在 Oracle® Solaris 11.1 中使用命名和目录服务

文件号码 E36691–02
2012 年 10 月

ORACLE

121218@25097

目录

表

示例

前言

《在 Oracle Solaris 11.1 中使用命名和目录服务》介绍了以下 Oracle Solaris 操作系统 (OS) 命名和目录服务的设置和管理：DNS、NIS 和 LDAP。本指南是多卷集的一部分，该卷集包含 Oracle Solaris 管理信息中的重要部分。

注 – 此 Oracle Solaris 发行版支持使用 SPARC 和 x86 系列处理器体系结构的系统。支持的系统可以在 Oracle Solaris OS: Hardware Compatibility Lists（Oracle Solaris OS：硬件兼容性列表）中找到。本文档列举了在不同类型的平台上进行实现时的所有差别。

相关书籍

- 《Oracle Directory Server Enterprise Edition Deployment Guide》
- 《Oracle Directory Server Enterprise Edition Administration Guide》
- 《DNS and Bind》，由 Cricket Liu 和 Paul Albitz 编著，（第 5 版，O'Reilly 出版社，2006 年）
- 《Understanding and Deploying LDAP Directory Services》，由 Timothy A. Howes 博士和 Mark C. Smith 编著

获取 Oracle 支持

Oracle 客户可以通过 My Oracle Support 获取电子支持。有关信息，请访问 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info`，或访问 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`（如果您听力受损）。

印刷约定

下表介绍了本书中的印刷约定。

表 P–1 印刷约定

字体或符号	含义	示例
`AaBbCc123`	命令、文件和目录的名称；计算机屏幕输出	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `machine_name% you have mail.`
`AaBbCc123`	用户键入的内容，与计算机屏幕输出的显示不同	`machine_name%` **`su`** `Password:`
aabbcc123	要使用实名或值替换的命令行占位符	删除文件的命令为 `rm` *filename*。
AaBbCc123	保留未译的新词或术语以及要强调的词	这些称为 *Class* 选项。 **注意**：有些强调的项目在联机时以粗体显示。
新词术语强调	新词或术语以及要强调的词	**高速缓存**是存储在本地的副本。 请**勿**保存文件。
《书名》	书名	阅读《用户指南》的第 6 章。

命令中的 shell 提示符示例

下表显示了 Oracle Solaris OS 中包含的缺省 UNIX shell 系统提示符和超级用户提示符。请注意，在命令示例中显示的缺省系统提示符可能会有所不同，具体取决于 Oracle Solaris 发行版。

表 P–2 shell 提示符

shell	提示符
Bash shell、Korn shell 和 Bourne shell	`$`
Bash shell、Korn shell 和 Bourne shell 超级用户	`#`
C shell	`machine_name%`
C shell 超级用户	`machine_name#`

第 1 部 分

关于命名和目录服务

本部分介绍 Oracle Solaris OS 的命名和目录服务。此外，本部分介绍了如何使用服务管理工具 (Service Management Facility, SMF) 来配置命名服务，以便您可以通过使用不同的本地和远程目录服务来协调查找。本部分还介绍了如何配置域名服务 (Domain Name Service, DNS) 以及 Active Directory 客户机。

◆ ◆ ◆ 第 1 章

1 命名和目录服务（概述）

本章概述了 Oracle Solaris 发行版中包括的命名和目录服务。此外，还简要介绍了 DNS、NIS 和 LDAP 命名服务。

本章包含以下主题：

什么是命名服务？

命名服务执行对所存储的信息的查找工作，例如：

- 主机名和地址
- 用户名
- 口令
- 访问权限
- 组成员关系、自动挂载映射，等等。

提供该信息是为了让用户能够登录到其主机、对资源进行访问以及被授予权限。名称服务信息可以在各种形式的数据库文件中存储在本地，或者存储在基于网络的中央系统信息库或数据库中。

如果没有中央命名服务，则每台主机都必须单独维护一份此信息的副本。命名服务信息可以存储在文件、映射或数据库表中。如果集中存储所有数据，管理将变得更加轻松。

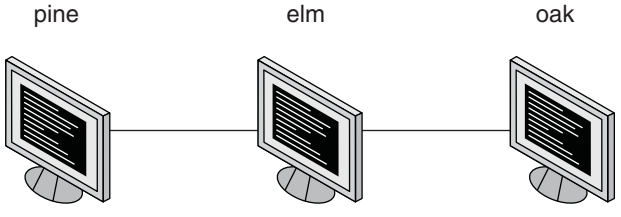
命名服务对任何计算网络都是至关重要的。除了其他功能外，命名服务还提供了执行以下任务的功能。

- 将名称与对象关联（**绑定**）
- 将名称解析为对象

- 删除绑定
- 列出名称
- 重命名信息

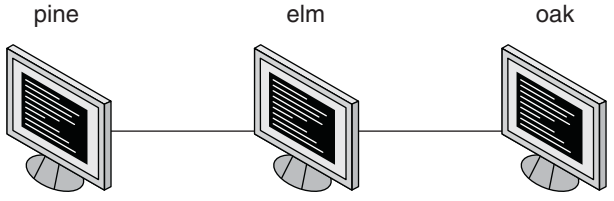
有了网络信息服务，可以用通用名称而不是数字地址来标识系统。这样可以简化通信，因为用户不需要记住并尝试输入那些繁琐的地址（例如 192.168.0.0）。

例如，以一个包含三个系统（分别名为 pine、elm 和 oak）的网络为例。pine 必须事先知道 elm 或 oak 的数字网络地址，才能向其发送消息。因此，pine 维护了一个文件 /etc/inet/hosts，该文件存储着网络中每个系统（包括 pine 自身）的网络地址。



/etc/inet/hosts
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak

同样，elm 和 oak 要想与 pine 进行通信或者彼此之间进行通信，这两个系统也必须维护类似的文件。



/etc/inet/hosts
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak

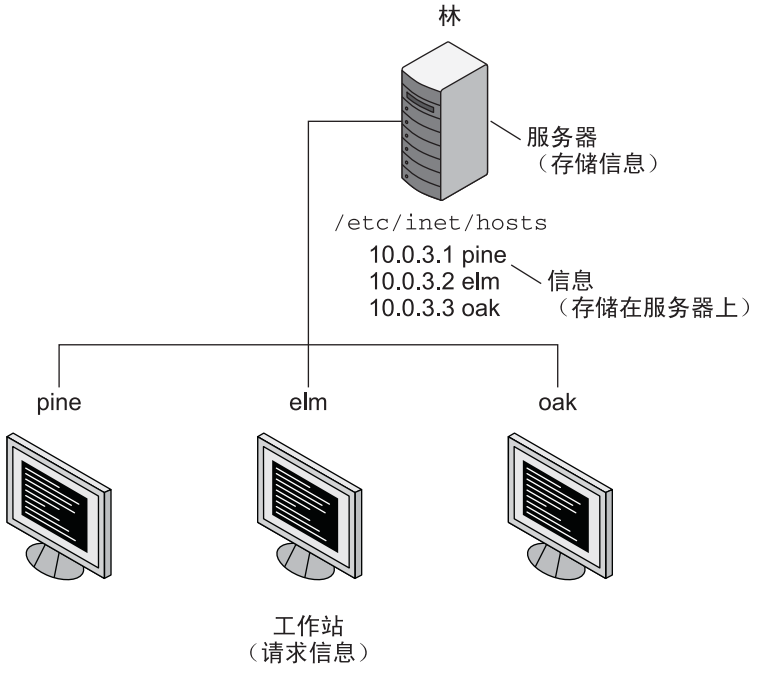
/etc/inet/hosts
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak

/etc/inet/hosts
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak

除了存储地址外，系统还存储着安全信息、邮件数据、网络服务信息，等等。随着网络提供的服务越来越多，存储信息的列表会不断增大。因此，每个系统都可能维护着与 /etc/inet/hosts 类似的一整套文件。

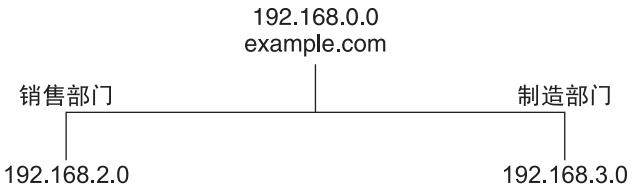
网络信息服务将网络信息存储在服务器上，可供任何系统查询。

这些系统被称作服务器的**客户机**。下图显示客户机/服务器布局。每次网络信息发生变化时，管理员将只更新网络信息服务存储的信息，而不更新每个客户机的本地文件。这样做可以减少错误、客户机之间的不一致性以及任务的绝对工作量。

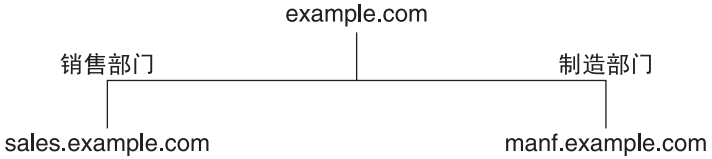


这种由服务器向网络中的客户机提供集中式服务的布置称为**客户机/服务器计算**。

尽管网络信息服务的主要用途是集中存储信息，但它也可以简化网络名称。例如，假设您的公司设置了一个与 Internet 连接的网络。Internet 已为您的网络指定了网络地址 `192.168.0.0` 和域名 `example.com`。公司有两个部门：销售和制造 (Manf)，因此，其网络将划分为一个主网和两个子网（每个部门对应一个子网）。每个网络有自己的地址。



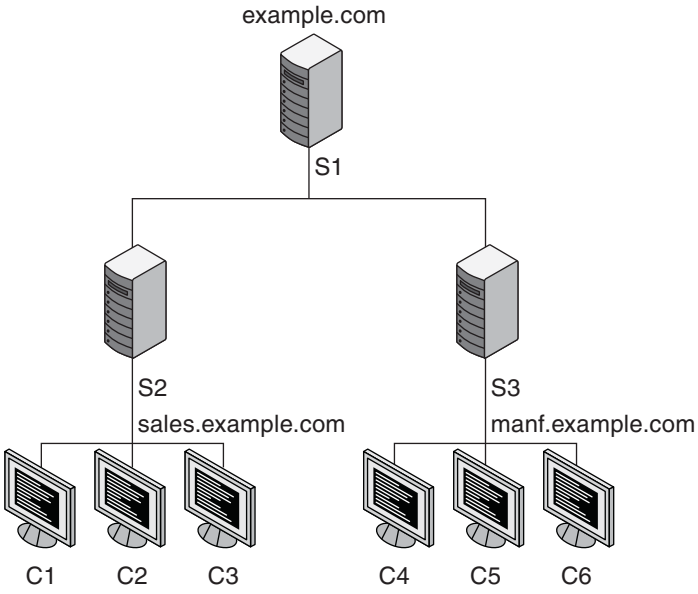
如上所述，每个部门可由网络地址来标识，但用命名服务提供的描述性名称来标识会更好。



可以将邮件发送到 example.com，而不是将邮件或其他网络通信发送到 198.168.0.0。可以将邮件发送到 sales.example.com 或 manf.example.com，而不是将邮件发送到 192.168.2.0 或 192.168.3.0。

名称还比物理地址更灵活。因为物理网络通常不会改变，而公司组织可能会发生变动。

例如，假设 example.com 网络由三台服务器 S1、S2 和 S3 提供支持。假设这些服务器中有 S2 和 S3 这两台服务器来支持客户机。

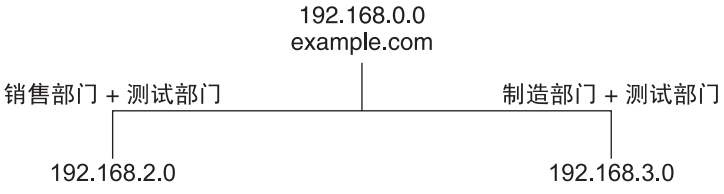


客户机 C1、C2 和 C3 将从服务器 S2 获取其网络信息。客户机 C4、C5 和 C6 将从服务器 S3 获取信息。下表对生成的网络进行了汇总。该表是该网络的大致说明，与实际的网络信息映射并不相似。

表 1–1 example.com 网络的表示

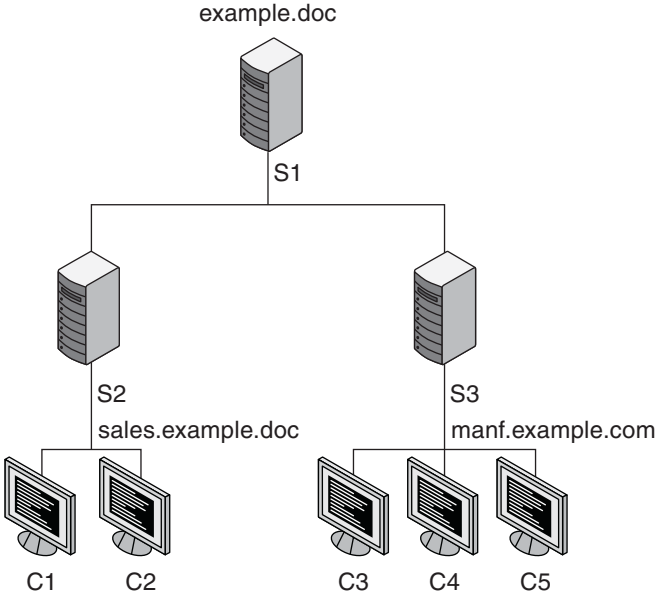
网络地址	网络名称	服务器	客户机
192.168.1.0	example.com	S1	
192.168.2.0	sales.example.com	S2	C1、C2、C3
192.168.3.0	manf.example.com	S3	C4、C5、C6

现在，假设创建了第三个部门（测试部门），该部门从其他两个部门借入一些资源，但并未创建第三个子网。物理网络将不再与公司结构类似。



测试部门的流量原本将不具有自己的子网，而是将在 192.168.2.0 与 192.168.3.0 之间拆分。但是，通过网络信息服务，测试部门的流量可以具有自己的专用网络。

因此，当组织更改时，其网络信息服务可以按此处所示更改其映射。



现在，客户机 C1 和 C2 将从服务器 S2 获取其信息。C3、C4 和 C5 将从服务器 S3 获取信息。

通过更改网络信息结构，无需重新组织网络结构，即可适应组织结构的后续更改。

Oracle Solaris 命名服务

Oracle Solaris 平台提供了以下命名服务：

- 域名系统 (Domain Name System, DNS)（请参见第 27 页中的 “DNS 命名服务的说明”）
- `/etc` 文件，原始的 UNIX 命名系统（请参见第 28 页中的 “/etc 文件命名服务的说明”）
- 网络信息服务 (Network Information Service, NIS)（请参见第 28 页中的 “NIS 命名服务的说明”）
- 轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP)（请参见第 3 部分 LDAP 命名服务设置和管理）

大多数现代网络都组合使用这些服务中的两个或多个。使用哪个命名服务进行特定的查找是由名称服务转换来协调的，这在第 2 章，名称服务转换（概述）中进行了讨论。

DNS 命名服务的说明

域名系统 (Domain Name System, DNS) 是在 TCP/IP 网络上实施的一个分层次的分布式数据库。它主要用来为 Internet 主机名查找 IP 地址以及为 IP 地址查找主机名。数据分布在网络中，并通过使用以句点分隔的名称（从右向左读取）进行定位。DNS 还用来存储其他与 Internet 相关的主机信息，例如邮件交换路由信息、位置数据以及可用的服务。该服务的分层特性使得可以对本地域进行本地管理，同时对连接到 Internet、内联网或这两者的其他域提供国际性覆盖。

DNS 客户机从一台或多台名称服务器请求关于主机名的信息并等待响应。DNS 服务器通过以下途径对请求进行响应：使用从位于 DNS 主服务器上的文件或第三方数据库装入的信息缓存、通过网络使用协作 DNS 从属服务器、或者使用所存储的来自以前查询的信息。如果未找到响应并且服务器不负责有问题的域，则该服务将以递归方式从其他服务器请求主机名并缓存该响应（如果允许这样做）。

多播 DNS 和服务搜索的说明

DNS 协议的两个扩展由 `svc:network/dns/multicast` 服务进行管理。多播 DNS (Multicast DNS, mDNS) 在未安装传统 DNS 服务器的小型网络中实施 DNS。DNS 服务搜索 (DNS Service Discovery, DNS-SD) 对多播 DNS 进行了扩展，使之还提供简单的服务搜索（网络浏览）。有关更多信息，请参见第 39 页中的 “多播 DNS”和第 39 页中的 “多播 DNS 服务搜索”。

注意 – mDNS 服务使用 `.local` 域名，因此在 DNS 中不应当再使用该名称以避免可能的冲突。

/etc 文件命名服务的说明

原始的基于主机的 UNIX 命名系统是为标准的独立 UNIX 计算机开发的，后来为用于网络进行了改编。许多旧的 UNIX 操作系统和计算机仍然仅通过使用本地文件管理所有命名数据。不过，通过使用本地文件管理主机、用户和其他命名数据不是很适用于大型的复杂网络。每个 `/etc` 文件在其关联的手册页中进行了描述。例如，`/etc/inet/hosts` 文件在 `hosts(4)` 手册页中进行了描述。

NIS 命名服务的说明

网络信息服务 (Network Information Service, NIS) 是独立于 DNS 开发的。DNS 通过使用计算机名代替数字 IP 地址来简化通信。NIS 的主要作用是通过对各种网络信息进行集中控制来更好地管理网络。NIS 存储有关网络、计算机名称和地址、用户、以及网络服务的信息。这种网络信息的集合被称为 *NIS* **名称空间**。

NIS 名称空间信息存储在 NIS 映射中。NIS 映射旨在替换 UNIX `/etc` 文件以及其他配置文件。NIS 除了存储名称和地址外，还存储大量的其他信息。因此，NIS 名称空间存在大量映射。有关更多信息，请参见第 93 页中的 “使用 NIS 映射”。

NIS 使用与 DNS 类似的客户机/服务器布局。复制的 NIS 服务器可向 NIS 客户机提供服务。主要的服务器称为**主**服务器，为确保其可靠，主服务器还具有备份，即**从属**服务器。主服务器和从属服务器都使用 NIS 检索软件，并且都存储 NIS 映射。有关 NIS 体系结构和 NIS 管理的更多信息，请参见第 6 章，设置和配置 NIS（任务）和第 7 章，管理 NIS（任务）。

LDAP 命名服务的说明

轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP) 是用来访问目录服务器以使用分布式命名和其他目录服务的安全网络协议。该基于标准的协议支持一个分层次的数据库结构。在 UNIX 和多平台环境中都可以使用同一协议来提供命名服务。

Oracle Solaris OS 支持将 LDAP 与 Oracle Directory Server Enterprise Edition（以前称为 Sun Java System Directory Server）以及其他 LDAP 目录服务器一起使用。

有关 LDAP 命名服务的信息，请参见第 9 章，LDAP 命名服务介绍（概述）。

有关从 NIS 转换到 LDAP 的信息，请参见第 15 章，从 NIS 转换为 LDAP（任务）。

有关单点登录以及设置和维护 Kerberos 验证服务的信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的第 VI 部分, “Kerberos 服务”。

名称服务转换的说明

名称服务转换是允许客户机通过 DNS、LDAP、NIS 或本地文件数据源搜索命名信息的一种机制。该转换是通过 `svc:/system/name-service/switch` 服务进行管理的。有关更多信息，请参见第 2 章，名称服务转换（概述）。

命名服务：简要比较

	DNS	NIS	LDAP	文件
名称空间	分层	不分层	分层	文件
数据存储	文件/资源记录	两列映射	目录（视情况而定） 索引数据库	基于文本的文件
服务器	主/从	主/从	主/副本 多主副本	无
安全性	DNSSEC（视情况而定）	无（根或不包含任何内容）	Kerberos、TLS、SSL（视情况而定）	无
传输	TCP/IP	RPC	TCP/IP	文件 I/O
范围	全局	LAN	全局	仅本地主机
数据	主机	所有	所有	所有

注 – 对于基于 LDAP 和基于文件的命名，建议使用 DNS 服务进行主机或网络地址查找。

◆ ◆ ◆ 第 2 章

2 名称服务转换（概述）

本章介绍名称服务转换。名称服务转换可用于协调各个命名服务的使用。本章包含以下主题：

关于名称服务转换

名称服务转换是一项可配置的选择服务，管理员可通过它来指定为每种类型的网络信息使用的名称信息服务或源。服务被称为一个数据库。名称服务转换由调用任意 `getXbyY()` 接口（如以下接口）的客户机应用程序使用。

- `gethostbyname ()`
- `getpwuid ()`
- `getpwnam ()`
- `getaddrinfo ()`

每个系统在 SMF 系统信息库中都有其自己的配置。名称服务转换中定义的每个属性都标识一个特定的数据库，例如主机、口令或组。指定给每个属性的值列出了可从中请求信息的一个或多个源。有时，这些值包括指导或选项。指导可以包括应当对服务进行多少次尝试、要应用的超时，以及如果服务失败要执行的操作。

用于名称服务转换的数据库和源

名称服务转换支持以下数据库。

表 2–1 名称服务转换的数据库

信息数据库	说明
alias	列出电子邮件地址和别名
auth_attr	列出授权名称和说明
automount	列出有关可以在本地挂载的远程文件系统的信息
bootparam	列出无磁盘客户机的引导信息
ether	列出以太网地址和匹配的主机名
group	列出可以用来共享对文件的访问权限的组的相关信息
host	列出 IP 地址和匹配的主机名
netgroup	列出共享 NFS 文件系统的信息
netmask	列出用来实施 IP 子网的网络掩码
network	列出每个网络的名称和编号
password	列出用户帐户信息
prof_attr	列出执行配置文件名称、说明和其他属性
project	列出项目名称、唯一标识符和关联的资源分配
protocol	列出 Internet 协议名称、编号和任何别名
publickey	列出公钥信息
rpc	列出 RPC 程序的名称和编号
service	列出 Internet 服务的名称、端口和协议
tnrhdb	列出使用 Oracle Solaris 的 Trusted Extensions 功能的主机的安全属性
tnrhtp	列出 Trusted Extensions 使用的模板

此外，名称服务转换中的 `default` 属性定义了当未定义源字符串时用于任何数据库的源字符串。如果您的网络为大多数数据库使用了相同的源，则可以更改 `default` 属性并且不为每个数据库定义属性。有关过程，请参见第 37 页中的 “如何为所有命名数据库更改源”。

要支持以前的发行版，可以将 `enable_passwd_compat` 和 `enable_group_compat` 属性设置为 `true` 以启用口令和组信息的 `compat` 模式。该模式在相应的数据库中提供了对旧式 + 或 - 语法的支持。在当前发行版中，此功能已被 `pam_list` 模块替代。

下表介绍了在名称服务转换中可以为上面列出的数据库列出的源的种类。

表 2–2 用于名称服务转换的信息源

信息源	说明
ad	标识 Active Directory 服务器上存储的数据库。
compat	compat 可用于口令和组信息，以支持 /etc/passwd、/etc/shadow 和 /etc/group 文件中的旧式 + 或 - 语法。此功能已被 pam_list 模块替代。
dns	指定将从 DNS 获取主机信息。
files	指定存储在客户机的 /etc 目录中的一个文件，例如 /etc/passwd。
ldap	指定将从 LDAP 目录中获取项。
mdns	使用多播 DNS (Multicast DNS, mDNS) 指定主机信息。
nis	指定一个 NIS 映射，例如 hosts 映射。

用于名称服务转换的搜索条件

以下搜索条件格式可用来选择一个或多个信息源，并可用来指定源的使用顺序。

- **单个源** – 如果某个信息类型只有一个源（例如 files），则使用名称服务转换的搜索例程将**仅**在该源中搜索信息。如果该例程找到了此信息，将返回 success 状态消息。如果该例程未找到此信息，则会停止搜索并返回不同的状态消息。不同的例程处理状态消息的方式也不同。
- **多个源** – 如果数据库中针对某个给定的信息类型包含了多个源，则名称服务转换会指示搜索例程在列出的第一个源中搜索。如果该例程找到了此信息，将返回 success 状态消息。如果该例程未在第一个源中找到此信息，将尝试在下一个源中进行搜索。该例程将依次搜索所有的源，直到找到此信息或者该例程被一个 return 指定停止。如果在搜索了列出的所有源之后仍未找到此信息，该例程将停止搜索并返回 non-success 状态消息。

缺省情况下，在 Oracle Solaris 11 发行版 中，第一个源是 files。当所列出的下一个源不可用时，此配置可防止系统挂起。

用于名称服务转换的状态消息

如果某个例程找到了此信息，则该例程返回 success 状态消息。如果该例程未找到此信息，则会返回下面的三个错误状态消息之一。下表列出了可能的状态消息。

表 2–3 用于名称服务转换的状态消息

状态消息	说明
SUCCESS	在指定的源中找到了所请求的项。
UNAVAIL	该源不响应或者不可用。换句话说，无法找到或访问数据库源。

表 2–3 用于名称服务转换的状态消息 （续）

状态消息	说明
NOTFOUND	该源给出 "No such entry"（该项不存在）的响应。换句话说，已访问了数据库，但未找到所需的信息。
TRYAGAIN	该源正忙，下次可能会响应。换句话说，已找到了数据库但无法响应查询。

名称服务转换的转换操作选项

可以指示名称服务转换用下表中显示的两个**操作**之一来响应状态消息。

表 2–4 从名称服务转换对状态消息的响应

操作	说明
return	停止查找信息。
continue	尝试在下一个源中查找。

此外，对于 TRYAGAIN 状态消息，可以定义以下操作：

- forever－不限次数地重试当前源
- *n*－将当前源额外重试 *n* 次

用于名称服务转换的缺省搜索条件

名称服务转换状态消息和操作选项的组合决定了搜索例程在每个步骤执行的操作。状态消息和操作选项的组合构成了**搜索条件**。

对于每个源，该转换的缺省搜索条件是相同的。此列表包括了对多个搜索条件的描述。

- SUCCESS=return。停止查找信息。使用已经找到的信息以继续。
- UNAVAIL=continue。转到下一个名称服务转换源并继续搜索。如果该源是最后一个源或唯一的源，将返回 NOTFOUND 状态。
- NOTFOUND=continue。转到下一个名称服务转换源并继续搜索。如果该源是最后一个源或唯一的源，将返回 NOTFOUND 状态。
- TRYAGAIN=continue。转到下一个名称服务转换源并继续搜索。如果该源是最后一个源或唯一的源，将返回 NOTFOUND 状态。

可以通过使用前面列表中显示的 *STATUS=action* 语法显式指定某个其他条件来更改缺省搜索条件。例如，NOTFOUND 条件的缺省操作是继续搜索下一个源。网络数据库的搜索条件可能报告为：

```
svc:/system/name-service/switch> listprop config/network
config/network  astring             "nis [NOTFOUND=return] files"
```

networks: nis [NOTFOUND=return] files 项可以为 NOTFOUND 状态指定非缺省条件。非缺省条件由方括号分隔。

在本示例中，搜索条件按如下方式工作：

- 如果 network 数据库可用且包含需要的信息，搜索例程将返回 SUCCESS 状态消息。
- 如果 network 数据库不可用，搜索例程将返回 UNAVAIL 状态消息。缺省情况下，例程使用所列出的下一个条件继续搜索。
- 如果 network 数据库可用且已找到，但是不包含需要的信息，搜索例程将返回 NOTFOUND 消息。不过，例程将停止搜索，而不是执行缺省行为，即继续搜索下一个源。
- 如果 network 数据库处于繁忙状态，搜索例程将返回 TRYAGAIN 状态消息并且缺省情况下将继续搜索 network 数据库。

注 – 名称服务转换中的查找是按照项目的列出顺序执行的。但是，口令更新将以相反的顺序执行，除非使用 passwd -r *repository* 命令另行指定了更新顺序。有关更多信息，请参见第 37 页中的 “名称服务转换和口令信息”。

语法有误时该怎么办？

客户机库例程包含当没有在名称服务转换中定义特定的 SMF 属性或 default SMF 属性时或者该属性的语法不正确时使用的内建缺省项。通常，这些内建的缺省项只有 "files"。

auto_home 和 auto_master

auto_home 和 auto_master 表和映射的转换搜索条件组合成一个名为 automount 的类别。

timezone 和名称服务转换

timezone 表不使用名称服务转换，因此该表不包括在该转换的属性列表中。

名称服务转换中的 keyserv 和 publickey 项

注意 – 在对名称服务转换进行更改后，您必须重新启动 keyserv 守护进程，更改才会生效。

只有当 keyserv 重新启动时，keyserv 守护进程才会读取名称服务转换中的 publickey 属性。如果您更改了名称服务转换属性，则在使用 svcadm refresh svc:/network/rpc/keyserv:default 重新启动 keyserv 守护进程之前，keyserv 不会注册这些更改。在更改属性并刷新 name-service/switch 服务之后，必须运行此命令以便将属性更改装入到 SMF 系统信息库中。

管理名称服务转换

更改计算机的命名服务时，需要相应地修改计算机的名称服务转换信息。例如，如果将计算机的命名服务从 files 更改为了 NIS，则需要对名称服务转换进行配置以使用 NIS。

▼ 如何使用传统的 nsswitch.conf 文件

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **将 nsswitch.conf 文件复制到新系统。**

确保将文件命名为 `/etc/nsswitch.conf`。

3 **将信息从该文件装入到 SMF 系统信息库中。**

```
# nscfg import -f svc:/system/name-service/switch:default
```

4 **刷新名称服务转换的服务。**

```
# svcadm refresh name-service/switch
```

▼ 如何为数据库转换源

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **为选定的数据库更改源定义。**

在此示例中，数据库搜索顺序是先 `files` 后 `nis`。

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files nis"
svc:/system/name-service/switch> quit
```

3 **刷新名称服务转换的服务。**

```
# svcadm refresh name-service/switch
```

▼ 如何为所有命名数据库更改源

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **更改 `config/default` 属性。**

此属性应使用最常见的源定义。在此示例中，数据库搜索顺序是先 `files` 后 `nis`。

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/default = astring: "files nis"
svc:/system/name-service/switch> quit
```

3 **可选更改各个数据库的属性。**

使用此命令为未使用在 `config/default` 属性中选择的顺序的任何数据库更改源定义。

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns nis"
svc:/system/name-service/switch> quit
```

4 **刷新名称服务转换的服务。**

```
# svcadm refresh name-service/switch
```

DNS 和 Internet 访问

名称服务转换还控制客户机的 DNS 转发，如下章所述。DNS 转发允许客户机访问 Internet。

名称服务转换和口令信息

可以将口令信息包括在多个系统信息库（如 `files` 和 `nis`）中并访问它们。您可以在名称服务转换中使用 `config/password` 属性来设定该信息的查找顺序。

注意 – 在名称服务转换中，`files` 应当是 `passwd` 信息的第一个源以防止系统上发生拒绝服务 (denial of service, DoS) 攻击。

在 NIS 环境中，名称服务转换中的 `config/password` 属性应当按以下顺序列出系统信息库：

```
config/password  astring            "files nis"
```

提示 – 首先列出 `files` 将允许 `root` 用户在大多数情况下登录，甚至当系统遇到某些网络或命名服务问题时。

不要为**同一用户**维护多个系统信息库。在大多数情况下，命名服务仅查找并返回第一个定义。重复的项通常会掩盖安全问题。

例如，在文件和网络系统信息库中同时包含同一用户将（根据 `config/password name-service/switch` 配置）优先使用一个登录 ID 而不使用另一个。给定计算机的第一个匹配 ID 将成为用于登录会话的 ID。如果某个 ID 同时在文件和网络系统信息库中，并且因为安全原因已经禁用了网络系统信息库，则包含该 ID 且在其上访问该 ID 的计算机在网络 ID 被禁用之前可能是不安全的，并且容易遭受不安全的和有害的访问。

◆ ◆ ◆ 第 3 章

管理 DNS（任务）

本章提供了关于 DNS 服务器和客户机服务的信息。本章包含以下主题：

DNS 概述

DNS 与大多数网络协议一样，也有两个部分：一个用来提供答复的服务和一个用来查询服务的客户机。在 Oracle Solaris 操作系统 中，缺省 DNS 服务是由互联网系统协会 (Internet Systems Consortium, ISC) 开发的 BIND 及其关联的守护进程 named 提供的。DNS 客户机包含很多实用程序和库。

多播 DNS

多播 DNS (Multicast DNS, mDNS) 为本地链路上的系统提供了一个易于设置和维护的命名服务系统。同一本地链路上所有参与的网络设备都执行标准的 DNS 功能，使用 mDNS 而不是单播，并且不需要单播 DNS 服务器。对于管理员，mDNS 的主要优点是不需要在本地网络上维护单播 DNS 服务器。例如，对于本地链路上使用 mDNS 的系统，不需要在文件中更新和维护主机名就可以解析主机名到 IP 地址转换请求。

多播 DNS 服务搜索

网络服务包括打印、文件传输、音乐共享、照片服务器、文档和其他文件共享，以及由其他本地设备提供的服务。Oracle Solaris 中的 DNS 服务搜索支持包括来自 Apple Inc. 的一个开源框架和许多工具，使得在此 Oracle Solaris 发行版中应用程序能够使用 DNS 来通告和搜索网络服务。

对于用户而言，网络服务搜索使计算更为容易，因为他们可以浏览网络上的服务，而不需要手动查找服务。现有的标准和其他公司与工作组所做的工作确保了跨平台支持的可用性。

有关 DNS 的相关资料

有关 DNS 和 BIND 管理的信息，请参见下面的文档：

- ISC Web 站点 http://www.isc.org 中的《BIND 9 Administrator's Manual》
- `/usr/share/doc/bind/migration.txt` 文件中的 BIND 9 迁移说明文档
- ISC Web 站点 http://www.isc.org 中有关 BIND 功能、已知错误和缺陷的列表以及指向其他材料的链接
- 《DNS and Bind (5th Edition)》，由 Paul Albitz 和 Cricket Liu 编著（O'Reilly 出版社，2006 年）

DNS 和服务管理工具

必须使用服务管理工具 (Service Management Facility, SMF) 来管理 DNS 服务器守护进程 `named`。有关 SMF 的概述，请参见《在 Oracle Solaris 11.1 中管理服务和故障》中的第 1 章 “管理服务（概述）”。有关更多详细信息，另请参阅 `svcadm(1M)`、`svcs(1)` 和 `svccfg(1M)` 手册页。

以下列表提供了使用 SMF 服务来管理 DNS 服务时所需的某些重要信息的简短概述。

- 要对此服务执行管理操作，例如启用、禁用或重新启动，请使用 `svcadm` 命令。

  提示 – 通过使用 `-t` 选项临时禁用某个服务可以为服务配置提供一定的保护。如果服务是通过 `-t` 选项禁用的，则在重新引导后会为服务恢复原始设置。如果服务不是通过 `-t` 选项禁用的，则在重新引导后服务仍保持禁用状态。

- DNS 服务的故障管理资源标识符 (Fault Managed Resource Identifier, FMRI) 是 `svc:/network/dns/server:`*instance* 和 `svc:/network/dns/client:`*instance*。
- 使用 `svcs` 命令可以查询 DNS 服务器和客户机的状态。
  - 下面是 `svcs` 命令的示例及其输出：

    ```
    # svcs \*dns\*
    STATE          STIME    FMRI
    disabled       Nov_16   svc:/network/dns/multicast:default
    online         Nov_16   svc:/network/dns/server:default
    online         Nov_16   svc:/network/dns/client:default
    ```

  - 下面是 `svcs -l` 命令的示例及其输出。

```
# svcs -l /network/dns/server
fmri         svc:/network/dns/server:default
name         BIND DNS server
enabled      true
state        online
next_state   none
state_time   Tue Jul 26 19:26:12 2011
logfile      /var/svc/log/network-dns-server:default.log
restarter    svc:/system/svc/restarter:default
contract_id  83
manifest     /lib/svc/manifest/network/dns/server.xml
dependency   require_all/none svc:/system/filesystem/local (online)
dependency   require_any/error svc:/network/loopback (online)
dependency   optional_all/error svc:/network/physical (online)
```

- 如果您需要以不同的选项启动 DNS 服务，请使用 `svccfg` 命令更改 `svc:/network/dns/server` 服务的属性。有关示例，请参见第 43 页中的 “如何配置 DNS 服务器选项”。

当 DNS 服务器守护进程 `named` 由 SMF 管理时，如果发生了导致 `named` 不正常退出的意外事件，服务器会自动重新启动。此外，您可以使用 `svcadm` 命令来重新启动服务。通过使用 `rndc` 命令实现的特定于 BIND 的管理可以与 SMF 同时使用。

管理 DNS（任务）

本节介绍了以下任务：

▼ 如何安装 DNS 软件包

通常，DNS 软件包随 Oracle Solaris 发行版自动安装。如果在安装服务器时没有包括该软件包，请使用以下过程来安装该软件包。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **安装 DNS 软件包。**

```
# pkg install pkg:/service/network/dns/bind
```

▼ 如何配置 DNS 服务器

注 – 不建议通过配置 named 来指定一个更改根目录。更安全的选择是创建一个 Solaris 区域并将 named 配置为在该区域内运行。

1. **成为管理员。**

   有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2. **创建并验证 DNS 配置文件。**

   在 named 将启动之前，必须存在一个有效的配置文件。缺省情况下，此文件名为 /etc/named.conf。named 的配置可能非常简单。假如有 DNS 根服务器可供访问，一个空文件即可提供足够的信息来配置高速缓存专用服务器。

   ```
   # touch /etc/named.conf
   # named-checkconf -z /etc/named.conf
   ```

3. **可选创建 rndc 配置文件。**

   该文件用来配置 DNS 服务器的远程控制访问。

   ```
   # rndc-confgen -a
   wrote key file "/etc/rndc.key"
   ```

4. **可选更改 dns/server 服务的配置信息。**

   请参见第 43 页中的 “如何配置 DNS 服务器选项”。

5. **启动 DNS 服务。**

   ```
   # svcadm enable network/dns/server
   ```

▼ 如何创建 rndc.conf 文件

/etc/rndc.conf 用于通过使用 rndc 命令配置 DNS 服务器守护进程 named 的远程控制访问。要创建一个缺省文件，请使用以下过程。有关更多选项，请参阅 rndc.conf(4) 手册页。

1. **成为管理员。**

   有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2. **创建 rndc 配置文件。**

   ```
   # rndc-confgen -a
   wrote key file "/etc/rndc.key
   ```

3 **重新启动 DNS 服务。**

```
# svcadm restart dns/server:default
```

▼ 如何配置 DNS 服务器选项

此过程说明了如何为 named 通信选择 IPv4 传输协议。请参见 named(1M) 手册页。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **更改 dns/server 服务的配置信息。**

```
# svccfg -s network/dns/server
svc:/network/dns/server:default> setprop options/ip_interfaces = "IPv4"
svc:/network/dns/server:default> quit
```

3 **更新 SMF 系统信息库并启用 DNS 服务。**

```
# svcadm refresh network/dns/server
# svcadm enable network/dns/server
```

▼ 如何作为替代用户运行 DNS 服务

此过程说明了如何为用户指定相关授权来管理 named 守护进程。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **将用户添加到合适的角色。**

```
# usermod -A solaris.smf.manage.bind dnsadmin
```

3 **设置用户的服务属性。**

```
# svccfg -s network/dns/server
svc:/network/dns/server:default> setprop start/user = dnsadmin
svc:/network/dns/server:default> setprop start/group = dnsadmin
svc:/network/dns/server:default> exit
```

4 **为新的进程 ID 文件创建一个目录。**

因为只有 root 具有写入权限来创建缺省的进程 ID 文件 /var/run/named/named.pid，因此必须将 named 守护进程配置为使用一个替代文件。

```
# mkdir /var/named/tmp
# chown dnsadmin /var/named/tmp
```

5 **更改配置以使用新目录。**

将以下行添加到 named.conf 文件：

```
# head /etc/named.conf
options {
directory "/var/named";
pid-file "/var/named/tmp/named.pid";
};
```

6 **更新 SMF 系统信息库并重新启动 DNS 服务。**

```
# svcadm refresh svc:/network/dns/server:default
# svcadm restart svc:/network/dns/server:default
```

▼ 如何启用 DHCP 客户机

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **配置 DNS 域。**

首先，列出要搜索的域和 DNS 名称服务器的 IP 地址。然后，更新 SMF 系统信息库。

```
# svccfg -s network/dns/client
svc:/network/dns/client> setprop config/search = astring: ("example.com" "sales.example.com")
svc:/network/dns/client> setprop config/nameserver = net_address: (192.168.1.10 192.168.1.11)
svc:/network/dns/client> select network/dns/client:default
svc:/network/dns/client:default> refresh
svc:/network/dns/client:default> quit
```

3 **更新名称服务转换信息以使用 DNS。**

第一个命令更新 SMF 系统信息库中 DNS 配置信息。

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

4 **将新信息写入到 /etc/resolv.conf 文件中。**

/etc/resolv.conf 仍在被某些进程使用，因此在对 SMF 系统信息库进行了会更改该文件内容的任何更改后，都应当重新创建该文件。

```
# nscfg export svc:/network/dns/client:default
```

5 **启动运行 DNS 客户机所需的服务。**

```
# svcadm enable network/dns/client
# svcadm enable system/name-service/switch
```

▼ 如何对 DNS 服务器启动问题进行故障排除

不是必须执行所有这些步骤。如果您认为您在较早的步骤中查明了问题，可以前进到步骤 6 来使服务正常运行。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **检查 DNS 服务状态。**

```
# svcs -x dns/server:default
svc:/network/dns/server:default (BIND DNS server)
 State: online since Tue Oct 18 19:35:00 2011
   See: named(1M)
   See: /var/svc/log/network-dns-server:default.log
Impact: None.
```

3 **检查 DNS 服务日志文件。**

```
# tail /var/svc/log/network-dns-server:default.log
```

4 **检查系统日志消息。**

```
# grep named /var/adm/messages
```

5 **手动启动 named 守护进程。**

在前台运行 named 会强制将所有日志记录写入到标准错误，以便更容易找出问题。

```
# named -g
```

6 **在修复问题后，请清除“需要维护”状态。**

```
# svcadm clear dns/server:default
# svcs dns/server:default
STATE          STIME    FMRI
online         17:59:08 svc:/network/dns/server:default
```

▼ 如何验证 DNS 配置

在修改 DNS 配置时，您可以使用 named-checkzone 命令验证 /etc/named.conf 文件的语法。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **根据需要更改配置文件。**

在此示例中，更改了缺省目录。

```
# echo 'options {directory "/var/named";};' > /etc/named.conf
```

3 **验证文件内容。**

```
# named-checkconf
/etc/named.conf:1: change directory to '/var/named' failed: file not found

/etc/named.conf:1: parsing failed
```

在此示例中，检查失败，因为 `/var/named` 目录尚未创建。

4 **更正报告的所有错误。**

```
# mkdir /var/named
```

5 **重复步骤 3 和 4，直到不再报告错误。**

6 **可选要在正在运行的服务中反映更改，请使用下面的方法之一：**

- **使用 `rndc` 命令和 `reload` 或 `reconfig` 选项来更新配置，具体取决于所做的更改。**
- **重新启动 `named` 服务。**

  ```
  # svcadm restart svc:/network/dns/server:default
  ```

管理多播 DNS

以下各节介绍了如何启用多播 DNS (multicast DNS, mDNS) 和 DNS 服务搜索。此外，还提供了有关如何为 DNS 服务搜索来通告资源的示例。

▼ 如何启用 mDNS 和 DNS 服务搜索

要使 mDNS 和 DNS 服务搜索正常运行，必须在将要参与 mDNS 的所有系统上部署 mDNS。mDNS 服务用来通告系统上提供的服务的可用性。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **如果需要，安装 mDNS 软件包。**

```
# pkg install pkg:/service/network/dns/mdns
```

3 **更新名称服务转换信息。**

为了能够解析本地主机，请更改 `name-service/switch` 服务的 `config/host` 属性来将 `mdns` 包括为源。例如：

```
#  /usr/sbin/svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns mdns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch> quit
```

4 **启用 mDNS 服务。**

