
7. 单击 “OK”。
8. 单击 “Apply”。
9. 选择 “Load Configuration Files”动态应用更改。

为虚拟服务器指定 chroot

通过执行以下步骤可以为特定虚拟服务器指定 `chroot` 目录：

1. 访问 Server Manager 并从下拉列表中选择服务器实例。
2. 选择 “Virtual Server Class”选项卡。
3. 从服务器的树视图中，单击要指定 `chroot` 目录的虚拟服务器的链接。
4. 选择 “Settings”选项卡。

   将显示 “Settings”。
5. 在 “Chroot Directory”旁边的 “Set to”字段中输入完整的路径名。
6. 单击 “OK”。
7. 单击 “Apply”。
8. 选择 “Load Configuration Files”动态应用更改。

您也可以使用 “Class Manager Virtual Servers”选项卡和 “CGI Settings”链接为虚拟服务器指定 `chroot` 目录。

有关如何为虚拟服务器指定 `chroot` 目录的详细信息，请参见 Sun ONE Web Server 6.1 *Programmer's Guide*。

第 7 章

管理服务器群集

本章介绍 Sun ONE Web 服务器群集的概念并说明如何使用服务器群集在服务器之间共享配置。

本章包括以下部分：

关于群集

群集是可以通过单个 Administration Server 进行管理的一组 Sun ONE Web Server。每个群集必须包含一个指定为 Administration Server 的服务器。如果有多个群集，则可以通过一个 “主” Administration Server 来管理所有群集。主 Administration Server 将检索所有群集的相关信息并提供一个界面，以管理安装在各个群集中的 Sun ONE Web Server。

通过将服务器组织成群集可以完成以下任务：

- 为管理所有 Sun ONE Web Server 创建一个中心位置
- 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
- 查看选定服务器的访问日志和错误日志

通过建立 Sun ONE Web Server 群集，可以指定一个主 Administration Server 来管理所有群集。

注 单独的服务器可以安装在网络中的任何一台计算机上，但所指定的 “主” Administration Server 包含所有群集服务器的相关信息，并且必须能够访问每个群集中的每个 Administration Server。

使用服务器群集的指导原则

配置群集时，包含所有群集的相关信息的主 Administration Server 将与每个群集中的 Administration Server 进行通信。为每个群集的 Administration Server 指定的管理用户名和密码必须与主 Administration Server 的管理用户名和密码相同。

在创建群集之前，必须先安装要包含在群集中的所有服务器。例如，如果要创建 3 个群集，每个群集包含 5 个 Sun ONE Web Server，则需要：

1. 在相应的计算机上安装所有服务器，它们将使用与主 Administration Server 相同的管理用户名和口令运行。
2. 将每个群集中的一个 Sun ONE Web Server 配置为 Administration Server。
3. 将一个群集的 Administration Server 配置为所有群集的主 Administration Server。可以选择其中的任一服务器作为主 Administration Server。

注意 群集只能是同类的。群集中的所有服务器必须同时为 UNIX 或 Windows。将 UNIX 服务器和 Windows 服务器组合在同一个群集中可能会导致服务器挂起或崩溃。

下表提供了配置服务器群集的一些指导：

- 在创建任何群集之前，先安装要包含在特定群集中的所有服务器。
- 确保群集中的所有服务器都是 6.1 版的 Sun ONE Web Server。
- 确保所有特定群集的 Administration Server 的用户 ID 和密码都与主 Administration Server 的用户 ID 和密码相同。可以使用分布式管理在每个 Administration Server 上设置多个管理员。
- 在网络中的任意计算机上安装服务器，只要群集中的所有计算机都为 Windows 或都为 UNIX 即可。

- 可以将任意特定群集的 Administration Server 指定为主 Administration Server。
- 确保主 Administration Server 能够访问每个特定群集的 Administration Server。主 Administration Server 将检索安装的所有 Sun ONE Web Server 的相关信息。
- 确保所有 Administration Server 都是 Sun ONE Web Server 6.0 或 6.1 版本，并且使用相同的协议 （HTTP 或 HTTPS）。只有 Sun ONE Web Server 6.0 或 6.1 版本的服务器才可以添加到群集中。
- 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。然后使用 “Modify Server”界面来修改群集中的单个服务器。

设置群集

要设置 Sun ONE Web Server 群集，请执行以下步骤：

1. 在要包含到群集中的计算机上安装 Sun ONE Web 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。可以使用缺省的用户名和密码或通过设置分布式管理来实现此目的。

2. 安装将包含主 Administration Server 的服务器，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。
4. 通过从群集表单访问其 Server Manager 表单，或将配置文件从群集中的一台服务器复制到另一台服务器来管理远程服务器。

注 更改远程服务器的配置后，重新启动远程服务器。

将服务器添加到群集中

将服务器添加到群集中时，需要指定其 Administration Server 及端口号。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。您可以在稍后删除单个服务器。

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

要将远程服务器添加到群集中，请执行以下步骤：

1. 确保主 Administration Server 已打开。
2. 访问主 Administration Server 并选择 “Cluster Mgmt”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. 在 “Admin Server Hostname”字段中，输入 `magnus.conf` 文件中显示的远程服务器的全限定域名。

   例如：`plaza.sun.com`
6. 输入远程 Administration Server 的端口号。
7. 单击 “OK”。

   现在，主 Administration Server 将尝试联系远程服务器。这需要几分钟时间。稍后，您将收到一条消息，确认该服务器已添加到群集中。
8. 单击 “OK”。

注 如果不同计算机上的两台或多台服务器使用了相同的标识符，则会显示每台计算机的服务器标识符和主机名。如果服务器标识符和主机名都相同，还会显示端口号。

注 当启用群集控制时，群集的主服务器将在 `https-`*server-instance*`/config/cluster/`*server-name*`/https-`*server-name*`/` 目录下为群集中的每台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

在从属服务器上更改管理端口信息之后，使用 “Modify Server”选项只能更新该信息。如果更改群集中某个远程 Administration Server 的端口号，还需要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，完成后再将其重新添加到群集中。

对主群集数据库所做的修改不会影响远程 Administration Server，除非通过群集控制传送它们的文件。

要修改群集中的某台服务器的信息，请执行以下步骤：

1. 转至主 Administration Server 并选择 “Cluster Mgmt”选项卡。
2. 单击 “Modify Server”链接。

   将按服务器的唯一标识符列出所有服务器。
3. 按以下方式选择一台或多台要修改的服务器：
   - 选中特定的服务器
   - 单击 “Select All”

   单击 “Reset”可以撤消全部选择。
4. 输入新的端口号。
5. 单击 “OK”。

从群集中删除服务器

要从群集中删除服务器，请执行以下步骤：

1. 转至主 Administration Server 并选择 “Cluster Mgmt”选项卡。
2. 单击 “Remove Server”链接。
3. 按以下方式选择一台或多台要删除的远程服务器：
   - 选中特定的服务器
   - 单击 “Select All”

   单击 “Reset Selection”可以撤消全部选择。
4. 单击 “OK”。

将显示一条消息，确认该服务器已从群集中删除。现在，您不能再通过群集访问已删除的服务器，而只能通过服务器自己的 Administration Server 来访问它。

控制服务器群集

Sun ONE Web Server 6.1 允许您对群集中的远程服务器进行以下控制：

- 启动和停止远程服务器。
- 查看远程服务器的访问日志和错误日志。
- 将配置文件传送到远程服务器。

注意 群集必须是同类的。群集中的所有服务器必须同时为 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。

要控制群集中的服务器，请执行以下步骤：

1. 转至主 Administration Server 的 Server Manager 并选择 “Cluster Mgmt”选项卡。
2. 单击 “Cluster Control”链接。
3. 按以下方式选择一台或多台要控制的服务器：
   - 选中特定的服务器
   - 单击 “Select All”选择群集中的所有服务器

   单击 “Reset Selection”可以撤消全部选择。
4. 从下拉菜单中选择 “Start”或 “Stop”以启动或停止远程服务器。
5. 从下拉菜单中选择 “View Access”或 “View Error”并输入要查看的行号以查看访问日志或错误日志。
6. 要传送配置文件：
   a. 从下拉菜单中选择要传送的配置文件。
   b. 从下拉菜单中选择要从中进行传送的服务器。
   c. 单击 “Transfer”。

添加变量

当需要为群集中的服务器配置不同的值时，可以使用变量。这些值可能是用于定义从属服务器使用不同端口号的宏，或者是用于定义不同 shlib 路径的插件。

添加变量只影响主群集数据库，不会影响远程 Administration Server，除非通过群集控制传送它们的文件。定义变量后， Administration Server 将不能再单独运行。

要为群集中的远程服务器添加变量，请执行以下步骤：

1. 在主 Administration Server 中，选择 “Cluster Mgmt”选项卡。
2. 单击 “Add Variables”链接。
3. 选中要为其添加变量的特定服务器。
4. 在 “Name”字段中，输入要添加的变量的类型。

   例如：“Port”。
5. 在 “Value”字段中，输入要添加的值。

   例如：如果在 “Name”字段中输入了 “Port”，则此值应当为端口号。
6. 单击 “OK”。

   将显示一条消息，确认已添加该服务器变量。
7. 单击 “OK”。

还必须将该变量添加到服务器的配置文件 （即您传送给从属服务器的文件）中。例如，如果传送变量 port，则应当在服务器配置文件 （例如 server.xml）中声明该变量，如下所示：

```
<SERVER legacyls="ls1" qosactive="no" qosmetricsinterval="30"
qosrecomputeinterval="100">

...

<LS id="ls1" ip="0.0.0.0" port="$port" security="off"
acceptorthreads="1" blocking="no">

...

</SERVER>
```

您可以为配置文件中的每台从属服务器设置具有不同值的变量。完成添加后，还可以使用 “Add Variables”中的 “Option”下拉列表来编辑和删除变量。

第 3 部分

配置、监视和性能优化

第 8 章

控制对服务器的访问

本章讨论用于控制对 Administration Server 以及您 Web 站点上的文件或目录的访问的各种方法。例如，对于 Administration Server，您可以指定谁对安装在某台计算机上的所有服务器具有完全控制权限，以及谁具有控制其中一个或多个服务器的部分控制权限。在 Administration Server 上使用访问控制之前，您必须先从 LDAP 数据库中启用分布式管理并在 LDAP 数据库中设置一个管理组。本章假定您已经配置了分布式管理并在 LDAP 数据库中定义了用户和组。

您还应当确保 Web 服务器的安全性，如第 4 章 “用于 Web 容器和 Web 应用程序的 基于 J2EE 的安全性”和第 6 章 “使用证书和密钥”中所述。

本章包括以下部分：

什么是访问控制？

访问控制允许您确定以下事项：

- 谁可以访问 Sun ONE Web Administration Server
- 他们可以访问哪些程序
- 谁可以访问您 Web 站点上的文件或目录

您可以控制对整个服务器、部分服务器或您 Web 站点上的文件或目录的访问。您可以创建一个称为访问控制条目 (ACE) 规则的分层结构来允许或拒绝访问。每个 ACE 都指定了该服务器是否应当检查分层结构中的下一个 ACE。您创建的 ACE 的集合称为访问控制列表 (ACL)。

缺省情况下，服务器具有一个 ACL 文件，其中包含多个 ACL。当为某个传入的请求确定了要使用的虚拟服务器后， Sun ONE Web Server 将检查是否为该虚拟服务器配置了任何 ACL。如果找到适用于当前请求的 ACL， Sun ONE Web Server 将评估其 ACE 以确定是否允许访问。

是否允许访问将基于以下事项：

- 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)

为用户 / 组设置访问控制

您可以仅允许特定的用户或组访问您的 Web 服务器。用户 / 组访问控制要求用户输入用户名和密码，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。如果希望在 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。详细信息，请参见 “配置目录服务”一节。目录服务用来实现访问控制的的信息可能来自以下资源之一：

- 内部平面文件类型数据库
- 外部 LDAP 数据库

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

- Default
- Basic
- SSL
- Digest
- Other

当服务器使用基于文件的内部目录服务时，对于服务器实例它支持的用户 / 组验证方法包括：

- Default
- Basic
- Digest

用户 / 组验证要求用户在访问 Administration Server 或 Web 站点上的文件和目录之前先验证其身份。对于验证，用户可以通过输入用户名和口令、使用客户机证书或摘要验证插件来验证其身份。使用客户机证书时需要加密。有关加密和使用客户机证书的信息，请参见第 4 章 “用于 Web 容器和 Web 应用程序的 基于 J2EE 的安全性”。

缺省验证

缺省验证是首选方法。“Default”设置将使用 `obj.conf` 文件中的缺省方法；如果 `obj.conf` 文件中没有设置方法，将使用 “Basic”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。

基本验证

基本验证要求用户输入用户名和密码来访问您的 Web 服务器或 Web 站点。这是缺省设置。您必须在 LDAP 数据库 （例如 Sun ONE Directory Server）中或文件中创建并存储一个由用户和组组成的列表。您使用的目录服务器不能与您的 Web 服务器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。

当用户试图访问具有用户 / 组验证的 Administration Server 或 Web 站点上的资源时， Web 浏览器将显示一个对话框，要求用户输入用户名和密码。服务器将收到加密或未加密的信息，这取决于您的服务器是否启用了加密。

注 如果使用不带 SSL 加密的基本验证，将在网络中以未加密的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。当基本验证与 SSL 加密和 / 或主机 /IP 验证结合使用时会获得最佳效果。使用摘要验证可以避免此类问题。

当用户向服务器验证其身份时，将显示以下对话框：

用户名和密码提示实例

单击 “OK” 后，用户将看到以下内容：

- “Server Administration” 页面 （如果是通过验证来访问 Sun ONE Web Administration Server）
- 所请求的文件或目录列表 （如果是登录某个 Web 站点）
- 拒绝访问的消息 （如果用户名或密码无效）

您可以自定义未经授权的用户在 “Access Denied Response” 页面中收到的拒绝访问消息。

SSL 验证

使用安全性证书，服务器可以通过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）

当您将服务器设置为使用证书信息来验证客户机时，服务器将：

- 首先检查证书是否来自一个信任的 CA。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 130 页上的 “要求客户机验证”。
- 如果证书来自一个信任的证书授权机构 (CA)，则使用 `certmap.conf` 文件将此证书映射到某个用户的条目。要了解如何设置证书映射文件，请参见第 133 页上的 “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。如果您将服务器设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。如果您将服务器的访问控制设置为使用 SSL 方法来验证用户和组，则客户机需要：

- 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

当您要求为访问控制进行客户机验证时，需要为您的 Web 服务器启用 SSL 加密算法。要学习如何启用 SSL，请参见第 6 章 “使用证书和密钥”。

要成功访问要求进行 SSL 验证的资源，客户机证书必须来自 Web 服务器信任的 CA。如果 Web 服务器的 `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，则需要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` 文件配置为仅将浏览器证书中的用户 ID 和 Email 地址与目录服务器条目进行比较。要了解有关 `certmap.conf` 文件和证书映射的更多信息，请参见第 6 章 “使用证书和密钥”。

注 只有 SSL 验证方法要求对 `certmap.conf` 文件进行修改，这是因为需要根据 LDAP 目录来检查证书。而要求对服务器的所有连接进行客户机验证则不必如此。如果您选择使用客户机证书，则应当增加 `magnus.conf` 文件中 `AcceptTimeout` 指令的值。

摘要验证

可以将 Sun ONE Web Server 6.1 配置为使用基于 LDAP 或文件的目录服务执行摘要验证。

摘要验证允许用户基于用户名和口令进行验证，但不必以明文形式发送用户名和口令。浏览器使用用户的密码和 Web 服务器提供的某些信息，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，您的目录服务器需要访问明文形式的用户密码。 Sun ONE 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，您需要启用 Sun ONE Web Server 6.1 附带的可逆密码插件和特定的摘要验证插件。要配置 Web 服务器以处理摘要验证，请设置 `dbswitch.conf` 文件中数据库定义的 `digestauth` 特性。

服务器将尝试基于指定的 ACL 方法验证 LDAP 数据库，如表 8-1 所示。如果未指定 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。这是首选方法。

表 8-1 摘要验证的不同情况

ACL 方法	验证数据库支持摘要验证	验证数据库不支持摘要验证
“default”	摘要和基本	基本
未指定		
“basic”	基本	基本
“digest”	摘要	错误

使用 `method = digest` 处理 ACL 时，服务器将尝试按以下步骤进行验证：

- 检查 Authorization 请求标头。如果未找到，将生成要求进行摘要验证的 401 响应，并且进程将停止。

- 检查 Authorization 类型。如果验证类型是摘要验证，服务器将：
  - 检查当前验证情况。如果无效，将刷新此服务器生成的当前验证并生成 401 响应，且进程将停止。如果验证已过期，将生成 401 响应 （其中 `stale=true`），且进程将停止。

    您可以通过更改 `magnus.conf` 文件中 `DigestStaleTimeout` 参数的值来配置当前验证的保留时间， `magnus.conf` 文件位于 *`server_root`*`/https-`*`server_name`*`/config/` 中。要设置该值，请将下面一行文本添加到 `magnus.conf` 文件中：

    ```
    DigestStaleTimeout seconds
    ```

    其中 *seconds* 表示当前验证被保留的秒数。指定的秒数过后，当前验证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，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，将生成 401 响应，且进程将停止。
  - 从目录服务器或文件数据库获取请求 / 摘要值，并与客户机的请求 / 摘要值进行匹配检查。如果不匹配，将生成 401 响应，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 目录服务的摘要验证，需要安装摘要验证插件。服务器端将使用此插件计算摘要值，并将它与客户端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，该库可在下面两个文件中找到：

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

要在 UNIX 上安装摘要验证插件，请执行以下步骤：

1. 确保此共享库与 Sun ONE Directory Server 位于相同的服务器计算机上。
2. 确保知道 Directory Manager 的密码。

3. 修改 `libdigest-plugin.ldif` 文件，将所有对 `/path/to` 的引用更改为安装了摘要验证插件共享库的位置。
4. 要安装插件，请输入以下命令：

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

在 *Windows* 上安装摘要验证插件

您需要将 Sun ONE Web Server 安装中的几个 `.dll` 文件复制到 Sun ONE Directory Server 服务器计算机上，以便 Sun ONE Directory Server 能够使用摘要验证插件正确启动。

要在 Windows 上安装摘要验证插件，请执行以下步骤：

1. 访问位于以下位置的 Sun ONE Web Server 安装中的共享库：

   [*server_root*]`\bin\https\bin`
2. 复制以下文件：
   - `nsldap32v50.dll`
   - `libspnr4.dll`
   - `libplds4.dll`
3. 将这些文件粘贴到以下任一位置：
   - `\Winnt\system32`
   - Sun ONE Directory Server 的安装目录：[*server_root*]`\bin\sldap\server`

将 *Sun ONE Directory Server* 设置为使用 *DES* 算法

对存储摘要密码的属性进行加密需要使用 DES 算法。

要将 Sun ONE Directory Server 设置为使用 DES 算法，请执行以下步骤：

1. 启动 Sun ONE Directory Server 控制台。
2. 打开 iDS 5.0 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. 输入 `iplanetReversiblePassword`。

8. 单击 “Save”。
9. 重新启动 Sun ONE Directory Server 实例。

注 要在 `iplanetReversiblePassword` 属性中为用户设置一个摘要验证密码，您的输入必须包含 `iplanetReversiblePasswordobject` 对象。

其他验证

您可以使用访问控制 API 创建自定义验证方法。

为主机 /IP 设置访问控制

您可以通过将 Administration Server 或 Web 站点上的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。可以使用通配符模式指定多台计算机或整个网络。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。

因为可能有多个用户使用某台特定的计算机，所以主机 /IP 验证与用户 / 组验证结合使用时会更有效。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 验证不要求在您的服务器上配置 DNS。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。您可以通过 Server Manager 中 “Preferences”选项卡的 “Performance Tuning”页面在您的服务器上启用 DNS。

启用 DNS 会降低 Sun ONE Web Server 的性能，因为服务器将不得不搜索 DNS。为减少 DNS 搜索对服务器性能的影响，可以只为访问控制和 CGI 分析 IP 地址，而不为每个请求都分析 IP 地址。要实现此目的，请将 `iponly=1` 添加到 `obj.conf` 文件的 `AddLog fn="flex-log" name="access"` 中：

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

使用访问控制文件

对 Administration Server 或您 Web 站点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 *install_dir*/httpacl 目录中， *install_dir* 是服务器的安装位置。例如，如果将服务器安装在 /usr/Sun/Servers 中，则 Administration Server 和您服务器上配置的每个服务器实例的 ACL 文件将位于 /usr/Sun/Servers/httpacl/ 中。

主 ACL 文件的名称为 generated-https-*server-id*.acl ；而临时工作文件的名称为 genwork-https-*server-id*.acl。如果使用 Sun ONE Administration Server 来配置访问，您将拥有这两个文件。但是，如果您要进行更复杂的限制，可以创建多个文件并在 server.xml 文件中引用这些文件。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。

您也可以手动创建和编辑 .acl 文件，以便使用 API 来自定义访问控制。有关使用访问控制 API 的详细信息，请参见 *Programmer's Guide*。

有关访问控制文件及其语法的更多信息，请参见附录 C “ACL 文件语法”。

配置 ACL 用户高速缓存

缺省情况下， Sun ONE Web Server 将用户和组验证结果缓存在 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 用户高速缓存的有效时间。每次引用高速缓存中的某个条目时，都将计算其寿命并检查 ACLCacheLifetime。如果该条目的寿命大于或等于 ACLCacheLifetime，则不再使用它。缺省值为 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 Sun ONE Web Server。例如，如果将该值设置为 120 秒，则在长达两分钟的时间内， Sun ONE Web 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。

您可以使用 magnus.conf 文件中的 ACLUserCacheSize 参数来配置高速缓存中所能保留的最大条目数。此参数的缺省值为 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。

您还可以使用 magnus.conf 文件中的参数 ACLGroupCacheSize 来设置每个用户条目所能高速缓存的最大组成员数。此参数的缺省值为 4。遗憾的是，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。

有关 ACL 文件指令的详细信息，请参见 Sun ONE Web Server 6.1 *NSAPI Programmer's Guide*。

访问控制的工作原理

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

例如，以下 ACL 文件包含 Administration Server (`admin-serv`) 的两个缺省条目，以及一个用于允许 “admin-reduced” 组中的用户访问 Administration Server 中的 “Preferences” 选项卡的附加条目。

```
version 3.0;
# 以下 “es-internal” 规则用于保护诸如
# 图标和图像等与 Sun ONE Web Server 相关的文件。
# 这些 “es-internal” 规则不应当被修改。
  acl "es-internal";
  allow (read, list, execute,info) user = "anyone";
  deny (write, delete) user = "anyone";
# 以下 “default” 规则适用于
# Sun ONE Web Server 的整个文档目录。在本例中，这些规则被设置为
# 允许目录服务器中的所有 (all) 用户
# 读取、执行、列出和获取信息，
# 但所有 (all) 用户都不能写入或删除任何文件。
# 访问该 Web 服务器的文档目录的所有客户机都需要
# 提供用户名和密码，因为本例
# 使用了基本 (basic) 验证
# 方法。客户机必须位于目录服务器中才能
# 访问此缺省目录，因为不在目录服务器中的任何用户 (anyone) 都
# 将被拒绝，而位于目录服务器中的所有用户 (all) 都将被
# 允许访问。
  acl "default";
  authenticate (user,group) {
     database = "default";
     method = "basic";
  };
  deny (all)
  (user = "anyone");
  allow (read,execute,list,info)
  (user = "all");
# 以下规则将拒绝不在目录服务器中的任何用户以及
# 位于目录服务器中但不在 GroupB 中的任何用户
# 访问 web 目录。
# 只有 GroupB 中的用户能够读取、执行、列出
# 以及获取信息。GroupA 不能访问
# web 目录，即使（在下面的 ACL 规则中）它们
# 能够访问 “my_stuff” 目录。此外，GroupB 的成员
# 不能写入或删除文件。
  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");

# 以下规则将拒绝不在目录服务器中的任何用户
# 以及位于目录服务器中但
# 其用户 ID 不是 SpecificMemberOfGroupB 的任何用户进行访问。此设置中的
ACL 规则
# 还要求用户连接自
# 特定的 IP 地址。规则中的 IP 地址设置
# 是可选的；添加它是为了获得额外的
# 安全性。此外，此 ACl 规则还具有一个自定义的
# 提示 “Presentation Owner”。此自定义提示出现在
# 客户机浏览器的用户名和密码
# 对话框中。

   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");

# 以下 ACL 规则将拒绝不在目录服务器中的任何用户
# 以及位于目录服务器中但不在
# GroupA 或 GroupB 中的任何用户访问 “my_stuff” 目录。
   acl "path=/export/user/990628.1/docs/my_stuff/";
   authenticate (user,group) {
      database = "default";
      method = "basic";
   };
   deny (all)
   (user = "anyone");
   allow (read,execute,list,info)
   (group = "GroupA,GroupB");
```

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

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

注	如果有多个匹配的 ACL，服务器将使用最后一个匹配的 ACL 语句。因为 `uri` ACL 是最后一个匹配语句，所以 `default` ACL 将被忽略。

设置访问控制

本节介绍如何限制对您 Web 站点上的文件或目录的访问。您可以为所有服务器设置全局访问控制规则，也可以单独为特定的服务器进行设置。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，但是只允许负责工资单的人员更新数据。

您可以通过 Administration Server 为所有服务器设置全局访问控制。下面的选择访问控制选项一节中有每个选项的详细介绍。

注	在创建全局访问控制之前，必须先配置并激活分布式管理。

设置全局访问控制

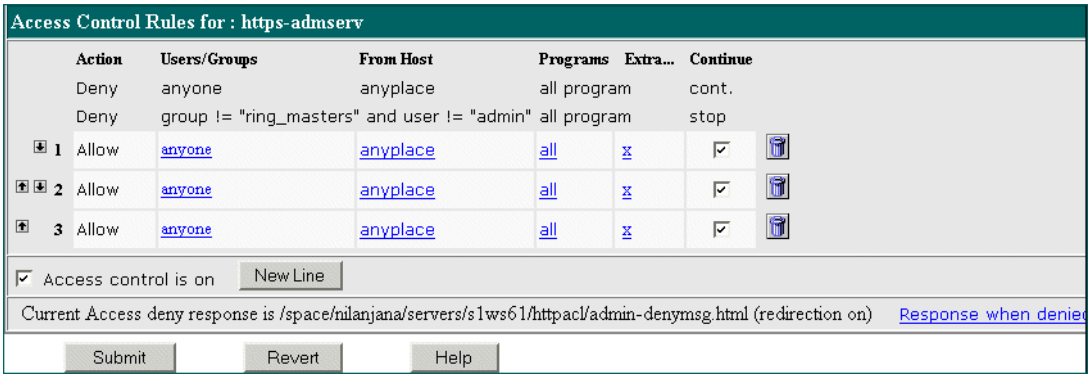
要为所有服务器创建或编辑全局访问控制，请执行以下步骤：

1. 访问 Administration Server 并选择 “Global Settings”选项卡。
2. 单击 “Restrict Access”链接。
3. 从下拉列表中选择 Administration Server (https-admserv)。

4. 单击 “Create ACL” 和 “Go” 按钮。

   将显示 uri=/https-admserv/ 的 “Access Control Rules” 页面：

   “Access Control Rules” 页面



   Administration Server 具有两行不能编辑的缺省访问控制规则。

5. 选中 “Access control is on”（如果尚未选中）。

6. 要将一个缺省 ACL 规则添加到该表的底部一行，请单击 “New Line” 按钮。

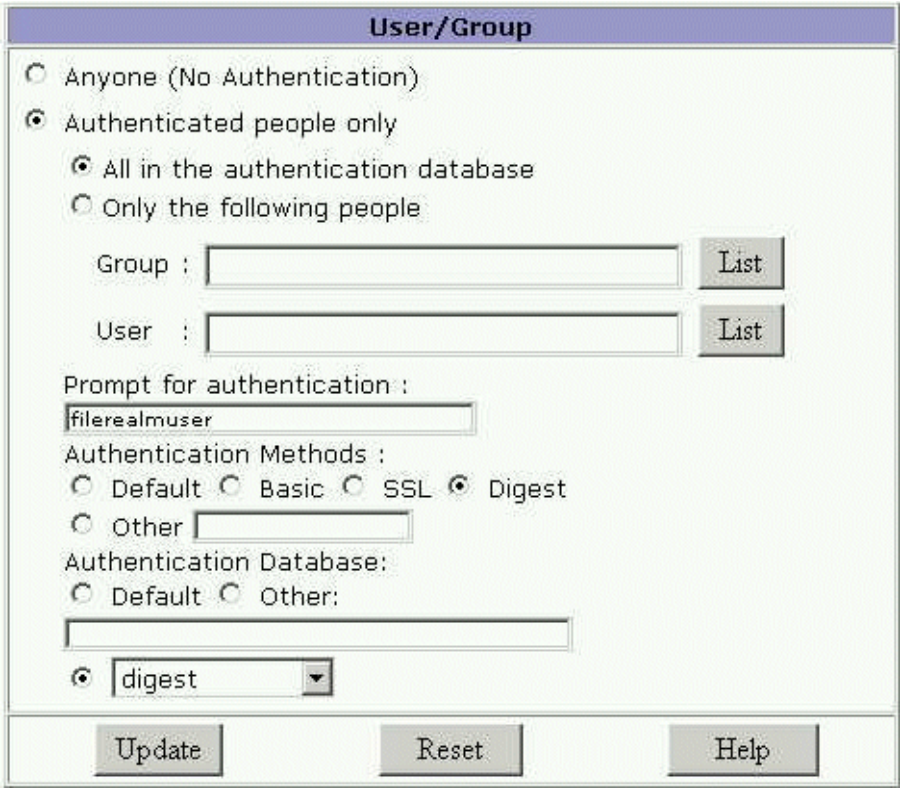
   要将某个访问控制限制与其前面的访问控制限制交换位置，请单击向上箭头。

   要将某个访问控制限制与其后面的访问控制限制交换位置，请单击向下箭头。

7. 单击“Users/Groups”列中的“anyone”。

   “User/Group”页面将显示在下面的框架中：

   “User/Group”页面



8. 选择您要允许其访问的用户和组，然后单击“Update”。

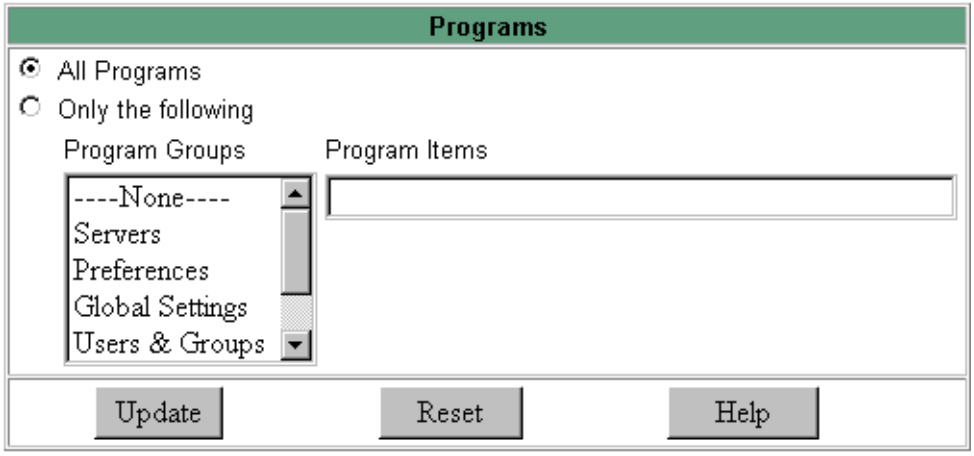
   单击“Group”和“User”的“List”将提供列表供您从中选择。

9. 单击“From Host”列中的“anyplace”。

10. 输入允许其访问的主机名和 IP 地址，然后单击“Update”。

11. 单击 “Programs”列中的 “all programs”。

“Programs”



12. 选择 “Program Groups”，或在 “Program Items”字段中输入您要允许其访问的特定文件名，然后单击 “Update”。
13. （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。
14. 选中 “Continue”列中的相应复选框 （如果尚未选定为缺省设置）。

    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。
15. （可选）单击 “Response when denied”将用户定向到其他 URL 或 URI。
16. 输入 URL 的绝对路径或相对的 URI 路径，然后单击 “Update”。
17. 单击 “Submit”，将新的访问控制规则存储在 ACL 文件中。

注 单击 “Revert”将删除刚刚创建的所有设置。

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。

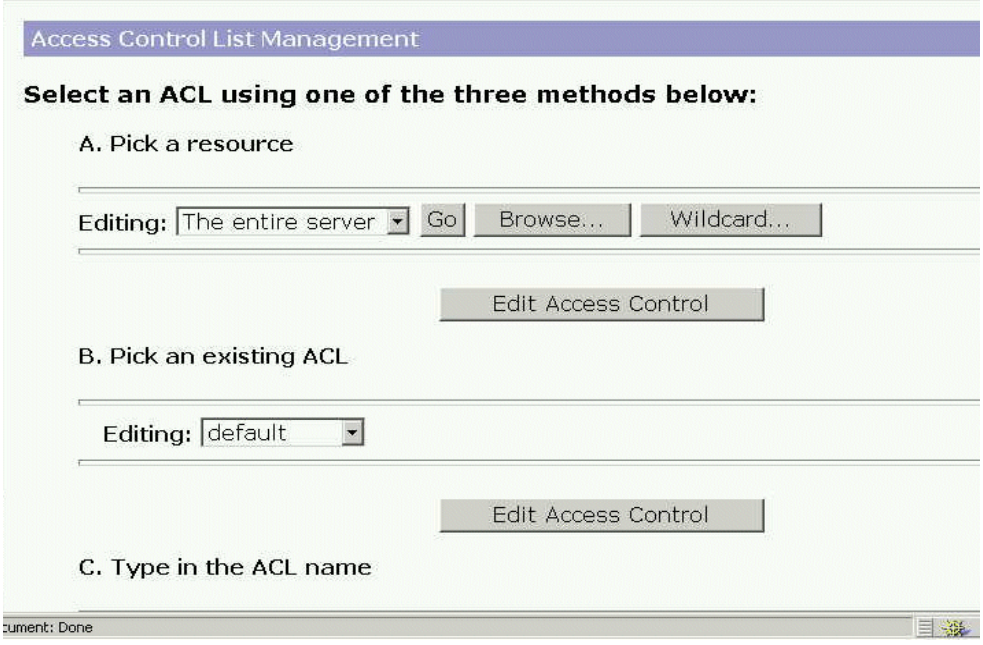
注 如果要删除，您不应删除 ACL 文件中的所有 ACL 规则。至少要保留一个 ACL 文件，并且其中至少要包含一个 ACL 规则，以便启动服务器。删除所有 ACL 规则并重新启动服务器将导致语法错误。

要为某个服务器实例创建访问控制，请执行以下步骤：

1. 访问 Server Manager 并选择要为其创建或编辑 ACL 的服务器实例。
2. 选择 Server Manager 的 “Preferences” 选项卡。
3. 单击 “Restrict Access” 链接。
4. 在 “Option” 列下，选择以下选项之一：
   - “Add”，然后输入 ACL 文件位置
   - “Edit”，然后从下拉菜单中选择 ACL 文件
   - “Delete”，然后从下拉菜单中选择 ACL 文件

   将显示 “Access Control List Management” 页面，其中提供了三个选项：

“Access Control List Management” 页面



5. 选择以下选项之一：

- “Pick a resource”，指定文件或目录的通配符模式（例如 `*.html`），选择要限制的目录或文件名，或浏览以查找某个文件或目录。
- “Pick an existing ACL”，从您已启用的所有 ACL 列表中选择。尚未启用的现有 ACL 不会显示在此列表中。
- “**Enter the ACL name**”，允许创建命名 ACL。仅当您熟悉 ACL 文件时，才能使用此选项。如果要将已命名的 ACL 应用到资源，您需要手动编辑 `obj.conf` 文件。

表 8-2 介绍了您可以使用的资源通配符。

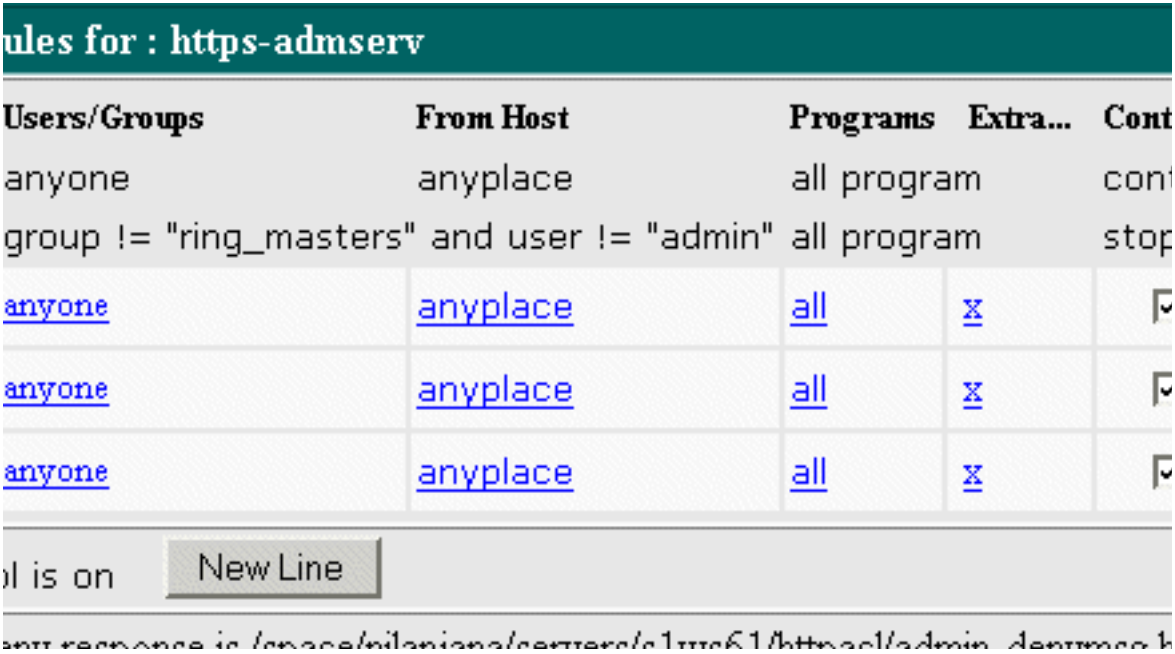
表 8-2 服务器资源通配符

资源通配符	含义
default	在安装过程中创建的一个命名 ACL，用于限制写访问，使得只有 LDAP 目录中的用户可以发布文档。
Entire Server	一组规则，用于确定对整个 Web 站点（包括已运行的任何虚拟服务器）的访问。要限制对某个虚拟服务器的访问，请指定其文档根目录的路径。
`/usr/sun/server4/docs/cgi-bin/*`	控制对 `cgi-bin` 目录中的所有文件和目录的访问。您必须指定一个绝对路径。在 Windows 上，该路径必须包括驱动器号。
`uri="/sales"`	控制对文档根目录中的 `sales` 目录的访问。要指定 URI，请创建一个命名 ACL。

6. 单击 “Edit Access Control”。

   将显示 “Access Control Rules for: （服务器实例）”。

   “Access Control Rules”页面

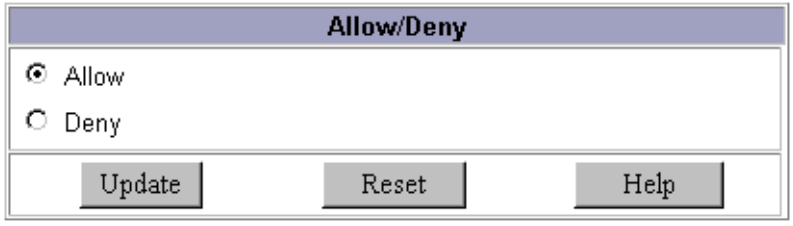


7. 选中 “Access control is on”（如果尚未选中）。

8. 要创建或编辑此服务器实例的 ACL，请单击 “Action”列中的 “Deny”。

   “Allow /Deny”页面将显示在下面的框架中：

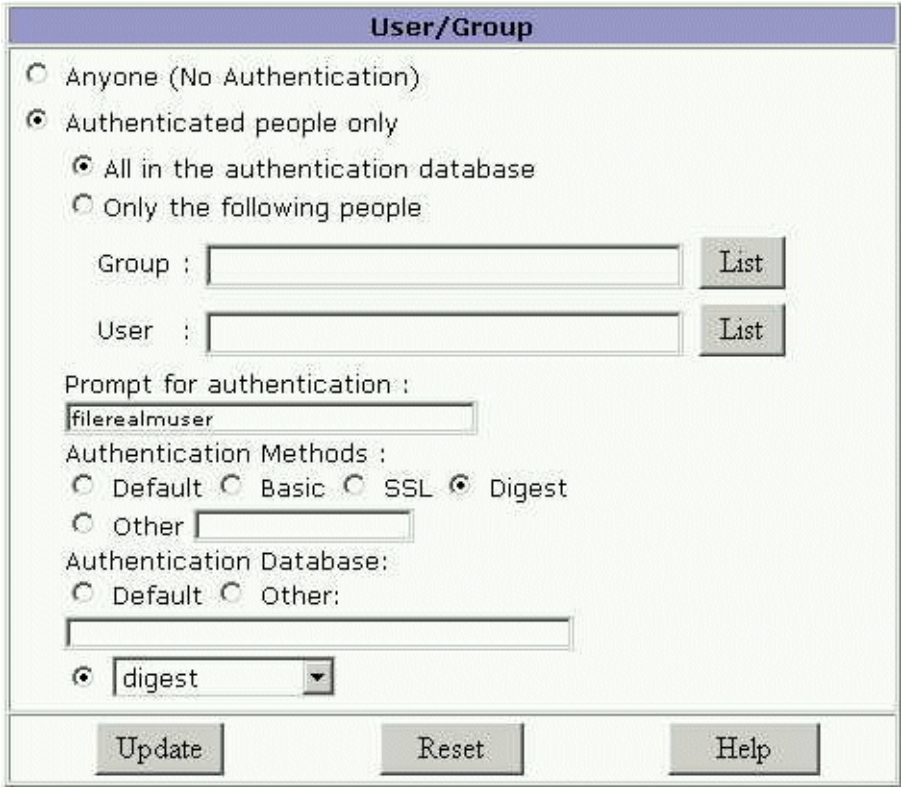
   “Allow /Deny”页面



9. 选择 “Allow”（如果尚未选定为缺省设置），然后单击 “Update”。
10. 单击 “Users/Groups”列中的 “anyone”。

    “User/Group”页面将显示在下面的框架中：

    “User/Group”页面



11. 选择您要允许其访问的用户和组，然后单击 “Update”。

    单击 “Group”和 “User”的 “List”将提供列表供您从中选择。
12. 单击 “From Host”列中的 “anyplace”。
13. 输入允许其访问的主机名和 IP 地址，然后单击 “Update”。

14. 单击 “Rights”列中的 “all”。

    “Access Rights”页面

15. 选择以下选项之一，然后单击 “Update”：
    - “All Access Rights”
    - “Only the following rights”，然后为该用户选中所有相应的权限。
16. （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。
17. 在 “Continue”列中选中一个复选标记 （如果尚未选定为缺省设置）。

    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。
18. （可选）单击 “Response when denied”将用户定向到其他 URL 或 URI。
19. 输入 URL 的绝对路径或相对的 URI 路径，然后单击 “Update”。
20. 单击 “Submit”，将新的访问控制规则存储在 ACL 文件中。

注 单击 “Revert”将删除刚刚创建的所有设置。

21. 为每个要创建访问控制的服务器实例重复执行上述所有步骤。
22. 完成后，单击 “Apply”。
23. 选择硬启动 / 重新启动或动态应用。

您也可以基于每个虚拟服务器启用 ACL 设置。要了解如何进行此操作，请参见第 199 页上的 “编辑虚拟服务器的访问控制列表”。

选择访问控制选项

以下各节介绍在设置访问控制时可以选择的各种选项。对于 Administration Server，头两行为缺省设置，且不能编辑。

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

服务器将检查整个访问控制表达式 (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。如果第一个 ACE 被设置为 “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**选中 “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，或该 ACE 匹配但未被设置为 “Continue”。最后一个匹配的 ACE 将确定是否允许访问。

指定用户和组

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

Sun ONE Web Server 将检查在 LDAP 服务器 （例如 Sun ONE 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每个用户的访问，也可以使用通配符模式允许或拒绝特定用户的访问，还可以从用户和组的列表中选择允许或拒绝访问的用户。

- “**Anyone** （**无验证**）”是缺省设置，意味着任何用户都可以访问该资源而不必输入用户名或密码。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，这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**”使您可以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**”使您可以输入要在验证对话框中显示的消息文本。您可以使用此文本来描述用户需要输入的内容。基于不同的操作系统，用户大约会看到该提示的头 40 个字符。 Netscape Navigator 和 Netscape Communicator 将高速缓存用户名和密码并将它们与提示文本相关联。当用户访问具有相同提示符的服务器的文件和目录时，不必再次输入用户名和口令。如果您要让用户对特定的文件和目录再次进行验证，只需更改该资源的 ACL 的提示。
- “**Authentication Methods**”指定服务器从客户机获取验证信息所使用的方法。Administration Server 仅提供了基本验证方法。
  - “**Default**”使用您在 `obj.conf` 文件中指定的缺省方法，如果 `obj.conf` 中没有进行设置，则使用 “Basic”。如果选中 “Default”， ACL 规则将不会在 ACL 文件中指定方法。如果选择 “Default”，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后才对用户名和密码加密。
  - “**SSL**”将使用客户机证书来验证用户。要使用此方法，必须为服务器启用 SSL。启用加密后，您可以结合使用 “Basic”和 “SSL”方法。
  - “**Digest**”将使用一种验证机制，使得浏览器能够基于用户名和密码进行验证，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 Web 服务器提供的某些信息，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。
  - “**Other**”将使用您通过访问控制 API 创建的自定义方法。
- “**Authentication Database**”使您可以选择一个数据库，服务器将使用该数据库来验证用户。此选项仅在 Server Manager 中可用。如果选择 “Default”，服务器将查找配置为缺省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，请选择 “Other”，然后从下拉列表中选择数据库。非缺省的数据库和 LDAP 目录需要已经在 *server_root*`/userdb/dbswitch.conf` 文件中指定。如果为某个自定义数据库 （例如 Oracle 或 Informix）使用访问控制 API，请选择 “Other”并输入数据库的名称。

指定 “From Host”

您可以基于请求来自的计算机限制对 Administration Server 或 Web 站点的访问。

- “**Anyplace**”允许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”字段中输入通配符模式或逗号分隔的列表。按主机名进行限制比按 IP 地址进行限制更灵活：如果用户的 IP 地址更改了，您不需要更新此列表。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，要允许或拒绝访问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，如 `*.sun.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， `*` 必须替换名称中的整个部分。也就是说， `*.sun.com` 可以接受，但 `*users.sun.com` 不能接受。当 `*` 出现在主机名中时，它必须是最左侧的字符。例如， `*.sun.com` 可以接受，但 `users.*.com` 不能接受。

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

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 并确定他们是否能够配置该服务器。例如，您可以允许某些管理员配置 Administration Server 的 “Users & Groups”部分，而不允许他们访问 “Global Settings”部分。

您可以配置不同的用户访问不同的功能域。为某个用户设置了对若干选定功能域的访问权限后，当该用户登录时，只有您授权该用户访问的那些功能域的 Administration Server 页面才可见。

- “**All Programs**”允许或拒绝访问所有程序。缺省情况下，管理员可以访问某个服务器的所有程序。

- “**Only the following Program Groups**”允许您指定用户可以访问哪些程序。请从下拉列表中选择这些程序。在按住 Control 键的同时单击程序组可以选择多个程序组。您可以限制对以下程序组的访问：
  - None （缺省）
  - Servers
  - Preferences
  - Global Settings
  - Users & Groups
  - Security
  - Cluster Mgmt

  列出的 “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 来确定他们能查看哪些页面。
- “**Program Items**”使您可以在 “Program Items”字段中输入页面名称，以控制对程序中特定页面的访问。

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 Web 站点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。

- “**All Access Rights**”是缺省设置，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，其中包括 HTTP 方法 GET、 HEAD、 POST 和 INDEX
  - “**Write**”允许用户更改或删除文件，其中包括 HTTP 方法 PUT、 DELETE、 MKDIR、 RMDIR 和 MOVE。要删除文件，用户必须同时具有写权限和删除权限
  - “**Execute**”允许用户执行服务器端应用程序，例如 CGI 程序、 Java 小应用程序和代理程序
  - “**Delete**”允许具有写权限的用户删除文件或目录

- “**List**”允许用户访问不包含 `index.html` 文件的目录中的文件列表。
- “**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及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上午 8:00 到下午 5:00 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，请参见附录 C “ACL 文件语法”和第 439 页上的 “在 obj.conf 中引用 ACL 文件”。

禁用访问控制

如果取消选中标记为 “Access control is on”的选项，您将收到一个提示，询问是否要删除 ACL 中的记录。单击 “OK”后，服务器将从 ACL 文件中删除该资源的 ACL 条目。

如果要取消激活 ACL，可以注释掉文件 `generated-https-server-id.acl` 中的 ACL 行，即在每行的开头放置一个 # 号。

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（缺省情况下为禁用）。例如，您可以通过 Administration Server 页面拒绝对 Server Manager 的任何访问。对于缺省情况下启用了分布式管理且禁用了访问控制的其他服务器，管理员仍可以访问和配置这些服务器，但不能配置 Administration Server。

注 此访问控制将附加在位于为分布式管理设置的管理员组中的用户上。Administration Server 首先检查用户 （非超级用户）是否位于管理员组中，然后评估访问控制规则。

访问被拒绝时的响应

访问被拒绝时， Sun ONE Web Server 提供了以下缺省消息：“FORBIDDEN.Your client is not allowed access to the restricted object。”您可以选择当访问被拒绝时的其他响应。也可以为每个访问控制对象创建不同的消息。

要为特定 ACL 更改发送的消息，请执行以下步骤：

1. 单击 ACL 页面中的 “Response when denied”链接。
2. 在下面的框架中选中 “Respond with the following file”。
3. 输入 URL 的绝对路径或相对的 URI 路径，然后单击 “Update”。

   确保用户对他们被重定向到的 URL 或 URI 具有访问权限。
4. 单击 “Update”。
5. 在上面的框架中单击 “Submit”，提交该访问控制规则。

限制对服务器中的区域的访问

本节介绍一些常用的对 Web 服务器及其内容的访问限制。每个过程的步骤都详述了需要执行的特定操作；但是，您仍需要完成第 170 页上的 “设置服务器实例的访问控制”中介绍的所有步骤。

本节介绍了以下过程：

- 限制对整个服务器的访问
- 限制对目录 （路径）的访问
- 限制对 URI （路径）的访问
- 限制对文件类型的访问基于一天中的某个时间限制访问
- 基于安全性限制访问

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。

使用所介绍的为服务器实例设置访问控制的步骤，您需要执行以下步骤：

1. 使用 Server Manager 选择该服务器实例。
2. 选择 “Preferences”选项卡。
3. 单击 “Restrict Access”链接。
4. 选择要编辑的 ACL 文件。
5. 拾取整个服务器资源，然后单击 “Edit Access Control”。
6. 添加一个新规则以拒绝所有用户的访问。
7. 添加另一个新规则以允许特定组的访问。
8. 输入允许访问的计算机的主机名的通配符模式。

   例如， `*.employee.sun.com`
9. 取消选中” Continue”复选框。
10. 单击 “Submit”和 “Apply”以提交和应用所做的更改。

限制对目录 （路径）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。

要限制对服务器中目录的访问 （使用所介绍的为服务器实例设置访问控制的步骤），请执行以下步骤：

1. 使用 Server Manager 选择该服务器实例。
2. 选择 “Preferences”选项卡。
3. 单击 “Restrict Access”链接。
4. 选择要编辑的 ACL 文件。
5. 浏览 “Pick a sesource”部分并选择您要限制的目录。

   将显示服务器文档根目录中的目录。选定目录后，“Editing”下拉列表将显示该目录的绝对路径。

注 如果要查看服务器根目录中的所有文件，请单击 “Options”，然后选中 “List files as well as directories”。

6. 单击 “Edit Access Control”。
7. 创建一个新规则并保留缺省设置，即拒绝任何位置的任何用户的访问。
8. 创建另一个新规则，允许某个特定组中的用户仅具有读权限和执行权限。
9. 创建第三行规则，允许某个特定用户具有所有权限。
10. 取消选中第二行和第三行的” Continue”复选框，然后单击 “Update”。
11. 单击 “Submit”和 “Apply”以提交和应用所做的更改。

该文件或目录的绝对路径将创建在文档根目录中。 ACL 文件中的条目将如下所示：

```
acl "path=d:\sun\suitespot\docroot1\sales/";
```

限制对 URI （路径）的访问

您可以使用 URI 控制对 Web 服务器上单个用户内容的访问。 URI 是相对于服务器文档根目录的路径和文件。如果您需要频繁地重命名或移动服务器的所有或部分内容 （例如，为了调整磁盘空间），则使用 URI 可以方便地管理服务器的内容。如果您还有其他文档根目录，这也是一种很好的处理访问控制的方法。

要限制对 URI 的访问 （使用所介绍的为服务器实例设置访问控制的步骤），请执行以下步骤：

1. 使用 Server Manager 选择该服务器实例。
2. 选择 “Preferences”选项卡。
3. 单击 “Restrict Access”链接。
4. 在 “ACL name”部分的 “Type”中输入要限制的 URI。

   例如：`uri=/my_directory`。
5. 单击 “Edit Access Control”。
6. 创建一个新规则，为所有用户授予读权限。
7. 创建另一个新规则，为目录的所有者授予访问权限。
8. 取消选中第一个和第二个规则的” Continue”复选框。
9. 单击 “Submit”和 “Apply”以提交和应用所做的更改。

将相对于文档根目录创建该 URI 的路径。 ACL 文件中的条目将如下所示：
`acl "uri=/my_directory";`

限制对文件类型的访问

您可以限制对服务器或 Web 站点上的文件类型的访问。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。

要限制对文件类型的访问 （使用所介绍的为服务器实例设置访问控制的步骤），请执行以下步骤：

1. 使用 Server Manager 选择该服务器实例。
2. 选择 “Preferences”选项卡。
3. 单击 “Restrict Access”链接。
4. 单击 “Pick a resource”部分中的 “Wildcard”并输入一个通配符模式。

