安装和调整指南

Sun™ ONE Directory Server

版本5.2

816-6848-10
2003 年 6 月

目录

关于本指南

Sun™ ONE Directory Server 5.2 是功能强大且具伸缩性的分布式目录服务器，该服务器基于符合工业标准的轻型目录访问协议 (LDAP)。Sun ONE Directory Server 软件是 Sun Open Net Environment (Sun ONE) 的一部分，后者是 Sun 推出的一种基于标准的软件界面、体系结构、平台以及专业技术，旨在按需建立和部署服务。

Sun ONE Directory Server 是建立集中化分布式数据库的基础，您可在内部网中使用该数据库，也可将其用于外联网中以便与商业合作伙伴共享数据资源，或运行在公用 Internet 之上与客户进行交流与沟通。

本指南的用途

本指南演示了如何安装在生产环境中使用的 Directory Server。为获得高性能，在生产环境中准备 Directory Server 经常会涉及大量的配置和调整工作。

如果安装 Directory Server 的目的只是为了评估，而不是在生产环境中使用，则可以选择只读第 1 章 “安装 Sun ONE Directory Server”。

前提条件

安装在生产环境中使用的 Directory Server 之前，应确保部署目标清楚明确。详细信息，请参阅 *Sun ONE Directory Server 部署指南*。

印刷约定

本节说明本书中使用的印刷约定。

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

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

命名菜单或子菜单中的项时，使用大于符号 (>) 作为分隔符。例如，对象 > 新建 > 用户是指应选择 “对象”菜单的 “新建”子菜单中的 “用户”项。

注意 “注意”、“警告”以及 “提示”突出显示了重要的条件或限制。确保在继续之前阅读此信息。

默认路径和文件名

Sun ONE Directory Server 产品文档中的所有路径和文件名示例均采用以下两种形式之一：

- *ServerRoot*/...- *ServerRoot* 是 Sun ONE Directory Server 产品的位置。此路径包含 Directory Server、Sun ONE Administration Server 和命令行工具的共享二进制文件。

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

- *ServerRoot*/slapd-*serverID*/...- *serverID* 是在安装或配置期间定义的 Directory Server 实例的名称。此路径包含给定实例所特有的数据库和配置文件。

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

表 1 默认的 *ServerRoot* 路径

产品版本	***ServerRoot* 路径**
Solaris 软件包[1]	`/var/mps/serverroot` - 配置后，该目录包含到下列位置的链接： • `/etc/ds/v5.2`（静态配置文件） • `/usr/admserv/mps/admin`（Sun ONE Administration Server 二进制） • `/usr/admserv/mps/console`（Server Console 二进制） • `/usr/ds/v5.2`（Directory Server 二进制）
Solaris 和其他 UNIX 系统上的压缩存档安装	`/var/Sun/mps`
Windows 系统上的 Zip 安装	`C:\Program Files\Sun\MPS`

1. 如果正使用 Solaris 操作环境，并且不明确安装的是 Sun ONE Directory Server 软件的哪一个版本，则请使用 `pkginfo` 命令检查是否存在诸如 `SUNWdsvu` 之类的关键软件包。例如：`pkginfo | grep SUNWdsvu`。

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

表 2 默认示例 `dirserv` 实例位置

产品版本	**实例位置**
Solaris 软件包	`/var/mps/serverroot/slapd-dirserv`
Solaris 和其他 UNIX 系统上的压缩存档安装	`/usr/Sun/mps/slapd-dirserv`
Windows 系统上的 Zip 安装	`C:\Program Files\Sun\MPS\slapd-dirserv`

下载 Directory Server 工具

某些受支持的平台可提供本机工具，用于访问 Directory Server。更多用于测试和维护 LDAP 目录服务器的工具，请下载 Sun ONE Directory Server Resource Kit (DSRK)。此软件可从以下位置获得：

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

有关 DSRK 工具的安装指导和参考文档可在 *Sun ONE Directory Server Resource Kit 工具参考* 中获得。

要开发目录客户机应用程序，还可以从同一位置下载 iPlanet Directory SDK for C 和 iPlanet Directory SDK for Java。

此外， Java 命名和目录接口 (JNDI) 技术支持使用 LDAP 和 DSML v2 从 Java 应用程序访问 Directory Server。有关 JNDI 的信息可从以下位置获得：

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

JNDI 教程包含如何使用 JNDI 的详细说明和示例。下载位置是：

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

建议的读物

Sun ONE Directory Server 产品文档包括以 HTML 和 PDF 格式传送的下列文档：

- *Sun ONE Directory Server 入门指南* - 提供了 Directory Server5.2 中许多主要功能的概述。
- *Sun ONE Directory Server 部署指南* - 解释了如何规划目录拓扑、数据结构、安全性和监视，并对部署示例进行了讨论。
- *Sun ONE Directory Server 安装和调整指南* - 包括了安装和升级过程，并提供了对 Directory Server 进行性能优化的提示。
- *Sun ONE Directory Server 管理指南* - 提供了如何通过控制台以及命令行，来管理目录内容并配置 Directory Server 的每项功能的过程。
- *Sun ONE Directory Server 参考手册* - 详细描述了 Directory Server 的配置参数、命令、文件、错误消息和架构。
- *Sun ONE Directory Server Plug-In API 编程指南* - 演示了如何开发 Directory Server 插件。

- *Sun ONE Directory Server Plug-In API 参考* - 详细描述了 Directory Server 插件 API 的数据结构和功能。
- *Sun ONE Server Console Server 管理指南* - 讨论了如何使用 Sun ONE Administration Server 和基于 Java 的控制台来管理服务器。
- *Sun ONE Directory Server Resource Kit 工具参考* - 包括了 Sun ONE Directory Server Resource Kit 的安装和功能，其中包含许多有用的工具。

可以在下列网站找到其他有用的信息：

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

第 1 部分

安装

第 1 章

安装 Sun ONE Directory Server

本章旨在指导您完成 Sun ONE Directory Server 软件的首次安装和卸载。它包含以下几节内容：

- 开始之前
- 安装
- 卸载
- 疑难解答

开始之前

在生产环境中安装使用 Directory Server 前，请确保最低限度地装备和配置了系统以运行目录服务。至少应熟悉 *Sun ONE Directory Server 部署指南* 中讨论的概念。

注意 要实现最佳性能，也可遵循本指南提供的调整和配置说明进行操作。

规划目录部署

请参阅操作系统文档以了解与基础平台相关的各种任务，并执行以下步骤。

1. 规划目录服务的部署。

   有关说明，请参阅 *Sun ONE Directory Server 部署指南*。

2. 如果部署涉及到集中式管理多目录安装的服务器配置、用户和组，则要确定配置和用户目录的位置。

   配置目录或 Configuration Directory Server (CDS) 存储有关 Directory Server 本身的配置方式的信息。通常，先安装该目录，随后的每个服务器都要向它注册。一个配置目录可以为所有服务器提供集中式管理。

   用户目录存储访问目录服务的用户和组的条目。用户目录在网域中一般具有唯一性，其他服务器通过访问它获取用户和组信息。一个用户目录可以提供对用户和组的集中式管理。

   对于小型部署，可在同一目录实例上安装配置、用户及其他目录。对于大型部署，可考虑在不同的服务器上放置配置和用户目录。

   有关配置、用户和分组数据的适当位置的详细信息，请参阅 *Sun ONE Server Console Server 管理指南*。

3. 确保主机系统在受支持的体系结构上运行受支持的平台，如表 1-1 中所概述。

表 1-1 受支持的平台和体系结构

平台	体系结构
Sun Solaris™ 操作环境 9	SPARC 处理器， 32 和 64 位模式
	受支持的 x86 平台
Sun Solaris 操作环境 8	UltraSPARC 处理器， 32 和 64 位模式
Sun Linux 5.0	Sun LX50 服务器
Hewlett Packard HP-UX 11i	PA-RISC 2.0 处理器， 32 和 64 位模式
IBM AIX 5.1	PowerPC 处理器
Microsoft Windows 2000 Server, SP 3	Pentium II 或更新的 IA-32 处理器
Microsoft Windows 2000 Advanced Server, SP 3	
Red Hat Linux 7.2	Pentium II 或更新的 IA-32 处理器

4. 确保主机系统至少满足最低限度的磁盘空间和内存要求，如表 4-1 （第 73 页）中所简述。

5. 限制物理访问主机系统。

6. 确保主机系统使用静态的 IP 地址。

7. 如果 Directory Server 实例本身不提供网络命名服务，或者如果部署涉及远程管理 Directory Server，请确保正确配置了主机的命名服务和域名。

获取 Directory Server 软件

执行完 “规划目录部署”（第 17 页）中概述的过程后，请完成以下步骤。

1. 请确保安装了解压缩公用程序以打开软件。
2. 下载该软件。在此次写入时，可从以下站点下载：

   `http://wwws.sun.com/software/download/`
3. 请将软件解包到另一目录下，而不是准备安装 Directory Server 的目录。

安装

遵循的 Directory Server 安装步骤取决于特定的部署要求。有了这些特定的部署要求，请根据相应节的内容进行操作：

- 确定安装内容
- 确定安装方式
- 准备安装信息
- 在 Solaris 系统上安装
- 在其他 UNIX 系统上安装
- 在 Windows 系统上安装

确定安装内容

在确定要安装的软件之前，可对若干备用方案进行评估。请考虑这些问题：

- 对于高容量部署，是否需要大缓存容量？

  如果需要，请考虑使用 Directory Server 作为运行 64 位进程的平台，并安装 64 位版本。

  如果 Directory Server 部署相对较小 （数据库大小小于 500 MB），请考虑仅安装 32 位支持，即使在支持 64 位版本的平台上也是如此。

- 是否计划通过图形用户界面管理 Directory Server？

  如果是，请安装 Sun ONE Server Console 和 Sun ONE Administration Server。

  如果计划仅从命令行界面管理 Directory Server，则可以选择不安装 Console 和 Administration Server。

  如果计划从图形用户界面使用用于远程管理的系统，则可以选择只安装 Console 和 Administration Server。

- 是否计划在 Sun Cluster 软件上部署 Directory Server？

  如果是，请参阅附录 C “安装 Sun Cluster HA for Directory Server”以获取有关说明。

确定安装方式

在确定最适合您部署的封装以及是否计划进行交互式安装之前，也可对若干备用方案进行评估。请考虑这些问题：

- 是否希望与 Solaris 系统管理进程更紧密地集成？是否希望在同一系统上的多个 Sun ONE 服务器之间共享组件？

  如果希望共享，请考虑使用 Solaris 软件包进行安装。

- 是否希望无需先成为超级用户就可以进行安装？是否希望在同一系统上安装多组独立的 Directory Server 二进制？

  如果希望安装，请考虑从压缩存档文件进行安装，即使是在 Solaris 系统上安装。

- 是否希望快速安装以评估 Directory Server？这是您第一次安装该版本的 Directory Server 吗？

  如果是，请考虑进行交互式安装。

- 是否希望进行脚本安装？是否希望使用相同配置安装多个系统？

  如果是，请考虑使用无提示安装过程。

准备安装信息

提前准备信息可有助于您快速完成安装过程。在执行交互式安装前，请考虑创建工作表以包含安装信息，如表 1-2 中的典型安装所概述。

表 1-2 典型安装期间所需的基本信息

说明	示例	您的回答 ...
管理域	`example.com`	
Administration Server 端口号	`5201`	
目录管理员 ID	`admin`	
目录管理员口令	`$3kReT4wD`	
目录管理员 DN[1]（目录的超级用户）	`cn=Directory Manager`	
目录管理员口令（至少 8 个字符）	`#$8Yk$-%&`	
Directory Server 端口号（1 至 65535，包括 1 和 65535）[2]	`389`（默认 LDAP） `636`（默认 LDAP/SSL）	
完全限定的主机标识名称	`dirserv.example.com`	

（可选）使用现有配置目录时的配置目录主机、端口、绑定 ID 和口令	`config.example.com`
	`389`
	`admin`
	`$3kReT4wD`	

（可选）使用现有用户目录时的用户目录主机、端口、绑定 DN、口令和后缀	`usergroup.example.com`
	`389`
	`cn=Directory Manager`
	`#$8Yk$-%&`
	`dc=example, dc=com`	

服务器 ID（不允许使用句点或空格）	`dirserv`	
服务器后缀（至少一个用于容纳目录内容）	`dc=example,dc=com`	

ServerRoot（软件安装目录；详细信息，请参阅“默认路径和文件名”（第 10 页）
不要安装在现有的较早版本上。
请不要在与 Directory Server 相同的 *ServerRoot* 中安装 Sun ONE Web Server。
（UNIX 平台）不允许有空格。
	`/var/mps/serverroot`
	`/var/Sun/mps`
	`C:\Program Files\Sun\MPS`	

（UNIX 平台）服务器组 ID[3] 使用名称，而不是组 ID 号。	`noaccess`	
（UNIX 平台）服务器用户 ID 使用名称，而不是用户 ID 号。	`diruser`	
(Windows) `Administrator` 口令 （可选，其他平台）超级用户口令	请与您的系统管理员联系。	

1. 所有 DN 必须以 UTF-8 编码输入；请参阅 RFC 2253。不支持较旧的编码 （例如， ISO-8859-1）。
2. Internet 号码指派机构分配小于 1024 的端口号。请作为超级用户进行安装以使用小于 1024 的端口。
3. 如安装过程中所述，创建相应的 UNIX 用户和组。

为目录管理员和目录管理员帐户提供信息时，取消了使用 Directory Server 访问控制机制管理目录管理员访问权限的限制。同时，还取消了 Directory Server 访问控制不应用于目录管理员帐户的限制。

无提示安装配置文件包含类似信息。

在 Solaris 系统上安装

Directory Server 软件的安装方式取决于决定使用的封装，以及是否希望与安装程序进行交互。根据相应章节中的说明进行操作：

- 从 Solaris 软件包进行安装的准备工作
- 使用 Solaris 软件包执行交互式安装
- 使用 Solaris 软件包执行无提示安装。

- 从压缩存档准备安装
- 从压缩存档文件执行交互式安装
- 从压缩存档文件执行无提示安装

- 正在完成安装过程

在 Sun Cluster 系统中安装 Directory Server 时，请按照附录 C “安装 Sun Cluster HA for Directory Server”中的说明进行操作。

从 Solaris 软件包进行安装的准备工作

1. （可选）创建 Directory Server 的用户和组帐户。

Directory Server 以安装期间指定的用户和组身份运行。设置权限，以防止对该系统上的目录和其他资源进行未授权访问。详细信息，请参阅 “（UNIX 平台）用户和组”（第 91 页）。

2. （可选）允许使用 xhost(1) 命令访问显示。

   在适当设置 DISPLAY 环境变量并以具备访问显示权限的用户身份执行安装时，默认情况下，安装程序会显示图形用户界面。

   如果安装程序不能显示图形用户界面，则会以命令行的模式开始安装。

3. 在使用区域设置并非为美国英语的平台上进行安装前，请将 LANG 环境变量设置为 C。

4. 请确保安装了表 1-3 中列出的所需软件包，另外，所有的 Solaris 软件包在默认情况下使用基本的系统安装。

表 1-3 Solaris 软件包前提条件

软件包	说明	32 位 Directory Server 所需	64 位 Directory Server 所需
SUNWj3rt[1]	J2SDK 1.4 运行时环境	是	是
SUNWzlib	Zip 压缩库	是	是
SUNWzlibx	Zip 压缩库 （64 位）)	否	是

1. 强烈建议您使用 Java Runtime Environment 版本 1.4.1 或更新的版本。

使用 Solaris 软件包执行交互式安装

完成以下过程中的步骤。

安装 Solaris 软件包

可以使用 pkgadd(1M) 公用程序安装 Solaris 软件包。例如，在执行升级时，可使用 pkginfo(1) 确定已安装了哪些软件包。在多个主机上安装软件包时，可使用 admin(4) 中说明的默认安装文件定义默认的安装操作。在任何情况下，所有软件包必须共享相同的 *basedir*。

有关处理软件包的更多详细信息，请参阅 Solaris 操作环境系统管理文档。

1. 请考虑表 1-4 或表 1-5 中列出的软件包完整列表。

表 1-4 提供的 Solaris 软件包 （SPARC 平台）

软件包	说明
SUNWasha	用于 Sun Cluster 的 Sun ONE Administration Server 组件
SUNWasvc	Sun ONE 管理控制台
SUNWasvcp	Sun ONE Administration Server Console 插件

表 1-4 提供的 Solaris 软件包 （SPARC 平台）（续）

软件包	说明
SUNWasvr	Sun ONE Administration Server (Root)
SUNWasvu	Sun ONE Administration Server (Usr)
SUNWdsha	用于 Sun Cluster 的 Sun ONE Directory Server 组件
SUNWdsvcp	Sun ONE Directory Server Console 插件
SUNWdsvh	Sun ONE Directory Server 堆分配器 （仅 Solaris 8 系统）
SUNWdsvhx	Sun ONE Directory Server 堆分配器 （仅 64 位， Solaris 8 系统）
SUNWdsvpl	Sun ONE Directory Server PerLDAP 模块
SUNWdsvr	Sun ONE Directory Server (Root)
SUNWdsvu	Sun ONE Directory Server (Usr)
SUNWdsvx	Sun ONE Directory Server （64 位）
SUNWicu	Unicode 用户文件的国际组件
SUNWicux	Unicode 用户文件的国际组件 （64 位）
SUNWjss	用于 Java 的网络安全服务 (JSS)
SUNWldk	LDAP C SDK
SUNWldkx	LDAP C SDK （64 位）
SUNWpr	Netscape 便携式运行时接口
SUNWprx	Netscape 便携式运行时接口 （64 位）
SUNWsasl	简单认证和安全层
SUNWsaslx	简单认证和安全层 （64 位）
SUNWtls	网络安全服务
SUNWtlsx	网络安全服务 （64 位）

表 1-5 提供的 Solaris 软件包 （x86 平台）

软件包	说明
SUNWasvc	Sun ONE Administration Console
SUNWasvcp	Sun ONE Administration Server Console 插件
SUNWasvr	Sun ONE Administration Server (Root)
SUNWasvu	Sun ONE Administration Server (Usr)

表 1-5 提供的 Solaris 软件包 （x86 平台）（续）

软件包	说明
SUNWdsvcp	Sun ONE Directory Server Console 插件
SUNWdsvpl	Sun ONE Directory Server PerLDAP 模块
SUNWdsvr	Sun ONE Directory Server (Root)
SUNWdsvu	Sun ONE Directory Server (Usr)
SUNWicu	Unicode 用户文件的国际组件
SUNWjss	用于 Java 的网络安全服务 (JSS)
SUNWldk	LDAP C SDK
SUNWpr	Netscape 便携式运行时接口
SUNWsasl	简单认证和安全层
SUNWtls	网络安全服务

建议您安装所有软件包时使用可写的 *basedir*，如 /var。重新分配软件包时，请注意 SUNWasvr 和 SUNWdsvr 将启动和关机脚本放置在 *basedir*/etc 中。

2. 使用表 1-6 中的提示来确定安装哪些软件包。

表 1-6 安装哪些软件包

配置	要安装的软件包列表[1]
32 位 Directory Server， Administration Server 和 Console	SUNWascv SUNWasvcp SUNWasvr SUNWasvu SUNWdsvcp SUNWdsvh SUNWdsvpl SUNWdsvr SUNWdsvu SUNWicu SUNWjss SUNWldk SUNWpr SUNWsasl SUNWtls
仅 32 位 Directory Server （无 Console）	SUNWasvu SUNWdsvh SUNWdsvpl SUNWdsvr SUNWdsvu SUNWicu SUNWjss SUNWldk SUNWpr SSUNWsasl SUNWtls
64 位 Directory Server， 32 位 Administration Server 和 Console	SUNWascv SUNWasvcp SUNWasvr SUNWasvu SUNWdsvcp SUNWdsvh SUNWdsvhx SUNWdsvpl SUNWdsvr SUNWdsvu SUNWdsvx SUNWicu SUNWicux SUNWjss SUNWldk SUNWldkx SUNWpr SUNWprx SUNWsasl SUNWsaslx SUNWtls SUNWtlsx

表 1-6 安装哪些软件包 （续）

配置	要安装的软件包列表[1]
仅 64 位 Directory Server （无 Console）	SUNWasvu,SUNWdsvh SUNWdsvhx SUNWdsvpl SUNWdsvr SUNWdsvu SUNWdsvx SUNWicu SUNWicux SUNWjss SUNWldk SUNWldkx SUNWpr SUNWprx SUNWsasl SUNWsaslx SUNWtls SUNWtlsx
Cluster 节点	添加 SUNWasha， SUNWdsha
Sun ONE Server Console 和 仅 Administration Server （无 Directory Server，只有远程管理）	SUNWasvc SUNWasvcp SUNWasvr SUNWasvu SUNWdsvcp SUNWjss SUNWldk SUNWpr SUNWsasl SUNWtls

1. Solaris 8 系统上的 Directory Server 所需的软件包 SUNWdsvh （32 位）和 SUNWdsvhx （64 位）。

3. 验证要安装却没有安装的软件包。

   请不要安装已在系统上安装的软件包。

4. 成为超级用户。

5. 使用 pkgadd(1M) 公用程序将产品软件包传输到系统。

   软件包 SUNWicu 和 SUNWicux 取决于安装 Directory Server 的系统上的 Solaris 版本。

   此外，有关安装和增补程序组件软件包 SUNWpr、 SUNWprx、 SUNWsasl、 SUNWsaslx、 SUNWtls 和 SUNWtlsx 的详细信息，请参阅以下小节，“安装所需的增补程序”。

6. 退出 pkgadd 后，请验证安装了所有所需的产品软件包。

在从 IPLT* Solaris 软件包安装的 iPlanet Directory Server 5.1 升级时， 5.1 /usr/sbin/directoryserver 命令会重新命名为 /usr/sbin/directoryserver.51bak。可使用重命名命令管理 5.1 版本。

安装所需的增补程序

Directory Server 依赖于软件包 SUNWpr、 SUNWprx、 SUNWsasl、 SUNWsaslx、 SUNWtls 和 SUNWtlsx，它们已经更新为包括最新的修补程序和推荐的系统增补程序。

1. 与 -x 选项一起使用 pkginfo(1)，以确定在您的系统上安装其中哪些软件包。尤其要验证您的系统上是否已安装了适当的软件包版本，如表 1-7 所示。

表 1-7 组件的适当的版本和增补程序

系统版本和体系结构	SUNWpr(x) 版本	SUNWsasl(x) 版本	SUNWtls(x) 版本	增补程序
Solaris 9 （SPARC 平台）	4.1.2 或更新的版本	2.01 或更新的版本	3.3.2 或更新的版本	114049, 115342
Solaris 9 （x86 平台）	4.1.3 或更新的版本	2.01 或更新的版本	3.3.3 或更新的版本	114050, 115343
Solaris 8 （SPARC 平台）	4.1.2 或更新的版本	2.01 或更新的版本	3.3.2 或更新的版本	114045, 115328

2. 与 `-p` 选项一起使用 `showrev`(1M)，以确定表 1-7 中列出的适当的增补程序是否已应用于您的平台。
3. 使用表 1-8 中的提示以确定是否需要增补程序组件。

表 1-8 是否需要增补程序组件

在您的系统上 ...	执行该操作 ...
软件包已安装，且增补程序已应用。	继续执行步骤 4。
软件包已安装，但增补程序尚未应用。	对 Directory Server 提供的平台应用适当的增补程序。
软件包尚未安装。	安装随 Directory Server 提供的软件包和适当的增补程序。

4. 以超级用户身份运行下列命令：

   ```
   root# /usr/sbin/directoryserver idsktune -q > idsktune.out
   ```

   `idsktune` 建议对系统的更改。子命令本身不会对系统进行更改。
5. 至少修复所有指明的 `ERROR` 状况。

   如果不修复 `ERROR` 状况，安装可能会失败。注意 `idsktune` 子命令将报告丢失所有增补程序，包括发行时推荐的增补程序和未在系统上安装的增补程序，甚至还包括未在系统上安装的软件包增补程序。

   可以从 `http://sunsolve.sun.com/` 下载增补程序。

   详细信息，请参阅第 5 章 “调整操作系统”。

配置 Directory Server

1. 启动该配置程序。

   使用图形用户界面：

   ```
   root# /usr/sbin/directoryserver configure
   ```

   使用命令行界面：

   ```
   root# /usr/sbin/directoryserver configure -nodisplay
   ```

   出现第一个安装屏幕。

2. 使用 “准备安装信息”（第 20 页）时制作的工作表，按照每个屏幕上的指示操作。

配置 Administration Server

1. 启动该配置程序。

   使用图形用户界面：

   ```
   root# /usr/sbin/mpsadmserver configure
   ```

   使用命令行界面：

   ```
   root# /usr/sbin/mpsadmserver configure -nodisplay
   ```

   出现第一个安装屏幕。

2. 使用 “准备安装信息”（第 20 页）时制作的工作表，按照每个屏幕上的指示操作。

继续执行 “正在完成安装过程”（第 32 页）。

使用 Solaris 软件包执行无提示安装。

完成以下过程中的步骤。

安装 Solaris 软件包

请按照 “安装 Solaris 软件包”（第 23 页）中的说明进行操作。

安装所需的增补程序

请按照 “安装所需的增补程序”（第 26 页）中的说明进行操作。

创建规范文件

要执行完全无提示安装，您必须首先创建包含安装规范的两个文件，一个用于 Directory Server，另一个用于 Administration Server。有关 Directory Server 安装规范文件模板，请参阅 `/usr/ds/v5.2/setup/typical.ins`。有关 Administration Server，请参阅 `/usr/sadm/mps/admin/v5.2/setup/admin/typicalInstall.ins`。

注意 规范文件可能包含明文口令。使用适当的文件权限保护此类文件。

可通过手动编辑模板文件的副本或使用 Directory Server 和 Administration Server 配置程序执行交互式配置，创建无提示安装规范文件。

要为 Directory Server 和 Administration Server 交互式创建无提示安装规范文件，请按照以下步骤执行：

1. 使用 `-saveState` 选项执行 Directory Server 配置。

   ```
   root# /usr/sbin/directoryserver configure -saveState dirserv-file
   ```

   以创建规范文件 *dirserv-file*。

2. 使用 `-saveState` 选项执行 Administration Server 配置。

   ```
   root# /usr/sbin/mpsadmserver configure -saveState admserv-file
   ```

   以创建规范文件 *admserv-file*。

3. 使用它们在其他系统上安装之前，请调整规范文件 *dirserv-file* 和 *admserv-file*。

   一些无提示安装规范文件指令 （例如， `FullMachineName`）直接取决于基础主机系统，因此一般无法生成。

无提示安装规范文件包含对应于安装程序内部版本的校验和字符串。要重新使用该安装程序不同内部版本或发行的无提示安装规范文件，可更新各行中以 `[STATE_BEGIN` 和 `[STATE_DONE` 开头的校验和字符串。更新的校验和在 Directory Server 的 `/usr/ds/v5.2/setup/typical.ins` 和管理服务器的 `/usr/sadm/mps/admin/v5.2/setup/admin/typicalInstall.ins` 中。代码示例 1-1 显示了示例校验和。

代码示例 1-1 无提示安装校验和行

```
[STATE_BEGIN Sun ONE Directory Distribution a7cc64b2f71a0452899e1c3b853ecead72027b3b]
```

使用规范文件进行安装

要交互式配置 Directory Server 和 Administration Server，请按照以下步骤执行：

1. 验证对无提示安装规范文件所做的更改。
2. 在无提示模式下执行 Directory Server 配置。

   ```
   root# /usr/sbin/directoryserver configure -f dirserv-file
   ```

   此处的 *dirserv-file* 是指无提示安装配置文件。
3. 在无提示模式下执行 Administration Server 配置。

   ```
   root# /usr/sbin/mpsadmserver configure -f admserv-file
   ```

   此处的 *admserv-file* 是指无提示安装配置文件。

继续执行 “正在完成安装过程”（第 32 页）。

从压缩存档准备安装

1. 依照 “获取 Directory Server 软件”（第 19 页）中描述，从包含解包软件的目录中，运行 `idsktune` 公用程序。 `idsktune` 检查适当的增补程序，并验证系统调整到支持高目录服务性能。

   作为超级用户，请输入以下命令：

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

   请按照建议对系统执行手动更改。 `idsktune` 本身不会对系统进行更改。
2. 修复至少由 `idsktune` 指明的所有 `ERROR` 状况。如果不修复 `ERROR` 状况，安装可能会失败。注意 `idsktune` 将报告丢失所有增补程序，包括发行时推荐的增补程序和未在系统上安装的增补程序，甚至还包括未在系统上安装的软件包增补程序。

   可以从 `http://sunsolve.sun.com/` 下载增补程序。

   详细信息，请参阅第 5 章 “调整操作系统”。
3. （可选）创建 Directory Server 的用户和组帐户。

   Directory Server 以安装期间指定的用户和组身份运行。设置权限，以防止对该系统上的目录和其他资源进行未授权访问。详细信息，请参阅 “（UNIX 平台）用户和组”（第 91 页）。

4. （可选）在以另一用户身份执行交互式安装时，请使用 xhost(1) 命令以允许访问显示。

   在适当设置 DISPLAY 环境变量并以具备访问显示权限的用户身份执行安装时，默认情况下，安装程序会显示图形用户界面。

   如果安装程序不能显示图形用户界面，则会以命令行模式开始安装。

5. 在使用区域设置并非为美国英语的平台上进行安装前，请将 LANG 环境变量设置为 C。

从压缩存档文件执行交互式安装

1. 启动包含解包软件的目录中的安装程序。

   对于图形用户界面：

   ```
   root# ./setup
   ```

   对于命令行界面：

   ```
   root# ./setup -nodisplay
   ```

   出现第一个安装屏幕。

2. 使用 “准备安装信息”（第 20 页）时制作的工作表，按照每个屏幕上的指示操作。

注意 要安装 32 位 Directory Server，请确保清除名为 “选择组件”的向导屏幕中 Sun ONE Directory Suite > Sun ONE Directory Server （64 位支持）旁边的复选框。

不要将此版本安装在 Directory Server 早期版本所在的同一目录中。如果必须重新使用同一目录位置，请先卸载早期版本。详细信息，请参阅第 2 章 “从以前版本升级”。

从压缩存档文件执行无提示安装

完成以下过程中的步骤。

创建规范文件

要执行无提示安装，首先必须创建包含安装规范的文件。要获取无提示安装规范文件模板，请参阅解包软件的目录下的 setup_data/typical.ins。

注意 规范文件可能包含明文口令。使用适当的文件权限保护此类文件。

可通过手动编辑模板文件的副本或使用安装程序执行交互式配置，创建无提示安装规范文件。

1. 成为超级用户。
2. 启动包含 `-saveState` 选项的安装程序。

   root# ./setup -saveState filename

   以创建规范文件 *filename*。
3. 执行交互式安装。
4. 在使用规范文件 *filename* 以在其他系统上进行安装前，请对其进行调整。

   一些无提示安装规范文件指令 （例如， `FullMachineName`）直接取决于基础主机系统，因此一般无法生成。

无提示安装规范文件包含对应于安装程序内部版本的校验和字符串。要重新使用该安装程序不同内部版本或发行的无提示安装规范文件，可更新各行中以 `[STATE_BEGIN` 和 `[STATE_DONE` 开头的校验和字符串。更新的校验和位于 `typical.ins`。代码示例 1-1 （第 29 页）显示了示例校验和。

使用规范文件进行安装

1. 验证对安装规范文件所做的更改。
2. 在无提示模式下启动安装程序。

   `root# ./setup -noconsole -nodisplay -state` *filename*

   此处的 *filename* 是指无提示安装规范文件。

正在完成安装过程

1. 请确保 *ServerRoot*`/alias` 下面文件的访问权限已设置为阻止所有用户访问，*ServerRoot* 下安装的服务器除外。
2. （可选）如果从压缩存档文件进行安装，请添加支持以在系统重引导时启动 Directory Server。 Solaris 软件包版本中包括此支持。

   详细信息，请参阅 Solaris 系统管理文档。

3. （可选）启用核心文件生成。

   如果已经以超级用户的身份安装了 Directory Server，但却将用户和组 ID 设置为另一个帐户的用户和组 ID，则发生故障时， Directory Server 可能无法生成核心文件。强烈建议您为核心文件规划足够的空间，并允许 Directory Server 在故障期间生成核心文件。

   可以使用 `coreadm`(1M) 管理核心文件生成，允许 Directory Server 生成如下核心文件，例如：

   ```
   root# coreadm -e proc-setid
   ```

   详细信息，请参阅 “（UNIX 平台）核心文件”（第 81 页）。

4. （可选）许多用 Perl 编写的命令行脚本现在可以交互地读取绑定口令 （`-w -` 选项）。要启用此功能：

   a. 安装 `Term::ReadKey` Perl 模块，它与 CPAN 所在位置不同。

   b. 通过取消对相应行的注释，编辑各个 Perl 脚本以交互地读取绑定口令。

   所有其他 Perl 脚本功能在没有 `Term::ReadKey` 模块的情况下仍然可用。

现在， Directory Server 已最低限度地进行了配置和启动。

在其他 UNIX 系统上安装

根据相应章节中的说明进行操作：

- 准备安装
- 执行交互式安装
- 执行无提示安装
- 正在完成安装过程

准备安装

根据相应章节中的说明进行操作：

- 针对所有 UNIX 平台的说明
- 针对 AIX 系统的其他说明
- 针对 HP-UX 系统的其他说明

针对所有 UNIX 平台的说明

1. 运行 idsktune 公用程序，该公用程序可在包含解包软件的目录中找到。idsktune 会检查适当的增补程序，并验证系统是否已进行调整以支持高性能的目录服务。

   作为超级用户，请输入以下命令：

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

   请按照建议对系统执行手动更改。 idsktune 本身不会对系统进行更改。

2. 修复至少由 idsktune 指明的所有 ERROR 状况。如果不修复 ERROR 状况，安装可能会失败。

   表 1-9 指出查找系统上尚未安装的正式增补程序的位置。

表 1-9 获取增补程序的位置 （针对不同平台）

平台	浏览 ...
Hewlett Packard HP-UX	http://www.hp.com/support/
IBM AIX	http://www.ibm.com/support/
Red Hat Linux	http://www.redhat.com/