```
# svcadm enable svc:/network/dns/multicast:default
```

以此方式启用 mDNS 可以确保您的更改在升级和重新引导后保持不变。有关更多信息，请参见 svcadm(1M) 手册页。

5 **可选如果需要，检查 mDNS 错误日志。**

检查 mDNS 服务日志 `/var/svc/log/network-dns-multicast:default.log` 来查看错误或消息。

为 DNS 通告资源

您可以使用 `dns-sd` 命令作为网络诊断工具来浏览和搜索服务，这类似于使用 `ping` 或 `traceroute` 命令的方式。

`dns-sd` 命令主要以交互方式进行使用，这主要是因为它的命令行参数和输出格式在以后可能会更改，这使得通过 shell 脚本调用它具有不可预测性和风险。此外，DNS 服务搜索 (DNS service discovery, DNS-SD) 的异步性质使其无法轻易地用于面向脚本的编程。

有关完整信息，请参见 `dns-sd` (1M) 手册页。要将 DNS 服务纳入应用程序中，请参见 `libdns-sd`(3DNS_SD) 手册页。

下面是使用 DNS 服务搜索来通告服务的示例。

示例 3–1 通告打印服务

以下命令通告 LPR 打印服务存在于名为 `My Test` 的系统的端口 `515` 上，因此它将可供 DNS-SD 兼容打印客户机使用：

```
# dns-sd -R "My Test" _printer._tcp. . 515 pdl=application/postscript
```

要使此注册可用，必须在端口 `515` 上提供 LPR 服务。

示例 3–2 通告 Web 页

以下命令通告 `My Test` 系统上的 HTTP 服务器正通过端口 `80` 提供的一个 Web 页。该 Web 页将出现在 Safari 中的 Bonjour 列表中和其他 DNS-SD 兼容 Web 客户机中。

示例 3–2 通告 Web 页 （续）

```
# dns-sd -R "My Test" _http._tcp . 80 path=/path-to-page.html
```

DNS 参考

本节包含其中列出了与 DNS 服务关联的文件、守护进程和命令的许多表。此外，还包含其中列出了在生成 BIND 的 ISC 版本时使用的一些标志的一个表。

DNS 文件

下表介绍了与 DNS 服务关联的文件。

表 3–1 DNS 文件

文件名	功能
/etc/named.conf	提供 named 守护进程的配置信息。有关更多信息，请参见 named.conf(4) 手册页。
/etc/rndc.conf	提供 rndc 命令的配置信息。有关更多信息，请参见 rndc.conf(4) 手册页。

DNS 命令和守护进程

下表介绍了与 DNS 服务关联的命令和守护进程。

表 3–2 DNS 命令和守护进程

文件名	功能
/usr/bin/dns-sd	查找或列出 mDNS 服务使用的资源。有关更多信息，请参见 dns-sd(1M) 手册页。
/usr/sbin/dig	从 DNS 服务器请求 DNS 响应。通常用于故障排除。有关更多信息，请参见 dig(1M) 手册页。
/usr/sbin/dnssec-dsfromkey	基于密钥文件生成 DS RR。有关更多信息，请参见 dnssec-dsfromkey(1M) 手册页。
/usr/sbin/dnssec-keyfromlabel	从加密设备检索选定的密钥并生成一个密钥文件。有关更多信息，请参见 dnssec-keygen(1M) 手册页。
/usr/sbin/dnssec-keygen	创建用于安全 DNS 和事务签名 (transaction signature, TSIG) 的密钥和密钥文件。有关更多信息，请参见 dnssec-keygen(1M) 手册页。

表 3–2 DNS 命令和守护进程 （续）

文件名	功能
/usr/sbin/dnssec-signzone	对 DNS 区域进行签名。有关更多信息，请参见 dnssec-signzone(1M) 手册页。
/usr/sbin/host	执行简单的 DNS 查找，通常是将主机名转换为 IP 地址或者将 IP 地址转换为主机名。有关更多信息，请参见 host(1M) 手册页。
/usr/sbin/named	DNS 服务器守护进程，它响应来自客户机的信息请求。有关更多信息，请参见 named(1M) 手册页。
/usr/sbin/named-checkconf	检查 named.conf 文件的语法。有关更多信息，请参见 named(1M) 手册页。
/usr/sbin/named-checkzone	检查 DNS 区域文件的语法和完整性。有关更多信息，请参见 named-checkzone(1M) 手册页。
/usr/sbin/named-compilezone	转换 DNS 区域文件。有关更多信息，请参见 named-compilezone(1M) 手册页。
/usr/sbin/nscfg	传统的名称服务配置实用程序，它从 SMF 系统信息库导入或导出 resolv.conf 内容。有关更多信息，请参见 nscfg(1M) 手册页。
/usr/sbin/nslookup	已过时：查询 DNS 服务器。请改用 dig 命令。
/usr/sbin/nsupdate	向 DNS 服务器提交 DNS 更新请求。有关更多信息，请参见 nsupdate(1M) 手册页。
/usr/sbin/rndc	提供对 DNS 服务器守护进程的远程控制。有关更多信息，请参见 rndc(1M) 手册页。
/usr/sbin/rndc-confgen	为 rndc 命令生成配置文件。有关更多信息，请参见 rndc-confgen(1M) 手册页。

在生成 BIND 时使用的编译标志

您可以使用 named -V 命令查看用于编译 BIND 的标志。此表显示了在为 Oracle Solaris 11 发行版生成 BIND 的 ISC 版本时使用的某些编译标志。

表 3–3 BIND 编译标志

标志名称	功能
with-openssl	使生成的 BIND 提供加密和安全套接字层 (Secure Sockets Layer, SSL) 支持，这是 DNSSEC 所必需的
enable-threads	启用多线程
enable-devpoll	使用 /dev/poll 驱动程序以快速轮询许多文件描述符

表 3–3 BIND 编译标志 （续）

标志名称	功能
disable-openssl-version-check	禁用 OpenSSL 版本检查，因为 OpenSSL 是由一个单独的动态库提供的
enable-fixed-rrset	启用固定的资源记录集排序，这是实现向后兼容性所必需的
with-pkcs11	启用 OpenSSL 加密硬件支持

◆ ◆ ◆ 第 4 章

4 设置 Oracle Solaris Active Directory 客户机（任务）

nss_ad 命名服务模块提供了 passwd、shadow 和 group 文件的后端。nss_ad 模块使用 Active Directory (AD) 及其本机架构作为命名服务从 AD 林解析用户和组名称及 ID。本章包含以下主题：

nss_ad 命名服务模块概述

Oracle Solaris 客户机必须先加入某个 AD 域，然后才能使用任何 AD 互操作功能（包括 nss_ad）。kclient 实用程序用于将客户机加入到 AD。执行加入操作时，kclient 在客户机上配置 Kerberos v5。然后，通过在受支持数据库的 nsswitch.conf 文件中将 ad 指定为源可以使用 nss_ad 来解析命名服务请求。nss_ad 模块使用主机凭证在 AD 中查找命名服务信息。

nss_ad 模块使用 DNS 服务器记录来自动搜索 AD 目录服务器，例如域控制器和全局目录服务器。因此，必须在 Oracle Solaris 客户机上正确配置 DNS。nss_ad 模块还使用 LDAP v3 协议访问 AD 服务器中的命名信息。由于 nss_ad 适用于本机 AD 架构，因此无需修改 AD 服务器架构。

nss_ad 模块当前不支持 Windows 用户登录到 Oracle Solaris 系统。在支持这类登录之前，这类用户应当继续使用传统的后端（例如 nis 和 ldap）进行登录。

必须启用 idmap 和 svc:/system/name-service/cache 服务才能使用 nss_ad。nss_ad 模块使用 idmap 服务在 Windows 安全标识符 (security identifiers, SID)、UNIX 用户标识符 (UNIX user identifier, UID) 和组标识符 (group identifier, GID) 之间进行映射。

请确保所有 AD 用户名和组名都以域名进行了限定，例如 user@domain 或 group@domain。例如，假如 dana 是名为 domain 的域中的一个有效的 Windows 用户，则 getpwnam(dana) 将失败，但 getpwnam(dana@domain) 将成功。

以下其他规则也适合 nss_ad 模块：

- 与 AD 一样，nss_ad 对用户名和组名执行不区分大小写的匹配。
- 在 UTF-8 语言环境中或者用户和组的名称中只有 ASCII 字符的域中，请仅使用 nss_ad 模块。
- 众所周知的 SID 是标识 Windows 系统中的通用用户或通用组的一组 SID。它们不是特定于域的，并且它们的值在所有 Windows 操作系统中保持不变。这些众所周知的 SID 的名称以字符串 BUILTIN 予以限定，例如 Remote Desktop Users@BUILTIN。
- nss_ad 模块不支持枚举。因此，使用它们的 getpwent() 和 getgrent() 接口与命令（例如 getent passwd 和 getent group） 无法从 AD 检索信息。
- nss_ad 模块当前仅支持 passwd 和 group 文件，nss_ad 不支持位于 passwd 项后的其他命名服务数据库，例如 audit_user 和 user_attr。如果 ad 后端已被处理（基于配置），则对于这些数据库，它将返回 "NOT FOUND"。

▼ 如何配置 nss_ad 模块

nss_ad 模块要求 Oracle Solaris 客户机使用 DNS 进行主机解析。

1 **配置 DNS 服务。**

有关说明，请参见第 44 页中的 “如何启用 DHCP 客户机”。

注 – AD 域名称必须通过 domain 指令进行指定，或者指定为由 search 指令指定的列表中的第一个项。

如果同时指定了这两个指令，将优先考虑最后指定的那个指令。这是 idmap 自动搜索功能正常工作所必需的。

在下面的示例中，dig 命令验证是否可以通过使用 AD 服务器的名称和 IP 地址来解析该服务器。

```
# dig -x 192.168.11.22 +short
myserver.ad.example
# dig myserver.ad.example +short
192.168.11.22
```

2 **将 dns 添加到 hosts 的命名服务的列表中。**

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

注 – 要包含其他命名服务（例如 nis 或 ldap）用于主机解析，请将其添加在 dns 之后。

3 **确认 DNS 服务已启用且处于联机状态。**

例如：

```
# svcs svc:/network/dns/client
STATE STIME FMRI
online Oct_14 svc:/network/dns/client:default
```

4 **使用 kclient 实用程序将系统加入 AD 域。**

例如：

```
# /usr/sbin/kclient -T ms_ad
```

5 **将 ad 添加到 password 和 group 的命名服务的列表中。**

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/password = astring: "files nis ad"
svc:/system/name-service/switch> setprop config/group = astring: "files nis ad"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

6 **启用 idmap 服务。**

```
# svcadm enable idmap
```

7 **更新名称服务转换服务的 SMF 系统信息库。**

```
# svcadm refresh name-service/switch
```

注 – 每次刷新名称服务转换时，如有必要，nscd 模块都将自动重新启动。

8 **确认您可以访问 AD 中的 user 和 group 信息。**

例如：

```
# getent passwd 'test_user@example'
test_user@example:x:2154266625:2154266626:test_user::
# getent passwd 2154266625
test_user@example:x:2154266625:2154266626:test_user::
```

口令更新

passwd(4) 手册页包含名称服务转换中的 config/passwd 属性的有效格式列表。支持将 ad 添加到这些配置中。不过，不支持通过 passwd 命令更改 AD 用户口令。如果在口令更新期间在 passwd 项中发现了 ad，则它将被跳过。请使用 kpasswd 命令来更新 AD 用户口令。

可以向名称服务转换中现有的有效 password 和 group 项中添加 ad 搜索顺序。例如：

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/password = astring: "files nis ad"
svc:/system/name-service/switch> setprop config/group = astring: "files nis ad"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

nss_ad 命名服务模块如何从 AD 检索数据

下节介绍了 nss_ad 模块如何通过从 AD 检索相应的数据来解析 passwd、shadow 和 group 文件的命名服务请求。

检索 passwd 信息

以下语法显示了 passwd 项的正确格式：

username:*password*:*uid*:*gid*:*gecos*:*home-directory*:*login-shell*

有关更多信息，请参见 passwd(4) 手册页。

nss_ad 模块从 AD 检索 passwd 信息，如下所述：

- *username*－字段使用 samAccountName AD 属性的值并且由对象所在的域名予以限定，例如 terryb@example.com。
- *password*－字段使用 x 的值，因为用户口令在 AD 对象中不可用。
- *uid*－字段使用来自 objectSID AD 属性的 Windows 用户的 SID，该 SID 通过使用 idmap 服务映射到 UID。
- *gid*－字段使用 Windows 用户的主组 SID，该 SID 通过使用 idmap 服务映射到 GID。组 SID 是通过将 primaryGroupID AD 属性的值附加到域 SID 之后获得的。对于 AD 中的用户，primaryGroupID 属性是一个可选属性，因此它可能不存在。如果该属性不存在，则 nss_ad 将使用 idmap 对角映射实用程序来从 objectSID 属性映射用户 SID。
- *gecos*－CN AD 属性的值。
- *home-directory*－homeDirectory AD 属性的值（如果存在一个值）。否则，该字段将保留为空。
- *login-shell*－字段保留为空，因为在本机 AD 架构中没有登录 shell 属性。

检索 shadow 信息

以下语法显示了 shadow 项的正确格式：

username:*password*:*lastchg*:*min*:*max*:*warn*:*inactive*:*expire*:*flag*

有关更多信息，请参见 shadow(4) 手册页。

nss_ad 模块从 AD 检索 shadow 信息，如下所述：

- *username*－字段使用 samAccountName AD 属性的值并且由对象所在的域名予以限定，例如 terryb@example.com。
- *password*－字段使用 *NP* 的值，因为用户口令在 AD 对象中不可用。

其余 shadow 字段将保留为空，因为 shadow 字段与 AD 和 Kerberos v5 没有关系。

检索 group 信息

以下语法显示了 group 项的正确格式：

groupname:*password*:*gid*:*user-list*

有关更多信息，请参见 group(4) 手册页。

nss_ad 模块从 AD 检索信息，如下所述：

- *groupname*－字段使用 samAccountName AD 属性的值并且由对象所在的域名予以限定，例如 admins@example。
- *password*－字段保留为空，因为 Windows 组没有口令。
- *gid*－此字段使用来自 objectSID AD 属性的 Windows 组的 SID，该 SID 通过使用 idmap 服务映射到 GID。
- *user-list*－字段保留为空。

第 2 部 分

NIS 设置和管理

本部分概述了网络信息服务 (Network Information Service, NIS) 命名服务，还介绍了有关 Oracle Solaris OS 中 NIS 的设置、管理及故障排除。

◆ ◆ ◆ 第 5 章

网络信息服务（概述）

本章概述了网络信息服务 (Network Information Service, NIS)。

NIS 是一种分布式命名服务，提供了一种标识和定位网络对象及资源的机制。NIS 以使用传输协议且独立于介质的方式为网络范围内的信息提供统一的存储和检索方法。

本章包含以下主题：

NIS 介绍

通过运行 NIS，系统管理员可在各种服务器（**主服务器**和**从属服务器**）中分布管理数据库，这些数据库称为**映射**。管理员可以通过一种自动而且可靠的方式从一个集中位置更新这些数据库，以确保整个网络中的所有客户机都一致共享相同的命名服务信息。

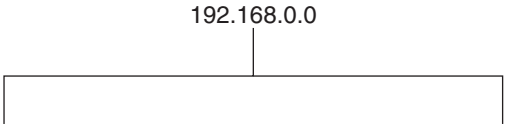
NIS 是独立于 DNS 开发的，并且其侧重点也稍有不同。DNS 侧重于使用计算机名称而不是数字 IP 地址来简化通信，而 NIS 侧重于对各种网络信息进行集中控制来更好地管理网络。NIS 不仅存储有关计算机名和地址的信息，还存储有关用户、网络本身以及网络服务的信息。这种网络**信息**的集合称为 NIS **名称空间**。

注 – 在一些上下文中，**计算机**名称是指**主机**名或**计算机**名称。本讨论中使用**计算机**，但一些屏幕消息或 NIS 映射名中可能使用**主机**或**计算机**。

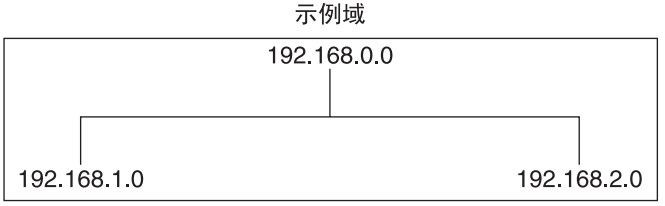
NIS 体系结构

NIS 使用客户机/服务器方案。NIS 服务器向 NIS 客户机提供服务。主要的服务器称为**主**服务器，为确保其可靠，主服务器还具有备份，即**从属**服务器。主服务器和从属服务器都使用 NIS 信息检索软件，并且都存储 NIS 映射。

NIS 使用域来编排其名称空间中的计算机、用户和网络。不过，它不使用域分层结构。NIS 名称空间是不分层的。



因此，此物理网络将被编排为一个 NIS 域。



NIS 域不能仅使用 NIS 直接连接到 Internet。但是，如果组织要使用 NIS 并且希望连接到 Internet，可以将 NIS 与 DNS 结合使用。您可以使用 NIS 管理所有本地信息，使用 DNS 进行 Internet 主机查找。NIS 还提供转发服务，当 NIS 映射中找不到信息时，该服务会将主机查找转发给 DNS。Oracle Solaris 系统还允许您设置名称服务转换以便可以按以下方式对主机查找请求进行定向：

- 仅访问 DNS
- 访问 DNS，但是如果在 DNS 中未找到主机，则访问 NIS
- 访问 NIS，但是如果 NIS 未找到主机，则访问 DNS

为实现最大的互操作性，建议使用 DNS 服务进行主机查找。有关详细信息，请参见第 2 章，名称服务转换（概述）。

NIS 计算机类型

NIS 计算机有三种类型。

- 主服务器
- 从属服务器
- NIS 服务器的客户机

任何计算机都可以成为 NIS 客户机，但只有带磁盘的计算机才能成为 NIS 服务器，包括主服务器或从属服务器。服务器也是客户机，通常是自身的客户机。

NIS 服务器

NIS 服务器分为两种：主服务器和从属服务器。指定为主服务器的计算机包含系统管理员根据需要创建和更新的映射集合。每个 NIS 域必须有且仅有一台主服务器，该服务器可以传播 NIS 更新，并最大程度地减少对性能的影响。

您可以将域中附加的其他 NIS 服务器指定为从属服务器。从属服务器具有主 NIS 映射集合的完整副本。只要主服务器映射进行更新，该更新便会传播到从属服务器。从属服务器可以处理主服务器的任何请求溢出，从而最大程度地减少“服务器不可用”错误。

通常，系统管理员会为所有 NIS 映射指定一台主服务器。但是，由于每个单个 NIS 映射中都对主服务器的计算机名进行了编码，因此，可以指定不同的服务器充当不同映射的主服务器和从属服务器。为了尽量避免混淆，请指定一台单个服务器作为您在一个域中创建的所有映射的主服务器。本章的示例假设将一台服务器用作域中所有映射的主服务器。

NIS 客户机

NIS 客户机运行进程，以向服务器中的映射请求数据。由于所有 NIS 服务器都应具有相同信息，因此客户机并不区分主服务器和从属服务器。

注 – Oracle Solaris 操作系统不支持 NIS 客户机与本地 LDAP 客户机共存于同一客户机系统中的配置。

NIS 元素

NIS 命名服务由以下元素组成：

- 域（请参见第 62 页中的 “NIS 域”）
- 守护进程（请参见第 62 页中的 “NIS 守护进程”）
- 命令（请参见第 63 页中的 “NIS 命令”）
- 映射（请参见第 64 页中的 “NIS 映射”）

NIS 域

NIS **域**是共享一组通用 NIS 映射的主机的集合。每个域都有一个域名，共享这组通用映射的每台计算机都属于该域。

NIS 域和 DNS 域不必相同。在某些环境中，NIS 域是基于企业范围内的网络子网管理布局定义的。DNS 名称和域是根据 Internet DNS 命名标准和分层结构定义的。这两种命名域命名系统可以配置为完全匹配的，也可以不配置为完全匹配的。这两种服务的域名是分别控制的，并可以按不同的方式进行配置。

任何主机都可以属于某个给定域，只要同一网络或子网中存在用于该域映射的服务器即可。NIS 域查找使用远程过程调用 (remote procedure call, RPC)。因此，NIS 要求所有客户机和向这些客户机提供直接服务的所有服务器计算机必须存在于同一个可访问的子网中。将每个管理子网作为单独的 NIS 域（不同于企业范围的 DNS 域）进行管理但使用从一台通用的主计算机管理的通用数据库，这一做法并不罕见。NIS 域名和所有共享的 NIS 配置信息通过 `svc:/network/nis/domain` SMF 服务进行管理。

NIS 守护进程

NIS 服务是由下表中显示的守护进程提供的。NIS 服务由 SMF 进行管理。使用 `svcadm` 命令可以对此服务执行启用、禁用或重新启动等管理操作。有关 SMF 的概述，请参见《在 Oracle Solaris 11.1 中管理服务和故障》中的第 1 章 “管理服务（概述）”。有关更多详细信息，另请参阅 `svcadm(1M)` 和 `svcs(1)` 手册页。

表 5–1 NIS 守护进程

守护进程	功能
`nscd`	一项客户机服务，提供了一个用于大多数名称服务请求的高速缓存，该高速缓存由 `svc:/system/name-service/cache` 服务进行管理
`rpc.yppasswdd`	由 `svc:/network/nis/passwd` 服务管理的 NIS 口令更新守护进程 **注 –** `rpc.yppasswdd` 守护进程将所有以 `r` 开头的 shell 视为受限制的 shell。例如，如果您位于 `/bin/rksh` 中，将不允许从该 shell 更改到其他 shell 中。如果您有以 `r` 开头的 shell，但不想受到此类限制，请参阅第 8 章，NIS 故障排除了解解决方法。

表 5–1 NIS 守护进程 （续）

守护进程	功能
rpc.ypupdated	用于修改诸如 publickey 之类的映射的一个守护进程，由 svc:/network/nis/update 服务进行管理
ypbind	由 svc:/network/nis/client 服务管理的绑定进程
ypserv	由 svc:/network/nis/server 服务管理的服务器进程
ypxfrd	由 svc:/network/nis/xfr 服务管理的一个高速映射传送守护进程

NIS 命令

许多命令都支持 NIS 服务，下表中介绍了这些命令。

表 5–2 NIS 命令摘要

命令	说明
make	通过读取 /var/yp/Makefile 来更新 NIS 映射（当在 /var/yp 目录中运行此命令时）。您可以使用 make 根据输入文件来更新所有映射或更新个别映射。ypmake(1M) 手册页中介绍了用于 NIS 的 make 功能。
makedbm	接受一个输入文件并将其转换为 dbm.dir 和 dbm.pag 文件。NIS 使用有效的 dbm 文件作为映射。使用 makedbm -u 还可以反汇编映射，从而可以了解构成它的关键字-值对。
ypcat	显示 NIS 映射的内容。
ypinit	自动根据输入文件为 NIS 服务器创建映射。它还用来在客户机上构造初始的 /var/yp/binding/*domain*/ypservers 文件。初次设置主 NIS 服务器和从属 NIS 服务器时请使用 ypinit。
ypmatch	列显 NIS 映射中的一个或多个指定关键字的值。您不能指定要查看的 NIS 服务器映射的版本。
yppoll	显示在指定的服务器上运行的 NIS 映射的版本。还会列出映射的主服务器。
yppush	将 NIS 映射的新版本从 NIS 主服务器复制到其从属服务器。您需要在主 NIS 服务器上运行 yppush 命令。
ypset	指示 ypbind 进程绑定到指定的 NIS 服务器。该命令不能随意使用。出于安全原因，建议不要使用该命令。有关 ypbind 进程的 ypset 和 ypsetme 选项的信息，请参见 ypset(1M) 和 ypbind(1M) 手册页。
ypwhich	显示客户机此刻使用哪台 NIS 服务器提供 NIS 服务。如果调用时使用了 -m *mapname* 选项，则此命令将显示哪台 NIS 服务器是每个映射的主服务器。如果只使用 -m，此命令将显示所有可用映射的名称及其各自的主服务器。

表 5–2 NIS 命令摘要 （续）

命令	说明
ypxfr	使用 NIS 本身作为传输介质，将 NIS 映射从远程服务器引入到本地 /var/yp/*domain* 目录。您可以通过交互方式运行 ypxfr，或从 crontab 文件中定期运行该命令。ypserv 也会调用该命令以启动传送。

NIS 映射

NIS 映射中的信息是以 ndbm 格式存储的。ypfiles(4) 和 ndbm(3C) 手册页解释了映射文件的格式。

NIS 映射扩展了对 UNIX /etc 数据和其他配置文件（例如 passwd、shadow 和 group）的访问，以便可以在网络上的系统之间共享相同的数据。共享这些文件简化了那些数据文件的管理性更新和管理。只需做很少的工作即可部署 NIS。不过，大型企业尤其是那些有安全要求的大型企业应当考虑改用 LDAP 命名服务。在运行 NIS 的网络中，每个 NIS 域的 NIS 主服务器会保留一组 NIS 映射，以供域中的其他计算机查询。NIS 从属服务器也会保留主服务器映射的副本。NIS 客户机可从主服务器或从属服务器获取名称空间信息。

NIS 映射实质上是包含两个列的表。一列为**关键字**，另一列为与该关键字相关的信息。NIS 通过搜索关键字为客户机查找信息。由于每个映射使用不同的关键字，因此有些信息存储在多个映射中。例如，计算机的名称和地址存储在两个映射中：hosts.byname 和 hosts.byaddr。当服务器已知计算机的名称而需要查找其地址时，它将在 hosts.byname 映射中进行查找。当服务器已知计算机的地址而需要查找其名称时，它将在 hosts.byaddr 映射中进行查找。

NIS Makefile 存储在安装时被指定为 NIS 服务器的计算机上的 /var/yp 目录中。在该目录中运行 make 会使 makedbm 基于输入文件创建或修改缺省的 NIS 映射。

注 – 请始终在主服务器上创建映射，因为在从属服务器上创建的映射将不会自动推送到主服务器。

缺省 NIS 映射

Oracle Solaris 系统中提供了一组缺省 NIS 映射。您可能要使用所有这些映射，也可能只使用其中的部分映射。NIS 还可以使用您在安装其他软件产品时创建或添加的任何映射。

NIS 域的缺省映射位于每台服务器的 /var/yp/*domain–name* 目录中。例如，属于域 test.com 的映射位于每台服务器的 /var/yp/test.com 目录中。

下表介绍了缺省 NIS 映射并列出了每个映射的相应源文件名称。

表 5–3 NIS映射说明

映射名	相应的源文件	说明
audit_user	audit_user	包含用户审计预选数据。
auth_attr	auth_attr	包含授权名称和说明。
bootparams	bootparams	包含客户机在引导期间所需文件的路径名：root、swap，也可能是其他名称。
ethers.byaddr	ethers	包含计算机名和以太网地址。以太网地址是映射中的关键字。
ethers.byname	ethers	与 ethers.byaddr 相同，但关键字是计算机名而非以太网地址。
exec_attr	exec_attr	包含配置文件执行属性。
group.bygid	group	包含以组 ID 作为关键字的组安全信息。
group.byname	group	包含以组名作为关键字的组安全信息。
hosts.byaddr	hosts	包含计算机名和 IP 地址，以 IP 地址作为关键字。
hosts.byname	hosts	包含计算机名和 IP 地址，以计算机（主机）名作为关键字。
mail.aliases	aliases	包含别名和邮件地址，以别名作为关键字。
mail.byaddr	aliases	包含邮件地址和别名，以邮件地址作为关键字。
netgroup.byhost	netgroup	包含组名、用户名和计算机名。
netgroup.byuser	netgroup	与 netgroup.byhost 相同，但关键字为用户名。
netgroup	netgroup	与 netgroup.byhost 相同，但关键字为组名。
netid.byname	passwd、hosts group	用于 UNIX 形式的验证。包含计算机名和邮件地址（包括域名）。如果存在可用的 netid 文件，则除了查询通过其他文件提供的数据外，还会查询该文件。
publickey.byname	publickey	包含安全 RPC 使用的公钥数据库。
netmasks.byaddr	netmasks	包含要与 IP 一起提交的网络掩码，以地址作为关键字。
networks.byaddr	networks	包含系统已知的网络的名称及其 IP 地址，以地址作为关键字。

表 5–3 NIS 映射说明 （续）

映射名	相应的源文件	说明
networks.byname	networks	与 networks.byaddr 相同，但关键字为网络的名称。
passwd.adjunct.byname	passwd 和 shadow	包含 C2 客户机的审计信息和隐藏的口令信息。
passwd.byname	passwd 和 shadow	包含以用户名作为关键字的口令信息。
passwd.byuid	passwd 和 shadow	与 passwd.byname 相同，但关键字为用户 ID。
prof_attr	prof_attr	包含执行配置文件的属性。
protocols.byname	protocols	包含网络可识别的网络协议。
protocols.bynumber	protocols	与 protocols.byname 相同，但关键字为协议编号。
rpc.bynumber	rpc	包含系统可识别的 RPC 的程序编号和名称。关键字为 RPC 程序编号。
services.byname	services	列出网络可识别的 Internet 服务。关键字为端口或协议。
services.byservice	services	列出网络可识别的 Internet 服务。关键字为服务名。
user_attr	user_attr	包含用户和角色的扩展属性。
ypservers	N/A	列出网络可识别的 NIS 服务器。

当实现了 NIS 到 LDAP 转换时，ageing.byname 映射包含 yppasswdd 守护进程用来在目录信息树 (directory information tree, DIT) 中读写口令生命期信息的信息。如果不使用口令生命期，可以将其从映射文件中注释掉。有关 NIS 到 LDAP 转换的更多信息，请参见第 15 章，从 NIS 转换为 LDAP（任务）。

使用 NIS 映射

与使用 /etc 文件系统进行更新相比，NIS 可使更新网络数据库变得更加简单。您无需在每次修改网络环境时更改每台计算机中的管理 /etc 文件。

不过，与 /etc 文件相比，NIS 也没有提供额外的安全性。如果需要额外的安全性，例如限制对网络数据库的访问、通过网络在使用 SSL 的情况下发送搜索结果、使用更高级的功能（例如 Kerberos 保护的搜索），则应当改用 LDAP 命名服务。

例如，向运行 NIS 的网络中添加新用户时，只需要更新主服务器中的输入文件并运行 make 命令即可。此命令将自动更新 passwd.byname 和 passwd.byuid 映射。然后，这些映射将传送给从属服务器，并可供域中所有客户机及其程序使用。当客户机或应用程

序通过用户名或 UID 来请求信息时，NIS 服务器将相应地引用 passwd.byname 或 passwd.byuid 映射，并将所请求的信息发送到客户机。

您可以使用 ypcat 命令显示映射中的值。ypcat 基本格式为：

```
% ypcat mapname
```

其中，*mapname* 是要查看的映射的名称或其**昵称**。如果映射仅由关键字组成（如 ypservers），请使用 ypcat -k。否则，ypcat 将显示空白行。ypcat(1) 手册页介绍了 ypcat 的更多选项。

您可以使用 ypwhich 命令来确定哪台服务器是特定映射的主服务器。键入以下命令。

```
% ypwhich -m mapname
```

其中，*mapname* 是要查找其主服务器的映射的名称或昵称。ypwhich 给出的响应是显示主服务器的名称。有关完整信息，请参阅 ypwhich(1) 手册页。

NIS 映射昵称

昵称是完整映射名的别名。要获得可用映射昵称（如 passwd.byname 的 passwd）的列表，请键入 ypcat -x 或 ypwhich -x。

昵称存储在 /var/yp/nicknames 文件中，该文件中包含映射昵称，后跟映射的完全指定名称，两者之间以空格分隔。您可以对此列表进行添加或修改。目前，昵称限制在 500 个以内。

NIS 绑定

NIS 客户机通过绑定进程连接到一台 NIS 服务器。此进程由 svc:/network/nis/client 和 svc:/network/nis/domain 服务提供支持。必须启用这些服务，NIS 服务才能工作。svc:/network/nis/client 服务能够以下列两种模式之一工作：服务器列表或广播。

- 服务器列表－在服务器列表模式下，ypbind 进程查询 svc:/network/nis/domain 服务来获取域中所有 NIS 服务器的名称。ypbind 进程只绑定到此文件中的服务器。

  可以通过使用 svccfg 命令添加 NIS 服务器。它们将添加到 svc:/network/nis/domain 服务中的 config/ypservers 属性。每个属性值都代表一台特定的 NIS 服务器。

  此外，在 svc:/network/nis/domain 服务中指定的任何服务器名称在 /etc/inet/hosts 文件中都必须有一个对应的项，NIS 绑定功能才能工作。
- 广播－ypbind 进程还可以使用 RPC 广播来启动绑定。因为广播只是不会进一步路由的本地子网事件，所以必须至少有一台服务器（主服务器或从属服务器）与客户机位于同一个子网中。服务器本身可能会存在于不同的子网中，因为映射传播可跨越子网边界。在子网环境中，一种常用方法是使子网路由器成为 NIS 服务器。这样，域服务器便可为任何一个子网接口上的客户机提供服务。

通常情况下，广播模式是建议使用的运行模式。广播模式不要求指定额外的主机项（或对 /etc/inet/hosts 进行更改）。

通常，客户机绑定到服务器后，会保持与该服务器的绑定状态，直到某些原因引起状态更改为止。例如，如果服务器中断服务，它所服务的客户机将绑定到新服务器。

要确定当前正在为特定客户机提供服务的 NIS 服务器，请使用以下命令。

```
% ypwhich machinename
```

其中，*machinename* 是客户机的名称。如果不提供计算机名，ypwhich 命令将缺省认为是本地计算机（即运行命令时所在的计算机）。

服务器列表模式

在服务器列表模式下，绑定进程的工作过程如下：

1. 在 NIS 客户机上运行的、需要 NIS 映射所提供信息的任何程序都向 ypbind 请求服务器的名称。
2. ypbind 守护进程在 /var/yp/binding/*domainname*/ypservers 文件中查找域中 NIS 服务器的列表。
3. ypbind 守护进程启动到列表中第一台服务器的绑定。如果该服务器未响应，ypbind 会尝试第二台，直至找到一台服务器或找遍整个列表。
4. ypbind 守护进程将要联系的服务器告知客户机进程。然后，客户机会将请求直接发送到该服务器。
5. NIS 服务器上的 ypserv 守护进程通过查询相应映射来处理请求。
6. ypserv 守护进程将请求的信息发送回客户机。

广播模式

在广播模式下，绑定进程的工作过程如下：

1. ypbind 守护进程启动时必须设置了广播选项 (broadcast)。
2. ypbind 守护进程发出 RPC 广播来搜索 NIS 服务器。

注 – 为了支持此类客户机，需要让每个请求 NIS 服务的子网具有 NIS 服务器。

---

3. ypbind 守护进程启动到最先对广播做出响应的服务器的绑定。
4. ypbind 守护进程将要联系的服务器告知客户机进程。然后，客户机会将请求直接发送到该服务器。
5. NIS 服务器上的 ypserv 守护进程通过查询相应映射来处理请求。

6. ypserv 守护进程将请求的信息发送回客户机。

◆ ◆ ◆ 第 6 章

6 设置和配置 NIS（任务）

本章介绍网络信息服务 (Network Information Service, NIS) 的初始设置和配置。

注 – 在一些上下文中，**计算机**名称是指**主机**名或**计算机**名称。本讨论中使用“计算机”，但一些屏幕消息或 NIS 映射名中可能使用**主机**或**计算机**。

本章包含以下主题：

配置 NIS 任务列表

任务	说明	参考
为转换准备源文件。	在基于本地 /etc 文件生成 NIS 映射之前，您需要整理这些文件。	第 75 页中的“如何为转换准备源文件”
设置主服务器。	创建一台主服务器，这是 NIS 信息的主要来源。	第 78 页中的“如何设置主服务器”
在主服务器上启动 NIS。	开始从 NIS 服务器提供 NIS 信息。	第 80 页中的“在 NIS 服务器上启动和停止 NIS 服务”
设置从属服务器。	创建一台从属服务器，这是 NIS 信息的次要来源。	第 82 页中的“如何设置从属服务器”

任务	说明	参考
设置 NIS 客户机。	使客户机能够使用 NIS 信息。	第 85 页中的 “管理 NIS 客户机”

配置 NIS 之前的准备工作

在配置 NIS 名称空间之前，必须执行以下操作。

- 规划 NIS 域。有关详细信息，请参见第 73 页中的 “规划 NIS 域”。
- 在将使用 NIS 的所有计算机上安装正确配置的名称服务转换信息。有关详细信息，请参见第 2 章，名称服务转换（概述）。

NIS 和服务管理工具

NIS 服务由服务管理工具管理。有关 SMF 的概述，请参见《在 Oracle Solaris 11.1 中管理服务和故障》中的第 1 章 “管理服务（概述）”。有关更多详细信息，另请参阅 `svcadm(1M)` 和 `svcs(1)` 手册页。

以下列表提供了使用 SMF 服务来管理 NIS 时所需的某些重要信息的简短概述。

- 使用 `svcadm` 命令可以对此服务执行启用、禁用或重新启动等管理操作。不过，也可以从命令行使用 `ypstart` 和 `ypstop` 来启动和停止 NIS。有关更多信息，请参见 `ypstart(1M)` 和 `ypstop(1M)` 手册页。

  提示 – 使用 `-t` 选项暂时禁用服务可为服务配置提供一些保护。如果禁用服务时使用了 `-t` 选项，则服务在重新引导后将恢复原始设置。如果禁用服务时未使用 `-t`，则服务在重新引导后仍将保持禁用状态。

- NIS 故障管理资源标识符 (Fault Management Resource Identifier, FMRI) 包括：
  - 适用于 NIS 服务器的 `svc:/network/nis/server`
  - 适用于 NIS 客户机的 `svc:/network/nis/client`
  - 适用于域名的 `svc:/network/nis/domain`
- 可以使用 `svcs` 命令来查询 NIS 服务的状态。
  - 下面是 `svcs` 命令及其输出的示例：

```
$ svcs network/nis/server
STATE        STIME    FMRI
online       Jan_10   svc:/network/nis/server:default

$ svcs \*nis\*
STATE          STIME    FMRI
online         Oct_09   svc:/network/nis/domain:default
online         Oct_09   svc:/network/nis/client:default
```

- 下面是 svcs - l 命令的示例及其输出：

```
$ svcs -l /network/nis/client
fmri         svc:/network/nis/client:default
name         NIS (YP) client
enabled      true
state        online
next_state   none
state_time   Tue Aug 23 19:23:28 2011
logfile      /var/svc/log/network-nis-client:default.log
restarter    svc:/system/svc/restarter:default
contract_id  88
manifest     /lib/svc/manifest/network/nis/client.xml
manifest     /lib/svc/manifest/network/network-location.xml
manifest     /lib/svc/manifest/system/name-service/upgrade.xml
manifest     /lib/svc/manifest/milestone/config.xml
dependency   require_all/none svc:/system/filesystem/minimal (online)
dependency   require_all/restart svc:/network/rpc/bind (online)
dependency   require_all/restart svc:/network/nis/domain (online)
dependency   optional_all/none svc:/network/nis/server (absent)
dependency   optional_all/none svc:/network/location:default (online)
dependency   optional_all/none svc:/system/name-service/upgrade (online)
dependency   optional_all/none svc:/milestone/config (online)
dependency   optional_all/none svc:/system/manifest-import (online)
dependency   require_all/none svc:/milestone/unconfig (online)
```

- 可以使用 svccfg 实用程序获取有关服务的更多详细信息。请参见 svccfg(1M) 手册页。
- 可以使用 ps 命令检查守护进程是否存在。

```
$ ps -ef |grep ypbind
daemon 100813   1   0   Aug 23 ?     0:00 /usr/lib/netsvc/yp/ypbind -broadcast
```

规划 NIS 域

在将计算机配置为 NIS 服务器或客户机之前，必须规划 NIS 域。

您需要决定 NIS 域中要包括哪些计算机。NIS 域不必镜像您的 DNS 域。一个 DNS 域可以包含多个 NIS 域，并且位于 NIS 域之外的计算机可以存在于 DNS 域中。

NIS 域名的长度可为 256 个字符。比较好的做法是将域名长度限制在 32 个字符之内。NIS 域名区分大小写。为方便起见，可以选择根据 Internet 域名来命名 NIS 域名。请注意，如果 NIS 域名包括大写字母但 DNS 域名未包括，则用户可能会感到混乱。例如，如果您的 Internet 域名是 example.com，则您也可以将 NIS 域命名为 example.com。如果您希望将 example.com 拆分为两个 NIS 域，例如，一个用于销售部，另一个用于生产部，则您可以将一个域命名为 sales.example.com，将另一个域命名为 manf.example.com。

注 – 合并和管理拆分的 NIS 域可能非常难，因此请确保您有充分的理由拆分 NIS 域。

只有设置了正确的 NIS 域名和计算机名，计算机才能使用 NIS 服务。计算机的名称是通过 hostname 命令设置的。计算机的域名是通过 domainname 命令设置的。可以使用 hostname 和 domainname 命令显示计算机名称和 NIS 域名。

标识 NIS 服务器和客户机

选择一台计算机作为主服务器。决定哪些计算机将作为从属服务器。

决定哪些计算机将作为 NIS 客户机。通常情况下，NIS 域中的所有计算机都将设置为 NIS 客户机，虽然这不是必要的。

准备主服务器

以下各节介绍如何为主服务器准备源文件和 passwd 文件。

源文件目录

源文件通常位于主服务器上的 /etc 目录中。但是，将源文件存储在 /etc 中并不合适，因为这样映射中的内容将与主服务器上的本地文件中的内容相同。这是 passwd 和 shadow 文件的一个特殊问题，因为所有用户都具有对主服务器映射的访问权限，并且 root 口令将通过 passwd 映射传递到所有 NIS 客户机。有关其他信息，请参见第 74 页中的 “passwd 文件和名称空间安全性”。

但是，如果将源文件放在其他某个目录中，您必须修改 /var/yp 中的 Makefile，将 DIR=/etc 行更改为 DIR=/*your-choice*，其中，*your-choice* 是将用来存储源文件的目录的名称。这样便可将服务器上的本地文件视为客户机上的本地文件进行处理。（最好先保存原始 Makefile 的副本。）

此外，应当从某个非缺省目录创建 audit_user、auth_attr、exec_attr 和 prof_attr NIS 映射。通过将 RBACDIR =*/etc/security* 更改为 *RBACDIR=/your-choice* 来改进 /var/yp/Makefile。

passwd 文件和名称空间安全性

出于安全原因，用于生成 NIS 口令映射的文件不应包含 root 项，以防止未经授权的 root 用户访问。因此，不应使用主服务器 /etc 目录中的文件生成口令映射。对于用于生成口令映射的口令文件，应删除其中的 root 项，并将它们放置在可免遭未经授权的访问的目录中。

例如，只要主服务器口令输入文件本身不是指向其他文件的链接，并且其位置在 Makefile 中已指定，就应该将这些文件存储在诸如 /var/yp 等目录或您选择的任何目录中。将根据 Makefile 中指定的配置自动设置正确的目录选项。

注意 – 确保 PWDDIR 指定的目录中的 passwd 文件不包含 root 项。

如果您的源文件在不同于 /etc 的目录中，则您必须修改 /var/yp/Makefile 中的 PWDIR 口令宏以引用 passwd 和 shadow 文件所在的目录。您需要将 PWDIR=/etc 行更改为 PWDIR=/*your-choice*，其中 *your-choice* 是您将用来存储 passwd 映射源文件的目录的名称。

▼ 如何为转换准备源文件

此过程说明了如何为转换到 NIS 映射准备源文件。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **检查主服务器上的源文件以确保它们反映了您的系统。**

检查以下文件：

- audit_user
- auth_attr
- auto.home 或 auto_home
- auto.master 或 auto_master
- bootparams
- ethers
- exec_attr
- group
- hosts
- ipnodes
- netgroup
- netmasks
- networks
- passwd
- protocols
- rpc
- service
- shadow
- user_attr

3 **将上述所有源文件（passwd 和 shadow 除外）复制到您已选择的源目录中。**

该源目录是在 /var/yp/Makefile 中通过 DIR 宏定义的。

4 **将 passwd 和 shadow 文件复制到您已选择的口令源目录中。**

口令源目录是在 Makefile 中通过 PWDIR 宏定义的。

5 **将 audit_user、auth_attr、exec_attr 和 prof_attr 文件复制到您已选择的 RBAC 源目录中。**

RBAC 源目录是在 /var/yp/Makefile 中通过 RBACDIR 宏定义的。如果需要，将 /etc/security/auth_attr.d 目录中文件的内容合并为 auth_attr 文件的副本，然后复制该副本。同样，如果需要，通过 exec_attr 和 prof_attr 来组合 exec_attr.d 和 prof_attr.d 目录中的文件。

注意 – 因为这些文件在系统每次升级时都将需要重新合并，所以请将本地文件与 /etc/security/*.d 目录中的发行版文件相隔离。

6 **检查 /etc/mail/aliases 文件。**

与其他源文件不同，/etc/mail/aliases 文件不能移至其他目录。此文件必须位于 /etc/mail 目录中。有关更多信息，请参阅 aliases(4) 手册页。

注 – 通过将 /var/yp/Makefile 中的 ALIASES = /etc/mail/aliases 项指向其他位置，可以添加特定于 NIS 的邮件别名文件。然后当您运行 make 命令时，ALIASES 项将创建一个 mail.aliases 映射。当 /etc/nsswitch.conf 文件正确地将 files 和 nis 作为目标时，sendmail 服务除了使用 /etc/mail/aliases 文件，还使用此映射。请参阅第 96 页中的 “修改和使用 /var/yp/Makefile”。

7 **清除源文件中的所有注释以及其他多余的行和信息。**

这些操作可以通过一个 sed 或 awk 脚本或者使用文本编辑器来执行。/var/yp/Makefile 会自动为您执行某些文件清理，但最好在运行 make 命令之前手动检查并清理这些文件。

8 **确保所有源文件中的数据都具有正确的格式。**

对于该特定文件，源文件数据的格式必须是正确的。请检查各文件对应的手册页，以确保每个文件都具有正确格式。

准备 /var/yp/Makefile

检查源文件并将其复制到源文件目录之后，您现在需要将这些源文件转换为 NIS 服务使用的 ndbm 格式的映射。在主服务器上调用 ypinit 时，它会自动执行此操作，如第 78 页中的 “如何设置主服务器”中所述。

ypinit 脚本调用 make 程序，后者使用 /var/yp/Makefile。/var/yp 目录中提供了该文件的缺省副本，该文件包含将源文件转换为期望的 ndbm 格式的映射所需的命令。

您可以原样使用缺省的 Makefile，也可以修改它。如果确实要修改缺省的 Makefile，请确保先复制并存储原始的缺省 Makefile，以便将来需要时使用。您可能需要对 Makefile 进行以下一项或多项修改：

- **非缺省映射**

  如果您创建了自己的非缺省源文件并想将其转换为 NIS 映射，必须将这些源文件添加到 Makefile。

- **DIR 值**

  如果希望 Makefile 使用 /etc 目录以外的其他目录中存储的源文件（如第 74 页中的“源文件目录”中所述），必须将 Makefile 中的 DIR 的值更改为希望使用的目录。更改 Makefile 中的该值时，请勿使行缩进。

- **PWDIR 值**

  如果希望 Makefile 使用 /etc 目录以外的其他目录中存储的 passwd、shadow 和 adjunct 源文件，必须将 Makefile 中 PWDIR 的值更改为希望使用的目录。更改 Makefile 中的该值时，请勿使行缩进。

- **RBACDIR 值**

  如果您希望 Makefile 使用存储在不同于 /etc 的某个目录中的 audit_user、auth_attr、exec_attr 和 prof_attr 源文件，则必须将 Makefile 中的 RBACDIR 值更改为您要使用的目录。更改 Makefile 中的该值时，请勿使行缩进。

- **域名解析程序**

  如果希望 NIS 服务器对不在当前域中的计算机使用域名解析程序，请注释掉 Makefile 行 B=，并取消对行 B=-b 的注释（激活）。

Makefile 的功能是为列在 all 下的每个数据库创建相应的 NIS 映射。数据在通过 makedbm 传递之后，将收集在 mapname.dir 和 mapname.pag 这两个文件中。这两个文件都位于主服务器上的 /var/yp/*domainname* 目录中。

Makefile 相应地基于 /PWDIR/passwd、/PWDIR/shadow 和 /PWDIR/security/passwd.adjunct 文件生成 passwd 映射。

▼ 如何安装 NIS 主服务器软件包

通常，NIS 主服务器软件包是在适当的时候随 Oracle Solaris 发行版一起安装的。如果在安装系统时没有包括该软件包，请使用以下过程来安装该软件包。

1. **成为管理员。**

   有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2. **安装 NIS 主服务器软件包。**