   例如， `*.cgi`。
5. 单击 “Edit Access Control”。
6. 创建一个新规则，为所有用户授予读权限。
7. 创建另一个规则，仅为某个特定组授予写权限和删除权限。
8. 单击 “Submit”和 “Apply”以提交和应用所做的更改。

对于文件类型限制，您应当保持选中两个 “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。

`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。使用此方式可以禁止用户在工作时间内发布文档，这时其他用户可能正在访问文件。

要基于一天中的某个时间对访问进行限制 （使用所介绍的为服务器实例设置访问控制的步骤），请执行以下步骤：

1. 使用 Server Manager 选择该服务器实例。

2. 选择 “Preferences”选项卡。
3. 单击 “Restrict Access”链接。
4. 从 “Pick a resource”中的下拉列表中选择整个服务器，然后单击 “Edit Access Control”。
5. 创建一个新规则，为所有用户授予读权限和执行权限。

   这意味着如果某个用户要添加、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。
6. 创建另一个新规则，拒绝所有用户的写权限和删除权限。
7. 单击 X 链接，创建一个自定义表达式。
8. 输入允许进行访问的一周中的哪些天以及一天中的哪些时间。

   示例：

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

   创建自定义表达式时，“Users/Groups”和 “From Host”字段中将显示消息 “Unrecognized expressions”。
9. 单击 “Submit”和 “Apply”以提交和应用所做的更改。

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

从 Sun ONE Web Server 6.1 开始，您可以为同一个服务器实例配置 SSL 监听套接字和非 SSL 监听套接字。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。

要基于安全性对访问进行限制（使用所介绍的为服务器实例设置访问控制的步骤），请执行以下步骤：

1. 使用 Server Manager 选择该服务器实例。
2. 选择 “Preferences”选项卡。
3. 单击 “Restrict Access”链接。

4. 从 “Pick a resource”中的下拉列表中选择整个服务器，然后单击 “Edit Access Control”。
5. 创建一个新规则，为所有用户授予读权限和执行权限。

   这意味着如果某个用户要添加、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。
6. 创建另一个新规则，拒绝所有用户的写权限和删除权限。
7. 单击 X 链接，创建一个自定义表达式。
8. 输入 `ssl="on"`。

   示例：

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

9. 单击 “Submit”和 “Apply”以提交和应用所做的更改。

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。

在分布式管理中保证访问控制的安全性

本节列出了在启用分布式管理后，为在 Sun ONE Web Server 6.1 中保证访问控制的安全性所需执行的其他任务。

- 保护对资源的访问
- 保护对服务器实例的访问
- 启用基于 IP 的访问控制

保护对资源的访问

PathCheck 指令在 `generated.https-`*`server-id`*`.acl` 文件中的 `https-`*`server-id`* 对象标记中的出现顺序可能会授予并不希望的资源访问权限。要防止发生这种情况，请编辑 `<`*`server-root`*`>/generated.https-`*`server-id`*`.acl` 文件，指定要求进行访问控制的程序组列表 （由逗号分隔），如下所示：

在以下行之下：

```
allow (all)
```

`user=<`*`username`*`>` and `program=<`*`program group, program group...`*`>;`

添加以下行：

```
deny absolute (all)
user=<username> and program!=<program group, program group...>;
```

保护对服务器实例的访问

为配置 Sun ONE Web Server 6.1 以控制对服务器实例的访问，请编辑 <*server-root*>/httpacl/*.https-admserv.acl 文件并指定要授予其访问控制权限的用户。示例：

```
acl "https-<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*.https-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)。

1. 编辑 <*server-root*>/httpacl/gen*.https-admserv.acl 文件，除了 user 和 group 外，再将 ip 添加到验证列表中，如下所示：

   ```
   acl "https-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";
```

示例：

```
acl "https-admserv";

authenticate (user,group,ip) {

database = "default";

method = "basic";

};

deny absolute (all) ip !="205.217.243.119";
```

使用动态访问控制文件

服务器内容很少是由一个用户完全管理的。您可能需要允许终端用户访问配置选项的某个子集，以使他们能够进行所需的配置，而不必授权他们访问 Sun ONE Web Server。配置选项的子集存储在动态配置文件中。

本部分包括以下主题：

使用 .htaccess 文件

Sun ONE Web Server 支持 `.htaccess` 动态配置文件。您可以通过用户界面或手动更改配置文件来启用 `.htaccess` 文件。支持 `.htaccess` 的文件位于 *server_root*`/plugins/htaccess` 目录中。这些文件包括一个插件，使您可以使用 `.htaccess` 文件以及一个用于将 `.nsconfig` 文件转换为 `.htaccess` 文件的脚本。

您可以将 `.htaccess` 文件与服务器的标准访问控制结合起来使用。不管 `PathCheck` 指令的顺序如何，标准访问控制始终在 `.htaccess` 访问控制之前应用。如果用户 / 组验证是 “Basic”，请不要同时使用标准访问控制和 `.htaccess` 访问控制进行用户验证。您可以通过标准服务器访问控制使用 SSL 客户机验证，也可以通过 `.htaccess` 文件进行 HTTP “Basic”验证。

本部分包括以下主题：

从用户界面启用 .htaccess 文件

要将 Sun ONE Web Server 配置为使用 `.htaccess` 文件，请执行以下步骤：

1. 访问 Server Manager 并选择要为其启用 `.htaccess` 的服务器实例。
2. 单击屏幕顶部的 “Class Manager”链接。
3. 选择 “Content Mgmt”选项卡。
4. 单击 “`.htaccess` Configuration”链接。
5. 按以下方式选择要编辑的服务器：
   - 选择整个服务器或从下拉列表中选择特定的服务器
   - 单击 “Browse”选择要编辑的目录和文件
   - 单击 “Wildcard”选择要编辑的通配符模式
6. 选择 “Yes”激活 .htaccess 文件。
7. 输入要添加 `.htaccess` 配置的文件名。
8. 单击 “OK”。
9. 完成后，单击 “Apply”。
10. 选择硬启动 / 重新启动或动态应用。

从 magnus.conf 启用 .htaccess 文件

要以手动方式允许服务器使用 `.htaccess` 文件，需要先修改服务器的 `magnus.conf` 文件，以便装入、初始化和激活该插件。

1. 打开 *`server_root`*`/https-`*`server_name`*`/config` 中的 `magnus.conf` 文件。

2. 在其他 Init 指令之后，添加以下行：

   - 对于 UNIX/Linux：

     ```
     Init fn="load-modules" funcs="htaccess-init,htaccess-find"
     shlib="server_root/plugins/htaccess/htaccess.so"
     NativeThread="no"
     Init fn="htaccess-init"
     ```

   - 对于 Windows：

     ```
     Init fn="load-modules"
     funcs="htaccess-init,htaccess-find,htaccess-register"
     shlib="server_root/plugins/htaccess/htaccess.dll"
     NativeThread="no"
     Init fn="htaccess-init"
     ```

   - 对于 HP：

     ```
     Initfn="load-modules"
     funcs="htaccess-init,htaccess-find,htaccess-register"
     shlib="<server_root>/plugins/htaccess/htaccess.sl"
     NativeThread="no"

     Init fn="htaccess-init"
     ```

3. （可选）使最后一行为：

   ```
   Init fn="htaccess-init"[groups-with-users=yes]
   ```

4. 单击“File”—“Save”。

5. 打开 obj.conf 文件。

6. 将 PathCheck 指令添加为对象中的最后一个指令。

   a. 要为某个虚拟服务器管理的所有目录激活 .htaccess 文件处理，请将 PathCheck 指令添加到 object.conf 文件中的缺省对象中：

      ```
      <Object name="default">

      ...

      PathCheck fn="htaccess-find"

      </Object>
      ```

      .htaccess 处理应当是该对象中的最后一个 PathCheck 指令。

   b. 要为特定服务器目录激活 .htaccess 文件处理，请将 PathCheck 指令放在 magnus.conf 文件中的相应定义中。

7. 要将 .htaccess 文件命名为其他名称，您必须使用以下格式在 PathCheck 指令中指定该文件名：

```
PathCheck fn="htaccess-find" filename="filename"
```

注 下次使用 Administration Server 时，系统将警告您已经进行了手动编辑。单击 “Apply” 接受所做的更改。

对服务器的后续访问将使用指定目录中的 .htaccess 访问控制。例如，要限制对 .htaccess 文件的写访问，可以为这些文件创建一个配置式样，然后对该配置式样应用访问控制。有关详细信息，请参见第 17 章 “应用配置式样”。

将现有 .nsconfig 文件转换为 .htaccess 文件

Sun ONE Web Server 6.1 具有一个 htconvert 插件，可用于将现有的 .nsconfig 文件转换为 .htaccess 文件。系统已不再支持 .nsconfig 文件。如果您以前使用的是 .nsconfig 文件，应当将这些文件转换为 .htaccess 文件。

激活后， htconvert 将在给定的 server.xml 文件中搜索 pfx2dir 和 document-root 指令。每个找到的 .nsconfig 文件都将被转换为 .htaccess 文件。可以转换多个 obj.conf 文件，这取决于配置。

注 如果存在现有的 .htaccess 文件， htconvert 将生成一个 .htaccess.new 文件并给出警告。如果 .htaccess 和 .htaccess.new 已存在，该新文件将命名为 .htaccess.new.new。.new 会被重复附加。

htconvert 插件当前仅支持 RestrictAccess 和 RequireAuth 指令以及 <Files> 包装。如果显示的是 <Files> 而不是 <Files*>，脚本将给出警告，并且表现出好像目录中的所有文件都要进行访问控制。

要转换文件，请在命令提示符下输入您系统上的 Perl 的路径、插件脚本的路径以及 server.xml 文件的路径。例如：

```
server_root\install\perl server_root/plugins/htaccess/htconvert
server_root/https-server_name/config/server.xml
```

所有 .nsconfig 文件都将转换为 .htaccess 文件，但是不会被删除。

groups-with-users 选项使您可以方便地处理组中的大量用户。如果组中有许多用户，请执行以下步骤：

1. 修订用户文件的格式，列出某个用户所属的所有组：

   ```
   username:password:group1,group2,group3,...groupn
   ```

2. 修订 AuthGroupFile 指令，使其指向与 AuthUserFile 相同的文件。

或者，您也可以：

1. 完全删除 AuthGroupFile 指令。
2. 将以下内容添加到 magnus.conf 文件的 Init fn=htaccess-init 行：

   ```
   groups-with-users="yes"
   ```

使用 htaccess-register

htaccess-register 是一个新函数，使您可以创建自己的验证方法。像 Apache 一样，您可以创建外部验证模块并通过 htaccess-register 将其插入 .htaccess 模块。 *server_root*/plugins/nsapi/htaccess 中提供了两个样例模块。

您可以使用外部模块创建一个或多个新的指令。例如，可以指定用于验证的用户数据库。这些指令可能不会显示在 <Limit> 或 <LimitExcept> 标记中。

.htaccess 文件的实例

下面显示了一个 .htaccess 文件实例：

```
<Limit GET POST>
order deny,allow
deny from all
allow from all
</Limit>
<Limit PUT DELETE>
order deny,allow
deny from all
</Limit>
AuthName mxyzptlk.kawaii.com
AuthUserFile /server_root/mxyz-docs/service.pwd
AuthGroupFile /server_root/mxyz-docs/service.grp
```

支持的 .htaccess 指令

本版本支持以下 `.htaccess` 指令：

allow

语法

allow from host，其中：

- host 为 all，允许从所有客户机主机进行访问
- host 为完整的 DNS 主机名或 DNS 主机名的最后部分
- host 为完整的或部分 IP 地址

该指令不必包含在 `<Limit>` 或 `<LimitExcept>` 范围内，但通常会包含在内。

作用

允许访问指定的主机。通常显示在 `<Limit>` 范围内。

deny

语法

deny from host，其中：

- host 为 all，拒绝来自任何客户机主机的访问
- host 为完整的 DNS 主机名或 DNS 主机名的最后部分
- host 为完整的或部分 IP 地址

该指令不必包含在 `<Limit>` 或 `<LimitExcept>` 范围内，但通常会包含在内。

作用

拒绝访问指定的主机。通常显示在 `<Limit>` 范围内。

AuthGroupFile

语法

`AuthGroupFile` filename，其中 filename 是包含组定义的文件的名称，组定义的格式为：groupname:user user。

该指令不能显示在 `<Limit>` 或 `<LimitExcept>` 范围内。

作用
指定将该命名组文件应用于 require group 指令中引用的所有组定义。请注意，如果 `AuthGroupFile` 指令中指定的文件名与在 `AuthUserFile` 指令中指定的文件名相同，该文件将被认为按以下格式包含用户和组：

```
username:DES-encrypted-password:comma-separated-list-of-groups
```

AuthUserFile

语法
`AuthUserFile` filename，其中：

- filename 是包含用户定义的文件的名称，用户定义的格式为：`username:password`
- username 是用户登录名， password 是 DES 加密的密码。

该指令不能显示在 `<Limit>` 或 `<LimitExcept>` 范围内。

作用
指定将该命名用户文件应用于 require user 或 require valid-user 指令中引用的所有用户名。

请注意，在 `obj.conf` 文件中的 `Init fn=htaccess-init` 指令中使用 `groups-with-users=yes`，或指定具有相同文件名的 `AuthGroupFile` 指令，将导致该文件被认为使用以下格式：

```
username:DES-encrypted-password:comma-separated-list-of-groups
```

AuthName

语法
`AuthName` authentication realm，其中 authentication realm 是一个字符串，用来标识与任何用户验证请求相关联的某个授权领域。

该指令不能显示在 `<Limit>` 或 `<LimitExcept>` 范围内。

作用
authentication realm 字符串通常显示在客户端的用户名和密码提示中。它可能影响客户端的用户名和密码的高速缓存。

AuthType

语法
`AuthType` Basic。该指令不能显示在 `<Limit>` 或 `<LimitExcept>` 范围内。

作用
指定用户验证方法为 HTTP 基本验证，这是当前支持的唯一方法。

<Limit>

语法

```
<Limit method method ...>

allow, deny, order, or require directives

</Limit>
```

其中 method 是 HTTP 方法，例如 GET、 POST 或 PUT。此处可以使用 Web 服务器能够理解的任何方法。

作用
将包含的指令仅应用于使用指定的 HTTP 方法的请求。

<LimitExcept>

语法

```
<LimitExcept method method ...>

allow, deny, order, or require directives

</LimitExcept>
```

其中 method 是 HTTP 方法，例如 GET、 POST 或 PUT。此处可以使用 Web 服务器能够理解的任何方法。

作用
将包含的指令仅应用于指定的 HTTP 方法以外的请求类型。

order

语法

Order ordering，其中 ordering 是以下顺序之一：

- allow, deny
- deny, allow
- mutual-failure

该指令不必包含在 `<Limit>` 或 `<LimitExcept>` 范围内，但通常会包含在内。

作用

- “allows, denies”将先评估 allow 指令，然后评估 deny 指令
- “denies, allows”将先评估 deny 指令，然后评估 allow 指令
- “mutual-failure”将拒绝 allow 和 deny 指令中列出的主机的访问，而不管它们的顺序如何。

require

语法

- require group groupname groupname
- require user username username
- require valid-user

该指令不必包含在 `<Limit>` 或 `<LimitExcept>` 范围内，但通常会包含在内。

作用

- “require group”要求通过验证的用户必须是某个指定组的成员。
- “require user”要求通过验证的用户必须是某个指定的用户。
- “require valid-user”要求用户必须是通过验证的用户。

.htaccess 的安全性考虑

缺省情况下，服务器对 HTTP PUT 的支持被禁用。您可以使用 Class Manager 中“Content Mgmt”的 “Remote File Manipulation”页面来激活 HTTP PUT。允许对包含 .htaccess 文件的目录进行 PUT 访问时要十分小心，因为这种访问允许替换这些文件。通过限制访问可以禁止对目录中的所有文件进行 PUT 访问。请参见“第 182 页上的 “限制对目录 （路径）的访问””。

控制虚拟服务器的访问

Sun ONE Web Server 6.1 中的访问控制信息可以来自于每台虚拟服务器的 ACL 文件和文档目录中的 .htaccess 文件。自 iPlanet Web Server 4.x 以来， .htaccess 系统并没有发生改变。

您的 server.xml 文件可以包含一个或多个 ACLFILE 标记，这些标记定义了一个与特定的 Sun ONE Web Server 6.x 标准 ACL 文件相关联的 ID。例如：

```
<ACLFILE id="standard" file="standard.acl">
```

要使虚拟服务器可以使用访问控制，您必须在其 “aclids”特性中创建对一个或多个 ACL 文件 ID 的引用。示例：

```
<VS aclids="standard">
```

此配置允许多个虚拟服务器共享相同的 ACL 文件。如果要求对虚拟服务器进行用户 / 组验证，您必须将一个或多个 USERDB 标记添加到虚拟服务器的定义中。这些 USERDB 标记用于在您的 ACL 文件中的数据库名称与在 dbswitch.conf 文件中找到的实际数据库之间创建一个连接。

下面的实例将不具有 “database”属性的 ACL 映射到 dbswitch.conf 中的 “default”数据库：

```
<VS>
   <USERDB id="default” database="default"/>
</VS>
```

从虚拟服务器访问数据库

您可以在 dbswitch.conf 文件中全局定义用户验证数据库。此文件仅在服务器启动时被读取。

dbswitch.conf 文件中 LDAP URL 的 baseDN 定义了对数据库的所有访问的全局根目录。这保持了向后兼容性。对于大多数新安装， baseDN 将是空的。

dcsuffix 是 dbswitch.conf 中 LDAP 数据库的新属性，它根据 Sun ONE LDAP 模式定义了 DC 树的根。它是相对于 LDAP URL 中的 baseDN 定义的。当显示 dcsuffix 属性时， LDAP 数据库将与 Sun ONE LDAP 模式兼容，同时某些操作的行为将发生变化。有关 Sun ONE LDAP 模式的详细信息及实例，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration Reference* 第 2 章中的 "The Sun ONE LDAP Schema"。

对于每个虚拟服务器，您可以定义一个或多个 USERDB 块以指向其中一个目录，还可以定义其他信息。在 ACL 的数据库参数中可以引用 USERDB 块 ID。如果某个虚拟服务器没有 USERDB 块，则基于用户或组的 ACL 将失败。

USERDB 标记在 ACL 的数据库属性和 dbswitch.conf 之间定义了一个额外的间接层。此间接层为服务器管理员增添了必要的保护，使他们可以完全控制虚拟服务器管理员能够访问哪些数据库。

有关 USERDB 的详细信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration Reference* 第 2 章中的 "User Database Selection"。

在用户界面中指定 LDAP 数据库

您在 dbswitch.conf 中定义了一个或多个用户验证数据库后，可以使用 Class Manager 来配置每个虚拟服务器要用来进行验证的数据库。您也可以使用 Class Manager 为要验证的虚拟服务器添加 dbswitch.conf 中新创建的数据库定义。

要指定虚拟服务器要使用的 LDAP 数据库，请执行以下步骤：

1. 访问 Server Manager 并选择 “Virtual Server Class”选项卡。
2. 单击 “Virtual Server Class”链接，从中可以指定服务器树视图下列出的 LDAP 数据库。
3. 选择 “Virtual Servers”选项卡 （如果尚未显示）。
4. 单击 “ACL Settings”链接。

   将显示 “ACL Settings for Virtual Servers”页面。
5. 从 “Option”列中的下拉列表中选择 “Edit”（如果尚未显示）。

6. 从您正在编辑的虚拟服务器的 “Database”列中的下拉列表中选择数据库配置。
7. 单击 “OK”。
8. 关闭 “Edit ACL Files”窗口。
9. 单击 “Apply”。
10. 选择动态应用。

编辑虚拟服务器的访问控制列表

虚拟服务器的 ACL 是为该虚拟服务器所在的服务器实例创建的，虚拟服务器 ACL 的设置将缺省采用为该服务器实例创建的设置。不过，您可以通过 Class Manager 来编辑每个虚拟服务器的访问控制。您还可以使用此方法为虚拟服务器添加新创建的 ACL 文件。

要编辑虚拟服务器的 ACL 设置，请执行以下步骤：

1. 访问 Server Manager 并选择 “Virtual Server Class”选项卡。
2. 单击 “Virtual Server Class”链接，从中可以指定服务器树视图下列出的 LDAP 数据库。
3. 选择 “Virtual Servers”选项卡 （如果尚未显示）。
4. 单击 “ACL Settings”链接。
5. 从要为其进行更改的每个虚拟服务器的 “Option”字段中的下拉列表中选择 “Edit”或 “Delete”。
6. 单击 “ACL File”字段中的 “Edit”链接以显示可用的 ACL 文件。
7. 选择要为该虚拟服务器添加或删除的一个或多个 ACL 文件。

   一个虚拟服务器可以具有多个 ACL 文件，因为它们可能具有多个文档根目录。
8. 从下拉列表中选择要与 ACL 列表相关联的数据库。
9. （可选）输入 BaseDN。
10. 完成更改后，单击 “OK”。
11. 单击 “Apply”。
12. 选择动态应用。

为基于文件的验证创建 ACL

Sun ONE Web Server 6.1 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 Sun ONE Web Server 6.1 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。

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";
...
};
```

可以在 `server.xml` 文件中某个 `VS` 的 `USERDB` 元素中引用 `myfile` 数据库，其中该数据库将与 `server-root/userdb/dbswitch.conf` 文件中的相应定义相链接。示例：

```
<VS>
...
    <USERDB id="myfile" database="myfiledb">
...
</VS>
```

在 `server-root/userdb/dbswitch.conf` 文件中，有一个条目定义了文件 auth-db 及其配置。示例：

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

请参见下表

表 8-3 文件验证数据库支持的参数

syntax	（可选）值为 keyfile、 digest 或 htaccess。如果未指定，则缺省为 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。
groupfile	（syntax=htaccess 时需要） AuthGroupFile 的路径。
userfile	（syntax=htaccess 时需要） AuthUserFile 的路径。

注意 文件验证数据库文件（htaccess、digestfile 或 keyfile）中一行的最大长度为 255。

如果任何行的长度超过此限制，服务器将无法启动，日志文件中将记录一条错误。

注 在试图使用基于文件的验证数据库设置 ACL 之前，请确保满足以下前提条件：

- 已经配置了基于文件的验证目录服务。有关如何执行此操作的信息，请参见第 53 页上的 “配置目录服务”。
- 要为其设置 ACL 的虚拟服务器被配置为使用所需的基于文件的验证数据库 （keyfile、 htaccess 或 digestauth）类型。如果未执行此操作，将按照所配置的缺省目录服务来配置 ACL 限制。

为基于文件验证的目录服务创建 ACL

要为基于文件验证的目录服务创建 ACL 条目，请执行以下步骤：

1. 访问 Server Manager 并选择要为其创建或编辑 ACL 的服务器实例。
2. 选择 Server Manager 的 “Preferences”选项卡。
3. 单击 “Restrict Access”链接。
4. 在 “Option”列下，从下拉列表中选择 ACL 文件，然后单击 “Edit ACL”。

5. 在上面框架中的 “Access Control Rules”页面中，单击要编辑的 ACL 的 “Users/Groups”链接。
6. 在下面框架中的 “User/Group”页面中，从验证数据库下拉列表中选择 “keyfile”。
7. 单击 “Update”。

   当您按照基于 keyfile 的文件验证数据库设置 ACL 时， `dbswitch.conf` 文件使用相应 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 One Web Server 6.1";

  database = "mykeyfile";

  method = "basic";

  };

deny (all) user = "anyone";

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

为基于 .htaccess 验证的目录服务创建 ACL

Sun ONE Web Server 支持基于 .htaccess 的平面文件验证。如果您以前使用的是 .htaccess 验证，则可以迁移现有数据文件，而无需更改文件验证数据库。如 “使用 .htaccess 文件”中所述， .htaccess 用户和组数据可以存储在一个文件中，也可以分成两个文件 （一个存储用户数据，另一个存储组数据）。文件验证数据库对这两种现有格式都支持。

要为基于 htaccess 验证的目录服务创建 ACL，请执行以下步骤：

1. 访问 Server Manager 并选择要为其创建或编辑 ACL 的服务器实例。
2. 选择 Server Manager 的 “Preferences”选项卡。
3. 单击 “Restrict Access”链接。
4. 在 “Option”列下，从下拉列表中选择 ACL 文件，然后单击 “Edit ACL”。
5. 在上面框架中的 “Access Control Rules”页面中，单击要编辑的 ACL 的 “Users/Groups”链接。

6. 在下面框架中的 “User/Group”页面中，从验证数据库下拉列表中选择 “htaccess”。
7. 单击 “Update”。

   当您按照基于 htaccess 的文件验证数据库设置 ACL 时， `dbswitch.conf` 文件使用相应 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 One Web Server 6.1";
  database = "myhtaccessfile";
  method = "basic";
  };
deny (all) user = "anyone";
allow (all) user = "all";
```

将现有 .htaccess 信息迁移到文件验证数据库中

要在 Sun ONE Web Server 6.1 中将现有 .htaccess 信息迁移到文件验证数据库中，请执行以下步骤：

- 将 .htaccess userfile 数据库复制到 *server-root*/*server-instance*/config/userfile 中。
- 将 htaccess groupfile 数据库复制到 *server-root*/*server-instance*/config/groupfile 中。

用户文件格式如下所示：

```
#user:password
```

组文件格式如下所示：

```
#group1:user1 user2
#group2:user3 user4
```

注 成员名称用空格隔开。

当 userfile 和 groupfile 具有相同的文件名时，它们将合并在一起。合并后的每一行都使用如下所示的语法：

```
#user:password:group1,group2
```

注 列之间用冒号隔开。

htaccess 样例数据库

样例 1

```
#sample userfile  (user/password "j2ee/j2eepwd"  user/password
"user1/user1pwd" )

j2ee:9hmjfRwNxvJLU

user1:wvQirF86BsjSk
```

样例 2

```
#sample group file

staff:j2ee  user1

eng:j2ee
```

样例 3

```
#sample user/group file (username "j2ee", user password "j2eepwd")

j2ee:9hmjfRwNxvJLU:staff,eng
```

为基于摘要验证的目录服务创建 ACL

文件验证数据库还支持一种文件格式，适用于基于每个 RFC 2617 的摘要验证。此时将存储一个基于密码和领域的散列，且不维护明文密码。

要为基于摘要验证 （基于 digestauth）的目录服务创建 ACL，请执行以下步骤：

1. 访问 Server Manager 并选择要为其创建或编辑 ACL 的服务器实例。
2. 选择 Server Manager 的 “Preferences”选项卡。
3. 单击 “Restrict Access”链接。
4. 在 “Option”列下，从下拉列表中选择 ACL 文件，然后单击 “Edit ACL”。
5. 在上面框架中的 “Access Control Rules”页面中，单击要编辑的 ACL 的 “Users/Groups”链接。

6. 在下面框架中的 “User/Group” 页面中，从验证数据库下拉列表中选择 “digest”。
7. 单击 “Update”。

   当您按照基于 digestauth 的文件验证数据库设置 ACL 时， `dbswitch.conf` 文件使用相应 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

配置服务器首选项

本章介绍如何为 Sun ONE Web Server 配置服务器首选项。

本章包括以下部分：

启动和停止服务器

服务器将在安装后持续运行，侦听并接受 HTTP 请求。

服务器的状态显示在 “Server On/Off”。您可以使用以下方法之一启动和停止服务器：

- 单击 “Server On/Off”上的。
- 使用 “控制面板”中的 “服务”窗口。 (Windows)

- 使用 start。如果您将此脚本与 init 一起使用，则必须在 /etc/inittab 中包含 start 命令 http:2:respawn:*server_root*/*type-identifier*/start -start -i。(UNIX/Linux)
- 使用 stop 来完全关闭服务器。这将中断服务，直至重新启动。如果将 etc/inittab 文件设置为自动重新启动（使用 “respawn”），则必须在关闭服务器之前删除 etc/inittab 文件中与该 Web 服务器相关的一行文本，否则服务器将自动重新启动。(UNIX/Linux)

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”。

如果计算机崩溃或脱机，服务器将停止，正在处理的所有请求都将丢失。

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

注 在 UNIX 上，某些 Sun ONE Web Server 安装需要访问的内存和 / 或文件描述符可能比缺省情况下操作系统所允许访问的要多。如果无法启动服务器，请使用 ulimit 命令检查由操作系统强加的资源限制。有关详细信息，请参见操作系统的 ulimit 手册页。

设置终止超时

服务器停止后，将不再接收新的连接，而只是等待所有未完成的连接完成。在 magnus.conf 文件 （可在 *server_root*/https-*server_name*/config/ 中找到）中可以配置服务器在超时之前等待的时间。缺省情况下，该时间设置为 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用的时间。

重新启动服务器 (UNIX/Linux)

您可以使用以下方法之一重新启动服务器：

- 自动从 `inittab` 文件重新启动。

  请注意，如果所使用的 UNIX/Linux 版本不是源自系统 V （例如 SunOS 4.1.3），则无法使用 `inittab` 文件。

- 重新启动计算机时，自动使用 `/etc/rc2.d` 中的守护程序进行重新启动。
- 手动重新启动。

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

通常情况下，不能使用上述任何文件来启动启用了 SSL 的服务器，因为启动之前服务器会要求输入密码。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，但建议**不要**使用这种方法。

注意 将启用了 SSL 的服务器的密码以纯文本格式存储在服务器的启动脚本中会带来很大的安全风险。任何可以访问该文件的用户都有权访问启用了 SSL 的服务器的密码。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、密钥对文件和密钥口令应属于 root 用户 （如果服务器是由非 root 用户安装的，则应属于该用户帐户），并且只有所有者具有读 / 写权限。

自动启动启用了 SSL 的服务器

如果您不担心会带来安全风险，请执行以下步骤以自动启动启用了 SSL 的服务器：

1. 使用文本编辑器打开启动文件，该文件位于 *server_root*`/https-`*server_id* 中。
2. 找到脚本中的 `-start` 行并插入以下内容：

   `echo "`*password*`"|`

   其中 *password* 是您选择的 SSL 密码。

   例如，如果 SSL 密码是 `netscape`，则编辑后的该行文本可能为：

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

使用 inittab 重新启动 (UNIX/Linux)

要使用 inittab 重新启动服务器，请将下面一行文本添加到 /etc/inittab 文件中：

```
http:23:respawn:server_root/type-identifier/start -start -i
```

其中 *server_root* 是服务器的安装目录， *type-identifier* 是服务器的目录。

-i 选项可以防止将服务器置于后台进程。

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 (UNIX/Linux)

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/type-identifier/start
```

将 *server_root* 替换为服务器的安装目录。

手动重新启动服务器 (UNIX/Linux)

要从命令行重新启动服务器，如果服务器在端口号低于 1024 的端口上运行，请以 root 用户身份登录；否则，请以 root 用户身份或使用服务器的用户帐户登录。在命令行提示符下，键入下面一行文本并按 Enter 键：

```
server_root/type-identifier/start
```

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 选项将在 inittab 模式下运行服务器，因此如果服务器进程终止或崩溃， inittab 会重新启动服务器。此选项还可以防止将服务器置于后台进程。

注 如果服务器已经运行， start 命令将失败。您必须先停止服务器，然后再使用 start 命令。此外，如果服务器启动失败，则应当在尝试重新启动之前终止该进程。

手动停止服务器 (UNIX/Linux)

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。

要手动停止服务器，请以 root 用户身份或使用服务器的用户帐户 （如果您是使用它登录来启动服务器的）登录，然后在命令行中键入以下内容：

```
server_root/type-identifier/stop
```

重新启动服务器 (Windows)

您可以使用以下方法重新启动服务器：

- 使用 “服务控制面板”重新启动任何服务器。
- 使用 “服务控制面板”配置操作系统，以便在每次重新启动计算机时重新启动服务器或 Administration Server。

对于 Windows，请执行以下步骤：

1. 在 “控制面板”中，双击 “服务”图标。
2. 滚动服务列表并选择用于服务器的服务。
3. 选择 “自动”使计算机在每次启动或重新启动时启动服务器。
4. 单击 “OK”。

注 您也可以使用 “服务”对话框更改服务器使用的帐户。有关更改服务器使用的帐户的详细信息，请参见第 94 页上的 “更改用户帐户 (UNIX/Linux)”。

缺省情况下， Web 服务器将提示管理员在启动之前输入密钥数据库密码。如果希望重新启动一个无人参与的 Web 服务器，则需要将该密码保存在 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。

使用自动重新启动实用程序 (Windows)

如果服务器崩溃，将自动通过服务器监视实用程序来重新启动服务器。在安装了调试工具的系统上，如果服务器崩溃，系统将显示一个含有调试信息的对话框。要帮助调试服务器插件 API 程序（例如， NSAPI 程序），可以通过设置一个非常高的超时值来禁用自动启动功能。您也可以使用注册表编辑器来关闭调试对话框。

更改时间间隔 *(Windows)*

要更改启动与服务器可以自动重新启动之间所经过的时间间隔，请执行以下步骤：

1. 启动注册表编辑器。
2. 选择服务器的注册表主键 （在注册表编辑器窗口的左侧，位于 `HKEY_LOCAL_MACHINE\SOFTWARE\Netscape\Enterprise\6.0` 中）。
3. 从 “编辑” 菜单中选择 “添加值”。将显示 “添加主键” 对话框。
4. 在 “值名称” 中，键入 “`MortalityTimeSecs`”。
5. 从 “数据类型” 下拉列表中选择 “REG_DWORD”。
6. 单击 “确定”。将显示 “DWORD 编辑器” 对话框。
7. 键入启动和服务器可以自动重新启动的时间之间的时间间隔 （秒）。

   该间隔可以是二进制、十进制或十六进制格式。
8. 为在上一步中输入的值单击某个数字格式 （二进制、十进制或十六进制）。
9. 单击 “确定”。

   `MortalityTimeSecs` 值将以十六进制格式显示在注册表编辑器窗口的右侧。

关闭调试对话框 *(Windows)*

如果您安装的某个应用程序 （例如编译程序）修改了系统的调试设置，则服务器崩溃时，您可能会看到一个系统生成的应用程序错误对话框。单击 “确定” 后服务器才能重新启动。

要关闭服务器崩溃时显示的调试对话框，请执行以下步骤：

1. 启动注册表编辑器。
2. 选择 AeDebug 主键，该主键位于注册表窗口左侧的 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion` 中。
3. 在窗口的右侧双击 “自动” 值。

   将显示 “字符串编辑器” 对话框。
4. 将字符串值更改为 1。

优化服务器性能

优化线程限制有两种方法：编辑 `magnus.conf` 文件或使用 Server Manager。

如果编辑 `magnus.conf` 文件，则 `RqThrottleMinPerSocket` 是最小值，`RqThrottle` 是最大值。

最小限制是服务器试图在 `WaitingThreads` 状态中保持的线程数。该数目只是一个希望的目标。该状态中的实际线程数会稍微高于或低于此值。缺省值为 48。最大线程是对可同时运行的活动线程最大数目的硬性限制，它可能会成为性能的瓶颈。缺省值为 128。

如果使用 Server Manager，请执行以下步骤：

1. 转至 “Preferences”选项卡。
2. 单击 “Performance Tuning”链接。
3. 在 “Maximum simultaneous requests”字段中输入所需的值。

有关 `RqThrottleMinPerSocket` 和 `RqThrottle` 参数的详细信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference*。

有关这些设置和其他设置的隐含性能的详细信息，请参见 Sun ONE Web Server 6.1 *Performance Tuning, Sizing, and Scaling Guide*。

编辑 magnus.conf 文件

Sun ONE Web Server 启动时，它将查看 *server_root*/*server_id*/`config` 目录中的一个名为 `magnus.conf` 的文件，以创建一组影响服务器的行为和配置的全局变量设置。 Sun ONE Web Server 将执行 `magnus.conf` 中定义的所有指令。您可以使用 Server Manager 中的 “Magus Editor”来编辑 `magnus.conf` 文件中的某些设置。

有关 `magnus.conf` 文件的完整说明以及使用文本编辑器编辑该文件的信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference* 和 Sun ONE Web Server 6.1 *NSAPI Programmer's Guide*。

要访问 “Magnus Editor”，请执行以下步骤：

1. 访问 Server Manager 并选择 “Preferences”选项卡。
2. 单击 “Magnus Editor”链接。

3. 从下拉列表中选择要编辑的设置并单击 “Manage”。

   Server Manager 将显示指定设置的编辑器。

4. 根据需要对设置进行更改，然后单击 “OK”。

有关每个 “Settings”的详细信息，请参见联机帮助中的 “Magnus Editor”。

添加和编辑侦听套接字

在服务器能够处理请求之前，必须先通过侦听套接字接受请求，然后将请求发送给正确的虚拟服务器。安装 Sun ONE Web Server 时将自动创建一个侦听套接字 (ls1)。此侦听套接字使用 IP 地址 0.0.0.0 和在安装过程中指定为 HTTP 服务器端口号的端口号 （缺省值为 80）。不能删除缺省的侦听套接字。

您可以使用 Server Manager 的侦听套接字表来编辑服务器的侦听套接字设置。要访问该表，请执行以下步骤：

1. 访问 Server Manager 并单击 “Preferences”选项卡。
2. 单击 “Edit Listen Sockets”链接。
3. 进行所需的更改并单击 “OK”。

选择 MIME 类型

通过 “Mime Types”页面可以编辑服务器的 MIME 文件。

MIME （多用途 Internet 邮件扩展）类型控制邮件系统支持的多媒体文件的类型。它还可以指定属于特定服务器文件类型的文件扩展名 （例如，指定哪些文件是 CGI 程序）。

您无需为每台虚拟服务器创建单独的 MIME 类型文件。相反，可以根据需要创建任意数量的 MIME 类型文件，然后将它们与一台虚拟服务器相关联。缺省情况下，服务器中存在一个 MIME 类型文件 `mime.types`，该文件不可删除。此文件可以使用绝对路径。

要访问 “MIME Types”，请执行以下步骤：

1. 访问 Server Manager 并单击 “Preferences”选项卡。
2. 单击 “MIME Types”链接。
3. 进行所需的更改并单击 “OK”。

有关详细信息，请参见联机帮助中的 “Mime Settings”页面和第 13 章 “使用虚拟服务器”。

限制访问

您可以使用 Server Manager 的 “Restrict Access”页面控制对整个服务器或服务器中各部分 （即目录、文件、文件类型）的访问。当服务器评估传入的请求时，它将根据一个称为访问控制条目 (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 集合称为访问控制表 (ACL)。当一个请求传入服务器时，服务器将在 *vsclass*`.obj.conf` 文件 （其中 *vsclass* 是虚拟服务器类的名称）中查找对某个 ACL 的引用，然后用该 ACL 确定访问权限。缺省情况下，服务器具有一个 ACL 文件，其中包含多个 ACL。

您可以通过 Administration Server 为所有服务器设置全局访问控制，或通过 Server Manager 为特定服务器实例中的资源设置访问控制。有关为某个资源设置访问控制的详细信息，请参见第 8 章 “控制对服务器的访问”中的第 167 页上的 “设置访问控制”。

注 必须先启用分布式管理，然后才能限制服务器访问。

要限制对 Sun ONE Web Server 的访问，请执行以下步骤：

1. 访问 Server Manager 并选择 “Preferences”选项卡。
2. 单击 “Restrict Access”链接。

有关详细信息，请参见第 8 章 “控制对服务器的访问”和联机帮助中的 “Restrict Access”页面。

恢复配置设置

通过 “Restore Configuration”页面可以查看配置文件的备份副本，还可以恢复在某个特定日期保存的配置数据。

注	在 Windows 上，请仅使用此页面回滚您自己对配置文件所做的更改。请不要回滚到安装过程中创建的备份版本，它们可能不完整。

有关详细信息，请参见联机帮助中的 “Restore Configuration”。

配置文件高速缓存

Sun ONE Web Server 使用文件高速缓存以更快地提供静态信息。在服务器的前一个版本中，也有一个加速器高速缓存，可以将请求路由到文件高速缓存，但现在已不再使用。文件高速缓存包含有关文件和静态文件内容的信息，并且可以缓存用于加速处理服务器分析的 HTML 的信息。

缺省情况下，文件高速缓存处于打开状态。文件高速缓存设置包含在 `nsfc.conf` 文件中。可以使用 Server Manager 更改文件高速缓存设置。

有关详细信息，请参见 `http://docs.sun.com` 上的联机指南 *Performance Tuning and Sizing Guide*。

添加和使用线程池

您可以使用线程池将一定数量的线程分配给特定服务。

线程池的另一个用途是运行对于线程来说不安全的插件。如果将线程池的最大线程数定义为 1，则指定的服务函数只允许处理一个请求。

添加线程池时，需要指定的信息包括：最小和最大线程数、栈大小以及队列大小。

有关详细信息，请参见 `http://docs.sun.com` 上的联机指南 *Performance Tuning and Sizing Guide*。

本地线程池和普通线程池 (Windows)

在 Windows 上，您可以使用两种线程池：本地线程池 (`NativePool`) 和普通线程池。

要编辑本地线程池，请访问 Server Manager 中的 “Native Thread Pool”页。

您可以根据需要创建任意多个普通线程池以便用于各种目的。要创建普通线程池，请访问 Server Manager 中的 “Generic Thread Pools”页。

线程池 (UNIX/Linux)

由于 UNIX/Linux 上的线程始终是由操作系统而不是用户安排的，因此 UNIX/Linux 用户无需使用 `NativePool`，也没有可供编辑其设置的 “Server Manager”。但是， UNIX/Linux 用户仍然可以创建线程池。要创建线程池，请访问 Server Manager 中的 “Thread Pools”页。

编辑线程池

添加线程池后，可以通过 Server Manager 更改线程池设置的值 （例如最小线程数和最大线程数等）。

您也可以在 *vsclass*`.obj.conf` （其中 *vsclass* 是虚拟服务器类的名称）中更改线程池设置。

vsclass`.obj.conf` 中显示的线程池如下：

```
Init fn="thread-pool-init" name=name_of_the_pool MaxThreads=n
MinThreads=n QueueSize=n StackSize=n
```

使用以下参数更改线程池：`MinThreads`、 `MaxThreads`、 `QueueSize` 和 `StackSize`。

Windows 用户始终可以使用 Server Manager 来编辑本地池的设置。

使用线程池

对线程池进行设置后，可以通过将其指定为特定服务的线程池来使用它。

要配置线程池，请转到 “Server Manager Preferences”选项卡并选择 “Thread Pool”。配置线程池后，“Thread Pool”列表将显示可用于您所指定的特定服务的线程池

您也可以通过使用 *vsclass* `obj.conf` （其中 *vsclass* 是虚拟服务器类的名称）中的 `load-modules` 函数的 `pool` 参数来指定线程池。

```
pool="name_of_pool"
```

此外，可以对任意 NSAPI 函数使用 `pool` 参数，以便仅让该 NSAPI 函数在您指定的池中运行。

第 10 章

使用日志文件

您可以使用多种方法监视服务器的活动。本章介绍了通过记录和查看日志文件来监视服务器的方法。有关使用内置性能监视服务、服务质量功能或 SNMP 的信息，请参见 “监视服务器”。

本章包括以下部分：

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。错误日志文件 （位于服务器根目录中的 `https-`*`server_name`*`/logs/errors` 下）列出了服务器曾遇到的所有错误。访问日志 （位于服务器根目录中的 `https-`*`server_name`*`/logs/access` 下）记录了有关对服务器的请求以及服务器响应的信息。您可以配置 Sun ONE Web 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数据。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，Sun ONE Web Server 无法在 Linux 上处理大于 2GB 的日志文件。达到最大日志大小后，日志记录就会停止。

UNIX 和 Windows 平台上的日志

本节介绍如何创建日志文件。此外，还包括以下主题：

- 缺省错误日志
- 使用 syslog 记录日志
- 使用 Windows 事件日志记录日志

缺省错误日志

在 UNIX 和 Windows 平台上， Administration Server 的日志存储在该服务器的 `https-admserve/logs/` 目录下。服务器实例的日志存储在 `https-`*`server_name`*`/logs/` 目录下。

可以设置整个服务器的缺省日志级别，还可以将 stdout 和 stderr 重定向到服务器的事件日志以及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 的内容定向到服务器的事件日志。缺省情况下，日志消息除了发送到指定的服务器日志文件以外，还将发送到 stderr。

另一个可用的功能是使用日志消息记录虚拟服务器 ID。当使用多个虚拟服务器将消息记录到同一个日志文件时，此功能很有用。可以选择将日志消息写入系统日志。执行此操作时，不会在错误日志文件中进行日志记录，而是使用 UNIX 中的 syslog 日志服务或 Windows 平台上的系统日志服务来生成和管理日志。

还可以使用 server.xml 的属性来控制此文件的内容。有关 server.xml 文件的详细信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference*。

使用 syslog 记录日志

syslog 适用于要求集中记录日志的稳定的可操作环境。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或虚拟服务器日志可能比较容易管理。

注

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

通过将 syslog 日志文件与 syslogd 以及系统日志守护程序一起使用，可以将 syslog.conf 文件配置为：

- 将消息记入相应的系统日志
- 将消息写入系统控制台
- 将日志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 Sun ONE Web Server 以及其他守护程序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或虚拟服务器实例中专用于 Sun ONE Web Server 的消息：

- 唯一消息 ID
- 时间标记
- 实例名
- 程序名 （webservd 或 webserv-wdog）
- 进程 ID （webserv 进程的 PID）
- 线程 ID （可选）
- 服务器 ID

可以在 server.xml 文件中为 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手册命令：

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

使用 Windows 事件日志记录日志

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 “事件日志”。

日志级别

下表按严重程度升序定义了 Sun ONE Web Server 中的日志级别和消息。

表 10-1 日志级别

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

关于虚拟服务器和日志

Sun ONE Web Server 可以拥有虚拟服务器实例。Sun ONE Web Server 实例中的每个虚拟服务器都具有自己的标识，也可以具有自己的日志文件。可以使用每台虚拟服务器的单个日志文件追踪特定事务和资源的服务器活动。

也可以将来自多台虚拟服务器的日志消息定向到一个服务器日志文件。执行此操作时，用户可能需要启用 `logvsid`（位于 `server.xml` 文件中的 `LOG` 元素内）。这有助于区分来自不同虚拟服务器的日志消息。

```
<SERVER>

  ...

  <LOG file="/export//https-iws-files2.red.iplanet.com/logs/errors"
loglevel="finest" logtoconsole="true" usesyslog="false"
createconsole="false" logstderr="true" logstdout="true"
logvsid="true"/>

</SERVER>
```

在本实例中，`<LOG logvsid="true">` 的作用是将虚拟服务器 ID 包含在每个日志消息中。这样可以区分来自不同虚拟服务器的消息。如果 `VS` 元素中不包含 `errorlog` 属性，那么所有虚拟服务器上的消息都将记录到一个文件中。

重定向应用程序和服务器日志输出

对于开发者来说，在进行 Web 应用程序组件和 J2EE 应用程序的部件测试时，可以随时访问应用程序日志和服务器日志非常重要。在 Windows 平台上，开发者更希望看到日志消息显示在桌面命令窗口中。在 UNIX 平台上，只需将日志消息分发到从中启动了服务器实例的终端窗口中的 stderr，或使用命令 tail `-f` 就可以查看写入日志文件的日志消息给许多开发者带来了很大的方便。

`server.xml` 文件中包含了可以为 stdout 和 stderr 设置的属性，以将日志消息定向到日志文件或终端窗口等位置。有关使用 stdout 和 stderr 的详细信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference*。

归档日志文件

可以将访问日志文件和错误日志文件设置为自动归档。在某一时间或在指定的时间间隔后，用户的日志将被轮转。 Sun ONE Web Server 将保存旧的日志文件，并使用包含保存日期和时间的名称标记所保存的文件。

例如，可以将访问日志文件设置为每小时旋转一次，而 Sun ONE Web Server 将保存该文件并将其命名为 “`access.200307152400`”，其中将日志文件名、年月日和 24 小时制时间合成一个字符串。根据所设置的日志轮转类型，日志归档文件的实际格式会有所不同。

Sun ONE Web Server 为归档文件提供了两种日志轮转类型：内部守护程序日志轮转和基于守护程序的日志轮转。

内部守护程序日志轮转

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

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

```
error.<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.200307152400`。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.，则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

此类型的日志轮转将基于存储在 scheduler.conf 文件中的时间（该文件位于 *server_root*/https-admserv/config/ 目录下）。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 schedulerd.conf 文件中（位于 *server_root*/https-admserv/config/ 目录下）。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 将变成 access.200307151630。

日志轮转在服务器启动时进行初始化。如果开启了轮转， Sun ONE Web Server 将创建一个用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。

轮转开始以后，如果存在需要记录到访问日志文件或错误日志文件的请求或错误，Sun ONE Web Server 将在预先调度的 “下次旋转时间”之后创建用新时间标记的日志文件。

注 您应该在运行日志分析程序之前将服务器日志归档。

要将日志文件归档以及指定是采用内部守护程序方法还是采用基于调度程序的方法，请使用 Server Manager 中的 “Archive Log Files”。

设置访问日志首选项

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

要将 %vsid% 添加到日志文件格式字符串：

1. 访问 Server Manager 并选择 “Logs”选项卡。
2. 单击 “Access Log Preferences”链接。
3. 在 “Log File:”文本框中输入新的日志文件位置和文件名。
4. 单击 “Only Log:”单选按钮。
5. 单击 “Virtual Server Id”复选框。也可以单击 “Custom Format:”单选按钮并添加字符串 '%vsid%。

注 添加自定义格式字符串 '%vsid% 时，必须使用新的访问日志文件。

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

服务器访问日志可以使用通用日志文件格式、灵活日志格式或用户可自定义的格式。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。灵活的日志格式使您可以选择 （从 Sun ONE Web Server）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。有关可自定义的格式参数的列表，请参见 *NSAPI Programmer's Guide*。

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。

您可以使用 Server Manager 中的 “Access Log Preferences”来指定日志首选项，也可以手动配置 `obj.conf` 文件中的以下指令。在 `magnus.conf` 中，服务器将调用函数 `flex-init` 初始化灵活日志系统，并调用函数 `flex-log` 以灵活日志格式记录专用于请求的数据。要使用通用日志文件格式记录请求，服务器将调用 `init-clf` 初始化通用日志子系统 （该子系统在 `obj.conf` 中使用），并调用 `common-log` 以通用日志格式 （大多数 HTTP 服务器采用的格式）记录专用于请求的数据。

有关 NSAPI 日志函数 （包括有效的指令和参数）的详细信息，请参见 *NSAPI Programmer's Guide*。

简易 Cookie 日志

使用 flexlog 功能， Sun ONE Web Server 可以很容易地记录特定的 cookie。在配置文件 `obj.conf` 中，将 “`Req->headers.cookie.`*`cookie_name`*”添加到用于初始化 `flex-log` 子系统的行中。如果请求标头中存在 cookie 变量，则将记录 cookie 变量 *`cookie_name`* 的值；如果不存在该变量，将记录 “-”。

设置错误日志选项

Sun ONE Web Server 6.1 使您可以配置要记录到服务器错误日志中的信息。

对于 Administration Server 实例

1. 访问 Administration Server。
2. 选择 “Preferences”选项卡。
3. 单击 “Access Logging Options”链接。
4. 输入所需的信息。
5. 依次单击 “OK”和 “Apply”来保存并应用更改。

对于服务器实例

1. 访问服务器实例。
2. 选择 “Logs”选项卡。
3. 单击 “Error Log Preferences”链接。
4. 输入所需的信息。
5. 依次单击 “OK”和 “Apply”来保存并应用更改。

配置 LOG 元素

下表说明了可以在 `server.xml` 文件中配置的 LOG 元素：

表 2 LOG 属性

属性	缺省值	说明
`file`	`errors`	指定用来存储来自缺省虚拟服务器消息的文件。来自其他已配置虚拟服务器的消息也存储在该文件中，除非在 `VS` 元素中明确指定了 `errorlog` 属性。
`loglevel`	`info`	控制由其他元素记录到错误日志中的消息的缺省类型。允许的值如下所示 （从高到低排列）： `finest`、`fine`、`fine`、`info`、`warning`、`failure`、`config`、`security` 和 `catastrophe`。

表 2 LOG 属性

属性	缺省值	说明
logvsid	false	（可选）如果为 true，虚拟服务器日志中将显示虚拟服务器 ID。如果有多个 VS 元素共享同一个日志文件，这些属性会很有用。 请注意，在 Sun ONE Web Server 6.1 中，无法在 magnus.conf 文件中配置 logvsid 元素。
logstdout	true	（可选）如果为 true，则将 stdout 输出重定向到错误日志。有效值为 on、 off、 yes、 no、 1、 0、 true 和 false。
logstderr	true	（可选）如果为 true，则将 stderr 输出重定向到错误日志。有效值为 on、 off、 yes、 no、 1、 0、 true 和 false。
logtoconsole	true	（可选，仅限 UNIX）如果为 true，则将日志消息重定向到控制台。
createconsole	false	（可选，仅限 Windows）如果为 true，则为 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，则使用 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访问日志文件和已归档的访问日志文件。

要从 Administration Server 查看其访问日志，请依次选择 “Preferences”选项卡和 “View Access Log”页面。

要通过 Server Manager 查看服务器实例的访问日志，请依次选择 “Logs”选项卡和 “View Access Log”页面

要从 Class Manager 查看单个虚拟服务器的访问日志，请先从突出显示的 “Manage Virtual Servers”页面中选择要管理的虚拟服务器，然后在 “Virtual Server Manager”页面中单击 “Access Log”标题下的链接。您可以指定要查看的条目数或具有所选条件限定词的条目数。

以下是使用通用日志文件格式的访问日志的实例 （此格式在 “Log Preferences”窗口中指定，有关详细信息，请参见第 225 页上的 “设置访问日志首选项”）：