   详细信息，请参阅第 5 章 “调整操作系统”（第 89 页）。

3. （可选）创建 Directory Server 的用户和组帐户。

   Directory Server 以安装期间指定的用户和组身份运行。设置权限，以防止对该系统上的目录和其他资源进行未授权访问。详细信息，请参阅 “（UNIX 平台）用户和组”（第 91 页）。

4. （可选）在以另一用户身份执行交互式安装时，请使用 xhost(1) 命令以允许访问显示。

   在适当设置 DISPLAY 环境变量并以具备访问显示权限的用户身份执行安装时，默认情况下，安装程序会显示图形用户界面。

   如果安装程序不能显示图形用户界面，则会以命令行的模式开始安装。

5. 在使用区域设置并非为美国英语的平台上进行安装前，请将 LANG 环境变量设置为 C。

针对 AIX 系统的其他说明

- 如果计划使用控制台，则请安装 `X11.adt` 软件包。

  此软件包不是标准绑定的一部分，可以从 IBM 获取。

针对 HP-UX 系统的其他说明

1. 请确保已安装对 IPv6 的支持，即使不计划将 IPv6 界面用于 Directory Server。
2. 使用其字体不受美国英语支持的区域进行远程安装之前，请确保您可以访问远程会话的字体别名。

   有关说明，请参阅操作系统文档。

执行交互式安装

1. 启动包含解包软件的目录中的安装程序。

   对于图形用户界面：

   ```
   root# ./setup
   ```

   对于命令行界面：

   ```
   root# ./setup -nodisplay
   ```

   出现第一个安装屏幕。
2. 使用 “准备安装信息”（第 20 页）时制作的工作表，按照每个屏幕上的指示操作。

注意 要在支持 64 位服务器的平台上安装 32 位 Directory Server，请确保清除名为 “选择组件”的向导屏幕中 Sun ONE Directory Suite > Sun ONE Directory Server （64 位支持）旁边的复选框。

不要将此版本安装在 Directory Server 早期版本所在的同一目录中。如果必须重新使用同一目录位置，请先卸载早期版本。详细信息，请参阅第 2 章 “从以前版本升级”。

继续执行 “正在完成安装过程”（第 36 页）。

执行无提示安装

完成以下过程中的步骤。

创建规范文件

要执行无提示安装，首先必须创建包含安装规范的文件。要获取无提示安装规范文件模板，请参阅解包软件的目录下的 `setup_data/typical.ins`。

注意 规范文件可能包含明文口令。使用适当的文件权限保护此类文件。

可通过手动编辑模板文件的副本或使用安装程序执行交互式配置，创建无提示安装规范文件。

1. 成为超级用户。
2. 启动包含 `-saveState` 选项的安装程序。

   ```
   root# ./setup -saveState filename
   ```

   以创建规范文件 *filename*。
3. 执行交互式安装。
4. 在使用规范文件 *filename* 以在其他系统上进行安装前，请对其进行调整。

   一些无提示安装规范文件指令 （例如， `FullMachineName`）直接取决于基础主机系统，因此一般无法生成。

无提示安装规范文件包含对应于安装程序内部版本的校验和字符串。要重新使用该安装程序不同内部版本或发行的无提示安装规范文件，可更新各行中以 `[STATE_BEGIN` 和 `[STATE_DONE` 开头的校验和字符串。更新的校验和位于 `typical.ins`。代码示例 1-1 （第 29 页）显示了示例校验和。

使用规范文件进行安装

1. 验证对安装规范文件所做的更改。
2. 在无提示模式下启动安装程序。

   ```
   root# ./setup -noconsole -nodisplay -state filename
   ```

   此处的 *filename* 是指无提示安装规范文件。

正在完成安装过程

1. 请确保 *ServerRoot*`/alias` 下面文件的访问权限已设置为阻止所有用户访问，*ServerRoot* 下安装的服务器除外。
2. （可选）添加支持以在系统重引导时启动 Directory Server。

   详细信息，请参阅操作系统文档。

3. （可选）启用核心文件生成。

   如果已经以超级用户的身份安装了 Directory Server，但却将用户和组 ID 设置为另一个帐户的用户和组 ID，则发生故障时， Directory Server 可能无法生成核心文件。强烈建议您为核心文件规划足够的空间，并允许 Directory Server 在故障期间生成核心文件。

   详细信息，请参阅 “（UNIX 平台）核心文件”（第 81 页）。

4. （可选）许多用 Perl 编写的命令行脚本现在可以交互地读取绑定口令 （`-w -` 选项）。要启用此功能：

   a. 安装 `Term::ReadKey` Perl 模块，它与 CPAN 所在位置不同。

   a. 通过取消对相应行的注释，编辑各个 Perl 脚本以交互地读取绑定口令。

   所有其他 Perl 脚本功能在没有 `Term::ReadKey` 模块的情况下仍然可用。

Directory Server 现在已最低限度地进行了配置和启动。

在 Windows 系统上安装

根据相应章节中的说明进行操作：

- 准备安装
- 执行交互式安装
- 执行无提示安装
- 正在完成安装过程

准备安装

1. 安装 Windows 2000 时，应指定计算机是独立的服务器，而不是任何现有域或工作组的成员，以减小对网络安全服务的依赖。
2. 应用 Service Pack 3。
3. 确保显示驱动程序支持至少 256 色。
4. 以具有 `Administrator` 特权的用户身份登录。
5. 将 `TEMP` 环境变量设置为临时文件的有效文件夹。

执行交互式安装

1. 请双击包含解包软件的文件夹中的 `setup.exe`。

   出现第一个安装屏幕。

2. 使用 “准备安装信息”（第 20 页）时制作的工作表，按照每个屏幕上的指示操作。

   不要将此版本安装在 Directory Server 早期版本所在的同一文件夹中。如果必须重新使用同一文件夹位置，请先卸载早期版本。详细信息，请参阅第 2 章 “从以前版本升级”。

继续执行 “正在完成安装过程”（第 39 页）。

执行无提示安装

完成以下过程中的步骤。

创建规范文件

要执行无提示安装，首先必须创建包含安装规范的文件。要获取无提示安装规范文件模板，请参阅解包软件的文件夹中的 `setup_data\typical.ins`。

注意 规范文件可能包含明文口令。使用适当的文件权限保护此类文件。

可通过手动编辑模板文件的副本或使用安装程序执行交互式配置，创建无提示安装规范文件。

1. 以具有 Administrator 特权的用户身份登录。
2. 启动包含 `-saveState` 选项的安装程序。

   从解包产品的文件夹中，输入

   Prompt`>setup -saveState` *filename*

   以创建规范文件 *filename*。
3. 执行交互式安装。
4. 在使用规范文件 *filename* 以在其他系统上进行安装前，请对其进行调整。

   一些无提示安装规范文件指令 （例如， `FullMachineName`）直接取决于基础主机系统，因此一般无法生成。

无提示安装规范文件包含对应于安装程序内部版本的校验和字符串。要重新使用该安装程序不同内部版本或发行的无提示安装规范文件，可更新各行中以 `[STATE_BEGIN` 和 `[STATE_DONE` 开头的校验和字符串。更新的校验和位于 `typical.ins`。代码示例 1-1 （第 29 页）显示了示例校验和。

使用规范文件进行安装

1. 验证对安装规范文件所做的更改。
2. 在无提示模式下启动安装程序。

   从解包产品的文件夹中，输入

   Prompt`>setup -noconsole -nodisplay -state` *filename*

   此处的 *filename* 是指无提示安装规范文件。

正在完成安装过程

1. 请确保 *ServerRoot*`\alias` 下面文件的访问权限已设置为阻止所有用户访问，*ServerRoot* 下安装的服务器除外。
2. 完成安装后，请手动设置以下文件的特殊访问权限，使只有运行 Administration Server 的用户和组具有读写访问权限，而所有其他用户无权访问。
   - *ServerRoot*`\admin-serv\config\adm.conf`
   - *ServerRoot*`\admin-serv\config\admpw`
   - *ServerRoot*`\admin-serv\config\magnus.conf`
   - *ServerRoot*`\admin-serv\config\obj.conf`
   - *ServerRoot*`\admin-serv\config\secmod.db`
   - *ServerRoot*`\admin-serv\config\server.xml`

   请参阅 Windows 帮助，以了解有关设置文件特殊访问权限的说明。修改权限可避免未经授权的用户修改 Administration Server 的配置数据。
3. （可选）许多用 Perl 编写的命令行脚本现在可以交互地读取绑定口令（`-w -` 选项）。要启用此功能：
   a. 安装 `Term::ReadKey` Perl 模块，它与 CPAN 所在位置不同。
   b. 通过取消对相应行的注释，编辑各个 Perl 脚本以交互地读取绑定口令。

   所有其他 Perl 脚本功能在没有 `Term::ReadKey` 模块的情况下仍然可用。

Directory Server 现在已最低限度地进行了配置和启动。

卸载

卸载可从计算机中删除软件和关联数据。 Directory Server 将不可用，而且所有设置和数据全部丢失。

卸载不仅删除服务器软件，而且会删除系统上存储的注册数据。如果在使用卸载程序前手动删除文件，则会破坏注册。要避免破坏注册，可在手动删除任何产品文件前，使用卸载程序。

注意 在继续卸载包含后缀为 `o=NetscapeRoot` 的配置信息的配置目录前，不会收到警告。

如果卸载供其他目录获取配置信息的集中式配置目录，则以后不能管理这些目录。

根据相应章节中的说明进行操作：

- 在 Solaris 系统上卸载
- 在其他 UNIX 系统上卸载
- 在 Windows 系统上卸载

在 Solaris 系统上卸载

Directory Server 软件的卸载方式取决于安装过程期间使用的封装类型，以及是否希望与卸载程序进行交互。根据相应章节中的说明进行操作：

- 使用 Solaris 软件包进行安装后执行交互式卸载
- 从压缩存档文件进行安装后执行交互式卸载
- 使用 Solaris 软件包进行安装后执行无提示卸载
- 从压缩存档文件进行安装后执行无提示卸载

使用 Solaris 软件包进行安装后执行交互式卸载

根据相应章节中的说明进行操作：

- 卸载早期的 Directory Server 版本
- 取消配置 Administration Server
- 取消配置 Directory Server

- 正在删除软件包

卸载早期的 Directory Server 版本

- 要点 如果在 Solaris 系统上完成从 Directory Server 5.1 到 5.2 的升级，且 5.1 版本是从 IPLT* Solaris 软件包中安装的，则执行 5.1 版本的卸载程序：

  ```
  root# /usr/sbin/directoryserver.51bak uninstall
  ```

取消配置 Administration Server

- 删除 Administration Server 配置。

  ```
  root# /usr/sbin/mpsadmserver unconfigure
  ```

  出现第一个卸载屏幕。按照每个屏幕上的说明执行操作。

取消配置 Directory Server

- 删除 Directory Server 配置。

  ```
  root# /usr/sbin/directoryserver unconfigure
  ```

  出现第一个卸载屏幕。按照每个屏幕上的说明执行操作。

正在删除软件包

- 使用 pkgrm(1M) 公用程序，删除在 “使用 Solaris 软件包执行交互式安装”（第 23 页）中安装的软件包。

从压缩存档文件进行安装后执行交互式卸载

1. 在 *ServerRoot* 目录中，启动卸载程序。

   ```
   root# ./uninstall_dirserver
   ```

   出现第一个卸载屏幕。

2. 按照每个屏幕上的说明执行操作。

现在，即删除了选定的软件。如果卸载程序不能删除 *ServerRoot* 目录下的所有文件，则会显示一条消息。可手动删除 *ServerRoot* 下的其余文件。

使用 Solaris 软件包进行安装后执行无提示卸载

1. 编辑卸载规范文件 *ServerRoot*/setup/uninstall.ins，以包括适当的管理员标识符和口令。

代码示例 1-2 卸载规范文件示例

```
[STATE_BEGIN Sun ONE Directory Distribution checksum]

ConfigDirectoryAdminID = admin-user
ConfigDirectoryAdminPwd = admin-password

[STATE_DONE Sun ONE Directory Distribution checksum]
```

2. 如果在 Solaris 系统上完成从 Directory Server 5.1 到 5.2 的升级，且 5.1 版本是从 IPLT* Solaris 软件包中安装的，则执行 5.1 版本的卸载程序：

```
root# /usr/sbin/directoryserver.51bak uninstall -f 51-uninstaller-file
```

3. 使用 unconfigure 子命令删除 Administration Server 配置。

```
root# /usr/sbin/mpsadmserver unconfigure -f ServerRoot/setup/uninstall.ins
```

4. 使用 unconfigure 子命令删除 Directory Server 配置。

```
root# /usr/sbin/directoryserver unconfigure -f ServerRoot/setup/uninstall.ins
```

5. 使用 pkgrm(1M) 公用程序，删除在 “使用 Solaris 软件包执行无提示安装。”（第 28 页）中安装的软件包。

完成卸载后，可手动删除其余文件。

从压缩存档文件进行安装后执行无提示卸载

1. 编辑卸载规范文件 *ServerRoot*/setup/uninstall.ins （如代码示例 1-2 （第 42 页）中所示），以包括适当的管理员标识符和口令。

2. 在无提示模式下运行卸载程序。

```
root# cd ServerRoot
root# ./uninstall_dirserver -noconsole -nodisplay -state setup/uninstall.ins
```

完成卸载后，可手动删除其余文件。

在其他 UNIX 系统上卸载

根据相应章节中的说明进行操作。

执行交互式卸载

1. 在 *ServerRoot* 目录中，启动卸载程序。

   ```
   root# ./uninstall_dirserver
   ```

   出现第一个卸载屏幕。

2. 按照每个屏幕上的说明执行操作。

现在，即删除了选定的软件。如果卸载程序不能删除 *ServerRoot* 目录下的所有文件，则会显示一条消息。可手动删除 *ServerRoot* 下的其余文件。

执行无提示卸载

1. 编辑卸载规范文件 *ServerRoot*`/setup/uninstall.ins`（如代码示例 1-2（第 42 页）中所示），以包括适当的管理员标识符和口令。
2. 在无提示模式下运行卸载程序。

```
root# cd ServerRoot
root# ./uninstall_dirserver -noconsole -nodisplay -state setup/uninstall.ins
```

完成卸载后，可手动删除其余文件。

在 Windows 系统上卸载

根据相应章节中的说明进行操作。

执行交互式卸载

1. 单击“开始”，然后选择“设置”>“控制面板”。
2. 双击“添加 / 删除程序”。
3. 在 “添加 / 删除程序”窗口，选择 Directory Server，然后单击 “删除”。
4. 按照 Sun ONE “卸载”窗口中的说明执行操作。

   如果已升级 Directory Server，则可使用自定义卸载模式，并选择不删除 Basic System Libraries，它包括与新的 Directory Server 实例共享的 `.dll` 文件。

执行无提示卸载

1. 编辑卸载规范文件 *ServerRoot*`\setup\uninstall.ins`（如代码示例 1-2（第 42 页）中所示），以包括适当的管理员标识符和口令。
2. 在无提示模式下运行卸载程序。

```
Prompt>cd ServerRoot
Prompt>uninstall_dirserver -noconsole -nodisplay -state setup\uninstall.ins
```

完成卸载后，可手动删除其余文件。

强烈建议在卸载后重新启动 Windows 系统。

疑难解答

表 1-10 常见的安装问题及解决方案

问题	可能的解决方案
我收到有关缺少库的消息。	运行 `idsktune`，至少修复所有 `ERROR` 状况，并安装所有建议的增补程序。
安装未起作用，而且我现在无法卸载。该如何操作？	删除产品注册表文件，除非这样做将对其他产品产生负面影响： • 以超级用户身份安装时 Solaris 系统上的 `/var/sadm/install/productregistry` • 其他 UNIX 系统上的 `/var/tmp/productregistry` • Windows 系统文件夹下 `system32` 文件夹中的 `productregistry`，例如 Windows 上的 `C:\WINNT\system32\productregistry` 然后，在重新安装前手动删除部分安装的文件。
安装失败，而我不知道原因。在某处有安装日志吗？	有。可在以下位置找到日志： • 在 Solaris 系统上， `/var/sadm/install/logs`（以超级用户身份安装）或 `/var/tmp`（以普通用户身份安装） • 在其他 UNIX 系统上， `/var/tmp` • 在 Windows 系统上， `%TEMP%` 文件夹
客户机找不到该服务器。	尝试使用主机名，如 `dirserv`。 如果不起作用，请确保该服务器在使用的命名服务（如 DNS）中列出，并尝试使用完全限定域名（如 `dirserv.example.com`）。 如果不起作用，则可尝试使用主机的 IP 地址（如 `192.168.0.30`）。

表 1-10 常见的安装问题及解决方案 （续）

问题	可能的解决方案
该端口处于使用状态。	如果正在升级，则很可能在升级服务器之前没有关闭 Directory Server。请关闭旧服务器，然后手动启动已升级的服务器。 否则，另一个服务器可能会使用该端口。在 UNIX 系统上，使用适当的工具检查端口的使用情况 （如带 `-a` 选项的 `netstat`(1M) 公用程序）以确定可用的端口。
LDAP 验证错误导致安装失败。	安装期间提供的完全限定域名可能不正确 （如 `dirserv.nisDomain.Example.COM`），正确的应该是 `dirserv.example.com`。
我忘记了目录管理员的 DN 和口令。	在 *ServerRoot*`/slapd-`*serverID*`/config/dse.ldif` 中，目录管理员 DN 被记录为 `nsslapd-rootdn` 值。 在 `dse.ldif` 中，目录管理员口令被记录为 `nsslapd-rootpw` 值。如果尚未加密口令 - 强烈建议您对其进行加密！ - 然后，它会以明文的形式出现在 `dse.ldif` 中，不带有用加密方案标识符表示的前缀 （如 {`SSHA`}）。 如果口令已加密，则必须手动修复该问题。 1. 停止 Directory Server。 2. 更改 `dse.ldif` 中 `nsslapd-rootpw` 的值，注意不要添加尾空格。 3. 保存并关闭 `dse.ldif`。 4. 重新启动服务器。 5. 使用分配给 `nsslapd-rootpw` 的值，以目录管理员的身份登录。 6. 如 *Sun ONE Directory Server 管理指南* 中所述，设置目录管理员口令的加密方案，然后再次更改口令。

表 1-10 常见的安装问题及解决方案 （续）

问题	可能的解决方案
我误安装了 Directory Server 的 32 位版本。 如何改为运行 64 位版本？	1. 如 *Sun ONE Directory Server 管理指南* 中所述，将所有后缀全部导出到 LDIF 中。 2. 删除所有数据库文件。 按照该实例 `cn=config,cn=ldbm database,cn=plugins,cn=config` 时的 `nsslapd-directory` 的值所指明的路径找到了数据库文件。 3. 安装 64 位组件 （如果尚未安装）。 4. 使 *ServerRoot*`/bin/slapd/server/64/ns-slapd` 成为可执行文件。 5. 如果操作系统在 32 位模式下运行，则请在 64 位模式下重新启动它。 6. 如有必要，可更改缓存大小设置以在 32 位模式下使用。 详细信息，请参阅第 6 章 “调整缓存大小”。 7. 使用导出的 LDIF 对所有后缀进行初始化，如 *Sun ONE Directory Server 管理指南* 中所述。 8. 重新启动服务器。
我误安装了 Directory Server 的 64 位版本。 如何改为运行 32 位版本？	1. 如 *Sun ONE Directory Server 管理指南* 中所述，将所有后缀全部导出到 LDIF 中。 2. 删除所有数据库文件。 按照该实例 `cn=config,cn=ldbm database,cn=plugins,cn=config` 时的 `nsslapd-directory` 的值所指明的路径找到了数据库文件。 3. 更改 *ServerRoot*`/bin/slapd/server/64/ns-slapd` 的模式，使它成为不可执行的文件。 4. 使用导出的 LDIF 对所有后缀进行初始化，如 *Sun ONE Directory Server 管理指南* 中所述。 5. 重新启动服务器。

表 1-10 常见的安装问题及解决方案 （续）

问题	可能的解决方案
我编写了用于处理安装的脚本。使用我的脚本尝试安装时，安装程序返回 73，而不是 0。 这是为什么？	安装程序的返回代码如下： 0 - SUCCESS 1 - WARNING_REBOOT_REQUIRED 2 - WARNING_PLATFORM_SUPPORT_LIMITED 3 - WARNING_RESOURCE_NOT_FOUND 4 - WARNING_CANNOT_WRITE_LOG 5 - WARNING_LOCALE_NOT_SUPPORTED 50 - ERROR_FATAL 51 - ERROR_ACCESS 52 - ERROR_PLATFORM_NOT_SUPPORTED 53 - ERROR_NO_WINDOWING_SYSTEM_AVAILABLE 54 - ERROR_RESOURCE_NOT_FOUND 55 - ERROR_TASK_FAILURE 56 - ERROR_USER_EXIT 57 - ERROR_CANNOT_UPGRADE 58 - ERROR_NOTHING_TO_DO 59 - ERROR_IN_SERIALIZATION 60 - ERROR_ABNORMAL_EXIT 61 - ERROR_INCOMPATIBLE_STATEFILE 62 - ERROR_UNKNOWN_COMMANDLINE_OPTION 70 - ERROR_NOT_INSTALLED 71 - PARTIALLY_UNINSTALLED 72 - FULLY_UNINSTALLED 73 - INSTALLED 74 - ERROR_FAILED 75 - ERROR_STOPPED 76 - ERROR_STOPPED_ON_ERROR 77 - PARTIALLY_INSTALLED 换句话说， 73 表示安装成功。

第 2 章

从以前版本升级

本章介绍从 Netscape Directory Server 4.x 和 iPlanet Directory Server 5.x 升级到 Sun ONE Directory Server 5.2。

注意 本章不说明如何从 Innosoft Distributed Directory Server 4.5.1 升级。

本章主要讨论如何将目录数据从旧服务器移植到新服务器上。有关从旧服务器移植到新服务器上的配置属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册*。

升级之前

升级前，请熟悉 Sun ONE Directory Server 5.2 提供的新功能，在 “建议的读物”（第 12 页）下面的文档中进行了描述。并请检查在实施现有目录服务期间制定的设计决策。

升级单个服务器实例

升级服务器实例包括在现有服务器旁安装新服务器（在不同的 *ServerRoot* 中使用不同的 *serverID*，以及不同的 Administration Server 和 Directory Server 端口号）、停用旧服务器、移植配置和目录数据，然后使客户机向新服务器发出请求。

注意 确保运行现有服务器的主机上有足够的磁盘空间。升级过程不仅至少需要有足够的本地磁盘空间来存放旧服务器和新服务器的二进制数据和数据库，而且还需要有足够的额外空间来存放包含所有现有后缀中条目的 LDIF 文件。估计所需的本地磁盘空间可能要稍微大于：

2 *（现有服务器所需的空间） +（LDIF 文件所需的空间）

必须对同一主机上的两个服务器同时执行升级过程，因为不能通过联网的驱动器执行数据移植。

Sun ONE Directory Server 5.2 提供的脚本可帮助您移植服务器实例的数据。移植脚本按顺序执行下列任务：

1. 停用现有服务器，同时备份当前配置。
2. 检查架构配置文件，通知您标准架构配置文件和现有服务器使用的架构配置文件之间的差异。

   （仅用于 4.x 到 5.2）如果现有的 4.x 服务器使用未安装在默认位置的自定义架构，位于 *ServerRoot*/slapd-*serverID*/config，那么您必须在移植目录数据之前手动调整配置。
3. 为存储在旧服务器中的每个后缀创建数据库。

   （仅用于 4.x 到 5.2） 4.x 服务器支持每个数据库存在多个后缀。移植脚本为新服务器上的每个后缀都创建数据库。
4. 移植服务器和数据库配置参数。

   4.x 服务器将此类参数存储在 slapd.conf 中。 5.x 服务器将此类参数作为条目存储在 dse.ldif 中。

注意 该脚本不移植 o=NetscapeRoot 下的数据。

部署服务器 （例如依赖此后辍中数据的 Sun ONE Messaging Server）时，请手动移植 o=NetscapeRoot 中的数据，或使用此服务器提供的工具进行移植。

（仅用于 4.x 到 5.2）移植脚本不移植所有的 4.x 服务器参数。在某些情况下，必须手动移植 4.x 属性值。详细信息，请参阅 *Sun ONE Directory Server 参考手册* 的当前版本。

5. 移植用户定义的架构对象。

6. 移植索引。
7. 移植标准服务器插件。

   必须手动移植自定义的插件。至少，必须重新编译所有自定义插件。有关插件 API 变更的详细列表，请参阅 *Sun ONE Directory Server Plug-In API 编程指南*。
8. （仅用于 5.x 到 5.2）移植复制协议。

注意 从 5.2 Directory Server 复制到 5.1 服务器之前，请将 `cn=config` 时的 `nsslapd-schema-repl-useronly` 设置为 `on`。否则， 5.2 架构就加入 5.1 服务器，以防止 5.1 服务器由于存在重复对象而重新启动。

9. 移植证书数据库和 SSL 参数。
10. （仅用于 5.x 到 5.2）移植数据库链接。
11. （仅用于 5.x 到 5.2）移植复制条目。
12. 移植 SNMP 配置。

完成移植脚本后，客户机可以向新服务器发送请求。

升级多个已复制的服务器

升级多个服务器意味着单独升级每个服务器，这不足为奇。但是，升级服务器的顺序取决于现有服务器的软件版本和复制拓扑。

对于 5.x 到 5.2 的升级，标准过程是自下而上。首先移植使用者服务器。接着升级集线器。最后升级主服务器。有关在特定实例中如何执行此操作的信息，请参阅“5.x 升级方案示例”（第 63 页）。

对于 4.x 到 5.2 升级，由升级 4.x 主服务器开始，然后处理从主服务器复制的使用者服务器的每个分支，从最靠近主服务器的使用者服务器开始复制。有关在特定实例中如何执行此操作的信息，请参阅“4.x 升级方案示例”（第 57 页）。

如果现有环境包括多个已复制服务器，则请在升级前仔细阅读本章中所有相关的节。您必须制定详尽的计划，以避免产生不必要的停机时间。

获取升级帮助

Sun 专业服务可以帮助您升级关键的目录服务。

联系信息，请参阅 `http://www.sun.com/service/sunps/sunone/`。

升级单个服务器

本节介绍从单个现有服务器到单个 5.2 服务器的升级过程。

注意 如果现有的 4.x 服务器使用自定义架构，那么请确保在移植任何数据前，移植脚本可以找到自定义架构。详细信息，请参阅 “（用于 4.x 到 5.2）处理自定义架构”（第 53 页）。

如果移植脚本不识别自定义架构，则它不移植此架构；而是在将数据移植到新服务器后，应用标准架构文件。将标准架构应用到符合自定义架构的条目可能导致无法对其进行修改，从而使已升级的目录为只读。

安装新服务器

按照第 1 章 “安装 Sun ONE Directory Server”中的说明，在与现有服务器所在的同一主机上安装新服务器。

注意 安装新服务器之前，请确保拥有现有服务器的当前备份。

新服务器驻留的 *ServerRoot* 位置必须与现有服务器的位置不同。新服务器还必须由不同的 *serverID* 标识。

尽管可以选择重新使用为原始安装提供的大多数配置信息，但请不要重新使用现有的端口号。相反，在移植现有数据后可以更改新服务器的端口号。

（用于 4.x 到 5.2）处理自定义架构

提供的用于移植数据的脚本只能识别放置在标准 slapd.user_oc.conf 和 slapd.user_at.conf 文件中的自定义架构，或放置在其他文件中并使用 useroc 和 userat 指令包括在 slapd.conf 中的自定义架构。例如，如果自定义架构直接包含在 slapd.at.conf 或 slapd.oc.conf 中，则移植脚本不识别这些架构。

升级前请执行下列步骤。

1. 将 slapd.at.conf 或 slapd.oc.conf 与新服务器的 *ServerRoot*/bin/slapd/install/version4/ 下提供的标准文件进行比较，将自定义架构元素转录到 slapd.user_oc.conf 和 slapd.user_at.conf 文件中。

   如果自定义对象类有继承关系，那么请确保上一级对象类优先于架构配置文件中的其他对象类。

2. 如果自定义属性已添加到 slapd.oc.conf 中的标准对象类，则创建包含 slapd.user_oc.conf 中属性的新对象类，并将新对象类添加到现有目录中使用自定义属性的各个条目中。

3. 使用 useroc 和 userat 指令，将新指令放置在其他文件的 include 语句附近，将 slapd.user_oc.conf 和 slapd.user_at.conf 文件包含在现有服务器的 slapd.conf 文件中。

此时，现有服务器使用的所有自定义架构都应驻留在 slapd.user_oc.conf 或 slapd.user_at.conf 中，且应使用 useroc 和 userat 指令使 slapd.conf 包含这些文件。

移植现有数据

处理自定义架构后，执行下列步骤将现有数据移植到新服务器上。

1. 如果计划要在新的 Directory Server 上采用脱机方式从文件初始化复制，则在处理前要获得这些文件。

   有关导出 Directory Server 数据的说明，请参阅 *Sun ONE Directory Server 管理指南*。

2. 确保新的 Directory Server 正在运行。

3. 作为用户有权在旧服务器和新服务器上启动、停止和运行数据库导出和导入。

   例如，成为超级用户或以 Administrator 身份登录。

4. 设置如表 2-1 所示的环境变量。

表 2-1 移植时使用的环境变量

变量	值
PATH	(UNIX) *ServerRoot*/bin/slapd/admin/bin:$PATH
	(Windows) *ServerRoot*/bin/slapd/admin/bin;%PATH%
PERL5LIB	*ServerRoot*/bin/slapd/admin/bin

5. 在新服务器实例下运行移植脚本：

```
# cd ServerRoot/bin/slapd/admin/bin
# perl migrateInstance5 -p port52 -D "cn=directory manager" -w password -o oldServ -n newServ
```

其中， *oldServ* 代表到旧服务器实例的完整路径 （如 /usr/iplanet/servers/slapd-ldap 或 /usr/iplanet/ds5/slapd-ldap），*newServ* 代表到新服务器实例的完整路径 （如 /var/ds/v5.2/slapd-dirserv）。

脚本在运行时产生输出。可以选择将此输出重定向到文件中，以便在移植完成后进行检查。

仅在将现有数据移植到新服务器后停用旧服务器。

（用于 4.x 到 5.2）创建复制协议

如果现有的 4.x 服务器包含在复制范围内，则在移植数据后，升级需要重新创建复制协议。在执行升级过程之前，请参阅 “（用于 4.x 到 5.2）升级已复制的服务器”（第 55 页）。

有关为 5.2 服务器配置复制的说明，请参阅 *Sun ONE Directory Server 管理指南*。

（可选）重新使用现有端口号

将数据从旧服务器移植到新服务器后，可以选择停用旧服务器，并使新服务器使用旧服务器所使用的相同端口进行监听。使用同一端口可使客户机应用程序继续运行，而无需更改其配置。

有关更改服务器端口的说明，请参阅 *Sun ONE Directory Server 管理指南*。在新服务器开始使用旧端口进行监听之前，要确保停止旧服务器。

（用于 4.x 到 5.2）升级已复制的服务器

升级已复制的 4.x 服务器时，从复制到新的主服务器开始，然后通过复制拓扑逐个处理分支。此方法限制了服务器同步流量的大小。

注意 有关复制配置和初始化的详细说明，请参阅 *Sun ONE Directory Server 管理指南*。

准备新的主服务器

升级期间， 5.2 服务器配置为主服务器，但在 4.x 拓扑中它充当遗留使用者服务器。升级后，禁用 4.x 使用者服务器功能，新服务器则用作 5.2 拓扑中的主服务器。

此过程需要手动配置新的主服务器。因此，可以在与现有主服务器所在的不同主机上安装新的主服务器。

1. 按照第 1 章 “安装 Sun ONE Directory Server”中的说明安装新服务器。
2. 在新服务器上手动重新生成 4.x 主服务器的配置。
3. 将新服务器用作主服务器 （用于 5.2 拓扑）。

   有关说明，请参阅 *Sun ONE Directory Server 管理指南*。
4. 将新服务器用作 4.x 主服务器的遗留使用者服务器 （用于 4.x 拓扑）。

   有关说明，请再次参考 *Sun ONE Directory Server 管理指南*。
5. 对从 4.x 主服务器到新服务器的复制进行初始化。

   此过程在 *Netscape Directory Server 管理指南* 的第 13 章 “管理复制”中进行描述。请参阅标题为 “手动初始化使用者服务器”一节。

现在可以升级使用者服务器。

升级使用者服务器

本过程列出一些方法。详细信息，请参阅后续步骤。

1. 升级 4.x 拓扑中的所有分支。
2. 根据需要，向 5.2 拓扑添加其他服务器。

3. 在新的主服务器上禁用遗留使用者服务器协议以切断新拓扑与旧拓扑之间的联系。

此过程完成后，即完成了更新过程。

升级分支

将现有 4.x 复制拓扑视作一个树，主服务器作为根元素。这里，分支表示此树中一组已复制的服务器，复制流从根节点供应商服务器开始，通过树中的使用者服务器，最终达到叶节点使用者服务器。

升级分支包括自上而下使用新服务器替换分支中的所有旧服务器。

注意 升级服务器时，复制流停止流向此分支中的所有下游服务器。在升级期间，应考虑将客户机请求重定向到另一个分支。

1. 按照 “升级单个服务器”（第 52 页）中的说明，升级分支中的顶端服务器。

   此操作切断流向分支的复制流，暂时停止分支中的下游服务器上的复制更新。

2. 配置 5.2 分支中新服务器上的复制协议，以便接收复制拓扑中与新的主服务器较近的 5.2 服务器的更新。

   例如，在新分支中配置顶端服务器来接收 5.2 主服务器中的更新。

3. 对从 5.2 供应商服务器到新的 5.2 服务器的复制进行初始化。

   脱机初始化可能要快于联机初始化，这取决于网络性能和目录数据容量与更新比较的结果。

4. 沿着分支采用递归方式应用步骤 1、步骤 2 和步骤 3，直到对所有叶使用者服务器完成这些步骤为止。

有关配置复制协议和初始化复制的说明，请参阅 *Sun ONE Directory Server 管理指南*。

到此为止，完成了对分支的更新过程。对其余的 4.x 分支重复此过程。

添加其他服务器

完成从 4.x 拓扑到 5.2 拓扑的升级后，可以根据需要为新拓扑添加其他主服务器、集线器和使用者服务器。

针对每个其他服务器执行下列步骤。

1. 按照第 1 章 “安装 Sun ONE Directory Server”中的说明安装新服务器。
2. 调整新服务器上的复制协议以符合已规划的拓扑。

   有关说明，请参阅 *Sun ONE Directory Server 管理指南*。
3. 在新服务器上初始化复制。

   有关说明，请再次参阅 *Sun ONE Directory Server 管理指南*。

4.x 升级方案示例

请考虑某一 4.x 主服务器的升级，这个主服务器复制到两个分支，一个分支是单个使用者服务器，另一个分支是提供有两个使用者服务器的集线器。本节介绍升级到新的多主服务器拓扑所执行的步骤。