```
# pkg install pkg:/service/network/nis
```

▼ 如何设置主服务器

ypinit 脚本用于设置主服务器和从属服务器以及客户机，以使用 NIS。它还会首先运行 make 命令，以在主服务器上创建映射。

要使用 ypinit 命令在主服务器上生成一组新的 NIS 映射，请完成以下过程。

1 **成为 NIS 主服务器的管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **编辑 /etc/inet/hosts 文件。**

添加每台 NIS 服务器的主机名和 IP 地址。使用以下格式：*IPaddress FQDN-hostname aliases*。

例如：

```
129.0.0.1    master.example.com master
129.0.0.2    slave1.example.com slave1
129.0.0.3    slave2.example.com slave2
```

3 **在主服务器上生成新的映射。**

```
# /usr/sbin/ypinit -m
```

4 **键入 NIS 服务器的名称。**

当 ypinit 提示输入要成为 NIS 从属服务器的其他计算机的列表时，请键入您正在使用的服务器的名称以及您在 /etc/inet/hosts file 中指定的 NIS 从属服务器的名称。

5 **确认已设置了 NIS 域名。**

```
# domainname
example.com
```

6 **如果发生了非致命错误，请键入 y 以选择停止进程。**

当 ypinit 询问是希望在出现第一个非致命错误时终止过程，还是即使出现非致命错误也仍然继续时，请键入 **y**。当您选择 **y** 时，ypinit 将在遇到第一个问题时退出。然后，您可以修复问题并重新启动 ypinit。建议在初次运行 ypinit 时这样做。如果希望继续操作，可尝试手动修复出现的所有问题，然后重新启动 ypinit。

注 – 当某些映射文件不存在时，会出现非致命错误。此错误不会影响 NIS 的功能。如果未自动创建这些映射，可能需要手动添加。有关所有缺省 NIS 映射的说明，请参阅第 64 页中的 “缺省 NIS 映射”。

---

7 **选择是否应删除源文件。**

`ypinit` 命令将询问是否可以销毁 `/var/yp/`*domain-name* 目录中现有的文件。仅当之前已安装 NIS 时才会显示此消息。通常，如果您希望清除来自以前的安装的文件，您将选择删除源文件。

8 **`ypinit` 命令构造服务器列表之后，将调用 `make` 命令。**

此程序将使用 `/var/yp` 中的 `Makefile`（缺省或修改过的文件）中包含的说明。`make` 命令将清除指定的文件中剩余的所有注释行。它还会对这些文件运行 `makedbm`，创建适当映射并为每个映射建立主服务器的名称。

如果 `Makefile` 推送的映射所对应的域不是主服务器上的 `domainname` 命令返回的域，则可以使用正确的 `DOM` 变量标识启动 `ypinit` shell 脚本中的 `make` 来确保这些映射被推送到正确的域，如下所示：

```
# make DOM=domain-name  passwd
```

此命令会将 `passwd` 映射推送到目标域，而不是主服务器所属的域。

9 **如果需要，对名称服务转换进行更改。**

请参见第 36 页中的“管理名称服务转换”。

▼ 如何在一台主服务器上支持多个 NIS 域

通常，一台 NIS 主服务器仅支持一个 NIS 域。但是，如果要使用一台主服务器来支持多个域，则在设置服务器为更多域提供服务时，必须对第 78 页中的“如何设置主服务器”中所述的步骤稍做修改。

1 **成为 NIS 主服务器的管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **更改 NIS 域名。**

```
# domainname sales.example.com
```

3 **生成 NIS 文件。**

```
# make DOM=sales.example.com
```

在 NIS 服务器上启动和停止 NIS 服务

创建主服务器映射后，可以在主服务器上启动 NIS 守护进程，并启动服务。启用 NIS 服务时，将在服务器上启动 `ypserv` 和 `ypbind` 守护进程。当客户机向服务器请求信息时，`ypserv` 守护进程将在 NIS 映射中进行查找，然后再响应来自客户机的信息请求。`ypserv` 和 `ypbind` 守护进程作为一个单元来管理。

下面是在服务器中启动或停止 NIS 服务的三种方法：

- 如果以前已启用了 NIS 服务，则 SMF 服务在引导过程中会自动启动 NIS 服务。
- 使用 `svcadm enable` *fmri* 和 `svcadm disable` *fmri* 命令是首选的手动方法。
- 虽然首选使用 `svcadm` 命令以便您可以使用 SMF 来管理 NIS 服务，但 `ypstart` 和 `ypstop` 命令提供了另一种手动方法。

自动启动 NIS 服务

如果启用了 `svc:/network/nis/server` 服务，则 `ypserv` 守护进程在引导时会自动启动。有关更多信息，请参见第 78 页中的 “如何设置主服务器”。

▼ 如何手动启动 NIS 服务器服务

在使用 `svcadm` 命令时，只有当运行了该服务的多个实例时，实例名称才是必需的。有关更多信息，请参见第 72 页中的 “NIS 和服务管理工具”或 `svcadm(1M)` 手册页。

1. **成为管理员。**

   有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2. **启动所需的 NIS 服务器服务。**

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/server
```

注 – 尽管首选使用 `svcadm` 命令，但是也可以使用 `ypstart` 命令来启用 NIS 服务。

▼ 如何禁用 NIS 服务器服务

在使用 `svcadm` 命令时，只有当运行了该服务的多个实例时，特定实例名称才是必需的。有关更多信息，请参见第 72 页中的 “NIS 和服务管理工具”或 `svcadm(1M)` 手册页。

1. **成为管理员。**

   有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2. **禁用所需的 NIS 服务器服务。**

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/server
```

注 – 还可以使用 `ypstop` 命令禁用 NIS 服务。

▼ 如何刷新 NIS 服务器服务

此过程说明了在进行配置更改后如何刷新 NIS 服务器服务。

在使用 `svcadm` 命令时，只有当运行了该服务的多个实例时，特定实例名称才是必需的。有关更多信息，请参见第 72 页中的 “NIS 和服务管理工具”或 `svcadm(1M)` 手册页。

1. **成为管理员。**

   有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2. **刷新所需的 NIS 服务器服务。**

```
# svcadm refresh network/nis/domain
# svcadm refresh network/nis/server
```

设置 NIS 从属服务器

您的网络可以有一台或多台从属服务器。使用从属服务器可在主服务器不可用时确保 NIS 服务的连续性。

准备从属服务器

在实际运行 `ypinit` 命令来创建从属服务器之前，请首先确保已配置了 `svc:/network/nis/domain` 服务。

注 – 虽然 DNS 域名不区分大小写，但 NIS 域名区分大小写。

在配置 NIS 从属服务器之前，请确保网络正在正常运行。尤其是，请确保您可以使用 `sshd` 命令将文件从主 NIS 服务器发送到 NIS 从属服务器。

▼ 如何设置从属服务器

以下过程说明了如何设置从属服务器。如果您希望将每台计算机配置为 NIS 从属服务器，请为其重复此过程。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **编辑 `/etc/inet/hosts` 文件。**

添加其他每台 NIS 服务器的名称和 IP 地址。使用以下格式：*IPaddress FQDN-hostname aliases*。

例如：

```
129.0.0.1    master.example.com master
129.0.0.2    slave1.example.com slave1
129.0.0.3    slave2.example.com slave2
```

3 **在从属服务器上，将目录转至 `/var/yp`。**

注 – 必须先将新的从属服务器配置为 NIS 客户机，它才能首次从主服务器中获取 NIS 映射。有关详细信息，请参见第 85 页中的 “管理 NIS 客户机”。

---

4 **将从属服务器初始化为 NIS 客户机。**

```
# /usr/sbin/ypinit -c
```

`ypinit` 命令会提示输入 NIS 服务器的列表。首先键入您在使用的本地从属服务器的名称，然后键入主服务器的名称，再键入您的域中其他 NIS 从属服务器的名称。对于其他从属服务器，请按照从网络角度来看从物理距离最近到最远的顺序进行键入。

5 **确定客户机服务是否正在运行，然后根据需要启动或重新启动这些服务。**

```
# svcs \*nis\*
STATE          STIME     FMRI
online         20:32:56  svc:/network/nis/domain:default
online         20:32:56  svc:/network/nis/client:default
```

如果这些服务显示了 `online` 状态，则表示 NIS 正在运行。如果该服务的状态为 `disabled`，则表明 NIS 未运行。

a. **如果客户机服务正在运行，请重新启动客户机服务。**

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
```

b. **如果客户机服务未在运行，请启动客户机服务。**

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/client
```

6 **确定 NIS 主服务器是否正在运行，然后根据需要启动或重新启动该服务。**

```
# svcs network/nis/server
STATE          STIME     FMRI
offline        20:32:56  svc:/network/nis/server:default
```

a. **如果主 NIS 服务器正在运行，请重新启动该服务。**

```
# svcadm restart network/nis/server
```

b. **如果主 NIS 服务器未在运行，请启动该服务。**

```
# svcadm enable network/nis/server
```

7 **将此计算机初始化为从属服务器。**

```
# /usr/sbin/ypinit -s master
```

其中，*master* 是现有的 NIS 主服务器的计算机名。

▼ 如何在从属服务器上启动 NIS

以下过程说明了如何在从属服务器上启动 NIS。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **重新启动客户机服务并启动所有 NIS 服务器进程。**

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
# svcadm enable network/nis/server
```

▼ 如何添加新的从属服务器

NIS 运行后，您可能需要创建一些未包含在之前提供给 `ypinit` 命令的初始列表中的 NIS 从属服务器。使用以下过程添加新的 NIS 从属服务器。

1 **成为 NIS 主服务器的管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **转至 NIS 域目录。**

```
# cd /var/yp/domainname
```

3 **反汇编 `ypservers` 文件。**

```
# makedbm -u ypservers >/tmp/temp_file
```

makedbm 命令会将 ypservers 从 ndbm 格式转换为临时 ASCII 文件 /tmp/temp_file。

4 **编辑 /tmp/temp_file 文件。**

将新的从属服务器的名称添加到服务器列表中。然后，保存并关闭该文件。

5 **运行 makedbm 命令，并以 temp_file 和 ypservers 分别作为输入文件和输出文件。**

```
# makedbm /tmp/temp_file ypservers
```

然后，makedbm 命令会将 ypservers 重新转换回 ndbm 格式。

6 **验证 ypservers 映射是否正确。**

因为 ypservers 没有 ASCII 文件，因此请在从属服务器上键入以下命令：

```
slave3# makedbm -u ypservers
```

makedbm 命令会在屏幕上显示 ypservers 中的每项。

注 – 如果某计算机名不在 ypservers 中，则该计算机不会收到映射文件的更新，原因是 yppush 需要从此映射中查询从属服务器的列表。

---

7 **成为新的 NIS 从属服务器上的管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

8 **确认已设置了 NIS 域名。**

```
# domainname
example.com
```

9 **设置新从属服务器的 NIS 域目录。**

从主服务器复制 NIS 映射集，然后启动 NIS 客户机。运行 ypinit 命令时，请遵循提示并按优先级顺序列出 NIS 服务器。

```
slave3# cd /var/yp
slave3# ypinit -c
```

10 **将此计算机初始化为从属服务器。**

```
slave3# /usr/sbin/ypinit -s ypmaster
```

其中，*ypmaster* 是现有的 NIS 主服务器的计算机名。

11 **停止作为 NIS 客户机运行的计算机。**

```
slave3# svcadm disable network/nis/client
```

12 **确定客户机服务是否正在运行，然后根据需要启动或重新启动这些服务。**

```
# svcs \*nis\*
STATE          STIME     FMRI
online         20:32:56  svc:/network/nis/domain:default
```

```
online         20:32:56  svc:/network/nis/client:default
```

如果这些服务显示了 online 状态，则表示 NIS 正在运行。如果该服务的状态为 disabled，则表明 NIS 未运行。

a. **如果客户机服务正在运行，请重新启动客户机服务。**

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
```

b. **如果客户机服务未在运行，请启动客户机服务。**

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/client
```

13 **确定 NIS 服务器是否正在运行，然后根据需要启动或重新启动该服务。**

```
# svcs network/nis/server
STATE          STIME     FMRI
offline        20:32:56  svc:/network/nis/server:default
```

a. **如果 NFS 服务器正在运行，请重新启动该服务。**

```
slave3# svcadm restart network/nis/server
```

b. **如果 NIS 服务器未在运行，请启动该服务。**

```
slave3# svcadm enable network/nis/server
```

管理 NIS 客户机

本节介绍了两种配置客户机使用 NIS 作为其命名服务的方法。

注 – Oracle Solaris 操作系统不支持 NIS 客户机与本地 LDAP 客户机共存于同一客户机中的配置。

- **广播模式**－用于将客户机配置为使用 NIS 的首选方法。有关说明，请参见第 85 页中的 “如何在广播模式下配置 NIS 客户机”。
- **服务器列表方法**－用于配置客户机的另一种方法，它使用 ypinit 命令来指定服务器。有关说明，请参见第 86 页中的 “如何将 NIS 客户机配置为使用特定的 NIS 服务器”。

▼ 如何在广播模式下配置 NIS 客户机

这是用于建立 NIS 客户机的首选方法。

当您启动 nis/client 服务时，该服务运行 ypbind 命令，该命令在本地子网中搜索 NIS 服务器。如果找到了一个子网，则 ypbind 将绑定到该子网。这种搜索被称为**广播**。如

果在客户机的本地子网中不存在 NIS 服务器，则 ypbind 将无法绑定，并且客户机无法从 NIS 服务获取名称空间数据。有关说明，请参见第 86 页中的 “如何将 NIS 客户机配置为使用特定的 NIS 服务器”。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **设置 NIS 域名。**

```
# domainname example.com
```

3 **如果需要，对名称服务转换进行更改。**

请参见第 36 页中的 “管理名称服务转换”。

4 **启动 NIS 客户机服务。**

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/client
```

▼ 如何将 NIS 客户机配置为使用特定的 NIS 服务器

开始之前 以下过程要求在步骤 3 中输入的主机名可以由 DNS 进行解析。如果您未使用 DNS 或键入了主机名而不是 IP 地址，请确保在客户机上的 /etc/hosts 文件中添加每台 NIS 服务器的相应项。有关更多信息，请参见 ypinit(1M) 手册页。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **设置 NIS 域名。**

```
# domainname example.com
# svcadm enable network/nis/domain
```

3 **运行客户机配置脚本。**

```
# ypinit -c
```

系统将提示您列举客户机要从中获取命名服务信息的 NIS 服务器。您可以根据需要列出主服务器和任意多的从属服务器。列出的服务器可以位于域中的任意位置。最好先列出离计算机最近的服务器（从网络角度来说），然后再列出网络中处于更远距离的服务器。

▼ 禁用 NIS 客户机服务

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **禁用 NIS 客户机服务。**

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/client
```

◆ ◆ ◆ 第 7 章

7 管理 NIS（任务）

本章介绍了如何管理 NIS。本章包含以下主题：

注 – NIS 服务由服务管理工具管理。使用 `svcadm` 命令可以对此服务执行启用、禁用或重新启动等管理操作。有关将 SMF 与 NIS 结合使用的更多信息，请参见第 72 页中的 “NIS 和服务管理工具”。有关 SMF 的概述，请参见《在 Oracle Solaris 11.1 中管理服务和故障》中的第 1 章 “管理服务（概述）”。有关更多详细信息，另请参阅 `svcadm(1M)` 和 `svcs(1)` 手册页。

还可以使用 `ypstart` 和 `ypstop` 命令来启动和停止 NIS 服务。有关更多信息，请参见 `ypstart(1M)` 和 `ypstop(1M)` 手册页。

口令文件和名称空间安全

出于安全原因，请遵循以下原则。

- 最好限制对主服务器上的 NIS 映射的访问。
- 用于生成 NIS 口令映射的文件不应包含 `root` 项，以防止未经授权的访问。为此，应删除用于生成口令映射的口令文件中的 `root` 项，并将该文件移至不同于主服务器 `/etc` 目录的其他目录中。应确保此目录不会受到未经授权的访问。

例如，只要主服务器口令输入文件本身不是指向其他文件的链接并且在 Makefile 中已指定，就可将这些文件存储在诸如 `/var/yp` 之类的目录或您选择的任何目录中。使用服务管理工具或 `ypstart` 脚本启动 NIS 服务时，将根据 `Makefile` 中指定的配置设置正确的目录选项。

注 – 除了早期的 Solaris 1 版本的 passwd 文件格式外，此 NIS 实现还接受 Solaris 2 的 passwd 和 shadow 文件格式作为用于生成 NIS 口令映射的输入。

管理 NIS 用户

本节包括有关设置用户口令、向 NIS 域添加新用户以及将用户指定给 netgroups 的信息。

▼ 如何向 NIS 域添加新 NIS 用户

1 **成为 NIS 主服务器的管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **使用 useradd 命令创建新用户的登录 ID。**

```
# useradd userID
```

其中，*userID* 是新用户的登录 ID。此命令将在主 NIS 服务器上的 /etc/passwd 和 /etc/shadow 文件中创建项。

3 **创建新用户的初始口令。**

要创建新用户可用来登录的初始口令，请运行 passwd 命令。

```
# passwd userID
```

其中，*userID* 是新用户的登录 ID。系统将提示您输入要指定给此用户的口令。

由于 useradd 命令创建的口令项被锁定（这意味着新用户无法登录），因此必须执行此步骤。通过指定初始口令，可以解除对该项的锁定。

4 **将新项复制到主服务器的 passwd 映射输入文件中。**

主服务器上的映射源文件应位于 /etc 之外的某个目录中。将新行从 /etc/passwd 和 /etc/shadow 文件复制并粘贴到服务器上的 passwd 映射输入文件中。有关其他信息，请参见第 89 页中的 “口令文件和名称空间安全”。

例如，如果您添加了新用户 brown，则要从 /etc/passwd 复制到 passwd 输入文件中的行将如下所示：

```
brown:x:123:10:User brown:/home/brown:/bin/csh:
```

要从 /etc/shadow 中复制的有关 brown 的行将如下所示：

```
brown:$5$YiFpYWXb$6jJkG/gKdfkKtlTbemORnbeH.qsvO9MwBD3ulTihq9B:6445::::::
```

5 **确保 Makefile 正确指定了口令输入文件所在的目录。**

6 **从 /etc/passwd 和 /etc/shadow 输入文件中删除新用户的项。**

出于安全原因，请不要在 NIS 主服务器的 /etc/passwd 和 /etc/shadow 文件中保留用户项。在将新用户的项复制到其他某个目录中存储的 NIS 映射源文件后，请在主服务器上使用 userdel 命令删除新用户。

例如，要从主服务器的 /etc 文件中删除新用户 brown，可以输入以下命令。

```
# userdel brown
```

有关 userdel 的更多信息，请参见 userdel(1M) 手册页。

7 **更新 NIS passwd 映射。**

在更新主服务器上的 passwd 输入文件后，请在包含源文件的目录中运行 make，以更新 passwd 映射。

```
# userdel brown
# cd /var/yp
# make passwd
```

8 **通知新用户已为其登录 ID 指定的初始口令。**

登录后，新用户随时可以通过运行 passwd 设置不同口令。

设置用户口令

用户可以运行 passwd 来更改自己的口令。

% **passwd** *username*

您必须先在主服务器上启动 rpc.yppasswdd 守护进程来更新口令文件，然后用户才能更改其口令。

rpc.yppasswdd 守护进程会在主服务器上自动启动。请注意，如果为 rpc.yppasswdd 指定了 -m 选项，则在 /var/yp 中修改文件后将立即运行 make 命令。如果要避免在每次更改 passwd 文件后都运行此 make 命令，请在 ypstart 脚本的 rpc.yppasswd 命令中删除 -m 选项，并通过 crontab 文件控制 passwd 映射的推送。

NIS 网络组

NIS 网络组是您为实现管理目的而定义的用户或计算机组（集合）。例如，您可以创建网络组来执行以下任务。

- 定义一组可以访问特定计算机的用户
- 定义一组要被授予特定文件系统访问权限的 NFS 客户机
- 定义一组要对特定 NIS 域中的所有计算机具有管理员权限的用户

每个网络组都有一个网络组名。网络组不直接设置权限或访问权限。而是由其他 NIS 映射在通常使用用户名或计算机名的地方使用网络组名。例如，假设您创建了一个由网络管理员组成的网络组，名为 netadmins。要向 netadmins 网络组的所有成员授予对

给定计算机的访问权限，只需向该计算机的 /etc/passwd 文件中添加一个 netadmin 项即可。网络组名也可以添加到 /etc/netgroup 文件中并传播到 NIS netgroup 映射。有关使用网络组的更多详细信息，请参见 netgroup(4) 手册页。

在使用 NIS 的网络中，主 NIS 服务器上的 netgroup 输入文件用于生成三种映射：netgroup、netgroup.byuser 和 netgroup.byhost。netgroup 映射包含 netgroup 输入文件中的基本信息。另外两种 NIS 映射中包含的信息的格式可在给定计算机或用户名的情况下加速网络组信息的查找。

netgroup 输入文件中的项格式如下：*name ID*，其中 *name* 是您指定给网络组的名称，而 *ID* 用于标识属于该网络组的一个计算机或用户。您可以根据需要为网络组指定任意多的 ID（成员），ID 之间以逗号分隔。例如，要创建一个具有三个成员的网络组，netgroup 输入文件项将采取以下格式：*name ID*, *ID*, *ID*。netgroup 输入文件项中的成员 ID 采取以下格式。

```
([-|machine], [-|user], [domain])
```

其中，*machine* 是计算机名，*user* 是用户 ID，*domain* 是计算机或用户的 NIS 域。*domain* 元素是可选的，并且仅应用于标识其他某个 NIS 域中的计算机或用户。每个成员项的 *machine* 和 *user* 元素是必需的，但短划线 (-) 用来表示内容为空。项中的计算机和用户元素之间不存在必然联系。

下面是两个 netgroup 输入文件项样例，每个样例都创建了一个名为 admins 的网络组，网络组由远程域 sales 中的用户 hauri 和 juanita 以及计算机 altair 和 sirius 组成。

```
admins (altair, hauri), (sirius,juanita,sales)
admins (altair,-), (sirius,-), (-,hauri), (-,juanita,sales)
```

各种程序在登录、远程挂载、远程登录以及远程创建 shell 期间会使用 NIS 映射进行权限检查。这些程序包括 mountd 和 login。login 命令在 passwd 数据库中遇到网络组名时，会在网络组映射中查询用户分类。mountd 守护进程在 /etc/dfs/dfstab 文件中遇到网络组名时，会在网络组映射中查询用户分类。实际上，如果使用 ruserok 接口的任何程序遇到了 /etc/hosts.equiv 或 .rhosts 文件中的网络组名称，它们都将在网络组映射中检查计算机和用户分类。

如果您向网络中添加新 NIS 用户或计算机，请确保在 netgroup 输入文件中将其添加到适当的网络组中。然后使用 make 和 yppush 命令创建网络组映射，再将其推送到所有 NIS 服务器。有关使用网络组和网络组输入文件语法的详细信息，请参见 netgroup(4)。

使用 NIS 映射

本节包含以下信息：

获取映射信息

用户可以使用 ypcat、ypwhich 和 ypmatch 命令随时从映射中获取有关映射的信息。在下面的示例中，*mapname* 同时指映射的正式名称和昵称（如果有）。

要列出映射中的所有值，请键入以下命令：

```
% ypcat mapname
```

要同时列出映射中的关键字和值（如果有），请键入以下命令：

```
% ypcat -k mapname
```

要列出所有映射昵称，请键入以下任何命令：

```
% ypcat -x
% ypmatch -x
% ypwhich -x
```

要列出所有可用映射及其主服务器，请键入以下命令：

```
% ypwhich -m
```

要列出特定映射的主服务器，请键入以下命令：

```
% ypwhich -m mapname
```

要使映射中的项与关键字匹配，请键入以下命令：

```
% ypmatch key mapname
```

如果要查找的项不是映射中的关键字，请键入以下命令：

```
% ypcat mapname | grep item
```

其中，*item* 是要搜索的信息。要获取有关其他域的信息，请使用这些命令的 -d domainname 选项。

如果请求非缺省域的信息的计算机没有针对所请求的域的绑定，ypbind 将在 /var/yp/binding/*domainname*/ypservers 文件中查询该域的服务器列表。如果此文件不存在，该命令将发出服务器的 RPC 广播。在这种情况下，被请求域必须有一台服务器与请求计算机位于同一子网。

更改映射的主服务器

要更改选定映射的主服务器，必须先在新 NIS 主服务器上生成该映射。由于旧的主服务器名称以关键字-值对的形式出现在现有映射中（此对由 makedbm 自动插入），因此将该映射复制到新的主服务器或使用 ypxfr 将副本传送到新的主服务器是不够的。您必须将该关键字与新主服务器名重新关联。如果映射具有 ASCII 源文件，应将此文件复制到新的主服务器。

▼ 如何更改映射的主服务器

1. **成为 NIS 主服务器的管理员。**

   有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2. **更改目录。**

   ```
   newmaster# cd /var/yp
   ```

3. **/var/yp/Makefile 必须具有新映射的项，才能指定要进行的映射。**

   如果目前没有，现在请编辑 Makefile。对于此示例，请为名为 sites.byname 的映射添加一个项。

4. **要更新映射或重新进行映射，请键入以下命令：**

   ```
   newmaster# make sites.byname
   ```

5. **如果旧的主服务器仍为 NIS 服务器，请远程登录 (ssh) 到该旧的主服务器并编辑 /var/yp/Makefile。**

   确保注释掉 Makefile 中创建 sites.byname 映射的部分，使其不再被创建。

6. **如果 sites.byname 仅作为一个 ndbm 文件存在，请在新的主服务器上重新创建它。**

   首先，通过使用 ypcat 命令反汇编 sites.byname 文件的副本。然后，通过 makedbm 运行反汇编的版本。

   ```
   newmaster# cd /var/yp
   newmaster# ypcat sites.byname | makedbm domain/sites.byname
   ```

   在新的主服务器上创建映射后，必须向其他从属服务器发送新映射的副本。不要使用 yppush，因为其他从属服务器会试图从旧的主服务器（而不是新的主服务器）中获取

新副本。解决此问题的一个典型方法是从新的主服务器向旧的主服务器传送一份映射的副本。为此，请在旧的主服务器上成为超级用户或承担等效角色，并键入以下命令。

```
oldmaster# /usr/lib/netsvc/yp/ypxfr -h newmaster sites.byname
```

现在，即可安全运行 yppush。其余所有的从属服务器仍会认为旧的主服务器是当前的主服务器，并尝试从旧的主服务器中获取最新版本的映射。当客户机这样做时，它们将获得新得映射，该映射会将新的主服务器指定为当前主服务器。

如果此方法失败，可以使用 root 用户身份登录每台 NIS 服务器并执行上面所示的 ypxfr 命令。

修改配置文件

NIS 可以智能解析设置文件。尽管这样可以简化 NIS 管理，但它使 NIS 的行为对设置和配置文件中的更改更敏感。

进行以下任何一项操作时，请使用本节中的过程：

- 修改 /var/yp/Makefile 以添加或删除受支持的映射
- 添加或删除 $PWDIR/security/passwd.adjunct，以允许或拒绝 C2 安全性（$PWDIR 是在 /var/yp/Makefile 中定义的）

▼ 如何修改配置文件

请牢记以下几点。

- 在 NIS 主服务器中删除映射或源文件不会自动在从属服务器中执行同样的删除操作。您必须手动删除从属服务器中的映射和源文件。
- 新映射不会自动推送到现有的从属服务器。你必须在从属服务器中运行 ypxfr。

1. **成为管理员。**

   有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2. **停止 NIS 服务器。**

   ```
   # svcadm disable network/nis/server
   ```

3. **对文件进行必要的更改。**

4. **启动 NIS 服务器。**

   ```
   # svcadm enable network/nis/server
   ```

修改和使用 /var/yp/Makefile

您可以修改 /var/yp 中缺省提供的 Makefile 来满足自己的需要。您可以添加或删除映射，也可以更改某些目录的名称。

提示 – 请保留原始的 Makefile 的未修改副本，以供将来参考。

使用 Makefile

要添加新的 NIS 映射，必须将该映射的 ndbm 文件的副本放入域中每台 NIS 服务器上的 /var/yp/*domainname* 目录中。此操作通常由 Makefile 执行。在决定好将哪台 NIS 服务器用作映射的主服务器之后，请修改主服务器上的 Makefile，以便可以方便地重新生成映射。不同的服务器可以作为不同映射的主服务器，但在大多数情况下，这会导致管理上的混乱。请尽量只将一台服务器设置为所有映射的主服务器。

通常，会使用 awk、sed 或 grep 对适合人阅读的文本文件进行过滤，以使其适合输入到 makedbm。有关示例，请参阅缺省的 Makefile。有关 make 命令的一般信息，请参见 make(1S)。

在决定如何创建 make 可识别的相关性时，请使用 Makefile 中已经存在的机制。请注意，make 对于相关性规则中的行首是否存在制表符非常敏感。缺少制表符会使本来格式正确的项无效。

向 Makefile 中添加项涉及以下步骤。

- 向 all 规则中添加数据库名称
- 编写 time 规则
- 为数据库添加规则

例如，为使 Makefile 可以处理自动挂载程序输入文件，必须将 auto_direct.time 和 auto_home.time 映射添加到 NIS 数据库。

要将这些映射添加到 NIS 数据库，需要修改 Makefile。

更改 Makefile 宏/变量

通过更改等号 (=) 右侧的值，可以更改在 Makefile 顶部定义的变量的设置。例如，如果不想使用 /etc 中的文件作为映射的输入，而想使用另一个目录（如/var/etc/domainname）中的文件，应将 DIR 由 DIR=/etc 更改为 DIR=/var/etc/*domainname*。另外，还应将 PWDIR 由 PWDIR=/etc 更改为 PWDIR=/var/etc/*domainname*。

这些变量如下所示：

- *DIR*= 包含除 passwd 和 shadow 之外的所有 NIS 输入文件的目录。缺省值为 /etc。由于使用主服务器上 /etc 目录中的文件作为 NIS 输入文件并不是一种很好的做法，因此应更改此值。

- *PWDIR*= 包含 passwd 和 shadow NIS 输入文件的目录。由于使用主服务器上 /etc 目录中的文件作为 NIS 输入文件并不是一种很好的做法，因此应更改此值。
- *DOM*= NIS 域名。可以使用 domainname 命令设置 DOM 的缺省值。

修改 Makefile 项

以下过程介绍如何在 Makefile 中添加和删除数据库。

▼ 如何修改 /var/yp/Makefile 以使用特定数据库

此过程要求您已配置了一台 NIS 主服务器。

1. **成为管理员。**

   有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2. **通过添加要添加的数据库的名称来修改以单词 all 开头的行：**

```
all: passwd group hosts ethers networks rpc services protocols \
    netgroup bootparams aliases netid netmasks \
    audit_user auth_attr exec_attr prof_attr \
  auto_direct auto_home auto_direct.time auto_home.time
```

   各项的顺序不相关，但连续行开头的空白处必须为制表符，而不是空格。

3. **在 Makefile 的末尾添加以下行：**

```
auto_direct: auto_direct.time
auto_home: auto_home.time
```

4. **在该文件中间添加 auto_direct.time 的项。**

```
auto_direct.time: $(DIR)/auto_direct
 @(while read L; do echo $$L; done < $(DIR)/auto_direct
 $(CHKPIPE)) | \ (sed -e "/^#/d" -e "s/#.*$$//" -e "/^ *$$/d"
 $(CHKPIPE)) | \ $(MAKEDBM) - $(YPDBDIR)/$(DOM)/auto_direct;
 @touch auto_direct.time;
 @echo "updated auto_direct";
 @if [ ! $(NOPUSH) ]; then $(YPPUSH) auto_direct; fi
 @if [ ! $(NOPUSH) ]; then echo "pushed auto_direct"; fi
```

   其中

   - CHKPIPE 确保在将结果传输给后面的命令之前管道符号 (|) 左侧的运算已成功完成。如果管道符号左侧的运算未成功完成，该进程将中止，并显示 "NIS make terminated"（NIS make 中止）消息。
   - NOPUSH 阻止 makefile 调用 yppush 将新映射传送到从属服务器。如果不设置 NOPUSH，将自动完成推送。

   开头的 while 循环用于消除输入文件中的所有反斜杠扩展行。sed 脚本用于消除注释和空行。

对所有其他自动挂载程序映射（例如 auto_home 或任何其他非缺省映射）使用相同的过程。

5 **运行 make 命令。**

```
# make mapname
```

其中，*mapname* 是要创建的映射的名称。

▼ 如何修改 Makefile 以删除数据库

如果不希望 Makefile 为特定数据库生成映射，请按如下步骤编辑 Makefile。

1 **从 all 规则中删除数据库的名称。**

2 **为要删除的数据库删除或注释掉数据库规则。**

例如，要删除 hosts 数据库，应删除 hosts.time 项。

3 **删除 time 规则。**

例如，要删除 hosts 数据库，应删除 hosts: hosts.time 项。

4 **从主服务器和从属服务器中删除映射。**

更新和修改现有映射

安装 NIS 之后，您可能会发现，有些映射需要频繁更新，而其他映射则从来不需要更改。例如，在大公司的网络中，passwd.byname 映射可能会频繁更改，而 auto_master 映射则只需少量更改，甚至不进行任何更改。

如第 64 页中的 “缺省 NIS 映射”中所述，缺省 NIS 映射的缺省位置是主服务器上的 /var/yp/*domainname*，其中 *domainname* 是 NIS 域的名称。当您需要更新某个映射时，可以根据该映射是否为缺省映射来使用两个更新过程之一。

- 缺省映射是 ypinit 命令从网络数据库中创建的缺省集合中的映射。
- 非缺省映射可以是以下三种类型之一：
  - 从供应商处购买的应用程序中随附的映射
  - 专门为您的站点创建的映射
  - 在非文本文件中创建的映射

以下各部分介绍如何使用各种更新工具。在实践中，您可能会决定只在系统已启动并运行后添加非缺省映射或更改 NIS 服务器集合时才使用这些工具。

▼ 如何更新随缺省集合提供的映射

使用以下过程可以更新随缺省集合提供的映射。

1 **成为 NIS 主服务器的管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **编辑您要更改的映射的源文件。**

该文件可能位于 `/etc` 或您选择的某个其他目录中。

3 **运行 `make` 命令。**

```
# cd /var/yp
# make mapname
```

然后，`make` 命令将根据您在映射对应的文件中所做的更改来更新映射。此命令还会在其他服务器中传播这些更改。

维护更新后的映射

以下各节介绍完成更新随缺省集合提供的映射之后进行的其他过程。

传播 NIS 映射

更改映射后，`Makefile` 将使用 `yppush` 将新映射传播到从属服务器（除非在 `Makefile` 中设置了 `NOPUSH`）。它会通知 `ypserv` 守护进程并发送映射传送请求以完成此操作。然后，从属服务器上的 `ypserv` 守护进程会启动 `ypxfr` 进程，然后该进程将与主服务器上的 `ypxfrd` 守护进程联系。将执行某些基本检查（例如映射是否已真正更改？），然后传送映射。从属服务器上的 `ypxfr` 然后将向 `yppush` 进程发送一个响应来指示传输是否成功。

注 – 对于尚未存在于从属服务器上的新创建的映射，以上过程将**不**可行。必须通过在从属服务器上运行 `ypxfr` 将新映射发送到从属服务器。

有时候，映射无法传播，您必须使用 `ypxfr` 手动发送新的映射信息。您可以选择以两种不同方式使用 `ypxfr`：通过 `root crontab` 文件定期使用，或在命令行中交互使用。这些方法将在以下各节中进行讨论。

使用 `cron` 命令进行映射传送

不同映射的更改速度有所不同。例如，某些映射可能数月不更改一次，如缺省映射中的 `protocols.byname` 和非缺省映射中的 `auto_master`。不过，`passwd.byname` 可能一天更改数次。使用 `crontab` 命令调度映射传送，可以为各个映射设置特定的传播时间。

要以适合于映射的频率定期运行 ypxfr，每台从属服务器中的根 crontab 文件应包含适当的 ypxfr 项。ypxfr 与主服务器联系，并仅在主服务器中的副本比本地副本更新时才传送映射。

注 – 如果主服务器运行带有缺省 -m 选项的 rpc.yppasswdd，则每次 yp 口令发生更改时，passwd 守护进程都会运行 make，重新生成 passwd 映射。

将 Shell 脚本用于 cron 和 ypxfr

作为为每个映射创建单独的 crontab 项的备选方法，您可能更喜欢让根 crontab 命令运行 shell 脚本来定期更新所有映射。用于更新映射的 shell 脚本样例位于 /usr/lib/netsvc/yp 目录中。这些脚本名为 ypxfr_1perday、ypxfr_1perhour 和 ypxfr_2perday。您可以修改或替换这些 shell 脚本来满足站点需要。以下示例显示的是缺省 ypxfr_1perday shell 脚本。

示例 7–1 ypxfr_1perday Shell 脚本

```
#! /bin/sh
#
# ypxfr_1perday.sh - Do daily yp map check/updates
PATH=/bin:/usr/bin:/usr/lib/netsvc/yp:$PATH
export PATH
# set -xv
ypxfr group.byname
ypxfr group.bygid
ypxfr protocols.byname
ypxfr protocols.bynumber
ypxfr networks.byname
ypxfr networks.byaddr
ypxfr services.byname
ypxfr ypservers
```

如果根 crontab 每天执行一次，此 shell 脚本会每天更新一次映射。您还可以具有其他脚本，用以每周更新一次映射、每月更新一次映射、每小时更新一次映射，等等。不过请注意，频繁传播映射会引起性能降低。有关更多信息，请参见 crontab(1) 手册页。

在为 NIS 域配置的每台从属服务器上，以 root 用户的身份运行相同的 shell 脚本。逐个更改每台服务器上确切的执行时间，以避免使主服务器陷入停顿状态。

如果要从特定的从属服务器中传送映射，请在 shell 脚本中使用 ypxfr 的 -h *machine* 选项。放入脚本中的命令的语法如下所示。

```
# /usr/lib/netsvc/yp/ypxfr -h machine [ -c ] mapname
```

其中，*machine* 是要传送的映射所在服务器的名称，*mapname* 是所请求的映射的名称。如果使用了 -h 选项但未指定计算机，ypxfr 将尝试从主服务器中获取映射。如果执行 ypxfr 时 ypserv 未在本地运行，则必须使用 -c 标志，以使 ypxfr 不向本地 ypserver 发送清除当前映射的请求。

您可以使用 -s *domain* 选项从其他域向本地域传送映射。这些映射在各个域中必须相同。例如，两个域可能会共享相同的 services.byname 和 services.byaddr 映射。另外，为实现更多的控制，可以使用 rcp 或 rsync 来跨域传送文件。

直接调用 ypxfr 命令

调用 ypxfr 命令的另一种方法是将其作为命令来运行。通常，只在异常情况下才使用此方法－例如，在设置临时 NIS 服务器来创建测试环境时或在尝试使断开服务的 NIS 服务器快速与其他服务器保持一致时。

记录 ypxfr 活动

ypxfr 的传送尝试和结果可以捕获并存储在日志文件中。如果存在名为 /var/yp/ypxfr.log 的文件，则会向该文件中附加结果。对于该日志文件的大小没有任何限制。为防止日志文件无限制地增大，请键入以下命令定期清空该文件。

```
# cd /var/yp
# cp ypxfr.log ypxfr.log.old
# cat /dev/null > /var/yp/ypxfr.log
```

可让 crontab 一周执行一次上述命令。要禁用日志记录，请删除日志文件。

修改非缺省映射

要更新非缺省映射，必须执行下列操作：

1. 创建或编辑对应的文本文件。
2. 生成（或重新生成）新映射或更新的映射。生成映射的方法有两种。
   - 使用 Makefile。使用 Makefile 是生成非缺省映射的首选方法。如果映射在 Makefile 中具有一个项，请运行 make *name*，其中 *name* 是要生成的映射的名称。如果映射中没有 Makefile 项，请尝试按照第 96 页中的 “修改和使用 /var/yp/Makefile”中的说明创建一个项。
   - 使用 /usr/sbin/makedbm 程序。makedbm(1M) 手册页全面介绍了此命令。