```
wiley.a.com - - [16/Feb/2001:21:18:26 -0800] "GET / HTTP/1.0" 200 751
wiley.a.com - - [17/Feb/2001:1:04:38 -0800] "GET /docs/grafx/icon.gif
HTTP/1.0" 204 342
wiley.a.com - - [20/Feb/2001:4:36:53 -0800] "GET /help HTTP/1.0" 401 571
arrow.a.com - john [29/Mar/2001:4:36:53 -0800] "GET /help HTTP/1.0" 401 571
```

表 10-3 对该访问日志样例中的最后一行进行了说明。

表 10-3 样例访问日志文件中最后一行的字段

访问日志字段	实例
客户机的主机名或 IP 地址	arrow.a.com。（在这种情况下，显示主机名是因为启用了进行 DNS 查找的 Web 服务器的设置；如果禁用了 DNS 查找，将显示客户机的 IP 地址。）
RFC 931 信息	-（RFC 931 标识未实现）
用户名	john （客户输入的用于验证的用户名）
请求的日期 / 时间	29/Mar/1999:4:36:53 -0800
请求	GET /help
协议	HTTP/1.0
状态代码	401
传送的字节数	571

以下是使用灵活日志格式的访问日志的实例 （此格式在 “Log Preferences”中指定，详细信息请参见第 225 页上的 “设置访问日志首选项”）：

```
wiley.a.com - - [25/Mar/2001:12:55:26 -0800] "GET /index.htm HTTP/1.0" "GET"
"/?-" "HTTP/   1.0" 304 0 - Mozilla/2.0 (WinNT; I)
wiley.a.com - - [25/Mar/2001:12:55:26 -0800] "GET / HTTP/1.0" "GET" "/?-"
"HTTP/1.0" 304 0    - Mozilla/2.0 (WinNT; I)
wiley.a.com - - [25/Mar/2001:12:55:26 -0800] "GET / HTTP/1.0" "GET" "/?-"
"HTTP/1.0" 304 0    - Mozilla/2.0 (X11; I; IRIX 5.3 IP22)
```

查看错误日志文件

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

要从 Administration Server 查看其错误日志文件，请依次选择“Preferences”选项卡和“View Error Log”页面。

要从 Server Manager 查看服务器实例的错误日志文件，请依次选择“Logs”选项卡和“View Error Log”页面。

要通过 Class Manager 查看单个虚拟服务器的错误日志，请先从突出显示的“Manage Virtual Servers”页面中选择要管理的虚拟服务器，然后在“Virtual Server Manager”页面中单击“Error Log”标题下的链接。您可以指定要查看的条目数或具有所选条件限定词的条目数。

以下是两个错误日志中条目的实例：第一个实例显示的是一条表明服务器成功启动的提示性信息，第二个实例表明的是客户机 `wiley.a.com` 对文件 `report.html` 进行请求，但是该文件却未在服务器的主文档目录下。

```
[[22/Jan/2001:14:31:41] info (39700):successful server startup
[22/Jan/2001:14:31:41] info (39700):SunONE-WebServer/6.1 BB1-01/22/2001 01:45
[22/Jan/2001:14:31:42] warning (13751):for host wiley.a.com trying to GET
/report.html, send-file reports:can't find
/usr1/irenem/ES60-0424/docs/report.html (File not found)
```

运行日志分析程序

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` 目录下的 HTML 文档中介绍了此工具的参数。*server-root*`/extras/flex_anlg` 目录中包含适用于灵活日志文件格式的命令行日志分析程序。但在缺省情况下，Server Manager 使用灵活日志文件报告工具，而不管您是否已选择了通用日志文件格式或灵活日志文件格式。

使用日志分析程序可以生成有关缺省服务器的统计数据，例如活动摘要、最常访问的 URL、一天中访问服务器的高峰时段等等。可以从 Sun ONE Web Server 或命令行运行日志分析程序。除了可以生成缺省服务器的统计数据以外，日志分析程序不能生成任何虚拟服务器的统计数据。但是，可以查看每个虚拟服务器的统计数据，如第 228 页上的 “查看访问日志文件”中所述。

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/https/lib:$LD_LIBRARY_PATH
```

AIX：

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

HP-UX：

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

Windows：

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

注 在运行日志分析程序之前，应将服务器日志归档。有关将服务器日志归档的详细信息，请参见第 224 页上的 “归档日志文件”。

要从 Server Manager 运行日志分析程序，请执行以下步骤：

1. 在 Server Manager 中单击 “Logs”选项卡。
2. 单击 “Generate Report”。
3. 填写各个字段。
4. 单击 “OK”。

   报告将显示在新窗口中。

有关详细信息，请参见联机帮助中的 “Generate Report”页面。

要从命令行分析访问日志文件，请运行工具 `flexanlg`（位于目录 *server-install*`/extras/flex_anlg` 下）。

要运行 `flexanlg`，请在出现命令提示后键入以下命令和选项：

```
flexanlg [ -P ] [-n name] [-x] [-r] [-p order] [-i file]* [ -m
metafile ]* [ o file][ c opts] [-t opts] [-l opts]
```

下面将介绍语法。

```
flexanlg -h.):
-P: 代理日志格式                                          缺省值: no
-n servername: 服务器的名称
-x: HTML 中的输出                                         缺省值: no
-r: 将 IP 地址解析到主机名                                缺省值: no
-p [c,t,l]: 输出顺序 (计数、时间统计和列表)               缺省值: ctl
-i filename: 输入日志文件                                 缺省值: none
-o filename: 输出日志文件                                 缺省值: stdout
-m filename: 元文件                                       缺省值: none
-c [h,n,r,f,e,u,o,k,c,z]: 对这些项目进行计数 -            缺省值: hnreuokc
    h: 找到的总数
    n: 304 未修改的状态代码 (使用本地副本)
    r: 302 找到的状态代码 (重定向)
    f: 404 未找到的状态代码 (未找到文档)
    e: 500 服务器错误状态代码 (配置错误)
    u: 唯一 URL 的总数
    o: 唯一主机的总数
    k: 传送的千字节总数
    c: 高速缓存中保存的千字节总数
    z: 不对任何项目进行计数
-t [sx,mx,hx, xx,z]: 查找常规统计数据 - 缺省值: s5m5h24x10
    s (数目): 查找日志的最大 (数目) 秒钟数
    m (数目): 查找日志的最大 (数目) 分钟数
    h (数目): 查找日志的最大 (数目) 小时数
    u (数目): 查找日志的最大 (数目) 用户数
    a (数目): 查找日志的最大 (数目) 用户代理数
    r (数目): 查找日志的最大 (数目) 参考数
    x (数目): 查找最大 (数目) 的杂项关键字
    z: 不查找任何常规统计数据
-l [cx,hx]: 创建列表 - 缺省值: c+3h5
    c(x,+x): 最常访问的 URL
          (x: 仅列出 x 项)
          (+x: 仅当访问超出 x 次时列出)
    h(x,+x): 最常访问用户服务器的主机 (或 IP 地址)
          (x: 仅列出 x 项)
          (+x: 仅当访问超出 x 次时列出)
    z: 不创建任何列表
```

查看事件 (Windows)

除了将错误记录到服务器错误日志之外 （请参见第 230 页上的 “查看错误日志文件”），Sun ONE Web Server 还将严重的系统错误记录到事件查看器中。事件查看器可用于监视系统中发生的事件。在打开错误日志之前，可以使用事件查看器查看因基础配置问题而引起的错误。

要使用事件查看器，请执行以下步骤：

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。 Sun ONE Web Server 产生的错误具有 `https-`*`serverid`* 或 `WebServer6.1` 的源标签。
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。

   有关事件查看器的详细信息，请参见系统文档。

第 11 章

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、服务质量功能和简单网络管理协议 (SNMP)。

您可以将 SNMP 与 Sun ONE 管理信息库 (MIB) 以及网络管理软件 （例如 HP OpenView）结合使用以实时监视服务器 （就像监视网络中的其他设备一样）。

注 在 Windows 上，在安装 Sun ONE Web Server 6.1 之前，请确保计算机上已经安装了 Windows SNMP 组件。

您可以通过使用统计数据功能或 SNMP 来实时查看服务器的状态。在 UNIX 或 Linux 中，如果要使用 SNMP，则必须为 Sun ONE 服务器配置 SNMP。本章提供了在 UNIX 或 Linux 上将 SNMP 用于 Sun ONE 服务器所需的信息。

本章包括以下主题：

使用统计数据监视服务器

您可以使用统计数据功能监视服务器的当前活动。统计数据显示了服务器处理的请求的数目以及这些请求的处理状况。您可以查看单个虚拟服务器的某些统计数据，也可以查看整个服务器实例的其他统计数据。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。有关详细信息，请参见 Sun ONE Web Server 6.1 *Performance Tuning, Sizing, and Scaling Guide*。

启用统计数据功能后，您可以查看以下方面的统计数据：

- 连接
- DNS
- 保持活动
- 高速缓存
- 虚拟服务器

交互式服务器监视器会报告各种服务器统计数据的总计。有关这些数据的说明，请参见联机帮助中的 “Monitor Current Activity”页面。

注意 启用统计数据 / 探查时，服务器的所有用户都可以使用统计数据信息。有关详细信息，请参见 Sun ONE Web Server 6.1 *NSAPI Programmer's Guide* 中 stats-xml 的说明。

启用统计数据

要启用统计数据，请执行以下步骤：

1. 在 Server Manager 中，单击 “Monitor”选项卡。
2. 单击 “Monitor Current Activity”。
3. 单击 “Yes”启用统计数据。
4. 单击 “OK”。

5. 单击 “Apply”应用所做的更改。您无需重新启动服务器。

有关启用统计数据的更多信息，请参见联机帮助。

使用统计数据

启用统计数据功能后，您可以获得有关服务器实例和虚拟服务器运行状况的各种信息。统计数据按功能被划分为若干方面。

要访问统计数据，请执行以下步骤：

1. 在 Server Manager 中，单击 “Monitor”选项卡。
2. 单击 “Monitor Current Activity”。
3. 从下拉列表中，选择轮询时间间隔。

   轮询时间间隔是显示的统计数据信息更新之间的间隔秒数。
4. 从下拉列表中，选择要显示的统计数据类型。
5. 单击 “Submit”。

   如果您在服务器实例正在运行时启用了统计数据 / 探查，您将看到一个显示了选定统计数据类型的页面。该页面每隔 5-15 秒更新一次，这取决于您选定的轮询时间间隔。

您可以使用统计数据中显示的数据来优化服务器。有关详细信息，请参见 Sun ONE Web Server 6.1 *Performance Tuning, Sizing, and Scaling Guide*。

使用服务质量

服务质量是指为服务器实例虚拟服务器类或虚拟服务器设置的性能限制。例如，如果您是 ISP，则可能希望根据允许虚拟服务器使用的带宽数量对虚拟服务器收取不同的费用。可以在两个方面进行限制：带宽数量和连接数目。

您可以在 Server Manager 的 “Monitor”选项卡中为整个服务器或虚拟服务器的某个类启用这些设置。然而，您可以为某单个虚拟服务器覆盖这些服务器或类级别的设置。有关为单个服务器设置服务质量限制的详细信息，请参见第 312 页上的 “配置虚拟服务器的服务质量设置”。

有两个设置用于控制流量的计算方式以及带宽的重新计算频率：重新计算时间间隔和公制时间间隔。重新计算时间间隔是带宽的计算频率 （毫秒）。公制时间间隔是数据可用于流量计算的时间段。

本部分包括以下主题：

服务质量实例

以下示例显示了如何收集并计算服务质量信息：

服务器的公制时间间隔为 30 秒。

服务器在 0 秒启动。

在 1 秒时，至 / 自该服务器的 HTTP 连接产生了 5000 字节的流量。

之后没有进行更多连接。在 30 秒时，最后 30 秒内的总流量为 5000 字节。

在 32 秒时，在 1 秒时获得的流量采样数据被放弃，因为已经超过了 30 秒的公制时间间隔。现在，最后 30 秒的总流量为 0。

重新计算时间间隔的工作方式与此类似。服务器的重新计算时间间隔为 100 毫秒。

我们继续前面的示例，每隔 100 毫秒重新计算一次带宽。该计算以流量和公制时间间隔为基础。

在 0 秒时，将首次计算带宽。总流量为 0，除以 30 秒的公制时间间隔，得出带宽为 0。

在 1 秒时，将第 10 次 （1000 毫秒 /100 毫秒）计算带宽。总流量为 5000 字节，除以 30 秒，得出带宽为 5000/30 = 166 字节 / 秒。

在 30 秒时，将第 300 次计算带宽。总流量为 5000 字节，除以 30 秒，得出带宽为 5000/30 = 166 字节 / 秒。

在 32 秒时，将第 320 次计算带宽。现在流量为 0 （因为产生流量的那次连接发生的时间太早，所以不能计算在内），除以 30 秒，得出带宽为 0 字节 / 秒。

设置服务质量

要为服务器实例或虚拟服务器的某个类配置服务质量设置，您需要通过用户界面配置这些设置。要实际施行服务质量设置，您还必须在 obj.conf 文件中设置服务器应用程序函数 (SAF)。

要配置服务质量，请执行以下步骤：

1. 在 Server Manager 中，单击 “Monitor”选项卡。
2. 单击 “Quality of Service”。

   将显示一个页面，其中列出了服务质量的常规设置，下面还有一个列表，列出了作为一个整体的服务器实例以及虚拟服务器的每个类。
3. 要为整个服务器实例启用服务质量，请单击 “Enable”。

   缺省情况下，服务质量被启用。启用服务质量会略微增加服务器的负担。
4. 选择 “Recompute Interval”。

   重新计算时间间隔是所有服务器、类及虚拟服务器的每次带宽计算之间的毫秒数。缺省值为 100 毫秒。
5. 选择 “Metric Interval”。

   公制时间间隔是测量其间流量的时间间隔 （秒）。缺省值为 30 秒。此时间段内测量的所有带宽将被平均以得出每秒的字节数。

   如果站点中要传输很多大型文件，请在此字段中使用较大的值 （几分钟或更长时间）。如果公制时间间隔较短，大量文件的传输可能会占用所允许的所有带宽。如果您强制了最大带宽设置，这将导致连接被拒绝。由于带宽是按公制时间间隔均分的，因此较长的时间间隔可以缓和由大量文件引起的高峰流量。

   如果带宽限制比可用带宽低很多 （例如，带宽限制为 1 MB/ 秒，但是与主干的连接为 1 GB/ 秒），则应缩短公制时间间隔。

   请注意，如果传输很大的静态文件，而带宽限制又远远低于可用带宽，则需要确定要优化前者还是后者，因为两者的解决方案恰好相反。
6. 为服务器实例和 / 或虚拟服务器类启用服务质量。

   屏幕的底部列出了服务器实例和服务器类。在要为其启用服务质量的项的旁边，选择 “Enable”操作。
7. 设置最大带宽 （字节 / 秒）。

8. 选择是否强制最大带宽设置。

   如果选择强制最大带宽，当服务器达到其带宽限制时，额外的连接将被拒绝。

   如果没有强制最大带宽，当超过最大值时，服务器将在错误日志中记录一条消息。

9. 选择允许的最大连接数。

   该数值是处理的并行请求数。

10. 选择是否强制最大连接数设置。

    如果选择强制最大连接数，当服务器达到其限制时，额外的连接将被拒绝。

11. 如果没有强制最大连接数，当超过最大值时，服务器将在错误日志中记录一条消息。

12. 单击“OK”。

需要对 obj.conf 进行的更改

要启用服务质量，您必须在 `obj.conf` 中包含指令以调用两个服务器应用程序函数 (SAF)：AuthTrans `qos-handler` 和 Error `qos-error`。

要能够正常工作，`qos-handler` AuthTrans 指令必须是在缺省对象中配置的第一个 `AuthTrans`。服务质量处理程序的作用是检查虚拟服务器、虚拟服务器类以及整个服务器的当前统计数据并通过返回错误来强制限制。

Sun ONE Web Server 包含一个称为 `qos-handler` 的内置样例服务质量处理程序 SAF。当达到限制时，此 SAF 将进行记录并向服务器返回一个 503 “Server busy” 错误，以便由 NSAPI 处理。

Sun ONE Web Server 还包含一个称为 `qos-error` 的内置样例错误 SAF，它将返回一个错误页面，说明引起 503 错误的限制以及触发该限制的统计数据的值。您可以更改样例代码以提供不同的错误信息。

可以在 *server_root*`/plugins/nsapi/examples/qos.c` 处获得这些样例。您可以使用这些样例，以可以编写自己的 SAF。

有关这些 SAF 以及如何使用它们的详细信息，请参见 Sun ONE Web Server 6.1 *NSAPI Programmer's Guide*。

服务质量的已知限制

使用服务质量功能时，请记住以下限制：

- 由于性能的原因，不能在服务器进程之间共享连接或带宽统计数据。也就是说，没有考虑 `MaxProc` 设置。因此，所有限制都单独应用于某个服务器进程，而非所有进程的集合。有关 `MaxProcs` 和多进程的详细信息，请参见 Sun ONE Web Server 6.1 *Performance Tuning, Sizing, and Scaling Guide*。
- 服务质量功能仅测量应用程序级别的 HTTP 带宽。由于以下多种原因， HTTP 带宽可能与实际的 TCP 网络带宽不同：
  - 如果启用了 SSL，则握手和客户机证书交换将添加到流量中，但是不会被测量。
  - 如果单向或双向启用了块编码，则块层将删除块标头，并且块标头不会计算在流量中。其他标头或协议项将被计算。
- 服务质量功能不能精确测量 `PR_TransmitFile` 调用的流量。对于诸如 `PR_Send()/net_write` 或 `PR_Recv()/net_read` 等基本 I/O 操作，带宽管理器可以快速计算出传输的数据，因为在一个系统调用中传输的字节数通常即是缓冲区的大小，并且 I/O 调用会快速返回。这非常适用于测量动态内容应用程序的即时带宽。但是，因为 `PR_TransmitFile` 传输的数据量仅在传输结束时才会知道，所以在传输完成前无法进行测量。

  如果 `PR_TransmitFile` 很短，则服务质量功能将能够充分执行。但是，如果 `PR_TransmitFile` 很长，例如在拨号用户下载长文件的情况下，传输的全部数据量将在完成时计算。当带宽管理器在下一个重新计算时间间隔开始后重新计算带宽时，由于最近发生的这一较大的 `PR_TransmitFile`，计算的带宽将显著增加。这种状况可能导致服务器拒绝所有请求，直至下一个公制时间间隔。那时带宽管理器将使该传输文件操作 “过期”（因为它发生的时间已经太早），从而使带宽值回落。如果您的站点要下载很长的静态文件，您应当增加原来缺省为 30 秒的公制时间间隔。
- 计算的带宽始终是一个近似值，因为它不是即时测量的，而是在一段时间内以固定的时间间隔计算的。例如，如果公制时间间隔是缺省的 30 秒，而服务器空闲了 29 秒，然后在下一秒中，客户机有可能在 1 秒内使用了 30 倍的带宽限制。
- 无论何时动态重新配置了服务器，都将丢失服务质量带宽统计数据。此外，服务质量限制在具有基于较早的、非活动配置的连接的线程中不会被强制，因为带宽管理器线程仅计算活动配置的带宽统计数据。还有一种潜在可能，即长时间未关闭其套接字并保持活动 （从而服务器没有使其超时）的客户机在动态重新配置服务器后不会再受服务质量限制的约束。

- 虚拟服务器的并行连接计算间隔与虚拟服务器类和整个服务器实例的计算间隔不同。单个虚拟服务器的连接计数器在请求被分析并路由到虚拟服务器后会立即自动递增，而在该请求的响应处理结束时会自动减少。这意味着虚拟服务器的连接统计数据在任意时刻都是准确的。

  但是，虚拟服务器类和整个服务器实例的连接统计数据不能即时更新。它们按照每个重新计算时间间隔由带宽管理器线程更新。虚拟服务器类的连接数是该类的所有虚拟服务器上的连接总数；整个服务器实例的连接数是所有虚拟服务器类上的连接总数。

  由于这些值的计算方式，虚拟服务器的连接数始终是正确的 （如果强制了一个连接数限制，则永远也不会超过该限制）；虚拟服务器类和服务器实例的值则不会如此准确，因为它们只是按照一定的时间间隔计算的。

SNMP 基本原理

SNMP 是用于交换有关网络活动的数据的协议。利用 SNMP，可以在被管理的设备和网络管理站 (NMS) 之间传输数据。被管理的设备即运行 SNMP 的任何设备：主机、路由器、 Web 服务器和网络上的其他服务器。 NMS 是用于远程管理网络的计算机。NMS 软件通常提供图像来显示收集的数据，或使用这些数据确保服务器在特定的参数值范围内运行。

NMS 通常是安装有一个或多个网络管理应用程序的功能强大的工作站。网络管理应用程序 （例如 HP OpenView）以图形方式显示有关被管理设备 （例如 Web 服务器）的信息。例如，它可能显示您的企业中服务器的打开或关闭情况，或者收到的错误消息的数量和类型。将 SNMP 与 Sun ONE 服务器一起使用时，这些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。

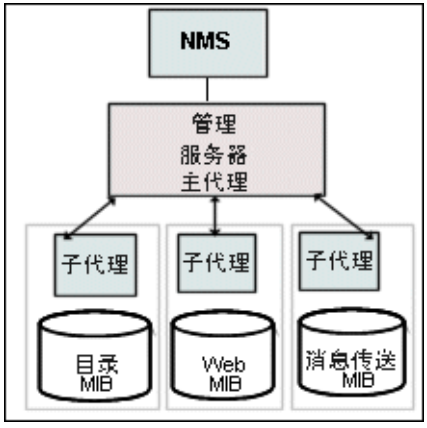
子代理收集有关服务器的信息并将信息传递给服务器的主代理。每个 Sun ONE 服务器 （除 Administration Server 外）都具有子代理。

注 对 SNMP 配置进行任何更改后，必须单击 “Apply”按钮，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、 Sun ONE Web Server 及 Messaging Server，则每个服务器的子代理将与同一个主代理通信，如下所示：

网络管理站和 SNMP 代理

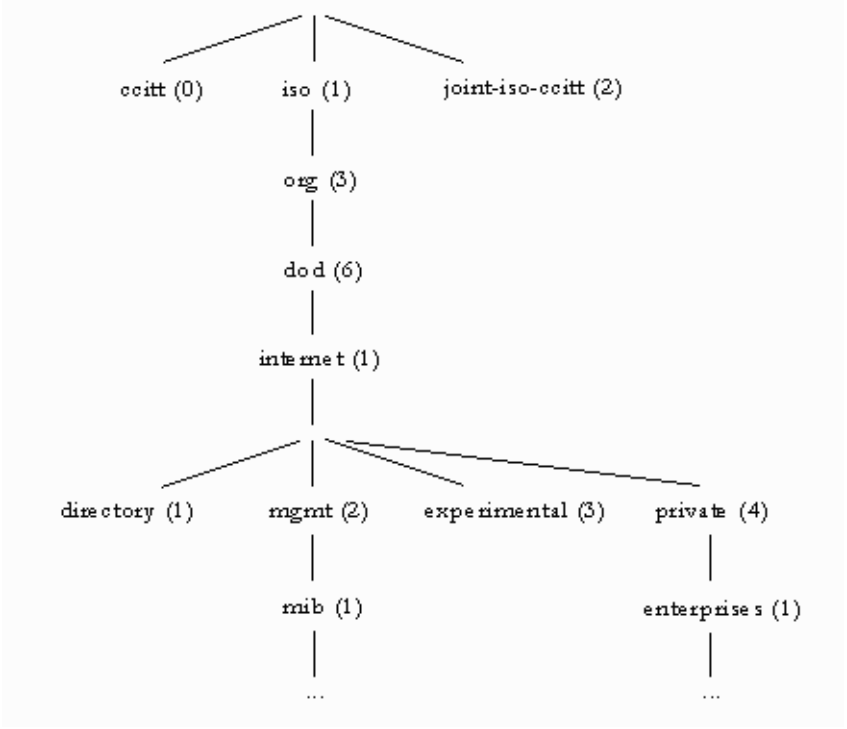


Sun ONE Web Server MIB

Sun ONE Web Server 存储了与网络管理有关的变量。主代理可以访问的变量称为被管理对象。这些对象在称为管理信息库 (MIB) 的树状结构中定义。 MIB 提供了对 Web 服务器的网络配置、状态和统计数据的访问。使用 SNMP 可以从网络管理工作站 (NMS) 查看此信息。

服务器的 MIB 包含有关该特定服务器的网络管理的变量定义。下图显示了 MIB 树的顶层。

MIB 树的顶层



MIB 树的顶层显示出 Internet 对象标识符具有四个子树：directory (1)、 mgmt (2)、experimental (3) 和 private (4)。 private (4) 子树包含 enterprises (1) 节点。 enterprises (1) 节点中的每个子树都被分配给一个单独的企业，企业是注册有自己特定 MIB 扩展的组织。然后，企业可以在其子树下创建特定产品的子树。由企业创建的 MIB 位于 enterprises (1) 节点下。 Sun ONE MIB 位于 enterprises (1) 节点下。

每个 Sun ONE 服务器子代理都提供了一个用于 SNMP 通信的 MIB。服务器通过发送包含这些变量的消息 （或陷阱）将重要事件报告给网络管理站 (NMS)。 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 ONE 服务器都有其自己的管理信息库 (MIB)。所有 Sun ONE MIB 都位于：

server_root`/plugins/snmp`

Sun ONE Web Server 的 MIB 是一个名为 `webserv61.mib` 的文件。此 MIB 包含与 Sun ONE Web Server 的网络管理有关的各种变量的定义。

Sun ONE Web Server 6.1 MIB 具有一个对象标识符 `http 60 (iws60 OBJECT IDENTIFIER ::= {http 60 })`，它位于 *server_root*`/plugins/snmp` 目录下。

您可以使用 Sun ONE Web Server MIB 查看有关 Web 服务器的管理信息并实时监视服务器。表 11-1 列出并说明了存储在 `webserv61.mib` 中的被管理对象。

表 11-1 `webserv61.mib` 被管理对象和说明

被管理对象	说明
iwsInstanceTable	Sun ONE Web Server 实例。
iwsInstanceEntry	Sun ONE Web Server 实例。
iwsInstanceIndex	服务器实例索引。
iwsInstanceId	服务器实例标识符。
iwsInstanceVersion	字符串，例如 `SunONE-WebServer/6.1 BB1-01/24/2001 17:15 (SunOS DOMESTIC)`。
iwsInstanceDescription	服务器实例的说明。
iwsInstanceOrganization	负责服务器实例的组织。
iwsInstanceContact	负责服务器实例的人员的联系信息。
iwsInstanceLocation	服务器的位置。
iwsInstanceStatus	服务器实例的状态。
iwsInstanceUptime	服务器已经运行的时间。
iwsInstanceDeathCount	服务器实例进程关闭的次数。
iwsInstanceRequests	服务器实例处理的请求数。
iwsInstanceInOctets	服务器实例接收的八位字节数。如果此信息不可用，将显示 0。
iwsInstanceOutOctets	服务器实例传输的八位字节数。如果此信息不可用，将显示 0。
iwsInstanceCount2xx	服务器实例发出的 200 级 （成功）响应的数目。
iwsInstanceCount3xx	服务器实例发出的 300 级 （重定向）响应的数目。
iwsInstanceCount4xx	服务器实例发出的 400 级 （客户机错误）响应的数目。

表 11-1 webserv61.mib 被管理对象和说明 （接上页）

被管理对象	说明
iwsInstanceCount5xx	服务器实例发出的 500 级 （服务器错误）响应的数目。
iwsInstanceCountOther	服务器实例发出的其他 （非 2xx、 3xx、 4xx 或 5xx）响应的数目。
iwsInstanceCount200	服务器实例发出的 200 （请求已满足）响应的数目。
iwsInstanceCount302	服务器实例发出的 302 （暂时移动）响应的数目。
iwsInstanceCount304	服务器实例发出的 304 （未修改）响应的数目。
iwsInstanceCount400	服务器实例发出的 400 （错误请求）响应的数目。
iwsInstanceCount401	服务器实例发出的 401 （未授权）响应的数目。
iwsInstanceCount403	服务器实例发出的 403 （禁止）响应的数目。
iwsInstanceCount404	服务器实例发出的 404 （未找到）响应的数目。
iwsInstanceCount503	已发出的 503 （不可用）响应的数目。
iwsVsTable	Sun ONE Web Server 虚拟服务器。
iwsVsEntry	Sun ONE Web Server 虚拟服务器。
iwsVsIndex	虚拟服务器索引。
iwsVsId	虚拟服务器标识符。
iwsVsRequests	虚拟服务器处理的请求数。
iwsVsInOctets	虚拟服务器接收的八位字节数。
iwsVsOutOctets	虚拟服务器传输的八位字节数。
iwsVsCount2xx	虚拟服务器发出的 200 级 （成功）响应的数目。
iwsVsCount3xx	虚拟服务器发出的 300 级 （重定向）响应的数目。
iwsVsCount4xx	虚拟服务器发出的 400 级 （客户机错误）响应的数目。

表 11-1 webserv61.mib 被管理对象和说明 （接上页）

被管理对象	说明
iwsVsCount5xx	虚拟服务器发出的 500 级 （服务器错误）响应的数目。
iwsVsCountOther	虚拟服务器发出的其他 （非 2xx、 3xx、 4xx 或 5xx）响应的数目。
iwsVsCount200	虚拟服务器发出的 200 （请求已满足）响应的数目。
iwsVsCount302	虚拟服务器发出的 302 （暂时移动）响应的数目。
iwsVsCount304	虚拟服务器发出的 304 （未修改）响应的数目。
iwsVsCount400	虚拟服务器发出的 400 （错误请求）响应的数目。
iwsVsCount401	虚拟服务器发出的 401 （未授权）响应的数目。
iwsVsCount403	虚拟服务器发出的 403 （禁止）响应的数目。
iwsVsCount404	虚拟服务器发出的 404 （未找到）响应的数目。
iwsVsCount503	已发出的 503 （不可用）响应的数目。
iwsProcessTable	Sun ONE Web Server 进程。
iwsProcessEntry	Sun ONE Web Server 进程。
iwsProcessIndex	进程索引。
iwsProcessId	操作系统进程标识符。
iwsProcessThreadCount	请求处理线程的数目。
iwsProcessThreadIdle	当前处于空闲状态的请求处理线程数。
iwsProcessConnectionQueueCount	连接队列中的当前连接数。
iwsProcessConnectionQueuePeak	同时排队的最大连接数。
iwsProcessConnectionQueueMax	连接队列中所允许的最大连接数。
iwsProcessConnectionQueueTotal	已接受的连接数。
iwsProcessConnectionQueueOverflows	由于连接队列溢出而被拒绝的连接数。
iwsProcessKeepaliveCount	保持活动的队列中的当前连接数。
iwsProcessKeepaliveMax	保持活动的队列中所允许的最大连接数。

表 11-1 webserv61.mib 被管理对象和说明 （接上页）

被管理对象	说明
iwsProcessSizeResident	进程驻留大小 （千字节）。
iwsProcessSizeVirtual	进程大小 （千字节）。
iwsProcessFractionSystemMemoryUsage	进程内存在系统内存中所占比例。
iwsListenTable	Sun ONE Web Server 侦听套接字。
iwsListenEntry	Sun ONE Web Server 侦听套接字。
iwsListenIndex	侦听套接字索引。
iwsListenId	侦听套接字标识符。
iwsListenAddress	套接字侦听的地址。
iwsListenPort	套接字侦听的端口。
iwsListenSecurity	加密支持。
iwsThreadPoolTable	Sun ONE Web Server 线程池。
iwsThreadPoolEntry	Sun ONE Web Server 线程池。
iwsThreadPoolIndex	线程池索引。
iwsThreadPoolID	线程池标识符。
iwsThreadPoolCount	排队的请求数。
iwsThreadPoolPeak	同时排队的最大请求数。
iwsThreadPoolMax	队列中所允许的最大请求数。
iwsInstanceStatusChange	iwsInstanceStatusChange 陷阱表示 iwsInstanceStatus 已经更改。
iwsInstanceLoad1MinuteAverage	1 分钟内的系统负载平均值。
iwsInstanceLoad5MinuteAverage	5 分钟内的系统负载平均值。
iwsInstanceLoad15MinuteAverage	15 分钟内的系统负载平均值。
iwsInstanceNetworkInOctets	网络上每秒传输的八位字节数。
iwsInstanceNetworkOutOctets	网络上每秒接收的八位字节数。
iwsCpuIndex	CPU 索引。
iwsCpuId	CPU ID。
iwsCpuIdleTime	CPU 空闲时间。
iwsCpuUserTime	CPU 用户时间。
iwsCpuKernelTime	CPU 内核时间。

设置 SNMP

一般来讲，要使用 SNMP，系统上必须安装了一个主代理和至少一个子代理，并且正在运行。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。表 8.1 概述了在不同情况下所要执行的过程。本章后面将对实际过程进行详细介绍。

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？ （如果您使用的是 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 服务或重新引导计算机。
- (UNIX) 使用 Administration Server 重新启动 SNMP 主代理。

表 11-2 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. 安装代理 SNMP Agent。 2. 启动主代理。 3. 启动代理 SNMP Agent。 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。

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。
• 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。

使用代理 SNMP Agent (UNIX/Linux)

如果已经运行了一个本地代理，并且希望将它与一个 Sun ONE Web Server 主代理一起并行使用，则需要使用一个代理 SNMP Agent。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，您需要安装并启动它。还必须使用 Sun ONE Web Server 主代理在其上运行的端口号以外的其他端口号来重新启动本地 SNMP 主代理。

本部分包括以下主题：

安装代理 SNMP Agent

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：

1. 安装 SNMP 主代理。请参见 “第 252 页上的 “安装 SNMP 主代理””。
2. 安装并启动代理 SNMP Agent，然后重新启动本地 SNMP 守护程序。请参见 “第 250 页上的 “使用代理 SNMP Agent (UNIX/Linux)””。
3. 启动 SNMP 主代理。请参见 “第 253 页上的 “启用和启动 SNMP 主代理””。
4. 启用子代理。请参见 “第 258 页上的 “启用子代理””。

要安装代理 SNMP Agent，请编辑位于服务器根目录下的 `plugins/snmp/sagt` 中的 `CONFIG` 文件（您可以为此文件指定其他名称），以使其包含 SNMP 守护程序要侦听的端口。其中还需要包括代理 SNMP Agent 要转发的 MIB 树和陷阱。

下面是一个 `CONFIG` 文件示例：

```
AGENT AT PORT 1161 WITH COMMUNITY public
SUBTREES 1.3.6.1.2.1.1,
        1.3.6.1.2.1.2,
        1.3.6.1.2.1.3,
        1.3.6.1.2.1.4,
        1.3.6.1.2.1.5,
        1.3.6.1.2.1.6,
        1.3.6.1.2.1.7,
        1.3.6.1.2.1.8
FORWARD ALL TRAPS;
```

启动代理 SNMP Agent

要启动代理 SNMP Agent，请在命令提示符下输入：

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

重新启动本地 SNMP 守护程序

启动代理 SNMP Agent 后，您需要在 `CONFIG` 文件中指定的端口重新启动本地 SNMP 守护程序。要启动本地 SNMP 守护程序，请在命令提示符下输入：

```
# snmpd -P port_number
```

其中 *port_number* 是在 `CONFIG` 文件中指定的端口号。例如，在 Solaris 平台上，使用前面提到的 `CONFIG` 文件实例中的端口，您需要输入：

```
# snmpd -P 1161
```

重新配置 SNMP 本地代理

如果 SNMP 守护程序运行在 AIX 上，则它支持 SMUX。因此，您无需安装主代理。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。需要更改 `snmpd.conf` （其中一个配置文件）以使 SNMP 守护程序接受从 SMUX 子代理传入的消息。有关详细信息，请参见 `snmpd.conf` 的联机手册页。您需要添加一行以定义每个子代理。

例如，您可以将此行添加到 `snmpd.conf` 中：

```
smux 1.3.6.1.4.1.1.1450.1 "" IP_address net_mask
```

IP_address 是运行子代理的主机的 IP 地址， *net_mask* 是该主机的网络掩码。

注 请勿使用回送地址 127.0.0.1 ；而应使用实际的 IP 地址。

安装 SNMP 主代理

要配置 SNMP 主代理，您必须以 `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 SNMP 任务 （例如 MIB 浏览）。

要使用 Server Manager 安装 SNMP 主代理，请执行以下步骤：

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 4 步。

   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。
3. 如果运行有 SNMP 守护程序，请结束它的进程。
4. 在 Server Manager 中，从 “Global Settings”选项卡中选择 “SNMP Master Agent Trap”页面。将显示 “Manager Entries”页面。
5. 键入正在运行网络管理软件的系统的名称。

6. 键入网络管理系统用来侦听陷阱的端口号。（常用的端口是 162。）有关陷阱的详细信息，请参见第 258 页上的 “配置陷阱目标”。
7. 键入要在陷阱中使用的社区字符串。有关社区字符串的详细信息，请参见第 258 页上的 “配置社区字符串”。
8. 单击 “OK”。
9. 在 Server Manager 中，从 “Global Settings”选项卡中选择 “SNMP Master Agent Community”页面。将显示 “Community Strings”页面。
10. 键入主代理的社区字符串。
11. 选择社区的操作。
12. 单击 “OK”。

启用和启动 SNMP 主代理

主代理操作在名为 `CONFIG` 的代理配置文件中进行了定义。您可以使用 Server Manager 编辑 `CONFIG` 文件，也可以手动编辑该文件。要启用 SNMP 子代理，必须先安装 SNMP 主代理。

如果在重新启动主代理时出现类似于 “System Error: Could not bind to port”的绑定错误，请使用 `ps -ef | grep snmp` 检查 `magt` 是否在运行。如果正在运行，请使用 `kill -9` *`pid`* 命令结束该进程。然后， SNMP 的 CGI 将重新开始工作。

本部分包括以下主题：

- 在其他端口上启动主代理
- 手动配置 SNMP 主代理
- 编辑主代理的 CONFIG 文件
- 定义 sysContact 和 sysLocation 变量
- 配置 SNMP 主代理
- 启动 SNMP 主代理

在其他端口上启动主代理

管理界面只能在 161 端口上启动 SNMP 主代理。但是，您可以使用以下步骤在其他端口上手动启动主代理：

1. 编辑 /*server_root*/plugins/snmp/magt/CONFIG 以指定所希望的端口。
2. 运行以下启动脚本：

   ```
   cd /server_root/https-admserv

   ./start -shell /server_root/plugins/snmp/magt/magt

   /server_root/plugins/snmp/magt/CONFIG

   /server_root/plugins/snmp/magt/INIT
   ```

然后，主代理将在所希望的端口上启动。但是，用户界面能够检测出主代理正在运行。

手动配置 SNMP 主代理

要手动配置 SNMP 主代理，请执行以下步骤：

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。然后结束它的进程。
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

CONFIG 文件定义了将与主代理一起工作的社区和管理器。管理器的值应当是有效的系统名称或 IP 地址。

下面是一个基本 CONFIG 文件的示例：

```
COMMUNITY           public
                    ALLOW ALL OPERATIONS

MANAGER             manager_station_name
                    SEND ALL TRAPS TO PORT 162
                     WITH COMMUNITY public
```

定义 sysContact 和 sysLocation 变量

您可以编辑 CONFIG 文件，为指定了 sysContact 和 sysLocation MIB-II 变量的 sysContact 和 sysLocation 添加初始值。此示例中 sysContact 和 sysLocation 的字符串放在了引号内。任何包含空格、换行符、制表符等的字符串都必须放在引号内。您也可以用十六进制记数法来指定值。

下面是一个 CONFIG 文件示例，其中定义了 sysContract 和 sysLocation 变量：

```
COMMUNITY           public
                    ALLOW ALL OPERATIONS

MANAGER             nms2
                    SEND ALL TRAPS TO PORT 162
                    WITH COMMUNITY public

INITIAL             sysLocation "Server room
501 East Middlefield Road
Mountain View, CA 94043
USA"

INITIAL             sysContact "John Doe
email:jdoe@netscape.com"
```

配置 SNMP 子代理

您可以配置 SNMP 子代理以监视服务器。

要配置 SNMP 子代理，请执行以下步骤：

1. 在 Administration Server 中，选择服务器实例并单击 “Manage”。
2. 选择 “Monitor”选项卡。
3. 选择 “SNMP Subagent Configuration”。
4. （只适用于 UNIX）在 “Master Host”字段中，输入服务器的名称和域。
5. 输入服务器的说明，包括操作系统信息。
6. 输入负责该服务器的组织。
7. 在 “Location”字段中，输入服务器的绝对路径。
8. 在 “Contact”字段中，输入负责该服务器的人员的姓名和联系信息。
9. 选择 “On”启用 SNMP 统计数据收集。
10. 单击 “OK”。
11. 单击 “Apply”。
12. 选择 “Apply Changes”重新启动服务器，使更改生效。

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，请在命令提示符下输入以下内容：

```
# magt CONFIG INIT&
```

INIT 文件是包含 MIB-II 系统组信息 （包括系统位置和联系信息）的非易失性文件。如果 INIT 不存在，首次启动主代理时将创建它。如果 CONFIG 文件中的管理器名称无效，将导致主代理启动失败。

要在非标准端口上启动主代理，请使用以下两种方法之一：

方法一：在 CONFIG 文件中，为主代理用来侦听来自管理器的 SNMP 请求的每个接口指定传输映射。传输映射允许主代理接受标准端口和非标准端口上的连接。主代理还可以在非标准端口上接受 SNMP 通信。并行 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。下面是一个传输映射条目示例：

```
TRANSPORT          extraordinary   SNMP
                   OVER UDP SOCKET
                    AT PORT 11161
```

手动编辑 CONFIG 文件后，您应当在命令提示符下键入以下内容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

要使用 Administration Server 启动 SNMP 主代理，请执行以下步骤：

1. 登录 Administration Server。
2. 在 Server Manager 中，从 “Global Settings”选项卡中选择 “SNMP Master Agent Control”页面。将显示 “SNMP Master Agent Control”页面。
3. 单击 “Start”。

   您还可以在 “SNMP Master Agent Control”页面中停止和重新启动 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，您需要配置主机的 Administration Server。这要求指定社区字符串和陷阱目标。

配置社区字符串

社区字符串是 SNMP 代理用来进行授权的文本字符串。这意味着网络管理站在发送给代理的每条消息中都带有一个社区字符串。然后，代理就可以验证网络管理站是否被授权获取信息。社区字符串在 SNMP 包中发送时没有被隐藏；字符串以 ASCII 文本格式发送。

您可以在 Server Manager 的 “Community Strings”页面中为 SNMP 主代理配置社区字符串。还可以定义特定社区所能执行的与 SNMP 相关的操作。在 Server Manager 中，您还可以查看、编辑和删除已配置的社区。

配置陷阱目标

SNMP 陷阱是 SNMP 代理发送给网络管理站的消息。例如，当接口的状态由打开变为关闭时， SNMP 代理将发送一个陷阱。 SNMP 代理必须知道网络管理站的地址，以便知道向何处发送陷阱。您可以通过 Sun ONE Web Server 为 SNMP 主代理配置陷阱目标。还可以查看、编辑并删除已配置的陷阱目标。使用 Sun ONE Web 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。有关安装主代理的详细信息，请参见第 252 页上的 “安装 SNMP 主代理”。您可以使用 Server Manager 启用子代理。

要在 UNIX/Linux 平台上停止 SNMP 功能，您必须先停止子代理，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 “SNMP Subagent Configuration”页面，然后在 “SNMP Subagent Control”页面中启动子代理。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，您可以通过 “SNMP Subagent Control”页面或 Windows 的服务控制面板来启动、停止或重新启动子代理。

注	对 SNMP 配置进行任何更改后，必须单击 “Apply”按钮，然后重新启动 SNMP 子代理。

了解 SNMP 消息

GET 和 SET 是 SNMP 定义的两种消息。GET 和 SET 消息由网络管理站 (NMS) 发送给主代理。您可以通过 Administration Server 使用其中一个或两个都使用。

SNMP 以协议数据单元 (PDU) 的格式交换网络信息。这些单元包含有关存储在被管理设备 （例如 Web 服务器）上的变量的信息。这些变量 （也称为被管理对象）具有值和标题，值和标题将在需要时报告给 NMS。由服务器发送给 NMS 的协议数据单元称为 “陷阱”。以下实例显示了 GET、 SET 和 “陷阱”消息的使用。

NMS 启动的通信。NMS 将从服务器请求信息，或者更改存储在服务器 MIB 中的变量的值。例如：

1. NMS 将消息发送给 Administration Server 主代理。消息可能是数据请求 （一条 GET 消息），也可能是在 MIB 中设置变量的说明 （一条 SET 消息）。
2. 主代理将消息转发给相应的子代理。
3. 子代理将检索数据或更改 MIB 中的变量。
4. 子代理将数据或状态报告给主代理，然后主代理将消息 （一条 GET 消息）转发回 NMS。
5. NMS 通过其网络管理应用程序以文字或图形方式显示该数据。

服务器启动的通信。发生重要事件时，服务器子代理将向 NMS 发送一条消息 （或 “陷阱”）。例如：

1. 子代理通知主代理服务器已停止。
2. 主代理发送一条消息 （或 “陷阱”），将该事件报告给 NMS。
3. NMS 通过其网络管理应用程序以文字或图形方式显示该信息。

第 12 章

配置命名和资源

基于组件的 Java™ 2 Platform, Enterprise Edition (J2EE™) 技术为 Web 服务提供了一个可简化企业开发和部署的框架结构。

本章介绍 Sun ONE Web Server 提供的 J2EE 资源并讨论用于创建和管理这些资源的方法。

有关 Java 安全性和基于区域的验证的信息，请参见第 4 章 “用于 Web 容器和 Web 应用程序的 基于 J2EE 的安全性”。

本章包括以下部分：

启用和禁用 Java

您可以全局 （即基于每个 Sun ONE Web Serve 实例）启用或禁用 Java，也可以为特定的虚拟服务器类启用或禁用 Java。默认情况下， Sun ONE Web Server 中启用了 Java，且在 `magnus.conf` 文件中添加了以下行：

```
Init fn="load-modules"
shlib="<server-root>/bin/https/lib/libj2eeplugin.so"
```

您也可以为特定的虚拟服务器启用 Java。执行此操作时，服务器将用所需的 J2EE 指令为该虚拟服务器类更新 `obj.conf` 文件。

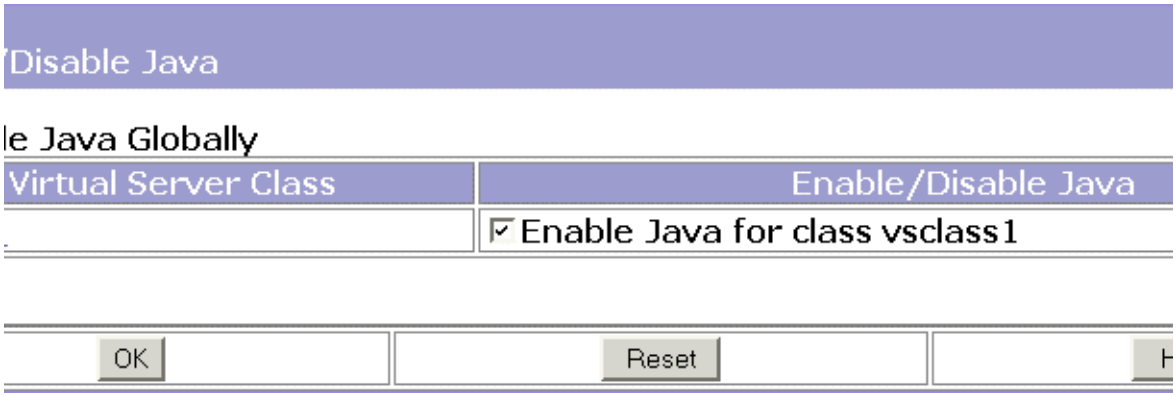
有关 `obj.conf` 和 `magnus.conf` 文件的详细信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference* 和 Sun ONE Web Server 6.1 *NSAPI Programmer's Guide*。

在某些情况下，您可能希望全局禁用 Java 或为特定的虚拟服务器类禁用 Java，例如，当整个服务器或该类仅提供静态内容时。

要启用或禁用 Java，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java”选项卡。
2. 单击 “Enable/Disable Servlets/JSP”。

   “Enable/Disable Servlets/JSP”界面



3. 要全局启用或禁用 Java，请选中或取消选中 “Enable/Disable Java Globally”。

   或者

   要为特定虚拟服务器类启用或禁用 Java，请选中或取消选中与该虚拟服务器类相对应的 “Enable/Disable Java”复选框。
4. 单击 “OK”。

配置 JVM 设置

与本产品以前的版本不同，Sun ONE Web Server 6.1 不再支持独立的 Java 运行时环境 (JRE)。相反，该服务器要求使用 JDK 1.4.1 或更高版本。安装服务器时，如果选择缺省的 JDK 选项， Java 开发工具 (JDK) 1.4.1_03 将安装在 *<server-root>*`/bin/https/jdk` 目录下。

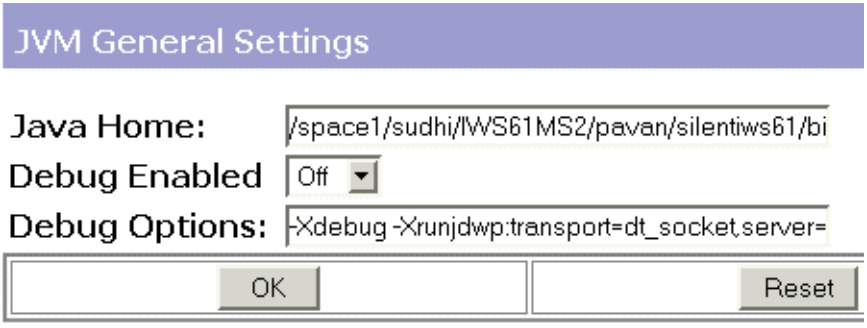
您可以为服务器实例配置 Java 虚拟机 (JVM) 设置。这些设置包括 Java 主页的位置、编译程序选项、调试选项和事件探查器信息。配置这些设置的原因之一是为了改善性能。有关性能的详细信息，请参见 Sun ONE Web Server 6.1 *Performance Tuning, Sizing, and Scaling Guide*。

配置常规设置

要编辑 JDK 的位置和指定调试选项，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java”选项卡。
2. 单击 “JVM General”。

   “JVM General”界面



3. 设置 “Java Home”。

   “Java Home”是 Java 开发工具 (JDK) 安装目录的路径。Sun ONE Web Server 支持 Sun JDK 1.4.1_03。
4. 选择是否启用调试并设置调试选项。

   调试选项的列表位于以下位置：
   `http://java.sun.com/products/jpda/doc/conninv.html#Invocation`
5. 单击 “OK”。

配置路径设置

出于某种原因，您可能要配置 JVM 的路径设置。例如，您可能要为系统的类路径选择一个后缀以覆盖系统类 （例如 XML 解析器类），或者可能要忽略环境类路径以防止环境变量对生产环境产生不利影响。

要在管理界面中配置 JVM 的路径设置，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java”选项卡。
2. 单击 “JVM Path Settings”。
3. 为系统的类路径选择后缀。
4. 选择是否忽略环境类路径。

   如果不忽略类路径，系统将读取 `CLASSPATH` 环境变量并将其附加到 Sun ONE Web Server 类路径。 `CLASSPATH` 环境变量添加到 `classpathsuffix` 的后面，即最后端。

   对于开发环境，应当使用类路径。对于生产环境，应当忽略类路径以防止环境变量产生不利的影响。
5. 设置本地库路径的前缀和后缀。

   本地库路径是自动生成的以下各项的合成，即 Web 服务器安装的本地共享库的相对路径、标准 JRE 本地库路径、 shell 环境设置 （UNIX 上的 `LD_LIBRARY_PATH`）以及在 `profiler` 元素中指定的任何路径。由于这是一个合成的路径，因此不会明确显示在服务器配置中。
6. 单击 “OK”。

配置 JVM 选项

要在管理界面中设置 JVM 命令行选项，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java”选项卡。
2. 单击 “JVM Options”并进行所需的更改。

   关于特定 JVM 选项的信息，请参见：

   `http://java.sun.com/docs/hotspot/VMOptions.html`
3. 单击 “OK”。

配置 JVM 事件探查器

您可以使用事件探查器在 Sun ONE Web Server 上执行远程事件探查，以查找服务器端性能方面的瓶颈。

要在管理界面中配置 JVM 事件探查器，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java” 选项卡。
2. 单击 “JVM Profiler”。
3. 指定类路径、本地库路径以及是否启用事件探查器。
4. 添加、删除或编辑事件探查器的 JVM 选项并单击 “OK”。

有关事件探查器的详细信息，请参见 Sun ONE Web Server 6.1 *Programmer's Guide*。

关于 J2EE 命名服务和资源

Web 应用程序可以访问多种资源，例如资源管理器、数据源 （如 SQL 数据源）、邮件会话和 URL 连接工厂。J2EE 平台通过 Java 命名和目录接口 (JNDI) 服务将这些资源提供给应用程序。

使用 Sun ONE Web Server，您可以创建和管理以下 J2EE 资源：

- JDBC 数据源
- JDBC 连接池
- Java 邮件会话
- 自定义资源
- 外部 JNDI 资源

JDBC 数据源

JDBC 数据源是一种 J2EE 资源，可以使用 Sun ONE Web Server 进行创建和管理。

JDBC API 是用于与关系数据库系统进行连接的 API。 JDBC API 包含两部分：

- 一个应用程序级接口，应用程序组件使用它来访问数据库。
- 一个服务提供者接口，用于将 JDBC 驱动程序连接到 J2EE 平台。

JDBC 数据源对象是用 Java 编程语言实现的数据源。从本质上讲，数据源是一种存储数据的设备。数据源可能像大型公司的综合数据库一样复杂，也可能像仅包含行和列的文件一样简单。 JDBC 数据源是一种 J2EE 资源，可以使用 Sun ONE Web Server 进行创建和管理。

JDBC API 使用标准的 SQL 数据库访问接口为 Java 提供了一组类，可以确保对多种关系数据库的统一访问。

事实上，使用 JDBC 可以将 SQL 语句发送到任何数据库管理系统 (DBMS)。它可以用作关系 DBMS 和对象 DBMS 的接口。

有关创建自定义资源的信息，请参见 “创建 JDBC 资源”。

JDBC 连接池

JDBC 连接池是一个到数据库的 JDBC 连接的命名组。这些连接是在启动 Sun ONE Web Server 时在连接池中首次进行连接请求时创建的。

JDBC 连接池定义了用于创建连接池的特性。每个连接池都使用 JDBC 驱动程序在服务器启动时创建一个到物理数据库的连接。

基于 JDBC 的应用程序或资源从池中提取并使用某个连接；之后，如果不再需要该连接，将通过关闭连接将其返回连接池。如果两个或多个 JDBC 资源指向同一个池定义，它们将在运行时使用相同的连接池。