图 2-1 显示升级前的 4.x 拓扑。

图 2-1 现有 4.x 拓扑示例

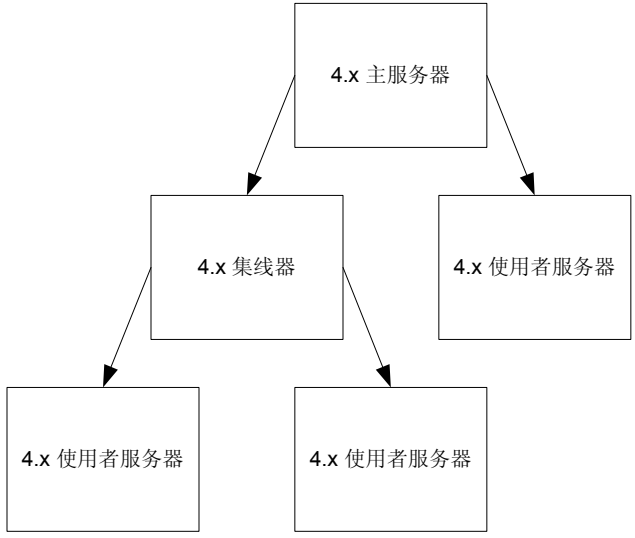


图 2-2 显示添加 5.2 主服务器的过程，此主服务器还充当 4.x 主服务器的遗留使用者服务器。

图 2-2 带有其他新服务器的 4.x 拓扑的示例

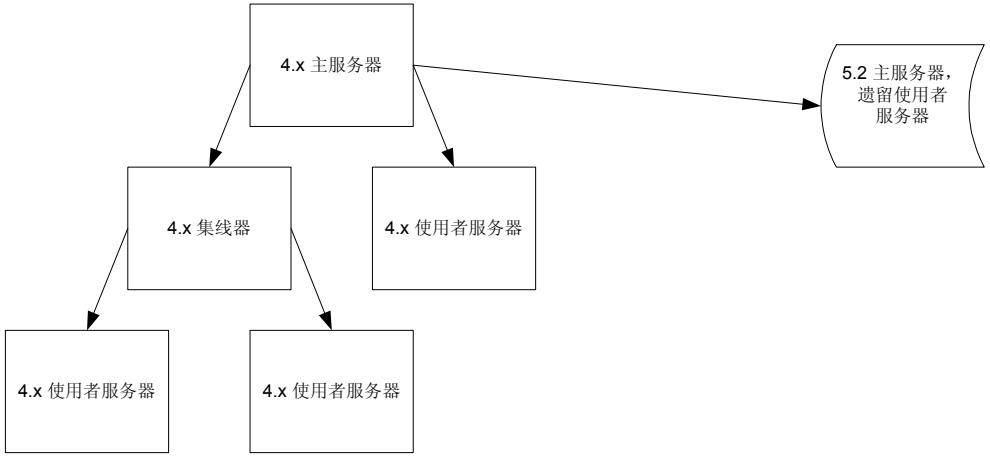


图 2-3 显示复制 4.x 分支的第一步。

注意，在升级期间整个分支都停止接收复制更新。此中断在停止上游 4.x 使用者服务器以进行升级时开始，在重新启动 4.x 使用者服务器时结束。

如说明中所述，如果客户机需要最新的可用更新，则可以选择将客户机请求导向另一个分支上的使用者服务器。

图 2-3 升级过程中 4.x 分支示例 - 第 1 步

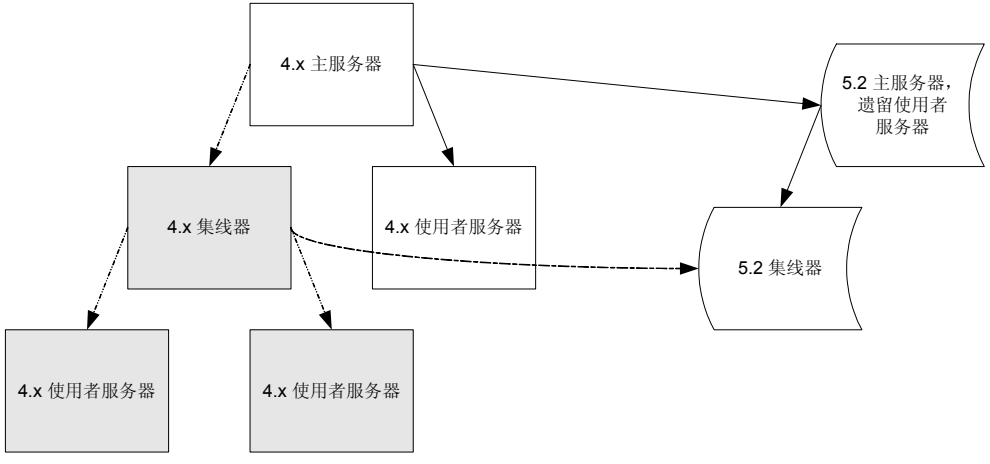


图 2-4 显示替换 4.x 分支的下一个步骤。

图 2-4 升级过程中 4.x 分支示例 - 第 2 步

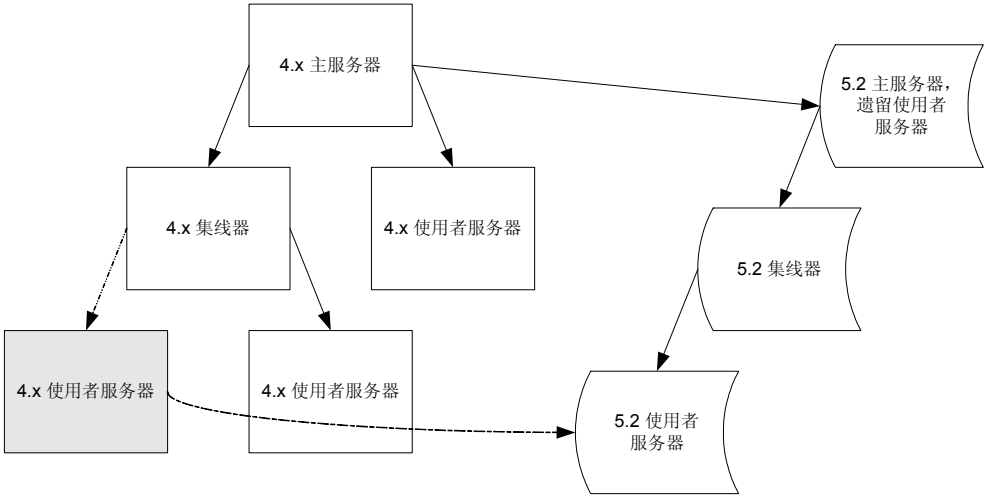


图 2-5 显示替换 4.x 分支的下一个步骤。

图 2-5 升级过程中 4.x 分支示例 - 第 3 步

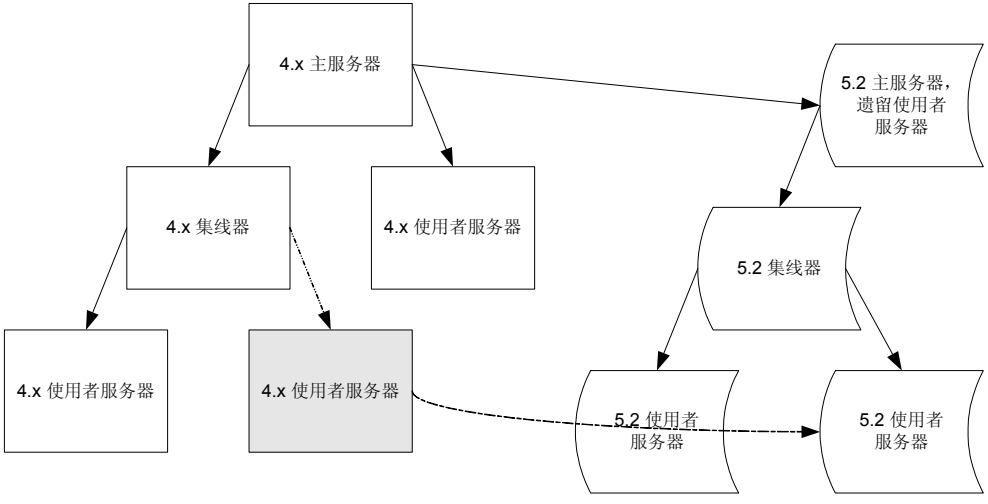


图 2-6 显示替换另一 4.x 分支。

图 2-6 升级过程中 4.x 分支示例 - 下一个分支

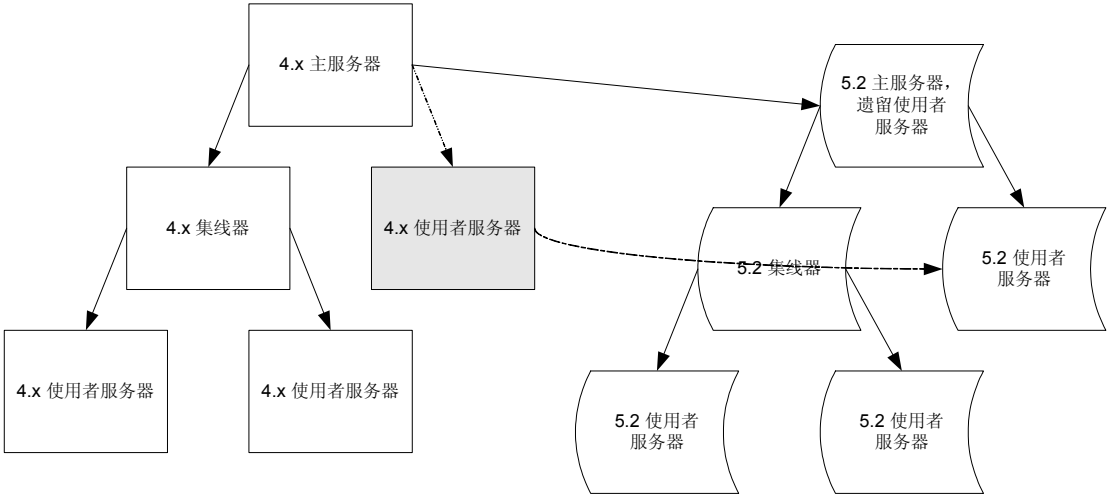


图 2-7 显示两个并列的拓扑。

图 2-7 升级过程中 4.x 和 5.2 拓扑示例

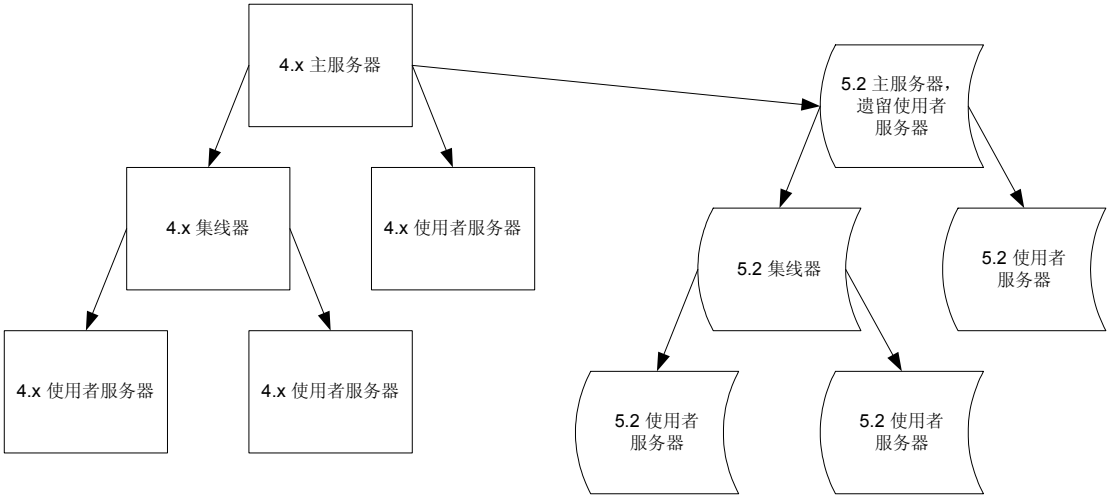
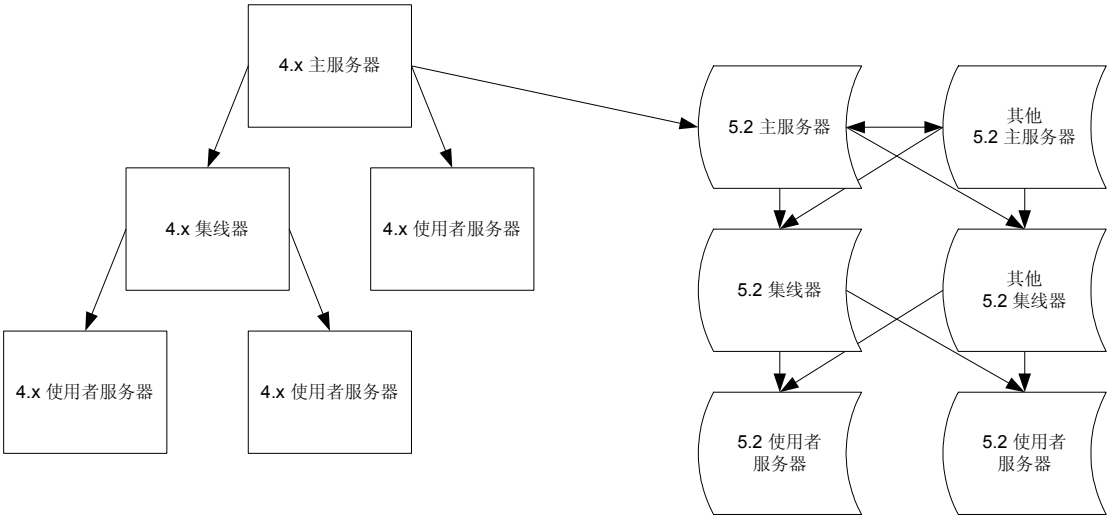


图 2-8 显示向新拓扑中添加主服务器、集线器和其他复制协议。

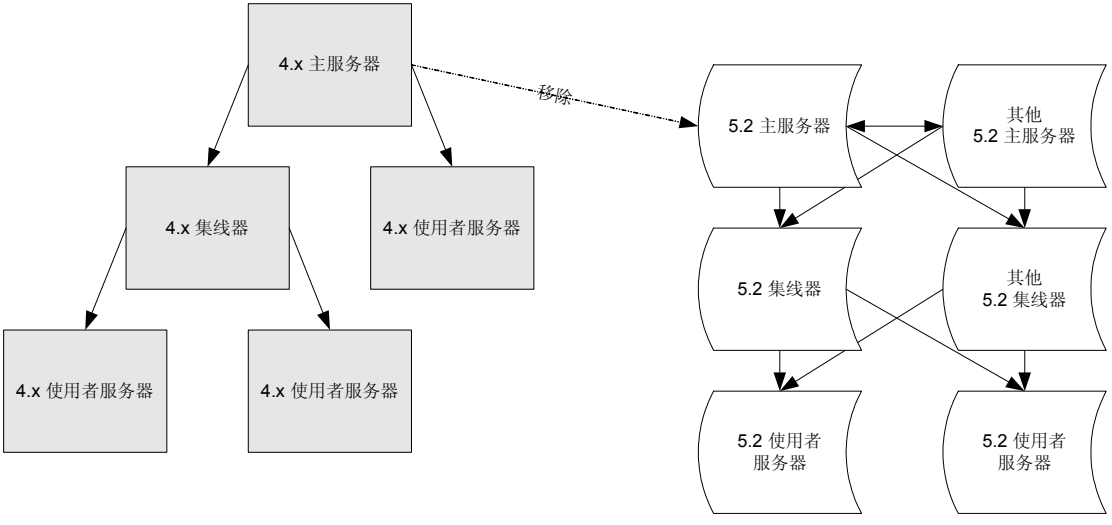
图 2-8　　向 5.2 拓扑中添加服务器



完成升级过程后还可以添加其他服务器。

图 2-9 显示复制协议从旧 4.x 主服务器移至 5.2 主服务器。

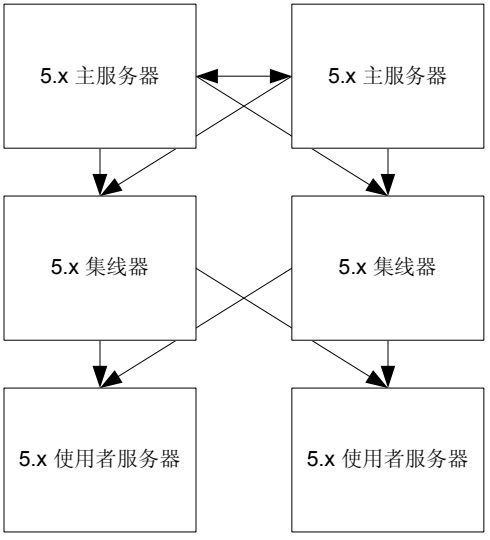
图 2-9　　删除复制协议



在重新定向客户机请求并删除复制协议后，可以禁用 4.x 服务器。

图 2-10 显示生成的 5.2 拓扑。

图 2-10 生成的 5.2 拓扑



现在客户机请求定向到 5.2 拓扑。

（用于 5.x 到 5.2）升级已复制的服务器

升级已复制的 5.x 服务器时，通常从升级使用者服务器开始，然后升级集线器，最后升级主服务器。该自下而上的方法每次只中断一个服务器，而不是中断复制拓扑的一个完整分支。该方法还可帮助您避免主服务器和使用者服务器之间可能的自定义架构同步问题。

注意 这里描述的过程应用标准方法升级 5.x 拓扑。

但是，如果自下而上的方法未能满足特定要求，则请采用其他方法。

升级 5.x 服务器

1. 对于现有拓扑中的每个使用者服务器，请按照 “升级单个服务器”（第 52 页）中的说明升级使用者服务器。
2. 对于现有拓扑中的每个集线器，请按照相同的说明更新集线器。
3. 对于现有拓扑中的每个主服务器，请按照相同说明更新主服务器。

添加其他服务器

完成从 5.x 拓扑到 5.2 拓扑的升级后，可以根据需要为新拓扑添加其他主服务器、集线器和使用者服务器。

针对每个其他服务器执行下列步骤。

1. 按照第 1 章 “安装 Sun ONE Directory Server”中的说明安装新服务器。
2. 调整新服务器上的复制协议以符合已规划的拓扑。
3. 在新服务器上初始化复制。

有关配置复制协议和初始化复制的说明，请参阅 *Sun ONE Directory Server 管理指南*。

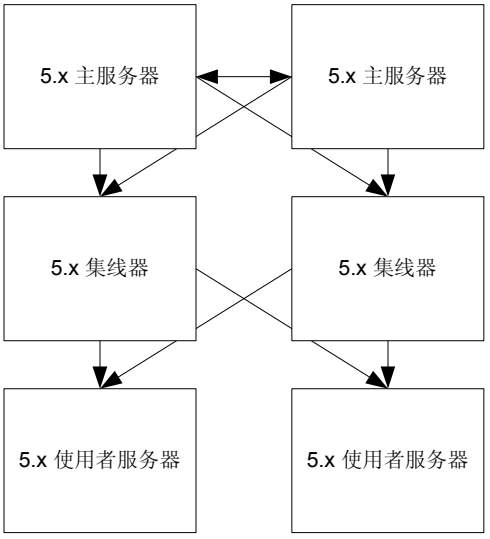
此过程完成后，即完成了更新过程。客户机可以开始使用已升级复制拓扑中的服务器。

5.x 升级方案示例

请考虑对复制到两个集线器 （提供两个使用者服务器）的 5.x 双主服务器进行升级。本节介绍升级此拓扑以使用 5.2 服务器所执行的步骤。

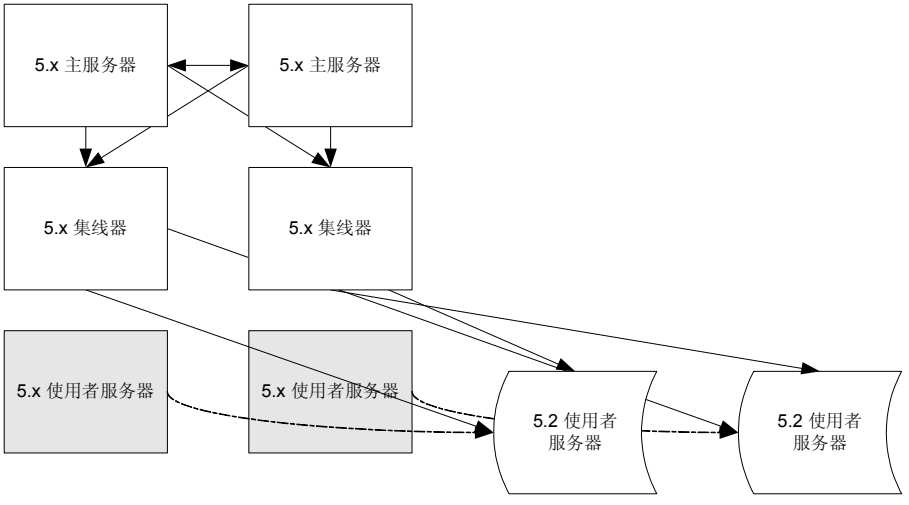
图 2-11 显示升级前的 5.x 拓扑。

图 2-11 现有 5.x 拓扑示例



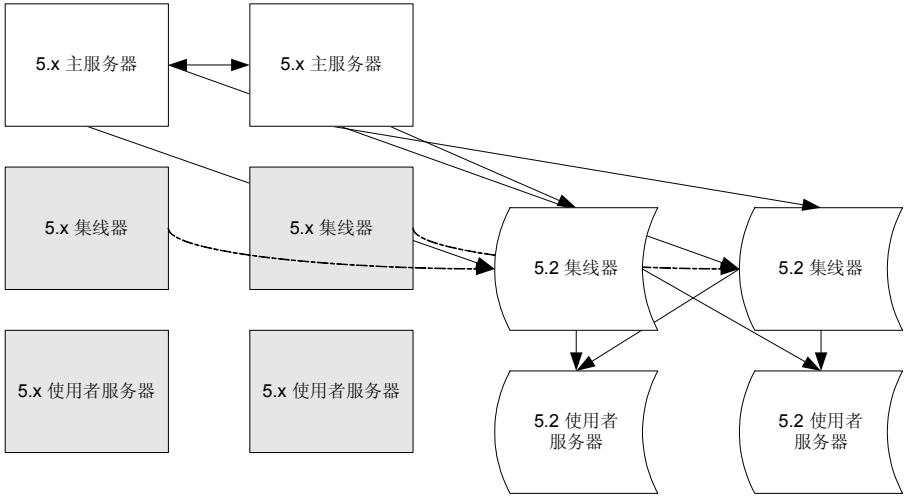
第一步涉及升级使用者服务器。图 2-12 显示生成的拓扑。

图 2-12 5.x 使用者服务器升级步骤示例



下一步涉及升级集线器。图 2-13 显示了升级后的结果。

图 2-13　　5.x 集线器升级步骤示例



下一步涉及升级主服务器。图 2-14 显示升级后的结果。

图 2-14　　5.x 主服务器升级示例 - 第 3 步

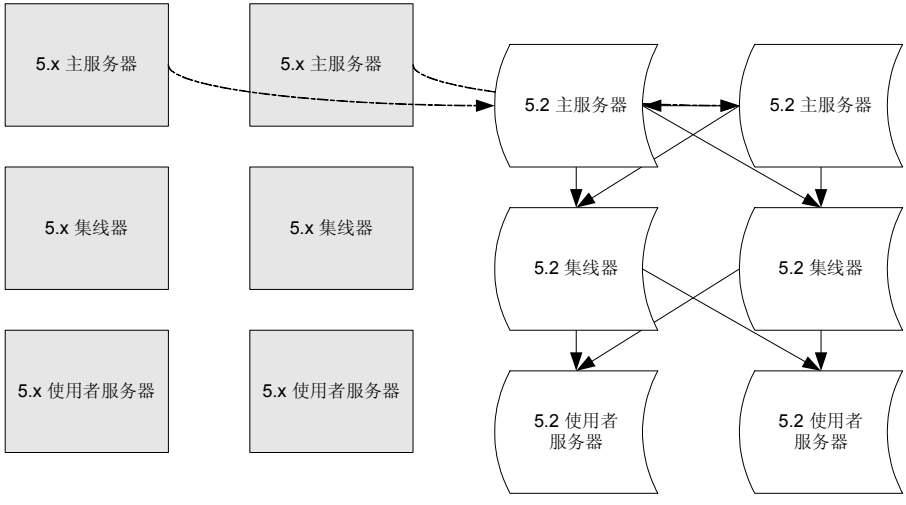
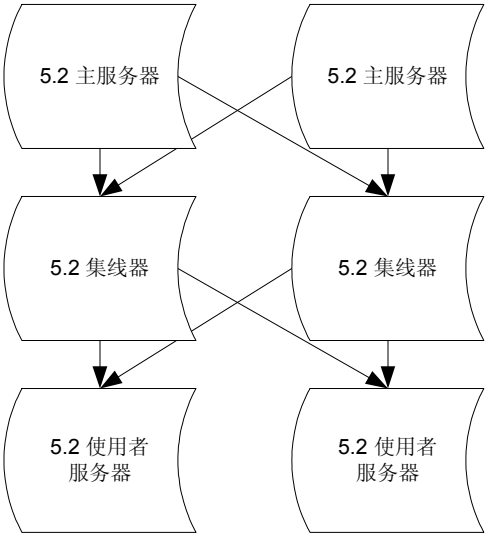


图 2-15 显示升级后的 5.2 拓扑。此时，可以停用旧拓扑中的服务器，新服务器已添加到 5.2 拓扑中。

图 2-15 升级后的 5.2 拓扑示例



现在客户机请求定向到 5.2 拓扑。

第 2 部分

调整

第 3 章 “最佳调整提示”

第 4 章 “硬件大小调整”

第 5 章 “调整操作系统”

第 6 章 “调整缓存大小”

第 7 章 “调整索引编制”

第 8 章 “调整日志记录”

第 9 章 “管理其他资源的使用情况”

第 3 章

最佳调整提示

调整性能意味着修改默认配置，以反映特定的部署要求。

本指南描述如何调整单一 Directory Server 实例。在此假定全部目录服务设计 （包括复制拓扑）已完成，并且您可以使用这里的信息调整 Directory Server 实例以满足设计需要。如果您还没有完成全部目录服务设计，请参阅 *Sun ONE Directory Server 部署指南* 的建议来执行。

如表 3-1 中所示，调整性能需要花费时间、精力，需要思考。

表 3-1 调整过程

阶段	说明
定义目标	按照部署要求，定义特定的、可测量的调整目标。请考虑如下问题： • 哪个应用程序使用 Directory Server？ • 系统是否专用于 Directory Server？系统是否还运行有其他应用程序？如果运行，有哪些其他应用程序？ • 部署需要多少条目？此类条目有多大？ • Directory Server 必须支持每秒多少条搜索？希望执行哪些搜索类型？ • Directory Server 必须支持每秒多少次更新？希望执行哪些更新类型？ • 希望采用怎样的最大更新率和搜索率？希望采用的平均速率是多少？ • 部署时，是否需要在此系统上重复执行批量导入初始化？如果需要，执行导入的频率是多少？一次可以导入多少条目？有哪些条目类型？服务器运行时是否必须联机执行初始化？ 此列表可能存在未尽翔实的部分。请确保您的列表完整而没有遗漏。
选择方法	确定如何制定计划来实施调整优化，以及如何对这些优化进行测量和分析。 是否可以更改系统的硬件配置？是否限制您只能使用现有硬件，只能调整基础操作系统及 Directory Server 本身？如何模拟其他应用程序？应如何生成测试的代表性数据样例？应如何测量结果？应如何分析结果？
执行测试	执行计划的测试。对于大型的复杂部署而言，此阶段可能需要相当长的时间才能完成。
验证结果	检查已测试的潜在优化是否达到此过程开始时定义的目标。 如果达到目标，则记录结果。 如果未达到目标，则记录并监视正在调整的 Directory Server。
记录和监视	应用可能的修改后，记录并监视 Directory Server 的行为。收集所有相关行为的测量结果。
绘图和分析	绘图并分析在记录和监视时观察到的行为。尝试找出可指示进一步测试的证据和模式。 可能需要返回到记录和监视阶段以搜索更多数据。

表 3-1 调整过程 （续）

阶段	说明
调节和调整	应用通过分析测量结果获得的进一步潜在优化。 返回到执行测试阶段。
记录结果	应用的优化达到此过程开始时定义的目标后，请详细记录这些优化，以便可以轻松重现这些优化。

本章列出一些基本建议，每次调整 Directory Server 实例时，几乎都会用到它们。尽管此处提出的建议在一般情况下均有效，但在不了解这些建议对即将到来的特定部署所造成的影响之前，请勿尝试。本章旨在提供核对清单，而非帮您作假。

1. 调整缓存大小。

理想情况下，服务器有足够的可用物理内存，来存放 Directory Server 使用的所有缓存。在此情况下，设置的条目缓存大小要能存放目录中的所有条目，数据库缓存大小要能存放所有索引。

详细信息，请参阅第 6 章 “调整缓存大小”。

2. 优化索引。

a. 删除不必要的索引并添加其他索引以支持需要的请求。

有时，添加一些支持新应用程序请求的附加索引是必要的。可以在 Directory Server 运行时添加、删除和修改索引，但有一个限制，即只能从该点开始向前渐进地对现有数据编制索引。

详细信息，请参阅 “优点：搜索使用索引的方式”（第 116 页）和 “缺点：更新时索引如何处理”（第 117 页）。

b. 仅允许执行已编制索引的搜索。

未编制索引的搜索对服务器性能有很大的负面影响，并可能消耗大量的服务器资源。请考虑添加索引以支持应用程序可能执行的特定搜索，并强制服务器拒绝执行未编制索引的搜索。

详细信息，请参阅 “只允许执行编制了索引的搜索”（第 124 页）。

c. 调整索引列表的最大长度。

详细信息，请参阅 “限制索引表的长度”（第 124 页）。

4. 调整基础操作系统。

详细信息，请参阅第 5 章 “调整操作系统”。

5. 调整操作限制。

   可调整的操作限制防止 Directory Server 将过多资源专用于任何单一操作。请考虑为需要增强性能的客户机应用程序分配唯一的绑定 DN，然后特别针对这些唯一的绑定 DN 设置资源限制。

   详细信息，请参阅第 9 章 “管理其他资源的使用情况”。

6. 禁用不必要的日志记录。

   磁盘访问的速度要比内存访问慢得多。频繁地向磁盘中的日志文件写入数据将对性能产生强烈的负面影响。如有可能，请在不使用访问、错误和审核日志记录功能时关闭这些功能，进而消除磁盘写入操作。至少应尝试将日志文件置于使用不同控制器的各个磁盘上，以降低日志记录的影响。

   详细信息，请参阅第 8 章 “调整日志记录”。

7. 分配磁盘活动。

   尤其是对于支持大量更新的部署而言， Directory Server 可能需要极为频繁的磁盘 I/O 操作。如有可能，请考虑将负载分布在使用不同控制器的多个磁盘中。

   详细信息，请参阅 “调整磁盘子系统的大小”（第 78 页）。

第 4 章

硬件大小调整

适当的硬件大小调整是目录服务计划和部署的一个关键组件。调整硬件大小时，可用内存的容量以及本地磁盘的可用空间容量非常重要。

注意 为取得最好的结果，请安装并配置一个具有代表生产中所使用情况的条目子集的测试系统。然后可以使用该测试系统估计生产服务器的行为。

优化特定系统时，应确保已了解系统总线、外围设备总线、 I/O 设备以及支持的文件系统的工作方式。这样，在调整这些特定系统以支持 Directory Server 时，就可以利用 I/O 子系统的功能。

本章介绍几种评估 Directory Server 实例的磁盘及内存需求的方法，此外，还涉及一些网络和 SSL 加速器的硬件要求。

建议的最低要求

表 4-1 建议了在生产环境中安装和使用该软件时，应满足的最小内存和磁盘空间要求。

事实上，指定条目数的最低要求可能和表 4-1 中提供的内容有所不同。这里的大小反映的是相对较小的条目，其索引是按照默认配置进行设置，并且只对缓存进行最低限度的调整。如果条目包含较大的二进制属性值 （例如数字照片），或者如果索引或缓存与默认配置有所不同，则相应地向上修订最小磁盘空间和内存评估。

表 4-1 最低的磁盘空间和内存要求

要求 ...	可用本地磁盘空间	可用 RAM
解包产品	至少 125 MB	-

表 4-1 最低的磁盘空间和内存要求 （续）

要求 ...	可用本地磁盘空间	可用 RAM
产品安装	至少 200 MB	至少 256 MB
10,000-250,000 个条目	添加至少 3 GB	添加至少 256 MB
250,000-1,000,000 个条目	添加至少 5 GB	添加至少 512 MB
超过 1,000,000 个条目	添加 8 GB 或更多	添加 1 GB 或更多