使用 makedbm 命令修改非缺省映射

如果您没有输入文件，可通过两种不同的方法使用 makedbm 来修改映射：

- 将 makedbm -u 输出重定向到一个临时文件中，修改该文件，然后使用修改过的文件作为 makedbm 的输入。
- 让 makedbm -u 的输出在向 makedbm 进行输入的管道内运行。如果您可以使用附加的 awk、sed 或 cat 更新反汇编的映射，则这种方法是适合的。

从文本文件创建新映射

假设使用编辑器或 shell 脚本在主服务器上创建了一个文本文件 /var/yp/mymap.asc。您希望基于此文件创建一个 NIS 映射并将其置于 *home-domain* 子目录中。为此，请在主服务器上键入以下命令。

```
# cd /var/yp
# makedbm mymap.asc home-domain/mymap
```

mymap 映射现在存在于主服务器上的 *home-domain* 目录中。要将该新映射分发到从属服务器，请运行 ypxfr。

向基于文件的映射中添加项

向 mymap 中添加项非常简单。首先，必须修改文本文件 /var/yp/*mymap*.asc。如果修改实际的dbm文件而不修改对应的文本文件，所做的修改会丢失。然后，按上面所示运行 makedbm。

通过标准输入创建映射

当不存在原始文本文件时，请向 makedbm 键入输入，从键盘创建 NIS 映射，如下所示（以 Ctrl-D 组合键结束）。

```
ypmaster# cd /var/yp
ypmaster# makedbm home-domain/mymap key1 value1  key2 value2  key3 value3
```

修改通过标准输入创建的映射

如果以后需要修改映射，可以使用 makedbm 反汇编映射，并创建一个临时的中间文本文件。要反汇编映射并创建一个临时文件，请键入以下命令：

```
% cd /var/yp
% makedbm -u homedomain/mymap > mymap.temp
```

在生成的临时文件 *mymap*.temp 中，每行包含一项。您可以根据需要，使用任何文本编辑器编辑此文件。

要更新映射，请键入以下命令将修改过的临时文件的名称提供给 makedbm：

```
% makedbm mymap.temp homedomain/mymap
% rm mymap.temp
```

然后，成为 root 用户并键入下列命令，将映射传播到从属服务器。

```
# yppush mymap
```

前面的段落解释了如何使用 makedbm 创建映射。不过，您实际上必须做的几乎所有事情都可以通过使用 ypinit 命令和 /var/yp/Makefile 来完成，除非您在系统已启动并运行后向数据库添加非缺省映射或更改 NIS 服务器集。

无论您在 /var/yp 中使用 Makefile 还是某个其他过程，目标都是相同的。主服务器上的映射目录中最终必须有格式正确的新 dbm 文件对。

使用 NIS 服务器

以下过程显示了用来修改 NIS 配置的方法，具体修改包括：绑定到特定的 NIS 服务器、设置 NIS 域名、将主机查找转发到 DNS，以及关闭 NIS 服务。

绑定到特定 NIS 服务器

使用下列步骤可以绑定到您指定的 NIS 服务器。有关更多信息，请参见 ypinit(1M)、ypstart(1M) 和 svcadm(1M) 手册页。

1. 将 NIS 服务器的主机名及其 IP 地址添加到 /etc/hosts 文件。
2. 确认已设置了 NIS 域名。

```
# domainname
example.com
```

3. 提示输入 NIS 服务器主机名。

```
# /usr/sbin/ypinit -c
Server name:      Type the NIS server host name
```

4. 执行以下步骤以重新启动 NIS 服务：
   - 对于在系统重新引导后持续有效的服务，请运行 svcadm 命令。

     ```
     # svcadm enable svc:/network/nis/client
     ```
   - 对于仅在重新引导之前持续有效的服务，请运行 ypstop 和 ypstart 命令。

     ```
     # /usr/lib/netsvc/yp/ypstop
     # /usr/lib/netsvc/yp/ypstart
     ```

▼ 如何设置计算机的 NIS 域名

要更改计算机的 NIS 域名，请执行以下过程。

1 成为管理员。

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **定义 NIS 域名。**

```
# domainname research.example.com
```

3 **更新并运行域名服务。**

```
# svccfg -s nis/domain:default refresh
# svcadm enable nis/domain
```

4 **将计算机设置为 NIS 客户机、从属服务器或主服务器。**

有关详细信息，请参见第 6 章，设置和配置 NIS（任务）。

▼ 如何配置通过 NIS 和 DNS 执行计算机主机名和地址查找

通常，NIS 客户机配置有 `nsswitch.conf` 文件，以便只使用 NIS 查找计算机名和地址。如果此类查找失败，NIS 服务器可将这些查找转发给 DNS。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **添加 `YP_INTERDOMAIN` 关键字。**

两个映射文件（`hosts.byname` 和 `hosts.byaddr`）中必须包括 `YP_INTERDOMAIN` 关键字。要测试此关键字，请编辑 `/var/yp/Makefile` 并修改以下各行。

```
#B=-b
B=
```

更改为：

```
B=-b
#B=
```

现在，`makedbm` 在创建映射时将以 `-b` 标志启动，并会在 `ndbm` 文件中插入 `YP_INTERDOMAIN` 关键字。

3 **运行 `make` 命令，以重新生成映射。**

```
# make hosts
```

4 **检查是否正确设置了 DNS 名称服务器。**

以下命令列出了 DNS 名称服务器的所有 IP 地址：

```
# svcprop -p config/nameserver network/dns/client
```

5 **要启用 DNS 转发，请重新启动每台服务器。**

```
# svcadm restart network/nis/server:instance
```

在此 NIS 实现中，ypserv 守护进程将自动以 -d 选项启动，将请求转发给 DNS。

禁用 NIS 服务

如果禁用了 NIS 主服务器上的 ypserv 守护进程，您将无法再更新任何 NIS 映射。

- 要禁用客户机上的 NIS，请键入以下命令：

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/client
```

- 要禁用特定从属服务器或主服务器上的 NIS，请在服务器上键入以下命令：

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/server
```

◆ ◆ ◆ 第 8 章

NIS 故障排除

本章介绍如何解决在运行 NIS 的网络中遇到的问题，其中涵盖在 NIS 客户机上和 NIS 服务器上遇到的问题。

在尝试调试 NIS 服务器或客户机之前，请先阅读第 5 章，网络信息服务（概述），其中对 NIS 环境进行了介绍。然后，在本节中查找最能恰当描述您所遇到的问题的副标题。

注 – NIS 服务由服务管理工具管理。使用 `svcadm` 命令可以对此服务执行启用、禁用或重新启动等管理操作。有关将 SMF 与 NIS 结合使用的更多信息，请参见第 72 页中的 “NIS 和服务管理工具”。有关 SMF 的概述，请参见《在 Oracle Solaris 11.1 中管理服务和故障》中的第 1 章 “管理服务（概述）”。有关更多详细信息，另请参阅 `svcadm(1M)` 和 `svcs(1)` 手册页。

还可以使用 `ypstart` 和 `ypstop` 命令来启动和停止 NIS 服务。有关更多信息，请参见 `ypstart(1M)` 和 `ypstop(1M)` 手册页。

NIS 绑定问题

NIS 绑定问题的症状

NIS 绑定问题具有以下常见症状。

- 有消息提示 `ypbind` 找不到服务器或无法与服务器通信
- 有消息提示服务器不响应
- 有消息提示 NIS 不可用
- 客户机上的命令在后台模式下缓慢运行，或运行速度远低于正常情况
- 客户机上的命令挂起。有时候，即使整个系统看似正常并且可以运行新命令，命令可能也已挂起

- 客户机上的命令崩溃，同时显示不明消息或根本不显示消息

影响一台客户机的 NIS 问题

如果只有一两台客户机出现了表明 NIS 绑定问题的症状，则可能是这些客户机存在问题。如果许多 NIS 客户机都无法正确绑定，则可能是一台或多台 NIS 服务器存在问题。请参见第 111 页中的 “影响多台客户机的 NIS 问题”。

ypbind 未在客户机上运行

一台客户机中存在问题，但同一子网上的其他客户机运行正常。在存在问题的客户机上，对满足以下条件的目录运行 `ls -l`：目录中的文件由许多用户拥有，并且其中一些用户不在该客户机的 `/etc/passwd` 文件中。例如，`/usr` 目录。如果显示结果将不在本地 `/etc/passwd` 中的文件所有者以数字形式（而非名称）列出，表明 NIS 服务未在该客户机上运行。

这些症状通常表示客户机的 `ypbind` 进程未运行。请验证 NIS 客户机服务是否正在运行。

```
client# svcs \*nis\*
STATE          STIME    FMRI
disabled       Sep_01   svc:/network/nis/domain:default
disabled       Sep_01   svc:/network/nis/client:default
```

如果服务处于 `disabled` 状态，请以 `root` 身份登录或承担等效的角色，然后启动 NIS 客户机服务。

```
client# svcadm enable network/nis/domain
client# svcadm enable network/nis/client
```

缺少域名或域名不正确

一台客户机中存在问题，其他客户机运行正常，但 `ypbind` 正在出问题的客户机上运行。该客户机的域可能设置不正确。

在该客户机上，运行 `domainname` 命令，查看它设置了哪个域名。

```
client7# domainname
example.com
```

将输出与 NIS 主服务器上 `/var/yp` 中的实际域名进行比较。实际的 NIS 域显示为 `/var/yp` 目录中的子目录。

```
client7# ls -l /var/yp
-rwxr-xr-x 1 root Makefile
drwxr-xr-x 2 root binding
drwx------ 2 root example.com
```

如果在计算机上运行 domainname 所返回的域名与 /var/yp 中作为目录列出的服务器域名不同，则计算机的 /etc/defaultdomain 文件中指定的域名不正确。请按第 103 页中的 “如何设置计算机的 NIS 域名”中所示重新设置 NIS 域名。

注 – NIS 域名区分大小写。

客户机未绑定到服务器

如果域名设置正确，并且 ypbind 正在运行，但命令仍然挂起，请运行 ypwhich 命令来确保客户机已绑定到服务器。如果您刚刚启动了 ypbind，可多运行几次 ypwhich（通常，第一次运行时会报告域未绑定，第二次便会成功）。

没有可用的服务器

如果域名设置正确，并且 ypbind 正在运行，但有消息提示客户机无法与服务器通信，则表示问题可能有多种：

- 客户机是否具有 /var/yp/binding/*domainname*/ypservers 文件（该文件中包含要绑定到的服务器的列表）？如果没有该文件，请运行 ypinit -c 并按优先级顺序指定客户机应绑定到的服务器。
- 如果客户机有 /var/yp/binding/*domainname*/ypservers 文件，该文件中列出的服务器数量是否足以应对一台或两台服务器不可用时的情况？如果没有足够多的服务器，请运行 ypinit -c 向列表中添加更多服务器。
- 选定的 NIS 服务器在 /etc/inet/hosts 文件中是否有相应的条目？要查看选定的 NIS 服务器，请使用 svcprop -p config/ypservers nis/domain 命令。如果这些主机不在本地 /etc/inet/hosts 文件中，请将服务器添加到 hosts NIS 映射并通过运行 ypinit - c 或 ypinit -s 命令重新生成您的映射，如第 93 页中的 “使用 NIS 映射”中所述。
- 是否已将名称服务转换设置为除了检查 NIS 外还检查计算机的本地 hosts 文件？有关该转换的更多信息，请参见第 2 章，名称服务转换（概述）。
- 是否已将名称服务转换设置为首先在 files 中检查 services 和 rpc？有关该转换的更多信息，请参见第 2 章，名称服务转换（概述）。

ypwhich 显示不一致

在同一客户机上多次使用 ypwhich 时，所显示的结果会随 NIS 服务器的更改而有所不同。这是正常的。当网络或 NIS 服务器繁忙时，NIS 客户机到 NIS 服务器的绑定会不时发生变化。只要可以进行绑定，网络便会在某一时间稳定，所有客户机在此期间从 NIS 服务器获取可接受的响应时间。只要您的客户机能够获得 NIS 服务，服务来源无关紧要。例如，一台 NIS 服务器计算机可以从网络中的其他 NIS 服务器获取其 NIS 服务。

当无法进行服务器绑定时

在无法进行本地服务器绑定的特殊情况下，使用 ypset 命令可以暂时允许绑定到其他网络或子网中的另一台服务器（如果可用）。但是，为了使用 -ypset 选项，必须使用 -ypset 或 -ypsetme 选项启动 ypbind。有关更多信息，请参见 ypbind(1M) 手册页。

```
# /usr/lib/netsvc/yp/ypbind -ypset
```

有关其他方法，请参见第 103 页中的 “绑定到特定 NIS 服务器”。

注意 – 出于安全原因，建议不要使用 -ypset 和 -ypsetme 选项。请仅在可控情况下将这些选项用于调试用途。使用 -ypset 和 -ypsetme 选项可能会导致严重的安全违规，因为在守护进程运行时，任何人都可以更改服务器绑定，这会给其他人带来麻烦，并将允许未经授权的用户访问敏感数据。如果您必须使用这些选项启动 ypbind 守护进程，则在修复问题后，您必须中止 ypbind 进程并在不使用这些选项的情况下将其重新启动。

要重新启动 ypbind 守护进程，请按以下方式使用 SMF：

```
# svcadm enable -r svc:/network/nis/client:default
```

ypbind 崩溃

如果 ypbind 守护进程几乎每次在启动后都会立即崩溃，请在 svc:/network/nis/client:default 服务日志中查找问题。键入以下内容检查是否存在 rpcbind 守护进程：

```
% ps -e |grep rpcbind
```

如果 rpcbind 不存在或没有保持运行或者行为奇怪，请检查 svc:/network/rpc/bind:default 日志文件。有关更多信息，请参见 rpcbind(1M) 和 rpcinfo(1M) 手册页。

您也许能够从正常运行的计算机上与存在问题的客户机中的 rpcbind 通信。从正常运行的计算机中，键入以下内容：

```
% rpcinfo client
```

如果存在问题的计算机中的 rpcbind 正常，rpcinfo 将生成以下输出内容：

```
    program    version    netid     address    service    owner
...
    100007    3    udp6       ::.191.161          ypbind     1
    100007    3    tcp6       ::.135.200          ypbind     1
    100007    3    udp        0.0.0.0.240.221     ypbind     1
    100007    2    udp        0.0.0.0.240.221     ypbind     1
    100007    1    udp        0.0.0.0.240.221     ypbind     1
    100007    3    tcp        0.0.0.0.250.107     ypbind     1
    100007    2    tcp        0.0.0.0.250.107     ypbind     1
    100007    1    tcp        0.0.0.0.250.107     ypbind     1
```

```
    100007    3    ticlts    2\000\000\000       ypbind     1
    100007    2    ticlts    2\000\000\000       ypbind     1
    100007    3    ticotsord 9\000\000\000       ypbind     1
    100007    2    ticotsord 9\000\000\000       ypbind     1
    100007    3    ticots    @\000\000\000       ypbind     1
...
```

您的计算机将具有不同地址。如果未显示这些地址，则 `ypbind` 无法注册其服务。请重新引导计算机并再次运行 `rpcinfo`。如果存在 `ypbind` 进程，并且这些进程在每次重新启动 NIS 服务时都会更改，请重新引导系统，即使 `rpcbind` 守护进程正在运行，也应如此。

影响多台客户机的 NIS 问题

如果只有一两台客户机出现了表明 NIS 绑定问题的症状，则可能是这些客户机存在问题。请参见第 108 页中的 “影响一台客户机的 NIS 问题”。如果许多 NIS 客户机都无法正确绑定，则可能是一台或多台 NIS 服务器存在问题。

rpc.yppasswdd 将以 r 开头的非受限 Shell 视为受限制

1. 创建包含以下特殊字符串的 `/etc/default/yppasswdd`：`"check_restricted_shell_name=1"`。
2. 如果将 `"check_restricted_shell_name=1"` 字符串注释掉，将不会进行 `"r"` 检查。

无法访问网络或服务器

如果网络或 NIS 服务器过载，导致 `ypserv` 守护进程无法在超时时间段内接收返回给客户机 `ypbind` 进程的响应，则 NIS 将挂起。如果网络发生故障，NIS 也可能会挂起。

在这些情况下，网络中的每台客户机都会遇到相同或相似的问题。在大多数情况下，这种问题是暂时的。在重新引导 NIS 服务器并重新启动 `ypserv` 时，NIS 服务器或网络自身的负载降低时，或者当网络恢复正常运行时，这些消息通常会消失。

服务器运转异常

确保服务器已启动并且正在运行。如果您的物理位置离服务器较远，请使用 `ping` 命令。

NIS 守护进程未运行

如果服务器已启动并且正在运行，请尝试找一台能够正常工作的客户机，然后运行 `ypwhich` 命令。如果 `ypwhich` 不响应，请将其中止。然后以 `root` 身份登录 NIS 服务器，并键入以下命令检查 NIS 进程是否正在运行：

```
# ptree |grep ypbind
100759 /usr/lib/netsvc/yp/ypbind -broadcast
        527360 grep yp
```

如果 ypserv（NIS 服务器）或 ypbind（NIS 客户机）守护进程都未运行，请通过键入以下命令重新启动它们：

```
# svcadm restart network/nis/client
```

如果 ypserv 和 ypbind 进程都在 NIS 服务器上运行，请运行 ypwhich 命令。如果该命令没有响应，则表明 ypserv 守护进程可能已挂起并应当重新启动。在以 root 身份登录到服务器后，请键入以下命令重新启动 NIS 服务：

```
# svcadm restart network/nis/server
```

服务器具有不同版本的 NIS 映射

因为 NIS 在服务器之间传播映射，所以有时您可能会在网络中的不同 NIS 服务器上找到同一个映射的不同版本。如果差别持续的时间不长，则此版本差异正常并且可以接受。

导致映射差异最常见的原因是某些因素阻止了正常的映射传播。例如，NIS 服务器或 NIS 服务器之间的路由器关闭。当所有 NIS 服务器以及它们之间的路由器都在运行时，ypxfr 应该会成功。

如果服务器和路由器运行正常，请检查以下各项：

- 检查 ypxfr 日志输出：请参见第 112 页中的 “记录 ypxfr 输出”。
- 检查 svc:/network/nis/xfr:default 日志文件以查找错误。
- 检查控制文件。请参见第 113 页中的 “检查 crontab 文件和 ypxfr Shell 脚本”。
- 检查主服务器上的 ypservers 映射。请参见第 113 页中的 “检查 ypservers 映射”。

记录 ypxfr 输出

如果特定从属服务器在更新映射时出现问题，请登录该服务器并以交互方式运行 ypxfr 命令。如果该命令失败，则它将指明为何失败，并且您可以修复问题。如果此命令运行成功，但您怀疑运行有时失败，请创建一个日志文件以便记录消息。要创建日志文件，请在从属服务器上键入以下命令。

```
ypslave# cd /var/yp
ypslave# touch ypxfr.log
```

这将创建一个 ypxfr.log 文件，该文件会保存 ypxfr 的所有输出。

该输出与 ypxfr 以交互方式运行时所显示的输出类似，但日志文件中的每行都带有时间戳。（您可能会在时间戳中看到异常的排序。这是正常情况－时间戳会告诉您 ypxfr 开始运行的时间。如果 ypxfr 的多个副本同时运行，但所用的时间不同，则它们可能实际上按照不同于调用顺序的顺序将摘要状态行写入日志文件。）任何形式的间歇性故障都会在日志中显示。

注 – 解决问题后，请删除日志文件以关闭记录功能。如果忘记删除该文件，它将继续无限制地增大。

检查 crontab 文件和 ypxfr Shell 脚本

检查 `root crontab` 文件，并检查它调用的 `ypxfr` shell 脚本。这些文件中的排字错误可能会引起传播问题。在 `/var/spool/cron/crontabs/root` 文件中引用 shell 脚本失败，或者在任何 shell 脚本中引用映射失败，也可能会导致错误。

检查 ypservers 映射

另外，请确保 NIS 从属服务器已列在域的主服务器的 `ypservers` 映射中。否则，从属服务器虽然仍可作为服务器正常运行，但 `yppush` 不会将映射的更改传播至从属服务器。

在有故障的从属服务器上更新映射的解决方法

如果 NIS 从属服务器问题不明显，则您可以采用以下解决方法来纠正问题：使用 `scp` 或 `ssh` 命令从正常运行的 NIS 服务器复制不一致映射的最新版本。下面显示了如何传送有问题的映射：

```
ypslave# scp ypmaster:/var/yp/mydomain/map.\* /var/yp/mydomain
```

命令行中的 * 字符已转义，以便它将在 `ypmaster` 上展开，而不是在 `ypslave` 本地展开。

ypserv 崩溃

如果 `ypserv` 进程几乎总是在启动后的瞬间崩溃，并且即使重复启动也无法持续运行，则基本上可按照第 110 页中的 “ypbind 崩溃”中所述的过程进行调试。首先，运行以下命令来查看是否会报告任何错误：

```
# svcs -vx nis/server
```

如下所示，检查是否存在 `rpcbind` 守护进程：

```
# ptree |grep rpcbind
```

如果找不到该守护进程，请重新引导服务器。否则，如果该守护进程正在运行，请键入以下命令查找类似输出：

```
% rpcinfo -p ypserver

% program     vers     proto     port     service
100000    4    tcp    111    portmapper
100000    3    tcp    111    portmapper
100068    2    udp    32813    cmsd
...
```

```
100007    1    tcp    34900    ypbind
100004    2    udp    731    ypserv
100004    1    udp    731    ypserv
100004    1    tcp    732    ypserv
100004    2    tcp    32772    ypserv
```

您的计算机可能具有不同的端口号。表示 ypserv 进程的四个项如下所示：

```
100004     2     udp     731     ypserv
100004     1     udp     731     ypserv
100004     1     tcp     732     ypserv
100004     2     tcp     32772     ypserv
```

如果不存在任何项并且 ypserv 无法向 rpcbind 注册其服务，请重新引导计算机。如果这些项存在，请在重新启动 ypserv 之前从 rpcbind 取消注册服务。要从 rpcbind 中取消注册服务，请在服务器上键入以下命令。

```
# rpcinfo -d number 1
# rpcinfo -d number 2
```

其中，*number* 是 rpcinfo 报告的 ID 号（在以上示例中，ID 号为 100004）。

第 3 部 分

LDAP 命名服务

本部分概述了 LDAP 命名服务。此外，还介绍了 Oracle Solaris OS 中 LDAP 命名服务的设置、配置、管理和故障排除，重点为 Oracle Directory Server Enterprise Edition 的使用。

◆ ◆ ◆ 第 9 章

9 LDAP 命名服务介绍（概述）

与 LDAP 相关的几章介绍了如何设置 LDAP 命名服务客户机来与 Oracle Directory Server Enterprise Edition（以前称作 Sun Java System Directory Server）一起工作。但是，尽管建议使用 Oracle Directory Server Enterprise Edition，但这不是必需的。第 14 章，LDAP 命名服务（参考信息）中简要说明了一般的目录服务器要求。

注 – 目录服务器不一定是 LDAP 服务器。但是，在这些章的上下文中，术语“目录服务器”与“LDAP 服务器”同义。

本章包含以下主题：

目标用户

有关 LDAP 命名服务的各章是为已经熟悉 LDAP 的系统管理员编写的。以下列出了用户必须非常熟悉的部分概念。否则，您使用本指南在 Oracle Solaris 系统中部署 LDAP 命名服务时可能会感到困难。

- LDAP 信息模型（项、对象类、属性、类型和值）

- LDAP 命名模型（目录信息树 (Directory Information Tree, DIT) 结构）
- LDAP 功能模型（搜索参数：基本对象 (base object, DN)、范围、大小限制、时间限制、过滤器（Oracle Directory Server Enterprise Edition 的浏览索引）和属性列表）
- LDAP 安全模型（验证方法和访问控制模型）
- 对 LDAP 目录服务的整体规划和设计（包括如何规划数据以及如何设计 DIT、拓扑、复制和安全性）

建议的背景读物

要更多地了解上述任一概念或者学习 LDAP 及目录服务部署的一般知识，请参阅以下文献：

- 《Oracle Directory Server Enterprise Edition Deployment Guide》

  本指南为目录的规划（包括目录设计、架构设计、目录树、拓扑、复制和安全性）提供基础。最后一章提供了部署方案样例，用于帮助您规划简单的小型部署和复杂的全球部署。
- 《Oracle Directory Server Enterprise Edition Administration Guide》

其他先决条件

如果您需要安装 Oracle Directory Server Enterprise Edition，请参阅所使用的 Oracle Directory Server Enterprise Edition 版本的安装指南。

LDAP 命名服务与其他命名服务的比较

有关 DNS、NIS 和 LDAP 命名服务的比较，请参见第 29 页中的 “命名服务：简要比较”。

LDAP 命名服务的优点

- 使用 LDAP，可以通过替换应用程序特定的数据库来整合信息，这可减少要管理的不同数据库的数目。
- LDAP 允许不同的命名服务共享数据。
- LDAP 可提供一个集中的数据信息库。
- LDAP 允许在主服务器和副本服务器之间更频繁地同步数据。
- LDAP 可兼容多种平台以及由多个供应商提供的产品。

LDAP 命名服务的限制

下面是与 LDAP 命名服务相关联的一些限制：

- 当前不支持 LDAP 服务器成为其自己的客户机。
- 设置和管理 LDAP 命名服务比较复杂且需要仔细规划。
- NIS 客户机和本地 LDAP 客户机不能在同一台客户机上共存。

注 – 目录服务器（LDAP 服务器）**不能**作为其自身的客户机。即，不能将运行目录服务器软件的计算机配置为 LDAP 命名服务客户机。

设置 LDAP 命名服务（任务列表）

任务	参考
规划网络模型。	第 141 页中的 “规划 LDAP 网络模型”
规划目录信息树。	第 10 章，LDAP 命名服务的规划要求（任务）
设置副本服务器。	第 143 页中的 “LDAP 和副本服务器”
规划安全模型。	第 144 页中的 “规划 LDAP 安全模型”
选择客户机配置文件和缺省属性值。	第 146 页中的 “规划 LDAP 的客户机配置文件和缺省属性值”
规划数据置备。	第 146 页中的 “规划 LDAP 数据置备”
配置 Oracle Directory Server Enterprise Edition 之后，再将其用于 LDAP 命名服务。	Oracle Directory Server Enterprise Edition
设置 Oracle Directory Server Enterprise Edition 以用于 LDAP 命名客户机。	第 11 章，为使用 LDAP 客户机设置 Oracle Directory Server Enterprise Edition（任务）
初始化 LDAP 客户机。	第 167 页中的 “初始化 LDAP 客户机”
使用配置文件初始化客户机。	第 167 页中的 “如何使用配置文件初始化 LDAP 客户机”
手动初始化客户机。	第 171 页中的 “如何手动初始化 LDAP 客户机”
取消对客户机的初始化。	第 172 页中的 “如何取消初始化 LDAP 客户机”
使用服务搜索描述符修改客户机配置文件。	第 152 页中的 “使用服务搜索描述符修改客户机对各个服务的访问”
检索命名服务信息。	第 175 页中的 “检索 LDAP 命名服务信息”
定制客户机环境。	第 177 页中的 “定制 LDAP 客户机环境”

LDAP 数据交换格式

LDAP 数据交换格式 (LDAP Data Interchange Format, LDIF) 在许多 LDAP 工具（例如 `ldapadd` 和 `ldapmodify`）之间用作通用的基于文本的交换格式。LDIF RFC 2849 中全面介绍了 LDIF。下面是 `ldapadd` 命令生成的 LDIF 输出的两个示例。使用 `ldaplist(1)` 及 `-l` 选项将显示以下信息。

```
% ldaplist -l hosts myhost
hosts

dn: cn=myhost+ipHostNumber=7.7.7.115,ou=Hosts,dc=mydc,dc=mycom,dc=com
cn: myhost
iphostnumber: 7.7.7.115
objectclass: top
objectclass: device
objectclass: ipHost
description: host 1 - floor 1 - Lab a - building b
% ldaplist -l passwd user1
passwd

dn: uid=user1,ou=People,dc=mydc,dc=mycom,dc=com
uid: user1
cn: user1
userpassword: {crypt}duTx91g7PoNzE
uidnumber: 199995
gidnumber: 20
gecos: Joe Smith [New York]
homedirectory: /home/user1
loginshell: /bin/csh
objectclass: top
objectclass: shadowAccount
objectclass: account
objectclass: posixAccount
```

随 LDAP 使用全限定域名

如果 LDAP 被用来解析主机名，则 LDAP 客户机始终返回主机名的全限定域名 (fully qualified domain name, FQDN)。LDAP 的 FQDN 与 DNS 返回的 FQDN 相似。例如，假设您的域名为以下形式：

```
west.example.net
```

查找主机名 *server* 时，`gethostbyname()` 和 `getnameinfo()` 都返回 FQDN 版本：

```
server.west.example.net
```

缺省目录信息树

缺省情况下，LDAP 客户机在访问信息时会假定目录信息树 (directory information tree, DIT) 具有一个给定的结构。对于 LDAP 服务器支持的每个域，都存在一个具有假定结构的子树。不过，通过指定服务搜索描述符 (Service Search Descriptor, SSD)，可以覆盖该缺省结构。对于一个给定的域，缺省 DIT 将具有一个基本容器，用于存放许多已知容器，这些已知容器存储有特定信息类型的条目。有关这些子树的名称，请参见下表。可以在 RFC 2307 和其他参考资料中找到该信息。

表 9–1 DIT 缺省位置

缺省容器	信息类型
`ou=Ethers`	bootparams、ethers
`ou=Group`	组
`ou=Hosts`	主机、IP 节点、主机的公钥
`ou=Aliases`	别名
`ou=Netgroup`	网络组
`ou=Networks`	网络、网络掩码
`ou=People`	口令、影子、user_attr、audit_user、用户的公钥
`ou=Protocols`	协议
`ou=Rpc`	rpc
`ou=Services`	服务
`ou=SolarisAuthAttr`	auth_attr
`ou=SolarisProfAttr`	prof_attr、exec_attr
`ou=projects`	项目
`automountMap=auto_*`	auto_*

缺省 LDAP 架构

架构是一些定义，用于描述哪些类型的信息可以作为条目存储在 LDAP 目录中。要支持 LDAP 命名客户机，目录服务器的架构可能需要进行扩展。第 14 章，LDAP 命名服务（参考信息）中提供了有关 IETF 架构和特定于 Oracle Solaris 的架构的详细信息。您还可以从 IETF Web 站点 `http://www.ietf.org` 访问各种 RFC。

服务搜索描述符和架构映射

注 – 如果您使用架构映射，请务必谨慎并采用一致的方式。应确保被映射的属性的语法与其映射到的属性的语法一致。换言之，应确保单值属性映射到单值属性，属性的语法保持一致，并且被映射的对象类应该具有正确的强制性属性（可能是映射的属性）。

如上所述，缺省情况下，LDAP 命名服务要求 DIT 以某种特定方式进行构造。如果需要，您可以通过使用服务搜索描述符 (service search descriptor, SSD) 指示 LDAP 命名服务在 DIT 中的其他位置而不是缺省位置进行搜索。另外，您可以指定使用不同的属性和对象类替代缺省架构所指定的属性和对象类。有关缺省过滤器的列表，请参见第 207 页中的 “LDAP 命名服务使用的缺省过滤器”。

SSD 说明

`serviceSearchDescriptor` 属性定义 LDAP 命名服务客户机如何以及在何处搜索特定服务的信息。`serviceSearchDescriptor` 包含一个服务名称，其后跟一个或多个以分号分隔的 base-scope-filter（基-范围-过滤器）三元参数。使用这些 base-scope-filter（基-范围-过滤器）三元参数，可以定义仅搜索特定服务并按顺序进行搜索。如果为某个给定服务指定了多个 base-scope-filter（基-范围-过滤器），则该服务在查找特定条目时，将使用指定的范围和过滤器在每个基容器中进行搜索。

注 – 使用 SSD 时，不会在缺省位置中搜索服务（数据库），除非该 SSD 中包括缺省位置。如果为某个服务指定了多个 SSD，将会产生不可预测的行为。

在下面的示例中，LDAP 命名服务客户机针对 `passwd` 服务在 `ou=west,dc=example,dc=com` 中执行一级搜索，然后在 `ou=east,dc=example,dc=com` 中执行一级搜索。为了查找某个用户的 `username` 的 `passwd` 数据，将针对每个 `BaseDN` 使用缺省的 LDAP 过滤器 `(&(objectClass=posixAccount)(uid=username))`。

```
serviceSearchDescriptor: passwd:ou=west,dc=example,dc=com;ou=east,
dc=example,dc=com
```

在下面的示例中，LDAP 命名服务客户机将针对 `passwd` 服务在 `ou=west,dc=example,dc=com` 中执行子树搜索。为了查找用户 `username` 的 `passwd` 数据，将使用 LDAP 过滤器 `(&(fulltimeEmployee=TRUE)(uid=username))` 来搜索子树 `ou=west,dc=example,dc=com`。

```
serviceSearchDescriptor: passwd:ou=west,dc=example,
dc=com?sub?fulltimeEmployee=TRUE
```

还可以将多个容器与一个特定的服务类型相关联。在以下示例中，服务搜索描述符指定在三个容器中搜索口令条目。

```
ou=myuser,dc=example,dc=com
ou=newuser,dc=example,dc=com
ou=extuser,dc=example,dc=com
```

请注意，在下面的示例中，SSD 中的结尾 ',' 表示 defaultSearchBase 将附加到相对基容器之后。

```
defaultSearchBase: dc=example,dc=com
serviceSearchDescriptor: \
passwd:ou=myuser,;ou=newuser,;ou=extuser,dc=example,dc=com
```

attributeMap 属性

LDAP 命名服务允许为其任何服务重新映射一个或多个属性名称。（LDAP 客户机使用第 14 章，LDAP 命名服务（参考信息）中介绍的众所周知的属性。）如果您映射某个属性，必须确保该属性与初始属性具有相同的含义和语法。请注意，映射 userPassword 属性可能会引起问题。

出于多种原因，您可能需要使用架构映射。

- 希望映射现有目录服务器中的属性
- 如果您的用户名只存在大小写差异，则必须将忽略大小写的 uid 属性映射到不忽略大小写的属性。

此属性的格式为 service:attribute-name=mapped-attribute-name。

如果要为给定服务映射多个属性，则可以定义多个 attributeMap 属性。

在以下示例中，只要将 uid 和 homeDirectory 属性用于 passwd 服务时，便会使用 employeeName 和 home 属性。

```
attributeMap: passwd:uid=employeeName
attributeMap: passwd:homeDirectory=home
```

但也存在可以将 passwd 服务的 gecos 属性映射到多个属性的特殊情况。下面是一个示例：

```
attributeMap: gecos=cn sn title
```

以上示例将 gecos 值映射到一个以空格分隔的包含 cn、sn 和 title 属性值的列表。

objectclassMap 属性

LDAP 命名服务允许为其任何服务重新映射对象类。如果要为给定服务映射多个对象类，则可以定义多个 objectclassMap 属性。在以下示例中，只要使用 posixAccount 对象类时，便会使用 myUnixAccount 对象类。

```
objectclassMap: passwd:posixAccount=myUnixAccount
```

LDAP 客户机配置文件

为简化客户机设置并避免重复为每个客户机输入相同的信息，请在目录服务器上创建单个客户机配置文件。这样，通过一个配置文件便可以为所有配置为使用该配置文件的客户机定义配置。之后配置文件属性的任何更改都会按刷新间隔所定义的频率传播到客户机。

当启动 `svc:/network/ldap/client` 服务时，在 LDAP 客户机配置文件中指定的配置信息会自动导入到 SMF 系统信息库中。

任何客户机配置文件都应当存储在 LDAP 服务器上的一个众所周知的位置中。给定域的根 DN 必须具有一个对象类 `nisDomainObject` 和一个包含客户机所在域的 `nisDomain` 属性。所有的配置文件都位于相对于此容器的 `ou=profile` 容器中。这些配置文件应可以匿名读取。

LDAP 客户机配置文件属性

下表列出了 LDAP 客户机的配置文件属性，这些属性可以在运行 `idsconfig` 时自动设置。有关如何手动设置客户机配置文件的信息，请参见第 171 页中的 “如何手动初始化 LDAP 客户机”和 `idsconfig(1M)` 手册页。

表 9–2 LDAP 客户机配置文件属性

属性	说明
`cn`	配置文件的名称。该属性没有缺省值。必须指定该属性值。
`preferredServerList`	首选服务器的主机地址是以空格分隔的服务器地址的列表。（请勿使用主机名。）将先尝试与该列表中的服务器建立连接，**然后**再尝试与 `defaultServerList` 中的服务器建立连接，直到成功建立连接。该属性没有缺省值。必须至少在 `preferredServerList` 或 `defaultServerList` 中指定一台服务器。
`defaultServerList`	缺省服务器的主机地址是以空格分隔的服务器地址的列表。（请勿使用主机名。）在尝试与 `preferredServerlist` 中的服务器建立连接之后，会先尝试与客户机所在子网中的缺省服务器建立连接，然后再尝试与其余的缺省服务器建立连接，直到成功建立连接。必须至少在 `preferredServerList` 或 `defaultServerList` 中指定一台服务器。只有在尝试与首选服务器列表中的服务器建立连接之后，才会尝试与该列表中的服务器建立连接。该属性没有缺省值。
`defaultSearchBase`	用于查找已知容器的相对 DN。该属性没有缺省值。不过，对于给定服务，可以使用 `serviceSearchDescriptor` 属性来覆盖该属性。
`defaultSearchScope`	定义客户机要搜索的数据库范围。可以使用 `serviceSearchDescriptor` 属性覆盖该属性。可能的值为 `one` 或 `sub`。缺省值为 `one` 级别搜索。

表 9–2 LDAP 客户机配置文件属性 （续）

属性	说明
authenticationMethod	标识了客户机使用的验证方法。缺省值为 none（无）。有关更多信息，请参见第 131 页中的 “为 LDAP 命名服务选择验证方法”。
credentialLevel	标识了客户机进行验证时应使用的凭证的类型。选项有 anonymous、proxy 或 self（也称为每用户）。缺省值为 anonymous。
serviceSearchDescriptor	定义客户机应如何以及应在何处搜索命名数据库，例如，客户机应在 DIT 中的一个点还是多个点执行查找。缺省情况下，不定义任何 SSD。
serviceAuthenticationMethod	客户机针对指定服务使用的验证方法。缺省情况下，不定义任何服务验证方法。如果某个服务未定义 serviceAuthenticationMethod，则使用 authenticationMethod 的缺省值。
attributeMap	客户机使用的属性映射。缺省情况下，未定义任何 attributeMap。
objectclassMap	客户机使用的对象类映射。缺省情况下，不定义任何 objectclassMap。
searchTimeLimit	客户机上的搜索操作在超时之前可以执行的最长时间（以秒为单位）。这不会影响在 LDAP 服务器上完成搜索所需的时间。缺省值为 30 秒。
bindTimeLimit	客户机与服务器的绑定在超时之前可以持续的最长时间（以秒为单位）。缺省值为 30 秒。
followReferrals	指定客户机是否应遵循 LDAP 引用。可能的值为 TRUE 或 FALSE。缺省值为 TRUE。
profileTTL	ldap_cachemgr(1M) 从 LDAP 服务器刷新客户机配置文件的间隔时间。缺省值为 43200 秒（即 12 小时）。如果指定的值为 0，则不刷新配置文件。

本地 LDAP 客户机属性

下表列出了可以使用 ldapclient 命令在本地设置的 LDAP 客户机属性。有关更多信息，请参见 ldapclient(1M) 手册页。

表 9–3 本地 LDAP 客户机属性

属性	说明
adminDN	指定管理凭证的管理员条目标识名。如果在客户机系统上 enableShadowUpdate 开关的值为 true，并且 credentialLevel 的值不是 self，则必须指定 adminDN。

表 9–3 本地 LDAP 客户机属性 （续）

属性	说明
adminPassword	指定管理凭证的管理员条目口令。如果在客户机系统上 enableShadowUpdate 开关的值为 true，并且 credentialLevel 的值不是 self，则必须定义 adminPassword。
domainName	指定客户机的域名（该域将成为此客户机系统的缺省域）。该属性没有缺省值。必须指定该属性值。
proxyDN	代理的标识名。如果为客户机系统配置的 credentialLevel 为 proxy，则必须指定 proxyDN。
proxyPassword	代理的口令。如果为客户机系统配置的 credentialLevel 为 proxy，则必须定义 proxyPassword。
certificatePath	本地文件系统中包含证书数据库的目录。如果为客户机系统配置了使用 TLS 的 authenticationMethod 或 serviceAuthenticationMethod，则将使用此属性。缺省值为 /var/ldap。

注 – 如果 SSD 中的 BaseDN **包含一个结尾逗号**，则会将其视为 defaultSearchBase 的相对值。在执行搜索之前，会将 defaultSearchBase 的值附加在 BaseDN 后面。

ldap_cachemgr 守护进程

ldap_cachemgr 是在 LDAP 客户机上运行的守护进程。ldap_cachemgr 守护进程是由 svc:/network/ldap/client 服务管理的，因此，要使此守护进程正确运行，必须启用该服务。该守护进程执行以下主要功能：

- 以 root 身份运行，获取对配置数据的访问权限
- 刷新服务器上的配置文件中存储的客户机配置信息，并从客户机提取这些数据
- 维护要使用的活动 LDAP 服务器的已排序列表
- 缓存不同客户机提交的一些常见查找请求，以提高查找效率
- 提高主机查找的效率
- 如果 enableShadowUpdate 开关设置为 true，则还获取对所配置的管理员凭证的访问权限并执行对 shadow 数据的更新。

注 – ldap_cachemgr 必须一直运行，LDAP 命名服务才能正常工作。

有关详细信息，请参阅 ldap_cachemgr(1M) 手册页。

LDAP 命名服务安全模型

LDAP 命名服务能够以两种不同的方式使用 LDAP 系统信息库。一种是同时用作命名服务和验证服务的源。另一种是严格用作命名数据的源。本节讨论了当 LDAP 系统信息库同时用作命名服务和验证服务时客户机标识、验证方法、`pam_ldap` 和 `pam_unix_*` 模块以及帐户管理的概念。本节还讨论了 LDAP 命名服务如何与 Kerberos 环境（《Oracle Solaris 11.1 管理：安全服务》中的第 VI 部分, “Kerberos 服务”）和 `pam_krb5(5)` 模块配合使用。

注 – 以前，如果启用了 `pam_ldap` 帐户管理，所有用户在每次登录系统时都必须提供登录口令以进行验证。因此，使用 `ssh` 等工具的非基于口令的登录将失败。

在用户登录时，在不向目录服务器进行验证的情况下执行帐户管理并检索用户的帐户状态。目录服务器上的新控件是 `1.3.6.1.4.1.42.2.27.9.5.8`，它在缺省情况下是启用的。

要将此控制从缺省状态修改为其他状态，请在目录服务器上添加访问控制指令 (Access Control Instructions, ACI)：

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

注 – 如果您使用 Kerberos 作为验证系统并将其与 LDAP 命名系统相集成，则您将能够在您的企业中通过 Kerberos 支持单点登录 (single sign on, SSO)。您还能够在按每用户或每主机查询 LDAP 命名数据时使用同一标识系统。

要访问 LDAP 系统信息库中的信息，客户机将首先向目录服务器证明自己的标识。该标识可以是匿名的，或者是 LDAP 服务器可以识别的主机或用户。LDAP 服务器将根据客户机的标识和服务器的访问控制信息 (access control information, ACI) 允许客户机读取目录信息。有关 ACI 的更多信息，请查阅所用的 Oracle Directory Server Enterprise Edition 版本的管理指南。

如果标识基于发出请求的主机，则您使用的是代理验证。一旦该主机通过验证，则该主机上的所有用户都将获得访问权限。如果标识基于用户，则您使用的是每用户验证。主机上的每个用户都必须通过验证才能获得访问权限。

如果客户机对于任何给定的请求以非匿名方式进行连接，则必须使用自己和服务器均支持的验证方法向服务器证明自己的身份。在确认了自己的身份之后，客户机即可发出各种 LDAP 请求。

当您登录到系统时，PAM 服务可以使用来自本地计算机、来自 LDAP 服务、来自 Kerberos 服务器或这三者的某种组合的信息决定登录尝试是否将成功。当使用 `pam_kerb` 模块时，允许访问的决定是由 Kerberos 服务器做出的。当使用 `pam_ldap` 模块时，一半决定必须由 LDAP 服务器做出，而另一半决定由本地主机做出。使用 `pam_unix_*` 模块时，信息来自本地主机，决定是在本地做出的。