有关如何创建新 JDBC 连接池的信息，请参见 “创建新的 JDBC 连接池”。

Java 邮件会话

JMS 目标是一种 J2EE 资源，可以使用 Sun ONE Web Server 进行创建和管理。

许多 Internet 应用程序都需要具有发送 Email 通知的能力，因此，J2EE 平台提供了 JavaMail API 以及一个使应用程序组件可以发送 Internet 邮件的 JavaMail 服务提供者。 JavaMail API 包含两部分：

- 一个应用程序级接口，应用程序组件使用它来发送邮件。
- 一个服务提供者接口，在 J2EE API 级别上使用。

JMS 邮件会话是一种 J2EE 资源，可以使用 Sun ONE Web Server 进行创建和管理。

注 Sun ONE Web Server 没有为创建 Java 邮件会话提供 Administration Server 界面。您可以使用命令行界面执行此操作。有关如何使用命令行实用程序创建邮件资源的详细信息，请参见 “创建邮件资源”。

自定义资源

自定义资源可以访问本地 JNDI 系统信息库。 `server.xml` 中定义的 `customresource` 元素提供了一种方法，可用于指定服务器范围的自定义资源对象工厂。这种对象工厂可实现 `javax.naming.spi.ObjectFactory` 接口。此元素将以下各项关联起来，即一个要在服务器范围的名称空间中使用的 JNDI 名称 （像其他 Sun ONE Web Server 资源一样通过 `jndiname` 子元素来指定）、类型、资源工厂类的名称以及一组用于实例化相同特性的标准特性。

您需要确保该资源引用的环境引用已链接到所配置的服务器范围的资源 （这些资源是使用 `server.xml` 中的 `customresource` 和 `externaljndiresource` 标记定义的）。应用程序组件的动态重新部署是一个有关 JNDI 命名环境的问题。 Sun ONE Web Server 将释放所有应用程序的特定引用并将所有新引用重新绑定到新安装的应用程序的命名上下文中。

有关创建自定义资源的信息，请参见 “创建自定义资源”。

外部 JNDI 资源

通常，Sun ONE Web Server 上运行的应用程序需要访问存储在外部 JNDI 系统信息库中的资源。例如，一般的 Java 对象可能会以 Java 模式存储在 LDAP 服务器中。虽然使用自定义资源可以访问本地 JNDI 系统信息库，但是要访问外部 JNDI 信息库，必须使用外部 JNDI 资源。外部 JNDI 工厂必须实现 `javax.naming.spi.InitialContextFactory` 接口。

有关创建外部 JNDI 资源的信息，请参见 “创建外部 JNDI 资源”。

关于 Java 命名和目录接口 (JNDI)

本节介绍 Java 命名和目录接口 (JNDI)。它是一种应用程序编程接口 (API)，用于访问不同类型的命名服务和目录服务。 J2EE 组件通过调用 JNDI 查找方法来找到对象。

本部分包括以下主题：

J2EE 命名服务

JNDI 名称是一种便于用户使用的对象名称。这些名称通过 J2EE 服务器提供的命名和目录服务绑定到其对象。由于 J2EE 组件通过 JNDI API 访问此服务，因而我们通常将某个对象的便于用户使用的名称称为该对象的 JNDI 名称。例如， Oracle 数据库的 JNDI 名称可以是 `jdbc/Oracle`。当它启动时，Sun ONE Web Server 将从配置文件中读取信息并自动将 JNDI 数据库名称添加到名称空间。

应用程序组件的命名环境是一种机制，使用它可以在部署或汇编期间自定义应用程序组件的业务逻辑。使用应用程序组件的环境即可对应用程序组件进行自定义，而无需访问或更改应用程序组件的源代码。

J2EE 容器实现了 Web 应用程序组件的环境并将该环境作为 JNDI 命名上下文提供给应用程序组件实例。 J2EE 应用程序组件的环境的使用方式如下：

- Web 应用程序组件的业务方法使用 JNDI 接口访问该环境。应用程序组件提供者在部署描述符中声明了运行时在环境中要向应用程序组件提供的所有环境条目。
- 容器可实现存储应用程序组件环境的 JNDI 命名上下文。容器还提供了部署者可用于创建和管理每个应用程序组件的环境的工具。
- 部署者可以使用容器提供的工具来初始化应用程序组件的部署描述符中声明的环境条目。部署者可以设置和修改环境条目的值。
- 容器使环境命名上下文在运行时可用于应用程序组件实例。应用程序组件的实例使用 JNDI 接口获取环境条目的值。

每个应用程序组件都定义了其自己的环境条目集合。一个应用程序组件在同一容器内的所有实例将共享相同的环境条目。应用程序组件实例不能在运行时修改环境。

命名引用和绑定信息

资源引用是部署描述符中的一种元素，用于标识该资源的组件的编码名称。更具体地说，编码名称将引用资源的连接工厂。在下节给出的示例中，资源引用名是 `jdbc/SavingsAccountDB`。

资源的 JNDI 名称与资源引用的名称是不同的。使用此命名方法，您需要在进行部署之前先映射这两个名称，但此方法也会将组件与资源分离开。由于这种分离，使得如果组件以后需要访问其他资源，将不必在代码中更改名称。这一灵活性使您可以更容易地由以前存在的组件来汇编 J2EE 应用程序。

下表列出了 Sun ONE Web Server 使用的 J2EE 资源的所推荐的 JNDI 查找及其关联引用。

表 1 JNDI 查找及其关联引用

JNDI 查找名称	关联引用
`java:comp/env`	应用程序环境条目
`java:comp/env/jdbc`	JDBC 数据源资源
`java:comp/env/mail`	JavaMail 会话连接工厂
`java:comp/env/url`	URL 连接工厂

J2EE 标准部署描述符中的命名引用

命名引用是一个字符串，应用程序使用该字符串在给定的命名上下文中查找对象。每个 Web 应用程序都有一个命名上下文，并且其引用在标准组件部署描述符中进行了配置。本节介绍了 Sun ONE Web Server 中使用的标准部署描述符功能。本部分包括以下主题：

- 应用程序环境条目
- 资源引用
- 资源环境引用

应用程序环境条目

环境条目是使用 `<env-entry>` 定义的，可用于为 J2EE Web 应用程序指定部署时间参数。请注意，虽然可以使用 `<context-param>` 来定义 servlet 上下文初始化参数，但 `<env-entry>` 是首选方法，因为应用程序部署者是通过明确指定此类应用程序参数的名称、类型和值来对其进行配置的。

以下样例说明了 J2EE 标准部署描述符中指定的 <env-entry> 的语法：

```
<env-entry>
<description> Send pincode by mail </description>
<env-entry-name> mailPincode </env-entry-name>
<env-entry-value> false </env-entry-value>
<env-entry-type> java.lang.Boolean </env-entry-type>
</env-entry>
```

<env-entry-type> 标记为条目指定了一个全限定的类名称。下面的代码段使用 JNDI 从 Servlet 或 JSP 查找 <env-entry>：

```
Context initContext = new InitialContext();
Boolean mailPincode = (Boolean)
initContext.lookup("java:comp/env/mailPincode");
// 用户可以在子上下文中使用相对名称
Context envContext = initContext.lookup("java:comp/env");
Boolean mailPincode = (Boolean)
envContext.lookup("mailPincode");
```

资源引用

工厂是一种根据需要创建其他对象的对象。资源工厂可以创建资源对象，例如，数据库连接或消息服务连接。它们是使用标准部署描述符中的 <resource-ref> 元素配置的。

以下示例说明了工厂的使用：

示例

对 JDBC 连接工厂 （返回 javax.sql.DataSource 类型的对象）的引用的声明：

```
<resource-ref>
<description> Primary database </description>
<res-ref-name> jdbc/primaryDB </res-ref-name>
<res-type> javax.sql.DataSource </res-type>
<res-auth>Container</res-auth>
</resource-ref>
```

<res-type> 是该资源工厂的全限定类名称。可以指定 Container 或 Application 作为 <res-auth> 变量的值。

如果指定 Container， Web 容器会在将资源工厂绑定到 JNDI 查找注册表之前处理验证。如果指定 Application， Servlet 必须以编程方式处理验证。不同类型的资源工厂将在描述了资源类型的单独的子上下文中进行查找，如下所示：

- jdbc/ （对于 JDBC javax.sql.DataSource 工厂）
- mail/ （对于 JavaMail javax.mail.Session 工厂）
- url/ （对于 java.net.URL 工厂）

在下面的代码片段中，将从一个以容器处理验证的应用程序组件中获取 JDBC 连接：

```
InitialContext initContext = new InitialContext();

DataSource source =

(DataSource) initContext.lookup("java:comp/env/jdbc/primaryDB");

Connection conn = source.getConnection();
```

请注意，为确保这些资源引用正常工作， res-ref-name 必须在运行时映射到有效的资源工厂。

资源环境引用

资源环境引用提供了一种可以通过 JNDI 查找访问与资源相关联的管理对象的方法。标准部署描述符中定义的 <resource-env-ref> 元素使应用程序可以声明资源要求。

<resource-env-ref> 与 <resource-ref> 元素之间的主要区别在于前者没有特定的资源验证要求，但这两种元素都得靠资源工厂描述符来支撑。

示例

```
<resource-env-ref>

    <description> My Topic </description>

    <res-env-ref-name> jdbc/MyTopic </res-ref-name>

    <res-env-ref-type> javax.jdbc.Topic </res-type>

</resource-env-ref>
```

下面的代码段将访问一个 JMS Topic 对象：

```
InitialContext initContext = new InitialContext();
```

```
javax.jms.Topic myTopic = (javax.jdbc.Topic)
initContext.lookup("java:comp/env/jdbc/MyTopic");
```

初始命名上下文

Sun ONE Web Server 中的命名支持主要基于 J2EE 1.3，同时还添加了一些增强功能。当应用程序组件通过 `InitialContext()` 创建初始上下文时， Sun ONE Web Server 将返回一个充当 Web 应用程序命名环境的句柄的对象。此对象又为 `java:comp/env` 名称空间提供了子上下文。每个 Web 应用程序将获取自己的名称空间，也就是说， `java:comp/env namespace` 是针对每个 Web 应用程序的，并且一个 Web 应用程序的名称空间中绑定的对象不与其他 Web 应用程序中绑定的对象发生冲突。

JNDI 连接工厂

对于 J2EE Web 应用程序， `web.xml` 文件中的部署描述符是占位符，用于定义对应用程序环境条目或资源管理器 （如 SQL 数据源）连接工厂的引用。应用程序使用 J2EE 容器提供的 `JNDI InitialNamingContext` 查找这些引用。这样，仅通过更改部署描述符 （而不必访问或修改应用程序的源代码）即可将应用程序移植到不同的 Web 服务器环境中。

连接工厂是一种对象，可生成使 J2EE 组件能够访问资源的连接对象。数据库的连接工厂是一种 `javax.sql.DataSource` 对象，它可创建 `java.sql.Connection` 对象。

在 Sun ONE Web Server 中，您可以配置访问以下资源和资源工厂的方式：

- JDBC 连接工厂
- JavaMail 会话连接工厂
- 用户编写的普通自定义资源对象工厂
- 对诸如 LDAP 等外部资源系统信息库的支持

所有 Sun ONE Web Server 资源工厂都在 `server.xml` 中的 `<resources> </resources>` 标记中指定，且具有使用 `jndiname` 属性指定的 JNDI 名称 （`jdbconnectionpool` 除外，它不具有 jndiname）。此属性用于在服务器范围内的名称空间中注册工厂。部署者可以使用 `sun-web.xml` 中的 `resource-ref` 元素将用户指定的、特定应用程序的资源引用名称 （在 `resource-ref` 或 `resource-env-ref` 元素中声明）映射到这些服务器范围内的资源工厂。这样有助于在部署时决定给定的应用程序使用哪些 JDBC 资源 （和其他资源工厂）。

自定义资源访问本地 JNDI 系统信息库，外部资源访问外部 JNDI 系统信息库。这两种资源类型都需要用户指定的工厂类元素、 JNDI 名称属性等。

本节将介绍如何创建各种 J2EE 资源以及如何访问这些资源。

创建基于 Java 的资源

本节介绍如何使用管理界面创建基于 J2EE 的不同资源：

创建新的 JDBC 连接池

可以通过以下方式创建新的 JDBC 连接池：

- 使用管理界面
- 使用命令行界面

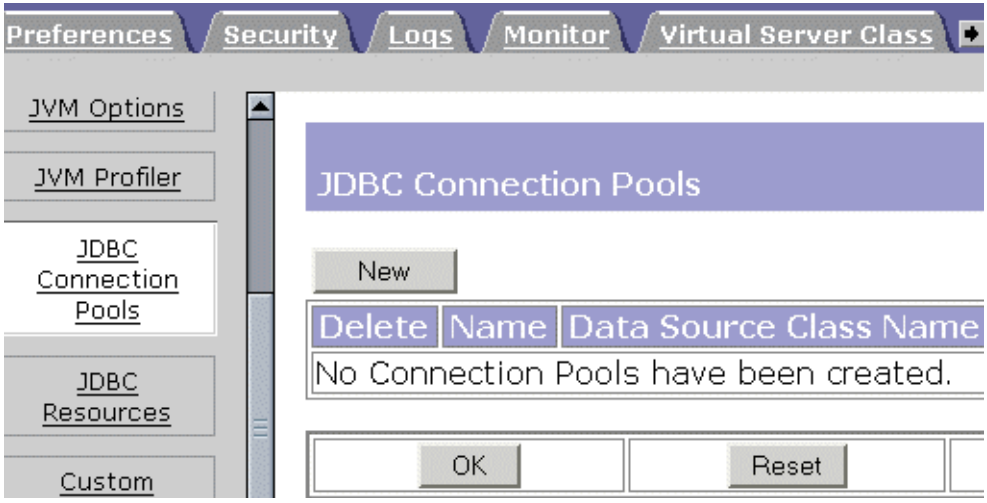
使用管理界面

要使用管理界面创建新的 JDBC 连接池，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java” 选项卡。
2. 单击 “JDBC Connection Pools”。

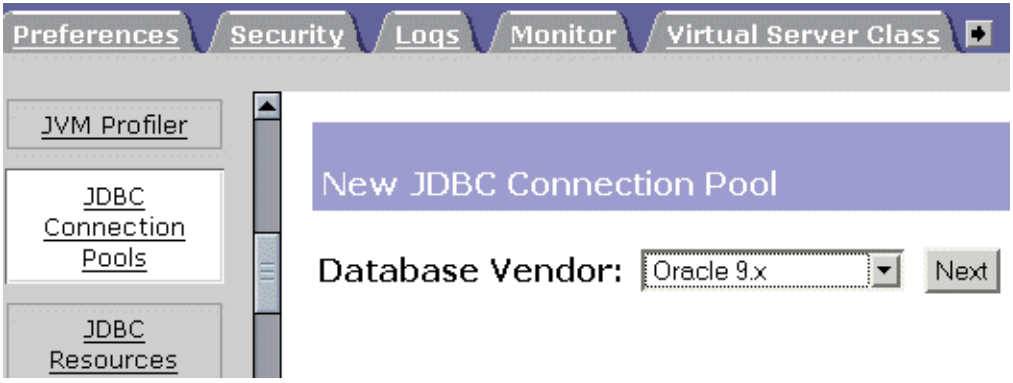
3. 单击 “New”。

“JDBC Connection Pools”界面



4. 从 “Database Vendor”下拉列表中选择要连接的数据库类型。如果未列出您的 DBMS，请选择 “Other”。

“New JDBC Connection Pool”界面



5. 单击 “Next”。

将显示 “Add New JDBC Connection Pool”。

6. 指定新连接池的特性并单击 “OK”。

   下面列出了必须指定的连接池特性：

   General

   - **Pool Name**。输入新连接池的名称。
   - **DataSource Classname**。实现数据源的供应商的特定类名称。如果在 “New JDBC Connection Pool” 的 “Database Vendor” 列表中选择了 “Other”，则必须输入要使用的数据源的供应商特定类名称。请注意，此类必须实现 `javax.sql.DataSource`。

   Properties

   指定标准的和专用的 JDBC 连接池特性；其中的许多特性都是可选的。默认情况下将提供所有标准特性的名称。您需要查阅数据库供应商的文档，以确定必需的标准特性和供应商的特定特性。

   Pool Settings

   - **Steady Pool Size**。指定连接池应当维护的最小连接数。连接提供给请求的线程之后，该连接将从池中删除，从而减小了当前的池大小。稳定池大小还要引用服务器启动时要添加到池中的连接数。
   - **Max Pool Size**。指定该池在任意指定时间所允许的最大连接数。
   - **Pool Resize Quantity**。当池向稳定池大小方向收缩时，将按批量调整大小。此值用于确定该批量的大小。将此值设置过大会延迟连接的回收，而设置过小会导致效率太低。请注意，池容量每次只增加一个连接，因此该字段不会导致池容量的增加。
   - **Idle Timeout (secs)**。连接在池中可保持空闲状态的最长时间 （秒）。超过此时间后，池实现可以关闭此连接。
   - **Max Wait Time (milli secs)**。达到连接超时前调用者等待的时间。缺省的等待时间为 `long`，即调用者可以等待很长时间。如果此值设置为 `0`，在存在可用的连接之前调用者将被拒绝。

   Connection Validation

   - **Connection Validation Required**。如果选中此字段，则连接在传递到应用程序之前将被验证。这样，如果由于网络出现故障或数据库服务器崩溃造成数据库不可用， Web 服务器将自动重新建立数据库连接。连接验证将引起额外负担，并且会导致性能稍有下降。

- **Validation Method**。指定 Web 服务器可用于验证数据库连接的方法。请从以下值中选择：
  - **auto-commit**。在此模式下，将执行查询语句并将其作为单个事务提交。如果禁用 `auto-commit`，查询语句将并入可通过提交或回滚机制终止的事务中。
  - **meta-data**。在此模式下，连接的数据库可提供元信息，说明其表及存储过程等。元数据对象的每个实例都具有与其相关联的特定查询。元数据对象将执行该查询并高速缓存其结果。
  - **table**。此方法要求 Web 服务器基于用户指定的表执行查询。
- **Table Name**。如果从 “Validation Method”下拉列表中选择了验证选项 “`table`”，则在此处指定表名称。
- **Fail All Connections**。指定在确定某个连接已失败时是否使池中的所有连接都失败并重新建立这些连接。如果未选中此复选框，则仅在使用连接时才单独重新建立连接。

Transaction Isolation

事务使用的隔离级别确定了应用程序对其他用户的事务所做更改的敏感程度，进而确定了事务为免受这些更改影响而必须持有锁的时间。

- **Transaction Isolation**。允许您为此连接选择事务隔离级别。请从以下值中选择：
  - **read-uncommitted**。也称为脏读取 (dirty read)，此隔离级别使事务可以读取数据页面上的任何当前数据，无论该数据是否被提交。
  - **read-committed**。此选项将在数据上放置共享锁，这样，将不会读取其他事务已经更改但尚未提交的任何数据。因为不会读取尚未提交的数据，所以如果以 `read-committed` 隔离方式运行的事务再次查询数据，则该数据可能已更改，或者可能会出现满足原始查询条件的其他数据。
  - **repeatable-read**。此选项可确保在查询中使用的所有数据上放置锁。在您提交或回滚事务之前，其他用户将无法修改您的事务访问的数据。
  - **serializable**。此选项将锁定数据的范围，这样，当再次执行查询时，在第一次和第二次查询之间的时间间隔内，数据不会更改，也不会出现其他数据行。
- **Guarantee Isolation Level**。此选项可确保从池中获取的任何连接都将具有相同的隔离级别。例如，如果上次使用连接时其隔离级别以编程的方式被更改 （例如， `con.setTransactionIsolation`），则此机制会将该连接的隔离级别更改回指定的隔离级别。

使用命令行界面

有关如何使用命令行界面创建新的 JDBC 连接池的信息，请参见附录 A “命令行实用程序”中的 “创建 JDBC 连接池”。

创建 JDBC 资源

JDBC 资源也称为数据源，通过它可以使用 `getConnection()` 创建到数据库的连接。可以通过以下方式之一创建 JDBC 资源：

- 使用管理界面
- 使用命令行界面

使用管理界面

要使用管理界面创建 JDBC 资源，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java”选项卡。
2. 单击 “JDBC Resources”。
3. 单击 “New”按钮。
4. 输入以下信息：
   - **JNDI Name** （必需）。输入应用程序组件访问 JDBC 资源所必须使用的 JNDI 名称。
   - **Pool Name** （必需）。从列表中选择此 JDBC 资源使用的连接池的名称（或 ID）。有关详细信息，请参见 “创建新的 JDBC 连接池”。
5. 要启用 JDBC 资源，请从 “Data Source Enabled”下拉列表中选择 “`On`”。

   如果禁用某个 JDBC 资源，则任何应用程序组件都不能与之连接，但其配置仍保留在服务器实例中。
6. 单击 “OK”。
7. 单击 “Apply Changes”。

使用命令行界面

有关如何使用命令行界面创建新的 JDBC 资源的信息，请参见附录 A “命令行实用程序”中的 “创建 JDBC 资源”。

创建自定义资源

您可以通过以下任一方式创建自定义资源：

- 使用管理界面
- 使用命令行界面

使用管理界面

1. 访问 Server Manager 并选择 “Java”选项卡。
2. 单击 “Custom Resources”。
3. 单击 “New”按钮。
4. 输入以下信息：
    - **JNDI Name** （必需）。输入应用程序组件访问自定义资源所必须使用的 JNDI 名称。
    - **Resource Type** （必需）。输入自定义资源的全限定类型。
    - **Factory Class** （必需）。输入用户编写的工厂类的全限定名称，它实现 `javax.naming.spi.ObjectFactory`。
    - **Custom Resource Enabled** （可选）。选择 “On”在运行时启用自定义资源。
5. 单击 “OK”。
6. 单击 “Apply Changes”。

使用命令行界面

有关如何使用命令行界面创建新的自定义资源的信息，请参见附录 A “命令行实用程序”中的 “创建自定义资源”。

创建外部 JNDI 资源

您可以通过以下方式创建外部资源：

- 使用管理界面
- 使用命令行界面

使用管理界面

1. 访问 Server Manager 并选择 “Java” 选项卡。
2. 单击 “External JNDI Resources”。
3. 单击 “New” 按钮。
4. 输入以下信息：
   - **JNDI Name** （必需）。输入应用程序组件访问自定义资源所必须使用的 JNDI 名称。
   - **Resource Type** （必需）。输入自定义资源的全限定类型。
   - **Factory Class** （必需）。输入用户编写的工厂类的全限定名称，它实现 `javax.naming.spi.ObjectFactory`。
   - **JNDI Lookup** （必需）。输入要在外部系统信息库中查找的 JNDI 值。例如，当您创建一个与外部系统信息库连接的外部资源时，为测试某个邮件类，“JNDI Lookup” 可能会读取 `cn=testmail`。
   - **External Resource Enabled** （可选）。选择 “`On`” 在运行时启用外部资源。
5. 单击 “OK”。
6. 单击 “Apply Changes”。

使用命令行界面

有关如何使用命令行界面创建新的自定义资源的信息，请参见附录 A “命令行实用程序” 中的 “创建外部 JNDI 资源”。

修改基于 Java 的资源

本节介绍如何使用管理界面修改您创建的基于 Java 的资源的特性：

修改 JDBC 连接池

要修改 JDBC 连接池的特性，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java” 选项卡。
2. 单击 “JDBC Connection Pools” 链接。
3. 单击代表您要编辑的 JDBC 连接池的链接。
4. 根据需要修改设置。
5. 单击 “OK”。

修改 JDBC 资源

要修改 JDBC 资源的特性，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java” 选项卡。
2. 单击 “JDBC Resources” 链接。
3. 单击代表您要编辑的 JDBC 资源的链接。
4. 根据需要修改设置。
5. 单击 “OK”。

修改自定义资源

要修改自定义资源的特性，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java” 选项卡。

2. 单击 “Custom Resources” 链接。
3. 单击代表您要编辑的自定义资源的链接。
4. 根据需要修改设置。
5. 单击 “OK”。

修改外部 JNDI 资源

要修改外部 JNDI 资源的特性，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java” 选项卡。
2. 单击 “External JNDI Resources” 链接。
3. 单击代表您要编辑的外部 JNDI 资源的链接。
4. 根据需要修改设置。
5. 单击 “OK”。

删除基于 Java 的资源

本节介绍如何使用管理界面删除基于 Java 的资源：

- 删除 JDBC 连接池
- 删除 JDBC 资源
- 删除 JDBC 资源
- 删除 JDBC 资源

删除 JDBC 连接池

您可以使用以下方法之一删除 JDBC 资源：

- 使用 Administration Server
- 使用命令行实用程序

使用 *Administration Server*

要使用 Administration Server 删除 JDBC 连接池，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java” 选项卡。
2. 单击 “JDBC Connection Pools” 链接。
3. 选中与要删除的 JDBC 连接池相对应的复选框。
4. 单击 “OK”。

使用命令行实用程序

有关可以使用的命令行选项的语法信息，请参见 “命令行实用程序”。

删除 JDBC 资源

您可以使用以下方法之一删除 JDBC 资源：

- 使用 Administration Server
- 使用命令行实用程序

使用 *Administration Server*

要使用 Administration Server 删除 JDBC 资源，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java” 选项卡。
2. 单击 “JDBC Resources” 链接。
3. 选中与要删除的 JDBC 资源相对应的复选框。
4. 单击 “OK”。

使用命令行实用程序

有关可以使用的命令行选项的语法信息，请参见 “命令行实用程序”。

删除自定义资源

您可以使用以下方法之一删除自定义资源：

- 使用 Administration Server
- 使用命令行实用程序

使用 *Administration Server*

要使用 Administration Server 删除自定义资源，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java” 选项卡。
2. 单击 “Custom Resources” 链接。
3. 选中与要删除的自定义资源相对应的复选框。
4. 单击 “OK”。

使用命令行实用程序

有关可以使用的命令行选项的语法信息，请参见 “命令行实用程序”。

删除外部 JNDI 资源

您可以使用以下方法之一删除外部 JNDI 资源：

- 使用 Administration Server
- 使用命令行实用程序

使用 *Administration Server*

要使用 Administration Server 删除外部 JNDI 资源，请执行以下步骤：

1. 访问 Server Manager 并选择 “Java” 选项卡。
2. 单击 “External JNDI Resources” 链接。
3. 选中与要删除的外部 JNDI 资源相对应的复选框。
4. 单击 “OK”。

使用命令行实用程序

有关可以使用的命令行选项的语法信息，请参见 “命令行实用程序”。

第 4 部分

管理虚拟服务器和服务

第 13 章

使用虚拟服务器

本章介绍了如何使用 Sun ONE Web Server 设置和管理虚拟服务器。

本章包括以下部分：

虚拟服务器概述

使用虚拟服务器时，您只需安装一台服务器便可以为多个公司或个人提供域名、 IP 地址以及某些服务器监视功能。对于用户来说，他们就像拥有了自己的 Web 服务器，只不过是由您提供硬件并进行基本的 Web 服务器维护。

注 如果未使用虚拟服务器，您仍然可以使用 Class Manager 中的项目为 Web 服务器实例配置内容、程序和其他功能。安装 Web 服务器时，将为该实例创建缺省的虚拟服务器。您可以使用虚拟服务器用户界面管理该缺省虚拟服务器的内容和服务。

要设置虚拟服务器，需要设置以下内容：

- 虚拟服务器类
- 侦听套接字
- 虚拟服务器

虚拟服务器的设置存储在 *server_root/server_ID*/`config` 目录下的 `server.xml` 文件中。虽然您可以编辑此文件，但是使用虚拟服务器无需编辑此文件。有关此文件以及如何对其进行编辑的详细信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference*。

本部分包括以下主题：

- 多个服务器实例
- 虚拟服务器类
- 侦听套接字
- 虚拟服务器
- 选择用于处理请求的虚拟服务器
- 文档根目录
- 日志文件
- 从上一个版本移植虚拟服务器

多个服务器实例

过去的 Sun ONE Web Server 版本在为虚拟服务器配置独特信息方面不十分灵活。用户经常会为了能以直接方式使各服务器分别具有单独的配置信息，而创建多个单独的服务器实例。从 Sun ONE Web Server 6.0 版开始，每个虚拟服务器类都具有了单独的配置信息。该版本仍然支持多个服务器实例，但如果要使多台服务器都具有独立的配置信息，那么最好选择虚拟服务器。

虚拟服务器类

虚拟服务器被归入到不同的类。使用类可以同时配置类似的虚拟服务器，因此不必逐个配置每台服务器。尽管一个类中的所有虚拟服务器共享同样的基本配置信息，但是您也可以为每台虚拟服务器设置变量，更改其配置。如果不希望虚拟服务器共享配置信息，可以在每个虚拟服务器类中创建单个虚拟服务器。但是如果虚拟服务器共享类似的特性，则可以将它们编组在一个类中，统一进行配置。

例如，如果您为 Internet 服务提供商 (ISP) 工作，希望为不同的客户提供不同级别的宿主服务并收取不同的费用，则可以为客户设置多个虚拟服务器类。您可以为某个虚拟服务器类启用 Java Servlet 和 JSP，而为另一个较便宜的虚拟服务器类禁用 Java Servlet 和 JSP。

通过命名虚拟服务器类并创建文档根目录可以创建虚拟服务器类，缺省情况下，属于该类的所有虚拟服务器都在此文档根目录下拥有自己的文档根目录。您可以使用 `$id` 变量，以便类中每个虚拟服务器都在类的文档根目录中拥有独立的文档根目录。有关详细信息，请参见第 292 页上的 “文档根目录”。

创建虚拟服务器类后，您可以将服务与其关联。您可以为虚拟服务器类打开或配置下列类型的服务：

- 程序 （参见 “使用程序扩展服务器”）。
- 内容管理 （参见 “内容管理”）。
- 配置式样 （参见 “应用配置式样”）。

obj.conf 文件

类中所有虚拟服务器都共享 `obj.conf` 文件，该文件用于存储有关虚拟服务器类的信息。有些信息存储在变量中，这样单个虚拟服务器即可实时替换特定变量值。

有关 `obj.conf` 和变量的详细信息，请参见 *NSAPI Programmer's Guide*。有关在用户界面中使用变量的详细信息，请参见第 296 页上的 “使用变量”。

类中的虚拟服务器

属于某个类的虚拟服务器称为该类的成员。有些虚拟服务器设置是为类中的所有虚拟服务器配置的，有些设置则是为某个虚拟服务器单独配置的。这些设置在 Class Manager 的 “Virtual Servers” 选项卡中进行配置。有关详细信息，请参见第 14 章 “创建和配置虚拟服务器”。

缺省类

安装 Sun ONE Web Server 时，安装程序将自动创建一个类 （称为 `defaultclass`）。缺省情况下，它包含服务器实例的一个虚拟服务器成员。您可以向缺省类中添加其他虚拟服务器，但不能从该类中删除缺省的虚拟服务器。也不能删除缺省类。

侦听套接字

服务器与客户机之间的连接在侦听套接字上进行。您创建的每个侦听套接字都有一个 IP 地址、端口号、服务器名和缺省虚拟服务器。要使侦听套接字侦听计算机给定端口上所有已配置的 IP 地址，请使用 0.0.0.0、 any、 ANY 或 INADDR_ANY 作为 IP 地址。

安装 Sun ONE Web Server 时将自动创建一个侦听套接字 (ls1)。此侦听套接字使用 IP 地址 0.0.0.0 和安装过程中指定为 HTTP 服务器端口号的端口号 （默认值为 80）。不能删除缺省的侦听套接字。如果您使用的不是虚拟服务器，这一个侦听套接字就足够了。但是如果您使用的是虚拟服务器，则可能需要为虚拟服务器创建多个侦听套接字。

由于侦听套接字是 IP 地址和端口号的组合，因此您可以拥有多个 IP 地址相同但端口号不同 （或 IP 地址不同但端口号相同）的侦听套接字。例如，您既可以使用 1.1.1.1:81 和 1.1.1.1:82，也可以使用 1.1.1.1:81 和 1.2.3.4:81，只要将计算机配置为响应这两个地址即可。

此外，还应在侦听套接字中指定接收方线程 （有时称作接受线程）的数目。接收方线程是等待连接的线程。它用于接受连接并将其置于队列中以便随后由工作线程拾取。理想情况下，您需要有足够的接受线程，以便在新请求传入时始终有一个可用的线程。但是，线程数目不能过多，否则会占用过多的系统资源。缺省线程数为 1。最好是系统上的每个 CPU 都有一个接受线程。如果发现性能受到影响，可以调整此值。

虚拟服务器

要创建虚拟服务器，必须先确定它所属的类，然后确定其类型。要创建虚拟服务器，只需要指定一个虚拟服务器 ID 以及一个或多个 URL 主机。

本部分包括以下主题：

虚拟服务器的类型

在 Sun ONE Web Server 6.0 以前的版本中，有两种类型的虚拟服务器：硬件虚拟服务器和软件虚拟服务器。硬件虚拟服务器与唯一 IP 地址相关联。软件虚拟服务器没有唯一的 IP 地址，但有唯一的 URL 主机。

在 Sun ONE Web Server 6.0 和 Sun ONE Web Server 6.1 中，这些概念都不再准确。所有虚拟服务器都需要指定 URL 主机，但虚拟服务器可能还与基于侦听套接字的 IP 地址相关联。

当新请求传入时，服务器将根据 IP 地址或 Host 标头中的值确定将此请求发送到哪个虚拟服务器。首先，它将提取 IP 地址。有关详细信息，请参见第 292 页上的 “选择用于处理请求的虚拟服务器”。

基于 IP 地址的虚拟服务器

要使一台计算机具有多个 IP 地址，必须通过操作系统对其进行映射或提供附加插卡。要通过操作系统设置多个 IP 地址，请使用 “网络控制面板” (Windows) 或 `ifconfig` 实用程序 (UNIX/Linux)。请注意， `ifconfig` 的用法因平台而异。有关详细信息，请参见操作系统文档。

通常，要创建基于 IP 地址的虚拟服务器，可创建一个用于侦听特定 IP 地址的侦听套接字。侦听套接字的缺省虚拟服务器是基于 IP 地址的虚拟服务器。有关如何部署虚拟服务器的详细信息，请参见第 303 页上的 “部署虚拟服务器”。

基于 URL 主机的虚拟服务器

可以通过提供唯一的 URL 主机来设置基于 URL 主机的虚拟服务器。Host 请求标头的内容将服务器定向到正确的虚拟服务器。

例如，如果要为用户 aaa、bbb 和 ccc 设置虚拟服务器以便每个用户都可以拥有单个域名，首先对 DNS 进行配置，使其能够识别每个用户的 URL （`www.aaa.com`、`www.bbb.com` 和 `www.ccc.com`），然后将这些 URL 解析为所使用的侦听套接字的 IP 地址。然后对每个虚拟服务器的 URL 主机进行正确的设置 （例如，`www.aaa.com`）。

由于基于 URL 主机的虚拟服务器使用 Host 请求标头将用户定向到正确的页面，因此并非所有客户机软件都可以与它们一起工作。不支持 HTTP Host 标头的旧客户机软件无法正常运行。这些客户机将接收侦听套接字的缺省虚拟服务器。

缺省虚拟服务器

系统使用 Host 请求标头选择基于 URL 主机的虚拟服务器。如果最终用户的浏览器未发送 Host 标头，或者服务器找不到指定的 Host 标头，则缺省虚拟服务器将处理该请求。

缺省虚拟服务器由侦听套接字设置。可在创建侦听套接字时指定缺省虚拟服务器。可以随时更改此缺省虚拟服务器。

选择用于处理请求的虚拟服务器

服务器处理请求之前，必须先通过侦听套接字接受该请求，再将其定向到正确的虚拟服务器。

然后按如下方式选择虚拟服务器：

- 如果侦听套接字只配置了一台缺省虚拟服务器，将选择此虚拟服务器。
- 如果侦听套接字配置了多台虚拟服务器，则将请求 `Host` 标头与虚拟服务器的 URL 主机相匹配。如果不存在 `Host` 标头或匹配的 URL 主机，则选择连接组的缺省虚拟服务器。

如果为 SSL 侦听套接字配置了虚拟服务器，则在服务器启动时将检查该虚拟服务器的 URL 主机与证书的主题模式是否匹配，如果不匹配，将生成警告并写入错误日志。

确定虚拟服务器后，服务器将执行虚拟服务器所属的虚拟服务器类的 `obj.conf` 文件。有关服务器如何确定在 `obj.conf` 文件中执行哪些指令的详细信息，请参见 Sun ONE Web Server 6.1 *NSAPI Programmer's Guide*。

文档根目录

主文档目录 （即文档根目录）是包含所有要提供给远程客户机的虚拟服务器文件的中心目录。

使用文档根目录可以轻松地限制对虚拟服务器上的文件的访问。还可以轻松地将文档移动到新目录 （可能位于其他磁盘上）而无需更改任何 URL，因为在 URL 中指定的路径相对于主文档目录。

例如，如果文档目录为 `C:\sun\servers\docs`，则请求 （例如 `http://www.sun.com/products/info.html`）将通知服务器在 `C:\sun\servers\docs\products\info.html` 中查找该文件。如果更改文档根目录 （即移动所有文件和子目录），则只需更改虚拟服务器使用的文档根目录，而不用将所有 URL 均映射到新目录，或以某种方式通知客户机在新目录中查找。

安装 Sun ONE Web Server 时，应为 Web 服务器实例指定一个文档根目录。该目录将成为缺省类的文档根目录。您可以在类级别上更改该目录或在单个虚拟服务器级别上覆盖该目录。

添加类时，还需要指定文档目录。该目录是绝对路径。但如果您只输入绝对路径，则属于该类的所有虚拟服务器的文档根目录将缺省为同一路径。如果您在文档根目录绝对路径的末尾添加变量 $id，则每个虚拟服务器都将有一个缺省文档根目录 *class_doc_root*/*virtual_server_ID*。例如，如果类的文档目录是 `/sun/servers/docs/$id`，则属于该类的虚拟服务器 `vs1` 的默认文档目录为 `/sun/servers/docs/vs1`。

有关变量的详细信息，请参见第 296 页上的 “使用变量”。

您也可以在单个虚拟服务器级别上覆盖类的缺省文档目录。

日志文件

创建新的虚拟服务器时，缺省情况下，日志文件与服务器实例的日志文件是同一文件。大多数情况下，用户可能希望每个单独的虚拟服务器都有自己的日志文件。要进行此设置，可以更改每个虚拟服务器的日志路径。

有关详细信息，请参见第 313 页上的 “配置虚拟服务器的日志设置”。

从上一个版本移植虚拟服务器

如果您在 iPlanet Web Server 4.1 版中使用了虚拟服务器，则可以使用移植工具将其移植到当前版本。有关详细信息，请参见 *Installation and Migration Guide*。

在虚拟服务器中使用 Sun ONE Web Server 的功能

Sun ONE Web Server 提供了很多可用于虚拟服务器的功能（例如， SSL 和访问控制）。很多功能涉及所有服务器、服务器实例、虚拟服务器类或单个虚拟服务器的配置。以下各部分介绍了这些功能，并介绍了如何查找详细信息。

本部分包括以下主题：

在虚拟服务器中使用 SSL

如果要在虚拟服务器上使用 SSL，通常应使用基于 IP 地址的虚拟服务器。通常使用端口 443。在基于 URL 主机的虚拟服务器上不宜使用 SSL，因为 Sun ONE Web Server 必须先读取请求，然后才能确定将请求发送到哪个 URL 主机。服务器读取请求与进行安全信息交换的初始信号握手同时发生。

唯一的例外是基于 URL 主机的虚拟服务器都具有相同的 SSL 配置，包括使用 “通配符证书”的相同服务器证书。有关详细信息，请参见第 6 章 “使用证书和密钥”。

在虚拟服务器中实现 SSL 的方法之一是使用两个侦听套接字，一个使用 SSL 并侦听端口 443，另一个不使用 SSL。用户通常通过非 SSL 侦听套接字访问虚拟服务器。当必须使用安全事务时，可以单击 Web 页上的按钮，以启动安全事务。此后，请求将通过安全侦听套接字来进行。

由于 SSL 事务的速度比非 SSL 事务慢很多，因此只在必要时使用 SSL 事务。其他情况下将使用更快的非 SSL 连接。

有关 Sun ONE Web Server 和虚拟服务器安全设置及使用方面的详细信息，请参见第 6 章 “使用证书和密钥”。有关在虚拟服务器中配置 SSL 的示例图表，请参见第 305 页上的 “实例 2：安全服务器”。

在虚拟服务器中使用访问控制

使用虚拟服务器，您能够以每个虚拟服务器为基础来设置访问控制。甚至可以对其进行配置，以便每个虚拟服务器可以使用 LDAP 数据库对用户和组进行验证。有关详细信息，请参见第 197 页上的 “控制虚拟服务器的访问”。

在虚拟服务器中使用 CGI

可以在虚拟服务器上使用 CGI。出于访问及安全原因，有许多项设置可供您进行配置。

有关设置和使用 CGI 的详细信息，请参见第 347 页上的 “安装 CGI 程序”。

在虚拟服务器中使用配置式样

使用配置式样可以很容易地将一组选项应用到各个虚拟服务器维护的特定文件或目录。有关使用配置式样的详细信息，请参见 “应用配置式样”。

使用虚拟服务器用户界面

要创建和编辑虚拟服务器，您可以使用用户界面或命令行实用程序。

管理虚拟服务器的用户界面包括三个部分：

- Server Manager 包含全面影响服务器 （或所有虚拟服务器）的设置。
- Class Manager 包含影响单个类和类中虚拟服务器的设置。
- Virtual Server Manager 包含用于单个虚拟服务器的设置。

此外，还可以使用拥有单个虚拟服务器的最终用户的用户界面。有关详细信息，请参见第 300 页上的 “允许用户监视单个虚拟服务器”。

本部分包括以下主题：

Class Manager

要访问 Class Manager，请执行下列步骤：

1. 在 Server Manager 中单击 “Virtual Server Class”选项卡。
2. 单击 “Manage Classes”。
3. 选择一个类并单击 “Manage”。

您也可以在服务器的树视图中单击类名，或单击位于 Server Manager 右上角的 “Class Manager”按钮链接。

Virtual Server Manager

要访问 Virtual Server Manager，请执行下列步骤：

1. 在 Class Manager 中单击 “Virtual Server Tab”。
2. 单击 “Manage Virtual Servers”。
3. 选择一个虚拟服务器并单击 “Manage”。

您也可以在服务器的树视图中单击虚拟服务器名称。

您可以使用命令行实用程序 `HttpServerAdmin` 执行虚拟服务器任务 （与使用用户界面执行的任务相同）。有关命令行实用程序 `HttpServerAdmin` 的详细信息，请参见第 409 页上的 “HttpServerAdmin （虚拟服务器管理）”。

使用变量

您可以使用变量给出类的虚拟服务器专用值，而不必分别定义每个值。变量在 `obj.conf` 文件中进行定义。您可以定义自己的变量，但用户界面无法不识别这些变量。用户界面中最有用的变量是 $id，它表示虚拟服务器的 ID。输入这个变量后，服务器将使用该值取代单个虚拟服务器的 ID。

您还会用到其他几个变量 （例如 $accesslog [每个虚拟服务器的访问日志的路径] 和 $docroot [每个虚拟服务器的文档根目录的路径]，但只有 $id 变量需要输入到字段中。

有关变量的详细信息，请参见 Sun ONE Web Server 6.1 *NSAPI Programmer's Guide*。

动态重新配置

动态重新配置使您可以对活动 Web 服务器的配置进行更改，而无需停止并重新启动 Web 服务器以使更改生效。您可以动态更改 `server.xml` 及其关联文件中的所有配置设置和属性，而无需重新启动服务器。因此无需重新启动服务器即可应用在虚拟服务器用户界面中所做的所有更改。更改后，您可以使用重新配置脚本或用户界面动态重新配置服务器。

在 UNIX 平台上，动态重新配置脚本是一个名为 “`reconfig`”的 shell 脚本，它位于每个实例的目录中。该脚本无命令行变量。只需从服务器实例的目录键入 “`reconfig`”即可运行重新配置脚本。

在 Windows 中，动态重新配置脚本是一个名为 “`reconfig.bat`”的批处理文件，它位于每个实例的目录中。该交本无命令行变量。只需从服务器实例的目录键入 “`reconfig`”或 “`reconfig.bat`”即可运行重新配置脚本。

运行该脚本时，将启动服务器的动态重新配置 （与用户界面相似）并显示与重新配置相关的服务器信息。

要访问动态重新配置屏幕，请单击 “Server Manager”、“Class Manager”和 “Virtual Server Manager”右上角的 “Apply”链接，然后单击 “Apply Changes”中的 “Load Configuration Files”按钮。如果安装新配置时出错，则恢复为以前的配置。

设置虚拟服务器

要设置虚拟服务器，请执行以下步骤：

1. 创建一个侦听套接字
2. 创建一个虚拟服务器类
3. 为该类配置服务
4. 在虚拟服务器类中创建虚拟服务器
5. 配置虚拟服务器

请注意，创建侦听套接字时，必须在缺省虚拟服务器字段中输入一个现有的虚拟服务器。可以使用安装服务器时创建的虚拟服务器，然后在创建其他虚拟服务器后，根据需要返回并对其进行更改。

创建侦听套接字

要创建侦听套接字，请执行以下步骤：

1. 在 Server Manager 中单击 “Preferences”选项卡。
2. 单击 “Add Listen Socket”。
3. 填写各个字段。

   侦听套接字必须有一个唯一的端口号和 IP 地址组合。可以使用 IPV4 地址，也可以使用 IPV6 地址。如果要为基于 IP 地址的虚拟服务器创建侦听套接字，则 IP 地址必须为 0.0.0.0、ANY 或 INADDR_ANY，这意味着它将侦听端口上所有的 IP 地址。

   您也可以为此侦听套接字启用安全性 (SSL)。

   “Server Name”字段在服务器发送给客户机的 URL 中指定主机名。这会影响服务器自动生成的 URL，但不会影响存储在服务器中的目录和文件的 URL。如果服务器使用别名，则此名称应为别名。
4. 单击 “OK”。

创建虚拟服务器类

要创建虚拟服务器类，请执行以下步骤：

1. 在 Server Manager 中单击 “Virtual Server Class”选项卡。
2. 单击 “Add Class”。
3. 对该类进行命名。
4. 为该类插入文档根目录。

   该目录必须已经存在。除非您另外指定，否则此类的所有虚拟服务器的文档根目录都位于此绝对路径中。如果您使用 `/$id` 作为路径的末尾部分，则将在类的文档根目录路径中自动创建为虚拟服务器 ID 命名的文档根目录文件夹。
5. 单击 “OK”。

创建虚拟服务器类后，选择与该类关联的服务。有关详细信息，请参见 “内容管理”。

编辑或删除虚拟服务器类

要编辑虚拟服务器类的设置，请执行以下步骤：

1. 在 Server Manager 中单击 “Virtual Server Class”选项卡。
2. 单击 “Edit Classes”。
3. 从所需的类旁边的下拉列表中，选择 “Edit”或 “Delete”。

   请注意，不能删除缺省类。
4. 使用 “Document Root”字段将路径改为类的默认文档根目录的绝对路径。

   缺省情况下，将在此目录中创建该类的虚拟服务器的文档根目录。
5. 如果希望该虚拟服务器类使用接受语言标头分析，请在 “Accept Language”字段输入 “On”。

   缺省值为 “Off”。
6. 如果要更改与某个类关联的 CGI 缺省值，请单击 “Advanced”。

   将显示带有 CGI 缺省值的窗口。编辑各字段，然后单击 “OK”返回 “Edit a Class”窗口。使用 “Reset”按钮可以退回去重新进行更改。
7. 单击 “OK”。类即被更改或删除。

指定与虚拟服务器类关联的服务

为某类虚拟服务器启用的服务可以作为区分不同类虚拟服务器的特征。例如，某类虚拟服务器可能启用了 CGI，而另一类未启用。有关设置服务的详细信息，请参见内容管理。

创建虚拟服务器

设置虚拟服务器类后，即可创建虚拟服务器。由于虚拟服务器是特定虚拟服务器类的成员，因此应在 Class Manager 中创建虚拟服务器。

有关详细信息，请参见第 309 页上的 “创建虚拟服务器”。

指定与虚拟服务器关联的设置

您可以在虚拟服务器级别上覆盖某些类设置，也可以配置附加设置。请在 Class Manager 中配置这些设置。

有关详细信息，请参见第 309 页上的 “创建虚拟服务器”。

允许用户监视单个虚拟服务器

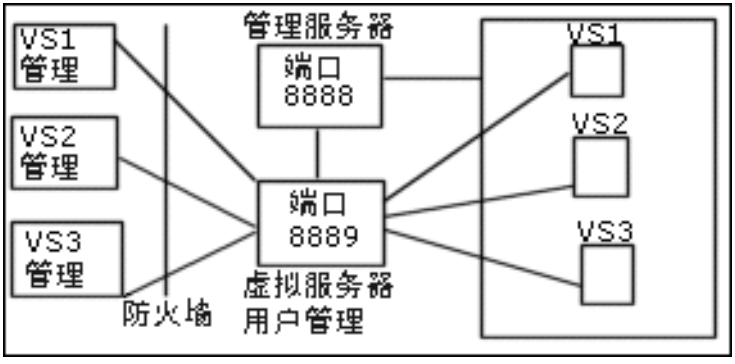
各个虚拟服务器的管理员可以通过特殊的用户界面查看虚拟服务器的设置以及访问日志和错误日志。例如，如果您的内部网中三个不同的部门使用三个不同的虚拟服务器，则每个部门都可以单独查看他们的设置和日志文件。

出于安全的考虑，该管理用户界面位于一个单独的端口 （既不是管理服务器端口，也不是 Web 服务器实例端口）。

该用户界面在管理服务器中的虚拟服务器上运行。缺省情况下将对此虚拟服务器进行设置，其名称为 useradmin。必须在管理服务器中设置一个侦听套接字 （该侦听套接字必须独立于运行管理服务器的侦听套接字），以便用户可以访问虚拟服务器管理用户界面，而无需访问管理服务器端口。

下图显示了各个虚拟服务器的管理员访问 useradmin 虚拟服务器以查看各自虚拟服务器信息的情况。

配置虚拟服务器管理员的用户界面



打开虚拟服务器时，如果您在 Administration Server 的 `/config/server.xml` 文件中编辑某些设置，则用户可以通过下列 URL 对其进行管理：

server_name:*port*/`user-app`/*server_instance*/*virtual_server_ID*

例如：

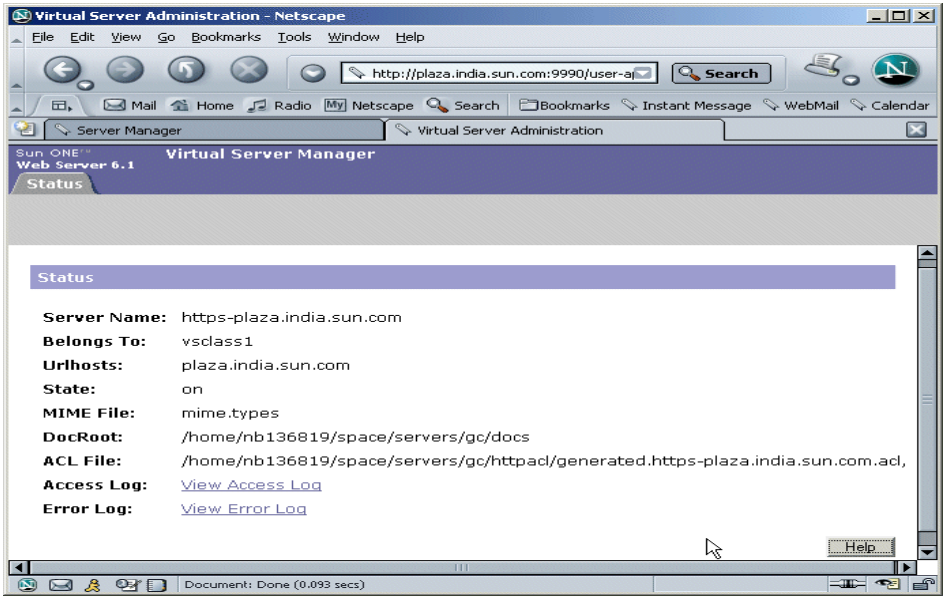
`sun:9999/user-app/sun/vs2`

服务器实例不包含服务器实例名称的 “`https`” 部分。

要确定虚拟服务器的 ID，请查看服务器实例的 `server.xml` 文件。

下图显示了最终用户看到的用户界面：

“Virtual Server Administration”用户界面



安装 Sun ONE Web Server 6.1 后，您会发现 *server_root*`/https-admserv/config/server.xml` 文件包含某些注释项，它们用于创建：

- 虚拟服务器的缺省侦听套接字（称作 “useradmin”）。
- 虚拟服务器的虚拟服务器类。

要设置 useradmin，需要取消这些项的注释。

要将服务器配置为可以使用此功能，请执行以下步骤：

1. 创建一个新的侦听套接字，它运行的端口应不同于管理服务器所使用的端口。

   例如，如果管理服务器在端口 8888 上运行，则新的侦听套接字必须使用其他端口号。使用不同的侦听套接字有助于确保管理服务器的安全。

   出于安全考虑，您不能通过用户界面添加此侦听套接字，而应该在管理服务器的 `server.xml` 文件中进行添加。

2. 打开管理服务器的 `server.xml` 文件 （位于 *server_root*`/https-admserv/config/server.xml`）。

3. 取消对包含 `LS`、`VSCLASS` 和 `VS` 元素缺省值的注释行的注释。示例：

```
<!--
<LS id="ls2" port="9999" servername="plaza"
defaultvs="useradmin"/>
-->
<!--
<VSCLASS id="userclass" objectfile="userclass.obj.conf">
   <VS id="useradmin" connections="ls2" mime="mime1"
aclids="acl1" urlhosts="plaza">
      <PROPERTY name="docroot" value="/export1/wsinst/docs"/>
      <USERDB id="default"/>
      <WEBAPP uri="/user-app"
path="/export1/wsinst/bin/https/webapps/user-app"/>
   </VS>
</VSCLASS>
-->
```