最低的磁盘空间要求包括用于访问日志的 1 GB。默认情况下， Directory Server 被配置为循环使用 10 个访问日志文件 (`cn=config` 时的 `nsslapd-accesslog-maxlogsperdir`)，每一个日志文件可存放最多 100 MB (`cn=config` 时的 `nsslapd-accesslog-maxlogsize`) 的信息。用于错误日志和审核日志的容量取决于 Directory Server 如何配置。有关配置日志文件的详细信息，请参阅 *Sun ONE Directory Server 管理指南*。

最小可用内存

最小内存估计反映典型部署中一个 Directory Server 实例所使用的内存。此估计没有计入系统和其他应用程序所占用的内存。若要进行更精确的计算，必须以经验为主对内存进行测量。详细信息，请参阅 “调整物理内存大小”（第 75 页）。

通常，可用内存越多，效果就越好。

最小本地磁盘空间

最小本地磁盘空间估计反映典型部署中一个 Directory Server 实例所需的空间。根据经验，建议如果目录条目较大，则所需空间至少是磁盘上等量 LDIF 大小的四倍。详细信息，请参阅 “调整磁盘子系统的大小”（第 78 页）。

请*不要*安装服务器或任何在网络磁盘上访问的数据。 Sun ONE Directory Server 软件不支持通过 NFS、 AFS 或 SMB 使用网络附加存储。相反，所有的配置、日志、数据库和索引文件必须始终驻留在本地存储器中 （即使安装完成以后）。

在 Windows 系统上，将驱动器格式化为 NTFS 格式而不是 FAT 格式。 Directory Server 不支持使用 FAT 格式。 NTFS 允许在文件和目录上设置访问控制。

最小处理能力

大容量系统通常会使用多个高速处理器来提供适当的处理能力，处理多个同时发生的搜索、大范围的索引、复制及其他功能。详细信息，请参阅 “为多处理器系统调整大小”（第 86 页）。

最低网络容量

测试证明， 100 Mbit 以太网甚至能够充分满足服务提供商的使用要求，这取决于预期的最大吞吐量。可采用以下公式估计理论上的最大吞吐量：

最大吞吐量 = 最大返回条目数 / 秒 x 条目的平均大小

设想这样一个示例，一个 Directory Server 必须响应峰值为每秒 5000 次的搜索，而每个搜索返回 1 个平均大小为 2000 字节的条目，因此理论最大吞吐量将为 10 MB 或 80 Mbit。 80 Mbit 看起来比单个 100 Mbit 以太网卡所能提供的吞吐量要多一些。但实际观察到的性能可能会有所不同。

如果希望在广域网上执行多主复制，请确保连接提供足够的吞吐量、最短滞后时间和近乎零的包丢失。

详细信息，请参阅 “调整网络容量大小”（第 86 页）。

调整物理内存大小

Directory Server 使用数据库技术存储信息。与任何依赖数据库技术的应用程序一样，足够多的快速内存是优化 Directory Server 性能的关键。通常，可用内存越多，可以被缓存用于快速访问的目录信息就越多。理想状态下，每个服务器随时都有足够的内存来缓存整个目录内容。由于 Sun ONE Directory Server 5.2 支持 64 位内存寻址，所以缓存大小不再限制为几个 GB。相反，目前 64 位体系结构理论上可处理超过 1.5 TB 的总缓存大小。

注意 当在生产环境中部署 Directory Server 时，请将缓存大小配置在理论处理限制之下，将适当资源留给一般系统操作使用。

对运行 Directory Server 所要求的内存大小的估计既涉及特定 Directory Server 配置需要的内存的估计，也包括运行 Directory Server 的基础系统需要的内存的估计。

为 Directory Server 调整内存大小

根据特定部署的估计配置值，可以估算一个 Directory Server 实例所需要的物理内存。表 4-2 总结了本节中用于计算的值。

表 4-2 调整 Directory Server 内存大小的值

值	说明[1]
nsslapd-cachememsize	用于后缀的条目缓存大小 条目缓存包含格式化的条目，准备发送以响应客户机请求。一个实例可处理多个条目缓存。
nsslapd-dbcachesize	数据库缓存大小 数据库缓存存放来自服务器所使用的数据库和索引的元素。
nsslapd-import-cachesize	用于批量导入的数据库缓存大小 导入缓存仅在导入条目时使用。如果仅执行脱机导入，则有可能通过重新使用为条目或数据库缓存预算的内存，避免为导入缓存预算额外的内存。
nsslapd-maxconnections	最大的受管理连接数。
nsslapd-threadnumber	服务器启动时创建的操作线程的数量

1. 有关完整的说明，请参阅 *Sun ONE Directory Server 参考手册*。

要大致估算内存大小，请执行以下步骤。

1. 估计服务器进程的基本大小， slapdBase。

```
slapdBase      = 75 MB +(nsslapd-threadnumber x 0.5 MB) +(nsslapd-maxconnections x 0.5 KB)
```

2. 确定条目缓存大小的总和， entryCacheSum。

```
entryCacheSum = Sum所有条目的缓存 (nsslapd-cachememsize)
```

3. 确定所有缓存的总大小， cacheSum。

```
cacheSum       = entryCacheSum + nsslapd-dbcachesize + nsslapd-import-cachesize
```

4. 确定 Directory Server 进程的总大小， slapdSize。

```
slapdSize      = slapdBase + cacheSum
```

可以使用 Solaris 系统上 pmap(1) 公用程序或 Windows 任务管理器来衡量 Directory Server 使用的物理内存。

5. 估算处理传入客户机请求所需的内存， slapdGrowth。

```
slapdGrowth    = 20% x slapdSize
```

作为初步估算，假定 20% 的开销用于处理客户机请求。实际百分比可根据特定部署的特性确定。在将 Directory Server 投入生产之前，请先凭经验验证此百分比。

6. 确定用于 Directory Server 的总内存大小， slapdTotal。

```
slapdTotal     = slapdSize + slapdGrowth
```

对于涉及 32 位服务器的大型部署， slapdTotal 可能超过大约 3.4 GB 的实际限制，甚至可能超过 3.7 GB 的理论处理限制。在这种情况下，可选择按第 6 章“调整缓存大小”中的建议调整缓存，进而在系统限制范围内工作，或者使用该产品的 64 位版本。

为操作系统调整内存大小

估计运行基础操作系统所需的内存必须凭经验进行，因为根据系统配置的细节的不同，操作系统内存要求会有很大的不同。基于这个原因，在尝试估算基础操作系统需要多少内存之前，请考虑为部署调整一个代表性系统，如第 5 章“调整操作系统”中所述。调整系统之后，监视内存的使用情况以获取初始估计 systemBase。可以使用 Solaris 系统上的 sar(1M) 公用程序或 Windows 中的任务管理器来衡量内存使用。

注意 为获得最高性能，请将运行 Directory Server 的系统专用于此项服务。

如果必须运行其他应用程序或服务，请在调整所需的总内存大小的同时监视它们使用的内存。

此外，还要为一般系统开销和正常管理使用分配内存。对此数量的初步估算，systemOverhead，应至少为几百兆字节，或者占总物理内存的 10％（取其中较大的值）。目的是向 systemOverhead 分配足够的空间，进而在系统生产时避免从内存交换页面。

操作系统所需的总内存 systemTotal，可用以下公式估算。

```
systemTotal = systemBase + systemOverhead
```

调整总内存大小

根据从前面几节估算的 slapdTotal 和 systemTotal，估计所需的总内存 totalRAM。

```
totalRAM = slapdTotal + systemTotal
```

注意：totalRAM 是对所需的总内存的估算，包括假定系统专用于 Directory Server 处理的内存，也包括期望在此系统上运行的所有其他应用程序和服务所估计使用的内存。

处理内存不足

很多情况下，提供足够的内存来缓存 Directory Server 使用的所有数据并不是经济有效的方法。

最低限度，应该为服务器配备足够的内存以保证运行 Directory Server 时不会引起持续的页面交换。持续的页面交换会对性能产生严重的负面影响。可使用 Solaris 和其他系统上的公用程序（如 vmstat(1M)），以便在启动 Directory Server 和填充条目缓存前后查看内存的统计情况。不受支持的单独发售的公用程序（如用于 Solaris 系统的 MemTool）可用于监视当应用程序在测试系统上运行时内存的使用和分配情况。

如果系统不能提供额外内存，而您又连续观察到持续的页面交换，请减少数据库和条目缓存的大小。交换空间耗尽可能会导致 Directory Server 崩溃。

如果不能提供足够的物理内存以缓存所有的目录数据，请参阅第 6 章 “调整缓存大小”，以获取有关其他备用方案的讨论。

调整磁盘子系统的大小

磁盘的使用情况和 I/O 的功能对性能有很大的影响。特别是对于支持大量修改的部署而言，磁盘子系统可能会变成一个 I/O 瓶颈。本节提供估算一个 Directory Server 实例的全部磁盘容量以及缓和磁盘 I/O 瓶颈的推荐方法。

请参阅第 8 章 “调整日志记录”，以获取有关缓和磁盘 I/O 瓶颈的详细信息。

调整目录后缀大小

后缀的磁盘空间要求不仅取决于目录中条目的大小和数量，而且取决于目录配置，特别是后缀编制索引的方式。若要测量大型部署所需的磁盘空间，请执行以下步骤：

1. 为三个代表性的条目集生成 LDIF，如同可能出现在部署中的那些一样，条目集的个数分别为 10,000、 100,000 和 1,000,000。

   生成的条目不仅应反映预期出现的条目类型 （用户、组、角色、用于扩展架构的条目）的混合，还应反映单个属性值的平均大小，特别是在期望出现诸如 `userCertificate` 和 `jpegPhoto` 之类的大型属性值时。

2. 按期望的部署配置 Directory Server 实例。

   特别要按生产目录的方式编制数据库索引。如果希望以后添加索引，则还必须为这些索引增加空间。

3. 加载每个条目集，记录每个条目集已用的磁盘空间。

4. 将结果用图形表示，以推断部署需要的估算后缀大小。

5. 增加额外的磁盘空间以弥补错误和变化占用的空间。

用于后缀的磁盘空间只是图形的一部分，还必须考虑 Directory Server 使用磁盘的方式。

Directory Server 使用磁盘的方式

目录后缀是 Directory Server 存储在磁盘上的一部分。许多影响磁盘使用的其他因素甚至会因 Directory Server 在部署后的使用方式而有很大的变化，因此这里概括地进行介绍。有关在此讨论的配置项目的说明，请参阅 *Sun ONE Directory Server 管理指南*。

Directory Server 二进制

需要大约 200 MB 磁盘空间来安装此版本的 Directory Server。此估算值不包括用于数据的空间，而是仅指产品二进制的空间。

事件日志记录

用于日志文件的磁盘使用估算取决于 Directory Server 的活动率、日志记录的类型和等级以及日志的轮换策略。

许多日志记录要求都可以事先预测和计划。如果 Directory Server 写入日志 （特别是审核日志），磁盘使用的加载级别就会增加。当高负载部署要求扩展日志记录时，应计划额外的磁盘空间以适应高负载。对于具有高负载日志记录的部署，可通过下列方式减少磁盘空间的需求：制定智能化日志轮换和存档系统、经常轮换日志、自动将旧文件移植为价格比较低廉、容量较高的存储介质，如磁带或比较便宜的磁盘簇上。

某些日志记录的要求不容易预测。例如，调试日志记录可能会引起 `errors` 日志的大小暂时性的急剧增加。对于大型的高负载部署而言，请考虑留出几个 GB 的专用磁盘空间用于临时的高容量调试日志记录。详细信息，请参阅第 8 章 “调整日志记录”。

事务日志

事务日志的大小取决于峰值写入负载。如果出现突发写入，事务日志就会使用比持续写入负载更多的空间。 Directory Server 会定期整理事务日志。因此事务日志不应该不加限制的持续增长。但是，事务日志不会在联机备份期间进行刷新。

Directory Server 通常在启用了持久事务处理的情况下运行。启用持久事务处理功能时， Directory Server 对每项修改 （`add`、 `delete`、 `modify`、 `modrdn`）操作都同步写入事务日志。在这种情况下，如果磁盘忙，就可能会阻止某项操作，从而导致潜在的 I/O 瓶颈。

如果更新性能至关重要，请计划为事务日志使用具有快速写入缓存的磁盘子系统。详细信息，请参阅第 8 章 “调整日志记录”。

复制 Changelog 数据库

如果部署涉及到复制，Directory Server 供应商就会执行更改日志记录。Changelog 的大小取决于修改的量和采用的 changelog 整理类型。请根据 changelog 的整理方式来计划容量。对于大型的高负载部署，请考虑留出几个 GB 的磁盘空间，以处理异常高修改率期间的 changelog 增长。详细信息，请参阅第 8 章 “调整日志记录”。

后缀初始化和 LDIF 文件

在后缀初始化 （也称为批量加载或导入）期间， Directory Server 需要磁盘空间以存放下列文件：后缀数据库文件和 LDIF （用于初始化后缀），以及中间文件 （初始化过程期间需要使用）。在与用于 LDIF 文件和中间文件 （初始化后缀期间使用）的数据库文件所在的相同目录中计划额外 （暂时）容量。

备份和 LDIF 文件

备份通常会消耗大量的磁盘空间。备份的大小与涉及的数据库文件的大小相同。通过分配等同于数据库文件数倍大小空间的方式来容纳多个备份，保证在单独的磁盘上维护数据库及其相应的备份。采用智能化策略移植备份，以随着时间的增长而降低存储介质的成本。

如果部署涉及复制，请计划额外的空间以存放初始化 LDIF 文件，因为它们与备份 LDIF 文件不同。

基于内存 （而非磁盘）的文件系统

一些系统支持基于内存的 `tmpfs` 文件系统。例如，在 Solaris 上， `/tmp` 经常被安装为基于内存的文件系统以提高性能。如果缓存文件放在 `/tmp` （一个与系统上其他应用程序共享的位置）上，请确保系统不会用掉 `/tmp` 下的所有空间。否则，当内存不足时，基于内存的文件系统中的 Directory Server 文件就会被分页到专用于交换分区的磁盘空间。

一些系统支持基于 RAM 磁盘和其他备用内存的文件系统。有关创建和管理基于内存的文件系统的指示，请参阅操作系统文档。请注意，此类文件系统中的所有文件都是易失，且在系统重引导后必须重新加载到内存中。

（UNIX 平台）核心文件

留出至少可供一至两个 `core` 文件使用的空间。虽然 Directory Server 不应转储核心，但是如果系统崩溃时生成的 `core` 文件可用于检查，则崩溃后的恢复和故障排除将会大大简化。生成时， `core` 文件存储在与 `cn=config` 时的 `nsslapd-errorlog` 指定的文件相同的目录中，或者存储在 *ServerRoot*`/bin/slapd/server/` 下 （如果启动时出现系统崩溃）。

管理空间

为预期的系统使用 （包括系统和 Directory Server 管理）留出空间。确保为基本的 Directory Server 安装、配置后缀 （如果驻留在本地实例上）、配置文件等分配足够的空间。

在磁盘上分发文件

通过将通常更新的 Directory Server 数据库和日志文件置于单独的磁盘子系统上，可以将 I/O 通信量分散到多个磁盘轴和控制器上，从而避免 I/O 瓶颈。请考虑为以下每个项目提供专用的磁盘子系统。

事务日志

当启用了持久事务功能时， Directory Server 会对每项修改操作执行同步写入事务日志。所以当磁盘忙时操作即被阻止。将事务日志置于专用的磁盘上可以改进写入性能，并提高 Directory Server 可以处理的修改率。

详细信息，请参阅 “事务日志记录”（第 136 页）。

数据库

多数据库支持允许每个数据库驻留在其各自的物理磁盘上。因而，可以在多个数据库各自的磁盘子系统上分配 Directory Server 负载。若要阻止数据库操作的 I/O 争用，请考虑将每组数据库文件置于单独的磁盘子系统上。

为达到最佳性能，可将数据库文件放在具备较大 I/O 缓冲区的专用快速磁盘子系统上。当在缓存中找不到候选条目时， Directory Server 将读取磁盘中的数据。它会定期刷新写入。对于此类操作，使用快速、专用的磁盘子系统可以减轻潜在的 I/O 瓶颈问题。

`cn=config,cn=ldbm database,cn=plugins,cn=config` 时的 `nsslapd-directory` 属性指定了 Directory Server 存储数据库文件 （包括索引文件）的磁盘位置。默认情况下，此类文件位于 *ServerRoot*`/slapd-`*ServerID*`/db/` 下。

当然，更改数据库位置不仅需要重新启动 Directory Server，而且还需要完全重建数据库。更改生产服务器上的数据库位置可能会是一项艰巨的任务，所以在将服务器用于生产前，应标识最重要的数据库并将其放在单独的磁盘上。

日志文件

Directory Server 提供具有缓冲日志记录功能的访问、错误和审核日志。尽管进行了缓冲，写入这些日志文件需要进行磁盘访问，这可能会与其他 I/O 操作发生争用现象。请考虑将日志文件置于单独的磁盘上，以改进性能、容量和管理。

详细信息，请参阅第 8 章 “调整日志记录”。

基于内存的文件系统上的缓存文件

例如，在 `tmpfs` 文件系统中，仅当物理内存耗尽时才会将文件交换到磁盘中。如果有足够内存来存放物理内存中的所有缓存文件，就可以通过为 Solaris 平台上的 `tmpfs` 文件系统或其他基于内存的文件系统 （如用于其他平台的 RAM 磁盘）分配等量的磁盘空间，并设置 `nsslapd-db-home-directory` 的值使 Directory Server 将缓存文件存储在该文件系统上，从而使性能得到改进。这可以避免系统不必要地将内存映射的缓存文件转储到磁盘。

磁盘子系统备用方案

“快速、廉价、安全：您可以任选两种。”- Sun Performance and Tuning, Cockroft and Pettit。

快速和安全

在实施性能和正常运行时间都至关重要的部署时，请考虑使用非易失内存缓存的基于硬件的 RAID 控制器，以提供在大型磁盘阵列上分发的高速缓冲区的 I/O。通过在多个轴上分布负载，以及在极快的连接上进行缓冲访问，可以对 I/O 进行优化，且可以通过高性能 RAID 条带或奇偶校验块提供极佳的稳定性。

大型非易失的 I/O 缓冲区和高性能磁盘子系统（如 Sun StorEdge™ 产品中所提供）可以极大地提高 Directory Server 性能和正常运行时间。

快速写入缓存卡提供潜在的写入性能改进，特别是在专用于事务日志使用的情况时。快速写入缓存卡提供非易失内存缓存，它独立于磁盘控制器。

快速和廉价

要获取快速、低成本的性能，请确保已在大量磁盘上分配了足够的容量。请考虑使用具有高转速和低寻道时间的磁盘。要获得最佳结果，请为每个分发的组件分配一个专用的磁盘。请考虑使用多主机复制以避免单点故障。

廉价和安全

若要获得廉价且安全的配置，请考虑使用低成本的、基于软件的 RAID 控制器，如 Solaris Volume Manager。

RAID 备用方案

RAID 表示廉价磁盘冗余阵列。顾名思义， RAID 的主要用途是提供恢复。如果阵列中的某个磁盘出现故障，该磁盘上的数据并不会丢失，仍可从此阵列中的一个或多个其他磁盘上得到该数据。为实现恢复， RAID 提出了一种抽象概念，允许多个磁盘驱动器被配置成一个较大的虚拟磁盘，通常称为一个卷。通过连接、镜像或条带化物理磁盘来实现此目的。连接是指通过让一个磁盘的块在逻辑上与另一个磁盘的块相连来实现目的。例如，磁盘 1 占有块 0-99，磁盘 2 占有块 100-199，以此类推。镜像是指通过将一个磁盘的块复制到另一个磁盘，然后使它们保持连续同步来实现目的。条带化则使用算法在多个物理磁盘上分配虚拟磁盘块。

条带化的目的是提高性能。可快速处理随机写入，因为写入的数据可能被指定到条带卷中的多个磁盘上，因此磁盘能并行工作。上述情况也适用于随机读取。对于大型的顺序读写来说，情况可能没有如此简单。但是据观察，顺序的 I/O 性能也可以提高。例如，一个生成许多 I/O 请求的应用程序会堵塞单个磁盘控制器。但是，如果条带卷中的磁盘都有其各自专用的控制器，堵塞情况就不太可能发生，性能也会因此提高。

使用软件或硬件 RAID 管理器设备都可实现 RAID。两种方法各有利弊：

- 硬件 RAID 是在硬件中实现的，因此一般可以提供较高的性能，从而比软件 RAID 产生较少的处理开销。此外，硬件 RAID 与主机系统脱离，主机资源可用于执行应用程序。
- 硬件 RAID 通常比软件 RAID 更昂贵。
- 软件 RAID 比硬件 RAID 更灵活。例如，硬件 RAID 管理器通常与单个磁盘阵列或指定阵列集相关联，而软件 RAID 则可以封装任意多个磁盘阵列，或者如果需要，可以只封装阵列中的某些磁盘。

以下几节讨论 RAID 的配置 （也称为级别）。这里详细讨论了最常见的 RAID 级别（0、 1、 1+0 和 5），对于不常见的级别仅作了一些比较和对照。

RAID 0，条带卷

条带化将数据分散在多个物理磁盘上。逻辑磁盘或卷被分成块或条带，然后以循环的方式分布在物理磁盘上。条带在大小上始终是一个或多个磁盘块，而且所有条带的大小都相同。

RAID 0 的名称是自相矛盾的说法，因为它不提供冗余。 RAID 0 条带中的任何磁盘故障都会导致整个逻辑卷丢失。但是， RAID 0 是所有 RAID 级别中最便宜的，因为其所有磁盘都专门用于存放数据。

RAID 1，镜像卷

镜像的目的是提供冗余。如果镜像中的一个磁盘发生故障，数据将仍然可用且处理可继续进行。但代价是每个物理磁盘都被镜像，这意味着有一半的物理磁盘空间专用于镜像。

RAID 1+0

RAID 1+0 （也称为 RAID 10）提供最高级别的性能和恢复力。因此，也是成本最高的 RAID 实现级别。在多达三个磁盘出现故障后数据仍保持可用，只要所有出现故障的磁盘形成不同的镜像。 RAID 1+0 是通过条带阵列 （其中的段为 RAID 1）实现的。

RAID 0+1

RAID 0+1 比 RAID 1+0 的恢复力稍差。条带被创建且被镜像。如果位于镜像同一边的一个或多个磁盘出现故障，数据将仍然可用。但是如果镜像另一边的某个磁盘也出现故障，那么逻辑卷就丢失了。这点与 RAID 1+0 的微妙差别意味着位于同一边的磁盘可同时出现故障，而数据仍然可用。 RAID 0+1 是通过镜像阵列 （其中段为 RAID 0）实现的。

RAID 5

RAID 5 不如镜像的可恢复性强，但仍提供了冗余，在单个磁盘出现故障后数据仍可用。 RAID 5 使用奇偶校验条带来实现冗余，这些奇偶校验带是通过执行逻辑排除或在其他磁盘上按相应带的字节而创建的。当一个磁盘出现故障时，该磁盘上的数据可使用其他磁盘上相应条带中的数据和奇偶校验来重新计算。不过在执行此类更正计算时，性能会受损。

在正常操作过程中， RAID 5 提供的性能通常比 RAID 0、 1+0 和 0+1 低，原因是 RAID 5 卷必须为每个逻辑写入执行四次物理 I/O 操作。即，读取旧数据和奇偶校验、执行两次排除或操作，以及写入新数据和奇偶校验。读取操作并不会受到同样的影响，因此提供的性能仅比使用相等数量磁盘的标准条带略低一些。也就是说，实际上 RAID 5 卷在其条带上少了一个专用于奇偶校验的磁盘。这也意味着， RAID 5 卷通常要比 RAID 1+0 和 0+1 成本更低，因为 RAID 5 有更多磁盘空间可用于存放数据。

考虑到性能问题，一般不建议使用 RAID 5，除非数据为只读，或者对该卷的写入操作很少。不过，具有写入缓存和快速排除或逻辑引擎的磁盘阵列能够缓解这些性能问题，这使得 RAID 5 在某些部署中成为一种成本低廉而又切实可行的镜像备用方案。

RAID 级别 2、 3 和 4

RAID 级别 2 和 3 适用于大型的顺序数据传输，如视频流。这两种级别都是每次只能处理一个 I/O 操作，因而不适用于要求进行随机访问的应用程序。RAID 2 是使用 Hamming 纠错码 (ECC) 实现的。这意味着需要用三个物理磁盘驱动器来存储 ECC 数据，因而其成本高于 RAID 5，但低于 RAID 1+0 （只要条带上的磁盘多于三个）。 RAID 3 使用逐位奇偶校验的方法来实现冗余。奇偶校验不是像 RAID 5 那样是分布式的，而是写入单个专用磁盘中。

同 RAID 2 和 3 不同， RAID 4 使用一种独立的访问技术，可同时访问多个磁盘驱动器。它所使用的奇偶校验方法与 RAID 5 类似，不同的是奇偶校验被写在一个磁盘中。这样一来，每次写入时都要访问奇偶校验磁盘，这实际上是将多次写入序列化了，因而奇偶校验磁盘可能会成为一个瓶颈。

软件卷管理器

诸如 Solaris™ Volume Manager 之类的卷管理程序也可用于 Directory Server 磁盘管理。在生产环境部署中， Solaris Volume Manager 要优于其他软件卷管理器。

监视 I/O 和磁盘使用

磁盘在正常操作情况下不应处于饱和状态。可以使用 Solaris 上的 `iostat`(1M) 和其他系统上的公用程序以隔离潜在的 I/O 瓶颈。有关处理 Windows 系统上 I/O 瓶颈的详细信息，请参阅 Windows 帮助。

为多处理器系统调整大小

Directory Server 软件已经作了优化以扩展到多处理器。一般来说，添加处理器可全面提高搜索、索引维护和复制操作的性能。

然而，在具体的目录部署中，可能会出现一个效率递减点，此时添加更多处理器不会对性能有很大帮助。如果对搜索、索引编制和复制操作的性能要求极高，那么请考虑将负载平衡和目录代理技术作为解决方案的一部分。

调整网络容量大小

Directory Server 是网络密集型应用程序。为提高 Directory Server 实例的网络可用性，可以为系统配备两个或更多的网络接口。 Directory Server 支持在同一进程中对多个网络接口进行监听的硬件配置。

如果计划在网络上建立目录服务器群集来平衡负载，那么请确保网络基础结构能够支持所产生的额外负载。如果打算在广域网环境下的复制操作中支持高更新率，那么请通过经验测试确保网络质量和带宽满足复制吞吐量的要求。

为 SSL 调整大小

默认情况下，安全套接字层 (SSL) 协议在软件中已实现。使用基于软件的 SSL 实现方式可能会对 Directory Server 的性能有很大的负面影响。在 SSL 模式下运行目录可能需要部署多个目录副本以满足整体的性能要求。

虽然硬件加速卡不能消除使用 SSL 的影响，但与基于软件的实现方式相比，加速卡可以极大地提高性能。 Sun ONE Directory Server 5.2 支持使用 SSL 硬件加速器，如受支持的 Sun Crypto Accelerator 硬件。

当 SSL 密钥计算是瓶颈时，使用 Sun Crypto Accelerator 板就很有用。然而，当 SSL 密钥计算不是瓶颈时，此硬件可能不会提高性能，由于在 SSL 握手以协商连接期间，它特别加快了密钥计算 （但不会对后面的消息进行加密和解密）。请参阅附录 B “使用 Sun Crypto Accelerator 板”来了解有关在 Directory Server 实例中使用此硬件的说明。

第 5 章

调整操作系统

默认的系统和网络设置不适合于高性能的目录服务。为达到最佳的 Directory Server 性能而对系统进行的调整至少包括检查建议的最新增补程序是否安装在系统上、强制实施基本的安全措施，以及更改某些系统和网络设置。本章将讨论这些调整问题。

产品中提供的 `idsktune` 公用程序 （Solaris 封装版本中的 `/usr/sbin/directoryserver idsktune`）可能会有助于诊断基本的系统配置缺点。为获得高性能的目录服务支持，该公用程序提供了系统调整建议。该公用程序不实际实施所提出的任何建议。调整建议应由合格的系统管理员实施。

检查平台支持

表 1-1（第 18 页）指定了此版本支持的平台以及相关硬件体系结构。请参阅产品发行说明，以获得受支持的平台的更新列表。

安装 Windows 系统时，应指定计算机是独立的服务器，而不是任何现有域或工作组的成员，以减小对网络安全性服务的依赖。

安装系统增补程序

为了保持系统整体安全性，并确保 Sun ONE Directory Server 5.2 的正确安装和操作，应安装最新推荐的系统增补程序、 Service Pack 或修补程序。表 5-1 提供了所需增补程序的位置。

表 5-1 获取增补程序的位置 （针对不同平台）

平台	浏览 ...
Sun Solaris™ 操作环境	http://sunsolve.sun.com/
Hewlett Packard HP-UX	http://www.hp.com/support/
IBM AIX	http://www.ibm.com/support/
Microsoft Windows	http://support.microsoft.com/
Red Hat Linux	http://www.redhat.com/

强制实施基本的安全措施

本节提出的建议并不能消除所有风险。相反，它们只作为简短的核对清单，以帮助您限制某些最显而易见的安全风险。

隔离系统

如果有可能，应使用网络防火墙将运行 Directory Server 的系统与公用 Internet 隔离开。当在必须防止基于 IP 攻击的 Windows 平台上运行 Directory Server 时，隔离系统尤为重要。

不进行双重引导

不要在运行 Directory Server 的系统上进行双引导或运行其他操作系统。其他系统可能允许访问可被限制的文件。

强口令

使用超级用户或管理员口令至少应有 8 个字符长，包括标点符号或其他非字母字符。在 Windows 平台上运行 Directory Server 时，使用强口令尤为重要。

如果选择使用较长的操作系统口令，则可能需要配置系统处理口令的方式。有关说明，请参阅操作系统文档。

(Windows) 本地安全策略

对 Windows 服务器实施本地安全策略，以便在登录尝试失败后将用户锁定。激活和配置事件日志记录，以管理部署的适当大小的日志。还要激活审核日志记录以进行登录尝试。应考虑重命名管理员帐户，使其难以猜测。

详细信息，请参阅 Windows 帮助。

（UNIX 平台）用户和组

出于安全方面的考虑，建议不要以超级用户特权运行 Directory Server 或 Administration Server。例如，可以创建一个没有登录权限的用户和组，然后以此用户和组的身份来安装和运行服务器。如果您将用户和组添加到本地文件，则 `/etc/passwd` 条目为，例如：

```
server:x:61001:Server User:/dev/null:/dev/null
```

对应的 `/etc/group` 条目为，例如：

```
servers::61001:
```

为便于调试，可以在 Solaris 系统上使用诸如 `coreadm`(1M) 的公用程序，选择允许以此用户和组身份运行的进程转储核心。

如果特定的部署要求与诸如消息服务器的其他服务器共享 Directory Server 文件，则应考虑使用同一用户和组运行这些服务器。

如果必须作为超级用户运行 Administration Server，则应考虑停止不使用的服务。

禁用不必要的服务

为获得最佳性能并减少风险，应将系统专用于 Directory Server。运行其他服务（特别是网络服务）会对服务器性能和可伸缩性造成负面影响，而且可能增加安全风险。

应尽可能多地禁用网络服务。 Directory Server 只使用 TCP/IP，而不需要文件共享和其他服务。应禁用一些服务，例如 IP 路由、Mail、NetBIOS、NFS、RAS、Web 发布，以及 Windows 网络客户服务。特别是在 Windows 上，应该停止和禁用除下面服务之外的所有服务：事件日志、即插即用、受保护存储、安全帐户管理器、Sun ONE Administration Server、 Sun ONE Directory Server、远程过程调用 (RPC) 和 SNMP。应考虑禁用 `telnet` 和 `ftp`。

与许多网络服务一样， `telnet` 和 `ftp` 会带来安全风险。这两种服务尤其危险，因为它们在网络上以明文传输用户口令。通过使用诸如 Secure Shell (`ssh`) 和 Secure FTP (`sftp`) 之类的客户机，可以避免使用 `telnet` 和 `ftp`。

如果 Directory Server 实例本身不为网络提供命名服务，则应考虑启用系统的命名服务。诸如 Sun ONE Server Console 的远程管理工具需要命名服务才能完成某些操作，如 IP 地址和主机名之间的转换。

有关禁用网络服务的详细信息，请参阅操作系统文档。

保持准确时间

确保系统时钟合理地与其他系统的系统时钟保持同步，以便于系统之间的日志文件中的日期和时间戳复制和相互关联。考虑使用网络时间协议 (NTP) 客户机来设置正确的系统时间，特别是在 Windows 系统上。

在系统故障之后重新启动

如果可能，请按 *Sun ONE Directory Server 管理指南* 中所述停止 Directory Server。如果在系统关机期间突然停止，而不是正确地关闭，则数据库损坏可能会导致 Directory Server 启动缓慢。恢复数据库可能需要一些时间。 .