使用 LDAP 服务时，当使用 `pam_ldap` 进行登录时，命名服务访问目录的方式与验证服务 (`pam_ldap`) 访问目录的方式有所不同。命名服务基于预定义的标识从目录中读取各个条目及其属性。验证服务使用用户名和口令向 LDAP 服务器验证用户身份，以确认用户是否输入了正确的口令。有关验证服务的更多信息，请参见 `pam_ldap(5)` 手册页。

当使用 Kerberos 执行验证并且在 LDAP 命名服务中也启用了验证（这是“每用户”模式所必需的）时，Kerberos 可以提供双重功能。Kerberos 向服务器验证身份，主体（用户或主机）的 Kerberos 标识用于向目录验证身份。这样，用于向系统验证身份的用户标识同样也将用于向目录验证身份，以执行查找或更新，如果需要，管理员可以在目录中使用访问控制信息 (Access Control Information, ACI) 来限制命名服务返回的结果。

传输层安全

传输层安全 (transport layer security, TLS) 可以用来保护 LDAP 客户机与目录服务器之间的通信安全，提供保密性和数据完整性。TLS 协议是安全套接字层 (Secure Sockets Layer, SSL) 协议的一个超集。LDAP 命名服务支持 TLS 连接。请注意，使用 SSL 会增加目录服务器和客户机的负荷。

您需要为 SSL 设置目录服务器。有关为 SSL 设置 Oracle Directory Server Enterprise Edition 的更多信息，请参阅您使用的 Oracle Directory Server Enterprise Edition 版本的管理指南。您还需要为 SSL 设置 LDAP 客户机。

如果使用 TLS，必须安装必要的安全数据库。特别的是，需要证书和密钥数据库文件。例如，如果您采用来自 Netscape Communicator 的较旧的数据库格式，则 `cert7.db` 和 `key3.db` 这两个文件是必需的。如果您使用来自 Mozilla 的新数据库格式，则 `cert8.db`、`key3.db` 和 `secmod.db` 这三个文件是必需的。`cert7.db` 或 `cert8.db` 文件中包含受信任证书。`key3.db` 文件中包含客户机的密钥。即使 LDAP 命名服务客户机不使用客户机密钥，此文件也必须存在。`secmod.db` 文件中包含安全模块，如 `PKCS#11` 模块。如果使用的是旧格式，则不需要此文件。

有关更多信息，请参见第 173 页中的 “设置 TLS 安全性”。

指定客户机凭证级别

LDAP 命名服务客户机根据客户机的凭证级别向 LDAP 服务器进行验证。可以为 LDAP 客户机指定多个用以向目录服务器进行验证的级别。

- `anonymous`
- `proxy`
- `proxy anonymous`
- `self`（在本文档中称为每用户）

LDAP anonymous 凭证级别

如果使用 `anonymous` 访问，则只能访问所有人都能使用的数据。在 anonymous 模式中，不能执行 LDAP BIND 操作。此外，还应考虑安全问题。允许对目录的某些部分进行 `anonymous` 访问，意味着任何具有该目录访问权限的人都有读取访问权限。如果使用 `anonymous` 凭证级别，您需要允许对所有 LDAP 命名条目和属性进行读取访问。

注意 – 绝不应当允许对目录进行 `anonymous` 写入，因为那样任何人都可以更改 DIT 中他们对其具有写入访问权限的信息，包括其他用户的口令或他们自己的标识。

注 – Oracle Directory Server Enterprise Edition 允许您基于 IP 地址、DNS 名称、验证方法和一天中的时段对访问进行限制。您可能希望通过进一步的约束来限制访问。有关更多信息，请参见您使用的 Oracle Directory Server Enterprise Edition 版本的管理指南中的“管理访问控制”。

LDAP proxy 凭证级别

客户机验证或者绑定到一组共享的 LDAP 绑定凭证，或者称为代理帐户。此代理帐户可以是任何允许绑定到目录的条目。此代理帐户需要有足够的权限才能在 LDAP 服务器上执行命名服务功能。此代理帐户是一个按系统共享的资源。也就是说，每个使用代理访问权限登录到某个系统的用户（包括 root 用户）与该系统上的所有其他用户看到的结果相同。您需要在使用 `proxy` 凭证级别的每台客户机上配置 `proxyDN` 和 `proxyPassword`。经过加密的 `proxyPassword` 存储在客户机本地。您可以为不同的客户机组设置不同的代理。例如，您可以为所有销售客户机配置一个代理来访问整个公司都可访问的目录以及销售目录，同时阻止销售客户机访问包含工资信息的人力资源目录。或者，在最极端的情况中，您可以为每个客户机指定不同的代理，或者为所有客户机仅指定一个代理。典型的 LDAP 部署应当介于这两种极端情况之间。请仔细考虑您的选择。代理太少可能会限制您对用户访问资源进行控制的能力。但是，代理太多，又会增加系统设置和维护的难度。您需要根据自己的环境向代理用户授予合适的权限。有关如何确定哪种验证方法最适合您的配置的信息，请参见第 131 页中的 “LDAP 客户机的凭证存储”。

如果某个代理用户的口令发生了更改，您需要在使用该代理用户的每台客户机上更新该口令。如果您为 LDAP 帐户使用口令生命期功能，请确保为代理用户关闭此功能。

注 – 请注意，proxy 凭证级别应用于任意给定系统上的所有用户和进程。如果两个用户需要使用不同的命名策略，他们必须使用不同的计算机，或者必须使用“每用户”验证模式。

另外，如果客户机使用 `proxy` 凭证进行验证，则 `proxyDN` 在所有服务器上都必须具有相同的 `proxyPassword`。

LDAP proxy anonymous 凭证级别

`proxy anonymous` 是一个多值条目，它定义了多个凭证级别。指定了 `proxy anonymous` 级别的客户机将首先尝试使用其代理标识进行验证。如果客户机由于某种原因（例如，用户锁定、口令失效）而无法作为代理用户进行验证，客户机将使用匿名访问。这可能会导致服务的级别有所不同，具体取决于目录的配置方式。

LDAP per-user 验证

“每用户”(self) 验证方式在向目录服务器验证身份时使用 Kerberos 标识（主体）来针对每个用户或每个系统执行查找。使用“每用户”验证，系统管理员可以使用访问控制指令 (access control instruction, ACI)、访问控制列表 (access control list, ACL)、角色、组或其他目录访问控制机制来向特定用户或系统授予或拒绝对特定命名服务数据的访问权限。

注 – 在配置“每用户”模式时，用于启用该模式的配置值是“self”，它表示“每用户”模式。

要使用“每用户”验证模型，必须部署 Kerberos 单点登录服务。此外，部署中使用的一个或多个目录服务器必须支持 SASL 和 SASL/GSSAPI 验证机制。因为 Kerberos 预期使用文件和 DNS（而非 LDAP）进行主机名查找，因此应当在该环境中部署 DNS。另外，要使用“每用户”验证，还必须启用 `nscd`。在该配置中，`nscd` 守护进程不是可选组件。

enableShadowUpdate 开关

如果在客户机上 `enableShadowUpdate` 开关设置为 `true`，则将使用管理凭证来更新影子数据。影子数据存储在目录服务器上的 `shadowAccount` 对象类中。管理凭证是由 `adminDN` 和 `adminPassword` 属性的值定义的，如第 125 页中的 “本地 LDAP 客户机属性”中所述。这些管理凭证不用于任何其他用途。

管理凭证具有与 `Proxy` 凭证类似的属性。不同之处在于，对于管理凭证，用户必须具有区域的所有特权或者有效的 `root` UID，才能读取或更新影子数据。管理凭证可以指定给任何允许绑定到目录的条目。不过，**不要**使用 LDAP 服务器的同一目录管理器标识 (`cn=Directory Manager`)。

具有管理凭证的该条目必须具有足够的访问权限才能读取和写入目录中的影子数据。因为该条目是按系统共享的资源，因此必须在每个客户机上配置 adminDN 和 adminPassword 属性。经过加密的 adminPassword 存储在客户机本地。口令使用为客户机配置的相同验证方法。给定系统上的所有用户和进程使用管理凭证读取和更新影子数据。

LDAP 客户机的凭证存储

如果您将客户机配置为使用代理标识，则客户机将代理信息保存在 svc:/network/ldap/client 服务中。当前的 LDAP 实现不将代理凭证存储在客户机的配置文件中。在初始化期间通过使用 ldapclient 设置的任何代理凭证都存储在 SMF 系统信息库中。这样便提高了代理的 DN 和口令信息的安全性。有关设置客户机配置文件的更多信息，请参见第 12 章，设置 LDAP 客户机（任务）。

同样，如果您对客户机进行配置以启用影子数据更新，并且客户机凭证级别不是 self，则客户机会将其信息保存在 svc:/network/ldap/client 服务中。

如果您将客户机配置为使用“每用户”验证，则在验证期间将使用每个主体（每个用户或主机）的 Kerberos 标识和 Kerberos 票证信息。在这样的环境中，目录服务器将 Kerberos 主体映射到一个 DN，并使用 Kerberos 凭证向该 DN 验证身份。然后，目录服务器根据需要使用其访问控制指令 (access control instruction, ACI) 机制来允许或拒绝对命名服务数据的访问。在这种情况下，Kerberos 票证信息用于向目录服务器验证身份，系统不会存储用于验证 DN 或口令。因此，对于此类型的配置，在使用 ldapclient 命令初始化客户机时，不需要指定 adminDN 和 adminPassword 属性。

为 LDAP 命名服务选择验证方法

为客户机指定 proxy 或 proxy-anonymous 凭证级别时，还需要选择代理用来向目录服务器进行验证的方法。缺省情况下，验证方法是 none，它表示匿名访问。验证方法还可以有与之关联的传输安全选项。

验证方法（例如凭证级别）可以是多值的。例如，在客户机配置文件中，您可以指定客户机首先尝试使用由 TLS 保护的 simple 方法进行绑定。如果失败，客户机将尝试使用 sasl/digest-MD5 方法进行绑定。这样，authenticationMethod 将是 tls:simple;sasl/digest-MD5。

LDAP 命名服务支持某些简单身份验证和安全层 (Simple Authentication and Security Layer, SASL) 机制。这些机制无需 TLS 便可安全地交换口令。但是，这些机制不提供数据完整性和保密性。有关 SASL 的信息，请参见 RFC 2222。

支持的验证机制如下所示：

- none

  客户机不向目录验证身份。这等效于 anonymous 凭证级别。

- simple

如果客户机系统使用 simple 验证方法，它将通过以明文形式发送用户口令来绑定到服务器。因此，除非会话受 IPsec 保护，否则口令很容易被窥探。使用 simple 验证方法的主要优点在于所有目录服务器都支持该验证方法且该方法容易设置。

- sasl/digest-MD5

  客户机的口令在验证期间会得到保护，但会话不会被加密。某些目录服务器（包括 Oracle Directory Server Enterprise Edition）还支持 sasl/digest-MD5 验证方法。digest-MD5 的主要优点在于，在验证过程中，口令不会以明文形式通过线路传输，因此比 simple 验证方法更安全。有关 digest-MD5 的信息，请参见 RFC 2831。因为提高了安全性，digest-MD5 被视为是以 cram-MD5 为基础的改进。

  使用 sasl/digest-MD5 时，验证过程是安全的，但会话无法受到保护。

注 – 如果您使用的是 Oracle Directory Server Enterprise Edition，则口令**必须以明文形式存储**在目录中。

- sasl/cram-MD5

  使用 sasl/cram-MD5 执行验证时，不会对 LDAP 会话进行加密，但是在验证期间会保护客户机的口令。此验证方法已过时，不应再使用。

- sasl/GSSAPI

  此验证方法与 self 凭证模式一起使用可启用“每用户”查找。为使用客户机凭证而为每位用户指定的 nscd 使用 sasl/GSSAPI 方法和客户机的 Kerberos 凭证绑定到目录服务器。在目录服务器中，可以对每位用户的访问进行控制。

- tls:simple

  客户机使用 simple 方法进行绑定，并且对会话进行加密。口令也将受到保护。

- tls:sasl/cram-MD5

  对 LDAP 会话进行加密，客户机使用 sasl/cram-MD5 向目录服务器验证身份。

- tls:sasl/digest-MD5

  对 LDAP 会话进行加密，客户机使用 sasl/digest-MD5 向目录服务器验证身份。

注意 – Oracle Directory Server Enterprise Edition 要求口令以明文形式存储才能使用 digest-MD5。如果验证方法设置为 sasl/digest-MD5 或 tls:sasl/digest-MD5，则代理用户的口令将需要以明文形式存储。要特别注意的是，如果 userPassword 属性以明文形式存储，它应具有正确的 ACI，以便它将是不可读的。

下表概述了各种验证方法及其各自的特征。

表 9–4 验证方法

	绑定	线路上的口令	Oracle Directory Server Enterprise Edition 上的口令	会话
none	否	N/A	N/A	无加密
simple	是	明文	任何	无加密
sasl/digest-MD5	是	加密	明文	无加密
sasl/cram-MD5	是	加密	N/A	无加密
sasl/GSSAPI	是	Kerberos	Kerberos	加密
tls:simple	是	加密	任何	加密
tls:sasl/cram-MD5	是	加密	N/A	加密
tls:sasl/digest-MD5	是	加密	明文	加密

为 LDAP 中的特定服务指定验证方法

可以在 serviceAuthenticationMethod 属性中为给定的服务指定验证方法。下列服务允许选择验证方法：

- passwd-cmd

  此服务由 passwd(1) 用来更改登录口令和口令属性。

- keyserv

  此服务由 chkey(1) 和 newkey(1M) 实用程序用来创建和更改用户的 Diffie-Hellman 密钥对。

- pam_ldap

  此服务用于通过 pam_ldap(5) 对用户进行验证。

  pam_ldap 支持帐户管理。

注 – 如果该服务未设置 serviceAuthenticationMethod，则缺省情况下将使用 authenticationMethod 属性的值。

注 – 在每用户模式中，第 135 页中的 “Kerberos 服务模块” (pam Kerberos) 用作验证服务。在此运行模式中，ServiceAuthenticationMethod 不是必需的。

注 – 如果 enableShadowUpdate 开关设置为 true，并且在 passwd-cmd 的 serviceAuthenticationMethod 参数中定义了验证方法，则 ldap_cachemgr 守护进程将使用该方法绑定到 LDAP 服务器。如果不存在，将使用 authenticationMethod。守护进程不会使用 none 验证方法。

下面的示例显示了某个客户机配置文件的一部分，其中，用户将使用 sasl/digest-MD5 来向目录服务器验证身份，但将使用 SSL 会话更改其口令。

```
serviceAuthenticationMethod=pam_ldap:sasl/digest-MD5
serviceAuthenticationMethod=passwd-cmd:tls:simple
```

可插拔验证方法

通过使用 PAM 框架，您可以从几种验证服务中进行选择，包括 pam_unix_*、pam_krb5 和 pam_ldap_* 模块。

如果使用“每用户”验证方法，则必须启用上面列出的三种方法中最强的验证服务 pam_krb5。请参见 pam_krb5(5) 和《Oracle Solaris 11.1 管理：安全服务》。

即使未启用“每用户”验证，也可以使用 pam_krb5 验证系统。如果使用 proxy 或 anonymous 凭证级别来访问目录服务器数据，则无法基于每个用户限制对目录数据的访问。

当使用 anonymous 或 proxy authentication 方法时，建议优先使用 pam_ldap 模块而不是 pam_unix_* 模块，因为其灵活性更强，支持更强的验证方法并且能够使用帐户管理。

pam_unix_* 服务模块

如果您没有更改 /etc/pam.conf 文件，则会缺省启用 UNIX 验证。

注 – pam_unix 模块已被删除并且在 Oracle Solaris 发行版中不再受支持。但是，Solaris 提供了一组其他服务模块，这些模块将提供等效或更强的功能。因此，在本指南中，pam_unix 是指等效的功能，而并非指 pam_unix 模块本身。

下面列出的模块提供了与原始 pam_unix 模块等效的功能。

pam_authtok_check(5)
pam_authtok_get(5)
pam_authtok_store(5)
pam_dhkeys(5)
pam_passwd_auth(5)

pam_unix_account(5)
pam_unix_auth(5)
pam_unix_cred(5)
pam_unix_session(5)

pam_unix_* 模块遵循传统的 UNIX 验证模型，如以下列表中所述。

1. 客户机从名称服务检索用户的加密口令。
2. 系统提示用户输入其口令。
3. 对用户的口令进行加密。
4. 客户机比较这两个经过加密的口令，确定用户是否应通过验证。

此外，使用 pam_unix_* 模块时有两个限制。

- 口令必须以 UNIX crypt 格式存储，而不应采用其他任何加密方法（包括明文）存储。
- 名称服务必须能够读取 userPassword 属性。

  例如，如果您将凭证级别设置为 anonymous，则任何人都必须能够读取 userPassword 属性。同样，如果您将凭证级别设置为 proxy，则代理用户必须能够读取 userPassword 属性。

注 – UNIX 验证与 sasl 验证方法 digest-MD5 不兼容，因为 Oracle Directory Server Enterprise Edition 要求口令以明文形式存储才能使用 digest-MD5。UNIX 验证要求口令以 crypt 格式存储。

注 – 当 enableShadowUpdate 开关设置为 true 时，pam_unix_account 模块支持帐户管理。对远程 LDAP 用户帐户实施控制的方式与对在 passwd 和 shadow 文件中定义的本地用户帐户实施控制的方式相同。在 enableShadowUpdate 模式中，对于 LDAP 帐户，系统将更新并使用 LDAP 服务器上的影子数据执行口令生命期和帐户锁定功能。当然，本地帐户的影子数据仅应用于本地客户机系统，而 LDAP 用户帐户的影子数据将应用于所有客户机系统上的用户。

只有本地客户机支持口令历史记录检查，LDAP 用户帐户不支持此功能。

Kerberos 服务模块

请参阅 pam_krb5(5) 手册页和《Oracle Solaris 11.1 管理：安全服务》。

LDAP 服务模块

当实施 LDAP 验证时，如果在 pam_ldap 的 serviceAuthenticationMethod 参数中定义了验证方法，则用户使用该方法绑定到 LDAP 服务器。否则，将使用 authenticationMethod。

如果 pam_ldap 能够使用用户的身份和提供的口令绑定到服务器，它将验证用户的身份。

注 – 以前，如果启用了 pam_ldap 帐户管理，所有用户在每次登录系统时都必须提供登录口令以进行验证。因此，使用 ssh 等工具的非基于口令的登录将失败。

在用户登录时，在不向目录服务器进行验证的情况下执行帐户管理并检索用户的帐户状态。目录服务器上的新控件是 1.3.6.1.4.1.42.2.27.9.5.8，它在缺省情况下是启用的。

要将此控制从缺省状态修改为其他状态，请在目录服务器上添加访问控制指令 (Access Control Instructions, ACI) :

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

---

pam_ldap 不读取 userPassword 属性。因此，不需要授予对 userPassword 属性的读取访问权限，除非有使用 UNIX 验证的其他客户机。此外，pam_ldap 不支持 none 验证方法。因此，您必须定义 serviceAuthenticationMethod 或 authenticationMethod 属性，以便客户机可以使用 pam_ldap。有关更多信息，请参见 pam_ldap(5) 手册页。

注意 – 如果使用 simple 验证方法，userPassword 属性在传输过程中可能会被第三方读取。

下表汇总了各种验证机制之间的主要区别。

表 9–5 LDAP 中的验证行为

事件	pam_unix_*	pam_ldap	pam_krb5
发送口令	使用 passwd 服务验证方法	使用 passwd 服务验证方法	使用 Kerberos 单点登录技术，不需要口令
发送新口令	加密	不加密（除非使用了 TLS）	使用 Kerberos，不通过线路发送口令
存储新口令	crypt 格式	Oracle Directory Server Enterprise Edition 中定义的口令存储方案	口令由 Kerberos 管理

表 9–5 LDAP 中的验证行为 （续）

事件	pam_unix_*	pam_ldap	pam_krb5
是否需要读取口令?	是	否	否
更改口令之后，是否与 sasl/digest-MD5 兼容	否。口令不以 clear 形式存储。用户无法进行验证。	是。只要将缺省的存储方案设置为 clear，用户即可验证身份。	否。使用了 sasl/GSSAPI。线路上没有口令，目录服务器中也不存储口令，除非所使用的 Kerberos kdc 在 LDAP 目录服务器中管理其口令数据库。
是否支持口令策略?	是。enableShadowUpdate 必须设置为 true。	是（如果进行了这样的配置）。	请参见 pam_krb5(5)（Kerberos V5 帐户管理模块）。

PAM 和更改口令

可使用 passwd 命令更改口令。如果 enableShadowUpdate 开关未设置为 true，则用户必须可以对 userPassword 属性进行写入。如果 enableShadowUpdate 开关设置为 true，则管理凭证必须能够更新 userPassword 属性。请记住，对于此操作，passwd-cmd 的 serviceAuthenticationMethod 会覆盖 authenticationMethod。当前口令在传输过程中可能是未加密的，具体取决于所使用的验证方法。

当使用 UNIX 验证时，在将新的 userPassword 属性写入到 LDAP 之前，将使用 UNIX crypt 格式对其进行加密和标记。因此，无论使用哪种验证方法绑定到服务器，在传输过程中都会对新口令进行加密。有关更多信息，请参见 pam_authtok_store(5) 手册页。

如果 enableShadowUpdate 开关设置为 true，则当用户口令被更改时，pam_unix_* 模块还更新相关的影子信息。pam_unix_* 模块更新的字段与本地用户口令被更改时该模块在本地 shadow 文件中更新的 shadow 字段相同。

pam_ldap 不再支持口令更新。现在，pam_authtok_store 与 server_policy 选项一起替代了 pam_ldap 口令更新功能。当使用 pam_authtok_store 时，新口令以明文形式发送到 LDAP 服务器。因此，为了确保保密性，请使用 TLS。如果不使用 TLS，新的 userPassword 将很容易被窥探。如果您随 Oracle Directory Server Enterprise Edition 设置了无标记的口令，则该软件将使用 passwordStorageScheme 属性对口令进行加密。有关 passwordStorageScheme 的更多信息，请参见所用的 Oracle Directory Server Enterprise Edition 版本的管理指南中有关用户帐户管理的章节。

注 – 设置 passwordStorageScheme 属性时，需要考虑以下配置问题。如果某个 NIS 或使用 UNIX 验证的另一客户机正在使用 LDAP 作为系统信息库，则 passwordStorageScheme 需要是 crypt。另外，如果将使用 sasl/digest-MD5 的 LDAP 验证用于 Oracle Directory Server Enterprise Edition，则 passwordStorageScheme 必须设置为 clear。

LDAP 帐户管理

如果您选择 pam_krb5 作为帐户和口令管理系统，Kerberos 环境将负责管理您所有的帐户、口令、帐户锁定和其他帐户管理详细信息。请参阅 pam_krb5(5) 和《Oracle Solaris 11.1 管理：安全服务》。

如果您不使用 pam_krb5，则可以配置 LDAP 命名服务以利用 Oracle Directory Server Enterprise Edition 中提供的口令和帐户锁定策略支持。您可以配置 pam_ldap(5) 以支持用户帐户管理。与正确的 PAM 配置一起使用时，passwd(1) 可强制实施由 Oracle Directory Server Enterprise Edition 口令策略设置的口令语法规则。

通过 pam_ldap(5)，可以支持以下帐户管理功能。这些功能取决于 Oracle Directory Server Enterprise Edition 的口令和帐户锁定策略配置。您可以根据需要启用任意多的功能。

- 口令生命期和到期通知

  用户必须按照计划更改其口令。如果在配置的时间内未更改口令，口令将过期。过期的口令会导致用户验证失败。

  在过期警告期间内登录时，用户每次都会看到一条警告消息。该消息指出口令将在多少小时或多少天之后到期。

- 口令语法检查

  新口令必须符合口令的最低长度要求。此外，口令不能与用户目录项中的 uid、cn、sn 或 mail 属性的值相同。

- 口令历史记录检查

  用户不能重复使用口令。如果用户尝试将口令更改为之前使用过的某个口令，则 passwd(1) 将失败。LDAP 管理员可以配置保留在服务器历史记录列表中的口令数目。

- 用户帐户锁定

  连续验证失败达到指定次数后，会锁定用户帐户。如果管理员取消激活了某个用户的帐户，该用户也会被锁定。在帐户锁定时间结束或管理员重新激活帐户之前，验证将一直失败。

注 – 上述帐户管理功能只能用于 Oracle Directory Server Enterprise Edition。有关在服务器上配置口令和帐户锁定策略的信息，请参见所用 Oracle Directory Server Enterprise Edition 版本的管理指南中的“用户帐户管理”一章。另请参见第 187 页中的“使用 pam_ldap 模块进行帐户管理的示例 pam_conf 文件”。不要启用对 proxy 帐户的帐户管理。

在 Oracle Directory Server Enterprise Edition 上配置口令和帐户锁定策略之前，请确保所有主机将“最新的”LDAP 客户机用于 pam_ldap 帐户管理。

此外，请确保客户机具有正确配置的 pam.conf(4) 文件。否则，当 proxy 或用户口令到期后，LDAP 命名服务将无法工作。

注 – 以前，如果启用了 pam_ldap 帐户管理，所有用户在每次登录系统时都必须提供登录口令以进行验证。因此，使用 ssh 等工具的非基于口令的登录将失败。

在用户登录时，在不向目录服务器进行验证的情况下执行帐户管理并检索用户的帐户状态。目录服务器上的新控件是 1.3.6.1.4.1.42.2.27.9.5.8，它在缺省情况下是启用的。

要将此控制从缺省状态修改为其他状态，请在目录服务器上添加访问控制指令 (Access Control Instructions, ACI) :

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

使用 pam_unix_* 模块管理 LDAP 帐户

如果在客户机上 enableShadowUpdate 开关设置为 true，则可用于本地帐户的帐户管理功能还可以用于 LDAP 帐户。这些功能包括口令生命期、帐户到期和通知、锁定登录失败的帐户等等。另外，LDAP 中现在支持 passwd 命令的 -dluNfnwx 选项。因此，LDAP 命名服务中支持文件命名服务中的 passwd 命令和 pam_unix_* 模块的全部功能。enableShadowUpdate 开关提供了一种为在文件和 LDAP 作用域中定义的用户实施一致的帐户管理的方法。

为防止用户修改自己的帐户管理数据并借此规避口令策略，LDAP 服务器被配置为阻止用户对服务器上自己的影子数据进行写入访问。具有管理凭证的管理员将负责为客户机系统执行影子数据更新。不过，这种配置与 pam_ldap 模块冲突，因为该模块要求口令可由用户修改。因此，由 pam_ldap 模块执行的帐户管理与由 pam_unix_* 模块执行的帐户管理不兼容。

注意 – 不要在同一个 LDAP 命名域中同时使用 pam_ldap 模块和 pam_unix_* 模块。要么所有客户机都使用 pam_ldap 模块，要么所有客户机都使用 pam_unix_* 模块。因为存在这种限制，您可能需要专用的 LDAP 服务器。例如，某个 web 或电子邮件应用程序可能希望用户能够在 LDAP 服务器上更改自己的口令。

enableShadowUpdate 实现还要求管理凭证（adminDN 与 adminPassword）存储在每个客户机本地。该信息存储在 svc:/network/ldap/client 服务中。

与使用 pam_ldap 进行帐户管理不同，使用 pam_unix_* 模块进行帐户管理不要求更改 /etc/pam.conf 文件。使用缺省的 /etc/pam.conf 文件足以满足要求。

◆ ◆ ◆ 第 10 章

10 LDAP 命名服务的规划要求（任务）

本章讨论在开始设置和安装服务器与客户机之前应进行的高级规划。

本章包含以下主题：

LDAP 规划概述

LDAP 客户机配置文件是配置信息的集合，LDAP 客户机使用这些配置信息访问有关支持 LDAP 服务器的 LDAP 命名服务信息。本章讨论如何规划 LDAP 命名服务的各个方面，其中包括网络模型、目录信息树、安全模型和各种配置文件属性的缺省值，最后讨论如何准备置备数据。

规划 LDAP 网络模型

出于可用性和性能方面的考虑，公司范围的网络的每个子网都应当有各自的 LDAP 服务器，以便为子网中的所有 LDAP 客户机提供服务。这其中只需要有一台服务器作为主 LDAP 服务器即可，其余服务器都可以是主服务器的副本。

要规划网络配置，请考虑可用服务器的数目，客户机如何与各台服务器通信，以及按什么顺序访问各台服务器。如果每个子网只有一台服务器，则可以使用 `defaultServerList` 属性列出所有的服务器，并由 LDAP 客户机排列和安排访问顺序。如果由于速度或数据管理方面的原因需要按特定的顺序访问服务器，则您应当使

用 preferredServerList 属性来定义固定的服务器访问顺序。defaultServerList 平等对待列表中的所有服务器，而 preferredServerList 是有优先顺序的，列表中的第一台服务器是要使用的最佳服务器。主要区别在于，当使用 preferredServerList 时，具有最高优先级的可用服务器将优先于具有较低优先级的其他可用服务器进行使用。当具有较高优先级的服务器变得可用时，客户机将从较低优先级的服务器断开连接。当使用 defaultServerList 时，所有服务器具有相同的优先级，一台服务器联机不会替换现有的服务器。在一个配置中可以同时使用两种列表。请注意，为了减少主服务器上的负荷，不应将主服务器放在其中任何一个列表中。

此外，在规划服务器和网络配置时，可能会发现还有以下三个值得考虑的属性。bindTimeLimit 属性可用于设置 TCP 连接请求的超时值。searchTimeLimit 属性可用于设置 LDAP 搜索操作的超时值。profileTTL 属性可用于控制 LDAP 客户机从服务器下载其配置文件的频率。对于较慢或不稳定的网络，bindTimeLimit 和 searchTimeLimit 属性的值可能需要大于缺省值。在部署的早期测试阶段，您可能需要减小 profileTTL 属性的值，以便客户机提取对存储在 LDAP 服务器中的配置文件的频繁更改。

规划目录信息树

LDAP 命名服务具有一个缺省的目录信息树 (Directory Information Tree, DIT) 和一个关联的缺省架构。例如，ou=people 容器包含用户帐户、口令和影子信息。ou=hosts 容器包含有关网络中各个系统的信息。ou=people 容器中的每个项都将属于 objectclass posixAccount 和 shadowAccount。

缺省 DIT 是一个设计良好的目录结构并且基于开放标准。有关更多信息，请参见 RFC 2307bis 和 RFC 4876。缺省 DIT 应当能够满足大多数命名服务需求，建议不加更改进行使用。如果选择使用缺省 DIT，您只需要决定将从目录树中的哪个节点（基标识名）为特定的域搜索命名服务信息。此节点使用 defaultSearchBase 属性来指定。另外，您可能还要设置 defaultSearchScope 属性，以通知客户机应当在哪个搜索范围内执行命名服务查找。是仅搜索该 DN 下的一层 (one)，还是搜索该 DN 下的所有子树 (sub)?

但有时候，LDAP 命名服务需要更大的灵活性，以便可以处理现有的 DIT 或命名服务数据分散在目录树中的复杂 DIT。例如，用户帐户项可能存在于树的不同部分。客户机配置文件中的 serviceSearchDescriptor、attributeMap 和 objectclassMap 属性设计用于处理这些情况。

使用服务搜索描述符可以覆盖特定服务的缺省搜索基础、搜索范围和搜索过滤器。请参见第 122 页中的 “服务搜索描述符和架构映射”。

attributeMap 和 objectclassMap 属性提供了一种进行架构映射的方法。这些属性使 LDAP 命名服务可以处理现有的 DIT。您可以将 posixAccount 对象类映射到现有的对象类，例如 myAccount。也可以将 posixAccount 对象类中的属性映射到 myAccount 对象类中的属性。

多台目录服务器

多台 LDAP 服务器可以为一个 DIT 提供服务。例如，DIT 的某些子树驻留在其他 LDAP 服务器上。这种情况下，一台 LDAP 服务器可能会指示 LDAP 客户机向其他服务器请求虽然已知、但自身数据库中没有的命名数据。如果您规划这种 DIT 配置，应当设置客户机的配置文件属性 `followReferrals`，指示 LDAP 命名服务遵循服务器引用，以继续执行命名服务查找。但是，应尽可能使给定域的所有命名数据都位于一个目录服务器上。

如果希望客户机在大多数时间访问只读副本，仅在必要时才按照引用访问读/写主服务器，则引用功能可能非常有用。这样，主服务器将不会因原本可以由副本服务器处理的过多请求而过载。

与其他应用程序共享数据

要充分利用 LDAP，每个逻辑项都应该有一个 LDAP 项。例如，对于用户，您不但可以具有公司白页信息、也可以具有帐户信息，还可能具有特定于应用程序的数据。因为 `posixAccount` 和 `shadowAccount` 是辅助对象类，所以它们可以添加到目录中的任何条目。这将需要您仔细规划、设置和管理。

选择目录后缀

有关如何选择合适的目录后缀的信息，请参见 Oracle Directory Server Enterprise Edition 文档。

LDAP 和副本服务器

设置副本服务器时可以采用三种不同的策略。

- 单主复制
- 浮动主复制
- 多主复制

单主

在单主复制中，对于任何给定的分区或非分区网络，仅有一台主服务器保存有目录项的可写副本。所有副本服务器拥有目录项的只读副本。副本服务器和主服务器都可以执行搜索、比较和绑定操作，但只有主服务器可以执行写入操作。

单主复制策略的潜在缺点是主服务器会出现单点故障。如果主服务器关闭，任何副本都无法处理写入操作。

浮动主

浮动主策略与单主策略类似，即在任何给定时间内，对于给定的分区或非分区网络，仅有一台主服务器具有写入功能。但是，实现浮动主策略时，如果主服务器关闭，会有一台副本服务器通过某种算法自动转换为主服务器。

浮动主复制策略的潜在缺点是，如果网络成为分区网络并且分区任一端的副本服务器成为主服务器，则网络重新连接后，协调新主服务器的过程会非常复杂。

多主

如果采用多主复制，多台主服务器各自拥有目录项数据的读写副本。尽管多主策略消除了单点故障问题，但服务器之间仍会发生更新冲突。换句话说，如果在两台主服务器上几乎同时修改某项的属性，则必须备有解决更新冲突的策略，如“最后写入者取得权限”。

有关如何设置副本服务器的信息，请参阅您使用的 Oracle Directory Server Enterprise Edition 版本的管理员指南。通常，对于大规模企业部署，建议使用多主复制。

规划 LDAP 安全模型

要规划安全模型，首先应当考虑 LDAP 客户机与 LDAP 服务器通信时应使用什么身份。例如，您必须确定是希望使用企业范围内的单点登录解决方案（该方案不通过线路发送口令），还是希望基于每个用户对数据进行线路加密并能够访问目录服务器中的控制数据结果。您还必须确定是否希望使用强验证来保护通过网络传输的用户口令，以及/或者是否需要加密 LDAP 客户机与 LDAP 服务器之间的会话来保护传输的 LDAP 数据。

配置文件中的 `credentialLevel` 和 `authenticationMethod` 属性用于此用途。`credentialLevel` 有四种可能的凭证级别：`anonymous`、`proxy`、`proxy anonymous` 和 `self`。有关 LDAP 命名服务安全概念的详细讨论，请参见第 127 页中的 “LDAP 命名服务安全模型”。

注 – 以前，如果启用了 pam_ldap 帐户管理，所有用户在每次登录系统时都必须提供登录口令以进行验证。因此，使用 ssh 等工具的非基于口令的登录将失败。

在用户登录时，在不向目录服务器进行验证的情况下执行帐户管理并检索用户的帐户状态。目录服务器上的新控件是 1.3.6.1.4.1.42.2.27.9.5.8，它在缺省情况下是启用的。

要将此控制从缺省状态修改为其他状态，请在目录服务器上添加访问控制指令 (Access Control Instructions, ACI)：

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

注 – 如果您启用 pam_krb5 和 Kerberos 作为企业范围内的单点登录解决方案，可以设计一个仅在启动会话时需要提供一次登录口令的系统。有关详细信息，请参见《Oracle Solaris 11.1 管理：安全服务》。如果您启用了 Kerberos，通常也需要启用 DNS。有关详细信息，请参见本手册中有关 DNS 的各章。

下面列出了在规划安全模型时需要做出的主要决策。

- 是否要使用 Kerberos 和按用户验证?
- LDAP 客户机将使用哪个凭证级别以及哪些验证方法?
- 是否要使用 TLS?
- 您是否需要向后兼容 NIS? 换句话说，客户机是否将使用 pam_unix_* 或 pam_ldap 模块?
- 如何设置服务器的 passwordStorageScheme 属性?
- 如何设置访问控制信息?

  有关 ACI 的更多信息，请查阅所用的 Oracle Directory Server Enterprise Edition 版本的管理指南。
- 客户机将使用 pam_unix_* 还是 pam_ldap 模块来执行 LDAP 帐户管理?

规划 LDAP 的客户机配置文件和缺省属性值

完成以上规划步骤（网络模型、DIT 和安全模型）之后，应当对以下配置文件属性的值有一些了解。

- cn
- defaultServerList
- preferredServerList
- bindTimeLimit
- searchTimeLimit
- profileTTL
- defaultSearchBase
- defaultSearchScope
- serviceSearchDescriptor
- attributeMap
- objectclassMap
- followReferrals
- credentialLevel
- authenticationMethod
- serviceCredentialLevel
- serviceAuthenticationMethod

在以上各属性中，仅有 cn、defaultServerList 和 defaultSearchBase 是必需的。这些属性没有缺省值。其余属性是可选的，其中有些具有缺省值。

有关设置 LDAP 客户机的更多信息，请参见第 12 章，设置 LDAP 客户机（任务）。

规划 LDAP 数据置备

在为 LDAP 服务器配置了正确的 DIT 和架构后，要向 LDAP 服务器置备数据，请使用新的 ldapaddent 工具。此工具将根据 LDAP 容器对应的 /etc 文件在容器中创建项。使用此工具，可以将数据置备到以下数据类型的容器中：aliases、auto_*、bootparams、ethers、group、hosts（包括 IPv6 地址）、netgroup、netmasks、networks、passwd、shadow、protocols、publickey、rpc 和 services。另外，还可以添加与 RBAC 相关的文件：/etc/user_attr、/etc/security/auth_attr、/etc/security/prof_attr 和 /etc/security/exec_attr。

缺省情况下，ldapaddent 从标准输入中读取数据并将其添加到与命令行中指定的数据库关联的 LDAP 容器中。但是，可以使用 -f 选项指定一个输入文件，以便从中读取数据。

由于项存储在基于客户机配置的目录中，因此必须将客户机配置为使用 LDAP 命名服务。

为了获得更好的性能，请按以下顺序装入数据库：

1. 装入 passwd 数据库后再装入 shadow 数据库
2. 装入 networks 数据库后再装入 netmasks 数据库
3. 装入 bootparams 数据库后再装入 ethers 数据库

请注意，在添加自动挂载程序项时，数据库名称的形式为 auto_*（例如 auto_home）。

如果您要添加到 LDAP 服务器的 /etc 文件来自不同的主机，您可以将它们合并到同一个 /etc 文件中然后在一台主机上使用 ldapaddent 命令，也可以依次在不同的主机上运行 ldapaddent 命令，除了已配置为 LDAP 客户机的每台主机。

如果您的命名服务数据已在 NIS 服务器中，并且您希望将 LDAP 命名服务的数据移动到 LDAP 服务器中，请使用 ypcat 命令将 NIS 映射转储到文件中。然后，对这些文件运行 ldapaddent 命令来将数据添加到 LDAP 服务器。

以下过程假定将要从 yp 客户机提取表。

▼ 如何使用 ldapaddent 命令向服务器置备 host 项

1 确保已使用 idsconfig 命令设置了 Oracle Directory Server Enterprise Edition。

2 在客户机上，成为超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的第 9 章 “使用基于角色的访问控制（任务）”。

3 使计算机成为 LDAP 客户机。

```
# ldapclient init -a profileName=new -a domainName=west.example.com 192.168.0.1
```

4 使用数据置备服务器。

```
# ldapaddent -D “cn=directory manager” -f /etc/hosts hosts
```

系统将提示您输入口令。

在此示例中，ldapaddent 命令将使用已在配置文件 "new" 中配置的验证方法。选择 "simple" 将以明文形式发送口令。有关更多信息，请参阅 ldapaddent(1M) 手册页。

在独立模式中，该命令应类似于以下内容：

```
# ldapaddent -h 192.168.0.1 -N new -M west.example.com -a simple-D “cn=directory manager” -f /etc/hosts hosts
```

◆ ◆ ◆ 第 11 章

为使用 LDAP 客户机设置 Oracle Directory Server Enterprise Edition（任务）

本章介绍了如何对 Oracle Directory Server Enterprise Edition 进行配置来支持 LDAP 命名服务客户机网络。本章中的信息特定于 Oracle Directory Server Enterprise Edition。有关安装和配置目录服务器的信息，请参见 Oracle Directory Server Enterprise Edition 文档。

注 – 您必须已执行了 Oracle Directory Server Enterprise Edition 随附的安装和配置文档中所述的所有过程，然后才能将 Oracle Directory Server Enterprise Edition 配置为与 LDAP 客户机一起工作。

注 – 目录服务器（LDAP 服务器）**不能**作为其自身的客户机。

本章包含以下主题：

使用 idsconfig 命令配置 Oracle Directory Server Enterprise Edition

基于服务器安装创建核对表

在服务器安装过程中，您将遇到一些已定义的极其重要的变量，在启动 idsconfig 之前，您应当为这些变量创建类似于下表的核对表。您可以使用第 185 页中的 “用于配置 LDAP 的空核对表 ”中提供的空白核对表。

注 – 下面包含的信息将用作与 LDAP 相关的章节中所有示例的基础。示例域属于一家装饰品公司 Example, Inc.，该公司在全国各地都有商店。示例涉及 West Coast Division（西海岸分公司），域名为 west.example.com。

表 11–1 为 example.com 网络定义的服务器变量

变量	针对示例网络的定义
安装了目录服务器实例的端口号	389（缺省值）
服务器名称	myserver（来自 FQDN myserver.west.example.com 或者为 192.168.0.1 的主机名）
副本服务器（IP 号:端口号）	192.168.0.2 [对于 myreplica.west.example.com]
目录管理器	cn=Directory Manager（缺省值）
要为其提供服务的域名	west.example.com
在超时之前处理客户端请求的最长时间（以秒为单位）	1
为每个搜索请求返回的最多项数	1

注 – 如果您在定义 defaultServerList 或 preferredServerList 时使用了主机名，则**必须**确保没有将 LDAP 用于主机查找。这意味着不能在 svc:/network/name-service/switch 服务的 config/host 属性中配置 ldap。

表 11–2 为 example.com 网络定义的客户机配置文件变量

变量	针对示例网络的定义
配置文件名（缺省名称是 default）	WestUserProfile

表 11–2 为 example.com 网络定义的客户机配置文件变量 （续）

变量	针对示例网络的定义
服务器列表（缺省值为本地子网）	192.168.0.1
首选服务器列表（按照对服务器进行查找的顺序列出）	none
搜索范围（沿着目录树向下查找的层数。'One'（缺省值）或 'Sub'）	one（缺省值）
用于获取服务器访问权限的凭证。缺省值为 anonymous	proxy
是否遵循引用（主服务器不可用时指向另一台服务器的指针）？ 缺省值为 no。	Y
等待服务器返回信息的搜索时间限制（缺省值为 30 秒）。	default
与服务器进行联系时的绑定时间限制（缺省值为 10 秒）。	default
验证方法（缺省值为 none）。	simple

注 – 客户机配置文件是按每个域进行定义的。必须至少为给定的域定义一个配置文件。

属性索引

idsconfig 命令为以下列表中的属性编制索引以提高性能：

```
membernisnetgroup    pres,eq,sub
nisnetgrouptriple    pres,eq,sub
ipHostNumber         pres,eq,sub
uidNumber            pres,eq
gidNumber            pres,eq
ipNetworkNumber      pres,eq
automountkey         pres,eq
oncRpcNumber         pres,eq
```

架构定义

idsconfig(1M) 自动添加所需的架构定义。除非您在 LDAP 管理方面经验丰富，否则请不要手动修改服务器架构。有关 LDAP 命名服务使用的架构的扩展列表，请参见第 14 章，LDAP 命名服务（参考信息）。