   这将启用 useradmin，它将在独立的端口上创建 （出于安全考虑）。

4. 将更改保存到 `server.xml`。

5. 重新启动 Administration Server 以应用更改。

6. 对于任何服务器实例中的任何虚拟服务器，都应该能够使用以下 URL 访问管理员 UI：

   server_name`:`*port*`/user-app/`*server_instance*`/`*virtual_server_ID*

   例如：

   `plaza:9999/user-app/plaza/https-plaza`

访问控制

要防止未经授权的用户擅自管理虚拟服务器，您可以设置 ACL。由于每个虚拟服务器的 URI 都是唯一的，因此可以对访问进行设置，以便只有正确的管理员才能访问虚拟服务器的设置。

有关详细信息，请参见第 8 章 “控制对服务器的访问”。

日志文件

每个虚拟服务器均可以有自己的日志文件。缺省情况下，所有虚拟服务器共享服务器实例的日志文件。如果允许用户查看其日志文件，则大多数情况下都必须更改日志文件设置，以使每个虚拟服务器拥有自己的访问和错误日志。

有关详细信息，请参见第 313 页上的 “配置虚拟服务器的日志设置”。

部署虚拟服务器

Sun ONE Web Server 的虚拟服务器体系结构非常灵活。服务器实例可以拥有任意数量的侦听套接字 （安全的和不安全的）。您可以使用基于 IP 地址的虚拟服务器，也可以使用基于 URL 主机的虚拟服务器。

此外，您可以将具有类似设置的虚拟服务器归入到任意数量的虚拟服务器类。虚拟服务器类中的所有虚拟服务器都共享 `obj.conf` 中相同的请求处理指令。

每个虚拟服务器都可以 （而非必须）拥有自己的 ACL 列表、 `mime.types` 文件和 Java Web 应用程序集。

此设计提供了最大的灵活性，使您可以为各种应用程序配置服务器。以下示例介绍了一些可能适用于 Sun ONE Web Server 的配置。

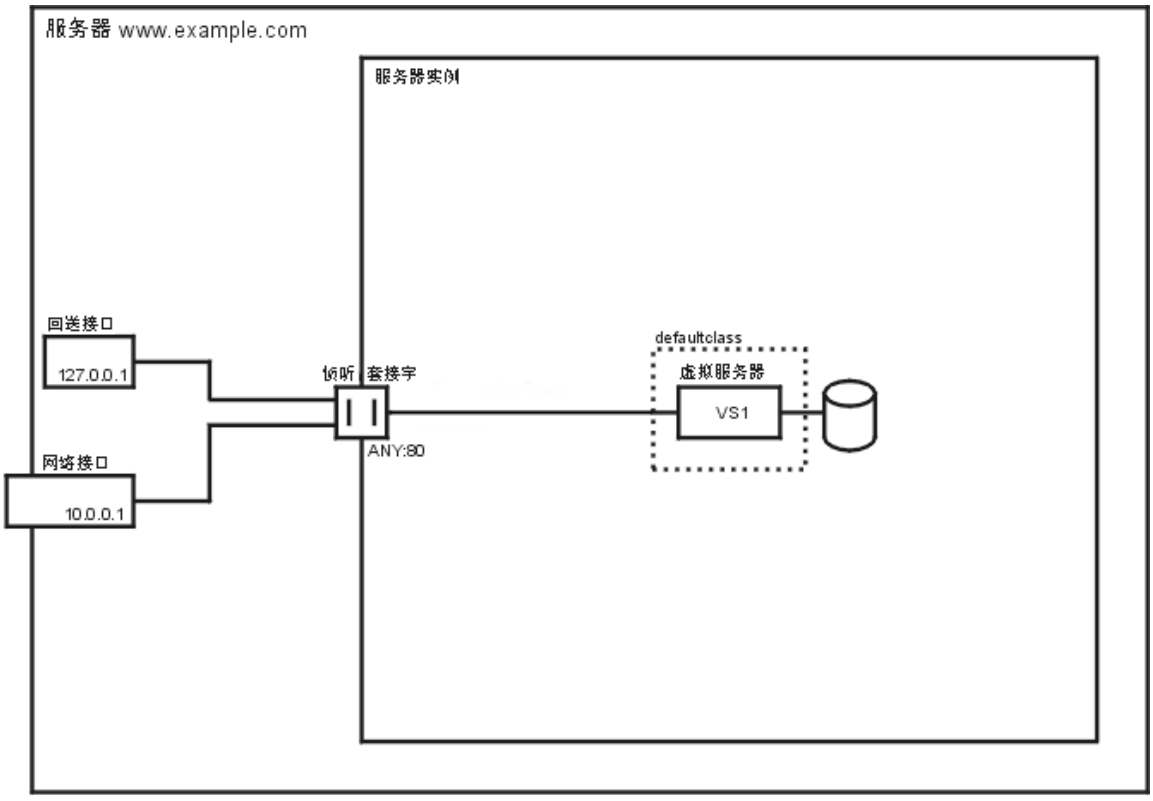
实例 1：缺省配置

安装新的 Sun ONE Web Server 后，您便拥有了一个服务器实例。它只使用一个侦听套接字侦听计算机配置的任何 IP 地址的端口 80 或安装时所选的任何端口。

本地网络中的某些机制为计算机配置的每个地址都建立了名称 - 地址映射。以下示例中的计算机有两个网络接口：地址 127.0.0.1 上的回送接口 （即使在没有网卡的情况下仍然存在的接口）和地址 10.0.0.1 上的以太网接口。

名称 example.com 通过 DNS 映射为 10.0.0.1。侦听套接字配置为侦听计算机配置的任何地址的端口 80 （“ANY:80”或 “0.0.0.0:80”）。

缺省配置



在此配置中，到以下地址的连接将到达服务器并由虚拟服务器 VS1 处理。

- `http://127.0.0.1/` （在 `example.com` 上启动）
- `http://localhost/` （在 `example.com` 上启动）
- `http://example.com/`
- `http://10.0.0.1/`

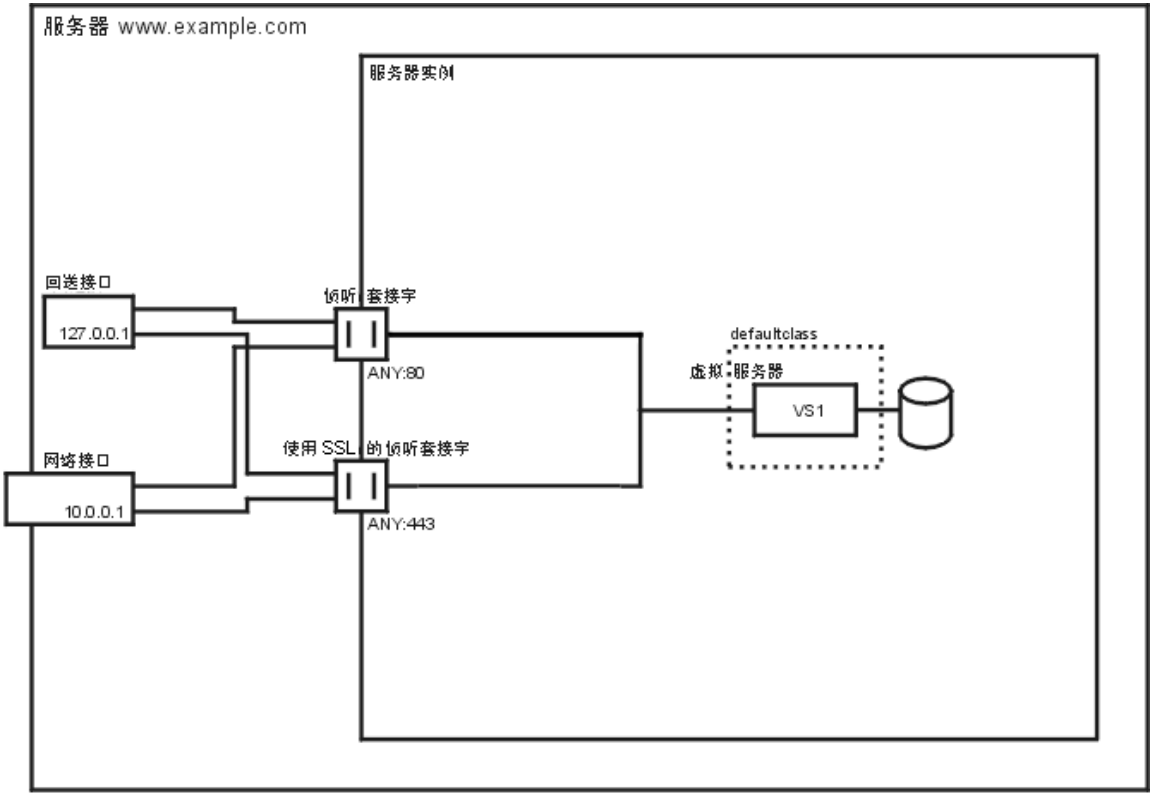
此配置适用于传统的 Web 服务器。无需添加附加的虚拟服务器或侦听套接字。可以通过更改 defaultclass（VS1 是 defaultclass 的成员）及 VS1 本身的设置来配置服务器的设置。

实例 2：安全服务器

如果要在缺省配置中使用 SSL，只需将侦听套接字更改为安全模式。这与以前版本的 Sun ONE Web Server 中设置安全的方法类似。

还可以添加一个为 ANY:443 配置的新的安全侦听套接字并将 VS1 关联到新的侦听套接字。虚拟服务器现在具有两种侦听套接字，一种使用 SSL，另一种不使用 SSL。现在，使用 SSL 和没有使用 SSL 的服务器将提供相同的内容，也就是说 `http://example.com/` 和 `https://example.com/` 提供的内容相同。

安全服务器



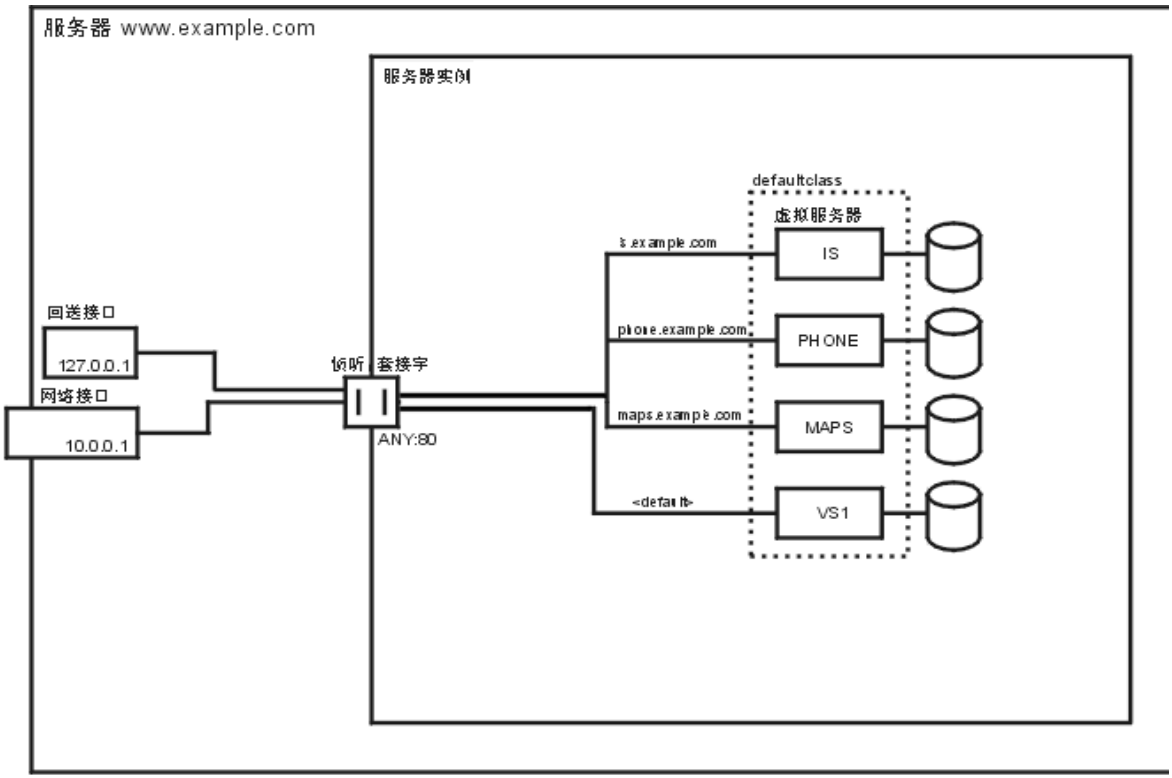
请注意， SSL 参数被附加到侦听套接字。因此，所有虚拟服务器只能有一组 SSL 参数配置为特定侦听套接字。

实例 3：内部网宿主

一个更复杂的 Sun ONE Web Server 配置是服务器在内部网部署中支持几个虚拟服务器。例如，假设您有三个内部站点，员工可在这些站点中查找其他用户的电话号码、查看校园地图以及跟踪发送到信息服务部门的请求的状态。以前（在本示例中），这些站点以三个不同的计算机为宿主，这些计算机映射为名称 `phone.example.com`、`maps.example.com` 和 `is.example.com`。

为了将硬件和管理开销减少到最低程度，用户希望将这三个站点合并为计算机 `example.com` 上的一个 web 服务器。可以使用以下两种方法进行此设置：使用基于 URL 主机的虚拟服务器或使用单独的侦听套接字。两者都有明显的优点和缺点。

使用基于 URL 主机的虚拟服务器的内部网宿主

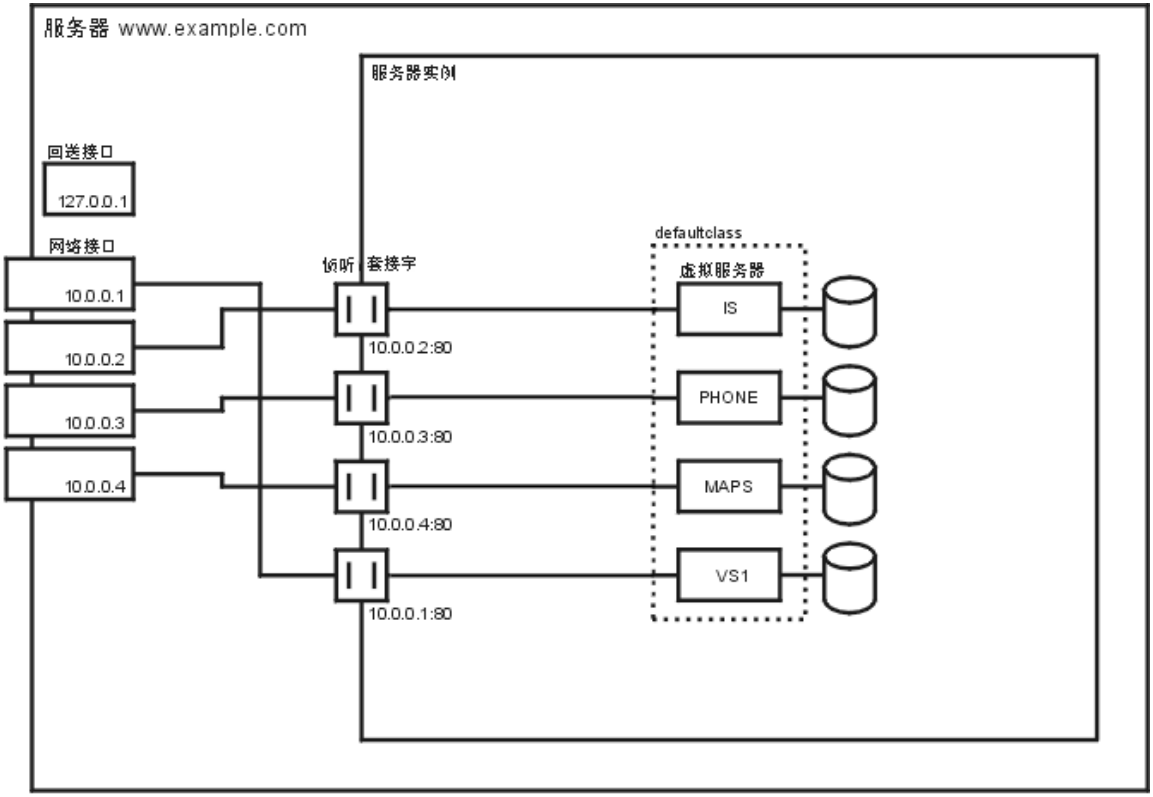


尽管基于 URL 主机的虚拟服务器易于设置，但它们具有以下缺点：

- 在此配置中支持 SSL 需要使用通配符证书进行非标准设置。有关详细信息，请参见第 4 章 “用于 Web 容器和 Web 应用程序的 基于 J2EE 的安全性”。
- 基于 URL 主机的虚拟服务器不能与传统的 HTTP 客户机一起使用。

您也可以设置基于 IP 地址的配置，每个地址一个侦听套接字：

使用单独侦听套接字的内部网宿主



基于 IP 地址的虚拟服务器的优点包括：

- 它们可以与不支持 HTTP/1.1 Host 标头的旧客户机一起使用。
- 提供 SSL 支持比较简便。

缺点包括：

- 它们要求更改主机上的配置 （实际或虚拟网络接口的配置）。
- 它们的使用规模有限，不适合具有数千个虚拟服务器的配置。

两种配置都要求为三种名称设置名称 - 地址映射。在基于 IP 地址的配置中，每个名称都映射为不同的地址。必须对主机进行设置，才能接收所有这些地址上的连接。在基于 URL 主机的配置中，所有名称都可以映射为同一地址 （计算机最初具有的地址）。

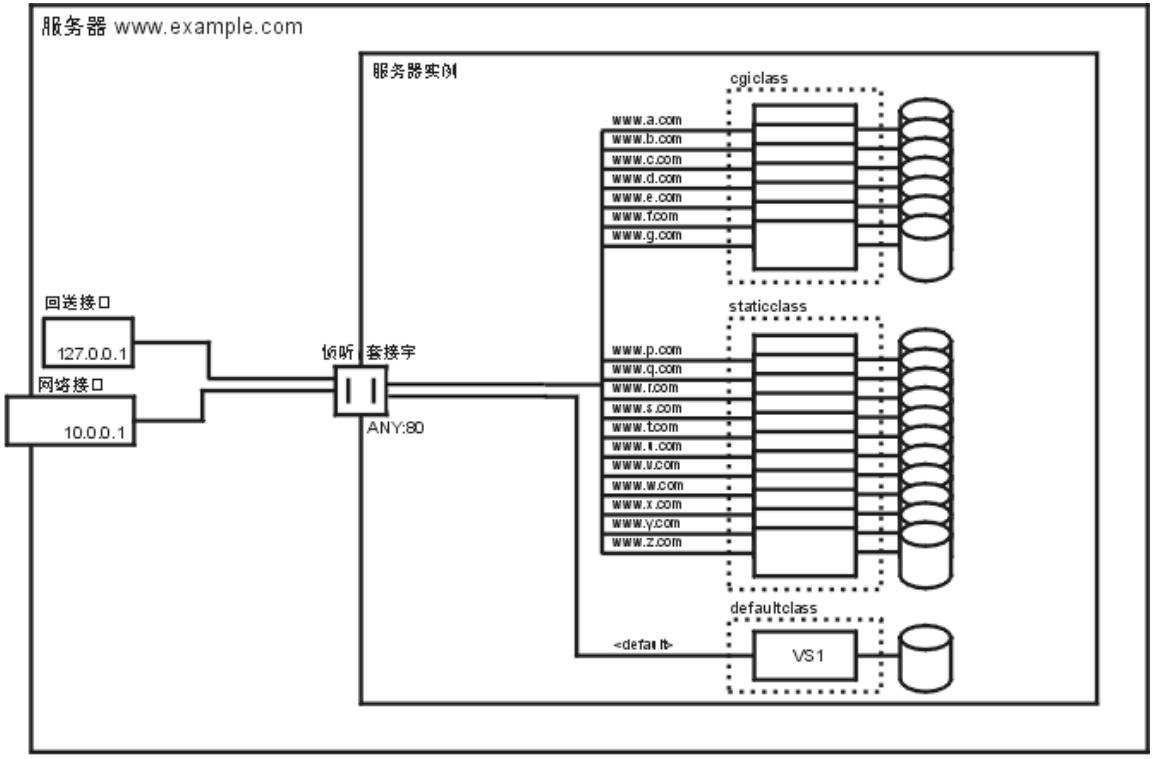
具有多个侦听套接字的配置所带来的性能增益可能最少，因为服务器不必查明传入请求的地址。但是由于其他接收方线程，使用多个侦听套接字也将导致额外负担（内存和调度）。

实例 4：海量宿主

海量宿主是一个可以启用许多低通信量虚拟服务器的配置。例如， ISP （承载许多低通信量的个人主页）便属于海量宿主。

虚拟服务器通常基于 URL 主机并属于多个虚拟服务器类之一，这取决于所提供的服务的级别。例如，可能有一个类只允许静态内容，而另一个类允许静态内容和 CGI。

海量宿主



请注意，安装服务器 VS1 时安装的虚拟服务器仍然存在于 `defaultclass` 中。

第 14 章

创建和配置虚拟服务器

一个虚拟服务器类与多台虚拟服务器 （类的成员）相关联。您可以在虚拟服务器级别覆盖某些类级别的设置。本章介绍如何创建和配置单个虚拟服务器。有关配置虚拟服务器类的信息，请参见 “内容管理”。有关虚拟服务器的概述，请参见 “使用虚拟服务器”。

本章包括以下部分：

创建虚拟服务器

使用虚拟服务器，您只需安装一台服务器便可以为多个公司或个人提供域名、 IP 地址以及某些服务器管理功能。有关虚拟服务器的简介以及在 Sun ONE Web Sever 中对其进行设置的方法，请参见 “使用虚拟服务器”。

要创建虚拟服务器，请执行以下步骤：

1. 在 Class Manager 中，选择 “Virtual Servers”选项卡。
2. 单击 “Add a Virtual Server”。
3. 为虚拟服务器选择一个名称。
4. 为虚拟服务器选择一个 URL 主机。

   您可以键入多个 URL 主机并用空格分开。

5. 单击“OK”。

这些设置都是创建虚拟服务器所必需的。此外，您还可以使用此选项卡上的其他页面配置其他虚拟服务器设置。

编辑虚拟服务器设置

设置虚拟服务器后，即可对其进行编辑。您可以通过两种方式进行这些编辑：使用 Class Manager 或 Virtual Server Manager。

在 Class Manager 中，页面是按照要编辑的设置的种类组织的。例如，您可以转至“Quality of Service”页面并更改类中一台或多台虚拟服务器的服务质量设置。

在 Virtual Server Manager 中，页面仅与一台虚拟服务器相关，这使您可以查看并更改它的所有设置。

使用 Class Manager 进行编辑

可以使用以下 Class Manager 页面编辑虚拟服务器设置。

编辑虚拟服务器设置

要编辑虚拟服务器的常规设置，请使用 “Edit Virtual Servers”页面。要访问此页面，请执行以下步骤：

1. 在 Class Manager 中，单击 “Virtual Servers”选项卡。
2. 单击 “Edit Virtual Servers”。
3. 要编辑虚拟服务器，请单击所需虚拟服务器旁边的下拉列表，然后选择 “Edit”或 “Delete”。

   对于缺省虚拟服务器，只能进行编辑，不能删除。

4. 将 “State”设置为 “On”、“Off”或 “Disabled”。

   如果将 “State”设置为 “Disabled”，您可以重新打开该服务器，但服务器的终端用户则不能。

   此状态是虚拟服务器的状态，与服务器实例的打开或关闭状态无关。如果此页面中显示虚拟服务器处于打开状态，则虚拟服务器仅在服务器实例也处于打开状态时才能接受请求。

   缺省服务器实例的缺省虚拟服务器也是如此。如果关闭服务器实例，则缺省虚拟服务器仍设置为 “On”，但不能接受连接请求。

   您不能关闭或禁用服务器实例的缺省虚拟服务器。

5. 键入要使用的 URL 主机 （如果与 “Urlhost”列下显示的不同）。

   您可以键入多个 URL 主机并用空格分开。

6. 完成虚拟服务器的编辑后，单击 “OK”。

配置虚拟服务器的 MIME 设置

您可以为单个虚拟服务器设置 MIME 类型文件。 MIME 类型文件包含文件扩展名针对文件类型的映射。例如，您可以在 MIME 类型文件中指定所有扩展名为 `.cgi` 的文件都被作为 CGI 文件处理。

您无需为每台虚拟服务器或每个虚拟服务器类创建单独的 MIME 类型文件。相反，您可以根据需要创建任意数量的 MIME 类型文件，然后将它们与一台虚拟服务器相关联。默认情况下，服务器上存在一个 MIME 类型文件 `mime.types`。要创建新的 MIME 类型文件，或者要编辑 MIME 类型文件中的定义，请参见第 214 页上的 “选择 MIME 类型”。

要设置特定虚拟服务器的 MIME 类型文件，请执行以下步骤：

1. 在 Class Manager 中，单击 “Virtual Servers”选项卡。
2. 单击 “MIME Settings”。
3. 从虚拟服务器旁边的下拉列表中选择一个 MIME 类型文件。
4. 单击 “OK”。

配置虚拟服务器的 ACL 设置

您可以使用 ACL 控制对虚拟服务器的访问。每台虚拟服务器在 LDAP 数据库中都可以有一个不同的基本 DN，因此每台虚拟服务器在 Sun ONE Web Server 使用的单一 LDAP 数据库中都可以有其自己的条目。

有关详细信息，请参见第 197 页上的 “控制虚拟服务器的访问”。

配置虚拟服务器的安全性

如果将虚拟服务器绑定到一个安全侦听套接字，则可以为其设置安全性。

有关安全性的详细信息，请参见第 4 章 “用于 Web 容器和 Web 应用程序的 基于 J2EE 的安全性”。

配置虚拟服务器的服务质量设置

服务质量是指为虚拟服务器设置的性能限制。例如， ISP 可能会根据虚拟服务器允许使用的带宽收取不同的费用。

您可以在 Server Manager 的 “Status”选项卡中为整个服务器或某个虚拟服务器类启用这些设置。不过，您可以为单个虚拟服务器覆盖这些服务器或类级别的设置。

在为虚拟服务器启用服务质量之前，必须先为整个服务器启用服务质量，此外还要设置一些基本值。请参见第 237 页上的 “使用服务质量”。

要配置虚拟服务器的服务质量设置，请执行以下步骤：

1. 在 Class Manager 中，单击 “Virtual Servers”选项卡。
2. 单击 “Quality of Service”。

   屏幕将显示一个页面，列出该类中的所有虚拟服务器及其服务质量设置。
3. 要启用虚拟服务器的服务质量，请从下拉列表中选择 “Enable”。

   默认情况下，服务质量被禁用。启用服务质量会略微增加服务器的负担。
4. 设置虚拟服务器的最大带宽 （以每秒钟的字节数为单位）。
5. 选择是否强制最大带宽设置。

   如果选择强制最大带宽，当服务器达到其带宽限制时，额外的连接将被拒绝。

   如果未强制最大带宽，当超过最大值时，服务器将在错误日志中记录一条消息。

6. 选择虚拟服务器允许的最大连接数。

   该数值是处理的并行请求数。

7. 选择是否强制最大连接数设置。

   如果选择强制最大连接数，当服务器达到其限制时，额外的连接将被拒绝。

   如果未强制最大连接数，当超过最大值时，服务器将在错误日志中记录一条消息。

8. 单击“OK”。

有关服务质量功能限制的详细信息，请参见第 237 页上的“使用服务质量”。

配置虚拟服务器的日志设置

要更改虚拟服务器访问日志和错误日志的缺省位置，请执行以下步骤：

1. 在 Class Manager 中，单击“Virtual Servers”选项卡。
2. 单击“Logging Settings”。

   屏幕将显示一个页面，列出该类中的所有虚拟服务器及其错误日志的位置。

3. 输入错误日志和访问日志的绝对路径。路径必须已经存在。

   缺省情况下，所有虚拟服务器的访问消息和错误消息都记录在服务器实例的访问日志和错误日志中。如果希望虚拟服务器使用单独的日志文件，可以在此处进行设置。

4. 如果要将路径更改回缺省路径，请单击“Default”。
5. 单击“OK”。

要查看特定虚拟服务器的日志，请执行以下步骤：

1. 在 Virtual Server Manager 中，选择 “Logs”选项卡。
2. 单击 “View Access Log”或 “View Error Log”。
3. 选择要显示的条目数以及显示条件。

   例如，如果日志中包含所有虚拟服务器的条目，可以选择只显示特定虚拟服务器的条目。
4. 单击 “OK”。

启用虚拟服务器的日志功能

要启用虚拟服务器级别的日志功能，请执行以下步骤：

1. 转至该服务器实例的 Server Manager 中的 “Logs”选项卡，然后选择 “Log Preferences”。
2. 在 “Log File”字段中输入路径和文件名，创建一个新的访问日志。

   您还可以在 magnus.conf 中手动创建新的访问日志：

   将 `Init fn=init access="$accesslog"` 更改为 `Init fn=init access="newaccesslog"`
3. 选择 “Format”下的 “Only Log”并选中 “Virtual Server Id”。

   对于自定义格式，可以选择 “Custom Format”并将 `%vsid%` 添加到该行的末尾。

   使用多台虚拟服务器时， `%vsid%` 会很有用。此条目用于在访问日志中记录 vsid（虚拟服务器 ID）。

   您还可以手动将 `%vsid%` 添加到 `magnus.conf` 文件中的 `Init fn` 的末尾。
4. 单击 “OK”。
5. 单击 “Apply”。
6. 单击 “Apply Changes”使所做的更改生效。

配置虚拟服务器的 Java Web 应用程序设置

Web 应用程序是 Java Servlet、JSP、HTML 页面、类以及其他资源的集合。所有资源都存储在一个目录中，对该目录的所有请求都将运行该应用程序。要部署和编辑特定虚拟服务器的 Web 应用程序，可以使用 Virtual Server Manager 中的 “Web Applications”选项卡下的各个页面。

有关 Web 应用程序和 Web 应用程序的部署描述符文件 `sun-web.xml` 的详细信息，请参见 Sun ONE Web Server 6.1 *Administrator's Configuration File Reference*。

使用 Virtual Server Manager 进行编辑

Virtual Server Manager 包含四个选项卡：Preferences、 Logs、 Web Applications 和 WebDAV。

“Preferences”选项卡包含以下页面：

- Status
- Settings

“Status”页面列出了一些设置并提供了虚拟服务器的访问日志和错误日志的链接。

“Settings”页面包含虚拟服务器的以下设置：

- 状态 （开或关）
- 文档根目录
- 访问日志和错误日志目录
- 目录服务
- ACL 文件
- MIME 类型文件
- CGI 设置

如果编辑单个虚拟服务器，则使用 Virtual Server Manager 并在一个页面上更改所有这些设置会很方便。

“Logs”选项卡只包含一个页面，使您可以为选定的虚拟服务器生成报告。

有关部署和编辑 Web 应用程序文件的详细信息，请参见第 16 章 “使用程序扩展服务器”。

使用 “WebDAV”选项卡，可以在虚拟服务器上创建和编辑 WebDAV 集合。WebDAV 集合是为 WebDAV 操作启用的一个或一组资源。使用 WebDAV，可以直接在 Web 上与其他人协作进行文档制作。 WebDAV 允许您在启用了 WebDAV 的资源上放置不同级别的锁，从而可以有效地避免在 Web 上进行协作内容制作时发生覆盖冲突。

“WebDAV”选项卡包含以下页面：

- “Add Collection”页面
- “Edit DAV Collection”页面
- “Lock Management”页面

“Add Collection”页面可用于创建 WebDAV 连接。

“Edit DAV Collection”页面可用于配置启用了 WebDAV 的集合。

“Lock Management”页面可用于查看与服务器上启用了 WebDAV 的资源相关的现有锁以及与锁有关的其他信息。

有关详细信息，请参见 “第 19 章 “使用 WebDAV 进行 Web 发布””。

为虚拟服务器生成报告

现在，您可以使用 Virtual Server Manager 为单个虚拟服务器生成报告。要执行此操作，首先要创建一个供虚拟服务器使用的新的访问日志并将其添加到虚拟服务器的设置中，如下所述。

要为虚拟服务器生成报告，请执行以下步骤：

1. 转至该服务器实例的 Server Manager 中的 “Logs”选项卡，然后选择 “Log Preferences”。
2. 在 “Log File”字段中输入路径和文件名，创建一个新的访问日志。

   您还可以在 magnus.conf 中手动创建新的访问日志：

   将 `Init fn=init access="$accesslog"` 更改为 `Init fn=init access="newaccesslog"`

3. 选择 “Format”下的 “Only Log”并选中 “Virtual Server Id”。

   对于自定义格式，可以选择 “Custom Format”并将 `%vsid%` 添加到该行的末尾。

   使用多台虚拟服务器时， `%vsid%` 会很有用。此条目用于在访问日志中记录 vsid（虚拟服务器 ID）。

   您还可以手动将 `%vsid%` 添加到 `magnus.conf` 文件中的 `Init fn` 的末尾。

4. 单击 “OK”。
5. 单击 “Apply”。
6. 单击 “Apply Changes”使所做的更改生效。
7. 选择要为其生成报告的虚拟服务器，转至 Virtual Server Manager 的 “Manage Classes”，然后从树视图中选择该虚拟服务器。
8. 转至 “Preferences”选项卡并选择 “Settings”。

   在 “Access Log”字段中，将访问日志更改为新创建的日志。

9. 单击 “OK”。
10. 单击 “Apply”。
11. 单击 “Apply Changes”使所做的更改生效。
12. 选择 “Logs”选项卡。

    将显示 “Generate Reports”页面。

    除非已创建虚拟服务器且 `LogVSid` 被设置为 “On”，否则将不会显示此页面。有关启用 “Virtual Server Id”的详细信息，请参见 “启用虚拟服务器的日志功能”。

13. （可选）如果需要，可以更改设置。
14. 单击 “OK”生成报告。

选择虚拟服务器的目录服务

您可以为特定的虚拟服务器指定特定的目录服务。执行此操作时，所选择的目录服务将记录在 `server.xml` 文件中相应 `VS` （虚拟服务器）元素的 `USERDB` 元素下。以后，服务器将使用与此目录服务相关联的权限来评估并强制执行访问控制规则。

要为虚拟服务器指定目录服务，请执行以下步骤：

1. 在 Virtual Server Manager 中，选择 “Settings”选项卡。

   将显示虚拟服务器的设置列表。

2. 单击 “Directory Services”旁边的 “Edit”链接。

   将在一个新窗口中启动 “Pick Directory Services for Virtual Server”页面。

3. 选择一个目录服务并单击 “OK”。

4. 保存并应用所做的更改。

注 为特定虚拟服务器选择的目录服务不能与其他虚拟服务器共享，而访问控制文件则可以在虚拟服务器之间共享。

删除虚拟服务器

要删除虚拟服务器，请执行以下步骤：

1. 在 Class Manager 中，单击 “Virtual Servers”选项卡。

2. 单击 “Edit Virtual Servers”。

3. 从所需虚拟服务器旁边的下拉列表中选择 “Delete”。

   不能删除在安装服务器时创建的缺省虚拟服务器。

4. 单击 “OK”。

   该虚拟服务器将被删除。

第 15 章

内容管理

本章介绍如何配置和管理虚拟服务器类以及虚拟服务器的内容。

本章包括以下部分：

设置主文档目录

主文档目录（也称为文档根目录）是您在其中存储了希望供远程客户机使用的所有文件的中心目录。

添加类时，您需要使用绝对路径来指定文档目录。如果没有在路径中使用变量，则类中每个虚拟服务器的文档根目录将默认使用相同的目录。然后，您可以在 Class Manager 中分别进行更改。

另一种方法是在设置类的路径时使用变量。例如，可以使用 `$id` 变量为类中每个虚拟服务器创建一个名称中带有虚拟服务器 ID 的目录。您可以将类的文档根目录设置为 *class_doc_root*/$id。使用此路径时，如果类的文档目录是 `/sun/servers/docs/$id`，则属于此类的虚拟服务器 `vs1` 的缺省文档目录将是 `/sun/servers/docs/vs1`。

有关文档目录以及如何在服务器实例、类和虚拟服务器级别使用文档目录的更多信息，请参见第 292 页上的 “文档根目录”。

要更改主文档目录以便使用其他路径或变量，请执行以下步骤：

1. 在 Class Manager 中，单击 “Content Management” 选项卡。
2. 单击 “Primary Document Directory”。
3. 在虚拟服务器旁边输入绝对目录路径或变量（或路径与变量的组合）。

   如果在文档根目录绝对路径的末尾处包含了变量 $id，则默认情况下，每个虚拟服务器的缺省文档根目录将是 *class_doc_root*/*virtual_server_ID*。例如，如果类的文档目录是 `/sun/servers/docs/$id`，则属于该类的虚拟服务器 `vs1` 的缺省文档目录为 `/sun/servers/docs/vs1`。

   有关变量的更多信息，请参见第 296 页上的 “使用变量”。
4. 单击 “OK”。

有关更多信息，请参见联机帮助中的 “Primary Document Directory”。

注 通常，每个虚拟服务器都有其自己的主文档目录。

设置其他文档目录

多数情况下，虚拟服务器或服务器实例的文档位于主文档目录中。但是，有时候您可能希望从主文档目录之外的目录提供文档。这可以通过设置其他文档目录来完成。通过从文档根目录之外的目录提供文档，您可以让其他用户管理文档组而无需赋予他们访问您的主文档根目录的权限。

如果设置其他文档目录时未使用变量，该目录将设置在类级别，并且由类中的所有虚拟服务器使用。

如果希望为类中的单个虚拟服务器设置其他文档目录，则必须使用变量，以使每个虚拟服务器的 URL 前缀映射到不同的目录。

要添加其他文档目录，请执行以下步骤：

1. 在 Class Manager 中，单击“Content Management”选项卡。
2. 单击“Additional Document Directories”。
3. 选择要映射的 URL 前缀。

   客户机在需要文档时将此 URL 发送到服务器。
4. 指定要将 URL 映射到的目录。
5. 要执行此操作，请使用一个现有的配置式样指定如何配置此目录。
6. 单击“OK”。

有关更多信息，请参见联机帮助中的“Additional Document Directories”。

默认情况下，服务器实例具有若干其他文档目录。这些文档目录具有以下前缀：

- `/manual`
- `/servlet`

您应当限制对这些目录的访问，使用户无法对其进行写入操作。下面是一个 ACL 样例：

```
deny (all) anyone;
allow (rxli) all;
allow (wd) privileged_user;
```

自定义用户公共信息目录 (UNIX/Linux)

有时用户会希望维护他们自己的 Web 页面。您可以配置公共信息目录，使服务器中的所有用户可以创建主页和其他文档而无需您的介入。

您只能为整个类进行这些设置，而不能基于每个虚拟服务器进行自定义设置。

通过此系统，客户机可以使用服务器将其识别为公共信息目录的 URL 来访问服务器。例如，假设您选择了前缀 ~ 和目录 public_html。如果收到一个对 http://www.sun.com/~jdoe/aboutjane.html 的请求，服务器将会认为 ~jdoe 指向一个用户的公共信息目录。服务器将在系统的用户数据库中查找 jdoe 并找到 Jane 的主目录。然后，服务器将视察 ~/jdoe/public_html/aboutjane.html。

要将服务器配置为使用公共目录，请执行以下步骤：

1. 在 Class Manager 中，单击 “Content Management”选项卡。
2. 单击 “User Document Directories”。
3. 选择用户 URL 前缀。

   该前缀通常为 ~，因为此波浪号字符是用于访问用户主目录的标准 UNIX/Linux 前缀。
4. 选择用户主目录中的子目录，服务器要在其中查找 HTML 文件。

   通常，该目录为 public_html。
5. 指定密码文件。

   服务器需要知道可以在何处找到列出了您的系统用户的文件。服务器使用该文件来确定有效的用户名并找到其主目录。如果您将系统密码文件用于此用途，服务器将使用标准库调用来查找用户。您也可以创建另一个用户文件来查找用户。您可以指定该用户文件的绝对路径。

   该文件中的每一行都应具有以下结构 （以 * 号表示 /etc/passwd 文件中不需要的元素）：

   ```
   username:*:*:groupid:*:homedir:*
   ```
6. 选择是否在启动时装入密码数据库。

   有关更多信息，请参见第 323 页上的 “启动时装入整个密码文件”。
7. 选择是否应用配置式样。
8. 单击 “OK”。

有关更多信息，请参见联机帮助中的 “User Document Directories”。

为用户提供独立的目录的另一种方法是：创建一个映射到所有用户都可以修改的中心目录的 URL。

限制内容发布

在某些情况下，系统管理员可能希望限制某些用户帐户，使其无法通过用户文档目录来发布内容。要限制某个用户的发布操作，请在 `/etc/passwd` 文件中该用户主目录路径的末尾添加一个斜杠：

```
jdoe::1234:1234:John Doe:/home/jdoe:/bin/sh
```

成为：

```
jdoe::1234:1234:John Doe:/home/jdoe/:/bin/sh
```

进行此修改后， Sun ONE Web Server 将不支持来自该用户的目录的页面。请求该 URI 的浏览器会收到 “404 File Not Found”错误，并且 Web Server 访问日志中将记录一个 404 错误。不会向错误日志中记录任何错误。

如果后来您又决定允许该用户发布内容，则可以从 `/etc/passwd` 条目中删除添加的斜杠，然后重新启动 Web 服务器。

启动时装入整个密码文件

您还可以选择在启动时装入完整的口令文件。如果选择此选项，服务器在启动时会将密码文件装入内存，以便用户可以更快地进行查找。但是，如果密码文件非常大，此选项会占用过多内存。

使用配置式样

您可以为服务器应用某种配置式样，以控制对公共信息目录中的目录的访问。这将禁止用户创建指向您不希望公开的信息的符号链接。有关配置文件的更多信息，请参见第 17 章 “应用配置式样”。

启用远程文件操作

启用远程文件操作后，客户机可以在您的服务器中进行以下操作：上载文件、删除文件、创建目录、删除目录、列出目录内容以及重命名文件。*server_root*/https-*serve-id*/config 目录中的文件 obj.conf 包含了启用远程文件操作时激活的命令。激活这些命令后，远程浏览器便可以更改服务器中的文档。您应当使用访问控制来限制对这些资源的写入操作，以防止未经授权的更改操作。

请注意，启用远程文件操作不会影响内容管理系统 （如 Microsoft Frontpage）的使用。

UNIX/Linux：您必须拥有访问文件的正确权限，否则该功能将无法使用；也就是说，文档根目录的用户必须与服务器的用户相同。

要启用远程文件操作，请执行以下步骤：

1. 在 Class Manager 中，单击 “Content Management”选项卡。
2. 单击 “Remote File Manipulation”。
3. 选择激活远程文件操作。
4. 单击 “OK”。

有关更多信息，请参见联机帮助中的 “Remote File Manipulation”。

配置文档首选项

可以使用 “Document Preferences”来设置文档首选项。本部分包括以下主题：

- 设置文档首选项
- 输入索引文件名
- 选择目录索引
- 指定服务器主页
- 指定缺省 MIME 类型

这些设置是为类而不是为单个虚拟服务器配置的。

设置文档首选项

要设置文档首选项，请执行以下步骤：

1. 在 Class Manager 中，单击 “Content Management”选项卡。
2. 单击 “Document Preferences”。
3. 选择相应的字段值，如以下各节所述。
4. 单击 “OK”。

以下各节详细介绍了您可以设置的首选项。有关更多信息，请参见联机帮助中的 “Document Preferences”。

输入索引文件名

如果没有在 URL 中指定文档的名称，服务器将自动显示索引文件。缺省的索引文件是 `index.html` 和 `home.html`。如果指定了多个索引文件，服务器将按照此字段中显示的文件名的顺序进行查找，直至找到一个文件。例如，如果索引文件名为 `index.html` 和 `home.html`，则服务器将查找 `index.html`，如果未找到该文件则查找 `home.html`。

选择目录索引

一个文档目录可能有若干个子目录。例如，可能有一个名为 `products` 的子目录，以及另一个名为 `people` 的子目录等等。通常，使客户机能够访问这些目录的概述（或索引）会很有用处。

服务器通过搜索一个名为 `index.html` 或 `home.html` 的索引文件 （您将该文件作为目录内容的概述进行创建和维护）来索引目录。有关更多信息，请参见上一节第 325 页上的 “输入索引文件名”。您可以通过将任何文件命名为这些缺省名称中的一个，将其指定为目录的索引文件，这意味着您也可以使用 CGI 程序作为索引 （如果激活了 CGI）。

如果未找到索引文件，服务器将在文档目录中生成一个列出所有文件的索引文件。

注意 如果服务器在防火墙外，请关闭目录索引，以确保目录结构和文件名不可访问。

指定服务器主页

当终端用户第一次访问服务器时，他们看到的第一个文件通常称为主页。通常，此文件包含服务器的常规信息和指向其他文档的链接。

默认情况下，服务器将查找在 “Document Preferences”的 “Index Filename”字段中指定的索引文件并将其用作主页。不过，您也可以指定某个文件作为主页。

指定缺省 MIME 类型

当文档发送到客户机时，服务器中的某一部分将识别该文档的类型，从而使客户机能够正确地显示文档。但是，服务器有时无法确定文档的正确类型，因为服务器中没有定义该文档的扩展名。在这种情况下，将发送缺省值。

缺省值通常为 text/plain，但是您应当将其设置为服务器中存储的最常见的文件类型。下面列出了一些常用的 MIME 类型：

- `text/plain`
- `text/richtext`
- `image/jpeg`
- `application/x-tar`
- `application/x-gzip`
- `text/html`
- `image/tiff`
- `image/gif`
- `application/postscript`
- `audio/basic`

配置 URL 转发

URL 转发使您可以将文档请求重定向到另一个服务器。转发 URL 或重定向是一种服务器用来通知用户 URL 已经发生更改 （例如， URL 由于文件已移动到其他目录或其他服务器而发生更改）的方法。您还可以使用重定向将对某服务器中的某文档的用户请求无缝发送到另一个服务器中的文档。

例如，如果将 `http://www.sun.com/info/movies` 转发至前缀 `film.sun.com`，则 URL `http://www.sun.com/info/movies` 将重定向至 `http://film.sun.com/info/movies`。

您可以使用变量将目录映射到新目录。例如，可以将 `/new` 映射到 `/$docroot/new`。这将映射到虚拟服务器的文档根目录。

有关变量的更多信息，请参见第 296 页上的 “使用变量”。

有时，您可能希望将对一个子目录中所有文档的请求重定向到特定的 URL。例如，如果必须删除某个目录（因为该目录产生的通信量过大，或者由于某种原因不再为该目录中的文档提供服务），则可以将对其中任何文档的请求定向到一个解释了该文档为何不再可用的页面。例如，可以将 `/info/movies` 中的前缀重定向到 `http://www.sun.com/explain.html`。

要配置 URL 转发，请执行以下步骤：

1. 在 Class Manager 中，单击“Content Management”选项卡。
2. 单击“URL Forwarding”。
3. 键入要重定向的 URL 前缀，并确定是将其重定向到另一个前缀还是一个静态 URL。
4. 单击“OK”。

有关更多信息，请参见联机帮助中的“URL Forwarding”。

自定义错误响应

您可以指定当客户机遇到错误时由虚拟服务器向客户机发送详细消息的自定义错误响应。可以指定要发送的文件或要运行的 CGI 程序。

例如，您可以更改服务器收到特定目录的错误时的响应方式。如果客户机尝试连接受访问控制保护的服务器内容，您可以返回一个其中包括如何获得说明信息的错误文件。

在启用自定义错误响应之前，必须创建为响应错误而发送的 HTML 文件或运行的 CGI 程序。创建后，在 Class Manager 中启用该响应。

要启用自定义错误响应，请执行以下步骤：

1. 在 Class Manager 中，单击“Content Management”选项卡。
2. 单击“Error Responses”。
3. 从 Resource Picker 中选择“Entire Server”将所做的更改应用到整个类，或者浏览到特定虚拟服务器的文档根目录，或者浏览到特定虚拟服务器中的特定目录。
4. 对于每个要更改的错误代码，请指定包含该错误响应的文件或 CGI 的绝对路径。
5. 单击“OK”。

有关更多信息，请参见联机帮助中的“Error Response”。

更改字符集

文档的字符集一部分取决于编写文档所用的语言。您可以通过选择资源并输入该资源的字符集来覆盖用于文档、文档集或目录的客户机的缺省字符集设置。

Netscape Navigator 可以在 HTTP 中使用 MIME 类型的 `charset` 参数来更改其字符集。如果服务器的响应中包含此参数， Netscape Navigator 将相应地更改其字符集。请参见以下示例：

- `Content-Type:text/html;charset=iso-8859-1`
- `Content-Type:text/html;charset=iso-2022-jp`

RFC 1700 中指定了 Netscape Navigator 识别的以下 `charset` 名称 （以 `x-` 开头的名称除外）：

- `us-ascii`
- `iso-2022-jp`
- `x-euc-jp`
- `iso-8859-1`
- `x-sjis`
- `x-mac-roman`

此外，以下是得到认可的 `us-ascii` 的别名：

- `ansi_x3.4-1968`
- `ansi_x3.4-1986`
- `ascii`
- `us`
- `cp367`
- `iso-ir-6`
- `iso_646.irv:1991`
- `iso646-us`
- `ibm367`

以下是得到认可的 `iso_8859-1` 的别名：

- `latin1`
- `iso_8859-1:1987`
- `ibm819`
- `iso_8859-1`
- iso-ir-100
- `cp819`

要更改字符集，请执行以下步骤：

1. 在 Class Manager 中，单击 “Content Management”选项卡。
2. 单击 “International Characters”。
3. 从 Resource Picker 中选择 “Entire Server”将所做的更改应用到整个类，或者浏览到特定虚拟服务器的文档根目录，或者浏览到特定虚拟服务器中的特定目录。
4. 为整个服务器或部分服务器设置字符集。

   如果将此字段保留为空，字符集将设置为 NONE。
5. 单击 “OK”。

有关更多信息，请参见联机帮助中的 “International Characters”。

设置文档页脚

您可以为服务器某一部分中的所有文档指定文档页脚，其中可以包含上次修改时间。除 CGI 脚本的输出信息或经分析的 HTML (.shtml) 文件外的所有文件都可以使用页脚。如果需要在 CGI 脚本的输出信息或经分析的 HTML 文件中显示文档页脚，请将页脚文本输入到单独的文件中并添加一行代码或另一个服务器端语句，以便将此文件附加到页面的输出信息中。

要设置文档页角，请执行以下步骤：

1. 在 Class Manager 中，单击 “Content Management”选项卡。
2. 单击 “Document Footer”。
3. 从 Resource Picker 中选择 “Entire Server”将所做的更改应用到整个类，或者浏览到特定虚拟服务器的文档根目录，或者浏览到特定虚拟服务器中的特定目录。

   如果选择了一个目录，则文档页脚仅在服务器收到该目录或该目录中任何文件的 URL 时才会应用。
4. 指定希望包含页脚的文件类型。
5. 指定日期格式。
6. 输入希望显示在页脚中的文本。

   文档页脚的字符数最多为 765 个。如果希望在页脚中包含文档的上次修改日期，请键入字符串 `:LASTMOD:`。

7. 单击 “OK”。

有关更多信息，请参见联机帮助中的 “Document Footer”。

使用 htaccess

有关使用 htaccess 的信息，请参见第 188 页上的 “使用 .htaccess 文件”。

限制符号链接 (UNIX/Linux)

您可以在服务器中限制文件系统链接的使用。文件系统链接是对存储在其他目录和文件系统中的文件的引用。使用引用，用户可以象访问当前目录中的文件一样访问远程文件。文件系统链接有两种类型：

- **硬链接** — 硬链接实际上是指向相同数据块集的两个文件名；原始文件和链接是相同的。因此，硬链接不能位于不同的文件系统上。
- **符号 （软）链接** — 符号链接包含两个文件；原始文件包含数据，另一个文件指向该原始文件。符号链接比硬链接更灵活。符号链接可以用于不同的文件系统，还可以链接到目录。

有关硬链接和符号链接的更多信息，请参见 UNIX/Linux 系统文档。

使用文件系统链接可以方便地创建指向位于主文档目录之外的文档的指针，并且任何人都可以创建这些链接。因此，您可能会担心有人会创建指向敏感文件 （例如，机密文件或系统密码文件）的指针。

要限制符号链接，请执行以下步骤：

1. 在 Class Manager 中，单击 “Content Management”选项卡。
2. 单击 “Symbolic Links”。
3. 从 Resource Picker 中选择 “Entire Server”将所做的更改应用到整个类，或者浏览到特定虚拟服务器的文档根目录，或者浏览到特定虚拟服务器中的特定目录。
4. 选择是否启用软链接和 / 或硬链接以及起始目录。
5. 单击 “OK”。

有关更多信息，请参见联机帮助中的 “Symbolic Link”。

设置服务器分析的 HTML

通常情况下， HTML 发送到客户机时就像它存储在磁盘上一样，无需服务器进行任何干预。但是，服务器可以在发送文档之前搜索 HTML 文件以查找特定的命令（也就是说，服务器可以分析 HTML）。如果希望服务器分析这些文件并在文档中插入特定于请求的信息或文件，必须首先启用 HTML 分析。

要分析 HTML，请执行以下步骤：

1. 在 Class Manager 中，单击 “Content Management”选项卡。
2. 单击 “Parse HTML”。
3. 选择服务器要为其分析 HTML 的资源。

   从 Resource Picker 中选择 “Entire Server”将所做的更改应用到整个类，或者浏览到特定虚拟服务器的文档根目录，或者浏览到特定虚拟服务器中的特定目录。

   如果选择一个目录，则服务器仅在收到该目录和该目录中任何文件的 URL 时才分析 HTML。
4. 选择是否激活服务器分析的 HTML。

   您可以为 HTML 文件而不为 exec 标记进行激活，也可以为 HTML 文件和 exec 标记同时进行激活，后一种方式允许 HTML 文件在服务器中执行其他程序。
5. 选择要分析的文件。

   您可以选择是只分析扩展名为 .shtml 的文件还是分析所有 HTML 文件 （分析所有 HTML 文件会降低性能）。如果使用的是 UNIX/Linux，还可以选择分析开启了执行权限的 UNIX/Linux 文件，但是这样做不可靠。
6. 单击 “OK”。

有关设置服务器以接受经分析的 HTML 的更多信息，请参见联机帮助中的 “Parse HTML”。

有关使用服务器分析的 HTML 的详细信息，请参见 Sun ONE Web Server 6.1 *Programmer's Guide*。

设置高速缓存控制指令

Sun ONE Web Server 通过高速缓存控制指令控制代理服务器高速缓存的信息。使用高速缓存控制指令，可以覆盖代理的缺省高速缓存，以防止以后对敏感信息进行高速缓存，或对其进行检索。代理服务器必须遵循 HTTP 1.1 协议，才能使这些指令正常运行。