(Solaris 软件包) 作为安装和配置过程的组成部分，可以使用适当的脚本在启动时间进行重新启动。

(Windows) 配置 Windows 以使其在系统故障之后自动重新启动。详细信息，请参阅 Windows 帮助。

对于其他平台，请参阅操作系统文档以了解有关在启动时间启动服务的详细信息。

生成基本的调整建议

使用 `idsktune` 公用程序 `/usr/sbin/directoryserver idsktune` （对于 Solaris 封装版本）或 `idsktune` （对于包含产品二进制文件的目录中存在的其他版本）在 Windows 之外的平台上生成基本的调整建议。

在以超级用户身份运行公用程序时，它会搜集有关系统的信息。显示通知、警告和错误，并提出建议的纠正措施。例如，公用程序检查：

- 此版本是否支持操作系统和内核版本。
- 可用内存和磁盘空间是否满足通常用途的最低要求。
- 系统资源限制是否满足通常用途的最低要求。
- 是否安装了所需的增补程序或 Service Pack。

注意 在计划用于生产目的的系统上安装 Directory Server 软件之前，至少应修复所有 ERROR 状况。

个别的部署要求可能会超出最低要求。可选择提供的资源比 idsktune 公用程序识别为最低系统要求的资源更多。

有关该公用程序的详细信息，请参阅 Sun ONE Directory Server Resource Kit 文档。可以按 “下载 Directory Server 工具”（第 12 页）中所述获得 Sun ONE Directory Server Resource Kit。

调整系统设置

可以使用 idsktune 工具读取当前系统设置，并提供更改建议。总的来说，实施这些建议可以优化专门运行 Directory Server 的系统以及运行其他应用程序的系统的性能。

在实施特定的建议之前，应考虑本地网络情况和其他应用程序。有关其他网络调整的技巧，请参阅操作系统文档。

表 5-2 在部署之前要检查的配置文件

平台	文件	注释
Solaris 操作环境	/etc/init.d/inetinit	添加 ndd 语句以进行调整
	/etc/system	检查系统限制
	/etc/vfstab	确保文件是本地文件
HP-UX	/etc/rc.config.d/nddconf	添加 ndd 语句以进行调整 也可以使用 sam(1M)。

表 5-2　在部署之前要检查的配置文件 （续）

平台	文件	注释
Red Hat Linux	/etc/fstab	确保文件是本地文件
	/etc/security/limits.conf	添加 nofile 硬限制指令
	/etc/sysctl.conf	检查，设置内核参数
	/proc/sys/fs/file-max	检查文件描述符限制

(Windows) 延缓进程调用

在多处理器系统中， Windows 默认的延缓进程调用 (DPC) 处理 （用于处理传入网络通信的延期中断请求）可能会对性能产生负面影响。实际上，变成 DPC 的延期中断可能会从一个处理器重新调度到另一个处理器，从而产生大量的开销。为避免这些 DPC 开销问题，应将下列注册表项下的 ProcessorAffinityMask 的值设置为 0：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NDIS\Parameters

文件描述符

Directory Server 在处理并发客户机连接时使用文件描述符。如果将系统中可用的或某个进程可用的文件描述符的最大数量设置为比较低的值，则可以限制并发连接的数量。因此，有关文件描述符数量的建议涉及 Directory Server 能够在系统上处理的并发连接的数量。

在 Solaris 系统上，如 /usr/sbin/directoryserver idsktune （封装版本）或 idsktune （无软件包）的输出中所述，可用的文件描述符的数量可以使用 rlim_fd_max 参数进行配置。有关修改可用的文件描述符数量的进一步说明，请参阅操作系统文档。

修改了系统上的可用文件描述符的最大数量之后，请参阅表 9-2 （第 142 页）以了解有关配置 Directory Server 以使用可用的文件描述符的信息。

(HP-UX) 大文件支持

在某些 HP-UX 系统上，默认情况下不支持大文件。有关在计划安装 Directory Server 的文件系统上启用大文件支持的说明，请参阅 HP-UX 产品文档。 idsktune 公用程序的输出中也提供了有关说明。

(HP-UX) 线程挂起超时

正如 idsktune 公用程序所指出的，在某些 HP-UX 系统上，挂起超时的最大线程数可能设置不当。有关增大挂起超时的最大线程数的说明，请参阅 HP-UX 文档。idsktune 公用程序的输出中也提供了有关说明。

(HP-UX) 每个进程的线程数

正如 idsktune 公用程序所指出的，在某些 HP-UX 系统上，每个进程的最大线程数可能太低。有关增大每个进程的最大线程数的说明，请参阅 HP-UX 文档。idsktune 公用程序的输出中也提供了有关说明。

传输控制协议 (TCP) 设置

特定网络设置取决于平台。在某些系统上，可以通过修改 TCP 设置来提高 Directory Server 性能。本节讨论了 idsktune 有关 TCP 设置的建议背后的推理。

TIME-WAIT 状态中已关闭的连接

某些系统允许配置 TCP 连接在关闭后可保留在内核表中的时间长度。在保持连接期间，仍可以再次将其快速打开。当设置得太高时，系统可能会在比较长的时间间隔内跟踪内核表中的大量连接，从而减少 Directory Server 可用的连接数量。对于大多数部署，将此参数设置为 30 秒 （30,000 毫秒）以允许 Directory Server 有更多的并发连接。

在 Solaris 系统上，如 /usr/sbin/directoryserver idsktune （封装版本）或 idsktune （无软件包）的输出中所描述的，此时间间隔可以使用 tcp_time_wait_interval 参数进行配置。

连接挂起接受

某些系统允许配置 TCP 监听程序 （例如， Directory Server）接受挂起的 TCP 连接的数量。当设置得太低时，会限制 Directory Server 可以接受的挂起连接的数量。对于大多数部署，将此参数至少设置为 1024，以允许 Directory Server 处理更多的并发连接请求。

在 Solaris 系统上，如 /usr/sbin/directoryserver idsktune （封装版本）或 idsktune （无软件包）的输出中所描述的，所允许的挂起的连接数量可以使用 tcp_conn_req_max_q 参数进行配置。考虑将 tcp_conn_req_max_q0 增加到 2048。

延迟确认

对于未直接连接到系统的主机，某些系统允许配置延迟 TCP 确认的时间长度。不直接配置延迟时间，而如表 9-2 （第 142 页）中描述的位于 `cn=config` 时 `nsslapd-nagle` 设置为 `off`。

不活动的连接

某些系统允许配置 “保持连接”的数据包传输之间的时间间隔。此设置可确定当 TCP 连接处于不活动且潜在为断开的状态下保持该连接的时间长度。当设置得太高时，“保持连接”时间间隔可能会导致系统使用不必要的资源来为客户机保持连接，而此时客户机却已经断开了连接。对于大多数部署，将此参数设置为 600 秒（600,000 毫秒 = 10 分钟）以允许 Directory Server 有更多的并发连接。

在 Solaris 系统上，如 `/usr/sbin/directoryserver idsktune` （封装版本）或 `idsktune` （无软件包）的输出中所描述的，此时间间隔可以使用 `tcp_keepalive_interval` 参数进行配置。

传入连接

某些系统允许配置系统等待传入连接不发送确认的时间长度。当设置得太高时，这可能会导致在检测连接故障时出现长时间的延迟。对于快速而可靠的网络上的内部网部署，将此参数设置为 600 秒 （600,000 毫秒 = 10 分钟）可能会提高性能。

在 Solaris 系统上，如 `/usr/sbin/directoryserver idsktune` （封装版本）或 `idsktune` （无软件包）的输出中所描述的，此时间间隔可以使用 `tcp_ip_abort_interval` 参数进行配置。

传出连接

某些系统允许配置系统等待建立传出连接的时间长度。当设置得太高时，与目标服务器 （例如不能快速响应的副本）建立传出连接会产生长时间的延迟。对于快速而可靠的网络上的内部网部署，将此参数设置为 10 秒可能会提高性能。

在 Solaris 系统上，如 `/usr/sbin/directoryserver idsktune` （封装版本）或 `idsktune` （无软件包）的输出中所描述的，此时间间隔可以使用 `tcp_ip_abort_cinterval` 参数进行配置。

重新传输超时

某些系统允许配置重新传输数据包之间的初始时间间隔。此设置会影响重新传输未确认的数据包之前的等待时间。当设置得太高时，客户机可能会持续等待已丢失的数据包。对于快速而可靠的网络上的内部网部署，将此参数设置为 500 毫秒可能会提高性能。

在 Solaris 系统上，如 /usr/sbin/directoryserver idsktune （封装版本）或 idsktune （无软件包）的输出中所描述的，此时间间隔可以使用 tcp_rexmit_interval_initial 参数进行配置。

Windows 能够实现 Van Jacobson TCP 快速重新传输和恢复算法，以便在接收到 ACK 时快速重新传输缺少的段，而不必等待重新传输计时器到期。若要实现 Van Jacobson 算法，则请编辑注册表项：

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters

添加类型为 REG_DWORD 的 TcpMaxDupAcks。将该值设置为 ACK 的数量。范围为 1-3，默认值为 2。

序列号

某些系统允许配置系统处理初始序列号生成的方式。对于外联网和 Internet 部署，设置此参数以确保基于 RFC 1948 生成初始序列号以防止序列号攻击。

在 Solaris 系统上，如 /usr/sbin/directoryserver idsktune （封装版本）或 idsktune （无软件包）的输出中所描述的，此行为可以使用 tcp_strong_iss 参数进行配置。

第 6 章

调整缓存大小

Directory Server 将目录信息缓存到内存中或磁盘上，以便能够更快地对客户机请求作出响应。正确调整的缓存能够将处理客户机请求时对访问磁盘子系统的要求降至最低。

注意 除非正确调整缓存且工作正常，否则其他的调整可能仅会对性能产生有限的影响。

缓存类型

Directory Server 处理三种类型的缓存，如表 6-1 中所述。

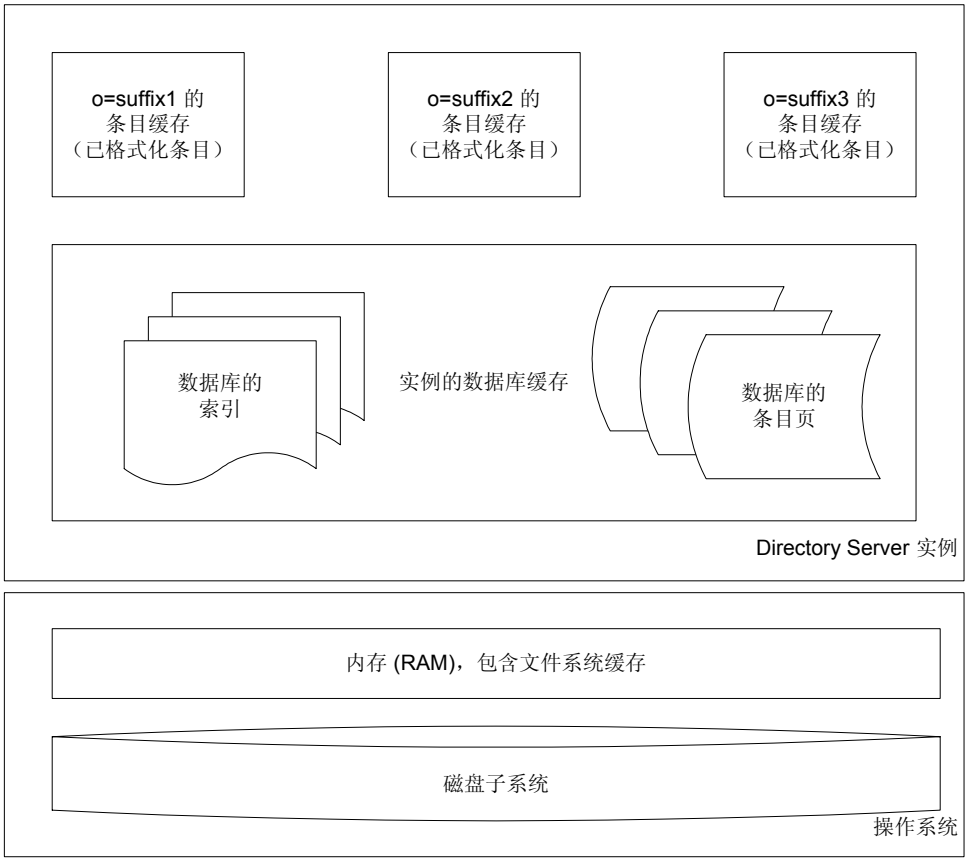
表 6-1 缓存

缓存类型	说明
数据库	每个 Directory Server 实例具有一个数据库缓存，以数据库格式存放索引和条目。
条目	每个后缀具有一个条目缓存，存放早先操作过程中从数据库检索到的条目，并将其格式化以便快速发送给客户机应用程序。
导入	每个 Directory Server 实例具有一个与数据库结构相似的导入缓存，在批量加载过程中使用。

Directory Server 也受益于基础操作系统处理的文件系统缓存，以及磁盘子系统中的 I/O 缓冲区。

图 6-1 显示了 Directory Server 处理三个后缀 （每个后缀具有其自己的条目缓存）实例的缓存。将该实例配置为处理大量磁盘活动，并如第 8 章 “调整日志记录”中所建议的那样将事务日志、数据库以及其他文件和日志置于单独的磁盘子系统上。

图 6-1 环境中的条目和数据库缓存



数据库缓存

每个 Directory Server 实例具有一个数据库缓存。数据库缓存可存放页面，此页面来自包含索引和条目的数据库。每页不是一个条目，而是包含部分数据库的内存扇区。指定数据库缓存大小 (`nsslapd-dbcachesize`)。对数据库缓存大小所作的更改在重新启动服务器以后生效，且服务器启动时分配数据库缓存空间。

Directory Server 在数据库文件和数据库缓存之间移动页面以保持最大数据库缓存容量。由于需要额外的内存来管理数据库缓存自身，因此 Directory Server 实际使用的内存数量可能多于指定的容量，达到 25%。

当使用容量极大的数据库缓存时，请在 Solaris 系统上凭经验测试和使用诸如 `pmap`(1) 的工具监视内存使用情况，确认 Directory Server 使用的内存没有超出可用物理内存的大小。超出可用物理内存造成系统重复地分页，导致性能严重降低。

也可将 Directory Server 支持的 `ps`(1) 公用程序 （位于 UNIX 平台上）与 `-p` *pid* 和 `-o` *format* 选项一起使用，以查看特定进程所使用的当前内存，例如 Directory Server (`ns-slapd`)。在 Windows 系统上，“任务管理器进程”选项卡页列出了每进程的内存使用情况 (`slapd.exe`)。详细信息，请参阅操作系统文档。

对于 32 位服务器，在实践中必须将数据库缓存大小限制为 2 GB 或更少。

注意 在 Windows 和 AIX 平台上，请不要为数据库缓存分配超过 1 GB （1,073,741,824 字节）。

有关 `nsslapd-dbcachesize` 值的有效范围的更多详细信息，请参阅 *Sun ONE Directory Server 参考手册*。

条目缓存

条目缓存存放最近访问的条目，并将其格式化以传递到客户机应用程序。指定后缀的条目缓存大小 (`nsslapd-cachememsize`) 和条目的最大数量 (`nsslapd-cachesize`)。条目缓存被按需分配。

随着格式化该缓存中的存储条目，Directory Server 可以极其高效地从条目缓存中返回条目。数据库中的条目存储为原始字符串字节，并且必须在传递到客户机应用程序之前格式化 （并存储在条目缓存中）。

指定条目缓存大小时，要清楚 `nsslapd-cachememsize` 表示 Directory Server 从基础内存分配库请求的内存大小。取决于内存分配库处理此类请求的方式，实际使用的内存可能比最终可用于 Directory Server 条目缓存的有效内存量大。

Directory Server 进程实际使用的内存主要取决于使用的内存分配库，以及条目缓存。通常，具有许多属性值小的条目比具有少量属性值大的条目需要更多开销。

对于 32 位服务器，在实践中必须将条目缓存大小限制为 2 GB 或更少。

注意 在 AIX 平台上，Directory Server 是使用 `maxdata = 0x50000000` 创建的，允许您为数据库缓存和条目缓存各分配 1 GB 的内存。如果必须更改 `maxdata` 的值，则请与 Sun ONE 支持代表联系。

有关 `nsslapd-cachememsize` 和 `nsslapd-cachesize` 值的有效范围的更多详细信息，请参阅 *Sun ONE Directory Server 参考手册*。

导入缓存

仅在后缀初始化过程中创建和使用导入缓存，也称为批量加载或导入。如果部署仅涉及 *offline* 后缀初始化，则不同时使用导入缓存和数据库缓存，所以无需如 “总聚合缓存大小”中所述的，在聚合缓存大小时同时添加它们。可以指定导入缓存大小 (`nsslapd-import-cachesize`)。对导入缓存大小的更改将在后缀下次重置和初始化时生效，同时为初始化分配导入缓存，然后在初始化之后释放该缓存。

Directory Server 处理导入缓存与处理数据库缓存的方法一致。这样就可以确保有足够的可用物理内存以防止交换。

对于 32 位服务器，在实践中必须将导入缓存大小限制为 2 GB 或更少。有关 `nsslapd-import-cachesize` 值的有效范围的更多详细信息，请参阅 *Sun ONE Directory Server 参考手册*。

文件系统缓存

操作系统将未被 Directory Server 缓存和其他应用程序使用的可用内存分配到文件系统缓存。该缓存存放最近从磁盘读取的数据，使得随后的请求可以获得从缓存复制的数据，而不是再次从磁盘读取数据。由于内存访问比磁盘访问快很多倍，所以保留一部分可用物理内存用于文件系统缓存可以增强性能。

有关文件系统缓存的详细信息，请参阅操作系统文档。

总聚合缓存大小

除去用于文件系统缓存的内存，同时使用的所有缓存的总和必须小于可用物理内存的总大小。对于 32 位服务器，这意味着总的聚合缓存大小在实践中必须限制为 2 GB 或更少。被使用的总缓存容量可能远远大于指定的容量。有关如何检查缓存大小及 Directory Server 进程大小没有超出可用物理内存的提示，请参阅 “数据库缓存”（第 100 页）。

注意 在 Windows 平台上，一个应用程序的最大可用地址空间为 2 GB。如果总聚合缓存大小超过该限制， Directory Server 显示一条错误信息并退出。

如果后缀在 Directory Server 联机时被初始化 （批量加载），那么数据库、条目和导入缓存大小的总和就应保持小于可用物理内存的总大小。

表 6-2 后缀初始化 （导入）操作和缓存使用

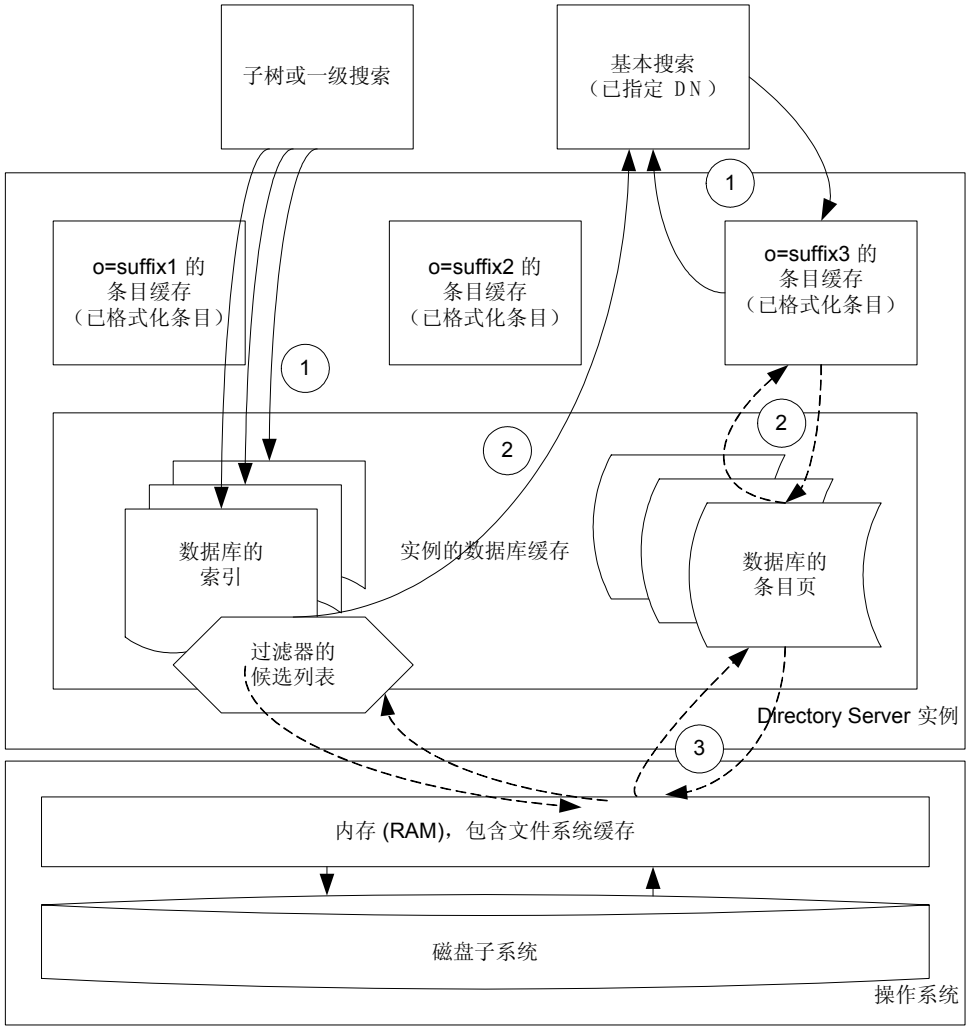
缓存类型	脱机导入	联机导入
数据库	否	是
条目	是	是
导入	是	是

如果所有后缀初始化在 Directory Server 停止的情况下脱机进行，您就可以避免此限制。在这种情况下，导入缓存与数据库缓存不能并存，因此可将同一内存分配给导入缓存以用于脱机后缀初始化，或者分配给数据库缓存用于联机使用。如果选择实现这一特殊情况，则请确保在生产系统上未执行联机批量加载。同时使用的缓存总和必须仍然保持小于可用物理内存的总大小。

搜索如何使用缓存

图 6-2 说明 Directory Server 如何处理指定基本 DN 的搜索和使用过滤器的搜索。单独的线代表访问不同级别内存的线程，断开的线代表通过有效调整减少的步骤。

图 6-2 搜索和缓存



基本搜索处理

如上所示，基本搜索 （指定基本 DN 的搜索）是 Directory Server 处理的最简单的搜索类型。要处理此类搜索， Directory Server：

1. 尝试从条目缓存检索具有指定基本 DN 的条目。

   如果在缓存中找到了条目， Directory Server 就会检查候选条目是否匹配为该搜索提供的过滤器。

   如果条目匹配，则 Directory Server 将把格式化的缓存条目快速返回到客户机应用程序。

2. 尝试从数据库缓存检索条目。

   如果在此找到了条目， Directory Server 就会将条目复制到后缀的条目缓存，然后进行处理，如同条目是在条目缓存中找到的一样。

3. 尝试从数据库本身检索条目。

   如果在此找到了条目， Directory Server 就会将条目复制到数据库缓存，然后进行处理，如同条目是在数据库缓存中找到的一样。

子树和一级搜索处理

同样如图 6-2 （第 104 页）中所示，在子树或者树一级上的搜索涉及处理条目集的其他处理。要处理此类搜索， Directory Server：

1. 尝试建立候选条目集，其中的条目与数据库缓存中索引的过滤器匹配。

   如果没有合适的索引存在，则候选条目集必须从数据库自身的相关条目生成。

2. 通过执行以下操作来处理每个候选条目：

   a. 执行基本搜索以检索条目。

   b. 检查条目是否匹配为该搜索提供的过滤器。

   c. 如果条目与过滤器匹配，则将条目返回到客户机应用程序。

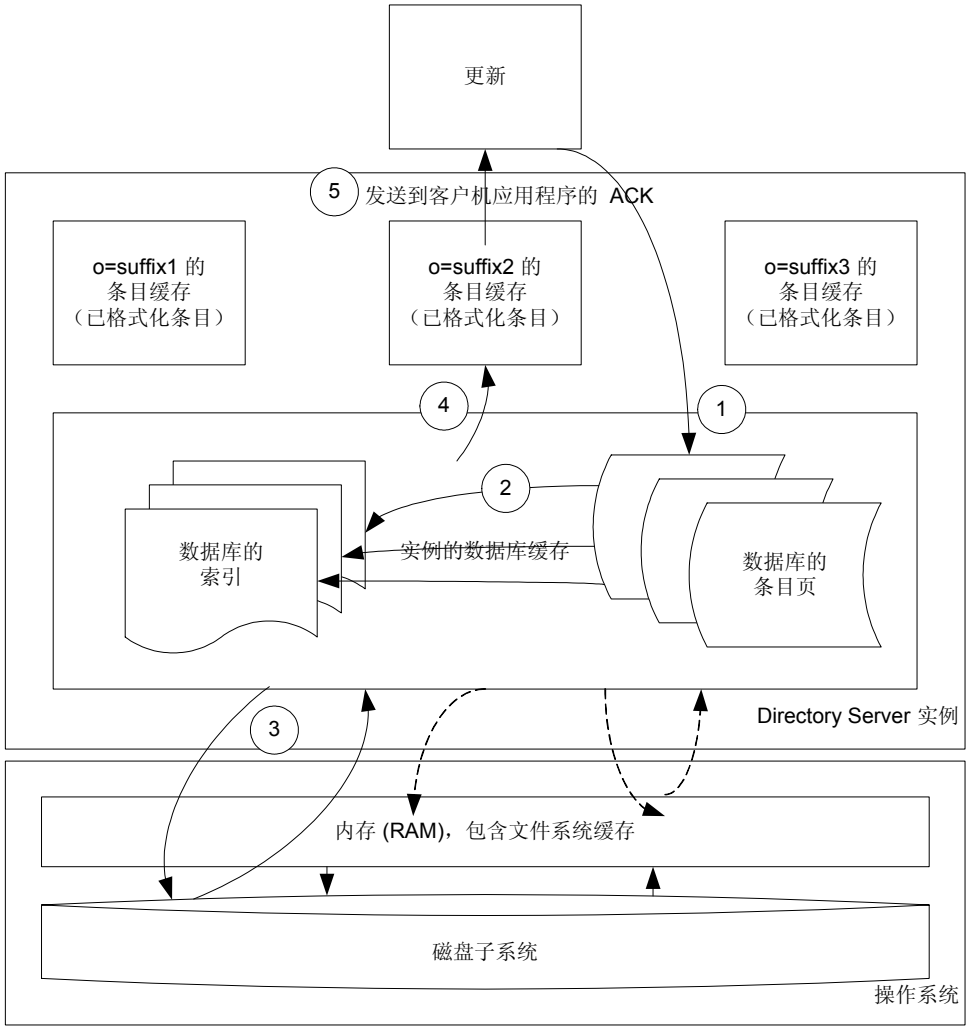
   这样， Directory Server 就避免了在内存中构造集。

理想情况下，您在调整 Directory Server 之前就知道将进行哪些搜索。在实践中，通过经验测试来验证假设。

更新如何使用缓存

图 6-3 说明 Directory Server 如何处理更新。单独的线代表访问不同级别内存的线程，断开的线代表通过有效调整减少的步骤。

图 6-3 更新和缓存



更新涉及比搜索更多的处理。要处理更新， Directory Server：

1. 执行基本 DN 搜索检索条目，以便在尚未存在的添加操作情况下更新或者验证。
2. 更改数据库缓存，尤其更新受更新影响的所有索引。

   如果受更新影响的数据未被加载到数据库缓存中，则当相关数据加载到缓存中时，该步骤会引起磁盘活动。

3. 将有关更改的信息写入事务日志，等待信息刷新到磁盘。

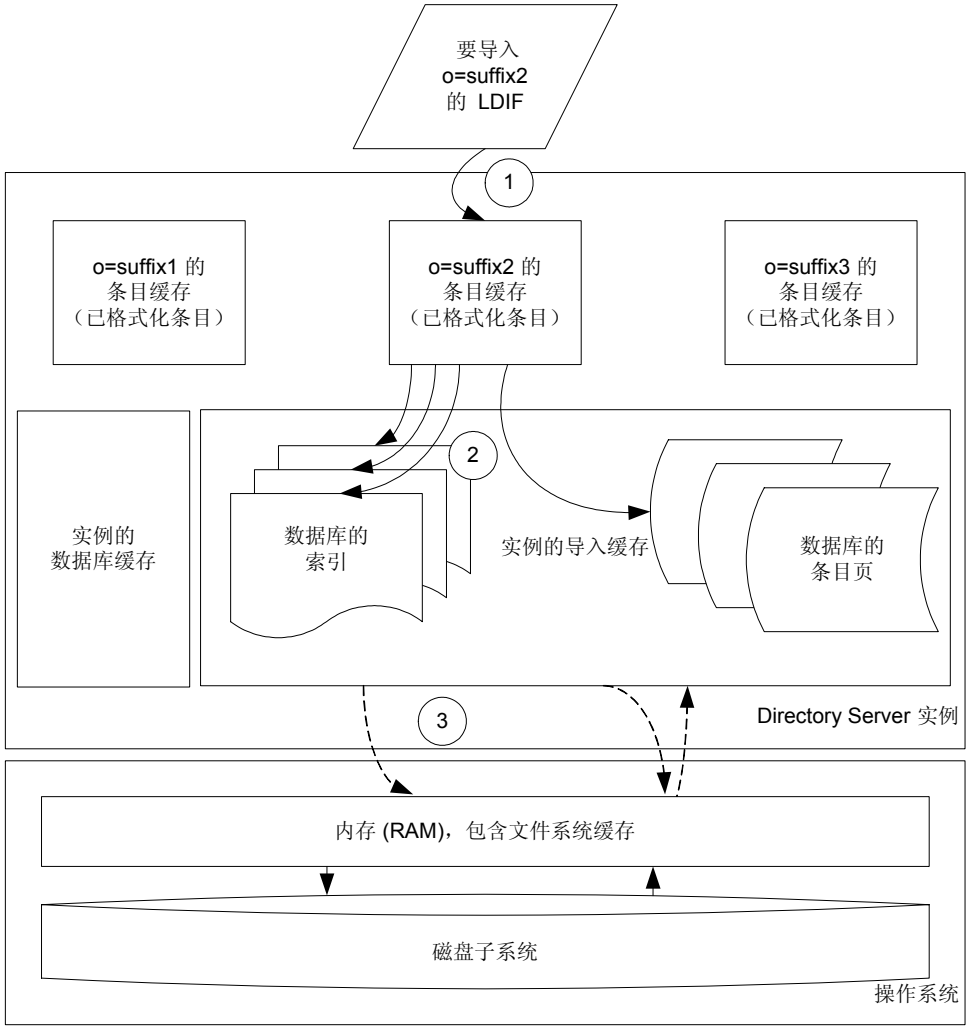
   详细信息，请参阅 “事务日志记录”（第 136 页）。

4. 将更新的条目格式化并复制到用于后缀的条目缓存。
5. 将成功更新的确认信息返回到客户机应用程序。

后缀初始化如何使用缓存

图 6-4 说明 Directory Server 如何处理后缀初始化，也称为批量加载导入。单独的线代表访问不同级别内存的线程，断开的线代表通过有效调整减少的步骤。

图 6-4 后缀初始化 （批量加载）和缓存



要初始化后缀， Directory Server：

1. 从 LDIF 启动一个线程，装入条目缓存，作为缓冲区使用。
2. 为每个受影响的索引启动一个线程，为在导入缓存中创建条目启动一个线程。这些线程会消耗装入到条目缓存中的条目。

3. 当导入缓存耗尽时，会从数据库文件读取和写入。

   Directory Server 可能还在后缀初始化期间写入日志消息，但不会写入事务日志。

用于后缀初始化的工具，如 Directory Server 包含的 `ldif2db` (`/usr/sbin/directoryserver ldif2db`)，它们提供有关缓存命中率和导入吞吐量的反馈。缓存命中率和导入吞吐量的同时降低意味着导入缓存可能太小。请考虑增加导入缓存大小。

为搜索进行优化

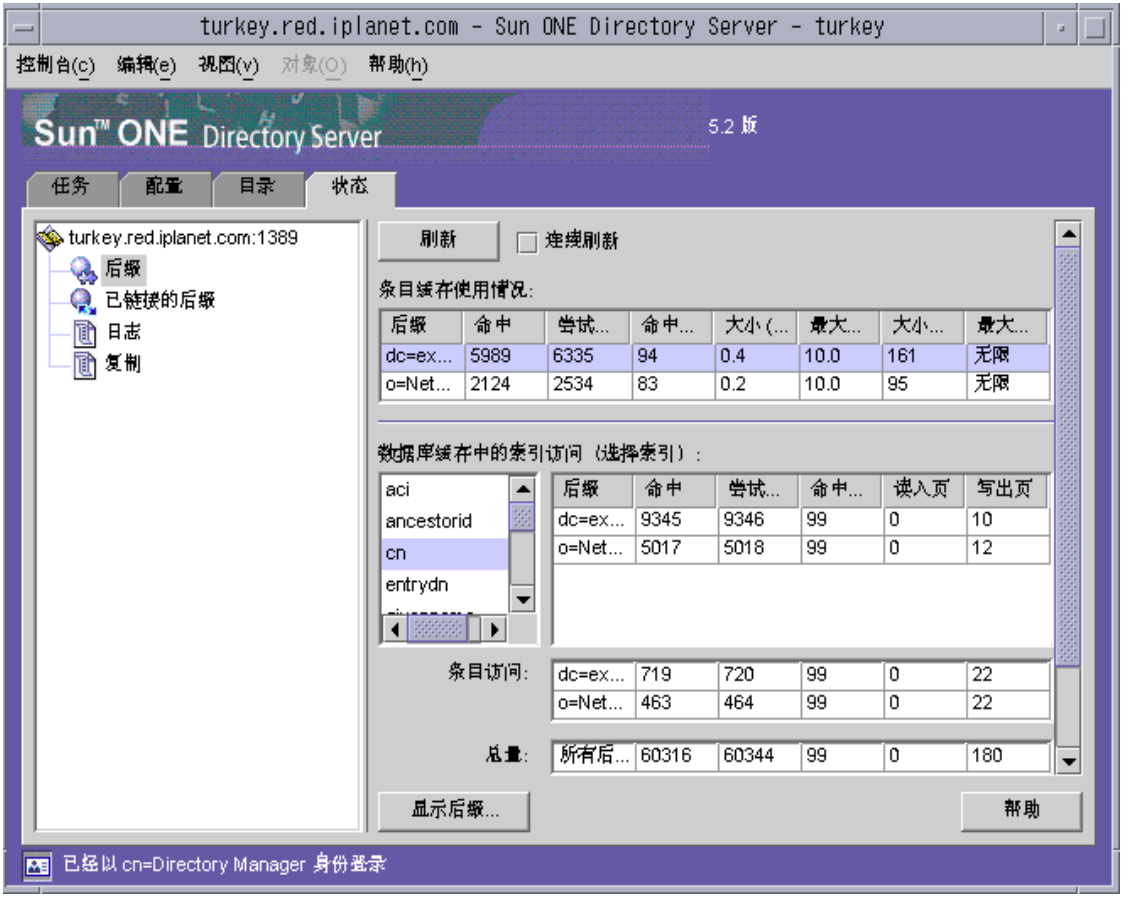
为获得最佳性能，请在内存中缓存尽可能多的目录数据。通过阻止目录从磁盘读取信息，可以限制磁盘 I/O 瓶颈。根据目录树的大小、可用内存数量和使用硬件的不同，要执行此操作可以有多种不同的方法。根据部署的不同，可以选择为条目和数据库缓存分配更多或更少的内存，从而优化搜索性能。也可以选择跨不同服务器上的 Directory Server 使用者分配搜索。