使用浏览索引

Oracle Directory Server Enterprise Edition 的浏览索引功能或者称为虚拟列表视图 (virtual list view, VLV) 提供了一种方法来使客户机可以查看从非常长的列表中挑选的一组或许多条目，从而使每个客户机的搜索过程少费时间。浏览索引提供了经优化的预定义搜索参数，通过它们，LDAP 命名客户机可以更快速地从各种服务访问特定的信息。请记住，如果您没有创建浏览索引，则在超出了服务器限制时，客户机将不会访问给定类型的所有条目。例如，如果有 5000 个口令条目，但启用的大小限制为 1000 个条目，则在某些查找操作中，将有 4000 个条目不会返回。这经常会导致客户机登录失败或出现其他严重故障。

VLV 索引是在目录服务器上配置的，代理用户对这些索引具有读取访问权限。

在 Oracle Directory Server Enterprise Edition 上配置浏览索引之前，请考虑与使用这些索引相关联的性能成本。有关更多信息，请参阅所用的 Oracle Directory Server Enterprise Edition 版本的管理指南。

`idsconfig` 为多个 VLV 索引创建项。有关更多信息，请参见 `idsconfig(1M)` 手册页。请参阅 `idsconfig` 命令的输出来确定由 `idsconfig` 创建的 VLV 条目。有关 `idsconfig` 输出样例，请参见第 154 页中的 “`idsconfig` 设置示例”。

使用服务搜索描述符修改客户机对各个服务的访问

服务搜索描述符 (service search descriptor, SSD) 可以将 LDAP 中给定操作的缺省搜索请求更改为您定义的搜索。例如，如果您一直使用的是具有定制容器定义的 LDAP 或其他操作系统，而现在要转为使用最新的 Oracle Solaris 发行版，则 SSD 将特别有用。使用 SSD，您不必更改现有的 LDAP 数据库和数据即可配置 LDAP 命名服务。

使用 idsconfig 命令设置 SSD

假设 Example, Inc. 中的前任管理员已经配置了 LDAP，并将用户存储在 `ou=Users` 容器中。您现在要升级到最新的 Oracle Solaris 发行版。根据定义，LDAP 客户机假定用户条目存储在 `ou=People` 容器中。因此，当开始搜索 `passwd` 服务时，LDAP 客户机将搜索 DIT 的`ou=people` 层，因而不会找到正确的值。

对于上述问题，一个比较繁琐的解决方案是完全覆盖 Example, Inc. 现有的 DIT，并重写 Example, Inc. 网络上现有的所有应用程序，以便它们与新的 LDAP 命名服务兼容。另外一种更可取的解决方案是，使用 SSD 通知 LDAP 客户机在 `ou=Users` 容器（而不是缺省的 `ou=people` 容器）中查找用户信息。

您将在配置 Oracle Directory Server Enterprise Edition 的过程中使用 `idsconfig` 定义所需的 SSD。提示行如下所示：

```
Do you wish to setup Service Search Descriptors (y/n/h? y
  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's

  Q  Exit menu
Enter menu choice: [Quit] a
Enter the service id: passwd
Enter the base: service ou=user,dc=west,dc=example,dc=com
Enter the scope: one[default]
  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's

  Q  Exit menu
Enter menu choice: [Quit] p

Current Service Search Descriptors:
==================================
Passwd:ou=Users,ou=west,ou=example,ou=com?

Hit return to continue.

  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's

  Q  Exit menu
Enter menu choice: [Quit] q
```

运行 idsconfig 命令

注 – 运行 idsconfig 无需特殊权限，也不必在 LDAP 命名客户机上运行。在为运行 idsconfig 做准备工作时，请记得创建第 150 页中的 “基于服务器安装创建核对表”中提到的核对表。您不必从服务器或 LDAP 命名服务客户机运行 idsconfig。您可以从网络上的任何 Oracle Solaris 计算机运行 idsconfig。

注意 – idsconfig 以明文形式发送目录管理器的口令。如果不希望如此，必须在目录服务器（而非客户机）上运行 idsconfig。

▼ 如何使用 idsconfig 命令配置 Oracle Directory Server Enterprise Edition

1 **确保目标 Oracle Directory Server Enterprise Edition 已启动并且正在运行。**

2 **运行 idsconfig 命令。**

```
# /usr/lib/ldap/idsconfig
```

有关使用本章开头的第 150 页中的 “基于服务器安装创建核对表”中的服务器和客户机核对表中列出的定义运行 idsconfig 的示例，请参阅示例 11–1。

3 **根据提示回答问题。**

请注意 "no" [n] 是缺省的用户输入。如果需要清楚理解任何给定的问题，请键入

```
h
```

此时将出现一个简短的帮助段落。

在 idsconfig 完成了目录的设置之后，您需要在服务器上运行指定的命令，然后才能完成服务器的设置过程，服务器此时即准备就绪，可以为客户机提供服务。

idsconfig 设置示例

本节提供了一个基本的 idsconfig 设置的示例，该示例使用了许多缺省值。修改客户机配置文件最复杂的方法就是创建 SSD。有关详细讨论，请参阅第 152 页中的 “使用服务搜索描述符修改客户机对各个服务的访问”。

提示后面方括号中的数据指示该提示的缺省值。要接受缺省值，请按下 Return 键。

注 – 对于摘要屏幕上任何留空的参数将不进行设置。

在 idsconfig 完成了目录的设置之后，您需要在服务器上运行指定的命令，然后才能完成服务器的设置过程，服务器此时即准备就绪，可以为客户机提供服务。

示例 11–1 为 Example, Inc. 网络运行 idsconfig 命令

以下示例中，在 LDAP 服务器上创建了服务器实例后，idsconfig 实用程序将立即运行。

```
# usr/lib/ldap/idsconfig
It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.
```

示例 11–1 为 Example, Inc. 网络运行 idsconfig 命令 （续）

```
Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  No valid suffixes were found for Base DN dc=west,dc=example,dc=com
Enter suffix to be created (b=back/h=help): [dc=west,dc=example,dc=com]
Enter ldbm database name (b=back/h=help): [west]
  sasl/GSSAPI is not supported by this LDAP server
Enter the profile name (h=help): [default] WestUserProfile
Default server list (h=help): [192.168.0.1]
Preferred server list (h=help):
Choose desired search scope (one, sub, h=help):  [one]
The following are the supported credential levels:
  1  anonymous
  2  proxy
  3  proxy anonymous
  4  self
Choose Credential level [h=help]: [1] 2
The following are the supported Authentication Methods:
  1  none
  2  simple
  3  sasl/DIGEST-MD5
  4  tls:simple
  5  tls:sasl/DIGEST-MD5
  6  sasl/GSSAPI
Choose Authentication Method (h=help): [1] 2


Current authenticationMethod: simple
Do you want to add another Authentication Method? n
Do you want the clients to follow referrals (y/n/h)? [n]
Do you want to modify the server timelimit value (y/n/h)? [n] y
Enter the time limit for DSEE (current=3600): [-1]
Do you want to modify the server sizelimit value (y/n/h)? [n] y
Enter the size limit for DSEE (current=2000): [-1]
Do you want to store passwords in "crypt" format (y/n/h)? [n] y
Do you want to setup a Service Authentication Methods (y/n/h)? [n]
Client search time limit in seconds (h=help): [30]
Profile Time To Live in seconds (h=help): [43200]
Bind time limit in seconds (h=help): [10]
Do you want to enable shadow update (y/n/h)? [n]
Do you wish to setup Service Search Descriptors (y/n/h)? [n]

              Summary of Configuration

  1  Domain to serve              : west.example.com
  2  Base DN to setup             : dc=west,dc=example,dc=com
        Suffix to create          : dc=west,dc=example,dc=com
        Database to create        : west
```

示例 11–1 为 Example, Inc. 网络运行 idsconfig 命令 （续）

```
  3  Profile name to create        : WestUserProfile
  4  Default Server List           : 192.168.0.1
  5  Preferred Server List         :
  6  Default Search Scope          : one
  7  Credential Level              : proxy
  8  Authentication Method         : simple
  9  Enable Follow Referrals       : FALSE
 10  DSEE Time Limit                : -1
 11  DSEE Size Limit                : -1
 12  Enable crypt password storage : TRUE
 13  Service Auth Method pam_ldap  :
 14  Service Auth Method keyserv   :
 15  Service Auth Method passwd-cmd:
 16  Search Time Limit             : 30
 17  Profile Time to Live          : 43200
 18  Bind Limit                    : 10
 19  Enable shadow update          : FALSE
 20  Service Search Descriptors Menu

Enter config value to change: (1-20 0=commit changes) [0]
Enter DN for proxy agent: [cn=proxyagent,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for proxyagent:
Re-enter passwd:

WARNING: About to start committing changes. (y=continue, n=EXIT) y

  1. Changed timelimit to -1 in cn=config.
  2. Changed sizelimit to -1 in cn=config.
  3. Changed passwordstoragescheme to "crypt" in cn=config.
  4. Schema attributes have been updated.
  5. Schema objectclass definitions have been added.
  6. Database west successfully created.
  7. Suffix dc=west,dc=example,dc=com successfully created.
  8. NisDomainObject added to dc=west,dc=example,dc=com.
  9. Top level "ou" containers complete.
  10. automount maps: auto_home auto_direct auto_master auto_shared processed.
  11. ACI for dc=west,dc=example,dc=com modified to disable self modify.
  12. Add of VLV Access Control Information (ACI).
  13. Proxy Agent cn=proxyagent,ou=profile,dc=west,dc=example,dc=com added.
  14. Give cn=proxyagent,ou=profile,dc=west,dc=example,dc=com read permission
      for password.
  15. Generated client profile and loaded on server.
  16. Processing eq,pres indexes:
      uidNumber (eq,pres)   Finished indexing.
      ipNetworkNumber (eq,pres)   Finished indexing.
      gidnumber (eq,pres)   Finished indexing.
      oncrpcnumber (eq,pres)   Finished indexing.
      automountKey (eq,pres)   Finished indexing.
  17. Processing eq,pres,sub indexes:
      ipHostNumber (eq,pres,sub)   Finished indexing.
      membernisnetgroup (eq,pres,sub)   Finished indexing.
      nisnetgrouptriple (eq,pres,sub)   Finished indexing.
  18. Processing VLV indexes:
      west.example.com.getgrent vlv_index   Entry created
      west.example.com.gethostent vlv_index   Entry created
```

示例 11–1 为 Example, Inc. 网络运行 idsconfig 命令 （续）

```
      west.example.com.getnetent vlv_index   Entry created
      west.example.com.getpwent vlv_index   Entry created
      west.example.com.getrpcent vlv_index   Entry created
      west.example.com.getspent vlv_index   Entry created
      west.example.com.getauhoent vlv_index   Entry created
      west.example.com.getsoluent vlv_index   Entry created
      west.example.com.getauduent vlv_index   Entry created
      west.example.com.getauthent vlv_index   Entry created
      west.example.com.getexecent vlv_index   Entry created
      west.example.com.getprofent vlv_index   Entry created
      west.example.com.getmailent vlv_index   Entry created
      west.example.com.getbootent vlv_index   Entry created
      west.example.com.getethent vlv_index   Entry created
      west.example.com.getngrpent vlv_index   Entry created
      west.example.com.getipnent vlv_index   Entry created
      west.example.com.getmaskent vlv_index   Entry created
      west.example.com.getprent vlv_index   Entry created
      west.example.com.getip4ent vlv_index   Entry created
      west.example.com.getip6ent vlv_index   Entry created

idsconfig: Setup of DSEE server myserver is complete.


Note: idsconfig has created entries for VLV indexes.

      For DS5.x, use the directoryserver(1m) script on myserver
      to stop the server.  Then, using directoryserver, follow the
      directoryserver examples below to create the actual VLV indexes.

      For DSEE6.x, use dsadm command delivered with DS on myserver
      to stop the server.  Then, using dsadm, follow the
      dsadm examples below to create the actual VLV indexes.

  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getgrent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.gethostent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getnetent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getpwent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getrpcent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getspent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauhoent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getsoluent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauduent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauthent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getexecent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getprofent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getmailent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getbootent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getethent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getngrpent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getipnent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getmaskent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getprent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getip4ent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getip6ent
```

示例 11–1　为 Example, Inc. 网络运行 idsconfig 命令　　（续）

```
<install-path>/bin/dsadm reindex -l -t west.example.com.getgrent <directory-instance-path>
 dc=west,dc=example,dc=com
<install-path>/bin/dsadm reindex -l -t west.example.com.gethostent <directory-instance-path>
 dc=west,dc=example,dc=com
.
.
.
<install-path>/bin/dsadm reindex -l -t west.example.com.getip6ent <directory-instance-path>
 dc=west,dc=example,dc=com
```

使用 ldapaddent 命令置备目录服务器

注 – 如果您使用的是 pam_unix_* 模块，则在用数据置备目录服务器之前，您必须将服务器配置为以 UNIX Crypt 格式来存储口令。如果您使用的是 pam_ldap，则可以用任何格式存储口令。有关以 UNIX crypt 格式设置口令的更多信息，请参见 Oracle Directory Server Enterprise Edition 文档。

ldapaddent 从标准输入（是一个类似 passwd 的 /etc/filename）中读取数据，然后将该数据放置在与服务关联的容器中。客户机的配置决定了数据的缺省写入方式。

▼ 如何使用 ldapaddent 命令向 Oracle Directory Server Enterprise Edition 置备用户口令数据

- **使用 ldapaddent 命令向服务器中添加 /etc/passwd 项。**

  ```
  # ldapaddent -D "cn=directory manager" -f /etc/passwd passwd
  ```

  请参见 ldapaddent(1M) 手册页。有关 LDAP 安全和对目录服务器的写入权限的信息，另请参见第 9 章，LDAP 命名服务介绍（概述）。

使用 Member 属性指定组成员关系

Internet 草稿 rfc2307bis 指定 groupOfMembers 对象类还可以用作组服务的 LDAP 项的方便结构化类。然后，这样的组项可以具有以标识名 (Distinguished Name, DN) 指定组成员关系的 member 属性值。Oracle Solaris LDAP 客户机支持这样的组项并使用 member 属性值进行组成员关系解析。

LDAP 客户机还支持使用 groupOfUniqueNames 对象类和 uniqueMember 属性的组项。不过，建议不要使用此对象类和属性。

为组项定义 posixGroup 对象类和 memberUid 属性的现有方法仍然受支持。这种类型的组项仍然是在为组服务置备 LDAP 服务器时由 ldapaddent 命令创建的。它不向组项添加 member 属性。

要为组项添加 groupOfMembers 对象类和 member 属性值，请使用 ldapadd 工具和类似于以下内容的一个输入文件：

```
dn: cn=group1,ou=group,dc=mkg,dc=example,dc=com
objectClass: posixGroup
objectClass: groupOfNames
objectClass: top
cn: group1
gidNumber: 1234
member: uid=user1,ou=people,dc=mkg,dc=example,dc=com
member: uid=user2,ou=people,dc=mkg,dc=example,dc=com
member: cn=group2,ou=group,dc=mkg,dc=example,dc=com
```

LDAP 客户机将在不使用 memberUid、member 和 uniqueMember 属性或者使用它们中的任意属性或使用所有这些属性的情况下处理组项。成员关系评估结果将是，组的成员为所有三个成员的合集，其中删除了重复项。也就是说，如果组项 G 具有一个引用了用户 U1 和 U2 的 memberUid 值、一个引用了用户 U2 的 member 值和一个引用了用户 U3 的 uniqueMember 值，则组 G 具有三个成员（U1、U2 和 U3）。还支持嵌套组，也就是说，member 属性可以具有指向其他组的值。

为有效地评估组成员关系以确定用户所属的组（包括嵌套的组），必须在 LDAP 服务器上配置并启用 memberOf 插件。如果没有，则将只会解析包含组，而不会解析嵌套的组。缺省情况下，memberOf 插件由 ODSEE 服务器启用。如果该插件未启用，请使用 ODSEE 的 dsconf 工具将其启用。

向目录服务器置备其他配置文件

使用 ldapclient 命令和 genprofile 选项基于所指定的属性创建配置文件的 LDIF 表示形式。所创建的配置文件随后可以装入 LDAP 服务器中用作客户机配置文件。客户机可以使用 ldapclient init 来下载客户机配置文件。

有关使用 ldapclient genprofile 的信息，请参阅 ldapclient(1M)。

▼ 如何使用 ldapclient 命令向目录服务器置备其他配置文件

1 成为管理员。

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 使用带 genprofile 的 ldapclient 命令。

```
# ldapclient genprofile \
-a profileName=myprofile \
-a defaultSearchBase=dc=west,dc=example,dc=com \
-a "defaultServerList=192.168.0.1 192.168.0.2:386" \> myprofile.ldif
```

3 将新配置文件上载到服务器。

```
# ldapadd -h 192.168.0.1 -D “cn=directory manager” -f myprofile.ldif
```

配置目录服务器以启用帐户管理

可以为使用 pam_ldap 的客户机和使用 pam_unix_* 模块的客户机实施帐户管理。

注意 – 不要在同一个 LDAP 命名域中同时使用 pam_ldap 和 pam_unix_* 模块。要么所有客户机都使用 pam_ldap 模块，要么所有客户机都使用 pam_unix_* 模块。因为存在这种限制，您可能需要专用的 LDAP 服务器。

对于使用 pam_ldap 模块的客户机

为了让 pam_ldap 能够正常工作，必须在服务器上正确配置口令和帐户锁定策略。您可以使用 Directory Server Console 或 ldapmodify 为 LDAP 目录配置帐户管理策略。有关过程和更多信息，请参见您使用的 Oracle Directory Server Enterprise Edition 版本的管理指南中的 "User Account Management"（用户帐户管理）一章。

注 – 以前，如果启用了 pam_ldap 帐户管理，所有用户在每次登录系统时都必须提供登录口令以进行验证。因此，使用 ssh 等工具的非基于口令的登录将失败。

在用户登录时，在不向目录服务器进行验证的情况下执行帐户管理并检索用户的帐户状态。目录服务器上的新控件是 1.3.6.1.4.1.42.2.27.9.5.8，它在缺省情况下是启用的。

要将此控制从缺省状态修改为其他状态，请在目录服务器上添加访问控制指令 (Access Control Instructions, ACI) :

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

绝不应当允许 proxy 用户的口令过期。如果代理口令过期，使用 proxy 凭证级别的客户机将无法从服务器检索命名服务信息。为了确保代理用户的口令不过期，请使用以下脚本修改代理帐户 :

```
# ldapmodify -h ldapserver -D administrator DN \
-w administrator password <<EOF
dn: proxy user DN
DNchangetype: modify
replace: passwordexpirationtime
passwordexpirationtime: 20380119031407Z
EOF
```

注 – pam_ldap 帐户管理依赖 Oracle Directory Server Enterprise Edition 为用户维护和提供口令生命期和帐户过期信息。目录服务器不对来自影子条目的对应数据进行解释以验证用户帐户。不过，pam_unix_* 模块会检查影子数据以确定帐户是否被锁定或口令是否已老化。因为影子数据未由 LDAP 命名服务或目录服务器保持为最新状态，所以这些模块不应当基于影子数据授予访问权限。影子数据是使用 proxy 标识检索的。因此，请不要允许 proxy 用户对 userPassword 属性具有读取访问权限。拒绝 proxy 用户对 userPassword 的读取访问权限可防止 PAM 服务进行无效的帐户验证。

对于使用 pam_unix_* 模块的客户机

要使 LDAP 客户机能够使用 pam_unix_* 模块进行帐户管理，必须对服务器进行设置以启用影子数据的更新。与 pam_ldap 帐户管理不同，pam_unix_* 模块不要求执行额外的配置步骤。所有配置都可以通过运行 idsconfig 实用程序来执行。对于基本的 idsconfig 运行，请参见示例 11–1。

下面显示了两个 idsconfig 运行的输出。

第一个 idsconfig 运行使用现有的客户机配置文件。

```
# /usr/lib/ldap/idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  sasl/GSSAPI is not supported by this LDAP server

Enter the profile name (h=help): [default] WestUserProfile

Profile 'WestUserProfile' already exists, it is possible to enable
shadow update now. idsconfig will exit after shadow update
is enabled. You can also continue to overwrite the profile
or create a new one and be given the chance to enable
shadow update later.


Just enable shadow update (y/n/h)? [n] y
Add the administrator identity (y/n/h)? [y]
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:
Re-enter passwd:
  ADDED: Administrator identity cn=admin,ou=profile,dc=west,dc=example,dc=com.
         Proxy ACI LDAP_Naming_Services_proxy_password_read does not
         exist for dc=west,dc=example,dc=com.
  ACI SET: Give cn=admin,ou=profile,dc=west,dc=example,dc=com read/write access
           to shadow data.
  ACI SET: Non-Admin access to shadow data denied.

  Shadow update has been enabled.
```

第二个 idsconfig 运行创建了新的配置文件供以后使用。这里显示的只是部分输出。

```
# /usr/lib/ldap/idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  sasl/GSSAPI is not supported by this LDAP server

Enter the profile name (h=help): [default] WestUserProfile-new
Default server list (h=help): [192.168.0.1]
.
.
.
Do you want to enable shadow update (y/n/h)? [n] y

              Summary of Configuration

  1  Domain to serve              : west.example.com
  2  Base DN to setup             : dc=west,dc=example,dc=com
        Suffix to create          : dc=west,dc=example,dc=com
  3  Profile name to create       : WestUserProfile-new
.
.
.
 19  Enable shadow update         : TRUE
.
.
.
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:
Re-enter passwd:


WARNING: About to start committing changes. (y=continue, n=EXIT) y

  1. Changed timelimit to -1 in cn=config.
  2. Changed sizelimit to -1 in cn=config.
.
.
.
  11. ACI for dc=test1,dc=mpklab,dc=sfbay,dc=sun,dc=com modified to
      disable self modify.
.
.
.
  15. Give cn=admin,ou=profile,dc=west,dc=example,dc=com write permission for shadow.
...
```

◆ ◆ ◆ 第 12 章

12 设置 LDAP 客户机（任务）

本章介绍了如何设置 LDAP 命名服务客户机。本章包含以下主题：

LDAP 客户机设置的先决条件

为了使 Oracle Solaris 客户机将 LDAP 用作命名服务，必须满足以下要求：

- 客户机的域名必须由 LDAP 服务器提供。
- 对于必需的服务，名称服务转换必须指向 LDAP。
- 必须为客户机配置定义其行为的所有给定参数。
- `ldap_cachemgr` 必须正在客户机上运行。
- 至少有一台要为其配置客户机的服务器已启动并正在运行。

`ldapclient` 实用程序可以执行上述除启动服务器之外的所有步骤，因此是设置 LDAP 客户机的关键。本章其余部分将举例说明如何使用 `ldapclient` 实用程序设置 LDAP 客户机，以及如何使用其他各种 LDAP 实用程序获取有关 LDAP 客户机的信息并检查其状态。

LDAP 和服务管理工具

LDAP 客户机服务可以使用服务管理工具进行管理 。有关 SMF 的概述，请参见《在 Oracle Solaris 11.1 中管理服务和故障》中的第 1 章 “管理服务（概述）”。有关更多详细信息，另请参阅 svcadm(1M) 和 svcs(1) 手册页。

以下列表简要概述了使用 SMF 服务管理 LDAP 客户机服务时所需的一些重要信息。

- 使用 svcadm 命令可以对 LDAP 客户机服务执行启用、禁用或重新启动等管理操作。

  提示 – 使用 -t 选项暂时禁用服务可为服务配置提供一些保护。如果禁用服务时使用了 -t 选项，则服务在重新引导后将恢复原始设置。如果禁用服务时未使用 -t，则服务在重新引导后仍将保持禁用状态。

- LDAP 客户机服务的故障管理资源标识符 (Fault Management Resource Identifier, FMRI) 是 svc:/network/ldap/client。
- 在配置过程中，还将启用 network/nis/domain 服务来提供由 network/ldap/client 服务使用的域名。
- 您可以使用 svcs 命令查询 LDAP 客户机和 ldap_cachemgr 守护进程的状态。
  - 下面是 svcs 命令及其输出的示例：

    ```
    # svcs \*ldap\*
    STATE          STIME     FMRI
    online         15:43:46  svc:/network/ldap/client:default
    ```

  - svcs -l 命令和输出示例。要获得如下所示的输出，必须在 FMRI 中使用实例名称。

    ```
    # svcs -l network/ldap/client:default
    fmri         svc:/network/ldap/client:default
    name         LDAP Name Service Client
    enabled      true
    state        online
    next_state   none
    restarter    svc:/system/svc/restarter:default
    manifest     /lib/svc/manifest/network/ldap/client.xml
    manifest     /lib/svc/manifest/network/network-location.xml
    manifest     /lib/svc/manifest/system/name-service/upgrade.xml
    manifest     /lib/svc/manifest/milestone/config.xml
    dependency   require_all/none svc:/system/filesystem/minimal (online)
    dependency   require_all/none svc:/network/initial (online)
    dependency   optional_all/none svc:/network/location:default (online)
    dependency   require_all/restart svc:/network/nis/domain (online)
    dependency   optional_all/none svc:/system/name-service/upgrade (online)
    dependency   optional_all/none svc:/milestone/config (online)
    dependency   optional_all/none svc:/system/manifest-import (online)
    dependency   require_all/none svc:/milestone/unconfig (online)
    ```

- 您可以使用下面的命令检查守护进程是否存在：
  - 在服务器上，使用 ptree 命令：

```
# ptree 'pgrep slapd'
6410 zsched
11565 /export/dsee/dsee6/ds6/lib/64/ns-slapd -D /export/dsee/test1 -i /export
```

- 在客户机上，使用以下命令：

```
# ldapsearch -h server-name -b "" -s base "objectclass=*" |grep -i context
namingContexts: dc=example,dc=com
```

初始化 LDAP 客户机

`ldapclient` 命令用于在 Oracle Solaris 系统上设置 LDAP 客户机。该命令假定已经为服务器配置了合适的客户机配置文件。您必须先安装服务器并用适当的配置文件对其进行配置，然后才能设置客户机。

注 – 因为 LDAP 和 NIS 使用在 `network/nis/domain` 服务中定义的同一域名组成部分，所以 Oracle Solaris OS 不支持 NIS 客户机和本机 LDAP 客户机共存于同一客户机系统上的配置。

使用 `ldapclient` 设置客户机主要有两种方法。

- **配置文件**

  您至少需要指定包含配置文件以及要使用的域的服务器地址。如果未指定配置文件，则会使用“缺省”的配置文件。服务器将提供其余的必需信息，但代理和证书数据库信息除外。如果客户机的凭证级别为 `proxy` 或 `proxy anonymous`，则必须提供代理的绑定 DN 和口令。有关更多信息，请参见第 129 页中的 “指定客户机凭证级别”。

  要启用影子数据更新，您必须提供管理凭证（`adminDN` 与 `adminPassword`）。

- **手动**

  在客户机上配置配置文件，这意味着要从命令行定义所有参数。这样，配置文件信息将存储在高速缓存文件中，服务器永远不会刷新这些信息。

注 – 在企业环境中，使用 LDAP 配置文件可以降低复杂性（如果该配置文件是在各台计算机之间共享的）。

▼ 如何使用配置文件初始化 LDAP 客户机

1 成为管理员。

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 运行带有 **init** 选项的 **ldapclient** 命令。

```
# ldapclient init -a profileName=new \
-a domainName=west.example.com 192.168.0.1
System successfully configured
```

▼ 如何使用每用户凭证初始化 LDAP 客户机

开始之前 使用每用户凭证设置 LDAP 客户机之前，必须已经配置以下各项：

- 必须已配置了一台或多台 Kerberos 密钥分发中心 (key distribution center, KDC) 服务器且这台（些）服务器正在运行。
- 必须已配置了 DNS、对 DNS 服务器的客户机访问以及至少一台 DNS 服务器，且它们正在运行。
- 客户机上的 Kerberos 必须已配置且已启用。
- 必须存在一个类似于以下内容的 Kerberos 客户机安装配置文件：

```
# cat /usr/tmp/krb5.profile
REALM EXAMPLE.COM
KDC kdc.example.com
ADMIN super/admin
FILEPATH /usr/tmp/krb5.conf
NFS 1
DNSLOOKUP none
```

- 必须安装并配置 LDAP 服务器来支持 `sasl/GSSAPI`。
- 必须存在适当的标识映射配置。
- 必须在 KDC 中设置了目录服务器和 KDC 的 Kerberos 主机主体。
- 必须已对要使用的目录服务器 DIT 运行 `idsconfig` 命令。
- 必须已创建适当的每用户 `gssapi` 配置文件（如 `gssapi_EXAMPLE.COM`）。

  `idsconfig` 命令中的每用户配置文件的说明如下面的部分示例所示：

```
# /usr/lib/ldap/idsconfig
Do you wish to continue with server setup (y/n/h)? [n] y
Enter the Directory Server's hostname to setup: kdc.example.com
Enter the port number for DSEE (h=help): [389] <Enter your port>
Enter the directory manager DN: [cn=Directory Manager] <Enter your DN>
Enter passwd for cn=Directory Manager : <Enter your password>
Enter the domainname to be served (h=help): [example.com] <Enter your domain>
Enter LDAP Base DN (h=help): [dc=example,dc=com] <Enter your DN>
GSSAPI is supported. Do you want to set up gssapi:(y/n) [n] y
Enter Kerberos Realm: [EXAMPLE.COM] EXAMPLE.COM
```

注 – 此外，对于 `gssapi` 配置文件，您必须提供 4 `self` 凭证级别和 6 `sasl/GSSAPI` 验证方法。

- KDC 中必须存在所需的用户主体。

- 在客户机上，必须使用含有诸如以下命令的客户机配置文件初始化 Kerberos：

```
# /usr/sbin/kclient -p /usr/tmp/krb5.profile
```

- 必须对名称服务转换进行配置以便为 `hosts` 使用 `dns`。以下命令检查当前的系统信息库值：

```
% svcprop -p config/host system/name-service/switch
files\ dns\ nis
```

- 必须已配置 DNS 且 DNS 服务必须正在运行。有关详细信息，请参见本文档中有关 DNS 的章节。
- 目录服务器 DIT 必须至少预装入此客户机的用户、客户机主机和必要的 `auto_home` LDAP 项。有关如何使用 `ldapaddent` 命令添加项的详细信息，请参见本手册的其他各节。

注 – 不要直接编辑任何一个客户机配置文件。请使用 `ldapclient` 命令创建或修改这些文件的内容。

---

1 使用 gssapi 配置文件运行 `ldapclient init` 来初始化客户机。

```
# /usr/sbin/ldapclient init -a profilename=gssapi_EXAMPLE.COM -a \
domainname=example.com 9.9.9.50
```

2 尝试以用户身份登录：

- **运行 `kinit -p` *user***
- **在用户的登录会话中运行 `ldaplist -l passwd` *user*，然后您应当看到 `userpassword`。**
- **运行 `ldaplist -l passwd bar` 可以获得不包含 `userpassword` 的项。缺省情况下，`root` 仍然可以看见每个人的 `userpassword`。**

更多信息 有关使用每用户凭证的注释

- 如果 `syslog` 文件包含以下消息：`libsldap: Status: 7 Mesg: openConnection: GSSAPI bind failed - 82 Local error`，这可能表示 Kerberos 未初始化或其票证已过期。运行 `klist` 命令来浏览该文件。例如，运行 `kinit -p foo` 或 `kinit -R -p foo` 并重试。
- 如果需要，可以将 `pam_krb5.so.1` 添加到 `/etc/pam.conf`，以便在您登录时它可以自动运行 `kinit` 命令。

  例如：

```
login   auth optional pam_krb5.so.1
rlogin  auth optional pam_krb5.so.1
other   auth optional pam_krb5.so.1
```

- 如果某个用户已运行了 `kinit` 命令并且 `syslog` 消息指示 `Invalid credential`，则问题可能是 `root` 主机条目或用户条目不在 LDAP 目录中或映射规则不正确。

- 执行 `ldapclient init` 命令时，它将检查 LDAP 配置文件是否包含一个 self/sasl/GSSAPI 配置。如果它在转换检查中失败，则常见的原因是 DNS 不是主机数据库的搜索条件。
  - 如果检查因为 DNS 客户机 id 未启用而失败，请运行 `svcs -l dns/client` 来确定服务是否被禁用。运行 `svcadm enable dns/client` 来启用服务。
  - 如果检查因为某个 sasl/GSSAPI 绑定而失败，请检查 `syslog` 来确定问题。

有关详细信息，请参见本指南和《Oracle Solaris 11.1 管理：安全服务》中的其他参考。

▼ 如何使用代理凭证初始化 LDAP 客户机

注 – 请勿直接编辑任何客户机配置文件。请使用 `ldapclient` 命令创建或修改这些文件的内容。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **定义代理值。**

```
# ldapclient init \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a domainName=west.example.com \
-a profileName=pit1 \
-a proxyPassword=test1234 192.168.0.1
System successfully configured
```

如果为 `proxy` 设置了要使用的配置文件，则 `-a proxyDN` 和 `-a proxyPassword` 是**必需的**。由于凭据并不是存储在服务器上保存的配置文件中，因此您必须在初始化客户机时提供该信息。与原先在服务器上存储代理凭证的方法相比，这种方法更安全。

代理信息存储在 `config` 和 `cred` 属性组中的 `svc:/network/ldap/client` 服务中。

▼ 如何初始化 LDAP 客户机以启用影子数据更新

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **要设置 enableShadowUpdate 开关并定义管理凭证，请运行 ldapclient 命令。**

- **要更新已在运行的 LDAP 客户机，请运行以下命令：**

```
# ldapclient mod -a enableShadowUpdate=TRUE \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
System successfully configured
```

- **要初始化某个 LDAP 客户机，请运行以下命令：**

```
# ldapclient init \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
-a domainName=west.example.com \
-a profileName=WestUserProfile \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a proxyPassword=<proxy_password> \
192.168.0.1
System successfully configured
```

3 **要验证配置，请显示 network/ldap/client 服务的 cred 属性的内容。**

输出内容类似如下：

```
# svcprop -p cred svc:/network/ldap/client
cred/read_authorization astring solaris.smf.value.name-service.ldap.client
cred/value_authorization astring solaris.smf.value.name-service.ldap.client
cred/bind_dn astring cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
cred/bind_passwd astring {NS1}4a3788f8eb85de11
cred/enable_shadow_update boolean true
cred/admin_bind_dn astring cn=admin,ou=profile,dc=west,dc=example,dc=com
cred/admin_bind_passwd astring {NS1}4a3788f8c053434f
```

▼ 如何手动初始化 LDAP 客户机

Root 用户或具有等效角色的管理员可以执行手动 LDAP 客户机配置。但是在手动配置期间，会跳过许多检查，因此系统配置相对容易出错。此外，您必须更改**每台计算机**上的设置，而不像使用配置文件时那样，只需在一个集中位置进行更改即可。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **初始化客户机。**

```
# ldapclient manual \
-a domainName=dc=west.example.com -a credentialLevel=proxy \
-a defaultSearchBase=dc=west,dc=example,dc=com \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a proxyPassword=testtest 192.168.0.1
```

3 **验证 LDAP 客户机配置。**

```
# ldapclient list
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
NS_LDAP_SERVERS= 192.168.0.1
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_CREDENTIAL_LEVEL= proxy
```

▼ 如何修改手动 LDAP 客户机配置

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **使用 `ldapclient mod` 命令将身份验证方法更改为 `simple`。**

```
# ldapclient mod -a authenticationMethod=simple
```

3 **验证是否已更改 LDAP 客户机配置。**

```
# ldapclient list
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
NS_LDAP_SERVERS= 192.168.0.1
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_AUTH= simple
NS_LDAP_CREDENTIAL_LEVEL= proxy
```

故障排除 您不能使用 `mod` 子命令更改 LDAP 客户机配置的某些属性。例如，您不能更改 `profileName` 和 `profileTTL` 属性。要更改这些属性，请使用 `ldapclient init` 命令创建一个新的配置文件，如第 167 页中的 “如何使用配置文件初始化 LDAP 客户机”中所述。或者运行 `ldapclient manual` 命令，如第 171 页中的 “如何手动初始化 LDAP 客户机”中所述。

▼ 如何取消初始化 LDAP 客户机

`ldapclient uninit` 命令可将客户机名称服务恢复到它在最近一次 `init`、`modify` 或 `manual` 操作之前的状态。换言之，该命令可对所采取的上一个步骤执行“撤消”操作。例如，如果客户机被配置为使用 `profile1`，然后更改为使用 `profile2`，则使用 `ldapclient uninit` 将使客户机恢复使用 `profile1`。

1 **成为管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 **取消初始化 LDAP 客户机。**

```
# ldapclient uninit
System successfully recovered
```

设置 TLS 安全性

注 – 安全数据库文件必须可供任何人读取。请勿在 key3.db 文件中包含任何私钥。

如果使用传输层安全 (transport layer security, TLS)，则必须安装必要的安全数据库。尤其要指出的是，证书和密钥数据库文件是必需的。例如，如果您使用来自 Mozilla Firefox 的较新的数据库格式，则 cert8.db、key3.db 和 secmod.db 这三个文件是必需的。cert8.db 文件包含受信任的证书。key3.db 文件中包含客户机的密钥。即使 LDAP 命名服务客户机不使用客户机密钥，此文件也必须存在。secmod.db 文件中包含安全模块，如 PKCS#11 模块。如果使用的是旧格式，则不需要此文件。

注 – 在运行 ldapclient 之前，应设置并安装本节中介绍的必需的安全数据库文件。

请参见您所使用的 Oracle Directory Server Enterprise Edition 版本的管理员指南中 "Managing SSL"（管理 SSL）一章中有关配置 LDAP 客户机以使用 SSL 的一节，了解如何创建和管理这些文件的信息。配置后，这些文件必须存储在 LDAP 命名服务客户机希望的位置。属性 certificatePath 用于确定此位置。缺省值为 /var/ldap。

例如，通过使用 Mozilla Firefox 设置所需的 cert8.db、key3.db 和 secmod.db 文件后，请按如下方式将文件复制到缺省位置：

```
# cp $HOME/.mozilla/firefox/*.default/cert8.db /var/ldap
# cp $HOME/.mozilla/firefox/*.default/key3.db /var/ldap
# cp $HOME/.mozilla/firefox/*.default/secmod.db /var/ldap
```

然后，向所有人授予读取访问权限。

```
# chmod 444 /var/ldap/cert8.db
# chmod 444 /var/ldap/key3.db
# chmod 444 /var/ldap/secmod.db
```

注 – Mozilla Firefox 在 $HOME/.mozilla 下的子目录中管理其 cert8.db、key3.db 和 secmod.db 文件。如果要将这些安全数据库用于 LDAP 命名服务客户机，必须将其副本存储在本地文件系统中。

配置 PAM

pam_ldap 模块是用于 LDAP 的一个验证和客户管理 PAM 模块选件。有关 pam_ldap 当前支持的功能的更多信息，请参见 pam_ldap(5) 手册页。

如果同时选择了每用户模式和 self 凭证选项，则还必须启用 PAM Kerberos pam_krb5 模块。有关更多详细信息，请参见 pam_krb5(5) 手册页和《Oracle Solaris 11.1 管理：安全服务》文档。

配置 PAM 以使用 UNIX policy

要将 PAM 配置为使用 UNIX policy，请使用缺省的 /etc/pam.conf 文件。不需要进行更改。有关详细信息，请参见 pam.conf(4) 手册页。

不过，如果由 shadow 数据控制的口令生命期和口令策略是必需的，则必须将客户机配置为在带有 enableShadowUpdate 开关的情况下运行。有关更多信息，请参见第 170 页中的 “如何初始化 LDAP 客户机以启用影子数据更新”。

配置 PAM 以使用 LDAP server_policy

要配置 PAM 以使用 LDAP server_policy，请遵照第 187 页中的 “使用 pam_ldap 模块进行帐户管理的示例 pam_conf 文件”中的样例。向客户机的 /etc/pam.conf 文件中添加包含 pam_ldap.so.1 的行。另外，如果样例 pam.conf 文件中有任何 PAM 模块指定了 binding 标志和 server_policy 选项，请在客户机的 /etc/pam.conf 文件中为对应模块使用相同的标志和选项。而且，还要将 server_policy 选项添加到包含服务模块 pam_authtok_store.so.1 的行中。

注 – 以前，如果启用了 pam_ldap 帐户管理，所有用户在每次登录系统时都必须提供登录口令以进行验证。因此，使用 ssh 等工具的非基于口令的登录将失败。

在用户登录时，在不向目录服务器进行验证的情况下执行帐户管理并检索用户的帐户状态。目录服务器上的新控件是 1.3.6.1.4.1.42.2.27.9.5.8，它在缺省情况下是启用的。

要将此控制从缺省状态修改为其他状态，请在目录服务器上添加访问控制指令 (Access Control Instructions, ACI) :

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

- binding 控制标志

  使用 binding 控制标志允许本地口令覆盖远程 (LDAP) 口令。例如，如果在本地文件和 LDAP 名称空间中都找到了某一用户帐户，则与本地帐户关联的口令将优先于远程口令。因此，如果本地口令过期，即使远程 LDAP 口令仍然有效，验证也将失败。

- server_policy 选项

  server_policy 选项指示 pam_unix_auth、pam_unix_account 和 pam_passwd_auth 忽略在 LDAP 名称空间中找到的用户，并允许 pam_ldap 执行身份验证或帐户验证。对于 pam_authtok_store，会向 LDAP 服务器传递一个未经加密的新口令。因此，该口令将根据服务器中配置的口令加密方案存储在目录中。有关更多信息，请参见 pam.conf(4) 和 pam_ldap(5)。

检索 LDAP 命名服务信息

您可以使用 ldaplist 实用程序检索关于 LDAP 命名服务的信息。此 LDAP 实用程序会以 LDIF 格式列出 LDAP 服务器中的命名信息。该实用程序可用于进行故障排除。有关详细信息，请参见 ldaplist(1)。

列出所有 LDAP 容器

ldaplist 显示输出时以空白行分隔记录，这对于显示包含多行的大量记录很有帮助。

注 – ldaplist 的输出取决于客户机配置。例如，如果 ns_ldap_search 的值是 sub 而不是 one，则 ldaplist 将列出在当前搜索 baseDN 下的所有项。

下面是 ldaplist 输出的示例。

```
# ldaplist
dn: ou=people,dc=west,dc=example,dc=com

dn: ou=group,dc=west,dc=example,dc=com

dn: ou=rpc,dc=west,dc=example,dc=com

dn: ou=protocols,dc=west,dc=example,dc=com

dn: ou=networks,dc=west,dc=example,dc=com

dn: ou=netgroup,dc=west,dc=example,dc=com

dn: ou=aliases,dc=west,dc=example,dc=com

dn: ou=hosts,dc=west,dc=example,dc=com

dn: ou=services,dc=west,dc=example,dc=com

dn: ou=ethers,dc=west,dc=example,dc=com

dn: ou=profile,dc=west,dc=example,dc=com

dn: automountmap=auto_home,dc=west,dc=example,dc=com

dn: automountmap=auto_direct,dc=west,dc=example,dc=com

dn: automountmap=auto_master,dc=west,dc=example,dc=com

dn: automountmap=auto_shared,dc=west,dc=example,dc=com
```

列出所有用户项属性

要列出特定信息（如用户的 passwd 项），请按如下所示使用 getent：

```
# getent passwd user1
user1::30641:10:Joe Q. User:/home/user1:/bin/csh
```

如果要列出所有属性，请将 ldaplist 与 -l 选项结合使用。

```
# ldaplist -l passwd user1
        dn: uid=user1,ou=People,dc=west,dc=example,dc=com
        uid: user1
        cn: user1
        uidNumber: 30641
        gidNumber: 10
```

```
gecos: Joe Q. User
homeDirectory: /home/user1
loginShell: /bin/csh
objectClass: top
objectClass: shadowAccount
objectClass: account
objectClass: posixAccount
shadowLastChange: 6445
```

定制 LDAP 客户机环境

以下各节介绍了如何定制 LDAP 客户机环境。

您可以更改任何服务，但一定要小心，因为如果未在服务器上为指定的服务置备数据，服务会停止工作。而且，在某些情况下，可能不会按缺省情况设置文件。

为 LDAP 修改名称服务转换

您可以修改名称服务转换以定制每个命名服务从何处访问其信息。请参见第 36 页中的 “管理名称服务转换”。

为 LDAP 启用 DNS

如果要启用 DNS，请参见第 44 页中的 “如何启用 DHCP 客户机”。如果使用的是每用户验证模式，则 sasl/GSSAPI 和 Kerberos 机制要求配置并启用 DNS 命名服务。