有关 HTTP 1.1 的更多信息，请参见超文本传输协议 — HTTP/1.1 规范 (RFC 2068)，该规范位于以下位置：

http://www.ietf.org/

要设置高速缓存控制指令，请执行以下步骤：

1. 在 Class Manager 中，单击 “Content Management” 选项卡。
2. 单击 “Cache Control Directives”。
3. 填写各个字段。响应指令的有效值如下：
   - **Public**。该响应可以被任何高速缓存进行缓存。这是缺省值。
   - **Private**。该响应只能被专用 （非共享）的高速缓存进行缓存。
   - **No Cache**。不能在任何地方高速缓存该响应。
   - **No Store**。高速缓存不应将请求或响应存储到非易失性存储器中的任何地方。
   - **Must Revalidate**。高速缓存条目必须在原始服务器中进行重新验证。
   - **Maximum Age (sec)**。客户机不接受寿命长于此设置的响应。
4. 单击 “OK”。

有关更多信息，请参见联机帮助中的 “Cache Control Directives”。

使用更强大的加密算法

有关设置更强大的加密算法的信息，请参见第 137 页上的 “设置更强大的加密算法”。

配置服务器的内容压缩

Sun ONE Web Server 6.1 支持 HTTP 内容压缩。内容压缩可以提高向客户机提供内容的速度，同时可以提供更多内容，而无需增加硬件的消耗。内容压缩减少了内容的下载时间，对使用拨号连接和高流量连接的用户尤其有用。

通过内容压缩， Web 服务器可以发送压缩的数据并同时指示浏览器如何解压缩数据，这减少了发送数据的数量并提高了页面的显示速度。

可以通过两种方式配置服务器以便处理压缩数据：

- 配置服务器以提供预压缩的内容
- 将服务器配置为根据需要压缩内容

有关增强服务器压缩处理能力的信息，请参见 obj.conf 中与压缩相关的更改。

配置服务器以提供预压缩的内容

您可以配置 Sun ONE Web Server 以便在指定的目录中生成和存储文件的预压缩版本。进行这种配置后 （且仅当收到 `Accept-encoding:gzip` 标头时），对配置为提供预压缩内容的目录中的文件的所有请求将重定向为对该目录中的等效压缩文件（如果存在）的请求。例如， Web 服务器收到对 `myfile.html` 的请求，且 `myfile.html` 和 `myfile.html.gz` 都存在，则那些带有相应 `Accept-encoding` 标头的请求将接收压缩的文件。

要将服务器配置为提供预压缩内容，请执行以下步骤：

1. 在 Class Manager 中，单击 “Content Management”选项卡。
2. 单击 “Serve Precompressed Content”。
3. 输入以下信息：
   - **Editing**。从下拉列表中选择要提供预压缩内容的资源。如果选择一个目录，则服务器仅在收到该目录和该目录中任何文件的 URL 时才提供预压缩内容。

     单击 “Browse”按钮浏览主文档目录，或单击 “Wildcard”按钮指定通配符模式。有关使用通配符模式的信息，请参见 “Resource Picker 中使用的通配符”。
   - **Activate Serving Precompressed Content?**允许您指示服务器为选定资源提供预压缩内容。

- **Check Age**。指定是否检查压缩版本是否早于非压缩版本。可能的值为“yes”和“no”

  如果设置为“yes”，则当压缩版本早于非压缩版本时将不会选择压缩版本。

  如果设置为“no”，将始终选择压缩版本，即使压缩版本早于非压缩版本。

  默认情况下，该值设置为“yes”。

- **Vary Header**。指定是否使用 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”。

4. 单击“OK”。

将服务器配置为根据需要压缩内容

您也可以配置 Sun ONE Web Server 6.1 以便在使用过程中压缩传输数据。自动生成的 HTML 页面仅在用户提出请求时才会存在。这对基于电子商务的 Web 应用程序和数据库驱动的站点尤其有用。

要将服务器配置为根据需要压缩内容，请执行以下步骤：

1. 在 Class Manager 中，单击“Content Management”选项卡。
2. 单击“Compress Content on Demand”。
3. 输入以下信息：

   - **Editing**。从下拉列表中选择要根据需要动态提供压缩内容的资源。如果选择一个目录，则服务器仅在收到该目录和该目录中任何文件的 URL 时才提供压缩内容。

     单击“Browse”按钮浏览主文档目录，或单击“Wildcard”按钮指定通配符模式。有关使用通配符模式的信息，请参见“Resource Picker 中使用的通配符”。

   - **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) 使用的内存片断大小 （以字节为单位）以控制一次压缩的量。缺省值为 `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。缺省值为 6，这将获得适中的速度和压缩效果。

4. 单击 “OK”。

obj.conf 中与压缩相关的更改

当服务器中启用了压缩后，将向 `obj.conf` 文件添加一个条目。下面显示了一个样例条目：

```
Output fn="insert-filter" filter="http-compression" type="text/*"
```

要将压缩仅限制为某个特定文档类型，或排除那些不能很好地处理压缩内容的浏览器，您可能需要编辑 `obj.conf` 文件。有关如何实现此目的的详细信息，请参见 Sun ONE Web Server 6.1 *NSAPI Programmer's Guide*。

第 16 章

使用程序扩展服务器

本章介绍如何在 Sun ONE Web Server 上安装可在响应客户机请求时动态生成 HTML 页面的程序。这些程序称为**服务器端应用程序**。（**客户端应用程序**将下载到客户机上并在客户端计算机上运行。）

本章包括以下部分：

服务器端程序概述

Java Servlet 和 CGI 程序具有不同的优点和用法。下表列出了这些服务器端程序之间的差异：

- Java Servlet 是用 Java 编写的， Java 是用于创建网络应用程序的编程语言，功能非常强大。
- CGI （通用网关接口）程序可以使用 C、 Perl 或其他编程语言编写。所有 CGI 程序均使用标准的方式在客户机与服务器之间传递信息。

服务器上运行的服务器端应用程序的类型

Sun ONE Web Server 可以运行以下类型的服务器端应用程序以动态生成内容：

- Java Servlet
- CGI 程序

Sun ONE Web Server 也可以运行扩展或修改服务器自身行为的程序。这些程序（称为插件）是使用 Netscape 服务器应用程序编程接口 (NSAPI) 编写的。有关编写和安装插件程序的信息，请参见 Sun ONE Web Server 6.1 *NSAPI Programmer's Guide*。

如何在服务器上安装服务器端应用程序

每个类型的程序在服务器上的安装方式都不同。下表概述了这些过程：

- 对于 Java Servlet，您可以创建和部署 Web 应用程序。有关详细信息，请参见第 340 页上的 “服务器运行 Servlet 所需的条件”。
- 对于 CGI 程序，您可以对服务器进行配置，使其能够识别具有某些文件扩展名的所有文件和 / 或指定目录 （如 CGI 程序）中的所有文件。有关详细信息，请参见第 347 页上的 “安装 CGI 程序”、第 351 页上的 “安装 Windows CGI 程序”和第 354 页上的 “安装 Windows Shell CGI 程序”。

这些安装过程将在以下各节中进行说明。

Java Servlet 和 JavaServer Pages (JSP)

本节介绍如何在 Sun ONE Web Server 上安装和使用 Java Servlet 和 JavaServer Pages。

其中包括以下主题：

Servlet 和 JavaServer Pages 概述

Sun ONE Web Server 6.1 支持 Servlet 2.3 API 规范，该规范允许将 Servlet 和 JSP 包括在 Web 应用程序中。

Web 应用程序是 Servlet、 JavaServer Pages、 HTML 文档和其他 Web 资源 （可能包括图像文件、压缩的归档文件和其他数据）的集合。 Web 应用程序可以打包至一个归档文件 （WAR 文件），也可以存在于打开的目录结构中。

注 Servlet API 2.3 版与 2.1 版完全兼容，因此所有现有的 Servlet 均可继续使用，而且无需修改或重新编译。

要开发 Servlet，请使用 Sun Microsystems 的 Java Servlet API。有关使用 Java Servlet API 的信息，请参见由 Sun Microsystems 提供的文档，其站点如下：

```
http://java.sun.com/products/servlet/index.jsp
```

JSP 是一个页面，同 HTML 页面很相似，可以在 Web 浏览器中查看。然而，除了 HTML 标记，它还可以包括一组与 Java 代码相混合的 JSP 标记和指令，用以扩展 Web 页面设计者将动态内容并入页面的能力。这些附加特性提供了诸如显示特性值和使用简单条件等功能。 Sun ONE Web Server 6.1 支持 JavaServer Pages (JSP) 1.2 API 规范。

注 请确保应用程序所请求的 URI 的大小写 （例如， `/foo.JSP`）与文件系统路径的规范大小写相匹配 （例如， `C:\Program Files\WebServer\docs\foo.jsp`）。这非常必要，因为 Sun ONE Web Server 6.1 Java Web 容器当前执行的模式匹配区分大小写。

有关创建 JSP 的信息，请参见 Sun Microsystems 的 JavaServer Pages，其 Web 站点如下：

```
http://java.sun.com/products/jsp/index.jsp
```

有关开发 Servlet 和 JSP 以与 Sun ONE Web Server 结合使用的信息，请参见 Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications*。

服务器运行 Servlet 所需的条件

Sun ONE Web Server 包括了 Java 开发工具 (JDK) 1.4.1_03 版。在旧版的 Web 服务器中， Java 在服务器范围内配置；而在 6.1 发行版中，您可以按 Web 服务器实例配置 Java。

您可以使用与 Sun ONE Web Server 6.1 捆绑的 JDK，也可以使用由您选择的 JDK（这时您必须指定 JDK 的路径）。有关如何执行此操作的详细信息，请参见第 263 页上的 “配置 JVM 设置”。

缺省情况下，安装 Sun ONE Web Server 时 Java 被禁用。要启用 Servlet，必须先启用 Java。

有关如何启用 Java 的信息，请参见第 261 页上的 “启用和禁用 Java”。

部署 Web 应用程序

以下各节将介绍如何使用 `wdeploy` 命令行实用程序手动部署、编辑或删除 Web 应用程序，以及如何通过用户界面执行这些操作。

使用 server.xml 文件

部署之后，缺省情况下您的 Web 应用程序将被启用。要手动禁用已部署的 Web 应用程序，需要修改 `server.xml` 文件，如下所示：

```
<VS>
<WEBAPP uri="/mywebapp" path="/webappdir" enabled = "false" >
</WEBAPP>

...

</VS>
```

如果无意中以同样的说明部署或编辑了多个 Web 应用程序，而且其中之一已被禁用，服务器将忽略 `enabled = "false"` 设置并继续使用 `enabled = "true"` 的缺省设置。

有关 `server.xml` 文件的详细信息，请参见 Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications*。

部署和编辑 Web 应用程序有以下两种方式：

- 使用 Administration Server 界面
- 使用命令行界面

使用 Administration Server 界面

使用 Sun ONE Web Server 6.1，您可以为某个指定的虚拟服务器部署、编辑、删除、启用和禁用 Web 应用程序。

部署 *Web* 应用程序

通过在 Virtual Server Manager 的 “Web Applications”选项卡下选择 “Deploy Web Applications”，可以访问 “Deploy Web Applications”。

要部署 Web 应用程序，请执行以下步骤：

1. 从 “WAR File On”下拉列表中选择 “Local Machine”或 “Server Machine”。

   要将 WAR 文件上载至服务器，请选择 “Local Machine”。如果已经存在 WAR 文件，请选择 “Server Machine”。

2. 在本地计算机或服务器计算机上，在提供的字段中输入包含 Web 应用程序的 `WAR` 文件的路径。

   在服务器计算机上，输入 WAR 文件的绝对路径。

   在本地计算计上，您可以浏览现有路径。单击 “browse”将显示 “File Upload”窗口，您可以选择要上载到服务器的 WAR 文件。

3. 在虚拟服务器上，在提供的字段中输入 Web 应用程序的 URI。

4. 输入服务器计算机上要提取 WAR 文件内容的目录的绝对路径。如果该目录不存在，将创建一个目录。

5. 单击 “OK”。

6. 单击 “Apply”。

7. 为要部署的 Web 应用程序选择 “Dynamic Reconfiguration”。

编辑 *Web* 应用程序

您可以编辑、删除、禁用或启用已部署的 Web 应用程序。通过在 Virtual Server Manager 的 “Web Applications”选项卡下选择 “Edit Web Applications”，可以访问 “Edit Web Applications”。

要编辑、删除、禁用或启用已部署的 Web 应用程序，请执行以下步骤：

1. 从正在编辑的 Web 应用程序旁边的 “Action”列中的下拉列表中，选择要执行的操作。请进行以下选择：
   - 选择 “Edit”，更改从中可以访问 Web 应用程序的 URI。
   - 选择 “Delete”，从 Web 应用程序文件中删除 Web 应用程序条目并删除部署该应用程序所在的目录。
   - 选择 “Disable”，使 Web 应用程序无法从 URI 访问，但不删除它。
   - 选择 “Enable”，重新激活先前被禁用的 Web 应用程序。

注意 删除 Web 应用程序将同时删除部署该应用程序所在的目录。

2. （可选）在 “URI”字段中输入新的 URI （如果正在编辑 Web 应用程序）。
3. 单击 “OK”。
4. 单击 “Apply”。
5. 为要部署的 Web 应用程序选择 “Dynamic Reconfiguration”。

使用命令行界面

在手动部署 Web 应用程序之前，您必须确保 *server_root*`/bin/https/httpsadmin/bin` 目录处于路径中，并且 `IWS_SERVER_HOME` 环境变量已设置为 *server_root* 目录。

要部署虚拟服务器 *Web* 应用程序：

您可以在命令行中使用 `wdeploy` 实用程序将 WAR 文件部署到虚拟服务器 Web 应用程序环境中：

```
wdeploy deploy -u <uri_path> -i <instance> -v <vs_id> [ [-V
<verboseLevel>]| [-q] ] [-n] [-d <directory>] <war_file>
```

删除虚拟服务器 *Web* 应用程序：

```
wdeploy delete -u <uri_path> -i <instance> -v <vs_id> [ [-V
<verboseLevel>] | [-q] ] [-n] hard|soft
```

列出虚拟服务器 *Web* 应用程序的 *URI* 和目录：

```
wdeploy list -i <instance> -v <vs_id> [ [-V <verboseLevel>] | [ -q] ]
```

以上命令参数具有以下含义：

uri_path	Web 应用程序的 URI 前缀。
instance	服务器实例的名称。
vs_id	虚拟服务器的 ID。
directory	（可选）从中部署或删除应用程序的目录。如果部署未指定目录，应用程序将部署在文档根目录中。
hard | soft	指定是否删除目录和 server.xml 条目 (hard)，或只删除 server.xml 条目 (soft)。
war_file	WAR 文件名。
verboseLevel	在控制台上显示日志消息的冗余级别。该值的范围为 0 到 4。缺省值为 1。 请注意，在 Sun ONE Web Server 6.1 中，将用 server.xml 中 LOG 元素的 loglevel 属性替代该元素。
-q	（静音）将冗余级别设置为零。这相当于 -V 0 设置。
-n	避免 wdeploy 自动将重新配置命令发送给 Web 服务器。有关详细信息，请参见 “在 wdeploy 命令中使用 -n”。

注意 如果部署 Web 应用程序而未指定 *directory*，该应用程序将部署到文档根目录。如果您接着使用 hard 参数删除该应用程序，文档根目录将被删除。

当您执行 wdeploy deploy 命令时，会出现以下三种情况：

- 具有给定 *uri_path* 和 *directory* 的 Web 应用程序被添加到 server.xml 文件中。
- WAR 文件解压缩到目标 *directory* 中。
- 服务器被动态重新配置以装入新的 Web 应用程序。

例如：

```
wdeploy deploy -u /hello -i server.sun.com -v acme.com
-d /s1ws61/https-server.sun.com/acme.com/web-apps/hello
/s1ws61/plugins/servlets/examples/web-apps/HelloWorld/HelloWorld.war
```

该实用程序将产生以下 server.xml 条目：

```
<VS>
    <WEBAPP uri="/hello"
    dir="/s1ws61/https-server.sun.com/acme.com/webapps/hello"/>
</VS>
```

/s1ws61/https-server.sun.com/acme.com/web-apps/hello 目录具有以下内容：

```
colors
index.jsp
META-INF
WEB-INF/
    web.xml
    /classes/
        HelloWorldServlet.class
        HelloWorldServlet.java
        SnoopServlet.class
        SnoopServlet.java
```

在 *wdeploy* 命令中使用 *-n*

在 Sun ONE Web Server 的 6.1 版中，部署或删除 Web 应用程序之后， wdeploy 将动态重新配置服务器，使服务器可以装入或卸载已部署的或已删除的 Web 应用程序。以前，您必须通过执行以下任一操作，明确地重新配置服务器以使更改生效：

- 使用 reconfig 脚本
- 重新启动服务器
- 在管理用户界面中单击“Apply”链接。

现在，将自动启用一个成功的 wdeploy 命令，以处理新的 Web 应用程序请求，或停止处理已删除 Web 应用程序的请求。

-n 选项可用于避免 wdeploy 自动向 Web 服务器发送重新配置命令。当部署或取消部署多个 Web 应用程序（例如在脚本中），且在部署完最后一个 Web 应用程序后，您希望仅重新配置服务器一次时，请在命令中使用 -n 选项。

访问已部署的 *Web* 应用程序

部署应用程序之后，您可以从浏览器中访问它，如下所示：

`http://`*vs_urlhost*`[:`*vs_port*`]/`*uri_path*`/[`*index_page*`]`

URL 的各部分具有以下含义：

vs_urlhost	用于虚拟服务器的 `urlhosts` 值之一。
vs_port	（可选）仅用于虚拟服务器使用非缺省端口时。
uri_path	用于部署应用程序的同一路径。这也是上下文路径。
index_page	（可选）最终用户首先应访问的应用程序页面。

例如：

```
http://acme.com:80/hello/index.jsp
```

或：

```
http://acme.com/hello/
```

返回值

wdeploy 选项将返回以下退出值：

- `0`。表示已成功执行 `wdeploy` 选项。
- `1`。表示执行 `wdeploy` 选项时，由于无效的命令行变量或无效的配置文件内容而出现错误。
- `2`。表示由于操作系统设置而出现错误。或者是指定的目录不存在，或者是未设置文件权限。

在 Web 应用程序之外部署 Servlet 和 JSP

您可以在 Web 应用程序之外部署 4.*x* Servlet 和 JSP，但仅限于缺省虚拟服务器。有关详细信息，请参见 Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications*。

配置 JVM 设置

您可以在 Server Manager 的 “Java” 选项卡中配置 Java 虚拟机 (JVM) 的属性。

有关这些选项的详细信息，请参见 Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications*。

删除版本文件

使用 Server Manager 的 “Java” 选项卡上的 “Delete Version Files”，您可以删除包含 JavaServer Pages 类缓存和会话数据缓存的版本号的文件。该页面具有以下字段：

清除会话数据

删除 SessionData 目录，如果服务器使用 MMapSessionManager 会话管理器，该目录将存储持久性会话信息。

删除 JSP ClassCache 文件

删除缓存 JavaServer Pages (JSP) 信息的 ClassCache 目录。该目录的缺省位置为：

`server_root/https-server_id/ClassCache/virtual_server_id/webapp_uri/`

当服务器为 JSP 页面提供服务时，它将创建与 JSP 相关联的 .java 文件和 .class 文件，然后将这些文件存储在 ClassCache 目录下的 JSP 类缓存中。

服务器使用以下两个目录来高速缓存 JavaServer Pages (JSP) 和 Servlet 的信息：

- `ClassCache`

  服务器使用以下目录来高速缓存 JavaServer Pages (JSP) 的信息：

  server_root`/https-`*server_id*`/ClassCache/`*virtual_server_id*`/webapp_uri/`

  当服务器提供 JSP 页面时，它将创建与 JSP 相关联的 `.java` 文件和 `.class` 文件，然后将这些文件存储在 `ClassCache` 目录下的 JSP 类缓存中。

- `SessionData`

  如果服务器使用 `MMappedSessionManager` 会话管理器，它会将持久性会话信息存储在 `SessionData` 目录中。

每个缓存均有一个 `version` 文件，其中包含了服务器用来确定缓存中的目录和文件结构的版本号。只要删除该版本文件即可清除缓存。

服务器启动时，如果未找到版本文件，将删除相应缓存的目录结构并重新创建版本文件。服务器下次提供 JSP 页面时，将重新创建 JSP 类缓存。服务器在下次为 JSP 页面或 Servlet 提供服务时使用 MMappedSessionManager 会话管理器的过程中，会重新创建会话数据缓存。

如果未来升级版的服务器使用不同的缓存格式，服务器将检查版本文件中的版本号，并在版本号不正确时清除缓存。

安装 CGI 程序

本节讨论如何安装 CGI 程序。其中包括以下主题：

- CGI 概述
- 指定 CGI 目录
- 将 CGI 指定为文件类型
- 下载可执行文件

此外，以下各节将讨论如何安装 Windows 专用的 CGI 程序：

- 安装 Windows CGI 程序
- 安装 Windows Shell CGI 程序

CGI 概述

通用网关接口 (CGI) 程序可由多种编程语言定义。在 UNIX/Linux 计算机上，您很可能会发现 CGI 程序被编写成 Bourne shell 或 Perl 脚本。

注	UNIX/Linux 具有额外的 `CGIStub` 运行进程，服务器可用来帮助 CGI 执行。只有在首次访问 CGI 期间才创建这些进程。进程数量的变化取决于服务器上的 CGI 负荷。请不要删除这些 CGIStub 进程。服务器停止时，它们将消失。

在 Windows 计算机上，您可能会发现 CGI 程序是用 C++ 或批处理文件编写的。对于 Windows 而言，利用基于 Windows 的编程语言（如 Visual Basic）编写的 CGI 程序将使用不同的机制来操作服务器。这些程序被称为 Windows CGI 程序。有关 Windows CGI 的详细信息，请参见第 351 页上的 “安装 Windows CGI 程序”。

注 要运行命令行实用程序，需要手动设置 Path 变量以包括 *server_root*/bin/https/bin。

不管使用什么编程语言，所有 CGI 程序均以同样的方式接受和返回数据。有关编写 CGI 程序的更多信息，请参见以下信息源：

- Sun ONE Web Server 6.1 *Programmer's Guide*
- **通用网关界面**，可从以下站点访问：

  `http://hoohoo.ncsa.uiuc.edu/cgi/overview.html`
- 联机文档资料中关于 CGI 的文章，可从以下 Web 站点获得：

  `http://docs.sun.com`

在服务器计算机上存储 CGI 程序的方法有两种：

- 指定只包含 CGI 程序的目录。不管文件扩展名为何，所有文件均作为程序运行。
- 指定所有 CGI 程序均属于某一文件类型。也就是说，这些程序全都使用文件扩展名 `.cgi`、`.exe` 或 `.bat`。这些程序可以位于文档根目录中的任何目录中，也可以位于文档根目录下的任何目录中。

如果需要，您可以同时启用两个选项。

两种实现方法各有优点。如果只允许一组特定的用户添加 CGI 程序，请将 CGI 程序保留在指定的目录中并限制对这些目录的访问权限。如果允许任何可以添加 HTML 文件的用户都能添加 CGI 程序，请使用替代文件类型。用户可以将 CGI 文件和 HTML 文件保留在相同的目录中。

如果您选择了目录选项，服务器会将该目录中的所有文件看成 CGI 程序。通过使用相同的标记，如果您选择了文件类型选项，服务器会将具有 `.cgi`、`.exe` 或 `.bat` 文件扩展名的所有文件都当成 CGI 程序来处理。如果某个文件具有这些扩展名中的一个但不是 CGI 程序，用户试图访问时就会出现错误。

注 缺省情况下，CGI 程序的文件扩展名为 `.cgi`、`.exe` 和 `.bat`。但是，您可以通过修改 MIME 类型文件来更改哪些扩展名表示 CGI 程序。要执行此操作，请选择 “Server Preferences”选项卡并单击 “MIME Types”链接。

指定 CGI 目录

要为一组虚拟服务器指定 CGI 专用目录，请执行以下步骤：

1. 从 Class Manager 中选择 “Programs”选项卡。

   将显示 “CGI Directory”窗口。

2. 在 “URL Prefix”字段中，键入要用于该目录的 URL 前缀。也就是说，您键入的文本将在 URL 中作为 CGI 程序的目录显示出来。

   例如，如果您键入 `cgi-bin` 作为 URL 前缀，那么这些 CGI 程序的所有 URL 将具有以下结构：

   `http://`*`yourserver.domain.com`*`/cgi-bin/`*`program-name`*

注 您指定的 URL 前缀可能与在前一步骤中指定的真实 CGI 目录有差异。

3. 在 “CGI Directory”文本字段中，键入目录的位置作为绝对路径。请注意，该目录不必位于文档根目录下。因此，您需要在下一步骤中指定一个 URL 前缀。
4. 单击 “OK”。
5. 保存并应用所做的更改。

要删除现有的 CGI 目录，请在 “CGI Directory”表单中单击该目录的 “Remove”按钮。要更改现有目录的 URL 前缀或 CGI 目录，请单击该目录的 “Edit”按钮。

将 CGI 程序复制到指定的目录中。请记住，这些目录中的所有文件将被作为 CGI 文件处理，所以不要将 HTML 文件放入 CGI 目录中。

为每个软件虚拟服务器配置唯一的 CGI 属性

要为单个虚拟服务器指定 CGI 属性，请执行以下步骤：

1. 从 Class Manager 中选择 “Manager Virtual Servers”按钮。
2. 从 Virtual Server Manager 中选择 “Settings”链接。
3. 在 “CGI User”文本字段中，键入执行 CGI 程序的用户的名称。
4. 在 “CGI Group”文本字段中，键入执行 CGI 程序的组的名称。
5. 在 “CGI Directory”文本字段中，将 `chdir` 的目录键入到 `chroot` 之后，但在执行开始之前。

6. （仅限 UNIX）在 “CGI Nice” 文本字段中，键入用于确定 CGI 程序相对于服务器优先级的增量。通常，服务器在精度值为 0 的情况下运行，精度增量在 0（CGI 程序与服务器在同一优先级下运行）到 19 （CGI 程序的运行优先级远远低于服务器）之间。指定精度增量为 -1，就有可能增加 CGI 程序的优先级使其高于服务器，但不建议这样做。
7. 在 “Chroot Directory” 文本字段中，将 chroot 的目录键入到执行开始之前。
8. 单击 “OK”。
9. 保存并应用所做的更改。

将 CGI 指定为文件类型

要将 CGI 程序指定为文件类型，请执行以下步骤：

1. 从 Class Manager 中选择 “Programs” 选项卡。
2. 单击 “CGI File Type”。

   将显示 “CGI as a File Type” 窗口。
3. 从 Editing Picker 中选择您要应用该更改的资源。
4. 在 “Activate CGI as a File Type” 下，单击 “Yes” 单选按钮。
5. 单击 “OK”。
6. 保存并应用所做的更改。

CGI 文件必须具有文件扩展名 `.bat`、`.exe` 或 `.cgi`。如果具有这些扩展名的非 CGI 文件均被服务器作为 CGI 文件处理可能会导致错误。

下载可执行文件

如果使用 `.exe` 作为 CGI 文件类型，则不能将 `.exe` 文件作为可执行文件下载。

解决此问题的方法之一是压缩想让用户下载的可执行文件，这样扩展名就不是 `.exe` 了。该解决方法还有缩短下载时间的附加优点。

另一个可能的解决方法是从 `magnus-internal/cgi` 类型中删除作为文件扩展名的 `.exe`，而将其添加到 `application/octet-stream` 类型 （用于标准可下载文件的 MIME 类型）中。您可以通过 Server Manager 执行此操作，方法是选择 “Server Preferences” 选项卡并单击 “MIME Types” 链接。但是，该方法的缺点是进行该更改后无法将 `.exe` 文件用作 CGI 程序。

另一个解决方法是编辑服务器的 obj.conf 文件，设置一个下载目录，该目录中的文件将被自动下载。服务器的其他部分不会受到影响。有关详细信息，请参见：

http://developer.netscape.com/docs/manuals/enterprise/admnunix/programs.htm

安装 Windows CGI 程序

本节讨论如何安装 Windows CGI 程序。本节包括以下内容：

Windows CGI 程序概述

Windows CGI 程序的处理方法与其他 CGI 程序很相似。您可以指定一个只包含 Windows CGI 程序的目录，也可以指定所有 Windows CGI 程序具有相同的文件扩展名。请注意，像其他 CGI 程序一样，如果需要，您可以同时使用这两种方法。例如，您可以为所有 Windows CGI 程序创建一个目录，并指定一个 Windows CGI 文件扩展名。

尽管 Windows CGI 程序像常规的 CGI 程序一样操作，但服务器处理实际程序时有些不一样。因此，您需要为 Windows CGI 程序指定不同的目录。如果启用 Windows CGI 文件类型，则文件扩展名为 .wcg。

Sun ONE Web Server 支持 Windows CGI 1.3a 非正式规范，且具有以下差异：

- 以下关键字已添加到 [CGI] 部分以支持安全方法：
  - HTTPS：其值为 On 或 Off，这取决于是否通过 SSL 执行事务。
  - HTTPS Keysize：当 HTTPS 为 On 时，该值报告用于加密的会话密钥中的位数。
  - HTTPS Secret Keysize：当 HTTPS 为 On 时，该值将报告用于生成服务器专用密钥的位数。
- [CGI] 部分的关键字 Document Root 不一定是指所期望的文档根目录，因为服务器并不具有单一的文档根目录。此变量中返回的目录是 Windows CGI 程序的根目录。

- 不支持 [CGI] 部分中的关键字 Server Admin。
- 不支持 [CGI] 部分中的关键字 Authentication Realm。
- 不支持以多部分 / 表单数据编码发送的表单。

指定 Windows CGI 目录

要指定 Windows CGI 专用目录，请执行以下操作：

1. 从 Class Manager 中选择 “Programs”选项卡。
2. 单击 “WinCGI Directory”链接。

   将显示 “WinCGI Directory”窗口。
3. 在 “URL Prefix”文本字段中，输入要用于该目录的 URL 前缀。

   也就是说，您键入的文本将在 URL 中作为 Windows CGI 程序的目录显示出来。例如，如果键入 `wcgi-programs` 作为 URL 的前缀，这些 Windows CGI 程序的所有 URL 将具有以下结构：

   http://*yourserver*.domain.com/wcgi-programs/program-name

注 您指定的 URL 前缀可能与在第 5 步 中指定的真实 Windows CGI 目录有差异。

4. 选择是否要启用脚本跟踪。

   在 “Enable Script Tracing?”下，单击 “Yes”或 “No”单选按钮。

   CGI 参数通过文件从服务器传递到 Windows CGI 程序，通常服务器在 Windows CGI 程序执行完毕后将删除这些文件。如果启用了脚本跟踪，这些文件将保留在 `/temp` 目录中或环境变量 TMP 和 TEMP 所指向的位置中。同样，启用脚本跟踪时，将显示 Windows CGI 程序所产生的任何窗口。
5. 在 “WinCGI Directory”字段中，输入目录的位置作为绝对路径。

   请注意，该目录不必位于文档根目录下。因此，您需要在第 3 步 中指定一个 URL 前缀。
6. 单击 “OK”。
7. 保存并应用所做的更改。

要删除现有的 Windows CGI 目录，请在 “Windows CGI Directory”表单中单击该目录的 “Remove”按钮。要更改现有目录的 URL 前缀或 Windows CGI 目录，请单击该目录的 “Edit”按钮。

将 Windows CGI 程序复制到指定的目录中。请记住，这些目录中的所有文件都被作为 Windows CGI 文件处理。

将 Windows CGI 指定为文件类型

要为 Windows CGI 文件指定文件扩展名，请执行以下步骤：

1. 从 Server Manager 中选择 “Server Preferences”选项卡。
2. 单击 “MIME Types”链接。

   将显示 “Global MIME Types”窗口。有关全局 MIME 类型的详细信息，请参见第 214 页上的 “选择 MIME 类型”。
3. 请按以下设置添加新的 MIME 类型：
   - 类型：`type`
   - 内容类型：`magnus-internal/wincgi`。
   - 文件后缀：输入您希望服务器将其与 Windows CGI 相关联的文件的后缀。如果已激活 CGI、 WinCGI 和 Shell CGI 文件类型，您必须为每个类型的 CGI 指定不同的后缀。例如， CGI 程序和 shell CGI 程序不能同时使用后缀 `.exe`。如果需要，可以在页面上编辑其他 MIME 类型字段，以便后缀是唯一的。
4. 单击 “New Type”按钮。
5. 保存并应用所做的更改。

安装 Windows Shell CGI 程序

本节讨论如何安装 Windows Shell CGI 程序。本节包括以下内容：

Windows Shell CGI 程序概述

Shell CGI 是一种服务器配置，您可以使用在 Windows 中设置的文件关联来运行 CGI 应用程序。

例如，如果服务器接到一个请求需要一个名为 `hello.pl` 的 Shell CGI 文件，服务器将利用与 `.pl` 扩展名相关联的程序，使用 Windows 文件关联来运行该文件。如果 `.pl` 扩展名与程序 `C:\bin\perl.exe` 相关联，服务器将尝试执行 `hello.pl` 文件，如下所示：

```
c:\bin\perl.exe hello.pl
```

配置 shell CGI 的最简便方式是在只包含 shell CGI 文件的服务器文档根目录中创建一个目录。但是，您也可以通过从 Sun ONE Web Server 编辑 MIME 类型，配置服务器以使特定的文件扩展名与 Shell CGI 相关联。

注	有关设置 Windows 文件扩展名的信息，请参见相关的 Windows 文档。

指定 Shell CGI 目录 (Windows)

要创建 shell CGI 文件的目录，请执行以下步骤：

1. 在计算机上创建 Shell 目录。该目录不必是文档根目录的子目录。
2. 从 Server Manager 中选择 “Class Manager”链接。
3. 然后选择 “Class Manager”。

   将突出显示 “Shell CGI Directory”链接并显示 CGI 窗口。

4. 在 “URL Prefix”字段中，输入要与 Shell CGI 目录相关联的 URL 前缀。

   例如，假设您将所有 Shell CGI 文件存储在名为 `C:\docs\programs\cgi\shell-cgi` 的目录中，但是您希望用户看到的是 `http://www.`*yourserver*`.com/shell/` 目录。在这种情况下，应键入 `shell` 作为 URL 前缀。

5. 在 “Shell CGI Directory”字段中，输入已创建目录的绝对路径。

注意 服务器必须具有读取和执行该目录的权限。对于 Windows，运行服务器所用的用户帐户（例如，`LocalSystem`）必须具有读取和执行 Shell CGI 目录中的程序的权限。

6. 请确保 Shell CGI 目录中的所有文件也具有在 Windows 中设置的文件关联。如果服务器试图运行没有文件扩展名关联的文件，将返回错误。

将 Shell CGI 指定为文件类型 (Windows)

您可以使用 Sun ONE Web Server 的 “MIME Types”窗口，将文件扩展名与 shell CGI 特性相关联。这不同于在 Windows 中创建关联。

要在服务器中将文件扩展名与 Shell CGI 特性相关联，例如，您可以为具有 `.pl` 扩展名的文件创建关联。当服务器接到请求需要具有该扩展名的文件时，通过调用 Windows 中与该文件扩展名关联的可执行文件，服务器会将该文件当作 Shell CGI 文件处理。

要将文件扩展名与 Shell CGI 文件相关联，请执行以下步骤：

1. 在计算机上创建 Shell 目录。该目录不必是文档根目录的子目录。
2. 从 Server Manager 中选择 “Server Preferences”。
3. 单击 “MIME Types”链接。

   将显示 “Global MIME Types”窗口。有关全局 MIME 类型的更多信息，请参见第 214 页上的 “选择 MIME 类型”。

4. 请按以下设置添加新的 MIME 类型：
   - 类型：`type`
   - 内容类型：`magnus-internal/shellcgi`。

- 文件后缀：输入您希望服务器将其与 Shell CGI 相关联的文件的后缀。如果已激活 CGI、WinCGI 和 Shell CGI 文件类型，您必须为每个类型的 CGI 指定不同的后缀。例如， CGI 程序和 shell CGI 程序不能同时使用后缀 `.exe`。如果需要，您可以在页面上编辑其他 MIME 类型字段，以便后缀是唯一的。

5. 单击 “New Type” 按钮。
6. 保存并应用所做的更改。

使用查询处理程序

注 使用查询处理程序已经过时了。尽管 Sun ONE Web Server 和 Netscape Navigator 客户机仍支持该处理程序，但它已很少使用。用户更多地使用 HTML 页面中的表单来提交查询。

您可以指定一个缺省查询处理程序 CGI 程序。查询处理程序通过 HTML 文件中的 ISINDEX 标记处理发送给它的文本。

ISINDEX 类似于一个表单文本字段，即在可以接受输入内容的 HTML 页面中创建文本字段。但不同于表单文本字段信息的是，当用户按回车键时， ISINDEX 框中的信息将被立刻提交。当指定缺省查询处理程序时，您就告诉了服务器将输入定向到哪个程序。有关 ISINDEX 标记深层次的讨论，请参见 HTML 参考手册。

要设置查询处理程序，请执行以下步骤：

1. 从 Class Manager 中选择 “Programs” 选项卡。
2. 单击 “Query Handler” 链接。

   将显示 “Query Handler” 窗口。
3. 使用 “Editing Picker” 选择要和缺省查询处理程序一起设置的资源。

   如果选择了一个目录，指定的查询处理程序只在服务器接收到该目录的 URL 或该目录中任一文件时运行。
4. 在 “Default Query Handler” 字段中，输入要用作选定资源的缺省设置的 CGI 程序的完整路径。
5. 单击 “OK”。
6. 保存并应用所做的更改。

第 17 章

应用配置式样

使用配置式样可以很容易地将一组选项应用到多个虚拟服务器所维护的特定文件或目录中。例如，可以创建一个设置访问日志的配置式样。当您将该配置式样应用到要记录的文件和目录时，您不必为虚拟服务器中的每个文件和目录单独配置访问日志。

本章包括以下部分：

创建配置式样

要创建配置式样，请执行以下步骤：

1. 访问 Class Manager。
2. 选择 “Styles” 选项卡。
3. 单击 “New Style” 链接。
4. 键入配置式样的名称。单击 “OK”。

   Sun ONE Web Server 将显示 “Edit a Style”。
5. 从下拉列表中选择要编辑的配置式样，然后单击 “Edit this Style”。

6. 从可用链接列表中单击要配置式样的种类。

   您可以配置表 17-1 中列出的信息。

7. 填写显示的表单并单击 “OK”。

8. 重复步骤 4 和步骤 5，对配置式样进行其他更改。单击 “OK”。

选择要编辑的式样时， Resource Picker 将列出配置式样，而不是其他资源。编辑完式样后，单击 “OK”和 “Save and Apply”。 Resource Picker 将退出式样模式。您也可以通过从 Resource Picker 中选择 “Exit styles mode”退出式样模式。有关 Resource Picker 的详细信息，请参见第 1 章 “Sun ONE Web Server 简介”的第 40 页上的 “使用 Resource Picker”。

表 17-1 配置式样种类

种类	说明
CGI 文件类型	使您可以激活 CGI 作为文件类型。有关 CGI 的详细信息，请参见第 16 章 “使用程序扩展服务器”中第 347 页上的 “安装 CGI 程序 ,”。
字符集	使您可以更改资源的字符集。有关字符集的详细信息，请参见第 15 章 “内容管理”中第 328 页上的 “更改字符集 ,”。
缺省查询处理程序	使您可以设置服务器资源的缺省查询处理程序。有关查询处理的详细信息，请参见第 16 章 “使用程序扩展服务器”中第 356 页上的 “使用查询处理程序 ,”。
文档页脚	使您可以为服务器资源添加文档页脚。有关详细信息，请参见第 15 章 “内容管理”中的第 329 页上的 “设置文档页脚”。
`.htaccess` 配置	使您可以为用户提供配置选项的子集而不必授予用户访问 Server Manager 的权限。有关访问控制的详细信息，请参见第 8 章 “控制对服务器的访问”。
要求更强大的安全性	使您可以指定密钥大小限制，或使用特定文件拒绝访问。
错误响应	使您可以自定义客户遇到服务器错误时所看到的错误响应。
日志首选项	使您可以设置访问日志的首选项。有关日志首选项的详细信息，请参见第 10 章 “使用日志文件”中第 225 页上的 “设置访问日志首选项 ,”。
远程文件操作	使您可以激活文件操作命令，使远程浏览器可以更改您服务器的文档。有关详细信息，请参见。第 15 章 “内容管理”中的第 324 页上的 “启用远程文件操作”。
服务器分析的 HTML	使您可以指定将文件发送到客户机之前服务器是否分析这些文件。有关详细信息，请参见 Sun ONE Web Server 6.1 *Programmer's Guide*。

表 17-1 配置式样种类 （接上页）

种类	说明
提供预压缩内容	使您可以指定服务器是否发送文件的预压缩版本。有关详细信息，请参见第 15 章 “内容管理”中的第 333 页上的 “配置服务器以提供预压缩的内容”。
根据需要压缩内容	使您可以指定将内容发送到客户机之前服务器是否动态地压缩内容。有关详细信息，请参见第 15 章 “内容管理”中的第 334 页上的 “将服务器配置为根据需要压缩内容”。
符号链接 (UNIX/Linux)	使您可以限制服务器中文件系统链接的使用。有关详细信息，请参见第 15 章 “内容管理”中的第 330 页上的 “限制符号链接 (UNIX/Linux)”。

有关详细信息，请参见联机帮助中的 “New Style”页面。

指定配置式样

创建配置式样后，可以将其指定给虚拟服务器中的文件或目录。您可以指定单个文件和目录，也可以指定通配符模式 （例如 `*.gif`）。

要指定配置式样，请执行以下步骤：

1. 访问 Class Manager。
2. 选择 “Styles”选项卡。
3. 单击 “Assign Style”链接。
4. 输入要应用此配置式样的 URL 的前缀。

   如果选择了文档根目录内的目录，只需在文档根目录后输入该路径。如果在目录后输入了 `/*`，则配置式样将应用到目录的所有内容。
5. 选择要应用的配置式样。

   要删除先前应用于资源的所有配置式样，请应用 “None”配置式样。单击 “OK”。

有关详细信息，请参见联机帮助中的 “Assign a Style”页面。

列出配置式样指定

创建配置式样并将其应用于文件或目录后，您可以得到配置式样及配置式样应用于何处的列表。

要列出配置式样指定，请执行以下步骤：

1. 访问 Class Manager。
2. 选择 “Styles”选项卡。
3. 单击 “List Assignments”链接。

   Sun ONE Web Server 将显示 “List Assignments”，其中显示了应用于服务器资源的配置式样。
4. 要编辑配置式样指定，请单击配置式样名称旁的 “Edit”链接。

有关详细信息，请参见联机帮助中的 “List Assignments”页面。

编辑配置式样

要编辑配置式样，请执行以下步骤：

1. 访问 Class Manager。
2. 选择 “Styles”选项卡。
3. 单击 “Edit Style”链接。
4. 选择要编辑的配置式样，并单击 “Edit this style”按钮。
5. 从可用链接列表中单击要配置式样的种类。

   有关这些种类的详细信息，请参见第 357 页上的 “创建配置式样”一节。
6. 填写显示的表单并单击 “OK”。
7. 重复步骤 4 和步骤 5，对配置式样进行其他更改。单击 “OK”。

在选择要编辑的式样时， Resource Picker 将列出配置式样，而不是其他资源。编辑完式样后，单击 “OK”和 “Save and Apply”。 Resource Picker 将退出式样模式。您也可以通过从 Resource Picker 中选择 “Exit styles mode”退出式样模式。有关 Resource Picker 的详细信息，请参见第 1 章 “Sun ONE Web Server 简介”的第 40 页上的 “使用 Resource Picker”。

有关详细信息，请参见联机帮助中的 “Edit Style”页面。

删除配置式样

删除配置式样之前，请先删除已应用了配置式样的指定。如果删除配置式样之前未执行此操作，您必须手动编辑虚拟服务器类的 `obj.conf` 文件，搜索文件中的配置式样，然后将其替换为 “`None`”。如果您未执行此搜索和替换操作，访问应用了已删除配置式样的文件或目录的用户将收到服务器配置错误的错误消息。

要删除配置式样，请执行以下步骤：

1. 访问 Class Manager。
2. 选择 “Styles” 选项卡。
3. 单击 “List Assignments” 链接。
4. 选择要删除的 “Edit Style Assignment”。
5. 单击 “Remove this Assignment”。

有关详细信息，请参见联机帮助中的 “Remove Style” 页面。

第 18 章

使用搜索

Sun ONE Web Server 6.1 包含搜索功能，该功能使用户可以在服务器上搜索文档并将搜索结果显示在 Web 页上。服务器管理员可以根据用户要搜索的文档（称为集合）来创建文档索引，也可以自定义搜索界面以满足用户的需求。

本章包括以下部分：

关于搜索

在安装 Sun ONE Web Server 的过程中，搜索功能已与其他 Web 组件一起安装。与在 Sun ONE Web Server 6.0 中一样，搜索是在虚拟服务器级别而不是服务器实例级别上进行配置和管理的。

虚拟服务器管理器中的 “搜索”选项卡用于为各个虚拟服务器配置搜索功能。通过此选项卡，您可以执行以下操作：

- 启用和禁用搜索功能
- 创建、修改、删除搜索集合以及为搜索集合重新编制索引
- 为搜索集合创建、修改和删除已安排的维护任务

从管理界面获取的信息存储在 `<`*server-root*`>/config/server.xml` 文件中，并在该文件的 VS 元素内被映射。

服务器管理员可以自定义搜索查询和搜索结果页面。这可能包括使用公司徽标重新设置页面，或者更改搜索结果的显示方式。在早期的版本中，这些操作是通过使用模式文件来实现的。 Sun ONE Web Server 6.1 不支持模式文件。现在使用产品附带的一组 JSP 标记库来执行自定义操作。这些库所提供的功能与模式文件所提供的功能类似。有关自定义搜索界面的更多信息，请参见 “自定义搜索页面”。

本版本不具备早期版本中搜索的全局 “开”或 “关”功能，而是提供了一个缺省搜索 Web 应用程序，然后在特定虚拟服务器上启用或禁用该应用程序。此搜索应用程序提供了用于查询集合和查看结果的基本 Web 页面。此搜索应用程序包含样例 JSP，这些样例 JSP 说明了如何使用搜索标记库来建立自定义的搜索界面。

注意 与 Sun ONE Web Server 6.0 不同，6.1 版未提供检查搜索结果的功能。由于潜在的安全模式和安全区域的数量很多，因此无法通过搜索应用程序执行安全检查及过滤结果。服务器管理员负责确保使用相应的安全机制来保护内容。

Sun ONE Web Server 6.1 支持多文档搜索。可以为具有不同格式的文档 （例如 HTML、 ASCII 和 PDF）编制索引，并根据该索引进行搜索。

注 Sun ONE Web Server 6.1 不支持在 Linux 平台上进行多文档格式搜索。

Sun ONE Web Server 6.1 已使用新的搜索引擎来代替早期版本中使用的搜索引擎。因此，从 Web 服务器的早期版本迁移到 Sun ONE Web Server 6.1 时，不会迁移现有的搜索集合和索引。

启用虚拟服务器的搜索应用程序

通过启用 Sun ONE Web Server 附带的搜索应用程序，可以启用虚拟服务器的搜索功能，可以通过管理界面启用该功能。

注 要启用搜索功能，必须启用 Java Web 容器。

确保已为包含要配置的虚拟服务器的虚拟服务器类启用 Java 后，请执行以下步骤来启用搜索功能：

1. 选择要启用其搜索功能的虚拟服务器，然后单击 “管理”按钮。
2. 选择 “搜索”选项卡，然后单击 “搜索配置”链接。
3. 输入以下信息：
   - **最大命中次数**。指定搜索查询中检索到的最大结果数目。
   - **URI**。如果要使用自定义搜索应用程序，请输入 URI ；如果要使用缺省搜索应用程序，则无需在此指定值。
   - **路径**。如果要使用自定义搜索应用程序，请输入路径；如果要使用缺省搜索应用程序，则无需在此指定值。
   - **启用**。选中此选项以启用缺省搜索应用程序。
4. 单击 “确定”。

禁用虚拟服务器的搜索应用程序

通过禁用 Sun ONE Web Server 附带的搜索应用程序，可以禁用虚拟服务器的搜索功能，可以通过管理界面禁用该功能。

要禁用虚拟服务器的搜索功能，请执行以下步骤：

1. 选择要禁用其搜索功能的虚拟服务器，然后单击 “管理”按钮。
2. 选择 “搜索”选项卡，然后单击 “搜索配置”链接。
3. 取消选中 “启用”复选框。
4. 单击 “确定”。

关于搜索集合

搜索要求具备一个可搜索数据的数据库，用户将根据这些数据进行搜索。服务器管理员创建此数据库（称为集合），该数据库为有关服务器上文档的信息编制索引并存储这些信息。服务器管理员为全部或部分服务器文档创建索引后，就可以使用诸如标题、创建日期和作者等信息进行搜索。

请注意有关集合的以下信息：

- 集合特定于被管理的虚拟服务器
- 只有在虚拟服务器中可视的文档才显示在管理界面中，并可为其编制索引
- 服务器上可存在任意数量的集合
- 单个搜索集合只能包含位于文件系统中一个父目录下的文件
- 可以为具有不同格式的文档（例如 HTML、 ASCII 和 PDF）编制索引，并根据该索引进行搜索
- 搜索集合中的文档不是特定于某种字符编码，这意味着搜索集合可以与多种编码相关联
- 有关集合的信息存储在 `server.xml` 的 VS 元素中

本部分包括以下主题：

创建集合

集合是通过管理界面进行创建和管理的。可以通过指定要为其编制索引的文档来创建新的集合。

要创建新的集合，请执行以下步骤：

1. 选择要在其中创建集合的虚拟服务器，然后单击 “管理”按钮。
2. 选择 “搜索”选项卡，然后单击 “创建集合”链接。
3. 输入以下信息：
   - **要为其编制索引的目录**。从下拉列表中，选择将要在集合中为其中的文档建立索引的目录。只有在虚拟服务器中可视的目录才会列出。

     要查看目录的内容，请单击 “查看”。如果选定的目录具有子目录，这些子目录将列在 “查看 *directory_name*”页面上。要选择要为其编制索引的目录，请单击 “索引”。要查看目录，请在文件夹上单击。

     要将目录添加到可编制索引的目录列表中，必须先另外创建一个文档目录。有关更多信息，请参见 “设置其他文档目录”。
   - **集合名称**。输入集合的名称。
   - **显示名称**。（可选）在搜索查询页面中将显示为集合的名称。如果未指定显示名称，集合名称将充当显示名称。
   - **说明**。（可选）输入说明新集合的文本。
   - **是否包含子目录**？如果选择 “否”，将不为选定目录的子目录中的文档编制索引。缺省选项为 “是”。
   - **模式**。指定通配符以选择要为其编制索引的文件。有关通配符的更多信息，请参见 “Resource Picker 中使用的通配符”。

注意 请慎重使用通配符模式，以确保只为特定文件编制索引。例如，指定 *.* 可能导致也为可执行文件和 Perl 脚本文件编制索引。

   - **缺省编码**。指定要为其编制索引的文档的字符编码。缺省为 “ISO-8859-1”。索引编制引擎将尝试通过嵌入的元标记来确定 HTML 文档的编码。如果未指定，将使用缺省编码。

     集合中的文档不限于单一语言 / 编码。每次添加文档时，只能指定一种编码；但是，下一次将文档添加到集合中时，可以选择不同的缺省编码。
4. 单击 “确定”。

将在以下位置创建具有指定名称的新集合：

<*instance-root*>/collections/<*vs-id*>/<*collection-name*>

同时也将在 server.xml 文件中创建相应的 SEARCHCOLLECTION 项。

配置集合

创建集合后，您可以修改它的某些设置。这些设置存储在 server.xml 文件中。重新配置集合时，将更新 server.xml 文件以反映您所做的更改。

您应当避免对集合设置进行不必要的更改。

要重新配置现有集合，请执行以下步骤：

1. 选择包含要配置的集合的虚拟服务器，然后单击 “管理”按钮。
2. 选择 “搜索”选项卡，然后单击 “配置集合”链接。
3. 从 “集合”下拉列表中选择要配置的集合，然后单击 “转至”。
4. 您可以编辑选定集合的以下信息：
   - **显示名称**。（可选）在搜索查询页面中将显示为新集合的名称。
   - **说明**。（可选）编辑集合的文本说明。
   - **文档 URI**。为搜索集合的文档根目录编辑 URI。

注 请不要更改文档 URI，除非已从 “Additional Document Directories”更改了文档根目录的 URI 映射。有关详细信息，请参见 “设置其他文档目录”。

   - **启用**。选择 “是”以启用。如果选择 “否”，搜索查询页面上将不显示集合。
5. 单击 “确定”。

这将重新配置集合并修改 server.xml 文件中相应的 SEARCHCOLLECTION 项。

更新集合

创建集合后，您可以添加或删除文件。只能添加集合创建期间指定的目录下的文档。如果要删除文档，只能从集合中删除文件的项及其元数据。实际上并未从文件系统中删除文件。

要更新集合，请执行以下步骤：

1. 选择包含要更新的集合的虚拟服务器，然后单击 “管理” 按钮。
2. 选择 “搜索” 选项卡，然后单击 “更新集合” 链接。
3. 从 “集合” 下拉列表中选择要更新的集合。
4. Docs
5. 您可以更新选定集合的以下信息：
   - **是否包含子目录**？如果选择 “否”，将不会为选定目录的子目录中的文档编制索引。缺省选项为 “是”。

注 “**是否包含子目录**？” 只与添加文档有关。

   - **模式**。指定通配符，以选择要为其编制索引的文件或从集合中删除的文件。有关通配符的详细信息，请参见 Resource Picker 中使用的通配符。

注意 添加文档时，请慎重使用通配符模式，以确保只为特定文件编制索引。例如，指定 *.* 可能导致也为可执行文件和 Perl 脚本文件编制索引。

   - **缺省编码**。指定要为其编制索引的文档的字符编码。缺省为 “ISO-8859-1”。索引引擎将尝试从嵌入式元标记来确定 HTML 文档的编码。如果未指定，将使用缺省编码。