内存中的所有条目和索引

设想最佳情况。数据库和条目缓存适合可用的物理内存。条目缓存足够大，能够存放目录中的所有条目。数据库缓存足够大，至少可以存放所有索引。在这种情况下，搜索在缓存中找到所有所需的对象。 Directory Server 也无须到文件系统缓存或磁盘中检索条目。

在这种情况下，请确保即使更新后数据库缓存也能包含所有数据库索引。当数据库缓存中用于索引的空间耗尽后， Directory Server 必须从磁盘为每一个搜索请求读取索引，这样将严重影响吞吐量。 Directory Server Console 在 “状态”选项卡下显示命中率和其他有用信息，如图 6-5 中所示。

图 6-5 使用 Directory Server Console 监视缓存命中率



或者，搜索可以从命令行监视分页和缓存活动：

```
$ ldapsearch -D admin -w password \
-b cn=monitor,cn=database_name,cn=ldbm database,cn=plugins,cn=config
```

如果要粗略估计 .db3 文件中包含所有数据库索引所需的内存容量，以适合数据库缓存，请使用以下公式。对于与不具有大量二进制特性 （如照片）的典型条目一起使用的默认索引配置，该公式基本准确。

nsslapd-dbcachesize = 1.2 x SUM 所有 .db3 文件 （文件大小）

如果要粗略估计所有条目所需的条目缓存槽数目和内存数量，请使用以下公式。同样，对于与不具有大量二进制特性 （如照片）的典型条目一起使用的默认索引配置，该公式基本准确。

`nsslapd-cachesize = 4.5 x`（LDIF 中的条目数）

`nsslapd-cachememsize = 3.8 x`（id2entry.db3 文件大小）

通过经验测试验证和更正估计。特别是条目缓存可能使用比所分配给它们多很多的内存。

大量内存， 32 位 Directory Server

假设系统具有足够内存以容纳条目缓存和数据库缓存中的数据，但是不支持 64 位 Directory Server 进程。例如，如果硬件约束使您无法在 Solaris 系统上进行部署，则关键是按 32 位进程的内存限制对缓存大小进行相应调整，然后将可用内存留给文件系统缓存。

注意 可与系统上的其他进程共享文件系统缓存，特别是基于文件的操作。但是，这在很大程度上比其他缓存更难于控制，特别是在并非为 Directory Server 设计的系统上。

系统可能将文件系统缓存重新分配给其他进程。

更少内存、一些文件系统缓存

设想一个系统，其可用内存不足以将所有数据保存在条目和数据库缓存中，但仍然具有大量可用内存。在这种情况下，关键在于避免组合条目和数据库缓存的总大小超出可用物理内存，这样会造成过多的虚拟内存分页，从而导致系统进入虚拟中断。

请考虑将可用内存保留给文件系统缓存，将条目缓存和数据库缓存大小设置为低数值，如 500 KB。这样做可以允许系统在文件系统缓存中保留足够的数据以在此终止搜索，使 Directory Server 无需重复地从磁盘读取条目和索引。

或者，如果搜索模式不具备很强的随机性能，可以选择将条目和数据库缓存设置的高一些，假定特定部署中的大多数搜索都访问目录中所有条目的同一个小子集，且为这些搜索而缓存条目和索引带来的好处弥补处理偶然异常搜索请求的开销。通过经验测试验证和更正假设。

低内存、低文件系统缓存

设想一个系统，其可用内存不足以同时将数据存放到条目和数据库缓存中，但仍允许系统在文件系统缓存中缓存数据。这种情况的关键在于最大限度的利用可用内存。

请考虑设置尽可能低的条目和数据库缓存大小，为文件系统缓存留出尽可能多的内存。将内存保留给文件系统缓存至少可以阻止条目扩展到数据库，或条目的几率降低 3 到 4.5 倍，理论上限制了磁盘 I/O 活动。对于特定的部署，请通过经验测试验证该假设。

为更新进行优化

为获得最佳更新性能，请首先消除观察到的任何事务日志瓶颈。详细信息，请参阅“事务日志记录”（第 136 页）。

接下来，请尝试为数据库缓存提供足够的内存以在内存中处理更新，并将磁盘活动将为最低。可以通过读取 Directory Server Console 中的命中率来监视数据库缓存的效率。 Directory Server Console 在 “状态”选项卡下显示后缀的命中率，如图 6-5 （第 110 页）中所示。

最好还是尝试为文件系统缓存留出大量的可用内存。在 Directory Server 运行一段时间以后，文件系统缓存应该包含足够的条目和索引，从而无需再进行磁盘读取。更新应该影响内存中的数据库缓存，同时来自内存中大型数据库缓存的数据不会频繁的进行刷新。

将数据刷新到磁盘本身可能就是一个瓶颈，所以将数据库存储在单独的 RAID 系统（如 Sun StorEdge™ 磁盘阵列）上可以帮助提高更新性能。可以在 Solaris 系统上使用诸如 `iostat`(1M) 的公用程序以隔离潜在的 I/O 瓶颈。有关处理 Windows 系统上 I/O 瓶颈的详细信息，请参阅 Windows 帮助。

缓存填充和监视

*填充*缓存意味着使用数据填充它们，以使随后的 Directory Server 行为表现出正常的操作性能，而不是突然发生剧烈的变化。请在测量和分析潜在的优化之前填充缓存。

使用 `ldapsearch` 公用程序为后缀填充条目缓存。例如：

```
$ ldapsearch -D directoryManager -w password -b suffix objectclass=\* > /dev/null
```

执行搜索以填充数据库缓存，特别是将索引加载到缓存中。可以通过使用诸如 (mail=*) 的过滤器执行搜索，从而填充存在索引。对于其他索引，请考虑使用 Sun ONE Directory Server Resource Kit searchrate 公用程序应用过滤器格式，以搜索索引的每个特性所有可能的值。换句话来说，如果要为等式搜索检查 mail 特性的性能，例如，为每个邮件地址生成一个每行一个邮件地址的文件，然后使用 searchrate 公用程序执行使用该文件的搜索。例如：

```
$ searchrate -b suffix -f "(mail=%s)" -i mail.file -K -t 10
```

请考虑使用 -K 和 -t 以节省时间。当使用 -K 选项时， searchrate 保持连接打开，仅绑定一次，不是为每个搜索绑定。 -t 选项让您指定使用多少线程。有关 searchrate 公用程序的详细信息，请参阅 Sun ONE Directory Server Resource Kit 文档。可以按 “下载 Directory Server 工具”（第 12 页）中所述获得 Sun ONE Directory Server Resource Kit。

在填充了其他缓存后，可以填充可用的文件系统缓存。尽管无法保证文件系统缓存中的信息未被刷新，但填充文件系统缓存仍可提升发生剧烈变化的时间。要在 UNIX 系统上填充文件系统缓存，可作为超级用户使用 dd(1M) 命令。在 Solaris 系统上数据库文件位于默认位置，例如：

```
# for db in ServerRoot/slapd-serverID/db/*/*.db3
> do
> dd if=`pwd`/$db of=/dev/null bs=512k
> done
0+1 records in
0+1 records out
...
```

填充缓存后，可以运行测试并监视缓存调整是否产生了预期的效果。当在 “状态” 选项卡下选择 “后缀” 节点时， Directory Server Console 显示缓存的监视信息，如图 6-5 （第 110 页）中所示。或者，搜索可以从命令行监视分页和缓存活动：

```
$ ldapsearch -D admin -w password \
-b cn=monitor,cn=database_name,cn=ldbm\ database,cn=plugins,cn=config
```

如果数据库缓存大小足够大，且缓存已填充，则命中率 (dbcachehitratio) 将会很高，同时 (dbcachepagein) 中读取的页面数量和 (dbcacheroevict) 写出的干净页面将会很低。这里，必须理解 “高” 和 “低” 与部署限制有关。

如果后缀的条目缓存足够大且缓存已填充，则命中率 (entrycachehitratio) 将会很高。条目缓存大小 (currententrycachesize) 应该不超过最大大小 (maxentrycachesize) 的 80%。最后，条目 (currententrycachecount) 中的大小应该等于或非常接近于后缀中条目的总数。

其他优化

调整缓存大小仅代表改进搜索、更新或批量加载率的方法之一。随着对缓存进行调整，缓存的性能瓶颈转移到系统的其他部分。详细信息，请参阅本指南中的其他章节。

第 7 章

调整索引编制

随着 Directory Server 处理的条目越来越多，搜索可能消耗的时间和系统资源也越来越多。索引是提高搜索性能的一个工具。本章介绍 Directory Server 索引的工作方式，以便于您了解在特定部署环境中使用某种索引的利与弊。

关于索引

索引将查找信息和 Directory Server 条目关联起来。索引表现为 Directory Server 数据库中所存储的文件。此处的数据库是后缀的物理表现。对于大多数部署而言，一个后缀对应一个数据库。对于某些部署而言，一个后缀可能对应着多个数据库。默认情况下， Directory Server 将数据库存储在 *ServerRoot*/slapd-*ServerID*/db/（nsslapd-directory 的默认值）下。在这里，您可以发现单独的数据库实例，它们的每个已编制索引的属性都对应一个索引文件。例如，数据库 example 有一个 CN 索引文件，其中的条目来自后缀 dc=example,dc=com，那么它将被称为 *ServerRoot*/slapd-*ServerID*/db/example/example_cn.db3。

索引内容取决于客户机应用程序访问目录数据的方式。表 7-1 中包括标准索引类型的简要说明。

表 7-1 标准索引类型

索引类型	回答的问题 ...
近似	对于此属性，哪些条目的值与搜索值相类似？
浏览	哪些条目适合该虚拟列表视图搜索？
等式	对于此属性，哪些条目的值与搜索值等同？
国际	哪些条目匹配该国际区域？
存在	哪些条目具有此属性？

表 7-1 标准索引类型 （续）

索引类型	回答的问题 ...
子字符串	对于此属性，哪些条目的值符合 * 搜索值 * 的格式？

特定属性 （如 CN）的索引文件可能含有多种索引类型。例如，如果在 `example` 数据库中针对 CN 编制索引来实现等式和子字符串匹配，那么 `example_cn.db3` 中将同时包含等式和子字符串索引。

请参阅 *Sun ONE Directory Server 管理指南*，了解以下内容：

- 各种索引类型的概述
- 有关创建和删除索引的说明
- 由 Directory Server 创建的默认索引列表
- Directory Server 所需的系统索引列表

在许多情况下，默认索引都可提高搜索性能，并且还为其他应用程序 （如消息发送）提供了一定的支持。在某些情况下，出于性能考虑，您可以选择禁用甚至删除特定的默认索引。系统索引是 Directory Server 依赖的索引。请不要将其删除或进行修改。

优点：搜索使用索引的方式

索引可提高搜索的速度。索引中包含一系列的值，每个值又关联到与该值对应的条目标识符列表。 Directory Server 可以使用索引中的条目标识符列表快速查找条目。如果没有用来管理条目列表的索引，那么 Directory Server 就必须检查后缀中的每个条目，来找出搜索的匹配结果。

编制了索引的搜索比没有编制索引的搜索所需的处理工作量要少得多；我们只需分析一下搜索请求的处理方式，就可以明白其中的原因。 Directory Server 处理每个搜索请求的方式如下：

1. 客户机应用程序将搜索请求发送到 Directory Server。
2. Directory Server 检查请求，确保搜索基础与它能够处理的某个后缀相对应。如果不对应，那么它将向客户机返回一个错误消息，同时可能会返回一个到其他 Directory Server 实例的引用。

3. Directory Server 检查它所管理的索引中是否有哪一个适用于此次搜索。

   对于存在的每个此类索引， Directory Server 都会查找其中的候选条目 - 可能与搜索请求相匹配的条目，如图 6-2 （第 104 页）中所示。

   请注意，如果没有这样的索引，那么 Directory Server 会以数据库中的所有条目为基础生成候选条目集。对于大型部署，本步骤可能会消耗相当多的时间和系统资源，具体情况因搜索任务而各有不同。

4. Directory Server 检查每个候选条目，确定它们是否与搜索条件匹配。找到匹配条目后， Directory Server 会将其返回到客户机应用程序。

   Directory Server 继续检查候选对象，直至所有候选对象检查完毕，或者达到了某项资源限制 （如 `nsslapd-lookthroughlimit`、`nsslapd-sizelimit`、或 `nsslapd-timelimit`），具体内容在 “限制客户机可用的资源”（第 139 页）中有所描述。

从步骤 3 中可明显看出，索引能够显著地减少 Directory Server 在响应客户机搜索请求时需执行的处理任务。

缺点：更新时索引如何处理

更新不仅更改条目本身，还更改引用这些条目的索引。索引中对某一条目的引用越多，更新期间修改索引的潜在处理成本就越高。特别地，在向客户机应用程序发送更新确认之前，Directory Server 需要修改所有受到影响的索引，如图 6-3（第 106 页）所示。

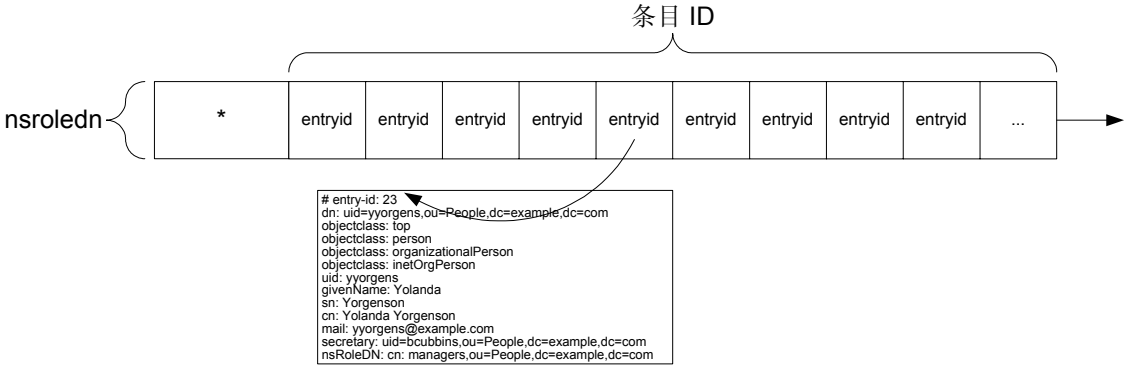
除了索引维护的处理成本之外，其他成本还包括磁盘空间和可能的内存空间成本。如 “为搜索进行优化”（第 109 页）中所述，在优化用于搜索的数据库缓存大小时，您可能倾向于提供足够容量的内存，以便在数据库缓存中同时容纳条目和索引。索引越大，所需的空间也就越大。而且 64 位索引需要的空间要比 32 位索引大。

一般来说，对某个 Directory Server 实例的索引进行调整，就是要对索引进行筛选，确保它们在实现更快搜索方面的优点能够抵消更新开销和空间占用方面的不足。维护有用的索引是一种很好的做法；而维护客户机很少搜索的闲置属性索引则是一种浪费。

存在索引

图 7-1 显示了 `nsRoleDN` 属性的存在索引；可以看到此索引与属性值无关，而只是包括了数据库中具有 `nsRoleDN` 属性的所有条目。属性的每个值都匹配 `*`。

图 7-1 存在索引的例子



如上所示，内部 `entryid` 属性值允许 Directory Server 存储条目的引用，以便进行快速检索。事实上， Directory Server 使用 *dbinstance*`_id2entry.db3` 索引文件来检索条目，其中的 *dbinstance* 取决于 “关于索引”（第 115 页）中介绍的数据库标识符。

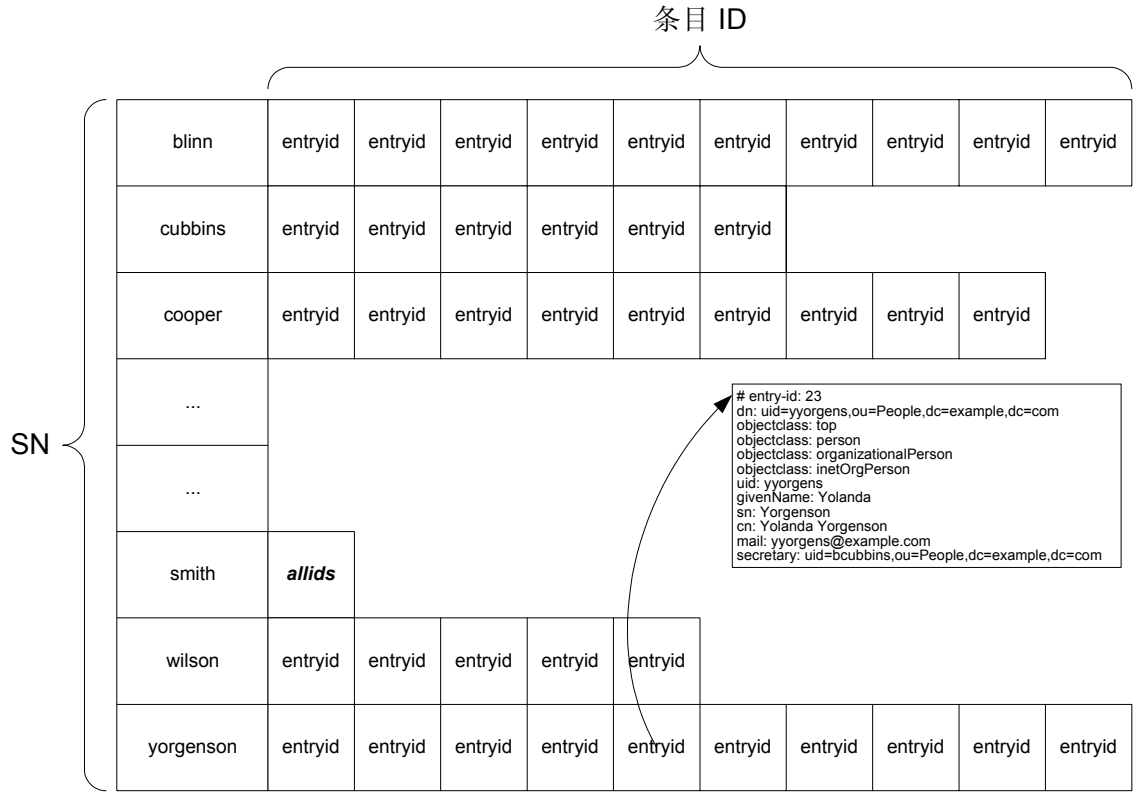
当 Directory Server 接收到请求，要更新具有存在索引属性的条目时，它必须确定该条目是否必须从索引中删除，并且必须执行所有必要的修改，然后才能向客户机应用程序返回更新确认。

存在索引的成本一般要比其他索引类型低，但它要维护的条目列表可能很长。

等式索引

图 7-2 显示了 `SN` （姓氏）属性的等式索引。可以看到对于此索引中的每一个属性值，都有一个以此值为 `SN` 属性值的项目的列表与之对应。

图 7-2 等式索引的例子



当 Directory Server 接收到请求，要对具有等式索引属性的条目进行更新时，它必须确定是否必须将该条目从索引中删除，是否必须向索引中添加一个列表或从索引中删除某个列表，并且在将更新确认返回给客户机应用程序之前，必须完成所有必要的修改。

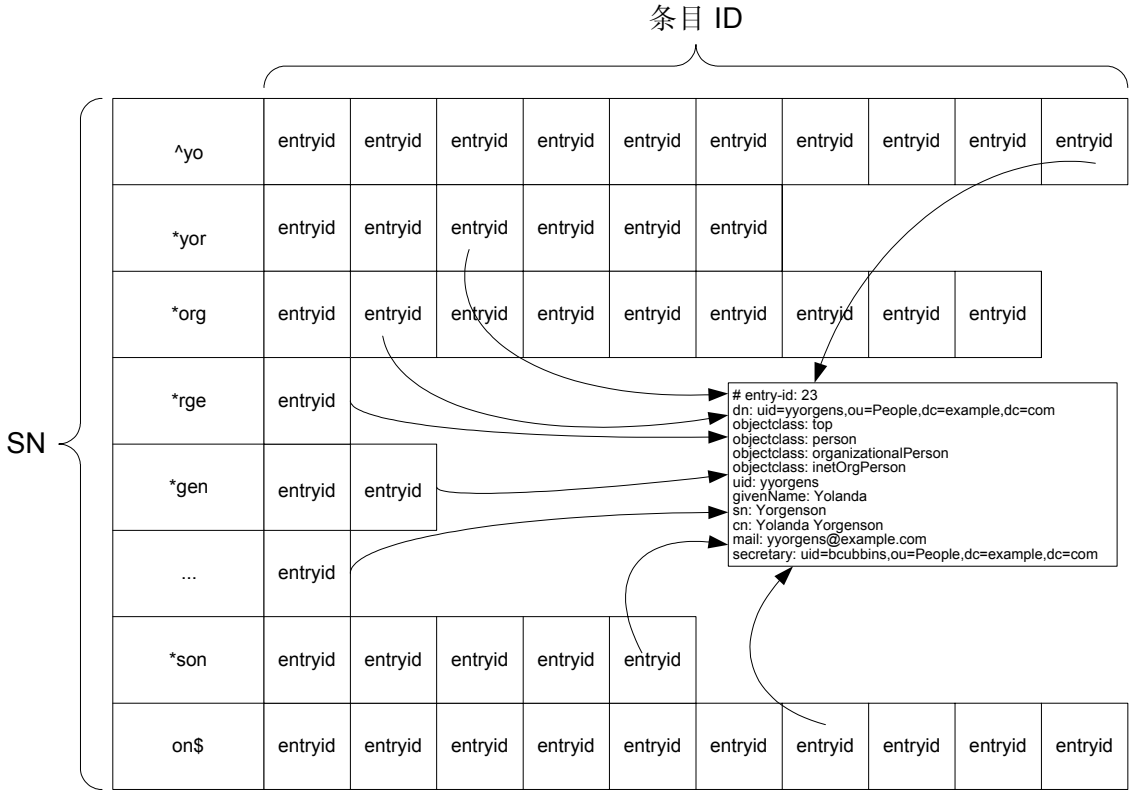
等式索引的成本一般比子字符串索引低，但在空间方面的要求要比存在索引高。不过，某些客户机应用程序 （如消息服务器）可能会依靠等式索引来获得顶级的搜索性能。请不要对照片和加密口令这样的大型二进制属性使用等式索引。

子字符串索引

图 7-3 显示了 SN（姓氏）属性的子字符串索引。它通过摘要说明了此索引如何根据属性值维护一系列列表。

Directory Server 编制的子字符串索引使您能够在索引中查找双字符的子字符串。例如，使用索引可加快搜索（sn=*ab*）的速度，但不能加快搜索（sn=*a*）的速度。

图 7-3　　子字符串索引的例子



Directory Server 还提供了进一步的优化，允许您对字符串首字母加通配符的子字符串进行搜索。例如，当子字符串索引可用时，可以加快（sn=a*）搜索的速度，但（sn=*a*） 或（sn=*a）则不行。

请注意， Directory Server 根据其内置的规则构建子字符串的索引。这些子字符串不可以通过系统管理员配置。

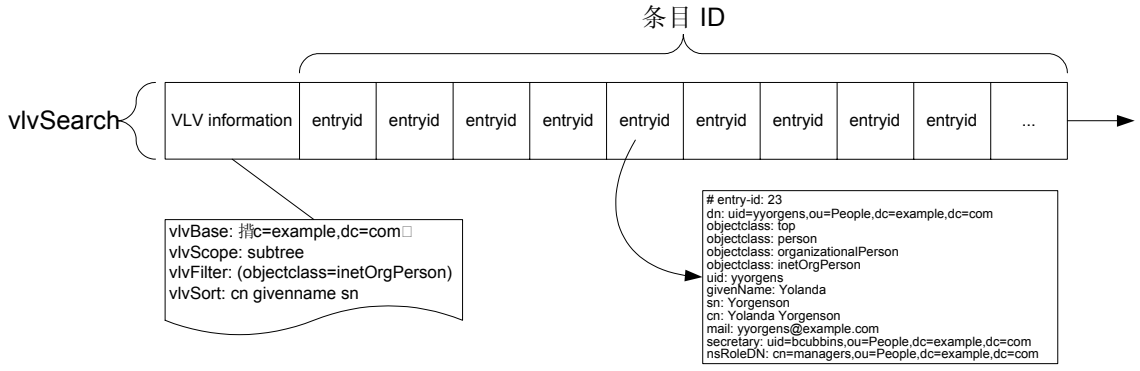
当 Directory Server 接收到请求，要对具有子字符串索引属性的条目进行更新时，它必须确定该条目是否必须从索引中删除、条目的更改是否以及如何影响索引、是否必须向索引中添加条目 ID 或从索引中删除条目 ID 列表；并且在将更新确认返回给客户机应用程序之前，它必须执行所有必要的修改。更新的数目取决于属性值字符串的长度。

一般而言，维护子字符串索引的成本相当高。因为该成本是编制索引的字符串长度的函数，所以应避免使用不必要的子字符串索引；对于可能具有长字符串值的属性（如 `description`）更是如此。子字符串索引不能应用于二进制属性，如照片。

浏览 （虚拟列表视图）索引

图 7-4 显示了虚拟列表视图的浏览索引。它说明了此索引如何利用虚拟列表视图的信息。具体讲，就是用于实现浏览索引的 `vlvBase`、 `vlvScope`、 `vlvFilter` 和 `vlvSort` 属性值。此类索引中的条目 ID 根据 `vlvSort` 标准进行排序。

图 7-4 浏览索引的例子



当 Directory Server 接到请求，要对与某个 `vlvFilter` 值相匹配的条目进行更新时，它必须确定该条目是否一定要从索引中删除，必须找出条目在列表中的正确位置，并且必须在将更新确认返回给客户机应用程序之前执行所有必要的修改。

近似索引

Directory Server 使用变音位语音算法的一种变体来维护近似索引。此算法将属性字符串的值分解成与其大致近似的英语语音发音。传入的搜索请求中要匹配的值也使用同一算法进行处理。因为此算法不严格地基于音节，所以对于含有电话号码等数字的属性无效。

该算法为每个属性值字符串生成一个目标字符串。因此，这种英语字符串的 “音似”索引编制方法，其成本与等式索引类似。

国际索引

国际索引使用特定区域设置的匹配规则来维护索引。因此，这种索引的成本近似于子字符串和等式索引的成本。

通过使用自定义的匹配规则服务器插件，可以对国际索引其他类型索引的标准支持进行扩展。有关自定义匹配规则插件的详细信息，请参阅 *Sun ONE Directory Server Plug-In API 编程指南*。

示例：编制条目索引

假设有一个后缀，其多项属性已编有索引，其中包括：对 uid 编制了等式索引；对通用名称 (cn) 和姓氏 (sn) 属性编制了等式、子字符串和近似索引；对 mail 属性编制了等式索引；对 telephoneNumber 属性编制了等式和子字符串索引；以及对 description 属性编制了子字符串索引。现在要将如下所示的用户条目加入其中。

代码示例 7-1　　用户条目样例

```
dn:uid=yyorgens,ou=People,dc=example,dc=com
objectclass:top
objectclass:person
objectclass:organizationalPerson
objectclass:inetOrgPerson
uid:yyorgens
givenName:Yolanda
sn:Yorgenson
cn:Yolanda Yorgenson
mail:yolanda.yorgenson@example.com
telephoneNumber: 1-650-960-1300
description:Business Development Manager, Platinum Partners
```

添加此条目时， Directory Server 必须修改 cn、 sn、 mail、 telephoneNumber 和 description 的索引。表 7-2 中列出了预计的条目数。

表 7-2　　用户条目样例的索引更新

属性	近似	等式	子字符串[1]	总索引更新
uid		1		1
cn	1	1	17	19
sn	1	1	9	11

表 7-2 用户条目样例的索引更新 （续）

属性	近似	等式	子字符串[1]	总索引更新
mail		1		1
telephoneNumber		1	11	12
description			47	47

1. 对于像此处的 description 字符串这样的长字符串来说，在大多数部署中，不推荐使用子字符串索引。

可以看到， description 字符串的子字符串索引更新数 (47) 大于所有其他属性更新数目的总和 (44)。并且，如果对 description 字符串作进一步的修改，那么将再次使更新数目达到最大值甚至更多；具体数目还取决于新的字符串。在大多数情况下，对于像 description 这样的长字符串值，不要使用子字符串索引。

调整索引编制来改善性能

在很多情况下，为改善性能而调整索引编制意味着激活常用搜索的索引以提高速度，同时停用那些维护成本高但却不常用的索引。

注意 数据库备份中包括索引，所以应该与 Directory Server 的配置相匹配。

在更改了索引的配置方式后，应同时备份配置和数据。

对于那些包含专门应用于特定应用程序的复制副本的大型部署而言，可以选择为不同的 Directory Server 实例配置不同的索引。例如，可考虑如下拓扑：

- 主机只负责处理写入任务
- 集线器负责处理到使用者的复制任务
- 某些使用者专门用于特定应用程序 （如消息发送）

在这种情况下，主机并不处理搜索，因此可选择不在主机上维护高成本的子字符串索引。您也可以确定还有哪些索引很少使用，并将其停用。

实际上，除了管理请求外，集线器不会接到其他客户机请求，因而在这种情况下可以停用除 Directory Server 本身所需的系统索引外的所有其他索引。

在专门用于个别应用程序的特定使用者上，您可以停用所有该应用程序不使用的索引。具体停用哪些索引取决于特定应用程序所执行的搜索。

只允许执行编制了索引的搜索

Directory Server 能够防止执行成本很高的未编制索引的搜索；它将向那些请求执行未编制索引的搜索的客户机返回 LDAP_UNWILLING_TO_PERFORM。

要防止对特定数据库执行未编制索引的搜索，可将该数据库的 nsslapd-require-index 属性值设置为 on：

```
$ ldapmodify -h host -p port -D "cn=directory manager" -w password
dn:cn=example,cn=ldbm database, cn=plugins, cn=config
changetype:modify
replace:nsslapd-require-index
nsslapd-require-index:on
^D (^Z on Windows systems)
```

更改会立即生效。无需重新启动 Directory Server。

限制索引表的长度

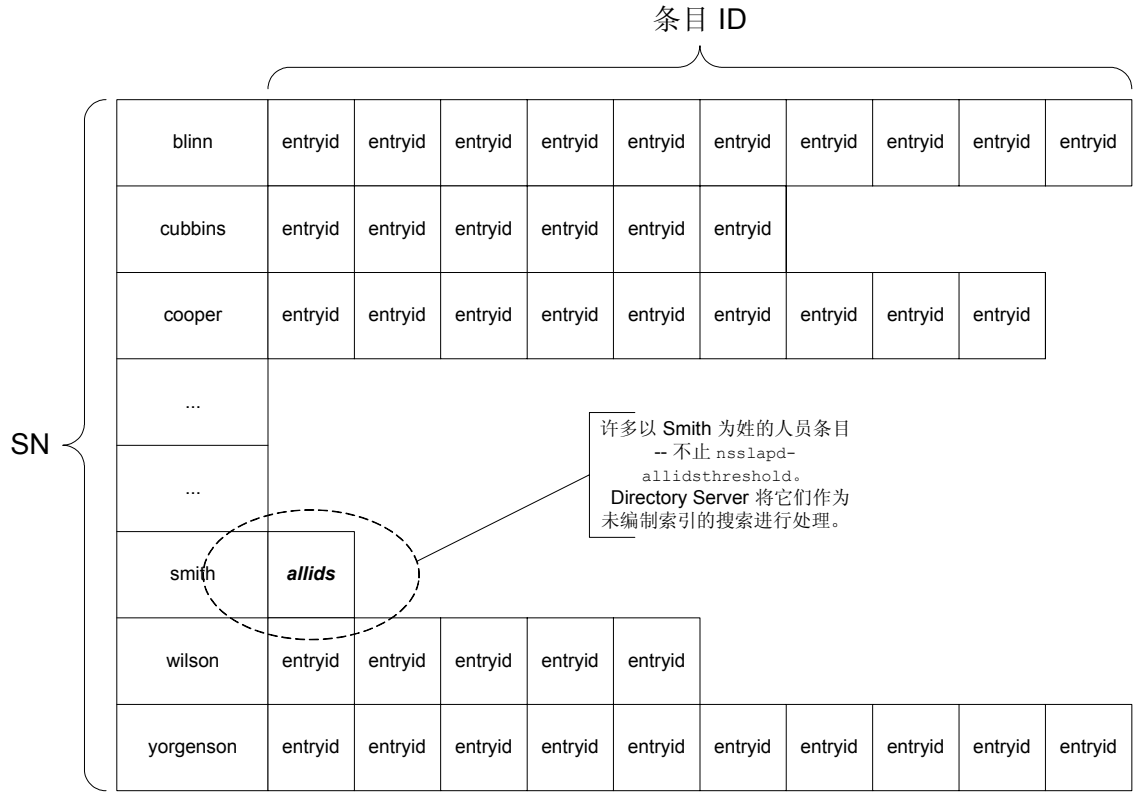
在规模较大、增长迅速的目录部署中，特定索引关键字的索引可能会到达一个效率递减点。在效率递减点，与特定关键字相关联的列表会变得很长，以致于维护该列表的成本超过了偶尔对该关键字执行未编制索引的搜索来查找候选条目的成本。例如，有一个对姓氏进行了等式索引编制的超大型电话簿应用程序。假设该电话簿中有很多个 Smith，以致于维护 Smith 索引耗用的成本超过了它在加速查找方面的益处。此时， Directory Server 应停止编制 Smith 姓氏的索引，但应继续编制其他姓氏的索引。

Directory Server 具备一种处理此类问题的机制。可为配置属性设置临界值。如果特定关键字列表中的条目数达到了所设置的值，那么 Directory Server 将把该关键字列表替换为一个令牌，指明在查找该关键字的候选条目时应执行未编制索引的搜索。该值应当接近但小于此次搜索候选条目的最大个数；请使用 nsslapd-lookthroughlimit 来进行设置，具体内容见于表 9-1 （第 140 页）。