◆ ◆ ◆ 第 13 章

13 LDAP 故障排除（参考信息）

本章介绍了 LDAP 配置问题以及用于解决这些问题的建议解决方案。

监视 LDAP 客户机状态

以下各节介绍了各种可帮助确定 LDAP 客户机环境状态的命令。有关可以使用的选项的其他信息，另请参见相应的手册页。

有关服务管理工具 (Service Management Facility, SMF) 的概述，请参阅《在 Oracle Solaris 11.1 中管理服务和故障》中的第 1 章 “管理服务（概述）”。有关更多详细信息，另请参阅 svcadm(1M) 和 svcs(1) 手册页。

验证 ldap_cachemgr 守护进程是否正在运行

ldap_cachemgr 守护进程必须一直正常运行。否则，系统将无法正常工作。当您设置并启动 LDAP 客户机服务 svc:/network/ldap/client 时，客户机 SMF 方法会自动启动 ldap_cachemgr 守护进程。以下方法确定 LDAP 客户机服务是否已联机：

- 使用以下 svcs 命令查看该服务是否已启用。

```
# svcs \*ldap\*
STATE          STIME    FMRI
disabled       Aug_24   svc:/network/ldap/client:default
```

- 使用以下命令查看有关该服务的所有信息。

```
# svcs -l network/ldap/client:default
fmri svc:/network/ldap/client:default
name LDAP Name Service Client
enabled false
state disabled
next_state none
state_time Thu Oct 20 23:04:11 2011
logfile /var/svc/log/network-ldap-client:default.log
```

```
restarter svc:/system/svc/restarter:default
contract_id
manifest /lib/svc/manifest/network/ldap/client.xml
manifest /lib/svc/manifest/milestone/config.xml
manifest /lib/svc/manifest/network/network-location.xml
manifest /lib/svc/manifest/system/name-service/upgrade.xml
dependency optional_all/none svc:/milestone/config (online)
dependency optional_all/none svc:/network/location:default (online)
dependency require_all/none svc:/system/filesystem/minimal (online)
dependency require_all/none svc:/network/initial (online)
dependency require_all/restart svc:/network/nis/domain (online)
dependency optional_all/none svc:/system/manifest-import (online)
dependency require_all/none svc:/milestone/unconfig (online)
dependency optional_all/none svc:/system/name-service/upgrade (online)
```

- 将 `-g` 选项传递给 `ldap_cachemgr`。

  此选项提供更广泛的状态信息，这些信息对于问题的诊断很有帮助。

```
# /usr/lib/ldap/ldap_cachemgr -g
cachemgr configuration:
server debug level          0
server log file "/var/ldap/cachemgr.log"
number of calls to ldapcachemgr         19

cachemgr cache data statistics:
Configuration refresh information:
  Previous refresh time: 2010/11/16 18:33:28
  Next refresh time:     2010/11/16 18:43:28
Server information:
  Previous refresh time: 2010/11/16 18:33:28
  Next refresh time:     2010/11/16 18:36:08
  server: 192.168.0.0, status: UP
  server: 192.168.0.1, status: ERROR
    error message: Can't connect to the LDAP server
Cache data information:
  Maximum cache entries:          256
  Number of cache entries:          2
```

有关 `ldap_cachemgr` 守护进程的更多信息，请参见 `ldap_cachemgr(1M)` 手册页。

检查当前的配置文件信息

成为超级用户或承担等效角色，然后运行带 `list` 选项的 `ldapclient`。

```
# ldapclient list
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
NS_LDAP_SERVERS= 192.168.0.1, 192.168.0.10
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_AUTH= simple
NS_LDAP_SEARCH_REF= TRUE
NS_LDAP_SEARCH_SCOPE= one
NS_LDAP_SEARCH_TIME= 30
NS_LDAP_SERVER_PREF= 192.168.0.1
```

```
NS_LDAP_PROFILE= pit1
NS_LDAP_CREDENTIAL_LEVEL= proxy
NS_LDAP_SERVICE_SEARCH_DESC= passwd:ou=people,?sub
NS_LDAP_SERVICE_SEARCH_DESC= group:ou=group,dc=west,dc=example,dc=com?one
NS_LDAP_BIND_TIME= 5
```

可以使用 `svccfg` 或 `svcprop` 命令或者带 `list` 选项的 `ldapclient` 命令查看当前配置文件信息。有关每个可用属性设置的具体信息，请参见 `ldapclient(1M)` 手册页。

验证基本的客户机/服务器通信

检查客户机是否正在与 LDAP 服务器通信的最佳方法是使用 `ldaplist` 命令。使用不带任何参数的 `ldaplist` 会转储服务器上的所有容器。只要这些容器存在且不必置备，此方法就起作用。有关更多信息，请参见 `ldaplist(1)` 手册页。

如果第一步起作用，您可以尝试使用 `ldaplist passwd` *username* 或 `ldaplist hosts` *hostname*，但是如果容器中包含大量数据，您可能需要选取一个置备量较小的服务，或者将它们传输到 `head` 或 `more`。

从非客户机检查服务器数据

前面几节中的大多数命令都假定您已创建了一个 LDAP 客户机。如果您尚未创建客户机，但仍然希望检查服务器上的数据，请使用 `ldapsearch` 命令。以下示例列出了所有容器。

```
# ldapsearch -h server1 -b "dc=west,dc=example,dc=com" -s one "objectclass=*"
```

`ldapsearch` 命令的缺省输出采用行业标准化的 LDIF 格式，该格式由 RFC-2849 定义。所有版本的 `ldapsearch` 都可以使用 `-L` 选项输出 LDIF 格式。

LDAP 配置问题及解决方案

以下各节描述了 LDAP 的配置问题以及建议的解决方案。

未解析的主机名

LDAP 客户机后端针对主机查找返回全限定的主机名，例如由 `gethostbyname()` 和 `getaddrinfo()` 返回的主机名。如果存储的名称是限定名称（即至少包含一个点），则客户机将按原样返回该名称。例如，如果存储的名称是 `hostB.eng`，则返回的名称是 `hostB.eng`。

如果 LDAP 目录中存储的名称不是限定名称（即不包含点），则客户机后端会在该名称后面附加域名部分。例如，如果存储的名称是 `hostA`，则返回的名称是 `hostA.domainname`。

无法远程访问 LDAP 域中的系统

如果 DNS 域名不同于 LDAP 域名，除非所存储的主机名是全限定名称，否则 LDAP 命名服务不能用于提供主机名。

登录功能不起作用

在登录期间，LDAP 客户机使用 PAM 模块进行用户验证。在使用标准的 UNIX PAM 模块时，口令是从服务器读取并在客户机端检查的。该过程可能会因下列原因之一而失败：

1. `ldap` 没有与名称服务转换中的 `passwd` 数据库相关联。
2. 代理无法读取服务器列表中用户的 `userPassword` 属性。您需要至少允许一个代理可以读取口令，因为该代理需要将口令返回给客户机进行比较。`pam_ldap` 不需要对口令具有读取访问权限。
3. 代理可能没有正确的口令。
4. 该项没有 `shadowAccount` 对象类。
5. 没有为该用户定义口令。

   在使用 `ldapaddent` 时，必须使用 `-p` 选项确保已向该用户项中添加了口令。如果您使用不带 `-p` 选项的 `ldapaddent`，用户的口令将不存储在目录中，除非使用 `ldapaddent` 另外添加了 `/etc/shadow` 文件。
6. 没有可访问的 LDAP 服务器。

   检查服务器的状态。

   ```
   # /usr/lib/ldap/ldap_cachemgr -g
   ```
7. `pam.conf` 的配置有误。
8. 没有在 LDAP 名称空间中定义该用户。
9. 为 `pam_unix_*` 模块将 `NS_LDAP_CREDENTIAL_LEVEL` 设置为了 `anonymous`，且 `userPassword` 对匿名用户不可用。
10. 口令没有以 `crypt` 格式存储。
11. 如果所配置的 `pam_ldap` 支持帐户管理，则登录失败可能是由以下某种原因引起的：
    - 用户的口令已过期。
    - 用户的帐户由于登录失败尝试的次数过多而被锁定。
    - 用户的帐户已被管理员停用。
    - 用户试图使用非基于口令的程序（例如 `ssh` 或 `sftp`）进行登录。
12. 如果使用了每用户验证方式和 sasl/GSSAPI，则 Kerberos 的某个组件或 `pam_krb5` 配置的设置有误。有关解决这些问题的详细信息，请参阅《Oracle Solaris 11.1 管理：安全服务》。

查找速度太慢

LDAP 数据库依赖索引来改进搜索性能。如果索引的配置有误，会大大降低性能。本文档中包括一组应当编制索引的常见属性。您也可以添加自己的索引来提高站点的性能。

ldapclient 命令无法绑定到服务器

在指定了 profileName 属性的情况下使用 init 选项时，ldapclient 命令未能初始化客户机。失败的可能原因包括：

1. 命令行上指定的域名有误。
2. 没有在 DIT 中设置 nisDomain 属性，该属性表示指定客户机域的入口点。
3. 未在服务器上正确设置访问控制信息，从而无法在 LDAP 数据库中进行匿名搜索。
4. 向 ldapclient 命令传递了错误的服务器地址。请使用 ldapsearch 命令验证服务器地址。
5. 向 ldapclient 命令传递了错误的配置文件名称。请使用 ldapsearch 命令验证 DIT 中的配置文件名称。
6. 对客户机网络接口使用 snoop，看传出的是哪种通信，并确定哪台服务器正与之通信。

使用 ldap_cachemgr 守护进程进行调试

在使用 -g 选项的情况下运行 ldap_cachemgr 守护进程可能是一个非常有用的调试方法，因为您可以查看当前客户机配置和统计信息。例如，

```
# ldap_cachemgr -g
```

将按上面提到的那样，在标准输出中列显当前的配置和统计信息（包括所有 LDAP 服务器的状态）。请注意，**不必**成为超级用户即可执行此命令。

ldapclient 命令在设置期间挂起

如果 ldapclient 命令挂起，则在恢复先前的环境之后按 Ctrl-C 将退出。如果出现这种情况，请与服务器管理员核对，以确保该服务器正在运行。

还要在配置文件中或从命令行检查服务器列表中的属性，并确保服务器信息正确无误。

◆ ◆ ◆ 第 14 章

LDAP 命名服务（参考信息）

本章包含以下主题：

用于配置 LDAP 的空核对表

表 14–1 用于服务器变量定义的空核对表

变量	针对 _____ 网络的定义
安装目录服务器实例的端口号 (389)	
服务器名称	
副本服务器（IP 号:端口号）	
目录管理器 [dn: cn=directory manager]	
要为其提供服务的域名	
在超时之前处理客户端请求的最长时间（以秒为单位）	
为每个搜索请求返回的最多项数	

表 14–2 用于客户机配置文件变量定义的空核对表

变量	针对 _____ 网络的定义
配置文件名称	
服务器列表（缺省值为本地子网）	
首选服务器列表（按照对服务器进行查找的顺序列出）	
搜索范围（沿着目录树向下查找的层数。'One' 或 'Sub'）	
用于获取服务器访问权限的凭证。缺省值为 anonymous。	
是否遵循引用？（主服务器不可用时指向另一台服务器的指针）缺省值为 no。	
等待服务器返回信息的搜索时间限制（以秒为单位）。缺省值为 30 秒。	
与服务器进行联系时的绑定时间限制（以秒为单位）。缺省值为 30 秒。	
验证方法（缺省值为 none）。	

LDAP 命令

Oracle Solaris 系统中有两组与 LDAP 相关的命令。一组命令是常规 LDAP 工具，它们不要求用 LDAP 命名服务配置客户机。另一组使用客户机上的通用 LDAP 配置并可以在配置有或者未配置有 LDAP 命名服务的客户机上运行。

常规 LDAP 工具

LDAP 命令行工具支持一组通用选项（包括验证和绑定参数）。下列工具支持以通用的文本格式来表示目录信息，这种格式称为 LDAP 数据交换格式 (LDAP Data Interchange Format, LDIF)。您可以使用这些命令直接处理目录项。

ldapsearch(1)
ldapmodify(1)
ldapadd(1)
ldapdelete(1)

需要 LDAP 命名服务的 LDAP 工具

表 14–3 LDAP 工具

工具	功能
ldapaddent(1M)	用于根据对应的 /etc 文件在 LDAP 容器中创建项。此工具允许根据文件置备目录。例如，它读取 /etc/passwd 格式的文件，并置备目录中的 passwd 项。
ldaplist(1)	用于列出目录中各个服务的内容。
idsconfig(1M)	用于设置 Oracle Directory Server Enterprise Edition，使其为 LDAP 命名服务客户机提供服务。

使用 pam_ldap 模块进行帐户管理的示例 pam_conf 文件

注 – 以前，如果启用了 pam_ldap 帐户管理，所有用户在每次登录系统时都必须提供登录口令以进行验证。因此，使用 ssh 等工具的非基于口令的登录将失败。

在用户登录时，在不向目录服务器进行验证的情况下执行帐户管理并检索用户的帐户状态。目录服务器上的新控件是 1.3.6.1.4.1.42.2.27.9.5.8，它在缺省情况下是启用的。

要将此控制从缺省状态修改为其他状态，请在目录服务器上添加访问控制指令 (Access Control Instructions, ACI)：

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

```
#
# Authentication management
#
# login service (explicit because of pam_dial_auth)
#
login   auth requisite          pam_authtok_get.so.1
login   auth required           pam_dhkeys.so.1
login   auth required           pam_unix_cred.so.1
login   auth required           pam_dial_auth.so.1
login   auth binding            pam_unix_auth.so.1 server_policy
```

```
login   auth required         pam_ldap.so.1
#
# rlogin service (explicit because of pam_rhost_auth)
#
rlogin  auth sufficient       pam_rhosts_auth.so.1
rlogin  auth requisite        pam_authtok_get.so.1
rlogin  auth required         pam_dhkeys.so.1
rlogin  auth required         pam_unix_cred.so.1
rlogin  auth binding          pam_unix_auth.so.1 server_policy
rlogin  auth required         pam_ldap.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh     auth sufficient       pam_rhosts_auth.so.1
rsh     auth required         pam_unix_cred.so.1
rsh     auth binding          pam_unix_auth.so.1 server_policy
rsh     auth required         pam_ldap.so.1
#
# PPP service (explicit because of pam_dial_auth)
#
ppp     auth requisite        pam_authtok_get.so.1
ppp     auth required         pam_dhkeys.so.1
ppp     auth required         pam_dial_auth.so.1
ppp     auth binding          pam_unix_auth.so.1 server_policy
ppp     auth required         pam_ldap.so.1
#
# Default definitions for Authentication management
# Used when service name is not explicitly mentioned for authentication
#
other   auth requisite        pam_authtok_get.so.1
other   auth required         pam_dhkeys.so.1
other   auth required         pam_unix_cred.so.1
other   auth binding          pam_unix_auth.so.1 server_policy
other   auth required         pam_ldap.so.1
#
# passwd command (explicit because of a different authentication module)
#
passwd  auth binding          pam_passwd_auth.so.1 server_policy
passwd  auth required         pam_ldap.so.1
#
# cron service (explicit because of non-usage of pam_roles.so.1)
#
cron    account required      pam_unix_account.so.1
#
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other   account requisite     pam_roles.so.1
other   account binding       pam_unix_account.so.1 server_policy
other   account required      pam_ldap.so.1
#
# Default definition for Session management
# Used when service name is not explicitly mentioned for session management
#
other   session required      pam_unix_session.so.1
#
# Default definition for  Password management
# Used when service name is not explicitly mentioned for password management
```

```
#
other   password required     pam_dhkeys.so.1
other   password requisite    pam_authtok_get.so.1
other   password requisite    pam_authtok_check.so.1
other   password required     pam_authtok_store.so.1 server_policy
#
# Support for Kerberos V5 authentication and example configurations can
# be found in the pam_krb5(5) man page under the "EXAMPLES" section.
#
```

LDAP 的 IETF 架构

架构是一些定义，用于描述哪些类型的信息可作为条目存储在服务器的目录中。

要使目录服务器支持 LDAP 命名客户机，必须在服务器中配置本章中定义的架构，除非使用客户机的架构映射功能对架构进行映射。

IETF 定义了几种必需的 LDAP 架构：RFC 2307 网络信息服务架构和 RFC 2307bis、一个用于基于轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP) 的代理的配置文件架构 (RFC 4876) 以及用于打印机服务的 LDAP 架构。要支持 NIS，必须将这些架构的定义添加到目录服务器中。可以从 IETF Web 站点 `http://www.ietf.org` 访问各种 RFC。

注 – Internet 草稿（例如 RFC 2307bis）是有效期最长为六个月的草稿文档，随时可能会被更新或废弃，从而被其他文档取代。

RFC 2307bis 网络信息服务架构

必须对 LDAP 服务器进行配置以支持修订的 RFC 2307bis：

`nisSchema` OID 是 `1.3.6.1.1`。RFC 2307bis 属性如下所示。

```
( nisSchema.1.0 NAME 'uidNumber'
DESC 'An integer uniquely identifying a user in an
        administrative domain'
EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.1 NAME 'gidNumber'
DESC 'An integer uniquely identifying a group in an
        administrative domain'
EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.2 NAME 'gecos'
DESC 'The GECOS field; the common name'
EQUALITY caseIgnoreIA5Match
SUBSTRINGS caseIgnoreIA5SubstringsMatch
SYNTAX 'IA5String' SINGLE-VALUE )
```

```
( nisSchema.1.3 NAME 'homeDirectory'
DESC 'The absolute path to the home directory'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' SINGLE-VALUE )

( nisSchema.1.4 NAME 'loginShell'
DESC 'The path to the login shell'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' SINGLE-VALUE )

( nisSchema.1.5 NAME 'shadowLastChange'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.6 NAME 'shadowMin'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.7 NAME 'shadowMax'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.8 NAME 'shadowWarning'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.9 NAME 'shadowInactive'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.10 NAME 'shadowExpire'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.11 NAME 'shadowFlag'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.12 NAME 'memberUid'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String' )

( nisSchema.1.13 NAME 'memberNisNetgroup'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String' )

( nisSchema.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 'nisNetgroupTripleSyntax' )

( nisSchema.1.15 NAME 'ipServicePort'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.16 NAME 'ipServiceProtocol'
SUP name )
```

```
( nisSchema.1.17 NAME 'ipProtocolNumber'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.18 NAME 'oncRpcNumber'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.19 NAME 'ipHostNumber'
DESC 'IP address as a dotted decimal, eg. 192.168.1.1
        omitting leading zeros'
SUP name )

( nisSchema.1.20 NAME 'ipNetworkNumber'
DESC 'IP network as a dotted decimal, eg. 192.168,
        omitting leading zeros'
SUP name SINGLE-VALUE )

( nisSchema.1.21 NAME 'ipNetmaskNumber'
DESC 'IP netmask as a dotted decimal, eg. 255.255.255.0,
         omitting leading zeros'
EQUALITY caseIgnoreIA5Match
SYNTAX 'IA5String{128}' SINGLE-VALUE )

( nisSchema.1.22 NAME 'macAddress'
DESC 'MAC address in maximal, colon separated hex
      notation, eg. 00:00:92:90:ee:e2'
EQUALITY caseIgnoreIA5Match
SYNTAX 'IA5String{128}' )

( nisSchema.1.23 NAME 'bootParameter'
DESC 'rpc.bootparamd parameter'
SYNTAX 'bootParameterSyntax' )

( nisSchema.1.24 NAME 'bootFile'
DESC 'Boot image name'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' )

( nisSchema.1.26 NAME 'nisMapName'
SUP name )

( nisSchema.1.27 NAME 'nisMapEntry'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String{1024}' SINGLE-VALUE )

( nisSchema.1.28 NAME 'nisPublicKey'
DESC 'NIS public key'
SYNTAX 'nisPublicKeySyntax' )

( nisSchema.1.29 NAME 'nisSecretKey'
DESC 'NIS secret key'
SYNTAX 'nisSecretKeySyntax' )

( nisSchema.1.30 NAME 'nisDomain'
DESC 'NIS domain'
SYNTAX 'IA5String' )
```

```
( nisSchema.1.31 NAME 'automountMapName'
DESC 'automount Map Name'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

( nisSchema.1.32 NAME 'automountKey'
DESC 'Automount Key value'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

( nisSchema.1.33 NAME 'automountInformation'
DESC 'Automount information'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

nisSchema OID 是 1.3.6.1.1。RFC 2307 objectClasses 如下所示。

```
( nisSchema.2.0 NAME 'posixAccount' SUP top AUXILIARY
  DESC 'Abstraction of an account with POSIX attributes'
  MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
  MAY ( userPassword $ loginShell $ gecos $ description ) )

( nisSchema.2.1 NAME 'shadowAccount' SUP top AUXILIARY
  DESC 'Additional attributes for shadow passwords'
  MUST uid
  MAY ( userPassword $ shadowLastChange $ shadowMin
        shadowMax $ shadowWarning $ shadowInactive $
        shadowExpire $ shadowFlag $ description ) )

( nisSchema.2.2 NAME 'posixGroup' SUP top STRUCTURAL
  DESC 'Abstraction of a group of accounts'
  MUST ( cn $ gidNumber )
  MAY ( userPassword $ memberUid $ description ) )

( nisSchema.2.3 NAME 'ipService' SUP top STRUCTURAL
  DESC 'Abstraction an Internet Protocol service.
        Maps an IP port and protocol (such as tcp or udp)
        to one or more names; the distinguished value of
        the cn attribute denotes the service's canonical
        name'
  MUST ( cn $ ipServicePort $ ipServiceProtocol )
  MAY ( description ) )

( nisSchema.2.4 NAME 'ipProtocol' SUP top STRUCTURAL
  DESC 'Abstraction of an IP protocol. Maps a protocol number
        to one or more names. The distinguished value of the cn
        attribute denotes the protocol's canonical name'
  MUST ( cn $ ipProtocolNumber )
  MAY  description )

( nisSchema.2.5 NAME 'oncRpc' SUP top STRUCTURAL
  DESC 'Abstraction of an Open Network Computing (ONC)
        [RFC1057] Remote Procedure Call (RPC) binding.
        This class maps an ONC RPC number to a name.
        The distinguished value of the cn attribute denotes
```

```
        the RPC service's canonical name'
  MUST ( cn $ oncRpcNumber $ description )
  MAY  description )

( nisSchema.2.6 NAME 'ipHost' SUP top AUXILIARY
  DESC 'Abstraction of a host, an IP device. The distinguished
        value of the cn attribute denotes the host's canonical
        name. Device SHOULD be used as a structural class'
  MUST ( cn $ ipHostNumber )
  MAY ( l $ description $ manager $ userPassword ) )

( nisSchema.2.7 NAME 'ipNetwork' SUP top STRUCTURAL
  DESC 'Abstraction of a network. The distinguished value of
        the cn attribute denotes the network's canonical name'
  MUST ipNetworkNumber
  MAY ( cn $ ipNetmaskNumber $ l $ description $ manager ) )

( nisSchema.2.8 NAME 'nisNetgroup' SUP top STRUCTURAL
  DESC 'Abstraction of a netgroup. May refer to other netgroups'
  MUST cn
  MAY ( nisNetgroupTriple $ memberNisNetgroup $ description ) )

( nisSchema.2.9 NAME 'nisMap' SUP top STRUCTURAL
  DESC 'A generic abstraction of a NIS map'
  MUST nisMapName
  MAY description )

( nisSchema.2.10 NAME 'nisObject' SUP top STRUCTURAL
  DESC 'An entry in a NIS map'
  MUST ( cn $ nisMapEntry $ nisMapName )
  MAY description )

( nisSchema.2.11 NAME 'ieee802Device' SUP top AUXILIARY
  DESC 'A device with a MAC address; device SHOULD be
        used as a structural class'
  MAY macAddress )

( nisSchema.2.12 NAME 'bootableDevice' SUP top AUXILIARY
  DESC 'A device with boot parameters; device SHOULD be
  used as a structural class'
  MAY ( bootFile $ bootParameter ) )

( nisSchema.2.14 NAME 'nisKeyObject' SUP top AUXILIARY
  DESC 'An object with a public and secret key'
  MUST ( cn $ nisPublicKey $ nisSecretKey )
  MAY ( uidNumber $ description ) )

( nisSchema.2.15 NAME 'nisDomainObject' SUP top AUXILIARY
  DESC 'Associates a NIS domain with a naming context'
  MUST nisDomain )

( nisSchema.2.16 NAME 'automountMap' SUP top STRUCTURAL
  MUST ( automountMapName )
  MAY description )

( nisSchema.2.17 NAME 'automount' SUP top STRUCTURAL
  DESC 'Automount information'
  MUST ( automountKey $ automountInformation )
  MAY description )
```

```
( nisSchema.2.18 NAME 'groupOfMembers' SUP top STRUCTURAL
  DESC 'A group with members (DNs)'
  MUST cn
  MAY ( businessCategory $ seeAlso $ owner $ ou $ o $
        description $ member ) )
```

邮件别名架构

邮件别名信息使用此 Internet 草稿定义的架构。除非有新的架构可用，否则 LDAP 客户机将继续为邮件别名信息使用此架构。

原来的 LDAP 邮件组架构中包含大量属性和对象类。LDAP 客户机只使用两个属性和一个对象类。这些属性和对象类如下所示。

邮件别名属性如下所示。

```
( 0.9.2342.19200300.100.1.3
  NAME 'mail'
  DESC 'RFC822 email address for this person'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String(256)'
  SINGLE-VALUE )

( 2.16.840.1.113730.3.1.30
  NAME 'mgrpRFC822MailMember'
  DESC 'RFC822 mail address of email only member of group'
  EQUALITY CaseIgnoreIA5Match
  SYNTAX 'IA5String(256)' )
```

`mailGroup` 对象类的架构如下所示。

```
( 2.16.840.1.113730.3.2.4
  NAME 'mailGroup'
  SUP top
  STRUCTURAL
  MUST mail
  MAY ( cn $ mailAlternateAddress $ mailHost $ mailRequireAuth $
   mgrpAddHeader $ mgrpAllowedBroadcaster $ mgrpAllowedDomain $
   mgrpApprovePassword $ mgrpBroadcasterModeration $ mgrpDeliverTo $
   mgrpErrorsTo $ mgrpModerator $ mgrpMsgMaxSize $
   mgrpMsgRejectAction $ mgrpMsgRejectText $ mgrpNoMatchAddrs $
   mgrpRemoveHeader $ mgrpRFC822MailMember ))
```

目录用户代理配置文件 (DUAProfile) 架构

DUAConfSchemaOID 为 1.3.6.1.4.1.11.1.3.1。

```
DESC 'Default LDAP server host address used by a DUA'
            EQUALITY caseIgnoreMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.0 NAME 'defaultServerList'
            DESC 'Default LDAP server host address used by a DUAList'
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.1 NAME 'defaultSearchBase'
            DESC 'Default LDAP base DN used by a DUA'
            EQUALITY distinguishedNameMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.2 NAME 'preferredServerList'
            DESC 'Preferred LDAP server host addresses to be used by a
            DUA'
            EQUALITY caseIgnoreMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.3 NAME 'searchTimeLimit'
            DESC 'Maximum time in seconds a DUA should allow for a
            search to complete'
            EQUALITY integerMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.4 NAME 'bindTimeLimit'
            DESC 'Maximum time in seconds a DUA should allow for the
            bind operation to complete'
            EQUALITY integerMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.5 NAME 'followReferrals'
            DESC 'Tells DUA if it should follow referrals
            returned by a DSA search result'
            EQUALITY caseIgnoreIA5Match
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.6 NAME 'authenticationMethod'
            DESC 'A keystring which identifies the type of
            authentication method used to contact the DSA'
            EQUALITY caseIgnoreMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.7 NAME 'profileTTL'
            DESC 'Time to live before a client DUA
```

```
  should re-read this configuration profile'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )

( DUAConfSchemaOID.1.9 NAME 'attributeMap'
  DESC 'Attribute mappings used by a DUA'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUAConfSchemaOID.1.10 NAME 'credentialLevel'
  DESC 'Identifies type of credentials a DUA should
  use when binding to the LDAP server'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE )

( DUAConfSchemaOID.1.11 NAME 'objectclassMap'
  DESC 'Objectclass mappings used by a DUA'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUAConfSchemaOID.1.12 NAME 'defaultSearchScope'
  DESC 'Default search scope used by a DUA'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.13 NAME 'serviceCredentialLevel'
  DESC 'Identifies type of credentials a DUA
  should use when binding to the LDAP server for a
  specific service'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUAConfSchemaOID.1.14 NAME 'serviceSearchDescriptor'
  DESC 'LDAP search descriptor list used by Naming-DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( DUAConfSchemaOID.1.15 NAME 'serviceAuthenticationMethod'
  DESC 'Authentication Method used by a service of the DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

    ( DUAConfSchemaOID.2.4 NAME 'DUAConfigProfile'
        SUP top STRUCTURAL
       DESC 'Abstraction of a base configuration for a DUA'
       MUST ( cn )
       MAY ( defaultServerList $ preferredServerList $
      defaultSearchBase $ defaultSearchScope $
      searchTimeLimit $ bindTimeLimit $
      credentialLevel $ authenticationMethod $
      followReferrals $ serviceSearchDescriptor $
      serviceCredentialLevel $ serviceAuthenticationMethod $
      objectclassMap $ attributeMap $
      profileTTL ) )
```

Oracle Solaris 架构

Oracle Solaris 平台所需的架构如下所示。

- 项目架构
- 基于角色的访问控制和执行配置文件架构
- 打印机架构

项目架构

/etc/project 文件是与项目关联的属性的本地源。有关更多信息，请参见 user_attr(4) 手册页。

项目属性如下所示。

```
( 1.3.6.1.4.1.42.2.27.5.1.1 NAME 'SolarisProjectID'
  DESC 'Unique ID for a Solaris Project entry'
  EQUALITY integerMatch
  SYNTAX INTEGER SINGLE )

( 1.3.6.1.4.1.42.2.27.5.1.2 NAME 'SolarisProjectName'
  DESC 'Name of a Solaris Project entry'
  EQUALITY caseExactIA5Match
  SYNTAX IA5String SINGLE )

( 1.3.6.1.4.1.42.2.27.5.1.3 NAME 'SolarisProjectAttr'
  DESC 'Attributes of a Solaris Project entry'
  EQUALITY caseExactIA5Match
  SYNTAX IA5String )

( 1.3.6.1.4.1.42.2.27.5.1.30 NAME 'memberGid'
  DESC 'Posix Group Name'
  EQUALITY caseExactIA5Match
  SYNTAX 'IA5String' )
```

项目 objectClass 如下所示。

```
( 1.3.6.1.4.1.42.2.27.5.2.1 NAME 'SolarisProject'
  SUP top STRUCTURAL
  MUST ( SolarisProjectID $ SolarisProjectName )
  MAY ( memberUid $ memberGid $ description $ SolarisProjectAttr ) )
```

基于角色的访问控制和执行配置文件架构

/etc/user_attr 文件是与用户和角色关联的扩展属性的本地源。有关更多信息，请参见 user_attr(4) 手册页。

基于角色的访问控制属性如下所示。

```
( 1.3.6.1.4.1.42.2.27.5.1.4 NAME 'SolarisAttrKeyValue'
  DESC 'Semi-colon separated key=value pairs of attributes'
  EQUALITY caseIgnoreIA5Match
  SUBSTRINGS caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.7 NAME 'SolarisAttrShortDesc'
  DESC 'Short description about an entry, used by GUIs'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.8 NAME 'SolarisAttrLongDesc'
  DESC 'Detail description about an entry'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.9 NAME 'SolarisKernelSecurityPolicy'
  DESC 'Solaris  kernel security policy'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.10 NAME 'SolarisProfileType'
  DESC 'Type of object defined in profile'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.11 NAME 'SolarisProfileId'
  DESC 'Identifier of object defined in profile'
  EQUALITY caseExactIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.12 NAME 'SolarisUserQualifier'
  DESC 'Per-user login attributes'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.13 NAME 'SolarisReserved1'
  DESC 'Reserved for future use'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.14 NAME 'SolarisReserved2'
  DESC 'Reserved for future use'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )
```

基于角色的访问控制 `objectClassses` 如下所示。

```
( 1.3.6.1.4.1.42.2.27.5.2.3 NAME 'SolarisUserAttr' SUP top AUXILIARY
  DESC 'User attributes'
  MAY ( SolarisUserQualifier $ SolarisAttrReserved1 $ \
        SolarisAttrReserved2 $ SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.4 NAME 'SolarisAuthAttr' SUP top STRUCTURAL
  DESC 'Authorizations data'
  MUST cn
  MAY ( SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisAttrShortDesc $ SolarisAttrLongDesc $ \
```

```
        SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.5 NAME 'SolarisProfAttr' SUP top STRUCTURAL
  DESC 'Profiles data'
  MUST cn
  MAY ( SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisAttrLongDesc $ SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.6 NAME 'SolarisExecAttr' SUP top AUXILIARY
  DESC 'Profiles execution attributes'
  MAY ( SolarisKernelSecurityPolicy $ SolarisProfileType $ \
        SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisProfileId $ SolarisAttrKeyValue ) )
```

LDAP 的 Internet 打印协议信息

以下各节提供了关于 Internet 打印协议和打印机的属性和 `ObjectClasses` 的信息。

Internet 打印协议属性

```
( 1.3.18.0.2.4.1140
NAME 'printer-uri'
DESC 'A URI supported by this printer.
This URI SHOULD be used as a relative distinguished name (RDN).
If printer-xri-supported is implemented, then this URI value
MUST be listed in a member value of printer-xri-supported.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )

( 1.3.18.0.2.4.1107
NAME 'printer-xri-supported'
DESC 'The unordered list of XRI (extended resource identifiers) supported
by this printer.
Each member of the list consists of a URI (uniform resource identifier)
followed by optional authentication and security metaparameters.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( 1.3.18.0.2.4.1135
NAME 'printer-name'
DESC 'The site-specific administrative name of this printer, more end-user
friendly than a URI.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1119
NAME 'printer-natural-language-configured'
DESC 'The configured language in which error and status messages will be
```

```
generated (by default) by this printer.
Also, a possible language for printer string attributes set by operator,
system administrator, or manufacturer.
Also, the (declared) language of the "printer-name", "printer-location",
"printer-info", and "printer-make-and-model" attributes of this printer.
For example: "en-us" (US English) or "fr-fr" (French in France) Legal values of
language tags conform to [RFC3066] "Tags for the Identification of Languages".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1136
NAME 'printer-location'
DESC 'Identifies the location of the printer. This could include
things like: "in Room 123A", "second floor of building XYZ".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} SINGLE-VALUE )

( 1.3.18.0.2.4.1139
NAME 'printer-info'
DESC 'Identifies the descriptive information about this printer.
This could include things like: "This printer can be used for
printing color transparencies for HR presentations", or
"Out of courtesy for others, please print only small (1-5 page)
jobs at this printer", or even "This printer is going away on July 1, 1997,
please find a new printer".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}
SINGLE-VALUE )

( 1.3.18.0.2.4.1134
NAME 'printer-more-info'
DESC 'A URI used to obtain more information about this specific printer.
For example, this could be an HTTP type URI referencing an HTML page
accessible to a Web Browser.
The information obtained from this URI is intended for end user consumption.'
EQUALITY caseIgnoreMatch ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )

( 1.3.18.0.2.4.1138
NAME 'printer-make-and-model'
DESC 'Identifies the make and model of the device.
The device manufacturer MAY initially populate this attribute.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1133
NAME 'printer-ipp-versions-supported'
DESC 'Identifies the IPP protocol version(s) that this printer supports,
including major and minor versions,
```

```
i.e., the version numbers for which this Printer implementation meets
the conformance requirements.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1132
NAME 'printer-multiple-document-jobs-supported'
DESC 'Indicates whether or not the printer supports more than one
document per job, i.e., more than one Send-Document or Send-Data
operation with document data.'
EQUALITY booleanMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )

( 1.3.18.0.2.4.1109
NAME 'printer-charset-configured'
DESC 'The configured charset in which error and status messages will be
generated (by default) by this printer.
Also, a possible charset for printer string attributes set by operator,
system administrator, or manufacturer.
For example: "utf-8" (ISO 10646/Unicode) or "iso-8859-1" (Latin1).
Legal values are defined by the IANA Registry of Coded Character Sets and
the "(preferred MIME name)" SHALL be used as the tag.
For coherence with IPP Model, charset tags in this attribute SHALL be
lowercase normalized.
This attribute SHOULD be static (time of registration) and SHOULD NOT be
dynamically refreshed attributetypes: (subsequently).'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} SINGLE-VALUE )

( 1.3.18.0.2.4.1131
NAME 'printer-charset-supported'
DESC 'Identifies the set of charsets supported for attribute type values of
type Directory String for this directory entry.
For example: "utf-8" (ISO 10646/Unicode) or "iso-8859-1" (Latin1).
Legal values are defined by the IANA Registry of Coded Character Sets and
the preferred MIME name.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} )

( 1.3.18.0.2.4.1137
NAME 'printer-generated-natural-language-supported'
DESC 'Identifies the natural language(s) supported for this directory entry.
For example: "en-us" (US English) or "fr-fr" (French in France).
Legal values conform to [RFC3066], Tags for the Identification of Languages.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} )

( 1.3.18.0.2.4.1130
NAME 'printer-document-format-supported'
DESC 'The possible document formats in which data may be interpreted
and printed by this printer.
Legal values are MIME types come from the IANA Registry of Internet Media Types.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )
```

```
( 1.3.18.0.2.4.1129
NAME 'printer-color-supported'
DESC 'Indicates whether this printer is capable of any type of color printing
at all, including highlight color.'
EQUALITY booleanMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.7  SINGLE-VALUE )

( 1.3.18.0.2.4.1128
NAME 'printer-compression-supported'
DESC 'Compression algorithms supported by this printer.
For example: "deflate, gzip".  Legal values include; "none", "deflate"
attributetypes: (public domain ZIP), "gzip" (GNU ZIP), "compress" (UNIX).'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1127
NAME 'printer-pages-per-minute'
DESC 'The nominal number of pages per minute which may be output by this
printer (e.g., a simplex or black-and-white printer).
This attribute is informative, NOT a service guarantee.
Typically, it is the value used in marketing literature to describe this printer.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1126 NAME 'printer-pages-per-minute-color'
DESC 'The nominal number of color pages per minute which may be output by this
printer (e.g., a simplex or color printer).
This attribute is informative, NOT a service guarantee.
Typically, it is the value used in marketing literature to describe this printer.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1125 NAME 'printer-finishings-supported'
DESC 'The possible finishing operations supported by this printer.
Legal values include; "none", "staple", "punch", "cover", "bind", "saddle-stitch",
"edge-stitch", "staple-top-left", "staple-bottom-left", "staple-top-right",
"staple-bottom-right", "edge-stitch-left", "edge-stitch-top", "edge-stitch-right",
"edge-stitch-bottom", "staple-dual-left", "staple-dual-top", "staple-dual-right",
"staple-dual-bottom".'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1124 NAME 'printer-number-up-supported'
DESC 'The possible numbers of print-stream pages to impose upon a single side of
an instance of a selected medium. Legal values include; 1, 2, and 4.
Implementations may support other values.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27 )

( 1.3.18.0.2.4.1123 NAME 'printer-sides-supported'
DESC 'The number of impression sides (one or two) and the two-sided impression
rotations supported by this printer.
Legal values include; "one-sided", "two-sided-long-edge", "two-sided-short-edge".'
```

```
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1122 NAME 'printer-media-supported'
DESC 'The standard names/types/sizes (and optional color suffixes) of the media
supported by this printer.
For example: "iso-a4",  "envelope", or "na-letter-white".
Legal values  conform to ISO 10175, Document Printing Application (DPA), and any
IANA registered extensions.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1117 NAME 'printer-media-local-supported'
DESC 'Site-specific names of media supported by this printer, in the language in
"printer-natural-language-configured".
For example: "purchasing-form" (site-specific name) as opposed to
(in "printer-media-supported"): "na-letter" (standard keyword from ISO 10175).'
EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1121 NAME 'printer-resolution-supported'
DESC 'List of resolutions supported for printing documents by this printer.
Each resolution value is a string with 3 fields:
1) Cross feed direction resolution (positive integer), 2) Feed direction
resolution (positive integer), 3) Resolution unit.
Legal values are "dpi" (dots per inch) and "dpcm" (dots per centimeter).
Each resolution field is delimited by ">".  For example:  "300> 300> dpi>".'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1120 NAME 'printer-print-quality-supported'
DESC 'List of print qualities supported for printing documents on this printer.
For example: "draft, normal".  Legal values include; "unknown", "draft", "normal",
"high".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1110 NAME 'printer-job-priority-supported'
DESC 'Indicates the number of job priority levels supported.
An IPP conformant printer which supports job priority must always support a
full range of priorities from "1" to "100"
(to ensure consistent behavior), therefore this attribute describes the
"granularity".
 Legal values of this attribute are from "1" to "100".'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1118
NAME 'printer-copies-supported'
DESC 'The maximum number of copies of a document that may be printed as a single job.
A value of "0" indicates no maximum limit.
A value of "-1" indicates unknown.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )
```

```
( 1.3.18.0.2.4.1111
NAME 'printer-job-k-octets-supported'
DESC 'The maximum size in kilobytes (1,024 octets actually) incoming print job that
this printer will accept.
A value of "0" indicates no maximum limit.  A value of "-1" indicates unknown.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1113
NAME 'printer-service-person'
DESC 'The name of the current human service person responsible for servicing this
printer.
It is suggested that this string include information that would enable other humans
to reach the service person, such as a phone number.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}
SINGLE-VALUE )

( 1.3.18.0.2.4.1114
NAME 'printer-delivery-orientation-supported'
DESC 'The possible delivery orientations of pages as they are printed and ejected
from this printer.
Legal values include; "unknown", "face-up", and "face-down".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1115
NAME 'printer-stacking-order-supported'
DESC 'The possible stacking order of pages as they are printed and ejected from
this printer.
Legal values include; "unknown", "first-to-last", "last-to-first".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1116
NAME 'printer-output-features-supported'
DESC 'The possible output features supported by this printer.
Legal values include; "unknown", "bursting", "decollating", "page-collating",
"offset-stacking".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1108
NAME 'printer-aliases'
DESC 'Site-specific administrative names of this printer in addition the printer
name specified for printer-name.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.6.1.4.1.42.2.27.5.1.63
NAME 'sun-printer-bsdaddr'
DESC 'Sets the server, print queue destination name and whether the client generates
protocol extensions.
```

```
"Solaris" specifies a Solaris print server extension. The value is represented b the
following value: server "," destination ", Solaris".'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.64
NAME 'sun-printer-kvp'
DESC 'This attribute contains a set of key value pairs which may have meaning to the
print subsystem or may be user defined.
Each value is represented by the following: key "=" value.'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Internet 打印协议 ObjectClasses

```
objectclasses: ( 1.3.18.0.2.6.2549
NAME 'slpService'
DESC 'DUMMY definition'
SUP 'top' MUST (objectclass) MAY ())

objectclasses: ( 1.3.18.0.2.6.254
NAME 'slpServicePrinter'
DESC 'Service Location Protocol (SLP) information.'
AUXILIARY SUP 'slpService')

objectclasses: ( 1.3.18.0.2.6.258
NAME 'printerAbstract'
DESC 'Printer related information.'
ABSTRACT SUP 'top' MAY ( printer-name
$ printer-natural-language-configured
$ printer-location
$ printer-info
$ printer-more-info
$ printer-make-and-model
$ printer-multiple-document-jobs-supported
$ printer-charset-configured
$ printer-charset-supported
$ printer-generated-natural-language-supported
$ printer-document-format-supported
$ printer-color-supported
$ printer-compression-supported
$ printer-pages-per-minute
$ printer-pages-per-minute-color
$ printer-finishings-supported
$ printer-number-up-supported
$ printer-sides-supported
$ printer-media-supported
$ printer-media-local-supported
$ printer-resolution-supported
$ printer-print-quality-supported
$ printer-job-priority-supported
$ printer-copies-supported
$ printer-job-k-octets-supported
$ printer-current-operator
$ printer-service-person
$ printer-delivery-orientation-supported
$ printer-stacking-order-supported $ printer! -output-features-supported ))
```

```
objectclasses: ( 1.3.18.0.2.6.255
NAME 'printerService'
DESC 'Printer information.'
STRUCTURAL SUP 'printerAbstract' MAY ( printer-uri
$ printer-xri-supported ))

objectclasses: ( 1.3.18.0.2.6.257
NAME 'printerServiceAuxClass'
DESC 'Printer information.'
AUXILIARY SUP 'printerAbstract' MAY ( printer-uri $ printer-xri-supported ))

objectclasses: ( 1.3.18.0.2.6.256
NAME 'printerIPP'
DESC 'Internet Printing Protocol (IPP) information.'
AUXILIARY SUP 'top' MAY   ( printer-ipp-versions-supported $
printer-multiple-document-jobs-supported ))

objectclasses: ( 1.3.18.0.2.6.253
NAME 'printerLPR'
DESC 'LPR information.'
AUXILIARY SUP 'top' MUST ( printer-name ) MAY ( printer-aliases))

objectclasses: ( 1.3.6.1.4.1.42.2.27.5.2.14
NAME 'sunPrinter'
DESC 'Sun printer information'
SUP 'top' AUXILIARY MUST (objectclass $ printer-name)  MAY
(sun-printer-bsdaddr $ sun-printer-kvp))
```