     集合中的文档不限于单一语言 / 编码。每次添加文档时，只能指定一种编码；但是，下一次将文档添加到集合中时，可以选择不同的缺省编码。
6. 单击 “添加文档” 以将文档添加到索引，或单击 “删除文档” 以删除相应的索引条目。

注 只能添加创建集合时指定的目录中的文档。

删除集合

您可以删除已创建的集合。集合被删除后，将不再显示在搜索查询页面上，并且所有与该集合相关联的配置和索引文件也将被删除。构成集合的实际文档并未从文件系统中删除，只是删除了它们在集合中的索引条目。

要删除集合，请执行以下步骤：

1. 选择包含要删除的集合的虚拟服务器，然后单击 “管理”按钮。
2. 选择 “搜索”选项卡，然后单击 “维护集合”链接。
3. 从 “集合”下拉列表中，选择要删除的集合。
4. 单击 “删除集合”按钮。

注 删除集合后，也将删除该集合中已安排的维护。有关已安排维护的详细信息，请参见 “添加已安排的集合维护”。

注 请不要使用本地文件管理器来删除集合，因为这样将不能更新相应的配置文件。

维护集合

您可能希望定期维护您的集合。除非您经常为集合编制索引并经常更新集合，否则没有必要定期维护集合。您可以执行以下操作：

- 为集合重新编制索引
- 更新集合

为集合重新创建索引

您可以为已创建的集合重新编制索引。如果在创建集合后修改了任何文档，将为集合重新编制索引。为集合重新编制索引不会将任何新内容添加到集合中，只是更新集合的现有内容。如果文档的现有索引项不再存在于服务器文件系统中，这些项将被删除。

要为集合重新编制索引，请执行以下步骤：

1. 选择包含要为其重新编制索引的集合的虚拟服务器，然后单击 “管理”按钮。
2. 选择 “搜索”选项卡，然后单击 “维护集合”链接。
3. 从 “集合”下拉列表中选择要为其重新编制索引的集合。
4. 单击 “重新编制索引”按钮。

添加已安排的集合维护

您可以安排定期在集合上执行维护任务。可以安排的任务是重新编制索引和更新。可以使用管理界面为特定集合安排任务。您可以指定以下内容：

- 要执行的任务 （重新编制索引或更新）
- 执行任务的时间
- 在一星期中的哪一天执行任务

要添加集合的定期维护，请执行以下步骤：

1. 选择要为其安排维护的集合并单击 “添加已安排的维护”链接。
2. 输入以下信息：
   - **任务**。选择要自动执行的任务。选项包括 “重新编制索引”和 “更新”。

     如果选择 “更新”，必须输入以下信息：

     - **是否将子目录编入索引**？如果选择 “否”，将不把选定目录的子目录中的文档编入索引。缺省选项为 “是”。
   - **模式**。指定通配符以选择要为其编制索引的文件。有关通配符的详细信息，请参见 Resource Picker 中使用的通配符。

注意 请慎重使用通配符模式，以确保只为特定文件编制索引。例如，指定 *.* 可能导致也为可执行文件和 Perl 脚本文件编制索引。

   - **缺省编码**。指定要为其编制索引的文档的字符编码。缺省为 “ISO-8859-1”。索引引擎将尝试从嵌入式元标记来确定 HTML 文档的编码。如果未指定，将使用缺省编码。

     集合中的文档不限于单一语言 / 编码。每次添加文档时，只能指定一种编码；但是，下一次将文档添加到集合中时，可以选择不同的缺省编码。

- **安排的时间**。（必需）以 HH:MM 格式指定要运行已安排维护的时间。例如，您可能希望在一天的结束时运行已安排的维护，因为那时集合中的文档可能已经修改。
- **安排位于一星期中的哪一（几）天**。（必需）选中一个或多个复选框，以指定在一星期中的哪一（几）天运行已安排的维护。

3. 单击“确定”。

注 UNIX/Linux 用户在添加完已安排的维护后必须重新启动守护程序控制进程，以使所做的更改生效。

编辑已安排的集合维护

如果您的要求发生变化，可以更改为集合安排的维护的特性。例如，您可能决定在您的站点最有可能进行更新的时候重新安排维护。

要更改为集合安排的维护，请执行以下步骤：

1. 从“集合”下拉列表中选择要为其重新安排维护的集合。
2. 选择要重新配置的任务，然后输入必要的信息。有关详细信息，请参见联机帮助中的“Edit Scheduled Collection”。
3. 单击“确定”。

注 删除集合后，也将删除该集合中已安排的维护。

注 UNIX/Linux 用户在重新配置已安排的维护后必须重新启动守护程序控制进程，以使所做的更改生效。

删除已安排的集合维护

如果不再需要，您可以取消为集合安排的维护。

要取消已安排的维护，请执行以下步骤：

1. 从“集合”下拉列表中选择要为其删除维护的集合。
2. 选择要删除其已安排的维护的任务：“重新索引”或“更新”。如果任务已安排，将显示更多信息。

3. 对于 “更新”任务，请选中要删除的任务旁边的 “删除”复选框。
4. 单击 “确定”。

注 UNIX/Linux 用户在删除已安排的维护后必须重新启动守护程序控制进程，以使所做的更改生效。

执行搜索

用户主要关心在搜索集合中查询数据，然后获得作为查询结果的文档列表。与 Sun ONE Web Server 一起安装的搜索 Web 应用程序提供了缺省搜索查询和搜索结果页面。可以直接使用这些页面，或使用一组 JSP 标记对这些页面进行自定义（如 “自定义搜索页面”中所述）。

用户可以根据服务器管理员创建的集合进行搜索。用户可以执行以下操作：

- 输入一组关键字和可选的查询运算符进行搜索
- 仅搜索在虚拟服务器中可视的集合
- 根据单个集合进行搜索，或根据在虚拟服务器中可视的一组集合进行搜索

服务器管理员必须为用户提供访问虚拟服务器搜索查询页面所需的 URL。

注意 与 Sun ONE Web Server 6.0 不同，6.1 版未提供检查搜索结果的功能。由于潜在的安全模式和安全区域的数量很多，因此无法通过搜索应用程序执行安全检查及过滤结果。服务器管理员负责确保使用相应的安全机制来保护内容。

“搜索”页面

最终用户可用于访问搜索功能的缺省 URL 为：

`http://<server-instance>:port number/search`

示例：

```
http://plaza:8080/search
```

最终用户调用此 URL 时，将启动 “搜索”（一个 Java Web 应用程序）。

注 关于执行基本搜索和高级搜索的更多详细说明（包括关于关键字和可选的查询运算符的信息），请参见搜索引擎提供的联机帮助。要获得这些信息，请单击“搜索”上的帮助链接。

下图显示了缺省“搜索”界面：

缺省 Sun ONE Web Server “搜索”

如“自定义搜索页面”中所述，您可以使用一组 JSP 标记来自定义此页面。

进行查询

搜索查询页面用于根据集合进行搜索。用户输入一组关键字和可选的查询运算符，结果将显示在其浏览器中的 Web 页面上。结果页面包含指向服务器上符合搜索条件的文档的链接。

注	如 “自定义搜索页面”中所述，服务器管理员可以自定义此搜索查询页面。

要进行查询，请执行以下步骤：

1. 通过在浏览器的地址栏中按以下格式输入搜索 Web 应用程序的 URL 来访问该程序：

   `http://<`*server-instance*`>:`*port number*`/search`

2. 在显示的搜索查询页面中，选中代表要在 “搜索范围”字段中搜索的集合的复选框。
3. 键入用于说明查询的文字，然后按 ENTER 键 （或单击 “搜索”按钮）以获得相关 Web 页的列表。

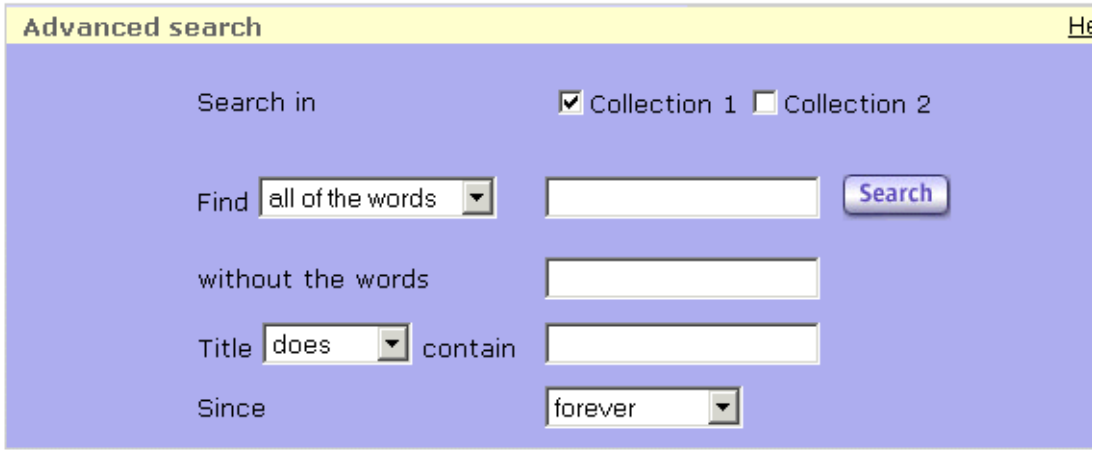
您可以使用下节所述的 “高级搜索”中提供的搜索参数来设置更精确的搜索。

高级搜索

用户可以通过添加用于微调关键字的运算符来提高搜索的准确性。可以从 “高级搜索”选择这些选项。

下图显示了 “高级搜索”：

“高级搜索”



要进行高级搜索查询，请执行以下步骤：

1. 通过在浏览器的地址栏中按以下格式输入搜索 Web 应用程序的 URL 来访问该程序：

   `http://<`*server-instance*`>:`*port number*`/search`

2. 单击 “高级”链接。
3. 输入以下信息中的一项或所有项：
   - **搜索范围**。选择要搜索的集合。
   - **查找**。支持四个选项：
     - **所有词**。查找包含 “查找”字段中指定的所有关键字的页面。
     - **任一词**。查找包含 “查找”字段中指定的任一关键字的页面。
     - **完全匹配的词组**。查找包含与 “查找”字段中的短语完全匹配的短语的页面。
     - **段落搜索**。在检索到的页面中突出显示包含关键字或词的段落。
   - **不包含词**。搜索将排除包含指定文字的 Web 页。
   - **标题 “包含 / 不包含”**。将搜索限制在标题中包含指定关键字的页面。
   - **自**。将搜索操作限制为在选定时间段内被编制索引的 Web 页。

查看搜索结果

搜索结果将显示在用户浏览器中的 Web 页面上，包含指向服务器上符合搜索条件的文档的 HTML 超级链接。缺省情况下，每个页面显示 10 个记录 （命中项），这些记录基于相关性按降序排序。每个记录都列出诸如文件名、大小、创建日期等信息。匹配的文字还被突出显示。

注 服务器管理员可以自定义这些搜索页面，如 “自定义搜索页面”中所述。

自定义搜索页面

Sun ONE Web Server 包含一个提供基本搜索查询和搜索结果页面的缺省搜索应用程序。可以直接使用这些 Web 页，也可以对其进行自定义以满足特定需要。这种自定义可以像使用不同徽标重新设置 Web 页一样简单，也可以像更改搜索结果的显示顺序一样复杂。

与 Sun ONE Web Server 6.0 不同，现在不再使用模式文件来自定义搜索界面，而是使用 Sun ONE Web Server 6.1 中附带的一组 JSP 标记库来进行自定义。缺省搜索应用程序提供了样例 JSP，这些样例 JSP 说明了如何使用搜索标记库来建立自定义的搜索界面。您可以参见位于 `/bin/https/webapps/search` 的缺省搜索应用程序，该样例应用程序说明了如何使用可自定义的搜索标记。

缺省搜索界面由四个主要的组件组成：标题、页脚、查询表单和结果。

通过更改标记的属性值，可以轻松地自定义这些基本元素。可以使用标记库实现更为详细的自定义。

本部分包括以下主题：

- 搜索界面组件
- 自定义搜索查询页面
- 自定义搜索结果页面
- 在单独的页面中自定义表单和结果
- 标记惯例
- 标记规范

搜索界面组件

搜索界面包含以下组件：

标题

标题包括徽标、标题和简短说明。

页脚

页脚包含版权信息。

表单

查询表单包含一组代表搜索集合的复选框、一个查询输入框以及 “提交”和 “帮助”按钮。

结果

缺省情况下每页列出 10 个记录。对于每个记录，将显示以下信息：标题、段落、大小、创建日期和 URL。段落是页面的一个片段，其中将突出显示匹配的文字。

自定义搜索查询页面

查询表单包含一个搜索集合的复选框列表、一个查询输入框和 “提交”按钮。此表单是使用具有以下缺省值的 `<s1ws:form>` 标记以及 `<collElem>`、`<queryBox>` 和 `<submitButton>` 标记创建的：

```
<s1ws:form>
    <s1ws:collElem />
    <s1ws:queryBox /> <s1ws:submitButton />
</s1ws:form>
```

可以将查询表单放到页面的任意位置：中间、边栏等等。也可以以不同格式显示查询表单，例如使用一个横栏，其中集合选择框、查询字符串输入框以及 “提交”按钮被水平排列；或显示为一个块，其中集合显示为复选框，查询输入框和 “提交”按钮位于下方。

以下实例显示了如何使用 `<searchForm>` 标记组来创建不同格式的查询表单。

水平栏

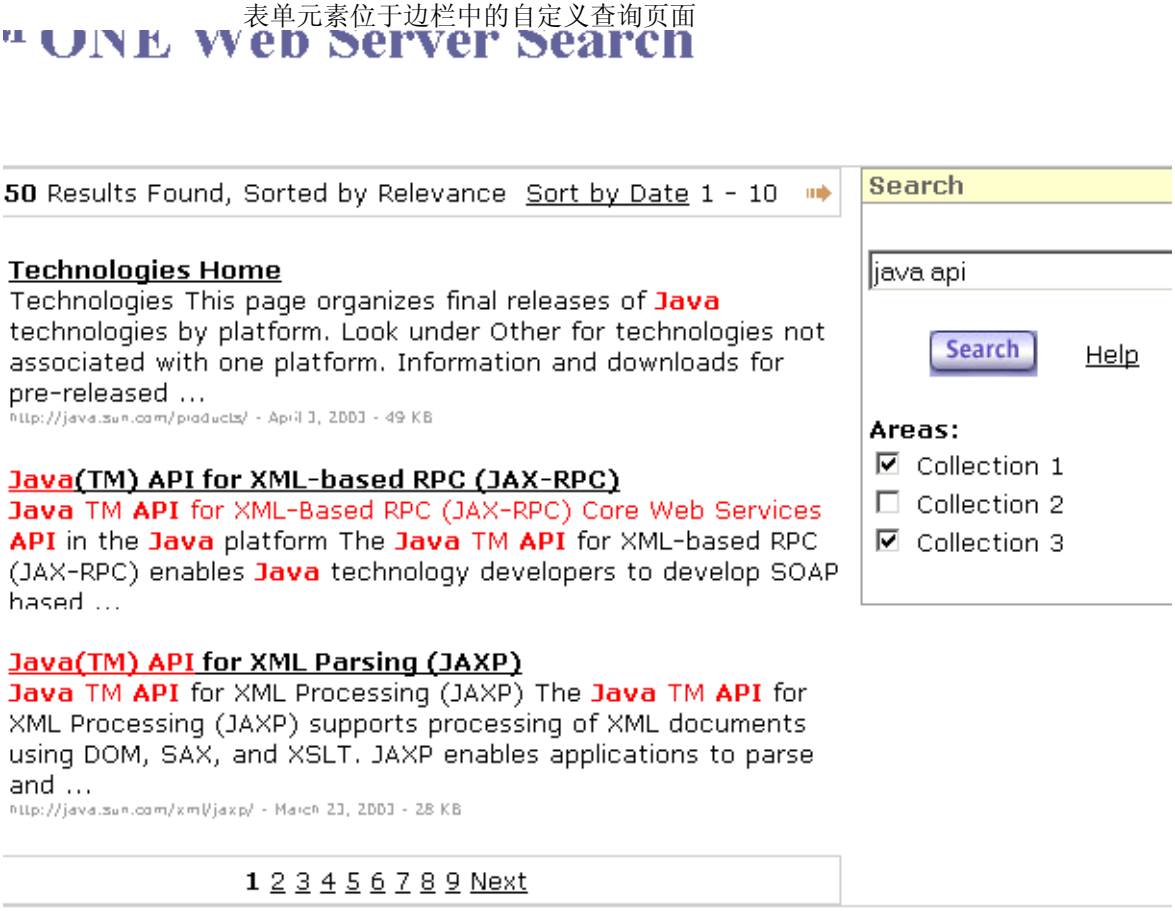
下面的样例代码将创建一个表单，其中包含一个所有集合的选择框、一个查询输入框和一个“提交”按钮，均排列在一行。

```
<s1ws:form>
   <table cellspacing="0" cellpadding="3" border="0">
   <tr class="navBar">
      <td class="navBar"><s1ws:collElem type="select" /></td>
      <td class="navBar">
         <s1ws:querybox size="30" />
         <s1ws:submitButton class="navBar" style="padding:0px;
margin:0px; width:50px" />
      </td>
   </tr>
   </table>
</s1ws:form>
```

边栏块

您可以创建一个表单块，其中表单元素被排列在一个边栏中，表单块的标题为“搜索”，使用的格式与边栏中其他项的格式相同。这种排列的效果如下图所示：

表单元素位于边栏中的自定义查询页面



在下面的样例代码中，表单主体包含三个排成一列的复选框，列出了可用的搜索集合。查询输入框和 “提交”按钮位于下方：

```
<slws:searchForm>
    <table>
<!--... other sidebar items ... -->
    <tr class="Title"><td>Search</td></tr>
    <tr class="Body">
```

```
        <td>
        <table cellspacing="0" cellpadding="3" border="0">
        <tr class="formBlock">
           <td class="formBlock"> <s1ws:collElem type="checkbox"
cols="1" values="1,0,1,0" /> </td>
        </tr>
        <tr class="formBlock">
           <td class="formBlock"> <s1ws:querybox size="15"
maxlength="50" /> </td>
        </tr>
        <tr class="formBlock">
           <td class="formBlock"> <s1ws:submitButton class="navBar"
style="padding:0px; margin:0px; width:50px" /> </td>
        </tr>
        </table>
        </td>
    </tr>
    </table>
</s1ws:searchForm>
```

自定义搜索结果页面

搜索结果的生成过程如下：

- <formAction> 标记检索所有表单元素的值并进行基本验证。
- <formAction> 标记中出现的 <search> 标记、 <resultIteration> 标记和其他标记可以访问所有表单元素的值。
- <search> 标记通过 <formAction> 使用查询字符串和集合来执行搜索，并将搜索结果保存在 pageContext 中。
- <resultIteration> 标记随后对结果集进行检索并重新显示。

通过更改标记的属性值，您可以自定义搜索结果页面。

以下样例代码以标题栏开始，随后显示一些指定的记录，最后显示导航栏。标题栏包含搜索中使用的查询字符串以及返回的全部记录的范围 （例如 1 – 10）。对于每个记录，记录部分显示了带有指向该文件的链接的标题、最多三个关键字被突出显示的段落、 URL、创建日期以及文档大小。

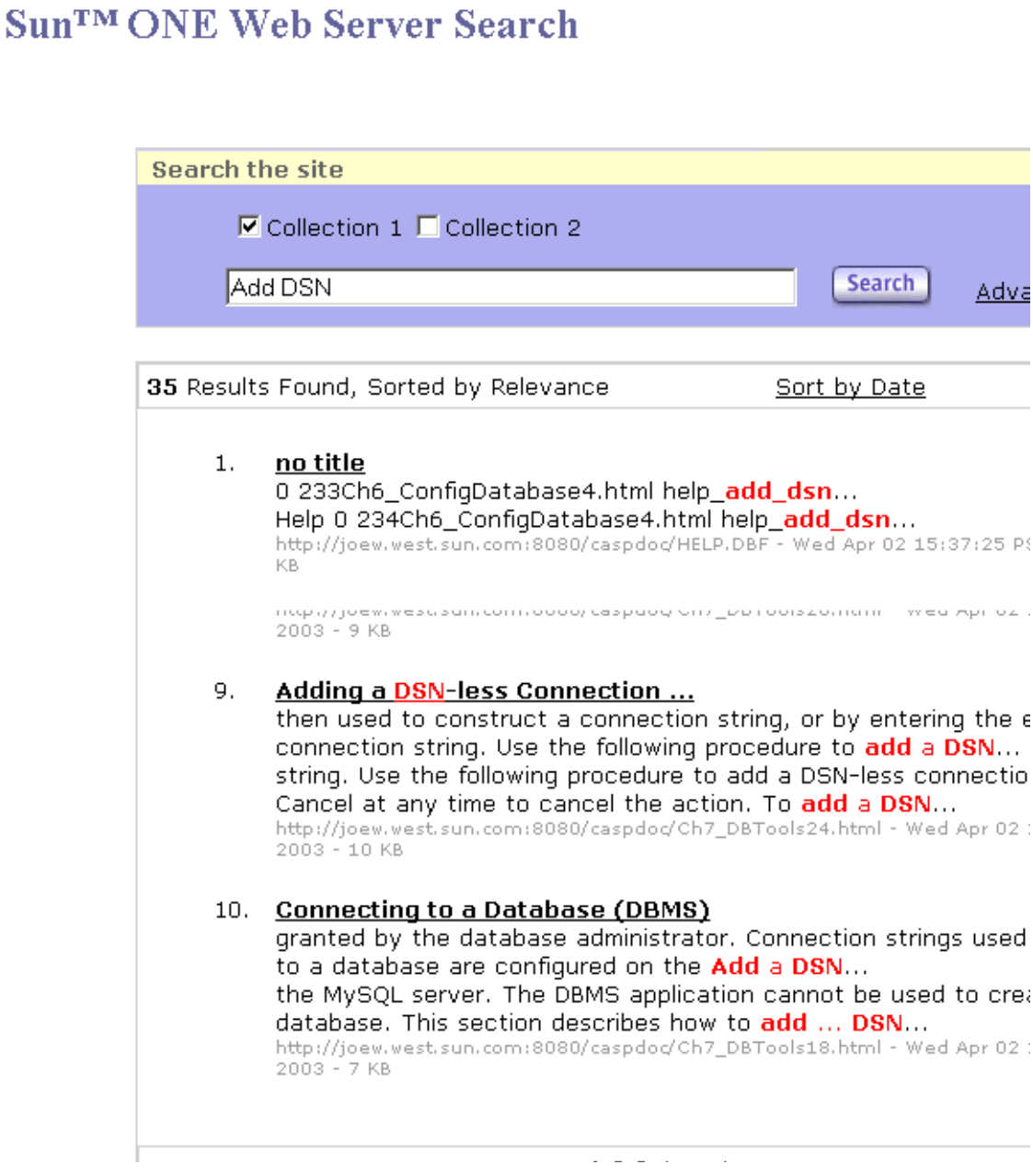
在该部分的末尾处，导航栏提供了指向上一页和下一页的链接，以及指向当前页之前和之后八个页面的直接链接。

```
<s1ws:formAction />

<s1ws:formSubmission success="true" >

   <s1ws:search scope="page" />

   <!--search results-->

   (...html omitted...)

      <s1ws:resultStat formId="test" type="total" /></b> Results
Found, Sorted by Relevance</span></td><td>

      <span class="body"><a href="/search/search.jsp?">Sort by
Date</a></span></td>

      <td align="right"><span class="body">

      <s1ws:resultNav formId="test" type="previous" caption="<img
border=0 src=\"images/arrow-left.gif\" alt=\"Previous\">" />

       <s1ws:resultStat formId="test" type="range" />

       <s1ws:resultNav formId="test" type="next" caption="<img
border=0 src=\"images/arrow-right.gif\" alt=\"Next\">" />

        <!img alt="Next" src="images/arrow-right.gif"
border="0" WIDTH="13" HEIGHT="9">

         (...html omitted...)

      <table border=0>

      <s1ws:resultIteration formId="test" start="1" results="15">

         <tr class=body>

            <td valign=top>

            <s1ws:item property='number' />.  

            </td>

            <td>

               <b><a href="<s1ws:item property='url'
/>"><s1ws:item property='title' /></a></b>

               <br>
```

```
                    <s1ws:item property='passages' />
                    <font color="#999999" size="-2">
                    <s1ws:item property='url' /> -
                    <s1ws:item property='date' /> -
                    <s1ws:item property='size' /> KB
                    </font><br><br>
                </td>
            </tr>
        </s1ws:resultIteration>
        </table>
        (...html omitted...)
        <s1ws:resultNav formId="test" type="previous" />
        <s1ws:resultNav formId="test" type="full" offset="8" />
        <s1ws:resultNav formId="test" type="next" />
    (...html omitted...)
</s1ws:formSubmission>
```

下图显示了自定义的搜索结果页面：

自定义的搜索结果页面



通过操作标记和修改 HTML 可以轻松地自定义基本搜索结果界面。例如，可以将导航栏复制并放到搜索结果前面。用户也可以选择显示或不显示搜索记录的任何特性。

除了与表单一起使用外，<search>、<resultIterate> 和相关标记还可用于列出的特定主题。以下样例代码列出了某个站点上有关 Java Web 服务的头十篇文章。

```
<s1ws:search Collection="Articles" Query="Java Web Services" />

<table cellspacing="0" cellpadding="3" border="0">

  <tr class="Title"><td>Java Web Services</td></tr>

</table>

<table cellspacing="0" cellpadding="3" border="0">

<s1ws:resultIteration>

<tr>

<td><a href="<s1ws:item property='URL' />"> <s1ws:item
property='Title'/></a></td>

</tr>

</s1ws:resultIteration>

</table>
```

在单独的页面中自定义表单和结果

如果需要将表单页面和结果页面分开，必须使用 <form> 标记组创建表单页面，并使用 <formAction> 标记组创建结果页面。

需要在结果页面中添加指向表单页面的链接以使页面衔接顺畅。

标记惯例

请注意以下标记惯例：

- 标记类属于 com.sun.web.search.taglibs 软件包。
- 所有 pageContext 属性均具有 com.sun.web 前缀。例如，搜索结果的属性为 com.sun.web.searchresults.*form_id*，其中 *form_id* 为表单的名称。
- 可以使用 s1ws 前缀来引用标记库。标记的名称及其属性是大小写混合的，其中每个内部单词的首字母大写，例如 pageContext。

标记规范

Sun ONE Web Server 包括一组 JSP 标记，这些标记可用于自定义搜索界面中的搜索查询和搜索结果页面。

有关可以用来自定义搜索页面的 JSP 标记的完整列表，请参见 Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications*。

第 19 章

使用 WebDAV 进行 Web 发布

Sun ONE Web Server 6.1 支持 WebDAV （即基于 Web 的分布式制作和版本发布），这是一种新兴的基于 Web 的协作标准。WebDAV 是 HTTP/1.1 协议的扩展，它允许客户机执行远程 Web 内容制作操作。

本章主要介绍如何在 Sun ONE Web Server 6.1 中使用 WebDAV。其中包括以下部分：

关于 WebDAV

WebDAV 是对 HTTP/1.1 协议的扩展，添加了新的 HTTP 方法和标头，支持任意类型的 Web 制作，不仅支持 HTML 和 XML，还支持文本、图形、电子表格等格式。

使用 WebDAV 可以完成的工作包括：

- **特性 （元数据）处理**。您可以使用 WebDAV 方法 PROPFIND 和 PROPPATCH 创建、删除和查询有关 Web 页面的信息，例如作者和创建日期。
- **集合和资源管理**。您可以使用 WebDAV 方法 GET、 PUT、 DELETE 和 MKCOL 创建文档集合并检索分层结构成员列表 （类似于文件系统中的目录列表）。
- **锁定**。您可以使用 WebDAV 禁止多人同时对一个文档进行操作。可以通过 WebDAV 方法 LOCK 和 UNLOCK 使用互斥锁或共享锁，这将有助于防止出现“丢失更新”（更改被覆盖）的问题。
- **名称空间操作**。您可以使用 WebDAV 方法 COPY 和 MOVE 让服务器复制和删除 Web 资源。

Sun ONE Web Server 6.1 中的 WebDAV 支持提供了以下功能：

- 与 RFC2518 的兼容性，与 RFC2518 客户机的互操作性
- 发布的安全性和访问控制
- 对基于文件系统的 WebDAV 集合和资源的有效发布操作

常见 WebDAV 术语

本节概述了使用 WebDAV 时经常遇到的术语。

URI。 URI （统一资源标识符）是一种文件标识符，通过使用缩写的 URL 提供了额外的安全保护。一个 URL 映射代替了 URL 的第一部分，从而对用户隐藏了文件的完整物理路径名。

源 URI。术语“源 URI”是指能用来访问资源的源代码的 URI。为了更好地理解源 URI 的概念，请参见以下实例：

一个名为 foo.jsp 的 JSP 页面位于 URI /docs/date.jsp 处。该页面包含 HTML 标记和 Java 代码，当执行该代码时，将在客户机的浏览器中打印当前的日期。当服务器收到客户机获取 foo.jsp 的 GET 请求后，先执行该 Java 代码，然后提供该页面。客户机收到的并不是该 foo.jsp 页面 （因为它驻留在服务器上），而是一个显示当前日期的动态生成的页面。

如果您要创建一个源 URI （例如 /publish/docs）并将其映射到包含 foo.jsp 的 /docs 目录，则对 /publish/docs/foo.jsp 的请求将是请求 /docs/foo.jsp JSP 页面的源代码。在这种情况下，服务器将提供页面而不执行 Java 代码。客户机将收到未经处理的页面，与保存在磁盘中的一样。

这样，对源 URI 的请求也就成了请求资源的源代码。

集合。WebDAV 集合是为 WebDAV 操作启用的一个或一组资源。集合包含一组称为成员 URI 的 URI，它们标识了启用了 WebDAV 的成员资源。

成员 URI。集合中一组 URI 中的一个成员。

内部成员 URI。与集合的 URI 直接相关的一个成员 URI。例如，如果 URL 为 `http://info.sun.com/resources/info` 的资源启用了 WebDAV，并且如果 URL 为 `http://info.sun.com/resources/` 的资源也启用了 WebDAV，则 URL 为 `http://info.sun.com/resources/` 的资源就是一个集合，它包含 `http://info.sun.com/resources/info` 并将其作为一个内部成员。

特性。一个包含资源的相关说明性信息的 “名称 / 值”对。使用特性可以有效地查找和管理资源。例如，可以使用特性 “creationdate”按资源的创建日期索引所有资源，或者使用特性 “author”按作者姓名进行索引。

动态特性。由服务器强制实现的特性。例如，动态特性 `getcontentlength` 有一个值，即 GET 请求返回的实体的长度，它是由服务器自动计算的。动态特性具有以下特性：

- 特性值是只读的，由服务器维护。
- 特性值由客户机维护，但是服务器对提交的值执行语法检查。

静态特性。不是由服务器强制实现的特性。服务器仅记录静态特性的值；客户机负责维护其一致性。

Sun ONE Web Server 6.1 支持以下动态特性：

- `creationdate`
- `displayname`
- `getcontentlanguage`
- `getcontentlength`
- `getcontenttype`
- `gettag`
- `getlastmodified`
- `lockdiscovery`
- `resourcetype`
- `supportedlock`

- executable

注 Sun ONE web Server 支持动态特性 executable，它允许客户机更改与资源相关联的文件访问权限。

参见以下对 executable 动态特性的 PROPPATCH 请求：

```
PROPPATCH /test/index.html HTTP/1.1

Host:sun

Content-type:text/xml

Content-length:XXXX

<?xml version="1.0"?>

<A:propertyupdate
xmlns:A="DAV:"xmlns:B="http://apache.org/d
av/props/">

<A:set>

<A:prop>

<B:executable>T</B:executable>

</A:prop>

</A:set>

</A:propertyupdate>
```

锁定。锁定资源功能提供了这样一种机制，即可以保证在一个用户编辑资源时，其他用户不能进行修改。锁定可以防止发生覆盖冲突，解决了 “丢失更新”的问题。

Sun ONE Web Server 支持两种锁定类型：共享和互斥。

新 HTTP 标头。 WebDAV 扩展了 HTTP/1.1 协议。它定义了新的 HTTP 标头，客户机可以通过这些新标头传递 WebDAV 资源请求。这些标头为：

- Destination:
- Lock-Token:
- Timeout:
- DAV:
- If:
- Depth:
- Overwrite:

新 HTTP 方法。 WebDAV 引入了若干新 HTTP 方法，用于告知启用了 WebDAV 的服务器如何处理请求。这些方法是对现有方法（例如 `GET`、 `PUT` 和 `DELETE`）的补充，可用来执行 WebDAV 事务。下面简要介绍这些新 HTTP 方法：

- `COPY`。用于复制资源。可以使用 `Depth:` 标头移动资源，使用 `Destination:` 标头指定目标。如果适用， COPY 方法也使用 `Overwrite:` 标头。
- `MOVE`。用于移动资源。可以使用 `Depth:` 标头移动资源，使用 `Destination:` 标头指定目标。如果适用， MOVE 方法也使用 `Overwrite:` 标头。
- `MKCOL`。用于创建新集合。使用此方法可避免过载 PUT 方法。
- `PROPPATCH`。用于设置、更改或删除单个资源的特性。
- `PROPFIND`。用于获取一个或多个资源的一个或多个特性。当客户机向服务器提交对某个集合的 PROPFIND 请求时，该请求可能会包含一个值为 `0`、 `1` 或 `infinity` 的 Depth: 标头。
  - `0`。指定将获取指定 URI 处的集合的特性。
  - `1`。指定将获取该集合以及位于该指定 URI 之下与其紧邻的资源的特性。
  - `infinity`。指定将获取该集合及其包含的所有成员 URI 的特性。由于深度为无穷大的请求需要遍历整个集合，因而会大大增加服务器的负担。
- LOCK。为资源添加锁。使用 `Lock-Token:` 标头。
- UNLOCK。删除资源的锁。使用 `Lock-Token:` 标头。

使用 WebDAV

一个完整的 WebDAV 事务包括一个启用了 WebDAV 的服务器（例如 Sun ONE Web Server 6.1），它可以为 WebDAV 资源请求提供服务，还包括一个启用了 WebDAV 的客户机（例如 Adobe® GoLive® 或 Macromedia® DreamWeaver®），它支持启用了 WebDAV 的 Web 发布请求。

在服务器端，需要启用并配置 Sun ONE Web Server 6.1 以便能够为 WebDAV 请求提供服务。

要配置 Sun ONE Web Server 6.1 以便使用 WebDAV，需要执行以下步骤：

- 启用 WebDAV
- 创建 WebDAV 集合
- 配置 WebDAV

- 为 WebDAV 启用访问控制

启用 WebDAV

安装 Sun ONE Web Server 6.1 时，缺省情况下 WebDAV 被禁用。

为了在集合级别启用 WebDAV，还需要在服务器实例级别和虚拟服务器类级别启用 WebDAV。

注 在集合级别上指定的属性将覆盖在虚拟服务器级别上设置的属性值。

以下各部分对在不同级别上启用 WebDAV 进行了说明：

- 为服务器实例启用 WebDAV
- 为虚拟服务器类启用 WebDAV
- 为集合启用 WebDAV

为服务器实例启用 WebDAV

您可以使用 Administration Server 为整个服务器启用 WebDAV。执行此操作时，以下指令将添加到用于加载 WebDAV 插件的 `magnus.conf` 文件中：

```
Init fn="load-modules" shlib="/s1ws6.1/lib/libdavplugin.so"
funcs="init-dav,ntrans-dav,pcheck-dav,service-dav"

shlib_flags="(global|now)"

Init fn="init-dav" LateInit=yes
```

`init-dav` Init 函数将初始化并注册 WebDAV 子系统。

要全局启用 WebDAV，请执行以下步骤：

1. 访问要为其启用 WebDAV 的服务器的 Server Manager。
2. 单击 “Preferences”中的 “Enable/Disable WebDAV”链接。
3. 选中 “Enable WebDAV Globally”复选框。

   为实例启用 WebDAV

4. 单击 “Apply”。
5. 单击 “Apply Changes”按钮，重新启动服务器。

   或

   单击 “Load Configuration Files”，动态应用所做的更改。

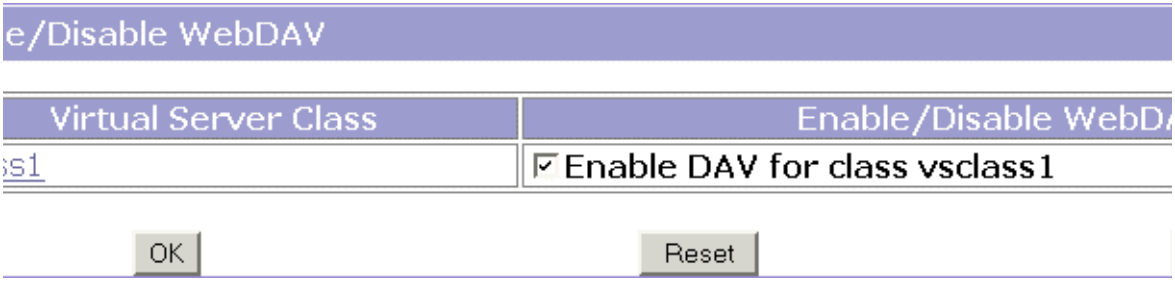
为虚拟服务器类启用 WebDAV

要为特定虚拟服务器类启用 WebDAV，请执行以下步骤：

1. 选择虚拟服务器类。
2. 单击 “Content Mgmt”选项卡。

3. 单击 “Enable/Disable WebDAV”链接。

   为虚拟服务器类启用 WebDAV。



4. 选中 “Enable DAV”复选框。
5. 单击 “OK”。

为虚拟服务器类启用 WebDAV 时，将使用以下条目更新相关联的 `obj.conf` 文件：

```
<Object name="default">
...
Service fn="service-dav"
method="(OPTIONS|PUT|DELETE|COPY|MOVE|PROPFIND|PROPPATCH|LOCK|UN
LOCK|MKCOL)"
Error fn="error-j2ee"
...
</Object>
...
<Object name="dav">
PathCheck fn="check-acl" acl="dav-src"
Service fn="service-dav"
method="(GET|HEAD|POST|PUT|DELETE|COPY|MOVE|PROPFIND|PROPPATCH|L
OCK|UNLOCK|MKCOL)"
</Object>
```

为集合启用 WebDAV

如果向某个虚拟服务器添加了一个或多个 WebDAV 集合，您可以随时启用或禁用它们。有关如何执行此操作的信息，请参见第 396 页上的 “编辑 WebDAV 集合”。

创建 WebDAV 集合

WebDAV 集合是为 WebDAV 操作启用的一个或一组资源。这些操作包括 Web 发布和协作制作、名称空间管理以及元数据管理。

要向虚拟服务器添加 WebDAV 集合，请执行以下步骤：

1. 确保为服务器实例和虚拟服务器类启用了 WebDAV。有关详细信息，请参见第 392 页上的 “为服务器实例启用 WebDAV”和第 393 页上的 “为虚拟服务器类启用 WebDAV”。
2. 访问您要管理的虚拟服务器并单击 “WebDAV”选项卡。
3. 在 “Add DAV Collection”中，输入以下信息：
   - **URI** （必需）。用于访问内容的 URI。
   - **Source URI** （可选）。用于访问源的 URI。

注 如果要发布动态内容 （例如 CGI 或 SHTML），必须配置一个源 URI。

有关术语 “源 URI”的解释，请参见 “常见 WebDAV 术语”。

   - **Lock Database** （可选）。用于维护锁数据库的目录。缺省值为 *server-instance*`/lock-db/vs-id`。
   - **Minimum Lock Timeout** （可选）。锁的最小生命周期 （秒）。缺省值为 `0`。有关详细信息，请参见 “最小锁超时”。
   - **Limit XML Request Body** （可选）。请求正文中 XML 内容的最大大小。对大小进行限制可防止可能出现的拒绝服务 （Denial of Service， DOS）攻击。
   - **Maximum Property Depth** （可选）。 `PROPFIND` 请求的深度。
     - `0` 只适用于指定的资源。
     - `1` 适用于指定的资源及其包含的下一级资源。
     - `infinity` 适用于指定的资源及其包含的所有资源。

     缺省情况下，该值被设置为 `0`。
   - **Enabled** （可选）。为集合启用 WebDAV 功能。
4. 单击 “OK”。

注

- 使用 Administration Server 添加集合时，服务器不会自动在文件系统上为集合创建目录。管理员需要确保在文件系统上创建一个与该集合对应的目录。
- 在 UNIX 系统上，如果您以 `root` （超级用户）身份安装了 Web 服务器，然后使用其他用户身份运行该服务器，请确保运行服务器的用户身份对您创建的 WebDAV 集合的相应目录具有读 / 写权限。

编辑 WebDAV 集合

您可以编辑现有 DAV 集合的属性，例如，配置集合的访问控制。

要编辑现有的 WebDAV 集合，请执行以下步骤：

1. 访问集合所在的虚拟服务器，然后单击 “WebDAV” 选项卡。
2. 在 “Edit DAV Collections” 中，修改以下信息：
   - **Delete**。允许您删除集合。
   - **URI**。显示用于访问内容的 URI。
   - **Enabled**。表示是启用 (`true`) 还是禁用 (`false`) WebDAV。
   - **Edit Collection**。单击此按钮可进行以下配置：
     - **URI** （必需）。用于访问内容的 URI。
     - **Source URI** （可选）。用于访问源的 URI。
     - **Lock Database** （可选）。用于维护锁定数据库的目录。
     - **Minimum Lock Timeout** （可选）。锁的最小生命周期 （秒）。有关详细信息，请参见 “最小锁超时”。

注

如果 `minlocktimeout` 的值为 -1，则表示无限期锁。

     - **Limit XML Request Body** （可选）。请求正文中 XML 内容的最大大小。

- **Maximum Property Depth** （可选）。 PROPFIND 请求的深度。

  — 0 只适用于指定的资源。

  — 1 适用于指定的资源及其包含的下一级资源。

  — infinity 适用于指定的资源及其包含的所有资源。

  缺省情况下，该值被设置为 0。

- **Enabled** （可选）。为集合启用 WebDAV 功能。

o **Edit ACL**。单击此按钮可为该集合或 URI 设置访问控制限制。

配置 WebDAV

由于以下原因，您可能希望对 WebDAV 进行配置：例如，要优化服务器性能、消除安全风险或提供无冲突的远程制作。

为满足您的配置要求，您可以更改服务器对 WebDAV 资源的最小锁时间、对集合的 PROPFIND 请求的深度以及请求正文所允许的 XML 内容的最大大小等设置。

可以在虚拟服务器级别为虚拟服务器下的所有集合配置缺省 WebDAV 属性。此处配置的值与 server.xml 文件中的 DAV 元素相对应。

也可以在集合级别配置 WebDAV 属性，这将覆盖为集合配置的任何虚拟服务器级别属性。在集合级别配置的属性与 server.xml 文件中的 DAVCOLLECTION 元素相对应。

- 在虚拟服务器级别配置 WebDAV
- 在 URI 级别配置 WebDAV

在虚拟服务器级别配置 WebDAV

要为虚拟服务器配置 WebDAV 功能，需要编辑 DAV 对象的属性。您可以通过使用 Administration Server 或手动编辑 server.xml 文件来执行此操作。

下表说明了可配置的 DAV 对象的属性：

表 19-1 DAV 对象的属性

属性	说明
enabled	指定是否为该虚拟服务器启用了 WebDAV 功能。 这是一个可选属性。缺省值为 true。 可能的值为 true 和 false。
lockdb	指定用于维护锁定数据库的目录。 这是一个可选属性。
minlocktimeout	指定锁的最小生命周期 （秒）。此值表示锁被自动删除之前某元素被锁定的时间。有关详细信息，请参见 “最小锁超时”。 这是一个可选属性。
maxxmlrequestbodysize	指定请求正文中 XML 内容的最大大小。 这是一个可选属性。缺省值为 8K。 对大小进行限制可防止可能出现的拒绝服务 (DOS) 攻击。
maxpropdepth	指定 PROPFIND 请求的深度。 这是一个可选参数。缺省值为 0。 通过限制此参数的大小可防止过度消耗内存。

在 URI 级别配置 WebDAV

要在 URI 级别配置 WebDAV 功能，需要编辑 `server.xml` 文件中 `DAVCOLLECTION` 对象的属性。

下表说明了可配置的 `DAVCOLLECTION` 对象的属性：

表 19-2 `DAVCOLLECTION` 对象的属性

属性	说明
`enabled`	指定是否为该集合启用了 DAV 功能。 这是一个可选属性。 可能的值为 `true` 和 `false`。缺省值为 `true`。
`uri`	指定用于访问内容的 URI。 这是一个必需属性。
`sourceuri`	指定用于访问源的 URI。有关详细信息，请参见常见 WebDAV 术语和在启用了 WebDAV 的服务器上使用源 URI 和 Translate:f 标头。 这是一个可选属性。 如果未指定 `sourceuri`，则缺省行为是拒绝对集合中任何动态内容的源代码的访问。 您可以为 `uri` 和 `sourceuri` 指定相同的 URI，这样，服务器将始终返回动态内容的源代码。如果您使用一个独立的、安全的虚拟服务器进行发布，这会很有用。
`lockdb`	指定用于维护锁定数据库的目录。 这是一个可选属性。
`minlocktimeout`	指定锁的最小生命周期（秒）。此值表示锁被自动删除之前某元素被锁定的时间。有关详细信息，请参见“最小锁超时”。 这是一个可选属性。
`maxxmlrequestbodysize`	指定请求正文中 XML 内容的最大大小。 这是一个可选属性。 对大小进行限制可防止可能出现的拒绝服务 (DOS) 攻击。
`maxpropdepth`	指定 PROPFIND 请求的深度，它列出了集合的成员资源。 这是一个可选参数。 通过限制此参数的大小可防止过度消耗内存。

在启用了 WebDAV 的服务器上使用源 URI 和 Translate:f 标头

WebDAV 方法处理资源或集合的源。 HTTP 方法 （例如 GET 和 PUT）会被 WebDAV 协议过载。因此，使用这些方法的请求可以是对资源的源代码的请求，也可以是对资源的内容的请求。

Microsoft 和许多其他 WebDAV 供应商通过以下方式解决了此问题，即随请求发送一个 `Translate:f` 标头来告知服务器所请求的是源代码。为了能够与常用的 WebDAV 客户机 Microsoft WebFolders 实现互操作， Sun ONE Web Server 6.1 将 `Translate:f` 标头识别为对资源的源代码的请求。针对不发送 `Translate:f` 标头的客户机， Sun ONE Web Server 6.1 定义了一个源 URI。有关术语 “源 URI” 的更详细说明，请参见 “常见 WebDAV 术语”。

对于启用了 WebDAV 的集合，对 URI 的请求将检索资源的内容 （输出），而对源 URI 的请求将检索资源的源代码。带有 `Translate:f` 标头的 URI 请求被看作是对源 URI 的请求。

请注意，缺省情况下，所有对资源的源代码的访问均被 `dav-src` ACL 拒绝，即在服务器实例的特定 ACL 文件中包含以下声明：

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

用户可以通过添加对源 URI 的访问权限来允许另一个用户对源代码进行访问。有关添加特定 URI 的 ACL 的详细信息，请参见 “为 WebDAV 启用访问控制”。

锁定和解除锁定资源

Sun ONE Web Server 允许服务器管理员锁定资源，以实现对该资源的有序访问。通过使用锁，正在访问某特定资源的用户可以确定其他用户不会修改同一资源。这样就解决了多用户共享服务器上的资源时的 “丢失更新” 问题。由服务器维护的锁数据库将跟踪客户机发出和正在使用的锁标记。

Sun ONE Web Server 6.1 支持 `opaquelocktoken` URI 方案，该方案被设计为在所有资源中始终是唯一的。它使用了通用唯一标识符 (UUID) 机制，如 ISO-11578 中所述。

Sun ONE Web Server 6.1 可识别两种锁定机制：

- 互斥锁
- 共享锁

互斥锁

互斥锁仅将资源的访问权限授予一个用户。其他用户要想访问同一资源，只能等到互斥锁被解除。

人们有时觉得互斥锁定这种资源锁定机制太死板，代价也很大。例如，当程序崩溃或锁所有者忘记解除锁定资源时，便需要通过锁定超时或管理员参与来解除互斥锁。

共享锁

共享锁允许多个用户接收某个资源的锁。这样，具有适当访问权限的任何用户都可以获得该锁。

使用共享锁时，锁所有者之间可以使用其他通信通道来协调工作。共享锁的目的是让协作者知道谁还在使用同一资源。

锁管理

Sun ONE Web Server 6.1 提供了一个锁管理功能，使您可以查看所有现有锁、锁的类型、锁的资源以及锁的持续时间等。

要使用锁管理功能，请执行以下步骤：

1. 访问启用了 WebDAV 的虚拟服务器。
2. 单击 “WebDAV” 选项卡。
3. 单击 “Lock Management” 链接。
4. 选择锁数据库和启用了 WebDAV 的 URI，以便查看其现有锁及其他信息。
5. 单击 “List Lock Info”。

最小锁超时

您可以通过在 `server.xml` 文件中配置 `DAV` 或 `DAVCOLLECTION` 对象的 `minlocktimeout` 属性值来控制锁定。`minlocktimeout` 属性指定锁的最小生命周期 （秒）。此值表示锁被自动删除之前某元素被锁定的时间。

这是一个可选属性。如果此值被设置为 -1，锁将永远不会过期。如果将此值设置为 `0`，则可以使用请求中指定的 Timeout 标头锁定集合中的所有资源。

如果未指定 Timeout 标头，资源将被锁定且永远不会超时。如果将请求中的 Timeout 标头值设置为 `Infinite`，同样，资源将被锁定且永远不会超时。

如果对 WebDAV 资源的请求的 Timeout 标头值大于或等于 `server.xml` 文件中指定的 `minlocktimeout` 值，则资源的锁定时间将是请求中指定的时间。

但是，如果请求中的 Timeout 标头值小于 `server.xml` 文件中指定的 `minlocktimeout` 值，则使用 `server.xml` 文件中指定的 `minlocktimeout` 值来锁定资源。

下表列出了 Sun ONE Web Server 处理锁定请求的方式：

表 19-3 Sun ONE Web Server 处理锁定请求的方式

如果请求中的 Timeout 标头被设置为：	**则资源：**
`Infinite`	被锁定且超时值被设置为 -1 （无限）
无	被锁定且超时值被设置为 -1 （无限）
`Second-`*xxx*	• 如果 *xxx* 等于或大于 `server.xml` 文件中设置的 `minlocktimeout` 值，则使用 *xxx* 值来锁定。 或者 • 如果 *xxx* 小于 `server.xml` 文件中设置的 `minlocktimeout` 值，则使用 `server.xml` 文件中指定的 `minlocktimeout` 值来锁定。

锁定请求实例

该实例显示了一个资源 /col1/myfile.html 上的互斥写锁定请求，超时值为 500 秒。

```
LOCK /col1/myfile.html HTTP/1.1
Host:sun
Content-Type:text/xml; charset="utf-8"
Content-Length: 259
Timeout:Second-500
<?xml version="1.0" encoding="utf-8" ?>
<d:lockinfo xmlns:d="DAV:">
    <d:locktype><d:write/></d:locktype>
    <d:lockscope><d:exclusive/></d:lockscope>
    <d:owner>
    <d:href>http://info.sun.com/resources/info.html</d:href>
    </d:owner>
</d:lockinfo>
```

为 WebDAV 启用访问控制

您可以控制哪些用户可访问启用了 WebDAV 的文档和目录，以及不同的用户或用户组可对文件执行何种操作。您也可以完全禁止对某个文件或文件夹的访问，或只允许特定的授权用户访问。

如果管理您的服务器的缺省访问控制 (ACL) 没有对您进行限制或限制不多，您便可以使用限制访问功能（选择 “Server Preferences”，然后单击 “Restrict Access” 链接）创建一个更适合的 ACL 来限制对启用了 WebDAV 的资源的访问。

WebDAV 请求分别在 AuthTrans 和 PathCheck NSAPI 阶段进行验证和授权。下面的实例定义了一个访问控制规则，禁止除名为 “joe” 以外的所有用户对 /catalog 集合进行写入和删除操作：

```
acl "uri=/catalog/*";

deny(all)

user="anyone";

allow (read,list,execute,info)

user = "all";

allow(write,delete)
```

```
user="joe";
```

有关详细信息，请参见编辑 WebDAV 集合。

限制对启用了 WebDAV 的资源的访问

对 WebDAV 集合的访问控制是使用本地 ACL 文件指定的。每个 WebDAV 方法都会请求一个对启用了 WebDAV 的资源的特定访问权限。例如，如果某个启用了 WebDAV 的文件要被多个并行用户共享，为锁定或解除锁定资源以便进行并行控制，需要具备资源的写权限。

下表汇总了 WebDAV 方法所需的权限。

表 19-1 WebDAV 所需的权限

DAV 方法	所需访问权限
DELETE	删除
PROPFIND	读
PROPPATCH	写
LOCK/UNLOCK	写
MKCOL	写
COPY （*src*/*dst*）	*src* - 读
	dst - 写
MOVE （*src*/*dst*）	*src* - 删除
	dst - 写
GET on request-uri	读
GET on request-uri Translate:f	读
PUT on request-uri	写
PUT on request-uri Translate:f	写

安全性考虑

使用 WebDAV 时，请注意以下安全性考虑：

- 确保启用了 WebDAV 的服务器进程对要控制的文件系统具有读 / 写权限。
- 出于安全性考虑，您可以在另一个侦听端口上配置启用了 WebDAV 的虚拟服务器，该端口限制了访问权限并使用了 SSL 来加密传送的数据。有关使用 SSL 的详细信息，请参见 “使用证书和密钥”。
- 限制请求正文中 XML 内容的大小以防止拒绝服务 (DOS) 攻击。缺省情况下，该大小被限制为 8K。
- 由于基本验证使用明文来传送验证更多信息，所以除非您的连接是安全的，否则请使用摘要验证来验证 WebDAV 客户机，而不要使用基本验证。
- 由于 PROPFIND 请求有可能导致不希望的服务器内容访问，因而请使用访问控制技术保护启用了 WebDAV 的资源的安全。
- WebDAV 有可能通过其源 URI 工具暴露包含敏感信息（如脚本资源）的 URI。所以应当注意允许远程编写脚本的风险，并且应当只允许授权用户对源资源进行读 / 写访问。
- 限制 PROPFIND 请求的深度以防止过度消耗内存。缺省情况下，深度被限制为 0。