该机制被称为全部 ID 临界值，其由来是设置全局临界值所使用的配置属性的名称，cn=config,cn=ldbm database,cn=plugins,cn=config 时的 nsslapd-allidsthreshold。注意该值当前对于 Directory Server 实例是全局的。它不可以为不同索引设置不同值。

图 7-5 显示了为姓氏编制索引时， Smith 的个数超出 nsslapd-allidsthreshold 的情况。

图 7-5 达到某个索引关键字的全部 ID 临界值



请注意，临界值只影响索引表中的一个列表。其他关键字列表不受影响。

索引表大小不当的症状

如果客户机主要执行编制了索引的搜索，并且缓存大小也按照第 6 章 “调整缓存大小”中所述进行了正确的调整，但是搜索性能仍然不理想，则可能是由于临界值设置的不合适导致的。当发现已编制索引的搜索性能不佳时，请首先确认缓存大小是否已进行了适当的调整。接下来，检查 access 日志，看 Directory Server 是否经常达到全部 ID 临界值。

access 日志 RESULT 消息末尾的 notes=U 标记指明， Directory Server 执行了未编制索引的搜索。其前面属于同一连接与操作的 SRCH 消息中指出了所使用的搜索过滤器。以下两行示例记录了对 (cn=Smith) 的未编制索引搜索，该搜索返回了 10000 个条目。消息中的时间戳已经被删除。

```
conn=2 op=1 SRCH base="o=example.com" scope=0 filter="(cn=Smith)"
conn=2 op=1 RESULT err=0 tag=101 nentries=10000 notes=U
```

如果发现许多应为已编制索引的搜索中存在这样的记录对，那么就表明增大临界值可能会提高搜索性能。

更改索引表临界值的大小

比较理想的 `nsslapd-allidsthreshold` 值通常处于目录条目总数 5% 的范围内。例如，默认值 4000 一般适用于处理 80,000 或更少条目的 Directory Server 实例。如果预计近期将把大量条目添加到目录中，或者预计目录将会显著增加，那么可以将该值设置为远远高于 5%。也可以将支持许多搜索的使用者副本上的临界值设置为其他值，使之不同于仅支持写入的主机上的临界值。如果计划近期将从 LDIF 中重新初始化一个大型的目录，那么您可以选择在重新初始化之前调整 `nsslapd-allidsthreshold` 的值，因为对此属性值的每次更改都要求重建全部索引。在任何情况下都不要将全部 ID 临界值设置得很高 （50,000 以上），即使对于大型部署也是如此，除非您有极其充分和具体的理由。

全部 ID 临界值的更改方法如下。请注意，接受更改的 Directory Server 实例上的服务将发生中断。

1. 将需要做更改的 Directory Server 实例停止。
2. 将所有的目录数据库导出到 LDIF。

   详细信息，请参阅 *Sun ONE Directory Server 管理指南*。
3. 仔细调整 `nsslapd-allidsthreshold` 属性的值，该值位于 *ServerRoot*`/slapd-`*ServerID*`/config/dse.ldif` 中。
4. 从 LDIF 重新初始化所有目录数据库。

   详细信息，请参阅 *Sun ONE Directory Server 管理指南*。
5. 如果您曾为旧的全部 ID 临界值调整过数据库缓存大小，并且服务器也有充足的物理内存，那么可以考虑提高数据库的缓存大小，增幅比例为临界值增幅比例的 25%。

   换句话说，如果将全部 ID 临界值从 4000 增加到 6000，那么可以将数据库缓存大小增加 12.5%，以适应索引表大小的增加。在将更改应用到生产服务器之前，请根据经验找到最佳大小。有关数据库缓存调整的详细信息，请参阅第 6 章 “调整缓存大小”。
6. 重新启动 Directory Server 实例。

解决索引碎片问题

支持大型索引和高更新率的 Directory Server 实例可能会产生大量的索引关键字碎片。大量的索引关键字碎片会降低性能，即使数据库大小稳定也是如此。如果您认为大量的索引关键字碎片显著影响了服务器的性能，那么可以考虑重新生成受影响的索引以减少碎片。

有关创建索引的详细信息，请参阅 *Sun ONE Directory Server 管理指南*。

第 8 章

调整日志记录

Directory Server 提供多种日志类型，表 8-1 中对这些类型进行了概述。本章讨论如何处理不同类型的日志。

表 8-1 Directory Server 使用的日志类型

日志	类型	用途
访问	平面文件	评估目录使用模式，验证配置设置，诊断访问问题。
审核	平面文件	提供审核跟踪，以确保安全性和数据完整性。
更改日志	数据库	在副本间启用同步
错误	平面文件	调试目录部署。
回退更改日志	数据库	允许与先前版本实现向后兼容。
事务	数据库	维护数据库完整性。

在高容量部署中，写入日志可能会引发大量磁盘操作，从而对性能造成明显的负面影响。由于在高容量系统中作频繁记录可能会造成 I/O 瓶颈，所以应考虑将日志放在使用单独磁盘控制器的单独物理磁盘中。

访问日志记录

访问日志中包含客户机连接和已执行操作的详细信息。在诊断访问问题、验证服务器配置设置以及评估服务器使用模式时，访问日志往往是不可缺少的。不过，对于大多数部署，默认日志记录级别会导致磁盘活动频繁，而磁盘活动量太大可能会对服务器性能造成消极影响。

尽管访问日志提供了有益的疑难解答信息，但是它也可能成为 I/O 瓶颈。一旦目录部署完毕，并且运行时没有出现错误或性能问题，则应考虑禁用访问日志记录。如果生产环境要求使用访问日志记录，那么应将日志记录级别设为所需的最低级别。此外，还应考虑将访问日志放在单独的物理磁盘或具有较大 I/O 缓冲区的快速磁盘子系统中。表 8-2 提供了针对特定属性的进一步建议。

表 8-2 访问日志记录的调整建议

配置属性（ dn:cn=config 时）	简短说明和调整建议
nsslapd-accesslog	指定访问日志文件的路径和文件名。 对于低容量部署，访问日志可以与审核和错误日志共享一个磁盘。 对于高容量部署，应考虑将访问日志放在单独的磁盘或磁盘子系统中，并使用单独的控制器。选择具有大 I/O 缓冲区的磁盘。
nsslapd-accesslog-level	指定所使用的信息记录的级别。 除非需要较高的级别，否则请将其更改为 0，表示不使用访问日志记录，（默认设置为 256，表示记录对条目的访问）。
nsslapd-accesslog-logbuffering	确定是否缓存访问日志。 除非必须禁用缓存，以便在访问日志消息被触发时及时查看，否则请保留 on （默认值）。禁用缓存可能会导致整体性能下降。
nsslapd-accesslog-logging-enabled	启用和禁用访问日志记录。 切换为 off （默认值为 on），以获得最佳性能。 如果部署要求启用访问日志记录，则请将 nsslapd-accesslog-level 设置为可接受的最低设置，并将访问日志放在单独的磁盘或磁盘子系统中。经常轮换访问日志 （每天或每周），并使用 nsslapd-accesslog-logmaxdiskspace 和 nsslapd-accesslog-logminfreediskspace 来管理磁盘空间的使用。

表 8-2 访问日志记录的调整建议 （续）

配置属性 （ dn:cn=config 时）	简短说明和调整建议
nsslapd-accesslog-logmaxdiskspace	指定全部访问日志 （当前的和轮换的日志）可以占用的最大磁盘空间。 此值应低于访问日志记录的专用磁盘空间总量。 如果使用同一磁盘来保存审核、访问和错误日志记录，那么应确保有足够的磁盘空间来保存所有这三种日志。 如果访问日志驻留在单独的磁盘上，那么应将此变量设置为该磁盘的大小。
nsslapd-accesslog-logminfreediskspace	指定在清除旧日志之前允许达到的最低可用磁盘空间。 当可用磁盘空间量低于此属性上指定的值时，最旧的访问日志将被删除，直到释放出足够的磁盘空间来满足此属性的设置。如果由于磁盘已满而不能写入访问日志，那么服务器就会关闭。

有关单个配置属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册*。

Sun ONE Directory Server Resource Kit 文档中包含从访问日志中抽取的信息。详细信息，请参阅 “下载 Directory Server 工具”（第 12 页）。

审核日志记录

审核日志中包含有关对各数据库及服务器配置所作全部更改的详细信息。默认情况下，禁用审核日志记录。

当在大修改量的部署中启用时，审核日志记录可能会导致整体性能显著下降。除非部署中需要审核日志，否则请保留其禁用状态。对于需要审核日志记录的大容量部署，应考虑为审核日志分配一个位于单独的控制器上的独立磁盘。表 8-3 提供了针对特定属性的进一步建议。

表 8-3 审核日志记录的调整建议

配置属性 （dn:cn=config 时）	简短说明和调整建议
nsslapd-auditlog	指定审核日志文件的路径和文件名。 对于低容量部署，审核日志可以与访问和错误日志共享一个磁盘。 对于高容量部署，应考虑将审核日志放在单独的磁盘中，并使用单独的控制器。选择具有大 I/O 缓冲区的磁盘。
nsslapd-auditlog-logging-enabled	启用和禁用审核日志记录。 除非需要审核日志记录，否则请保留 off （默认设置）。
nsslapd-auditlog-logmaxdiskspace	指定全部审核日志 （当前的和轮换的日志）可以占用的最大磁盘空间。 此值应低于审核日志记录的专用磁盘空间总量。 如果使用同一磁盘来保存审核、访问和错误日志记录，那么应确保有足够的磁盘空间来保存所有这三种日志。 如果审核日志驻留在单独的磁盘上，那么应将此变量设置为该磁盘的大小。
nsslapd-auditlog-logminfreediskspace	指定在清除旧日志之前允许达到的最低可用磁盘空间。 当可用磁盘空间量低于此属性指定的值时，最旧的审核日志将被删除，直到释放出足够的磁盘空间来满足此属性的设置。如果由于磁盘已满而不能写入审核日志，那么服务器将会关闭。

有关单个配置属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册*。

错误日志记录

Directory Server 实例的错误日志中包含正常服务器操作期间出现的错误、警告和通知消息的详细信息。默认的低日志记录级别产生的磁盘活动相对较少。

不过，当设置较高日志级别以生成调试信息时， Directory Server 可能会开始将大量消息写入磁盘中。写入负载可能会导致整体性能显著下降。为避免性能下降，应渐进地增加日志级别，逐个完成组件，而不是一次激活所有组件的日志级别。

错误日志不支持日志缓存。所有消息都会立即写入磁盘。对于大容量部署，应考虑为错误日志分配单独的控制器上的独立磁盘，以便在各种需要进行调试的情况下使用。表 8-4 提供了针对特定属性的进一步建议。

表 8-4 错误日志记录的调整建议

配置属性 （dn:cn=config 时）	简短说明和调整建议
nsslapd-errorlog	指定错误日志文件的路径和文件名。 对于低容量部署，错误日志可以与访问和审核日志共享一个磁盘。 对于高容量部署，应考虑将错误日志放在单独的磁盘中，并使用单独的控制器。选择具有大 I/O 缓冲区的磁盘。
nsslapd-errorlog-logging-enabled	启用和禁用错误日志记录。 保留 on （默认设置）。
nsslapd-errorlog-logmaxdiskspace	指定全部错误日志 （当前的和轮换的日志）可以占用的最大磁盘空间。 此值应低于错误日志记录专用的磁盘空间总量。 如果使用同一磁盘来保存审核、访问和错误日志记录，那么应确保有足够的磁盘空间来保存所有这三种日志。 如果错误日志驻留在单独的磁盘上，那么应将此变量设置为该磁盘的大小。
nsslapd-errorlog-logminfreediskspace	指定在清除旧日志之前允许达到的最低可用磁盘空间。 当可用磁盘空间量低于此属性指定的值时，最旧的错误日志将被删除，直到释放出足够的磁盘空间来满足此属性的设置。如果由于磁盘已满而不能写入错误日志，那么服务器将会关闭。

表 8-4 错误日志记录的调整建议 （续）

配置属性 （dn:cn=config 时）	简短说明和调整建议
nsslapd-infolog-area	指定需要记录通知消息的组件。 除非需要对某个组件进行调试，否则请保留 0 （默认值）。在生产服务器上应避免一次为多个组件进行设置。
nsslapd-infolog-level	指定所使用的信息记录的级别。 除非在调试某个组件时，仅设置 nsslapd-infolog-area 无法生成足够的详细信息，否则请保留 0 （默认值）。

有关单个配置属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册*。

多主服务器复制更改日志记录

Directory Server 使用一个复制更改日志在副本间启用同步。有关更改日志的详细讨论，请参阅 *Sun ONE Directory Server 部署指南* 有关配置的详细信息，请参阅 *Sun ONE Directory Server 参考手册*。表 8-5 提供了特定属性的更多建议。

表 8-5 多主服务器更改日志记录的调整建议

配置条目 DN 和配置属性	简短说明和调整建议
dn:cn=changelog5,cn=config nsslapd-cachememsize	指定更改日志数据库缓存大小。 请考虑更改默认的 10 MB 以进行高容量部署。
dn:cn=changelog5,cn=config nsslapd-changelogdir	指定更改日志数据库的路径和文件名。 请考虑将更改日志放在单独的磁盘或磁盘子系统中，并使用单独的控制器。使用大的 I/O 缓冲区可能会有所帮助。
dn:cn=changelog5,cn=config nsslapd-changemaxage	指定更改日志中条目的最大存留期。 将 0 （默认值，表示无最大存留期）更改为一个时间间隔，达到此时间间隔后复制的服务器完全同步，并整理更改日志。

表 8-5 多主服务器更改日志记录的调整建议 （续）

配置条目 DN 和配置属性	简短说明和调整建议
dn:cn=changelog5,cn=config	指定更改日志中条目的最大数量。
nsslapd-changemaxentries	将此设置从 0 （默认值，表示不存在最大值）更改为某个数值，足以使修整更改日志之前允许复制服务器完全同步。
dn:cn=changelog5,cn=config	指定更改日志数据库缓存中条目的最大数量。
nsslapd-cachesize	将此设置从 -1 （默认值，表示不存在最大值）更改为条目刷新之前更改日志中保留的条目的最大数量。

有关单个配置属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册*。

回退更改日志记录

Directory Server 附带了一个回退更改日志插件，启用后可以记录供应商服务器上的更改；记录的格式与以前的 Directory Server 4.x 版本兼容，并且可通过 LDAP 访问。回退更改日志插件默认情况下是禁用的，除兼容性需要外不应启用。请参阅 *Sun ONE Directory Server 参考手册* 以了解详细信息。表 8-6 提供了针对特定属性的进一步建议。

表 8-6 回退更改日志记录的调整建议

配置条目 DN 和配置属性	简短说明和调整建议
dn:cn=Retro Changelog Plugin,cn=plugins,cn=config nsslapd-changelogdir	指定回退更改日志的路径和文件名。 请考虑将回退更改日志放在单独的磁盘或磁盘子系统中，并使用单独的控制器。使用大的 I/O 缓冲区可能会有所帮助。
dn:cn=Retro Changelog Plugin,cn=plugins,cn=config nsslapd-changelogmaxage	指定回退更改日志中条目的最大存留期。 将此设置从 0 （默认值，表示不存在最大存留期）更改为某个时间间隔，经过此时间间隔后，使用回退更改日志的客户机处理完生成的日志条目。

表 8-6 回退更改日志记录的调整建议 （续）

配置条目 DN 和配置属性	简短说明和调整建议
dn:cn=Retro Changelog Plugin,cn=plugins,cn=config nsslapd-changelogmaxentries	指定回退更改日志中条目的最大数量。 将此设置从 0 （默认值，表示不存在最大值）更改为修整之前回退更改日志中保留的条目的最大数量。

有关单个配置属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册*。

事务日志记录

Directory Server 通过事务日志记录来维护数据库的完整性。当接受更新操作 - add、 modify、 delete 或 modrdn 时， Directory Server 会将有关该操作的日志消息写入事务日志中。默认情况下启用的持久事务日志记录可确保数据的完整性。其具体方法是：确保将每个更新操作都提交到磁盘上的事务日志中，然后再将更新操作的结果代码返回给客户机应用程序。在发生系统崩溃的情况下， Directory Server 会使用事务日志来恢复数据库。由于事务日志有助于异常关闭的数据库的恢复，所以应考虑将事务日志和目录数据库存储在不同的磁盘子系统中。

事务日志记录会引发大量磁盘操作，特别是在启用持久性的情况下。这很可能成为更新操作的主要性能瓶颈。将事务日志和数据库分别存储在不同的 RAID 系统 （如 Sun StorEdge 磁盘阵列）中，不仅有助于在发生系统崩溃的情况下更好地保护数据完整性，还可以提高更新操作的性能。表 8-7 提供了针对特定属性的进一步建议。

表 8-7 事务日志记录的调整建议

配置条目 DN 和配置属性	简短说明和调整建议
dn:cn=config,cn=ldbm database,cn=plugins,cn=config nsslapd-db-checkpoint-interval	指定一个时间间隔，让 Directory Server 按此间隔定点检查事务日志，确保整个数据库系统与磁盘同步，并对事务日志进行清理。 请保留 60 （默认间隔，以秒为单位），除非基于经验测试的数据库性能优化工作表明应采用不同的值。增大此属性的值可能会使更新操作的性能提高，但也意味着非正常关机之后的恢复过程将花费更长的时间，且事务日志会占用更多的磁盘空间。

表 8-7 事务日志记录的调整建议 （续）

配置条目 DN 和配置属性	简短说明和调整建议
dn:cn=config,cn=ldbm database,cn=plugins,cn=config nsslapd-db-durable-transaction	指定在将结果代码发送给客户机之前是否应将更新操作提交到磁盘上的事务日志中。 对于数据完整性要求较高的部署，请保留 on （默认值）。对于某些部署，可以禁用持久的事务日志记录，以提高性能。不过，在禁用之后，那些已清空到文件系统但还没有记入磁盘的日志消息可能会在发生系统崩溃的情况下丢失。这意味着，在持久的事务日志记录被设置为 off 的情况下，即便客户机接收到了成功更新的结果代码，某些更新也可能是无法恢复的。
dn:cn=config,cn=ldbm database,cn=plugins,cn=config nsslapd-db-logdirectory	指定事务日志的路径和文件名。 应考虑将事务日志存储在单独的快速磁盘或磁盘子系统中，并使用单独的控制器。

有关单个配置属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册* 。

第 9 章

管理其他资源的使用情况

在优化缓存大小、属性值索引和日志管理之后，调整 Directory Server 限制客户机应用程序可用的资源的方式，以及 Directory Server 使用系统资源的方式是有用的。重新配置甚至禁用作为 Directory Server 插件提供的某些功能也可能是有用的。

限制客户机可用的资源

默认配置可能允许客户机应用程序使用多于实际需要的 Directory Server 资源。这种情况可能会容许客户机应用程序通过以下手段意外或故意地滥用资源，从而对服务器性能产生负面影响：打开许多连接，然后让这些连接空闲或不使用；启动开销大且不必要的无索引搜索；或将大量未计划的二进制属性值存储在目录中。

在某些部署情况下，不建议修改默认配置。对于选择不更改本节提及的配置属性值的部署，可以考虑使用 Sun ONE Directory Proxy Server 软件在外部设置限制，以帮助防止拒绝服务攻击。

在某些部署情况下，Directory Server 的一个实例必须支持占用目录比较严重的客户机应用程序（如消息服务器），以及临时的目录客户机应用程序（如用户邮件应用程序）。在这种情况下，如 *Sun ONE Directory Server 管理指南* 中所述，请考虑使用基于绑定 DN 的资源限制，来提高针对占用目录比较严重的应用程序的单个限制。

表 9-1 中的建议讨论了针对于限制所有客户机应用程序可用资源的设置。这些限制不应用于目录管理员用户，因此请确保客户机应用程序没有作为目录管理员用户连接。

表 9-1 针对限制客户机可用资源的调整建议

配置条目 DN 和属性	简短说明和调整建议
`dn:cn=config` `nsslapd-idletimeout`	以秒为单位设置一个时间值，在该时间之后 Directory Server 关闭空闲客户机连接。这里的*空闲*是指连接保持打开状态，但没有请求任何操作。默认情况下，未设置时间限制。 某些应用程序（如消息服务器）可能会在通讯量比较低时打开连接池，该连接池仍然处于空闲状态，但是不应该关闭。理想情况下，此时可专门使用一个副本以支持应用程序。如果不可行，则应考虑使用基于绑定 DN 的限制。 在任何情况下，将此值设置得很高并不会关闭其他应用程序期望其保持打开状态的连接，但如果将此值设置得很低，则无法让连接保持空闲状态。应考虑使用 120 秒（2 分钟）作为优化测试的起点。
`dn:cn=config` `nsslapd-ioblocktimeout`	设置以毫秒为单位的时间值，在该时间之后 Directory Server 关闭被阻塞的客户机连接。这里的被阻塞 是指服务器被阻止向客户机发送输出，或者被阻止从客户机读取输入。 对于特别容易遭受拒绝服务攻击的 Directory Server 实例，应考虑将此值设置成比默认值 1,800,000 毫秒（30 分钟）低的值。
`dn:cn=config,cn=ldbm database,cn=plugins,cn=config` `nsslapd-lookthroughlimit`	设置候选条目的最大数量，在搜索期间要对这些条目执行检查以便进行匹配。 某些应用程序（如消息服务器）可能需要搜索整个目录。理想情况下，此时可专门使用一个副本以支持应用程序。如果不可行，则应考虑使用基于绑定 DN 的限制。 在任何情况下，都应考虑从默认值 5000 条目降低此值，但不能低于 `nsslapd-sizelimit` 的阈值。
`dn:cn=config` `nsslapd-maxbersize`	以字节为单位设置传入消息的最大大小。 Directory Server 会拒绝添加大于此限制的条目的请求。 如果您确信能够准确地预测目录数据的最大条目大小，则应考虑将此值从默认值 2097152 (2 MB) 更改为所需的最大目录条目的大小。

表 9-1 针对限制客户机可用资源的调整建议 （续）

配置条目 DN 和属性	简短说明和调整建议
dn:cn=config	设置每个客户机连接的最大线程数。
nsslapd-maxthreadsperconn	某些应用程序 （如消息服务器）可以打开一个连接池，而且可以在每个连接上发出多个请求。理想情况下，此时可专门使用一个副本以支持应用程序。如果不可行，则应考虑使用基于绑定 DN 的限制。 如果预测某些应用程序可以对每个连接执行许多请求，则应考虑从默认值 5 增大此值，但不能超过 10。通常不建议为每个连接指定 10 个以上的线程。
dn:cn=config	设置 Directory Server 响应搜索请求而返回的最大条目数。
nsslapd-sizelimit	某些应用程序 （如消息服务器）可能需要搜索整个目录。理想情况下，此时可专门使用一个副本以支持应用程序。如果不可行，则应考虑使用基于绑定 DN 的限制。 在任何情况下，都应考虑将此值降为比默认值 2000 低的值。
dn:cn=config	设置 Directory Server 用于处理一个搜索请求的最大秒数。
nsslapd-timelimit	某些应用程序 （如消息服务器）可能需要执行非常大的搜索。理想情况下，此时可专门使用一个副本以支持应用程序。如果不可行，则应考虑使用基于绑定 DN 的限制。 在任何情况下，都应将此值设置得尽可能低，同时还应满足部署要求。对于许多部署，默认值 3600 秒 （1 小时）稍大，而实际不需要这么大。应考虑使用 600 秒 （10 分钟）作为优化测试的起点。

有关单个配置属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册* 。

使用可用的系统资源

根据部署要求，可以选择调整 Directory Server 实例使用系统和网络资源的方式、管理访问控制的方式，以及配置服务器插件的方式。表 9-2 中的建议讨论了针对系统资源的设置。

表 9-2 针对配置系统资源的使用情况的调整建议

属性 （dn:cn=config 时）	简短说明和调整建议
nsslapd-listenhost	设置用于 Directory Server 进行监听的 IP 接口的主机名。此属性为单值。 默认行为是在所有接口上进行监听。默认行为适合于使用冗余网络接口以提高可用性和吞吐量的高容量部署。 在多宿主系统上部署时，或者当在通过单独的接口支持每个协议的系统上只监听 IPv4 或 IPv6 通信时，应考虑设置此值。当使用 SSL 时，应考虑设置 nsslapd-securelistenhost。
nsslapd-maxdescriptors	设置 Directory Server 试图使用的文件描述符的最大数量。 Directory Server 使用文件描述符处理客户机连接，并在内部维护文件。如果错误日志指出 Directory Server 有时由于没有足够的文件描述符可用而停止监听新连接，则增大此属性的值可以增大 Directory Server 能够同时处理的客户机连接的数量。 如果已经如 “文件描述符”（第 94 页）中所述增大了系统上可用的文件描述符的数量，则应相应地设置此属性的值。此属性的值应该小于或等于系统上可用的文件描述符的最大数量。
nsslapd-nagle	设置是否在套接字级别延迟发送 TCP 数据包。 保留 off （默认值），以便在将结果发送到客户机应用程序时防止协议级别的延迟。

表 9-2 针对配置系统资源的使用情况的调整建议 （续）

属性 （dn:cn=config 时）	简短说明和调整建议
nsslapd-reservedescriptors	设置 Directory Server 所维护的用于管理索引、复制以及其他内部处理的文件描述符的数量。 Directory Server 不使用这样的文件描述符来处理客户机连接。 如果下列所有情况皆为真，则应考虑将此属性的值设置为大于默认值 64。 • Directory Server 复制到 10 个以上的使用者或 Directory Server 维护 30 个以上的索引文件。 • Directory Server 处理大量的客户机连接。 • 错误日志中的消息表明 Directory Server 已为与客户机连接*不*相关的操作用完了文件描述符。 注意，随着预留的文件描述符的数量增大，处理客户机连接可用的文件描述符的数量会减少。如果增大此属性的值，则应考虑增大系统上可用的文件描述符的数量，并且增大 nsslapd-maxdescriptors 的值。 如果决定更改此属性，则针对要预留的文件描述符数量的初步估计，应尝试将 nsslapd-reservedescriptors 的值设置为： 20 + 4 *（数据库的数量） +（索引的总数） +（nsoperationconnectionslimit 的值）*（链接后端的数量） + ReplDescriptors + PTADescriptors + SSLDescriptors 其中，如果使用复制，则 *ReplDescriptors* = 供应商副本的数量 + 8 ；如果 Pass Through Authentication (PTA) 插件已启用，则 *PTADescriptors* 为 3 （否则为 0）；如果使用 SSL，则 *SSLDescriptors* 为 5 （否则为 0）。 除非实例被配置为每个后缀使用多个数据库，否则，数据库的数量与实例的后缀数量相同。通过经验测试对估计进行验证。
nsslapd-securelistenhost	设置用于 Directory Server 进行监听 SSL 连接的 IP 接口的主机名。此属性为单值。 默认行为是在所有接口上进行监听。以对待 nsslapd-listenhost 相同的方式考虑此属性。

表 9-2 针对配置系统资源的使用情况的调整建议 （续）

属性 （dn:cn=config 时）	简短说明和调整建议
nsslapd-threadnumber	设置 Directory Server 使用的线程数。 如果下列条件皆为真，则应考虑调整此属性的值： • 客户机应用程序执行许多费时的操作 （如同时进行更新或复杂的搜索）。 • Directory Server 支持许多同时发生的客户机连接。 • Directory Server 处理 5,000,000 个以上的条目。 多处理器系统能够比单处理器系统维持更大的线程池。作为优化此属性值时的初步估计，可以使用两倍处理器的数量或 20 + 同时更新的数量。如表 9-1 中所讨论，还可考虑调整每个客户机连接的最大线程数 nsslapd-maxthreadsperconn。处理客户机连接的这些线程的最大数量不能超过系统上可用的文件描述符的最大数量。在某些情况下，减少而不是增加该属性的值将很有用。 通过经验测试对估计进行验证。结果不仅取决于特定的部署情况，而且还取决于基础系统。

有关单个配置属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册* 。

管理访问控制

Directory Server 目前为访问控制指令 (ACI) 提供性能和可伸缩性改进 （如增强的内存管理以及对宏 ACI 的支持）。虽然有这些改进，但是 Directory Server 还会使用大量的系统资源来评估复杂 ACI。因此，复杂 ACI 的广泛使用会给性能带来负面影响。

宏 ACI 帮助您限制所使用的 ACI 的数量。通过限制 ACI 的数量，可使访问控制更易于管理，并可减少系统上的负载。宏是表示 ACI 中的 DN （或 DN 的部分）的占位符。可以在 ACI 目标、 ACI 绑定规则中或同时在这两者中使用宏。当 Directory Server 接收请求时，它会对照结果操作所针对的资源检查哪些 ACI 宏匹配。如果一个宏匹配， Directory Server 就将它替换为实际 DN 的值。然后 Directory Server 对 ACI 进行常规评估。有关 ACI 的详细信息，请参阅 *Sun ONE Directory Server 管理指南*。

测试结果已经表明， Directory Server 能够支持 50,000 个以上的 ACI。各种部署情况对性能的影响当前尚在分析中。应尽可能将 ACI 的数量设置得小一点，以限制对性能造成的负面影响，并降低管理访问控制的复杂性。对于涉及复杂 ACI 环境的部署，应考虑使用 Sun ONE Directory Proxy Server 提供某些访问控制功能。

配置服务器插件

Directory Server 使用插件来实现许多关键功能 （如访问控制、复制、语法检查和属性唯一性）。在特定部署的环境中，您可能会发现重新配置某些插件是很有用的。表 9-3 中的建议讨论了针对某些标准插件的设置。

表 9-3 针对某些标准插件的调整建议

名称和 DN	简短说明和调整建议
7 位检查插件 `dn:cn=7-bit check,cn=plugins,cn=config`	允许 Directory Server 检查属性是否为 7 位干净值。换言之，提供的属性值只包含适合 7 位编码的那些字符。 如果基础结构设计用于支持较宽的编码 （如日语字符），则可以选择禁用此插件 （默认为 on）。
遗留复制插件 `dn:cn=Legacy Replication Plugin,cn=plugins,cn=config`	允许 Directory Server 作为 4.x 供应商的使用者来工作。 除非您希望在更新期间使用 Directory Server 作为 4.x 供应商的使用者，否则请关闭插件 （默认设置为 on，以便在需要 4.x 复制功能时使用）。
引荐完整性插件 `dn:cn=referential integrity postoperation,cn=plugins,cn=config`	允许 Directory Server 确保保持相关条目之间的关系。例如，当从目录中删除用户条目或重命名用户条目时，该用户所属的组便会按需要更新，而无需手动干预。 在所有主服务器上启用并配置此插件。 如果选择启用该插件，则请为配置为与该插件一起使用的所有属性创建等同性索引。该插件在搜索要更新的条目时使用此类索引。若没有它所使用属性的等同性索引，则该插件必须执行开销大的无索引搜索，从而会给性能带来负面影响。 有关配置和启用该插件的说明，请参阅 *Sun ONE Directory Server 管理指南*。

有关单个配置属性的详细信息，请参阅 *Sun ONE Directory Server 参考手册* 。

已安装产品的布局

本附录概述了在典型安装之后产品的软件布局。在已安装的文件中，只有此处列出并在产品文档中讨论的文件属于受支持的公用产品界面。

注意 此处显示的示例反映了 Solaris 操作环境的产品安装。对于在其他平台上的安装，文件名和扩展名可能有所不同。

在安装产品的 Solaris 封装版本之后，还可以使用 `pkgchk`(1M) 公用程序、`pkgchk -v` *package-name* 获得特定软件包的安装路径名称的完整列表。

诸如 Solaris 操作环境之类的某些平台提供了用于管理目录服务的集成工具。 Sun ONE Directory Server 也提供了这样的工具。有关此处列出的工具的详细信息，请参阅 *Sun ONE Directory Server 管理指南* 和 *Sun ONE Directory Server 参考手册* 。

ServerRoot 目录

ServerRoot 目录包含多个系统管理公用程序。要确定在您的平台、配置和安装情况下， *ServerRoot* 目录所对应的路径，请参阅 “默认路径和文件名”（第 10 页)。

表 A-1 *ServerRoot* 下的公用程序

公用程序	注释
ServerRoot/`restart-admin`	重新启动管理服务器
ServerRoot/`start-admin`	启动管理服务器
ServerRoot/`startconsole`	启动 Sun ONE Server Console

表 A-1 *ServerRoot* 下的公用程序 （续）

公用程序	注释
ServerRoot/stop-admin	停止管理服务器
ServerRoot/uninstall	卸载产品软件

ServerRoot/bin 目录包含在创建服务器实例时内部使用的产品二进制文件和配置模板。

表 A-2 *ServerRoot*/bin 下的文件

文件	注释
ServerRoot/bin/	内部使用，下列情况除外：
ServerRoot/bin/admin/admconfig	配置管理服务器
ServerRoot/bin/https/bin/ns-httpd	Sun ONE Administration Server
ServerRoot/bin/https/bin/uxwdog	管理服务器监视程序
ServerRoot/bin/slapd/server/ns-ldapagt	基于 LDAP 的 SNMP 副代理
ServerRoot/bin/slapd/server/ns-slapd	Sun ONE Directory Server

ServerRoot/lib 目录包含产品库，其中包括插件。

表 A-3 *ServerRoot*/lib 下的库

库	注释
ServerRoot/lib/	内部使用和插件
ServerRoot/lib/libnspr4.so	NSPR， 4.x 版

ServerRoot/manual 目录包含对控制台联机帮助的支持。

表 A-4 *ServerRoot*/manual 下的联机帮助支持

目录	注释
ServerRoot/manual/	联机帮助支持

ServerRoot/plugins 目录包含服务器插件示例、用于插件开发的标头文件以及用于提供 SNMP 支持的插件。

表 A-5 *ServerRoot*/plugins 下的插件支持

目录或文件	注释
ServerRoot/plugins/	示例、标头、 SNMP 支持
ServerRoot/plugins/slapd/slapi/examples/	插件示例
ServerRoot/plugins/slapd/slapi/include/	插件标头文件
ServerRoot/plugins/snmp/magt/magt	配置管理代理
ServerRoot/plugins/snmp/mibs/	SNMP MIB
ServerRoot/plugins/snmp/sagt/sagt	配置 SNMP 代理

ServerRoot/shared/bin 目录包含管理服务器的工具。

表 A-6 *ServerRoot*/shared/bin 下的工具和客户机

目录或文件	注释
ServerRoot/shared/bin	内部使用，下列情况除外
ServerRoot/shared/bin/admin_ip.pl	更改 IP 地址
ServerRoot/shared/bin/entrycmp	比较用于复制的条目
ServerRoot/shared/bin/fildif	转储过滤的 LDIF
ServerRoot/shared/bin/insync	检查复制同步
ServerRoot/shared/bin/ldapcompare	比较属性值
ServerRoot/shared/bin/ldapdelete	删除目录条目
ServerRoot/shared/bin/ldapmodify	修改目录条目
ServerRoot/shared/bin/ldapsearch	查找目录条目
ServerRoot/shared/bin/modutil	管理 PKCS #11 模块
ServerRoot/shared/bin/uconv	从 ISO 转换到 UTF-8
ServerRoot/shared/bin/repldisc	发现复制拓扑

ServerRoot/shared/config 目录包含用于将证书映射到目录条目的配置文件。

表 A-7 *ServerRoot*/shared/config 下的证书映射配置文件

目录或文件	注释
ServerRoot/shared/config	内部使用，下列情况除外
ServerRoot/shared/config/certmap.conf	将证书映射到条目

ServerRoot/setup5 目录包含用于进行无提示安装和卸载的模板示例。

表 A-8 *ServerRoot*/setup5 下的无提示安装和卸载模板

目录或文件	注释
ServerRoot/setup5	内部使用，下列情况除外
ServerRoot/setup5/typical.ins	无提示安装模板文件
ServerRoot/setup5/uninstall.ins	无提示卸载模板文件

服务器实例目录

slapd-*ServerID* 目录包含对应于服务器实例 *ServerID* 的文件。
ServerRoot/slapd-*ServerID* 目录本身包含多个用于进行命令行管理的脚本。

表 A-9 服务器实例脚本

脚本	注释
ServerRoot/slapd-*ServerID*/	服务器实例
ServerRoot/slapd-*ServerID*/bak2db	还原数据库 （脱机）
ServerRoot/slapd-*ServerID*/bak2db.pl	还原数据库 （联机）
ServerRoot/slapd-*ServerID*/db2bak	备份数据库 （脱机）
ServerRoot/slapd-*ServerID*/db2bak.pl	备份数据库 （联机）
ServerRoot/slapd-*ServerID*/db2index.pl	生成索引 （联机）
ServerRoot/slapd-*ServerID*/db2ldif	将数据库转储到 LDIF （脱机）
ServerRoot/slapd-*ServerID*/db2ldif.pl	将数据库转储到 LDIF （联机）
ServerRoot/slapd-*ServerID*/getpwenc	打印加密口令
ServerRoot/slapd-*ServerID*/ldif2db	导入 LDIF （脱机）

表 A-9 服务器实例脚本 （续）

脚本	注释
ServerRoot/slapd-*ServerID*/ldif2db.pl	导入 LDIF （联机）
ServerRoot/slapd-*ServerID*/ldif2ldap	导入 LDAP 上的 LDIF
ServerRoot/slapd-*ServerID*/monitor	检索监视信息
ServerRoot/slapd-*ServerID*/ns-accountstatus.pl	建立帐户状态
ServerRoot/slapd-*ServerID*/ns-activate.pl	激活条目
ServerRoot/slapd-*ServerID*/ns-inactivate.pl	禁用条目
ServerRoot/slapd-*ServerID*/restart-slapd	重新启动目录服务器
ServerRoot/slapd-*ServerID*/restoreconfig	还原管理服务器配置
ServerRoot/slapd-*ServerID*/saveconfig	保存管理服务器配置
ServerRoot/slapd-*ServerID*/start-slapd	启动目录服务器
ServerRoot/slapd-*ServerID*/stop-slapd	停止目录服务器
ServerRoot/slapd-*ServerID*/suffix2instance	将后缀映射到后端
ServerRoot/slapd-*ServerID*/vlvindex	创建虚拟列表视图索引

ServerRoot/slapd-*ServerID* 的子目录包含配置、日志和备份数据。

表 A-10 服务器实例子目录

目录	注释
ServerRoot/slapd-*ServerID*/	服务器实例
ServerRoot/slapd-*ServerID*/bak/	目录数据库备份
ServerRoot/slapd-*ServerID*/confbak/	管理服务器配置备份
ServerRoot/slapd-*ServerID*/conf_bk/	目录服务器配置备份
ServerRoot/slapd-*ServerID*/config/	目录服务器配置
ServerRoot/slapd-*ServerID*/config/schema/	目录架构配置
ServerRoot/slapd-*ServerID*/db/	目录数据库
ServerRoot/slapd-*ServerID*/ldif/	LDIF 文件示例
ServerRoot/slapd-*ServerID*/locks/	运行时间进程锁定
ServerRoot/slapd-*ServerID*/logs/	服务器日志文件

表 A-10 服务器实例子目录 （续）

目录	注释
ServerRoot/slapd-*ServerID*/tmp/	运行时间临时文件

使用提供的工具管理服务器实例。不要手动修改目录内容。

仅供内部使用

下面的内容由 Directory Server 内部使用。这些内部组件不属于受支持的公用界面。

- *ServerRoot*/adminacl/
- *ServerRoot*/admin-serv/
- *ServerRoot*/admserv
- *ServerRoot*/alias/
- *ServerRoot*/dist/
- *ServerRoot*/httpacl/
- *ServerRoot*/include/
- *ServerRoot*/install/
- *ServerRoot*/java/
- *ServerRoot*/userdb/

不要修改这些目录或其内容。

使用 Sun Crypto Accelerator 板

本附录提供有关与 Directory Server 一起使用 Sun Crypto Accelerator 板来增强连接性能的说明，此连接采用基于证书验证的安全套接字层 (SSL) 协议。

开始之前

表 B-1 包含了一些项目，在尝试使用 Sun Crypto Accelerator 板来增强 SSL 连接性能之前必须完成它们。

表 B-1 使用 Sun Crypto Accelerator 板的前提条件

前提条件	注释
安装 Sun Crypto Accelerator 板	当在主机上安装硬件、驱动程序、增补程序和管理公用程序时，请参阅为 Sun Crypto Accelerator 板提供的产品文档。
Directory Server 安装	有关说明，请参阅第 1 章 “安装 Sun ONE Directory Server”。
服务器证书 （PKCS#12 格式）	获取 Directory Server 的服务器证书 （作为 `.p12` 文件）
CA 证书 （PEM 格式）	为您的证书授权机构 (CA) 获取 CA 证书，作为增强保密邮件 (PEM) 格式文件。

请参阅 *Sun ONE Server Console Server 管理指南* 以获取对 SSL 协议自身和 SSL 证书的讨论，以及关于如何在 Sun ONE 服务器上使用协议的说明，该服务器支持 Sun ONE Server Console 管理。

创建令牌

Directory Server 使用令牌和口令访问 Accelerator 板上适当的加密密钥资料。令牌采用 *user@realm* 形式，其中 *user* 是指 Accelerator 板方面的用户 - 加密密钥材料的所有者，而 *realm* 是指 Accelerator 板方面的领域 - 用户及其密钥材料的逻辑分区。Accelerator 板 *user* 无需与系统上的用户帐户有任何关联。它是专用于该板的。请参阅 Accelerator 板产品文档，以获取有关用户和领域的进一步说明。

可利用供板使用的 `secadm`(1M) 公用程序为令牌创建用户和领域。 Accelerator 板也允许创建多个 *slots*，以便管理用于多个应用程序的令牌。这里假设由于性能原因，您将主机专用于 Directory Server，因此只使用一个插槽 （默认）。请参阅 Accelerator 板产品文档，以获取使用具有多个软件应用程序的板的详细信息。

执行以下步骤，为令牌创建用户和领域以访问默认插槽。

1. 启动 `secadm` 公用程序。

   ```
   $ CryptoPath/bin/secadm
   ```

   默认的 *CryptoPath* 是 `/opt/SUNWconn/crypto`。

2. 为该令牌创建领域。

   ```
   secadm> create realm=dsrealm
   System Administrator Login Required
   Login:super-user
   Password:
   Realm dsrealm created successfully.
   ```

3. 设置要在其中创建用户的领域。

   ```
   secadm> set realm=dsrealm
   secadm{dsrealm}> su
   System Administrator Login Required
   Login:super-user
   Password:
   secadm{root@dsrealm}#
   ```

4. 创建用户 `nobody` 以使用默认插槽，提供重新启动配置了 SSL 的 Directory Server 时使用的口令。

   ```
   secadm{root@dsrealm}# create user=nobody
   Initial password:password
   Confirm password:password
   User nobody created successfully.
   secadm{root@dsrealm}# exit
   ```

此时，已为令牌 `nobody@dsrealm` 创建了用户和领域，并提供了重新启动 Directory Server 时使用的口令。

生成用于板的绑定

用于 Accelerator 板的绑定采用您生成的外部安全模块的形式，这样 Directory Server 就可以绑定到板上。执行以下步骤以生成外部安全模块和 Directory Server 证书数据库之间的绑定，此数据库支持数种 SSL 算法。

1. 在使用 `modutil` 之前设置 `LD_LIBRARY_PATH`。

   ```
   $ set LD_LIBRARY_PATH=ServerRoot/lib ; export LD_LIBRARY_PATH
   ```

2. 创建一个安全模块数据库 （如果不存在）。

   ```
   $ cd ServerRoot/shared/bin
   $ ./modutil -create -dbdir ../../alias -dbprefix "slapd-serverID"
   ```

3. 将外部安全模块添加到安全模块数据库中。

   ```
   $ ./modutil -add "Crypto Mod" -dbdir ../../alias -nocertdb \
   -libfile CryptoPath/lib/libpkcs11.so \
   -mechanisms "RSA:DSA:RC4:DES" -dbprefix "slapd-serverID"
   ```

   默认的 *CryptoPath* 是 `/opt/SUNWconn/crypto`。

4. 请列出安全模块以确保可以成功添加。

   ```
   $ ./modutil -list -dbdir ../../alias -dbprefix "slapd-serverID"
   ```

   您应该看到在步骤 3 中为 `Crypto Mod` 添加的条目。

5. 请将外部安全模块设为针对 RSA、 DSA、 RC4 和 DES 的默认设置。

   ```
   $ ./modutil -default "Crypto Mod" -dbdir ../../alias \
   -mechanisms "RSA:DSA:RC4:DES" -dbprefix "slapd-serverID"
   ```

   这将会成功地更改默认安全模块。

此时已生成用于 Accelerator 板的绑定，并可以导入证书。

导入证书

在配置 SSL 之前，必须导入已获得的服务器和 CA 证书，如表 B-1（第 153 页）中所示。执行以下步骤以导入证书。

1. 导入服务器证书 `.p12` 文件。

```
$ cd ServerRoot/shared/bin
$ ./pk12util -i ServerCert.p12 -d ../../alias -P "slapd-serverID" \
-h "nobody@dsrealm"
Enter Password or Pin for "nobody@dsrealm": passward
Enter Password for PKCS12 file: password
```

2. 导入 CA 证书。

```
$ ./certutil -A -n "Crypto CA Cert" -t CT -i CACert.txt \
-d ../../alias -P "slapd-serverID" -h "nobody@dsrealm"
```

3. 列出与令牌相关联的证书以确保导入成功。

```
$ ./certutil -L -d ../../alias -P "slapd-serverID" \
-h "nobody@dsrealm"
```

   您应该可以看到在步骤 1 和步骤 2 中添加的证书的条目。

此时已导入证书，并可配置 Directory Server 以监听 SSL 连接。

配置 SSL

使用已创建的令牌和口令、外部安全模块和 Directory Server 证书数据库之间已生成的绑定以及已导入的证书，可以将 Directory Server 配置为以安全模式启动。执行这些步骤以配置 SSL，并以安全模式重新启动 Directory Server。

1. 创建文件 `ssl.ldif`，此文件内容为更改与 SSL 相关的 Directory Server 配置条目的修改信息。

代码示例 B-1　　使用该板 (`ssl.ldif`) 为激活 SSL 进行的修改

```
dn:cn=RSA,cn=encryption,cn=config
changetype:add
objectclass:top
objectclass:nsEncryptionModule
cn:RSA
nsSSLToken:nobody@dsrealm
nsSSLPersonalitySSL:ServerCertNickname[1]
nsSSLActivation:on

dn:cn=encryption,cn=config
changetype:modify
replace:nsSSL3
nsSSL3:on
-
replace:nsSSLClientAuth
nsSSLClientAuth:allowed
-
replace:nsSSL3Ciphers
nsSSL3Ciphers:-rsa_null_md5,+rsa_rc4_128_md5,+rsa_rc4_40_md5,
 +rsa_rc2_40_md5,+rsa_des_sha,+rsa_fips_des_sha,+rsa_3des_sha,
 +rsa_fips_3des_sha,+fortezza,+fortezza_rc4_128_sha,
 +fortezza_null,+tls_rsa_export1024_with_rc4_56_sha,
 +tls_rsa_export1024_with_rc4_56_sha,
 +tls_rsa_export1024_with_des_cbc_sha
-
replace:nsCertfile
nsCertfile:alias/slapd-serverID-cert7.db
-
replace:nsKeyFile
nsKeyFile:alias/slapd-serverID-key3.db

dn:cn=config
changetype:modify
replace:nsslapd-secureport
nsslapd-secureport:port
-
replace:nsslapd-security
nsslapd-security:on
```

1. 该昵称包含在 Directory Server 的证书中。

此处的 *port*（`nsslapd-secureport` 的值）是指一旦以安全模式启动时，Directory Server 用于监听 SSL 连接的端口。

2. 应用修改以更改 Directory Server 配置。

```
$ ldapmodify -p currPort -D "cn=directory manager" -w password -f ssl.ldif
```

其中的 *currPort* 是 Directory Server 当前监听客户机请求使用的端口号。

3. 以安全模式重新启动 Directory Server。

```
$ ServerRoot/slapd-serverID/restart-slapd
Enter PIN for nobody@dsrealm:password
```

此处的 *password* 是指当创建令牌 `nobody@dsrealm` 时提供的用于 `nobody` 的用户口令。

此时， Directory Server 使用指定的端口监听 SSL 通信量。可以配置 Sun ONE Administration Server 和客户机应用程序以通过指定端口访问 SSL 上的 Directory Server。详细信息，请参阅 *Sun ONE Directory Server 管理指南*。

安装 Sun Cluster HA for Directory Server

本附录说明如何安装和配置 Sun Cluster HA for Directory Server 数据服务和相关的 Administration Server 数据服务。请参阅 Sun Cluster 3.0 产品文档，以获取 Sun Cluster 安装说明和主要概念。

必须将数据服务配置为故障切换服务。

开始之前

请将本节与 *Sun Cluster 3.0 发行说明* 中的工作表结合使用，作为执行安装和配置前的清单。

开始安装之前，请先考虑以下问题。

- 是否计划在同一节点上运行多个 Directory Server 实例？

  如果是的话，则可选择将 `cn=config` 时的 `nsslapd-listenhost` 设置成适当的网络资源 （逻辑主机名称，如 `dirserv.example.com`），作为每个实例的 IP 地址。 Directory Server 默认行为是监听所有网络接口。

- 是否在 Sun Cluster 配置中运行多个数据服务？

  您可按任何顺序安装多个数据服务，但是以下情况除外：如果使用 Sun Cluster HA for DNS，则必须先完成 Sun Cluster HA for DNS 的安装，然后才能安装 Sun Cluster HA for Directory Server。

表 C-1 概述了 Sun Cluster HA for Directory Server 的安装和配置过程。

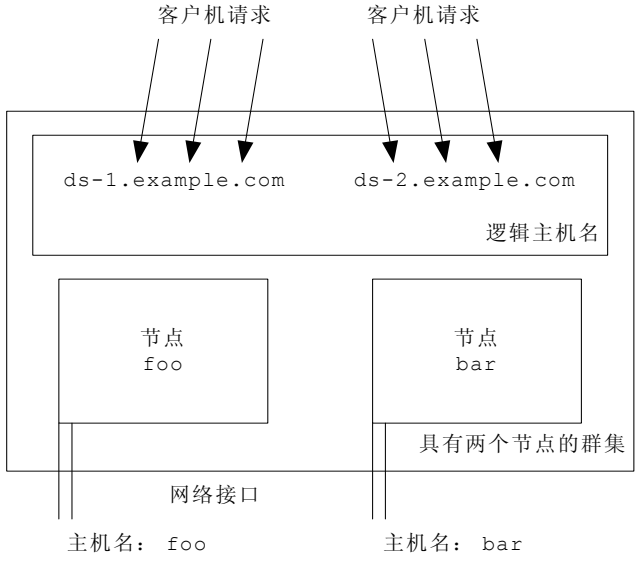
表 C-1 安装和配置过程

任务	应了解的内容
“安装网络资源”（第 160 页）	可控制数据服务的群集节点的名称。 客户机访问 Directory Server 使用的逻辑主机的名称，如 `ds1.example.com`、`ds2.example.com`。 请参阅 Sun Cluster 3.0 产品文档，以获取设置逻辑主机名称的说明。
“安装服务器”（第 162 页）	*ServerRoot* 在安装 Directory Server 的全局文件系统上的位置，如 `/global/ds`。 表 1-2 （第 21 页）中概述了安装的详细信息。
“安装数据服务软件包”（第 163 页）	`SUNWdsha` 和 `SUNWasha` 软件包提供数据服务的管理界面，所以可使用与管理群集中的其他数据服务相同的工具管理 Directory Server 和 Administration Server。
“配置服务器”（第 164 页）	用于 Directory Server 数据服务的资源类型名称 `SUNW.dsldap` 和用于 Administration Server 数据服务的资源类型名称 `SUNW.mps`。 可控制数据服务的群集节点的名称。 客户机访问 Directory Server 和 Administration Server 使用的逻辑主机名称。 *ServerRoot* 在安装 Directory Server 的全局文件系统上的位置。 Directory Server 监听客户机请求的端口。 Administration Server 监听客户机请求的端口。 “安装网络资源”（第 160 页）中定义的资源组的名称。
“配置扩展属性”（第 166 页）	（请参阅本节以获取详细信息。）

安装网络资源

Sun Cluster 软件管理逻辑主机名称，此名称不同于节点名称和用于单个网络接口的主机名称。图 C-1 显示了由双节点群集管理的逻辑主机名称是如何不与这两个节点的任一节点永久关联的。

图 C-1 双节点群集



当安装 Sun Cluster HA for Directory Server 数据服务时，将 Directory Server 和 Administration Server 配置成在逻辑主机名称接口监听，使它们不会限制于群集中的任何特定节点，且 Sun Cluster 软件可管理故障切换。在图 C-1 中，节点命名为 `foo` 和 `bar`。然而，安装时使用的逻辑主机名称 （如图 C-1 所示）将是 `ds-1.example.com` 和 `ds-2.example.com`，而不是 `foo` 和 `bar`。注意，使用的逻辑主机名称是完全限定域名。

请参阅 Sun Cluster 3.0 产品文档，以获取有关这些重要概念的详细信息和设置逻辑主机名称的说明。

设置了逻辑主机名称之后，请执行以下步骤：

1. 成为群集中节点上的超级用户。
2. 确认所有使用的网络地址已添加到名称服务数据库。

   为避免名称服务查找时出现故障，请确保所有完全限定域名、完全限定的逻辑主机名称和共享的 IP 地址包含在每个群集节点的 `/etc/hosts` 文件中。而且，配置每个群集节点上 `/etc/nsswitch.conf` 中的名称服务映射，以便在试图访问其他名称服务前先检查本地文件。
3. 创建故障切换资源组以保存网络和应用程序资源。例如：

```
# scrgadm -a -g resource-group [-h node-list]
```

此处的 *resource-group* 指定组的名称。

可选的 *node-list* 是标识群集的潜在主节点的物理节点名称或 ID 的列表（以逗号分隔）。节点名称的顺序决定了在故障切换时节点转换为主节点的顺序。如果群集中的所有节点均为潜在主节点，则没有必要指定 *node-list*。

4. 将逻辑主机名称资源添加到资源组。

```
# scrgadm -a -L -g resource-group -l logical-host-names [-n netif-list]
```

此处的 *logical-host-names* 是用作逻辑主机名称的完全限定域名的列表（以逗号分隔）。每个 Directory Server 实例使用一个逻辑主机名称。

可选的 *netif-list* 是标识每个节点上的 NAFO 组的列表（以逗号分隔）。如果未指定此选项， `scrgadm`(1M) 就会尝试在子网上寻找网络适配器，此子网是由步骤 3 指定的 *node-list* 中每个节点上指定的各个逻辑主机名称所使用。

5. 验证在步骤 4 中指定为逻辑主机名称的所有完全限定域名是否已添加到名称服务数据库中。

6. 启用资源组且使其联机。

```
# scswitch -Z -g resource-group
```

资源组联机后，可安装服务器。

安装服务器

在 Sun Cluster HA for Directory Server 中， Directory Server 和 Administration Server 都在 Sun Cluster 的控制下运行。这表示提供可故障切换到不同节点的完全限定的逻辑主机名称，而不是在安装时为服务器提供物理节点的完全限定域名。

从对于目录客户机应用程序使用的逻辑主机名称联机的节点开始执行安装，然后对要用于控制 Directory Server 数据服务的其他所有群集节点重复此过程。

在活动节点上安装

对于对目录客户机应用程序使用的逻辑主机名称联机的群集节点：

1. 要为 Directory Server 和 Administration Server 安装 Solaris 软件包，请参阅“安装 Solaris 软件包”（第 23 页）以获取详细说明。

2. 配置 Directory Server。有关说明，请参阅 “配置 Directory Server”（第 28 页）。

   当执行这一步时：

   - 将 Directory Server 实例置于全局群集文件系统上。
   - 使用逻辑主机名称，而不是节点名。

3. 配置 Administration Server，请参阅 “配置 Administration Server”（第 28 页）以获取详细说明，并使用配置 Directory Server 时使用的同一逻辑主机名。

4. 当仅以安全模式使用 Directory Server 时，创建名为 *ServerRoot*/slapd-*serverID*/keypass 的空文件，以便通知群集 Directory Server 实例正以安全模式运行。

   同时，也创建 *ServerRoot*/alias/slapd-*serverID*-pin.txt 文件，包含自动以安全模式启动实例所需的口令。这使群集可以在没有人为干涉的情况下重新启动数据服务。

在其他节点上安装

对于要用于控制 Directory Server 数据服务的各个节点：

1. 要为 Directory Server 和 Administration Server 安装 Solaris 软件包，请参阅 “安装 Solaris 软件包”（第 23 页）以获取详细说明。

2. 使用与 “在活动节点上安装”（第 162 页）时所提供的相同设置配置 Directory Server。

3. 使用与 “在活动节点上安装”（第 162 页）时所提供的相同设置配置 Administration Server。

4. 将 *ServerRoot*/alias/slapd-*serverID*-pin.txt 从第一个节点复制到 *ServerRoot*/alias/。

注意 请不要删除或重定位任何存放在全局文件系统上的文件。

安装数据服务软件包

数据服务软件包 SUNWdsha 和 SUNWasha 提供管理界面以管理群集内用作数据服务的服务器。

- 在要用于支持 Directory Server 数据服务的每个群集节点上，请使用 pkgadd(1M) 公用程序以安装数据服务软件包。

  ```
  # pkgadd -d dirContainingPackages SUNWasha SUNWdsha
  ```

配置服务器

仅在对 Directory Server 使用的逻辑主机名称联机的群集节点上执行下列步骤：

1. 成为超级用户。
2. 停止 Directory Server 和 Administration Server。

   ```
   # /usr/sbin/directoryserver stop
   # /usr/sbin/mpsadmserver stop
   ```

3. 为两种数据服务注册资源类型。

   ```
   # scrgadm -a -t SUNW.dsldap -f /etc/ds/v5.2/cluster/SUNW.dsldap
   # scrgadm -a -t SUNW.mps -f /etc/mps/admin/v5.2/cluster/SUNW.mps
   ```

   此处的 SUNW.dsldap 和 SUNW.mps 是预先定义的用于数据服务的资源类型名称。 /etc/ds/v5.2/cluster/SUNW.dsldap 和 /etc/mps/admin/v5.2/cluster/SUNW.mps 定义数据服务。

4. 将服务器添加到在 “安装网络资源”（第 160 页）中创建的故障切换资源组中。

   ```
   # scrgadm -a -j resource-name-ds -g resource-group -t SUNW.dsldap \
   -y Network_resources_used=logical-host-name \
   -y Port_list=port-number/tcp \
   -x Confdir_list=ServerRoot/slapd-serverID
   ```

```
# scrgadm -a -j resource-name-as -g resource-group -t SUNW.mps \
-y Network_resources_used=logical-host-name \
-y Port_list=port-number/tcp \
-x Confdir_list=ServerRoot
```

此处提供了新的 *resource-name-ds* 以标识 Directory Server 实例，以及新的 *resource-name-as* 以标识 Administration Server 实例。

resource-group 参数是在 “安装网络资源”（第 160 页）中指定的组的名称。

logical-host-name 标识用于当前 Directory Server 实例的逻辑主机名。

port-number 是服务器实例监听客户机请求的端口号，已在 “安装服务器”（第 162 页）中详细说明。注意，每条命令的 `Port_list` 参数只占用一个条目。

ServerRoot 和 *ServerRoot*/`slapd-`*serverID* 是 “安装服务器”（第 162 页）中指定的路径。注意，每条命令的 `Confdir_list` 参数只占用一个条目。

5. 启用服务器资源和监视器。

```
# scswitch -e -j resource-name-ds
# scswitch -e -j resource-name-as
```

此处的 *resource-name-ds* 和 *resource-name-as* 是用于标识步骤 4 中的服务器的名称。

注意 配置服务器后，不要在群集的非活动节点上运行备份和还原命令，如 `db2bak`、`db2ldif`、`back2db` 和 `ldif2db`。相反，应在所有活动节点上执行所有备份和还原过程。

6. 请考虑执行 “同步 HA 存储和数据服务”（第 168 页）一节中的步骤以在故障切换时提高性能。

注册和配置示例

代码示例 C-1 说明了如何为图 C-1 （第 161 页）中描述的群集注册和配置数据服务。

代码示例 C-1 注册和配置数据服务

```
（在联机节点上创建故障切换资源组。）
# scrgadm -a -g ds-resource-group-1 -h foo,bar
```

代码示例 C-1　　注册和配置数据服务 （续）

```
（将逻辑主机名资源添加到资源组。）
# scrgadm -a -L -g ds-resource-group-1 -l ds-1.example.com

（使资源组联机。）
# scswitch -Z -g ds-resource-group-1

（在群集中的每个节点上安装软件包。）

（停止联机节点上的服务器。）
# /usr/sbin/directoryserver stop
# /usr/sbin/mpsadminserver stop

（注册 SUNW.dsldap 和 SUNW.mps 资源类型。）
# scrgadm -a -t SUNW.dsldap -f /etc/ds/v5.2/cluster/SUNW.dsldap
# scrgadm -a -t SUNW.mps -f /etc/mps/admin/v5.2/cluster/SUNW.mps

（为服务器创建资源，并将其添加到资源组。）
# scrgadm -a -j ds-1 -g ds-resource-group-1 \
-t SUNW.dsldap -y Network_resources_used=ds-1.example.com \
-y Port_list=389/tcp \
-x Confdir_list=/global/ds/slapd-ds-1
# scrgadm -a -j as-1 -g ds-resource-group-1 \
-t SUNW.mps -y Network_resources_used=ds-1.example.com \
-y Port_list=5201/tcp \
-x Confdir_list=/global/ds

（启用应用程序资源。）
# scswitch -e -j ds-1
# scswitch -e -j as-1
```

配置扩展属性

扩展属性允许配置群集软件处理应用程序软件的方式。例如，可以调整群集确定数据服务何时必须进行故障切换的方式。

配置内容

通常可以使用 Sun Management Center 中的群集模块或 `scrgadm` 公用程序配置资源扩展属性。可使用带 `-x` *parameter*`=`*value* 选项的 `scrgadm` 公用程序，更改表 C-2 中列出的扩展属性。

表 C-2 SUNW.dsldap 资源扩展属性

属性	说明	默认	范围
Monitor_retry_count	整数值，表示处理监视工具 (PMF) 在由 Monitor_retry_interval 值指定的时间窗口期间重启故障监视器的次数	4 次	-1 至 2,147,483,641 次 -1 表示重试无数次。
Monitor_retry_interval	整数值，表示故障监视器计算故障的间隔时间 （以分钟为单位） 如果故障监视器发生故障的次数超过此时间段内 Monitor_retry_count 中指定的值，则 PMF 不能重启故障监视器。	2 分钟	-1 至 2,147,483,641 分钟 -1 表示无穷重试时间间隔。
Probe_timeout	整数值，表示故障监视器探测 Directory Server 实例所使用的超时值 （以秒为单位）	30 秒	0 至 2,147,483,641 秒

请参阅 Sun Cluster 3.0 产品文档，以获取有关 Sun Cluster 属性的更多信息。

故障监视器的工作原理

群集软件使用故障监视器确定数据服务是否正常。故障监视器探测数据服务，然后确定服务是正常，还是基于探测结果必须重启。

表 C-3　故障监视器解释探测的方式

Directory Server 正在运行 ...	使用的探测	算法
一般模式	ldapsearch	1. 尝试进行搜索。 2. 如果搜索操作导致： • LDAP_SUCCESS，则认为服务正常。 • 一个 LDAP 错误，则必须重启服务。 • 超时以外的错误，则故障监视器根据 Monitor_retry_count 和 Monitor_retry_interval 进行再次探测。 • 超出了 Probe_timeout 持续时间，则故障监视器根据 Monitor_retry_count 和 Monitor_retry_interval 进行再次探测。 超时的潜在原因包括系统、网络或 Directory Server 实例上的高负载。超时也可能表明对于被监视的 Directory Server 实例的数目来说， Probe_timeout 值设置过低。
安全模式 (SSL)	TCP 连接	1. 尝试进行连接。 2. 如果连接操作： • 成功，则认为服务正常。 • 失败，则必须重启服务。 • 超出了 Probe_timeout，则必须重启服务。

故障监视器使用 “配置服务器”（第 164 页）时指定的 IP 地址和端口号以执行探测操作。如果将 Directory Server 配置为使用两个端口进行监听 （一个用于 SSL 通信量，另一个用于一般通信量），则故障监视器按照用于安全模式端口的故障监视算法，使用 TCP 连接探测这两个端口。

同步 HA 存储和数据服务

SUNW.HAStorage 资源类型使 HA 存储和数据服务之间的操作同步，当磁盘密集型数据服务 （如 Directory Server）进行故障切换时提供较高性能。

要使 Directory Server 数据服务与 HA 存储同步，请在对数据服务使用的逻辑主机名称联机的节点上完成以下步骤：

1. 注册 HA 存储资源类型。

   ```
   # scrgadm -a -t SUNW.HAStorage
   ```

2. 配置存储资源以保持同步状态。

   ```
   # scrgadm -a -j HAStorage-resource-name -g HAStorage-resource-group \
   -t SUNW.HAStorage -x ServicePaths=volume-mount-point \
   -x AffinityOn=True
   ```

   此处， *volume-mount-point* 标识 Directory Server 存储数据的磁盘容量。

3. 启用存储资源和监视器。

   ```
   # scswitch -e -j HAStorage-resource-name
   ```

4. 在现有的 Directory Server 资源上添加依存关系。

   ```
   # scrgadm -c -j resource-name-ds \
   -y Resource_Dependencies=HAStorage-resource-name
   ```

请参阅 `SUNW.HAStorage`(5) 以获取背景信息，以及参阅 Sun Cluster 3.0 产品文档以获取为新资源安装 `SUNW.HAStorage` 资源类型的说明。

创建其他的 Directory Server 实例

执行以下步骤：

1. 使用 Sun ONE Server Console 创建其他的 Directory Server 实例。

   有关说明，请参阅 *Sun ONE Server Console Server 管理指南* 。

2. 在对数据服务使用的逻辑主机名称联机的节点上停止新的 Directory Server 实例。

   ```
   # /usr/sbin/directoryserver -server serverID stop
   ```

3. 将 Directory Server 添加到在 “安装网络资源”（第 160 页）中创建的故障切换资源组。

```
# scrgadm -a -j resource-name-ds -g resource-group -t SUNW.dsldap \
-y Network_resources_used=logical-host-name \
-y Port_list=port-number/tcp \
-x Confdir_list=ServerRoot/slapd-serverID
```

此处提供了新的 *resource-name-ds* 以标识 Directory Server 实例。

resource-group 参数是在 “安装网络资源”（第 160 页）中指定的组的名称。

logical-host-name 标识用于实例的逻辑主机名。

port-number 是实例监听客户机请求所用的端口号，已在 “安装服务器”（第 162 页）中详细说明。注意， `Port_list` 参数仅占一个条目。

ServerRoot 和 *ServerRoot*`/slapd-`*serverID* 是 “安装服务器”（第 162 页）中指定的路径。注意， `Confdir_list` 参数仅占一个条目。

4. 启用服务器资源和监视器。

```
# scswitch -e -j resource-name-ds
```

此处的 *resource-name-ds* 是用于在步骤 3 中标识 Directory Server 的名称。

卸载

若要从群集中删除 Sun Cluster HA for Directory Server 和关联的 Administration Server，请执行以下步骤：

1. 停止服务器实例。

```
# scswitch -n -j resource-name-ds
# scswitch -n -j resource-name-as
```

2. 删除资源。

```
# scrgadm -r -j resource-name-ds
# scrgadm -r -j resource-name-as
```

3. 从群集数据库中删除资源类型。

```
# scrgadm -r -t SUNW.dsldap
# scrgadm -r -t SUNW.mps
```

4. 删除服务器配置。

```
# /usr/sbin/mpsadmserver unconfigure
# /usr/sbin/directoryserver unconfigure
```

5. 使用 `pkgrm`(1M) 公用程序从每个节点删除安装的软件包，包括 `SUNWdsha` 和 `SUNWasha`。

索引

E

F

H

I

J

L

M

N

P

Q

R

S

T

W

X

Y

Z