第 5 部分

附录

附录 A

命令行实用程序

本附录包含了如何使用 HttpServerAdmin 命令行实用程序的说明。

HttpServerAdmin （虚拟服务器管理）

HttpServerAdmin 是一个命令行实用程序，可以用来与 Server Manager 或 Class Manager 中的虚拟服务器用户界面执行相同的管理功能。如果您愿意使用命令行界面设置虚拟服务器，请使用 HttpServerAdmin。

注 要使用 HttpServerAdmin 命令行实用程序，您必须具有系统的超级用户权限。

HttpServerAdmin 命令行实用程序位于 *server_root*/bin/https/httpadmin/bin 目录中。

运行 HttpServerAdmin 之前，您需要将环境变量 IWS_SERVER_HOME 设置为环境中的服务器根目录。

例如，在 UNIX/Linux 系统上：

```
setenv IWS_SERVER_HOME /usr/sun/servers
```

在 Windows 系统上：

1. 从 “控制面板”中选择 “系统”。
2. 单击 “环境”选项卡。
3. 在 “变量”字段中键入 IWS_SERVER_HOME，在 “值”字段中键入服务器根目录的路径。

4. 单击 “设置”。
5. 单击 “确定”。

注 要执行所有命令，您需要具有文件 `server.xml` 的写入权限，该文件中存储了虚拟服务器的信息。

HttpServerAdmin 语法

`HttpServerAdmin` 的语法如下所示：

`HttpServerAdmin` *command_name command_options* `-d` *server_root* `-sinst` *http_instance*

您可以键入以下命令获得命令参数的联机说明：

```
./HttpServerAdmin -h
```

command_name 参数有四个可能的值：

- control
- create
- delete
- list

每个命令都有其自己的命令选项集。有关更多信息，请参见本章中说明每个命令的小节。

无论命令参数的值是什么，表 A-1 中显示的参数都可应用于 `HttpServerAdmin` 命令的所有用法。

表 A-1 HttpServerAdmin 参数

参数	值
`-d` *server_root*	（必需）此参数用于指定服务器根目录的路径 （服务器的安装位置）。
`-sinst` *http_instance*	（必需）此参数用于指定 `HttpServerAdmin` 将影响哪一个实例。

control 命令

使用 `control` 命令可以启动、停止或禁用类和虚拟服务器。如果未指定虚拟服务器，此命令将启动、停止或禁用类中的每个虚拟服务器。

选项

使用表 A-2 中显示的选项和 `control` 命令可以控制类和虚拟服务器。

表 A-2 Control 命令选项

选项	值
-start	启动指定的虚拟服务器或类中所有的虚拟服务器 （如果未指定虚拟服务器）。
-stop	停止指定的虚拟服务器或类中所有的虚拟服务器 （如果未指定虚拟服务器）。
-disable	禁用指定的虚拟服务器或类中所有的虚拟服务器 （如果未指定虚拟服务器）。

语法

`HttpServerAdmin control -cl` *classname*`, -`*control_option* `[-id` *virtual_server*`] -d` *server_root* `-sinst` *http_instance*

参数

使用这些参数和命令选项可以控制虚拟服务器。

表 A-3 Control 命令参数

参数	值
-cl *classname*	指定虚拟服务器类。
-id *virtual_server*	（可选）指定要控制的虚拟服务器的 ID。

示例

```
HttpServerAdmin control -cl myclass -start -id myvirtualserver -d
/usr/sun/servers -sinst https-sun.com

HttpServerAdmin control -cl myclass -stop -id myvirtualserver -d
/usr/sun/servers -sinst https-sun.com

HttpServerAdmin control -cl myclass -disable -id myvirtualserver
-d /usr/sun/servers -sinst https-sun.com
```

create 命令

使用 `create` 命令可以创建虚拟服务器类、虚拟服务器和套接字。

选项

使用表 A-4 中显示的选项和 `create` 命令可以创建类、侦听套接字、虚拟服务器和资源。

表 A-4 Create 命令选项

选项	值
-c	创建虚拟服务器类。
-l	创建侦听套接字。
-v	创建虚拟服务器。
-r	创建资源。

每个选项又都具有自己的参数，这些参数将显示在以下部分。

创建虚拟服务器类

使用 create 命令的该选项可以创建一个虚拟服务器类。

语法

`HttpServerAdmin create -c -cl` *classname* `-docroot` *document_root* `[-obj` *obj.conf_file*`] [-acptlang` *accept_language*`] -d` *server_root* `-sinst` *http_instance*

参数

使用表 A-5 中显示的参数和 `create -c` 命令选项可以创建类。

表 A-5 创建虚拟服务器类参数

参数	值
-cl *classname*	要创建的类的名称。
-docroot *document_root*	类的文档根目录。它必须为绝对路径。
-obj *obj.conf_file*	（可选）类的 obj.conf 文件。如果未指定此参数，服务器会将 obj.conf 文件创建为 *classname*.obj.conf。如果要为类的 obj.conf 文件指定其他名称，请在此处指定。
-acptlang *accept_language*	（可选）如果未指定此参数，默认情况下 acptlang 将关闭。

示例

```
HttpServerAdmin create -c -cl myclass1 -docroot /docs -d
/export/sun/servers -sinst https-sun.com
```

创建侦听套接字

使用 create 命令的该选项可以创建一个侦听套接字。

语法

`HttpServerAdmin create -l -ip` *ip_address* `-port` *port_number* `-sname` *server_name* `-id` *default_virtual_server* `[-sec security] [-acct` *number_of_accept_threads*`] -d` *server_root* `-sinst http_instance`

参数

使用表 A-6 中显示的参数和 `create -l` 命令选项可以创建侦听套接字。

表 A-6 创建侦听套接字参数

参数	值
-ip *ip_address*	侦听套接字的 IP 地址。
-port *port_number*	侦听套接字的端口号。
-sname *server_name*	要与侦听套接字关联的服务器名称。

表 A-6 创建侦听套接字参数

参数	值
-id *default_virtual_server*	缺省虚拟服务器的 ID。使用虚拟服务器创建侦听套接字之前，该虚拟服务器必须已存在。
-acct *number_of_accept_threads*	（可选）侦听套接字接受线程的数目。
-sec *on*	（可选）如果指定了此参数，使用 On 以启用侦听套接字的安全性。如果未指定此参数，则不会启用安全性。

示例

```
HttpServerAdmin create -l -id ls3 -ip 0.0.0.0 -port 1333 -sname
austen -defaultvs vs2 -sec on -acct 4 -d /export/carey/server6
-sinst https-austen.com
```

创建虚拟服务器

使用 create 命令的该选项可以创建一个虚拟服务器。

请注意，如果未包括某些可选参数的值，则使用缺省值。您始终可以在创建虚拟服务器后更改缺省值。

语法

`HttpServerAdmin create -v -id` *virtual_server* `-cl` *classname* `-urlh` *urlhosts* `[-state` *state*`][-docroot` *document_root*`] [-mime` *mime_types_file*`] [-aclid` *acl_ID*`] -d` *server_root* `-sinst` *http_instance*

参数

使用表 A-7 中显示的参数和 `create -v` 命令选项可以创建虚拟服务器。

表 A-7 创建侦听套接字参数

参数	值
-id *virtual_server*	正在创建的虚拟服务器的 ID。
-cl *classname*	虚拟服务器将成为该类的成员。
-urlh *URL_hosts*	虚拟服务器的 URL 主机。您可以指定多个 URL 主机，主机之间以逗号分隔。
-state *state*	（可选）有效值为 On、 Off 和 Disable。

表 A-7 创建侦听套接字参数

参数	值
-docroot *document_root*	（可选）如果要为虚拟服务器指定文档根目录，请使用此参数。您必须使用绝对路径名称。
-mime *mime_types_file*	（可选）虚拟服务器的 MIME 类型文件的名称。
-aclid *acl_ID*	（可选）`server.xml` 文件中使用的 ACL 文件 ID <ACLID>。

示例

```
HttpServerAdmin create -v -id vs3 -cl class1 -urlh annh -d
/export/sun/server6 -sinst https-sun.com

HttpServerAdmin create -v -id vs4 -cl class1 -urlh annh,annh2
-state off -mime mime.types -d /export/sun/server6 -sinst
https-sun.com
```

创建 JDBC 连接池

通过命令行界面使用 `create -r` 命令可以创建新的 JDBC 连接池。

语法

`HttpServerAdmin -create -r -jdbcconnectionpool -poolname` *jdbcpoolname* `-classname` *classname* [`-steadypoolsize` *steadypoolsize*] [`-maxpoolsize` *maxpoolsize*] [`-poolresizequantity` *poolresizequantity*] [`-idletimeout` *idletimeout*] [`-maxwaittime` *maxwaittime*] [`-connectionvalidation` *true/false*] [`-connectionvalidationmethod` *connectionvalidationmethod*] [`-validationtablename` *validationtablename*] [`-failall` *true/false*] [`-desc` *description*] [[`-property` *propertyname=value*],...]

选项

下表概述了使用 `create -r` 命令选项创建连接池所需的所有选项。

表 A-8 创建连接池参数

参数	值
poolname *jdbcpoolname*	JDBC 连接池的池名称。
classname *classname*	实现数据源的供应商特定的类名。
steadypoolsize *steadypoolsize*	池中必须维持的最小连接数目。
maxpoolsize *maxpoolsize*	池中允许的最大连接数目。
poolresizequantity *poolresizequantity*	达到 steadypoolsize 值时，根据该批量大小调整池的大小。
idletimeout *idletimeout*	连接在池中保持空闲的最长时间 （以秒为单位）。
maxwaittime *maxwaittime*	达到连接超时前调用者等待的时间。
connectionvalidation *true/false*	指定将连接传递到应用程序之前是否验证连接。
connectionvalidationmethod *connectionvalidationmethod*	可以用于验证数据库连接的方法。有效值为 auto-commit、 meta-data 和 table。
validationtablename *validationtablename*	表的名称 （如果 connectionvalidationmethod 设置为 table）。
failall *true/false*	在确定某个连接已失败时，指定是否使池中所有连接都失败并重新创建这些连接。
desc *description*	池的说明。
property *propertyname=value*	指定标准和专用 JDBC 连接池特性的 “名称 - 值”对。

示例

```
HttpServerAdmin create -r -jdbcconnectionpool -poolname testpool
-classname "oracle.jdbc.pool.OracleDataSource" -property
"URL=jdbc:oracle:thin:@dbhost:1521:ORCL,user=scott,password=tige
r" -d /opt/Sun/S1WS6.1 -sinst testinstance
```

创建 JDBC 资源

通过命令行界面使用 `create -r` 命令可以创建新的 JDBC 资源。

语法

`HttpServerAdmin -create -r -jdbc -jndiname` *jndiname* `-poolname` *poolname* [`-desc` *description*] [`-enabled` *true*/*false*]

选项

下表概述了使用 `create -r` 命令选项创建新的 JDBC 资源所需的所有选项。

表 A-9 创建 JDBC 资源参数

参数	值
`jndiname` *jndiname*	资源的 JNDI 名称。
`poolname` *poolname*	JDBC 连接池的池名称。
`desc` *description*	池的说明。
`enabled` *true/false*	指定是否启用或禁用资源。 如果禁用了某个 JDBC 资源，则所有应用程序组件都不能连接到此资源，但资源的配置仍保留在服务器实例中。

示例

```
HttpServerAdmin create -r -jdbc -jndiname "jdbc/testjdbcresource"
-poolname testpool -d /opt/Sun/S1WS6.1 -sinst testinstance
```

创建自定义资源

通过命令行界面使用 `create -r` 命令可以创建新的自定义资源。

语法

`HttpServerAdmin -create -r -custom -jndiname` *jndiname* `-resourcetype` *resourcetype* -factoryclass *factoryclassname* [`-enabled` *true/false*] [`-desc` *description*] [[`-property` *propertyname=value*],...]

选项

下表概述了使用 `create -r` 命令选项创建新的 JDBC 资源所需的所有选项。

表 A-10 创建自定义资源参数

参数	值
`jndiname` *jndiname*	资源的 JNDI 名称。
`resourcetype` *resourcetype*	资源的类型。
`factoryclassname` *factoryclassname*	对象工厂的类名。
`enabled` *true/false*	指定是否启用或禁用资源。
`desc` *description*	池的说明。
`property` *propertyname=value*	指定自定义资源特性的 “名称 - 值” 对。

示例

```
HttpServerAdmin create -r -custom -jndiname "testcustomresource"
-resourcetype "java.lang.String" -factoryclass
"com.mycom.test.StringFactory" -d /opt/Sun/S1WS6.1 -sinst
testinstance
```

创建外部 JNDI 资源

通过命令行界面使用 `create -r` 命令可以创建新的外部 JNDI 资源。

语法

`HttpServerAdmin -create -r -external -jndiname` *jndiname* `-jndilookupname` *jndilookupname* `-restype` *restype* -factoryclass *factoryclass* [`-enabled` *true/false*] [`-desc` *description*] [[`-property` *propertyname=value*],...]

选项

下表概述了使用 `create -r` 命令选项创建新的外部 JNDI 资源所需的所有选项。

表 A-11 创建外部 JNDI 资源参数

参数	值
`jndiname` *jndiname*	资源的 JNDI 名称。
`jndilookupname` *jndilookupname*	资源的 JNDI 查找名称。
`restype` *restype*	资源的类型。
`factoryclass` *factoryclass*	对象工厂的类名。
`enabled` *true/false*	指定是否启用或禁用资源。
`desc` *description*	池的说明。
`property` *propertyname=value*	指定自定义资源特性的 “名称 - 值” 对。

示例

```
HttpServerAdmin create -r -external -jndiname
"testexternalresource" -jndilookupname "rmiconverter" -restype
"samples.rmi.simple.ejb.ConverterHome" -factoryclass
"com.sun.jndi.cosnaming.CNCtxFactory" -property
"java.naming.provider.url=iiop://localhost:3700" -d
/opt/Sun/S1WS6.1 -sinst testinstance
```

创建邮件资源

通过命令行界面使用 `create -r` 命令可以创建新的邮件资源。

语法

`HttpServerAdmin -create -r -mail -jndiname` *jndiname* `-host` *host* `-user` *user* `-from` *from* `[-storeprotocol` *storeprotocol*`] [-storeprotocolclass` *storeprotocolclass*`] [-transportprotocol` *transportprotocol*`] [-transportprotocolclass` *transportprotocolclass*`] [-enabled` *true/false*`] [-desc` *description*`] [[-property` *propertyname=value*`] . . .]`

选项

下表概述了使用 `create -r` 命令选项创建新的邮件资源所需的所有选项。

表 A-12 创建邮件资源参数

参数	值
`jndiname` *jndiname*	资源的 JNDI 名称。
`host` *host*	邮件服务器主机名。
`user` *user*	邮件服务器用户名。
`from` *from*	邮件服务器用来指明邮件发件人的 Email 地址。
`storeprotocol` *storeprotocol*	指定连接至邮件服务器、检索邮件和将邮件保存到文件夹中的存储协议服务。示例值为 `imap` 和 `pop3`。
`storeprotocolclass` *storeprotocolclass*	指定用于存储的服务提供商实现类。 可从以下位置查找该类： • `http://java.sun.com/products/javamail/` • `http://java.sun.com/products/javabeans/glassgow/jaf.html`
`transportprotocol` *transportprotocol*	指定发送邮件的传输协议服务。
`transportprotocolclass` *transportprotocolclass*	指定用于传输的服务提供商实现类。 可从以下位置查找该类： • `http://java.sun.com/products/javamail/` • `http://java.sun.com/products/javabeans/glassgow/jaf.html`
`enabled` *true*/`false`	确定是否在运行时启用该资源。有效值为 `On`、`Off`、`Yes`、`No`、`1`、`0`、`True` 和 `False`。

表 A-12 创建邮件资源参数

参数	值
desc *description*	资源的说明。
property *propertyname=value*	指定自定义资源特性的 “名称 - 值”对。

示例

```
HttpServerAdmin create -r -mail -jndiname "localmail" -host
localhost -user mailid -from mailid@mailhost -d /opt/Sun/S1WS6.1
-sinst testinstance
```

delete 命令

使用 delete 命令可以删除虚拟服务器类、虚拟服务器和侦听套接字。

选项

使用表 A-13 中显示的选项和 `delete` 命令可以删除类。

表 A-13 Delete 命令选项

选项	值
-c	删除指定的虚拟服务器类。
-l	删除指定的侦听套接字 ID。
-v	删除指定的虚拟服务器。
-r	删除指定的资源。

删除类

使用 delete 命令的该选项可以删除一个虚拟服务器类。

语法

`HttpServerAdmin delete -c -cl` *classname* `-d` *server_root* `-sinst` *http_instance*

参数

使用表 A-13 中显示的参数和 `delete` 命令可以删除类。

表 A-14 删除类参数

参数	值
-c l *class*	要删除的类名。

示例

```
HttpServerAdmin delete -c -cl class1 -d /export/sun/server6
-sinst https-sun.com
```

删除侦听套接字

使用 delete 命令的该选项可以删除一个侦听套接字。

语法

`HttpServerAdmin delete -l -id` *listen_socket* `-d` *server_root* `-sinst` *http_instance*

参数

使用表 A-13 中显示的参数和 `delete` 命令可以删除类。

表 A-15 删除类参数

参数	值
-id *listen_socket*	要删除的侦听套接字的 ID。

示例

```
HttpServerAdmin delete -l -id ls3 -d /export/sun/server6 -sinst
https-sun.com
```

删除虚拟服务器

使用 delete 命令的该选项可以删除一个虚拟服务器。

语法

```
HttpServerAdmin delete -v -id virtual_server -cl classname -d server_root
-sinst http_instance
```

参数

使用表 A-13 中显示的参数和 `delete` 命令可以删除虚拟服务器。

表 A-16 删除虚拟服务器参数

参数	值
-id *virtual_server*	要删除的虚拟服务器 ID。
-cl *class*	虚拟服务器所属的类。

示例

```
HttpServerAdmin delete -v -id vs3 -cl class1 -d
/export/sun/server6 -sinst https-sun.com
```

删除 JDBC 连接池

使用 delete 命令的该选项可以删除一个连接池。

语法

```
HttpServerAdmin delete -r jdbcconnectionpoolname
```

参数

使用表 A-13 中显示的参数和 `delete` 命令可以删除连接池。

表 A-17 删除连接池参数

参数	值
connectionpoolname	要删除的连接池的名称。

示例

```
HttpServerAdmin delete -r connpool
```

删除 JNDI 资源

使用 delete 命令的该选项可以删除一个 JNDI 资源。

语法

`HttpServerAdmin delete -r` *jndiname*

参数

使用表 A-13 中显示的参数和 `delete` 命令可以删除 JNDI 资源。

表 A-18 删除 JNDI 资源参数

参数	值
jndiname	要删除的资源的 JNDI 名称。

示例

```
HttpServerAdmin delete -r testresource
```

list 命令

使用 `list` 命令可以列出虚拟服务器类、虚拟服务器、侦听套接字和资源。

语法

`HttpServerAdmin list` *-command_option* `-d` *server_root* `-sinst` *http_instance*

选项

表 A-19 List 命令选项

选项	值
-c	列出所有的虚拟服务器类。
-l	列出所有的侦听套接字。
-v	列出所有的虚拟服务器。
-r	列出指定的资源。

示例

```
HttpServerAdmin list -c -d /export/sun/server6 -sinst
https-sun.com

HttpServerAdmin list -l -d /export/sun/server6 -sinst
https-sun.com
```

列出的信息将显示在命令窗口中。

超文本传输协议

本附录简单介绍了超文本传输协议 (HTTP) 的几项基本内容。有关 HTTP 的详细信息，请访问 Internet 工程任务组 (IETF) 主页：

```
http://www.ietf.org/home.html
```

本附录包括以下部分：

关于超文本传输协议 (HTTP)

超文本传输协议 (HTTP) 是一组说明如何在网络上交换信息的规则，该协议使 Web 浏览器和 Web 服务器能够使用 ISO Latin1 字母表 （带有欧洲语言扩展的 ASCII） 进行通信。

HTTP 建立在请求 / 响应模式基础上。客户机连接到服务器，然后向服务器发送请求。请求中包含以下信息：请求方法、 URI 和协议版本。然后客户机会发送某些标头信息。服务器的响应包括返回协议版本和状态码 （其后紧跟包含服务器信息的标头），然后是请求的数据。然后关闭连接。

iPlanet Web Server 4.x 支持 HTTP 1.1。以前版本的服务器支持 HTTP 1.0。服务器将有条件地与 HTTP 1.1 建议的标准兼容，这些标准由 Internet 工程指导组 (IESG) 和 Internet 工程任务组 (IETF) 的 HTTP 工作组批准。有关进行有条件兼容的标准的详细信息，请参见 IETF Web 站点上的超文本传输协议 HTTP/1.1 规范 (RFC 2068)。

请求

客户机向服务器发送的请求包含以下信息：

- 请求方法
- 请求标头
- 请求数据

请求方法

客户机可以使用多种方法请求信息。最常用的方法包括：

- GET — 请求指定的文档
- HEAD — 仅请求文档的标头信息
- POST — 在这种请求中，服务器会接受客户机的某些数据，例如 CGI 程序的表单输入
- PUT — 使用客户机数据替换服务器文档的内容

请求标头

客户机可以将标头字段发送给服务器。大多数标头是可选的。表 B-1 中列出了某些常用的请求标头。

表 B-1 常用的请求标头

请求标头	说明
Accept	客户机可以接受的文件类型。
Authorization	客户机向服务器证明其身份时使用，其中包含用户名和密码等信息。
User-agent	客户机软件的名称和版本。
Referer	用户单击链接时所链接文档的 URL。
Host	所请求资源的 Internet 主机和端口号。

请求数据

如果客户机发送 POST 或 PUT 请求，则可以在请求标头和空白行之后发送数据。如果客户机发送 GET 或 HEAD 请求，则不发送数据；客户机将等待服务器的响应。

响应

服务器的响应包括以下信息：

- 状态码
- 响应标头
- 响应数据

状态码

当客户机发出请求时，服务器将返回状态码，这是一个三位数字的代码。共有四类状态码：

- 100 - 199 范围内的状态码表示临时响应。
- 200 - 299 范围内的状态码表示事务成功。
- 300 - 399 范围内的状态码表示所请求的文档已被移走，因而无法检索到其 URL。
- 400 - 499 范围内的状态码表示客户机发生错误。
- 500 及 500 以上的状态码表示服务器无法执行请求，或者发生错误。

表 B-2 列出了一些常用的状态码。

表 B-2 常用的 HTTP 状态码

状态码	含义
200	很好；传输成功。这不是错误。
302	已找到。重定向到新的 URL。原来的 URL 已被移除。这不是错误；大多数浏览器将显示新的页面。

表 B-2 常用的 HTTP 状态码

状态码	含义
304	使用本地副本。如果一个页面已经位于浏览器的高速缓存中，当再次请求该页面时，某些浏览器（例如 Netscape Navigator）会将浏览器高速缓存副本的“last-modified”时间标记转发给 Web 服务器。如果服务器上的副本没有浏览器上的副本新，服务器将返回 304 代码，而不是返回请求的页面，以减少不必要的网络通信流量。这不是错误。
401	未授权。用户请求了一个文档，但未提供有效的用户名或口令。
403	禁止。禁止访问此 URL。
404	未找到。请求的文档不在服务器上。返回此代码的另外一种情况是，管理员对服务器进行了保护文档的设置，当未经授权的用户请求该文档时，将返回该文档不存在的信息。
500	服务器错误。服务器发生了错误。服务器管理员应查看服务器错误日志，了解具体原因。

响应标头

响应标头包含有关服务器的信息，以及有关随附文档的信息。表 B-3 列出了常用的响应标头。

表 B-3 常用的响应标头

响应标头	说明
Server	Web 服务器的名称和版本。
Date	当前日期（格林威治标准时间）。
Last-modified	上次修改文档的日期。
Expires	文档到期的日期。
Content-length	随附数据的长度（以字节为单位）。
Content-type	随附数据的 MIME 类型。
WWW-authenticate	在验证时使用，其中的内容用于告诉客户机软件需要提供哪些验证信息（例如用户名和密码）。

响应数据

服务器在最后一个标头字段后发送一个空白行，然后发送文档数据。

ACL 文件语法

本附录介绍了访问控制列表 (ACL) 文件及其语法。ACL 文件为文本文件，其中包含定义能够访问储存在 Web 服务器上资源的用户列表。缺省情况下， Web 服务器使用一个包含访问服务器的所有列表的 ACL 文件。但您可以创建多个 ACL 文件，并在 `obj.conf` 文件中对其进行引用。

如果您打算使用访问控制 API 自定义访问控制，则需要了解 ACL 文件的语法和函数。例如，您可能要使用访问控制 API 与另一数据库 （例如 Oracle 或 Informix 数据库）进行连接。有关 API 的详细信息，请访问 Sun ONE 文档站点：

```
http://docs.sun.com
```

本附录包括以下两部分：

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 文件都必须以其使用的版本号开头。只能有一个版本行，版本行可以位于任何注释行之后。 Sun ONE Web Server 6.1 使用版本 3.0。例如：

```
version 3.0;
```

通过将记号 “#”作为注释行的开头，您可以在文件中添加注释。

文件中每个 ACL 开头的语句都定义了 ACL 的类型。ACL 的类型可以是以下三种类型中的一种：

- **路径 ACL** （用于指定它们所影响的资源的绝对路径）。

- **URI（统一资源标识符） ACL**（用于指定相对服务器的文档根目录的目录或文件）。
- **命名 ACL**（用于指定在 `obj.conf` 文件的资源中引用的名称）。服务器带有一个“缺省”命名资源，任何用户都可以对其进行读访问，但只有 LDAP 目录中的用户可以对其进行写访问。尽管可以从 Sun ONE Web Server 窗口创建命名 ACL，但必须在 `obj.conf` 文件的资源中手动引用该命名 ACL。

路径 ACL 和 URI ACL 可以在项的末尾添加通配符。例如：`/a/b/*`。通配符只能位于项的末尾，否则将不起作用。

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。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。以下各行为多个不同 ACL 类型的实例：

```
acl "path=C:/sun/Servers/docs/mydocs/";
acl "default";
acl "uri=/mydocs/";
```

定义 ACL 的类型后，可以用一个或多个语句定义 ACL 使用的方法（验证语句）以及允许或拒绝哪些用户和计算机进行访问（授权语句）。以下各部分介绍了这些语句的语法。

本部分包括以下主题：

验证方法

ACL 可以任意指定服务器在处理 ACL 时必须使用的验证方法。以下为三种常规方法：

- Basic（缺省）
- Digest
- SSL

基本验证方法和摘要验证方法要求用户在访问资源之前输入用户名和密码。

SSL 验证方法要求用户具有客户证书。 Web 服务器必须启用加密，并且用户的证书颁发者必须位于要验证的信任 CA 列表中。

缺省情况下，服务器对未指定方法的任何 ACL 都使用 “Basic”方法。服务器的验证数据库必须能够处理用户发出的摘要验证。

每个验证行必须指定服务器验证的属性 （用户、组或用户和组）。以下验证语句（位于 ACL 类型行之后）将基本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字母 `sales` 开头的所有用户进行访问：

```
authenticate (user)

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。一般来说，最好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，这是因为规则具有分层结构。也就是说，如果您允许所有用户访问名为 `/my_stuff` 的目录，然后您又创建了一个只允许少数用户访问的子目录 `/my_stuff/personal`，则子目录的访问控制将不起作用，因为可以访问 `/my_stuff` 目录的所有用户也可以访问 `/my_stuff/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，如果将缺省 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";
```

本部分包括以下主题：

- 授权语句的分层结构
- 属性表达式
- 表达式运算符

授权语句的分层结构

ACL 的分层结构取决于资源。例如，如果服务器收到对文档 (URI) `/my_stuff/web/presentation.html` 的请求，服务器将建立一个适用于该 URI 的 ACL 列表。服务器首先添加其 `obj.conf` 文件的 “check-acl” 语句中列出的 ACL，然后附加匹配的 URI 和 PATH ACL。

服务器将以同样的顺序处理此列表。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，服务器将使用匹配的最后一个语句。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，服务器将在文件中使用第一个绝对语句并停止查找其他匹配的资源。

```
version 3.0;
acl "default";
authenticate (user,group) {
     prompt="Web Server";
};
allow (read,execute,list,info)
     user = "anyone";
allow (write,delete)
     user = "all";
acl "uri=/my_stuff/web/presentation.html";
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。以下各行为允许不同用户或计算机访问的实例：

- `user = "anyone"`
- `user = "smith*"`
- `group = "sales"`
- `dns = "*.sun.com"`
- `dns = "*.sun.com,*.mozilla.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。

注	请使用 24 小时制时间指定时间。例如，使用 0400 指定 4:00 a.m. 或 2230 指定 10:30 p.m.。

下列实例将名为 “guests”的一组用户的访问时间限制在 8:00 a.m. 到 4:59 p.m. 之间：

```
allow (read)

    (group="guests") and
    (timeofday<0800 or timeofday=1700);
```

您还可以限制用户在星期几来访问服务器。请使用以下三个字母的缩写来指定星期几：Sun、 Mon、 Tue、 Wed、 Thu、 Fri 和 Sat。

以下实例允许 “premium”组的用户在任意一天的任何时间进行访问。“discount”组的用户可以在周末全天、平时除 8:00 a.m. 至 4:59 p.m. 以外的任何时间进行访问。

```
allow (read) (group="discount" and dayofweek="Sat,Sun") or
(group="discount" and (dayofweek="mon,tue,wed,thu,fri" and
(timeofday<0800 or timeofday=1700)))
or
(group="premium");
```

表达式运算符

您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。在 `user`、 `group`、 `dns` 和 `ip` 中，可以使用以下运算符：

- and
- `or`
- not
- `=`（等于）
- `!=`（不等于）

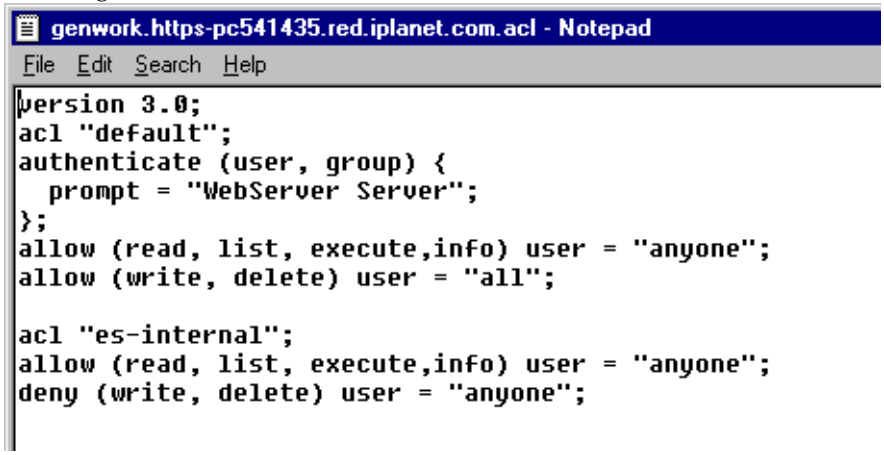
在 `timeofday` 和 `dayofweek` 中，可以使用：

- 大于
- `<`（小于）
- `=`（大于等于）
- `<=`（小于等于）

缺省的 ACL 文件

安装之后，*server_root*`/httpacl/generated.https-`*serverid*`.acl` 文件为服务器提供了缺省设置。服务器使用工作文件 `genwork.https-`*serverid*`.acl`，直到您在用户界面中创建设置。编辑 ACL 文件时，可以在 `genwork` 文件中进行更改，然后使用 Sun ONE Web Server 保存和应用更改。

genwork 文件



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

如果使用任何其他字符，则需要使用双引号将字符引起。

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 中引用 ACL 文件

如果您已命名了 ACL 或独立的 ACL 文件，则可以在 `obj.conf` 文件中引用它们。您可以在 `PathCheck` 指令中使用 `check-acl` 函数完成引用操作。该行使用以下语法：

```
PathCheck fn="check-acl" acl="aclname"
```

`aclname` 是 ACL 显示在任何 ACL 文件中的唯一名称。

例如，如果您要使用名为 testacl 的 ACL 文件限制对某个目录的访问，则可以将下列各行添加到 obj.conf 文件中：

```
<Object ppath="/usr/ns-home/docs/test/*"
PathCheck fn="check-acl" acl="testacl"
</Object>
```

在以上实例中，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，它使用 check-acl 函数将命名 ACL (testacl) 绑定到显示指令的对象。 testacl ACL 可以显示在 magnus.conf 中引用的任何 ACL 文件中。

国际化和本地化支持

Sun ONE Web Server 6.1 的国际化和本地化版本提供了多语言和多编码支持。

本附录介绍了以下主要功能：

输入多字节数据

如果要在 Server Manager 或 Administration Server 中输入多字节数据，您需要知道以下事项：

文件名称或目录名称

如果文件名称或目录名称要显示在 URL 中，则名称不能包含 8 位或多字节字符。

LDAP 用户和组

对于 Email 地址，请仅使用 RFC 1700 (`ftp://ds.internic.net/rfc/rfc1700.txt`) 中许可的字符。用户 ID 和密码信息必须以 ASCII 编码存储。

要确保为用户和组输入正确格式的字符，请使用兼容 UTF-8 格式的客户机 （例如 Netscape Communicator）输入 8 位或多字节数据。

支持多字符编码

Sun ONE Web Server 6.1 为以下功能提供了多字符编码支持：

- WebDAV
- 搜索

WebDAV

Sun ONE Web Server 6.1 支持在 PROPPPATCH 和 PROPFIND 方法中设置和检索多字节特性。尽管请求可以为任何编码格式，但服务器的响应始终为 UTF-8 格式。

搜索

Sun ONE Web Server 6.1 使用基于 Java 的搜索引擎，支持在基本 Java VM 支持的所有字符编码中对文档进行全文索引和搜索。文档的缺省编码可以在创建搜索集合时指定。对于 HTML 文档，索引生成器将尝试从 HTML 元标记来推断编码，如果无法进行推断，则使用缺省编码。

搜索界面基于 JSP 标记库，它可以自定义并以所需的语言和编码进行本地化。 Sun ONE Web Server 6.1 *Programmer's Guide to Web Applications* 中列出了这些标记库。有关更多信息，请参见 “第 378 页上的 “自定义搜索查询页面””。

语言首选项

使用服务器首选项中的 Magnus 编辑器，您可以为服务器设置用于所有最终用户错误信息的缺省语言。 Sun ONE Web Server 6.1 的本地化版本支持七种语言：

- en （英语）
- fr （法语）
- de （德语）
- ja （日语）

- ko （韩语）
- zh （简体中文）
- zh_TW （繁体中文）

Sun ONE Web Server 6.1 本地化版本中的最终用户搜索界面已完全本地化。

注 此设置不会影响非本地化版本的 Web 服务器。

配置服务器以提供本地化内容

最终用户可以配置其浏览器发送一个 Accept-language 标头，用以说明正在访问的内容的语言首选项。通过将 Administration Server 上 “Edit Classes”菜单中的 vs 类的 `acceptlanguage` 设置为打开，可以将服务器配置为提供基于 Accept-language 标头的内容。这样还可以确保所有最终用户错误信息也基于 Accept-language 标头。

例如，如果 `acceptlanguage` 设置为 `on`，客户发送具有值 `fr-CH,de` 的 Accept-language 标头并请求以下 URL：

```
http://www.someplace.com/somepage.html
```

服务器将按以下顺序搜索文件：

1. “`Accept-language`”列表 `fr-CH,de`。

   ```
   http://www.someplace.com/fr_ch/somepage.html
   http://www.someplace.com/somepage_fr_ch.html
   http://www.someplace.com/de/somepage.html
   http://www.someplace.com/somepage_de.html
   ```

2. 不包含国家 / 地区代码的语言代码 （`fr-CH` 时为 `fr`）：

   ```
   http://www.someplace.com/fr/somepage.html
   http://www.someplace.com/somepage_fr.html
   ```

3. `DefaultLanguage`，例如 `magnus.conf` 文件中定义的 `en`。

   ```
   http://www.someplace.com/en/somepage.html
   http://www.someplace.com/somepage_en.html
   ```

4. 如果上述项都未找到，服务器将尝试：

   ```
   http://www.someplace.com/somepage.html
   ```

注 请记住：命名本地化的文件时，类似于 CH 和 TW 的国家 / 地区代码将转换为小写字母，破折号 (-) 将转换为下划线 (_)。

注意 启用 `acceptlanguage` 设置会降低服务器的性能，因为根据上述算法，服务器必须检查 Accept-language 中指定的各种语言的内容。

词汇表

Administration Server　基于 Web 的服务器，包含用来配置所有 Sun ONE Web Server 的表单。

admpw　Enterprise Administrator Server 超级用户的用户名和密码文件。

CGI　通用网关接口。外部程序与 HTTP 服务器进行通信所用的接口。为使用 CGI 而编写的程序称为 CGI 程序或 CGI 脚本。CGI 程序用于处理表单或分析输出，服务器通常不会处理或分析这些表单或输出。

chroot　您可以创建其他根目录以便将服务器限制到特定目录。可以使用此功能来保护不受保护的服务器。

DHCP　动态主机配置协议。 Internet 推荐的标准协议，允许系统动态地将 IP 地址指定给网络中的单个计算机。

DNS　域名系统。网络中的计算机用来将标准 IP 地址 （如 198.93.93.10）与主机名（如 `www.iplanet.com`）相关联的系统。计算机通常从 DNS 服务器获取此翻译信息，或从其系统维护的表中查找该信息。

DNS 别名　DNS 服务器知道的主机名，指向不同的主机 - 确切地说，是 DNS CNAME 记录。计算机始终具有一个真实的名称，但可以有一个或多个别名。例如，一个别名 （如 `www.`*`yourdomain.domain`*）可能指向一台名为 `realthing` *`.yourdomain.domain`* 的真实的计算机 （服务器当前所在的计算机）。

expires 标头　由远程服务器指定的返回文档的过期时间。

FORTEZZA　美国政府机构用来管理敏感但未分类的信息的加密系统。

FTP　文件传输协议。一种 Internet 协议，用于将文件通过网络从一台计算机传输到另一台计算机。

GIF 图形交换格式。由 CompuServe 最早创建的一种跨平台的图像格式。 GIF 文件的大小通常比其他图形文件类型 （BMP 或 TIFF）小很多。 GIF 是最常用的交换格式之一。在 UNIX、 Microsoft Windows 和 Apple Macintosh 系统上都可以很容易地查看 GIF 图像。

HTML 超文本标记语言。万维网上的文档使用的格式化语言。 HTML 文件是带有格式化代码的纯文本文件，告知浏览器 （如 Netscape Navigator）如何显示文本、图形位置和表单项，以及如何显示指向其他页面的链接。

HTTP 超文本传输协议。用于在 HTTP 服务器与客户机之间交换信息的方法。

HTTP-NG 超文本传输协议的下一代。

HTTPD HTTP 守护程序或服务的缩写，是使用 HTTP 协议提供信息的程序。Sun ONE Web Server 通常被称为 HTTPD。

HTTPS HTTP 的安全版本，使用安全套接字层 (SSL) 来实现。

imagemap 使图像的各个区域处于活动状态的进程，从而使用户可以通过用鼠标单击图像的不同区域来进行浏览并获取信息。 Imagemap 还可以引用一个名为“imagemap”的 CGI 程序，该程序用来处理其他 HTTPD 实现中的 imagemap 功能。

inittab (UNIX) 一种 UNIX 文件，用于列出因各种原因而停止并需要重新启动的程序。该文件可确保程序连续运行。由于其位置的原因，该文件也被称为 `/etc/inittab`。该文件并非在所有 UNIX 系统上都可用。

IP 地址 Internet 协议地址。由点分隔的一组数字，指定计算机在 Internet 上的实际位置 （如 198.93.93.10）。

ISDN 集成服务数字网络。

ISINDEX 一种 HTML 标记，用于启用客户机中的搜索。文档可以使用网络浏览器的功能来接受搜索字符串并将其发送到服务器，以访问可搜索的索引而不必使用表单。为了使用 <ISINDEX>，必须创建一个查询处理程序。

ISMAP ISMAP 是 HTML 文档中使用的 IMG SRC 标记的扩展，用来告知服务器命名图像是一个 imagemap。

ISP Internet 服务提供者。提供 Internet 连接的组织。

Java 一种由 Sun Microsystems 创建的面向对象的编程语言，用来创建称为小应用程序的实时、交互式程序。

JavaScript 一种精简的、基于对象的脚本语言，用来开发客户机和服务器 Internet 应用程序。

JavaServer Pages 用于启用所有 JavaServer Pages (JSP) 元功能的扩展，包括实例化、初始化、破坏、从其他组件访问及配置管理。 JSP 是可重复使用的 Java 应用程序，运行在 Web 服务器而不是 Web 浏览器中。

Java Servlet 用于启用所有 Java Servlet 元功能的扩展，包括实例化、初始化、破坏、从其他组件访问及配置管理。 Java Servlet 是可重复使用的 Java 应用程序，运行在 Web 服务器而不是 Web 浏览器中。

last-modified 标头 在服务器的 HTTP 响应中返回的文档文件的上一次修改时间。

LDAP 数据库 存储了用于验证的用户和组列表的数据库。

magnus.conf 主 Web 服务器配置文件。该文件包含全局服务器配置信息 （如端口、安全性等）。它为用于在初始化过程中配置服务器的变量设置了值。企业服务器将读取该文件并在启动时执行这些变量设置。服务器只有在重新启动时才会再次读取该文件，因此每次对该文件进行更改后都必须重新启动服务器。

MD5 由 RSA Data Security 开发的一种消息摘要算法。MD5 可以用来生成短小的数据摘要，并且该摘要为唯一的概率很高。从算术角度讲，要想用它来生成一段可以生成相同消息摘要 Email 的数据几乎是不可能的。

MD5 签名 由 MD5 算法生成的消息摘要。

MIB 管理信息库。

MIME 多用途 Internet 邮件扩展。一种正在兴起的用于多媒体 Email 和消息传递的标准。

mime.types MIME （多用途 Internet 邮件扩展）类型配置文件。该文件将文件扩展名映射为 MIME 类型，以使服务器能够确定所请求的内容类型。例如，请求带有 `.html` 扩展名的资源表示客户机请求的是 HTML 文件，而请求带有 `.gif` 扩展名的资源则表示客户机请求的是 GIF 格式图像文件。

modutil 为外部加密或硬件加速器设备安装 PKCS#11 模块所需的软件实用程序。

MTA 消息传输代理。要在服务器上使用代理服务，必须定义服务器的 MTA 主机。

NIS (UNIX) 网络信息服务。 UNIX 计算机为在整个计算机网络中收集、整理和共享有关计算机、用户、文件系统和网络参数的特定信息而使用的程序及数据文件系统。

NNTP 新闻组网络新闻传输协议。要在服务器上使用代理服务，必须定义新闻服务器主机。

NSAPI 请参见 “服务器插件 API”。

obj.conf 服务器的对象配置文件。该文件包含附加初始化信息、服务器的自定义设置以及服务器用来处理客户机 （如浏览器）请求的指令。 Sun ONE Web Server 每次处理客户机请求时都要读取该文件。

pk12util 从内部计算机导出证书和密钥数据库并将它们导入外部 PKCS#11 模块所需的软件实用程序。

rc.2.d (UNIX) UNIX 计算机中对计算机启动时运行的程序进行说明的文件。由于其位置的原因，该文件也被称为 `/etc/rc.2.d`。

RAM 随机访问内存。计算机中基于半导体的物理内存。

RFC 征求意见文件。通常是指提交给 Internet 社区的过程或标准文档。人们可以在某些技术被接受为标准之前发送有关这些技术的意见。

root 用户 (UNIX) UNIX 计算机中具有最大权限的用户。root 用户对计算机中的所有文件具有完全访问权限。

SOCKS 用于在防火墙内部和外部之间建立连接的防火墙软件；如果不使用它而直接进行连接，会被防火墙软件或硬件 （如路由器配置）禁止。

SSL 安全套接字层。一种用于在双方 （客户机和服务器）之间建立安全连接的软件库，用来实现 HTTPS （HTTP 的安全版本）。

SSL 验证 使用安全证书来确认用户的身份，即通过使用客户机证书中的信息做为身份证明，或验证在 LDAP 目录中发布的客户机证书。

strftime 用于将日期和时间转换为字符串的函数。服务器在附加尾部内容时会使用此函数。 `strftime` 具有一种特殊的日期和时间格式语言，可供服务器在尾部说明文件的上一次修改日期。

Sun ONE Web Server 管理控制台 以前称为 Netscape 控制台，是一个 Java 应用程序，为服务器管理员提供了图形界面，用于从企业网络内的任一中心位置对所有 Sun ONE 服务器进行管理。通过安装的任何 Sun ONE Web Server 管理控制台实例，您都可以查看并访问您有权访问的企业网络上的所有 Sun ONE 服务器。

Sym 链接 (UNIX) 符号链接 (symbolic link) 的缩写，是 UNIX 操作系统使用的一种重定向类型。可以使用符号链接创建一个从文件系统的一部分到该文件系统另一部分的现有文件或目录的指针。

TCP/IP 传输控制协议 /Internet 协议。 Internet 和企业 （公司）网络的主要网络协议。

telnet 用于使网络中的两台计算机互相连接并支持远程登录终端仿真的协议。

TLS 安全套接字层。一种用于在双方 （客户机和服务器）之间建立安全连接的软件库，用来实现 HTTPS （HTTP 的安全版本）。

top (UNIX) 某些 UNIX 系统上用于显示系统资源当前使用状况的程序。

uid (UNIX) 与 UNIX 系统上的每个用户相关联的唯一编号。

URI 统一资源标识符。一种文件标识符，通过使用缩写的 URL 提供了额外一层安全性。一个 URL 映射代替了 URL 的第一部分，从而对用户隐藏了文件的完整物理路径名。请参见 URL 映射。

URL 统一资源定位器。服务器和客户机用来请求文档的寻址系统。 URL 通常称为位置。 URL 的格式为 *protocol://machine:port/document*。

例如， `http://www.iplanet.com/index.html` 就是一个 URL。

URL 数据库修复 对因软件故障、系统崩溃、磁盘故障或整个文件系统而损坏的 URL 数据库进行修复及更新的过程。

URL 映射 将文档目录的物理路径名映射到用户定义的别名的过程，这样，该目录中的文件只需引用目录的别名而不是文件的完整物理路径名。从而，可以将某个文件标识为 `/myDocs/index.html` 而不是 `usr/iplanet/servers/docs/index.html`。用户不必知道服务器文件的物理位置，这为服务器提供了额外的安全性。

Web 应用程序 Servlet、 JavaServer Pages、 HTML 文档以及可能包含图像文件、压缩的归档文件及其他数据的其他 Web 资源的集合。 Web 应用程序可以打包至一个归档文件 （WAR 文件）中，或存在于打开的目录结构中。

Web 应用程序归档文件 (WAR) 包含完整的压缩格式的 Web 应用程序的归档文件。 Sun ONE Web Server 无法访问 WAR 文件中的应用程序。必须先解压缩 Web 应用程序 （使用 `wdeploy` 实用程序进行部署），然后 Sun ONE Web Server 才能够为其提供服务。

Windows CGI (Windows) 用基于 Windows 的编程语言 （如 Visual Basic）编写的 CGI 程序。

超级用户 (UNIX) UNIX 计算机中具有最大权限的用户 （也称为根用户）。超级用户对计算机中的所有文件具有完全访问权限。

超时　一段指定的时间，超过该时间后，服务器将放弃完成某个显示为挂起的服务例程。

重定向　一种系统，用于将访问特定 URL 的客户机发送到相同或不同服务器上的某个不同位置。如果资源被移动，并且希望客户机透明地使用新位置，该系统会很有用。当没有使用结尾斜杠来访问目录时，该系统还可用来维护相对链接的完整性。

代理　在网络设备（如路由器、主机或 X 终端）中运行网络管理软件的软件。请参见智能代理。

顶层域权威　主机名分类中的最高类别，通常表示域的组织类型（例如，`.com` 为公司，`.edu` 为教育机构）或该域所属的国家（例如，`.us` 为美国，`.jp` 为日本，`.au` 为澳大利亚，`.fi` 为芬兰）。

防火墙　一种网络配置，通常既是指硬件也是指软件，用于保护组织内部的网络计算机不被外部访问。防火墙一般用来保护信息（如实际建筑物或组织办公场所内的网络 Email 及数据文件）。

访问控制列表 (ACL)　ACE 的集合。 ACL 是一种用于定义哪些用户有权访问您的服务器的机制。您可以定义专门针对某特定文件或目录的 ACL 规则，允许或拒绝一个或多个用户和组的访问。

访问控制条目 (ACE)　Web 服务器用来评估传入访问请求的分层结构规则体系。

放弃词　请参见禁用词。

服务器插件 API　一种扩展，允许扩展和 / 或自定义 Sun ONE 服务器的核心功能，并且为在 HTTP 服务器和后端应用程序之间建立接口提供了一种可伸缩的有效机制。也称为 NSAPI。

服务器根目录　服务器计算机上的目录，专门用于保存服务器程序、配置、维护和信息文件。

服务器守护程序　一种进程，当其运行时将侦听并接受客户的请求。

服务质量　为服务器实例、虚拟服务器类或虚拟服务器设置的性能限制。

高速缓存　存储在本地的原始数据的副本。高速缓存的数据被请求时，不必再从远程服务器进行检索。

公共密钥　在公共密钥加密中使用的加密密钥。

公共信息目录 (UNIX) 不在文档根目录下而在某个 UNIX 用户的主目录下的目录，或由用户控制的目录。

集合 包含有关文档的信息（如字列表和文件特性）的数据库。搜索功能使用集合来检索与指定的搜索条件相匹配的文档。

加密 转换信息的过程，使得只有预期的接收者能够解密和读取信息。

加密算法 加密算法是一种用来加密或解密的加密算法（一种数学函数）。

禁用词 所标识出的搜索功能不对其进行搜索的词。通常包括 the、a、an、and 这样的词。也称为放弃词。

客户机 用于请求或查看万维网资料的软件（如 Netscape Navigator）。也称为浏览器程序。

客户机验证 客户机验证。

口令文件 (UNIX) UNIX 计算机上用于存储 UNIX 用户登录名、密码和用户 ID 编号的文件。由于其位置的原因，该文件也被称为 `/etc/passwd`。

灵活的日志格式 服务器用来将信息输入到访问日志中的格式。

浏览器 请参见“客户机”。

密文 通过加密隐藏的信息，只有预期的接收者可以解密。

群集 添加到“主” Administration Server 并由“主” Administration Server 控制的一组远程“从属” Administration Server。群集中所有服务器的平台必须相同，并且必须具有相同的用户 ID 和密码。

认证机构 (CA) 颁发用于加密事务的数字文件的内部或第三方组织。

软重新启动 一种重新启动服务器的方法，使服务器可以在内部重新启动，即重新读取其配置文件。软重新启动将 HUP 信号（1 号信号）发送给进程。进程本身不会像在硬重新启动中那样终止。

守护程序 (UNIX) 负责特定系统任务的后台进程。

损坏的密钥列表 (CKL) 具有损坏的密钥的用户的密钥信息列表。此列表也由 CA 提供。

通用日志文件格式　服务器用来将信息输入到访问日志中的格式。在所有主要服务器（包括 Sun ONE Web Server）中，格式都是相同的。

外部网　公司内部网向 Internet 的扩展，从而使客户、供应商和远程工作人员能够访问该数据。

网络管理站 (NMS)　可供用户远程管理网络的计算机。被管理的设备可以是运行 SNMP 的任何设备（如主机、路由器和 Sun ONE 服务器）。 NMS 通常是安装有一个或多个网络管理应用程序的功能强大的工作站。

文档根目录　服务器计算机上的目录，包含要提供给访问该服务器的用户的文件、图像和数据。

文件扩展名　文件名的最后部分，通常定义文件的类型。例如，在 `index.html` 文件名中，文件扩展名为 `html`。

文件类型　给定文件的格式。例如，图形文件与文本文件具有不同的文件类型。文件类型通常由文件扩展名（`.gif` 或 `.html`）标识。

协议　描述网络上的设备如何交换信息的一组规则。

虚拟服务器类　共享 obj.conf 文件中相同的基本配置信息的虚拟服务器集合。

虚拟服务器　虚拟服务器是通过安装一个服务器即可设置多个域名、 IP 地址及服务器监视功能的一种方法。

验证　允许客户机向服务器验证他们的身份。基本验证或缺省验证要求用户输入用户名和密码来访问 Web 服务器或 Web 站点，并且要求在 LDAP 数据库中保存有用户和组列表。请参见摘要验证和 SSL 验证。

允许访问整个服务器或服务器上的特定文件及目录。可以利用条件（包括主机名和 IP 地址）来限制验证。

硬重新启动　进程或服务被终止然后重新启动。请参见软重新启动。

摘要验证。　允许用户进行验证而不必明文发送用户名和密码。浏览器使用 MD5 算法创建摘要值。服务器使用摘要验证插件来比较客户机提供的摘要值。

侦听套接字　端口号与 IP 地址的组合。服务器与客户机之间的连接在侦听套接字上进行。

证书　由通信双方信任的第三方颁发的不得转让、伪造的数字文件。

证书撤回列表 (CRL)　由 CA 提供的所有被撤回证书的 CA 列表。

智能代理　服务器中的一个对象，代表用户执行各种请求（如 HTTP、 NNTP、 SMTP 和 FTP 请求）。在某种意义上，智能代理充当服务器的客户机，提出请求让服务器来完成。

主机名　以 *machine.domain.dom* 形式表示的计算机的名称，它将被翻译成 IP 地址。例如， 是位于域 `com` 和子域 `sun` 中的 `www` 计算机。

主文档目录　请参见 “文档根目录”。

主页　服务器上存在的文档，作为服务器内容的目录或入口点。服务器的配置文件中定义了该文档的地址。

专用密钥　在公共密钥加密中使用的解密密钥。

资源　服务器可以访问并将其发送给提出请求的客户机的任何文档 (URL)、目录或程序。

索引

A

B

C

D

F

G

H

J

K

L

M

N

P

Q

R

S

T

W

X

Y

Z

Z