打印机属性

```
ATTRIBUTE ( 1.3.6.1.4.1.42.2.27.5.1.63
NAME sun-printer-bsdaddr
DESC 'Sets the server, print queue destination name and whether the
     client generates protocol extensions. "Solaris" specifies a
     Solaris print server extension.  The value is represented by
     the following value: server "," destination ", Solaris".'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
)


ATTRIBUTE ( 1.3.6.1.4.1.42.2.27.5.1.64
NAME sun-printer-kvp
DESC 'This attribute contains a set of key value pairs which may have
      meaning to the print subsystem or may be user defined.  Each
      value is represented by the following: key "=" value.'
EQUALITY caseIgnoreIA5Match
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15  )
```

Sun 打印机 ObjectClasses

```
OBJECTCLASS ( 1.3.6.1.4.1.42.2.27.5.2.14
NAME sunPrinter
DESC 'Sun printer information'
SUP  top
AUXILIARY
MUST ( printer-name )
MAY  ( sun-printer-bsdaddr $ sun-printer-kvp ))
```

LDAP 的常规目录服务器要求

要支持 LDAP 客户机，所有服务器都必须支持 LDAP v3 协议与组合命名和辅助对象类。另外，还必须至少支持下列控制之一。

- 简单分页模式 (RFC 2696)
- 虚拟列表视图控制

  服务器必须至少支持下列验证方法之一。

  ```
  anonymous
  simple
  sasl/cram-MD5
  sasl/digest-MD5
  sasl/GSSAPI
  ```

如果 LDAP 客户机在使用 `pam_unix_*` 模块，则服务器必须支持以 UNIX crypt 格式存储口令。

如果 LDAP 客户机在使用 TLS，则服务器必须支持 SSL 或 TLS。

如果 LDAP 客户机在使用 `sasl/GSSAPI`，则服务器必须支持 SASL、GSSAPI、Kerberos 5 验证。对 GSS 线上加密的支持是可选的。

LDAP 命名服务使用的缺省过滤器

如果没有使用 SSD 为给定的服务手动指定参数，将使用缺省过滤器。要列出给定服务的缺省过滤器，请使用带 `-v` 选项的 `ldaplist`。

在以下示例中，`filter=(&(objectclass=iphost)(cn=abcde)` 定义了缺省过滤器。

```
database=hosts
filter=(&(objectclass=iphost)(cn=abcde)
user data=(&(%s) (cn=abcde))
```

`ldaplist` 生成以下缺省过滤器列表，其中 `%s` 表示字符串，`%d` 表示数字。

```
hosts
(&(objectclass=iphost)(cn=%s))
--------------
passwd
(&(objectclass=posixaccount)(uid=%s))
--------------
services
(&(objectclass=ipservice)(cn=%s))
--------------
group
(&(objectclass=posixgroup)(cn=%s))
--------------
netgroup
(&(objectclass=nisnetgroup)(cn=%s))
--------------
networks
(&(objectclass=ipnetwork)(ipnetworknumber=%s))
--------------
netmasks
(&(objectclass=ipnetwork)(ipnetworknumber=%s))
--------------
rpc
(&(objectclass=oncrpc)(cn=%s))
--------------
protocols
(&(objectclass=ipprotocol)(cn=%s))
--------------
bootparams
(&(objectclass=bootableDevice)(cn=%s))
--------------
ethers
(&(objectclass=ieee802Device)(cn=%s))
--------------
publickey
(&(objectclass=niskeyobject)(cn=%s))
or
(&(objectclass=niskeyobject)(uidnumber=%d))
--------------
aliases
(&(objectclass=mailGroup)(cn=%s))
--------------
```

表 14–4 getXbyY 调用中使用的 LDAP 过滤器

过滤器	定义
bootparamByName	(&(objectClass=bootableDevice)(cn=%s))
etherByHost	(&(objectClass=ieee802Device)(cn=%s))
etherByEther	(&(objectClass=ieee802Device)(macAddress=%s))
groupByName	(&(objectClass=posixGroup)(cn=%s))
groupByGID	(&(objectClass=posixGroup)(gidNumber=%ld))
groupByMember	(&(objectClass=posixGroup)(memberUid=%s))

表 14–4 getXbyY 调用中使用的 LDAP 过滤器 （续）

过滤器	定义
hostsByName	(&(objectClass=ipHost)(cn=%s))
hostsByAddr	(&(objectClass=ipHost)(ipHostNumber=%s))
keyByUID	(&(objectClass=nisKeyObject)(uidNumber=%s))
keyByHost	(&(objectClass=nisKeyObject)(cn=%s))
netByName	(&(objectClass=ipNetwork)(cn=%s))
netByAddr	(&(objectClass=ipNetwork)(ipNetworkNumber=%s))
nisgroupMember	(membernisnetgroup=%s)
maskByNet	(&(objectClass=ipNetwork)(ipNetworkNumber=%s))
printerByName	(&(objectClass=sunPrinter)(|(printer-name=%s)(printer-aliases=%s)))
projectByName	(&(objectClass=SolarisProject)(SolarisProjectName=%s))
projectByID	(&(objectClass=SolarisProject)(SolarisProjectID=%ld))
protoByName	(&(objectClass=ipProtocol)(cn=%s))
protoByNumber	(&(objectClass=ipProtocol)(ipProtocolNumber=%d))
passwordByName	(&(objectClass=posixAccount)(uid=%s))
passwordByNumber	(&(objectClass=posixAccount)(uidNumber=%ld))
rpcByName	(&(objectClass=oncRpc)(cn=%s))
rpcByNumber	(&(objectClass=oncRpc)(oncRpcNumber=%d))
serverByName	(&(objectClass=ipService)(cn=%s))
serverByPort	(&(objectClass=ipService)(ipServicePort=%ld))
serverByNameAndProto	(&(objectClass=ipService)(cn=%s)(ipServiceProtocol=%s))
specialByNameserver	(ipServiceProtocol=%s))
ByPortAndProto	(&(objectClass=shadowAccount)(uid=%s))
netgroupByTriple	(&(objectClass=nisNetGroup)(cn=%s))
netgroupByMember	(&(objectClass=nisNetGroup)(cn=%s))
authName	(&(objectClass=SolarisAuthAttr)(cn=%s))
auditUserByName	(&(objectClass=SolarisAuditUser)(uid=%s))

表 14–4 getXbyY 调用中使用的 LDAP 过滤器 （续）

过滤器	定义
execByName	(&(objectClass=SolarisExecAttr)(cn=%s) (SolarisKernelSecurityPolicy=%s)(SolarisProfileType=%s))
execByPolicy	(&(objectClass=SolarisExecAttr)(SolarisProfileId=%s) (SolarisKernelSecurityPolicy=%s)(SolarisProfileType=%s))
profileByName	(&(objectClass=SolarisProfAttr)(cn=%s))
userByName	(&(objectClass=SolarisUserAttr)(uid=%s))

下表列出了 getent 属性过滤器。

表 14–5 getent 属性过滤器

过滤器	定义
aliases	(objectClass=rfc822MailGroup)
auth_attr	(objectClass=SolarisAuthAttr)
audit_user	(objectClass=SolarisAuditUser)
exec_attr	(objectClass=SolarisExecAttr)
group	(objectClass=posixGroup)
hosts	(objectClass=ipHost)
networks	(objectClass=ipNetwork)
prof_attr	(objectClass=SolarisProfAttr)
protocols	(objectClass=ipProtocol)
passwd	(objectClass=posixAccount)
printers	(objectClass=sunPrinter)
rpc	(objectClass=oncRpc)
services	(objectClass=ipService)
shadow	(objectclass=shadowAccount)
project	(objectClass=SolarisProject)
usr_attr	(objectClass=SolarisUserAttr)

◆ ◆ ◆ 第 15 章

15 从 NIS 转换为 LDAP（任务）

本章介绍如何对那些使用 LDAP 目录中存储的命名信息的 NIS 客户机启用支持。按照本章中的过程操作，可以从使用 NIS 命名服务转换为使用 LDAP 命名服务。

要了解转换到 LDAP 的益处，请参见第 118 页中的 “LDAP 命名服务与其他命名服务的比较”。

本章将介绍以下信息：

NIS 到 LDAP 转换服务概述

NIS 到 LDAP 转换服务（*N2L* **服务**）以 NIS 到 LDAP 转换守护进程取代了 NIS 主服务器上的现有 NIS 守护进程。N2L 服务还在该服务器上创建一个 NIS 到 LDAP 转换的映射文件。该映射文件指定 NIS 映射项和 LDAP 中目录信息树 (Directory Information Tree, DIT) 等效项之间的映射。已经进行这种转换的 NIS 主服务器称为 *N2L* **服务器**。从属服务器上没有 `NISLDAPmapping` 文件，因此它们继续以通常的方式工作。从属服务器定期从 N2L 服务器更新其数据，就好像 N2L 服务器是常规的 NIS 主服务器一样。

N2L 服务的行为由 `ypserv` 和 `NISLDAPmapping` 配置文件控制。借助脚本 `inityp2l` 可以对这些配置文件进行初始设置。一旦建立了 N2L 服务器，您便可以通过直接编辑这些配置文件来维护 N2L。

N2L 服务支持以下功能：

- 将 NIS 映射导入到 LDAP 目录信息树 (Directory Information Tree, DIT)
- 客户机以 NIS 的速度和可扩展性访问 DIT 信息

在任何命名系统中，只有一个信息源可以是权威来源。在传统的 NIS 中，NIS 源是权威信息。在使用 N2L 服务时，权威数据来源是 LDAP 目录。该目录是通过使用目录管理工具进行管理的，如第 9 章，LDAP 命名服务介绍（概述）中所述。

NIS 源仅保留用于紧急备份或卸载。在使用 N2L 服务后，您必须逐步淘汰 NIS 客户机。最终，所有 NIS 客户机都应当被 LDAP 命名服务客户机替换。

以下各小节中提供了其他概述信息：

NIS 到 LDAP 转换工具和服务管理工具

NIS 和 LDAP 服务由服务管理工具管理。使用 `svcadm` 命令可以对这些服务执行启用、禁用或重新启动等管理操作。使用 `svcs` 命令可以查询服务的状态。有关使用 SMF 对 LDAP 和 NIS 进行管理的更多信息，请参见第 166 页中的 “LDAP 和服务管理工具”和第 72 页中的 “NIS 和服务管理工具”。有关 SMF 的概述，请参见《在 Oracle Solaris 11.1 中管理服务和故障》中的第 1 章 “管理服务（概述）”。有关更多详细信息，另请参阅 `svcadm(1M)` 和 `svcs(1)` 手册页。

NIS 到 LDAP 转换的目标用户

您需要熟悉 NIS 和 LDAP 概念、术语以及 ID 才能执行本章中的过程。有关 NIS 和 LDAP 命名服务的更多信息，请参见本书中的以下两章：

- 第 5 章，网络信息服务（概述）（提供了 NIS 的概述）
- 第 9 章，LDAP 命名服务介绍（概述）（提供了 LDAP 的概述）

不应使用 NIS 到 LDAP 转换服务的情况

N2L 服务的用途是充当从使用 NIS 转换到使用 LDAP 的转换工具。在下列情况下不要使用 N2L 服务：

- 不计划在 NIS 和 LDAP 命名服务客户机之间共享数据的情况下

  在这种情况下，N2L 服务器将充当极其复杂的 NIS 主服务器。

- NIS 映射由修改 NIS 源文件的工具（而非 yppasswd）进行管理的情况下

  从 DIT 映射重新生成 NIS 源是一项不精确的任务，需要手动检查生成的映射。一旦使用了 N2L 服务，所提供的 NIS 源重新生成功能将仅用于卸载 NIS 或恢复为 NIS。
- 没有 NIS 客户机的情况下

  在这样的环境中，请使用 LDAP 命名服务客户机及其对应的工具。

NIS 到 LDAP 转换服务对用户造成的影响

单单安装与 N2L 服务相关的文件不会更改 NIS 服务器的缺省行为。在安装时，管理员会看到服务器上的 NIS 手册页会有一些变化并且其中会增加 N2L 帮助脚本 inityp2l 和 ypmap2src。但是，只要未在 NIS 服务器上运行 inityp2l 或未手动创建 N2L 配置文件，NIS 组件便会继续在传统的 NIS 模式下启动，并像往常那样工作。

运行 inityp2l 之后，用户会看到服务器和客户机的行为会发生一些变化。以下列表列出了 NIS 和 LDAP 用户的类型，并说明了部署 N2L 服务之后每种类型的用户应当注意到的情况。

用户类型	N2L 服务的影响
NIS 主服务器管理员	NIS 主服务器转换为 N2L 服务器。NISLDAPmapping 和 ypserv 配置文件将会安装在 N2L 服务器上。建立 N2L 服务器之后，可以使用 LDAP 命令来管理命名信息。
NIS 从属服务器管理员	N2L 转换之后，NIS 从属服务器继续以通常的方式运行 NIS。当 ypmake 调用 yppush 时，N2L 服务器将更新后的 NIS 映射推送到从属服务器。请参见 ypmake(1M) 手册页。
NIS 客户机	NIS 读取操作与传统的 NIS 没有区别。当 LDAP 命名服务客户机更改 DIT 中的信息时，该信息将被复制到 NIS 映射中。复制操作是在可配置的超时时间过期之后完成的。这类行为与连接到 NIS 从属服务器的常规 NIS 客户机的行为相似。 如果 N2L 服务器无法绑定到 LDAP 服务器进行读取，它将从自身的缓存副本中返回信息。或者，N2L 服务器还可能会返回内部服务器错误。您可以将 N2L 服务器配置为以上述任一方式响应。有关更多详细信息，请参见 ypserv(1M) 手册页。
所有用户	当 NIS 客户机发出更改口令的请求时，所做的更改将立即显示在 N2L 主服务器上并对本地 LDAP 客户机可见。 如果您试图在 NIS 客户机上更改口令，但 LDAP 服务器不可用，更改将被拒绝，并且 N2L 服务器会返回内部服务器错误。此行为可防止将不正确的信息写入高速缓存中。

NIS 到 LDAP 转换术语

以下是与 N2L 服务的实现相关的术语。

表 15–1 与 N2L 转换相关的术语

术语	说明
N2L configuration file（N2L 配置文件）	`/var/yp/NISLDAPmapping` 和 `/var/yp/ypserv` 文件，`ypserv` 守护进程使用这些文件在 N2L 模式下启动主服务器。有关详细消息，请参见 `NISLDAPmapping`(4) 和 `ypserv`(4) 手册页。
map（映射）	在 N2L 服务的上下文中，术语“映射”的用法有两种： ■ 指 NIS 用于存储特定类型信息的数据库文件 ■ 描述从 LDAP DIT 映射 NIS 信息或将 NIS 信息映射到 LDAP DIT 的过程
mapping（映射过程）	NIS 项与 LDAP DIT 项之间的相互转换过程。
mapping file（映射文件）	用来指定如何在 NIS 文件和 LDAP 文件之间映射各项的 `NISLDAPmapping` 文件。
standard map（标准映射）	无需手动修改映射文件即可由 N2L 服务支持的常用 NIS 映射。第 215 页中的 “支持的标准映射”中提供了支持的标准映射的列表。
nonstandard map（非标准映射）	经过定制的标准 NIS 映射，这些非标准映射使用 NIS 和 LDAP DIT 之间的映射，而不是 RFC 2307 或其后续版本中标识的映射。
custom map（定制映射）	任何不是标准映射并在从 NIS 转换至 LDAP 时需要手动修改映射文件的映射。
LDAP client（LDAP 客户机）	任何对 LDAP 服务器执行读写操作的传统 LDAP 客户机。传统的 LDAP 客户机是可以对任何 LDAP 服务器执行读写操作的系统。LDAP 命名服务客户机可处理部分定制的命名信息。
LDAP naming services client（LDAP 命名服务客户机）	用来处理部分定制命名信息的 LDAP 客户机。
N2L server（N2L 服务器）	已使用 N2L 服务重新配置为 N2L 服务器的 NIS 主服务器。重新配置过程包括替换 NIS 守护进程和添加新配置文件。

NIS 到 LDAP 转换的命令、文件和映射

与 N2L 转换相关联的共有两个实用程序、两个配置文件和一个映射。

表 15–2 N2L 命令、文件和映射的说明

命令/文件/映射	说明
`/usr/lib/netsvc/yp/inityp2l`	一个用来帮助创建 `NISLDAPmapping` 和 `ypserv` 配置文件的实用程序。此实用程序不是用来管理这些文件的通用工具。高级用户可通过使用文本编辑器检查和定制 `inityp2l` 输出来维护 N2L 配置文件或创建定制映射。请参见 `inityp2l`(1M) 手册页。
`/usr/lib/netsvc/yp/ypmap2src`	一个用来将标准 NIS 映射转换为等效 NIS 源文件的近似项的实用程序。`ypmap2src` 主要用于将 N2L 转换服务器转换为传统的 NIS。请参见 `ypmap2src`(1M) 手册页。

表 15–2 N2L 命令、文件和映射的说明 （续）

命令/文件/映射	说明
/var/yp/NISLDAPmapping	一个配置文件，用于指定 NIS 映射项与 LDAP 中目录信息树 (Directory Information Tree, DIT) 等效项之间的映射。请参见 NISLDAPmapping(4) 手册页。
/var/yp/ypserv	一个指定了 NIS 到 LDAP 转换守护进程的配置信息的文件。请参见 ypserv(4) 手册页。
ageing.byname	映射，yppasswdd 在实现 NIS 到 LDAP 转换时使用此映射在 DIT 中读写口令生命期信息。

支持的标准映射

缺省情况下，N2L 服务支持在以下映射列表与 RFC 2307、RFC 2307bis 及其后续版本的 LDAP 条目之间的映射。这些标准映射不需要手动修改映射文件。系统上任何未在下表中列出的映射都被视为定制映射，且需要手动修改。

N2L 服务还支持 auto.* 映射的自动映射。但是，由于大多数 auto.* 文件名和内容都特定于每种网络配置，因此该列表并未指定这些文件。但作为标准映射支持的 auto.home 和 auto.master 映射除外。

```
audit_user
auth_attr
auto.home
auto.master
bootparams
ethers.byaddr ethers.byname
exec_attr
group.bygid group.byname group.adjunct.byname
hosts.byaddr hosts.byname
ipnodes.byaddr ipnodes.byname
mail.byaddr mail.aliases
netgroup netgroup.byprojid netgroup.byuser netgroup.byhost
netid.byname
netmasks.byaddr
networks.byaddr networks.byname
passwd.byname passwd.byuid passwd.adjunct.byname
prof_attr
project.byname project.byprojectid
protocols.byname protocols.bynumber
publickey.byname
rpc.bynumber
services.byname services.byservicename
timezone.byname
user_attr
```

在 NIS 到 LDAP 转换过程中，yppasswdd 守护进程使用 N2L 特定的映射 ageing.byname 在 DIT 中读写口令生命期信息。如果没有使用口令生命期，则会忽略 ageing.byname 映射。

从 NIS 转换为 LDAP（任务列表）

下表列出了安装和管理 N2L 服务（使用标准的和定制的 NIS 到 LDAP 转换映射）所需的过程。

任务	说明	参考
完成所有先决条件。	确保已经正确配置了 NIS 服务器和 Oracle Directory Server Enterprise Edition（LDAP 服务器）。	第 216 页中的 “NIS 到 LDAP 转换的先决条件”
设置 N2L 服务。	在 NIS 主服务器上运行 `inityp2l` 以设置以下映射之一：	
	标准映射	第 218 页中的 “如何使用标准映射设置 N2L 服务”
	定制映射或非标准映射	第 220 页中的 “如何使用定制映射或非标准映射设置 N2L 服务”
定制映射。	查看如何为 N2L 转换创建定制映射的示例。	第 222 页中的 “定制映射的示例”
使用 N2L 配置 Oracle Directory Server Enterprise Edition。	将 Oracle Directory Server Enterprise Edition 配置并调整为用于 N2L 转换的 LDAP 服务器。	第 223 页中的 “使用 Oracle Directory Server Enterprise Edition 进行 NIS 到 LDAP 转换的最佳做法”
对系统进行故障排除。	确定和解决常见的 N2L 问题。	第 226 页中的 “NIS 到 LDAP 转换的故障排除”
恢复为 NIS。	使用相应的映射恢复为 NIS：	
	基于旧 NIS 源文件的映射	第 230 页中的 “如何基于旧的源文件恢复到 NIS 映射”
	基于当前 DIT 的映射	第 231 页中的 “如何基于当前的 DIT 内容恢复为 NIS 映射”

NIS 到 LDAP 转换的先决条件

在实施 N2L 服务之前，您必须检查或完成以下各项。

- 运行 `inityp2l` 脚本以启用 N2L 模式之前，确保将系统设置为可正常工作的传统 NIS 服务器。
- 在系统上配置 LDAP 目录服务器。

  NIS 到 LDAP 转换迁移工具支持 Oracle 提供的 Oracle Directory Server Enterprise Edition 以及兼容版本的目录服务器。如果您使用 Oracle Directory Server Enterprise Edition，在设置 N2L 服务**之前**，请使用 `idsconfig` 命令配置服务器。有关 `idsconfig`

的更多信息，请参见第 11 章，为使用 LDAP 客户机设置 Oracle Directory Server Enterprise Edition（任务）和 idsconfig(1M) 手册页。

其他（第三方）LDAP 服务器也许能够用于 N2L 服务，但是它们不受 Oracle 支持。如果您使用的 LDAP 服务器不是 Oracle Directory Server Enterprise Edition 或兼容的 Oracle 服务器，则在设置 N2L 服务**之前**，您必须手动配置服务器以支持 RFC 2307bis、RFC 4876 或其后续版本的架构。

- 对于 config/host 属性，在 dns 之前使用 files。
- 确保在 N2L 主服务器上的 hosts 文件中提供了 N2L 主服务器和 LDAP 服务器的地址。

  另一种解决方案是在 ypserv 中列出 LDAP 服务器地址，而不列出其主机名。这意味着 LDAP 服务器地址列在另一个位置，因此，在更改 LDAP 服务器或 N2L 主服务器的地址时，需要对文件进行额外的修改。

设置 NIS 到 LDAP 转换服务

您可以按照以下两个过程中的说明，使用标准映射或定制映射设置 N2L 服务。

在 NIS 到 LDAP 转换过程中，您需要运行 inityp2l 命令。该命令会运行一个交互式脚本，而您必须为该脚本提供配置信息。以下列表列出了需要提供的信息类型。有关这些属性的说明，请参见 ypserv(1M) 手册页。

- 创建的配置文件的名称（缺省为 /etc/default/ypserv）
- 用来将配置信息存储到 LDAP 中的 DN（缺省为 ypserv）
- 用来将数据映射到 LDAP 或从 LDAP 映射数据的首选服务器的列表
- 用来将数据映射到 LDAP 或从 LDAP 映射数据的验证方法
- 用来将数据映射到 LDAP 或从 LDAP 映射数据的传输层安全性 (Transport Layer Security, TLS) 方法
- 用来在 LDAP 中读写数据的代理用户绑定 DN
- 用来在 LDAP 中读写数据的代理用户口令
- LDAP 绑定操作的超时值（以秒为单位）
- LDAP 搜索操作的超时值（以秒为单位）
- LDAP 修改操作的超时值（以秒为单位）
- LDAP 添加操作的超时值（以秒为单位）
- LDAP 删除操作的超时值（以秒为单位）
- LDAP 服务器上搜索操作的时间限制（以秒为单位）
- LDAP 服务器上搜索操作的大小限制（以字节为单位）
- N2L 是否应当遵循 LDAP 引用

- 导致 LDAP 检索错误的操作、尝试检索的次数以及各尝试操作的超时值（以秒为单位）
- 导致存储错误的操作、尝试的次数以及各尝试操作的超时值（以秒为单位）
- 映射文件的名称
- 是否为 `auto_direct` 映射生成映射信息

  脚本将与定制映射相关的信息放入映射文件中的相应位置。
- 命名上下文
- 是否启用口令更改功能
- 是否更改所有映射的缺省 TTL 值

注 – 大多数 LDAP 服务器（包括 Oracle Directory Server Enterprise Edition）都不支持 `sasl/cram-md5` 验证。

▼ 如何使用标准映射设置 N2L 服务

如果要转换第 215 页中的 “支持的标准映射”中所列的映射，请使用此过程。如果要使用定制映射或非标准映射，请参见第 220 页中的 “如何使用定制映射或非标准映射设置 N2L 服务”。

设置 LDAP 服务器之后，请运行 `inityp2l` 脚本并在出现提示时提供配置信息。`inityp2l` 为标准映射和 `auto.*` 映射设置配置和映射文件。

1. **完成第 216 页中的 “NIS 到 LDAP 转换的先决条件”中所列的先决步骤。**

2. **成为 NIS 主服务器的管理员。**

   有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

3. **将 NIS 主服务器转换为 N2L 服务器。**

   ```
   # inityp2l
   ```

   在 NIS 主服务器上运行 `inityp2l` 脚本并按照提示操作。有关需要提供的信息的列表，请参见第 217 页中的 “设置 NIS 到 LDAP 转换服务”。

   有关更多详细信息，请参见 `inityp2l(1M)` 手册页。

4. **确定 LDAP 目录信息树 (Directory Information Tree, DIT) 是否已完全初始化。**

   如果 DIT 中已包含置备 `NISLDAPmapping` 文件中所列全部映射所需要的信息，则表明它已完全初始化。

   - 如果未包含，请继续执行步骤 5 并跳过步骤 6。

- 如果已包含，请跳过步骤 5 并转至步骤 6。

5 **初始化 DIT 以便从 NIS 源文件进行转换。**

仅当 DIT **尚未**完全初始化时，才需执行这些步骤。

a. **确保旧 NIS 映射是最新的版本。**

```
# cd /var/yp
# make
```

有关更多信息，请参见 ypmake(1M) 手册页。

b. **停止 NIS 服务**

```
# svcadm disable network/nis/server:default
```

c. **将旧映射复制到 DIT 中，然后为这些映射初始化 N2L 支持。**

```
# ypserv -IR
```

等待 ypserv 退出。

提示 – 原始的 NIS dbm 文件不会被覆盖。您可以根据需要恢复这些文件。

---

d. **启动 DNS 和 NIS 服务以确保它们使用新的映射。**

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

这样便完成了使用标准映射设置 N2L 服务的过程。您无需完成步骤 6。

6 **初始化 NIS 映射。**

仅当 DIT 已完全初始化并且跳过了步骤 5 时，才执行这些步骤。

a. **停止 NIS 服务。**

```
# svcadm disable network/nis/server:default
```

b. **使用 DIT 中的信息初始化 NIS 映射。**

```
# ypserv -r
```

等待 ypserv 退出。

提示 – 原始的 NIS dbm 文件不会被覆盖。您可以根据需要恢复这些文件。

---

c. **启动 DNS 和 NIS 服务以确保它们使用新的映射。**

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

▼ 如何使用定制映射或非标准映射设置 N2L 服务

如果符合以下情况，请使用此过程：

- 具有第 215 页中的 “支持的标准映射”中未列出的映射。
- 具有要映射到非 RFC 2307 LDAP 映射的标准 NIS 映射。

1 **完成第 216 页中的 “NIS 到 LDAP 转换的先决条件”中所列的先决步骤。**

2 **成为 NIS 主服务器的管理员。**

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的第 9 章 “使用基于角色的访问控制（任务）”。

3 **将 NIS 主服务器配置为 N2L 服务器。**

```
# inityp2l
```

在 NIS 主服务器上运行 `inityp2l` 脚本并按照提示操作。有关需要提供的信息的列表，请参见第 217 页中的 “设置 NIS 到 LDAP 转换服务”。

有关更多详细信息，请参见 `inityp2l`(1M) 手册页。

4 **修改 `/var/yp/NISLDAPmapping` 文件。**

有关如何修改映射文件的示例，请参见第 222 页中的 “定制映射的示例”。

5 **确定 LDAP 目录信息树 (Directory Information Tree, DIT) 是否已完全初始化。**

如果 DIT 中已包含置备 `NISLDAPmapping` 文件中所列全部映射所需要的信息，则表明它已完全初始化。

- 如果未包含，请完成步骤 6、步骤 8 和步骤 9。
- 如果已包含，请跳过步骤 6 并完成步骤 7、步骤 8 和步骤 9。

6 **初始化 DIT 以便从 NIS 源文件进行转换。**

a. **确保旧 NIS 映射是最新的版本。**

```
# cd /var/yp
# make
```

有关更多信息，请参见 `ypmake`(1M) 手册页。

b. **停止 NIS 守护进程。**

```
# svcadm disable network/nis/server:default
```

c. **将旧映射复制到 DIT 中，然后为这些映射初始化 N2L 支持。**

```
# ypserv -Ir
```

等待 ypserv 退出。

提示 – 原始的 NIS dbm 文件不会被覆盖。您可以根据需要恢复这些文件。

d. 启动 DNS 和 NIS 服务以确保它们使用新的映射。

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

e. 跳过步骤 7 并继续执行步骤 8。

7 初始化 NIS 映射。

仅当 DIT 已完全初始化时，才可以执行此步骤。

a. 停止 NIS 守护进程。

```
# svcadm disable network/nis/server:default
```

b. 使用 DIT 中的信息初始化 NIS 映射。

```
# ypserv -r
```

等待 ypserv 退出。

提示 – 原始的 NIS dbm 文件不会被覆盖。您可以根据需要恢复这些文件。

c. 启动 DNS 和 NIS 服务以确保它们使用新的映射。

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

8 检验 LDAP 项是否正确。

如果这些项不正确，LDAP 命名服务器客户机将无法找到这些项。

```
# ldapsearch -h server -s sub -b "ou=servdates, dc=..." \ "objectclass=servDates"
```

9 验证 LDAP_ 映射的内容。

以下样例输出说明如何使用 makedm 命令验证 hosts.byaddr 映射的内容。

```
# makedbm -u LDAP_servdate.bynumber
plato: 1/3/2001
johnson: 2/4/2003,1/3/2001
yeats: 4/4/2002
poe: 3/3/2002,3/4/2000
```

如果内容与预期一致，则表明已成功地从 NIS 转换到 LDAP。

请注意，原始的 NIS dbm 文件不会被覆盖，因此您始终可以恢复这些文件。有关更多信息，请参见第 230 页中的 “恢复为 NIS”。

定制映射的示例

以下两个示例说明如何定制映射。请使用首选的文本编辑器，根据需要修改 `/var/yp/NISLDAPmapping` 文件。有关文件属性和语法的更多信息，请参见 `NISLDAPmapping(4)` 手册页以及第 9 章，LDAP 命名服务介绍（概述）中的 LDAP 命名服务信息。

示例 15–1 移动主机项

本示例说明如何将主机项从缺省位置移到 DIT 中的另一个（非标准）位置。

将 `NISLDAPmapping` 文件中的 `nisLDAPobjectDN` 属性更改为新的 LDAP 标识名 (distinguished name, DN)。在本示例中，LDAP 对象的内部结构未更改，因此 `objectClass` 项也不会更改。

将以下内容：

```
nisLDAPobjectDN hosts: \
                        ou=hosts,?one?, \
                        objectClass=device, \
                        objectClass=ipHost
```

更改为：

```
nisLDAPobjectDN hosts: \
                        ou=newHosts,?one?, \
                        objectClass=device, \
                        objectClass=ipHost
```

此更改会导致按如下方式映射这些项：

```
dn: ou=newHosts, dom=domain1, dc=sun, dc=com
```

而不是按如下方式映射：

```
dn: ou=hosts, dom=domain1, dc=sun, dc=com。
```

示例 15–2 实现定制映射

本示例说明如何实现定制映射。

虚拟映射 *servdate.bynumber* 中包含有关为系统提供服务的日期的信息。此映射根据计算机的序列号（在本示例中为 123）建立索引。每一项都由计算机所有者的姓名、一个冒号和一个用逗号分隔的服务日期列表组成，如 John Smith:1/3/2001,4/5/2003。

旧映射的结构将映射到以下形式的 LDAP 项上：

```
dn: number=123,ou=servdates,dc=... \
                number: 123 \
                userName: John Smith \
```

示例 15–2 实现定制映射 （续）

```
                date: 1/3/2001 \
                date: 4/5/2003 \
                 .
                 .
                 .
                objectClass: servDates
```

通过检查 `NISLDAPmapping` 文件，可以看到与所需模式最接近的映射是 `group`。可以根据 `group` 映射建立定制映射的模型。由于仅有一个映射，因此不需要 `nisLDAPdatabaseIdMapping` 属性。以下是要添加到 `NISLDAPmapping` 中的属性：

```
nisLDAPentryTtl servdate.bynumber:1800:5400:3600

nisLDAPnameFields servdate.bynumber: \
                        ("%s:%s", uname, dates)

nisLDAPobjectDN servdate.bynumber: \
                        ou=servdates, ?one? \
                        objectClass=servDates:

nisLDAPattributeFromField servdate.bynumber: \
                        dn=("number=%s,", rf_key), \
                        number=rf_key, \
                        userName=uname, \
                        (date)=(dates, ",")

nisLDAPfieldFromAttribute servdate.bynumber: \
                        rf_key=number, \
                        uname=userName, \
                        dates=("%s,", (date), ",")
```

使用 Oracle Directory Server Enterprise Edition 进行 NIS 到 LDAP 转换的最佳做法

N2L 服务支持 Oracle Directory Server Enterprise Edition。其他第三方 LDAP 服务器也许能够用于 N2L 服务，但是它们不受 Oracle 支持。如果您使用的是 LDAP 服务器而不是 Oracle Directory Server Enterprise Edition 服务器或兼容的 Oracle 服务器，您必须手动配置服务器以支持 RFC 2307、RFC 2307bis 和 RFC 4876 或其后续版本的架构。

如果使用的是 Oracle Directory Server Enterprise Edition，则可以增强目录服务器以提高性能。必须对 Oracle Directory Server Enterprise Edition 具有 LDAP 管理员权限才能增强目录服务器。另外，目录服务器可能需要重新引导，此任务必须与服务器的 LDAP 客户机协调进行。可以在 Sun Java System Directory Server Enterprise Edition 6.2 Web 站点上找到 Oracle Directory Server Enterprise Edition 文档。

使用 Oracle Directory Server Enterprise Edition 创建虚拟列表视图索引

对于大型映射，必须使用 LDAP 虚拟列表视图 (virtual list view, VLV) 索引来确保 LDAP 搜索可返回全部结果。要了解关于在 Oracle Directory Server Enterprise Edition 上设置 VLV 索引的信息，请参见 Sun Java System Directory Server Enterprise Edition 6.2 文档。

VLV 搜索结果使用固定的页面大小 50000。如果在 Oracle Directory Server Enterprise Edition 上使用 VLV，则 LDAP 服务器和 N2L 服务器都必须可以传送此大小的页面。如果已知所有的映射都小于此限制，则不必使用 VLV 索引。但是，如果使用的映射大于此大小限制，或者不能确定所有映射的大小，请使用 VLV 索引，以避免返回的结果不完整。

如果您使用 VLV 索引，请按如下方式设置适当的大小限制。

- 在 Oracle Directory Server Enterprise Edition 上：必须将 `nsslapd-sizelimit` 属性设置为大于等于 50000 或 `-1`。请参见 `idsconfig(1M)` 手册页。
- 在 N2L 服务器上：必须将 `nisLDAPsearchSizelimit` 属性设置为大于等于 50000 或零。有关更多信息，请参见 `NISLDAPmapping(4)` 手册页。

创建 VLV 索引之后，请将其激活，方法是在 Oracle Directory Server Enterprise Edition 服务器上运行带有 `vlvindex` 选项的 `dsadm`。有关更多信息，请参见 `dsadm`(1M) 手册页。

标准映射的 VLV

如果符合以下条件，可以使用 Oracle Directory Server Enterprise Edition 的 `idsconfig` 命令设置 VLV：

- 正在使用 Oracle Directory Server Enterprise Edition。
- 要将标准映射映射到 RFC 2307bis LDAP 项。

VLV 特定于域，因此每次运行 `idsconfig` 时，都会为一个 NIS 域创建相应的 VLV。所以，在 NIS 到 LDAP 的转换过程中，必须对 `NISLDAPmapping` 文件中包含的**每个** `nisLDAPdomainContext` 属性都运行一次 `idsconfig`。

定制映射和非标准映射的 VLV

如果符合以下条件，则必须为映射手动创建新的 Oracle Directory Server Enterprise Edition VLV，或者复制并修改现有的 VLV 索引：

- 正在使用 Oracle Directory Server Enterprise Edition。
- 具有大型定制映射，或者具有映射到非标准 DIT 位置的标准映射。

要查看现有的 VLV 索引，请键入以下命令：

```
% ldapsearch -h hostname -s sub -b "cn=ldbm database,cn=plugins,cn=config" "objectclass=vlvSearch"
```

避免 Oracle Directory Server Enterprise Edition 服务器超时

N2L 服务器在刷新映射时，可能会对 LDAP 目录进行大量访问。如果 Oracle Directory Server Enterprise Edition 的配置不正确，刷新操作可能会因超时而无法完成。要避免目录服务器超时，请手动或者通过运行 `idsconfig` 命令修改以下 Oracle Directory Server Enterprise Edition 属性。

例如，要增加服务器执行搜索请求所需的最短时间（以秒为单位），请修改以下属性：

```
dn: cn=config
nsslapd-timelimit: -1
```

出于测试的目的，您可以使用属性值 `-1`，该值表示没有限制。确定最佳限制值之后，请更改属性值。**请勿**在生产服务器上保留任何值为 `-1` 的属性设置。在没有限制的情况下，服务器可能容易受到拒绝服务攻击。

有关为使用 LDAP 而配置 Oracle Directory Server Enterprise Edition 的更多信息，请参见本书的第 11 章，为使用 LDAP 客户机设置 Oracle Directory Server Enterprise Edition（任务）。

避免 Oracle Directory Server Enterprise Edition 缓冲区溢出

要避免缓冲区溢出，请手动或者通过运行 `idsconfig` 命令修改 Oracle Directory Server Enterprise Edition 属性。

1. 例如，要增加针对客户机搜索查询返回的最大项数，请修改以下属性：

   ```
   dn: cn=config
   nsslapd-sizelimit: -1
   ```
2. 要增加针对客户机搜索查询检验的最大项数，请修改以下属性：

   ```
   dn: cn=config, cn=ldbm database, cn=plugins, cn=config
   nsslapd-lookthroughlimit: -1
   ```

出于测试的目的，您可以使用属性值 `-1`，该值表示没有限制。确定最佳限制值之后，请更改属性值。**请勿**在生产服务器上保留任何值为 `-1` 的属性设置。在没有限制的情况下，服务器可能容易受到拒绝服务攻击。

如果使用 VLV，则应当按照第 224 页中的 “使用 Oracle Directory Server Enterprise Edition 创建虚拟列表视图索引”中的定义设置 `sizelimit` 属性值。如果未使用 VLV，则应当将大小限制设置得足够大，以便可以容纳最大的容器。

有关为使用 LDAP 而配置 Oracle Directory Server Enterprise Edition 的更多信息，请参见第 11 章，为使用 LDAP 客户机设置 Oracle Directory Server Enterprise Edition（任务）。

NIS 到 LDAP 转换的限制

设置 N2L 服务器之后，将不再使用 NIS 源文件。因此，请勿在 N2L 服务器上运行 `ypmake`。如果无意间（例如对于现有的 `cron` 作业）运行了 `ypmake`，N2L 服务不会受到影响。但是，会记录一个警告，提示应当显式调用 `yppush`。

NIS 到 LDAP 转换的故障排除

本节包括两个方面的故障排除：

- 第 226 页中的 “常见的 LDAP 错误消息”
- 第 227 页中的 “NIS 到 LDAP 转换的问题”

常见的 LDAP 错误消息

有时，N2L 服务器会记录与内部 LDAP 问题相关的错误，并生成与 LDAP 相关的错误消息。尽管这些错误不是致命的，但是它们指明有问题需要检查。例如，N2L 服务器可能会继续工作，但是会提供过时或不完整的结果。

以下列表包括一些在实现 N2L 服务时可能遇到的常见 LDAP 错误消息。也包括错误说明、造成这些错误可能的原因和解决方案。

`Administrative limit exceeded`（**超过管理限制**）

错误号： `11`

原因: 执行的 LDAP 搜索大于目录服务器的 `nsslapd-sizelimit` 属性所允许的大小。将仅返回部分信息。

解决方法: 增大 `nsslapd-sizelimit` 属性的值，或者对失败的搜索实施 VLV 索引。

`Invalid DN Syntax`（`DN` **语法无效**）

错误号： `34`

原因: 尝试写入的 LDAP 项的 DN 包含非法字符。N2L 服务器尝试对 DN 中生成的非法字符（如 + 号）转义。

解决方法: 检查 LDAP 服务器错误日志，找出写入的非法 DN，然后修改生成了非法 DN 的 `NISLDAPmapping` 文件。

`Object class violation`（**对象类违规**）

错误号： `65`

原因: 试图写入无效的 LDAP 项。通常，出现此错误是由于缺少 `MUST` 属性，以下任一情况都可能会导致缺少此属性。

- `NISLDAPmapping` 文件中存在导致所创建的项缺少属性的错误

- 尝试向不存在的对象添加 AUXILIARY 属性

  例如，如果仍未从 passwd.byxxx 映射建立用户名，向该用户添加辅助信息的尝试也会失败。

解决方法: 对于 NISLDAPmapping 文件中的错误，检查在服务器错误日志中写入的内容，以确定问题的性质。

Can’t contact LDAP server（**无法联系 LDAP 服务器**）

错误号：85

原因: ypserv 文件可能未正确配置，指向了错误的 LDAP 目录服务器。或者，目录服务器当前可能未运行。

解决方法: 重新配置并确认。

- 重新配置 ypserv 文件，使其指向正确的 LDAP 目录服务器。
- 要确认 LDAP 服务器正在运行，请键入：

```
% ping hostname 5 | grep "no answer" || \
      (ldapsearch -h hostname -s base -b ""  \
      "objectclass=*" >/dev/null && echo Directory accessible)
```

  如果服务器不可用，则会显示以下消息：no answer from *hostname*。如果 LDAP 服务器有问题，则会显示以下消息：ldap_search: Can’t connect to the LDAP server - Connection refused。最后，如果一切正常，则会显示以下消息：Directory accessible。

Timeout（**超时**）

错误号：85

原因: 通常，在从 DIT 更新映射时，LDAP 操作会超时。该映射当前可能包含过时的信息。

解决方法: 在 ypserv 配置文件中增大 nisLDAPxxxTimeout 属性的值。

NIS 到 LDAP 转换的问题

运行 N2L 服务器时可能会出现以下问题。此处提供了可能的原因和解决方案。

调试 NISLDAPmapping 文件

映射文件 NISLDAPmapping 非常复杂。很多潜在的错误可能会导致映射工作不正常。请使用以下技术解决此类问题。

运行 ypserv -ir（或 -Ir）时显示控制台消息

描述: 控制台上显示了一条简单的消息，并且服务器退出（向 syslog 中写入了一条详细描述）。

原因: 映射文件的语法可能不正确。

解决方法: 检查并更正 NISLDAPmapping 文件中的语法。

NIS 守护进程在启动时退出

描述: 运行 ypserv 或其他 NIS 守护进程时，记录了一条与 LDAP 相关的错误消息，并且守护进程退出。

原因: 这可能是下列某一原因造成的：

- 无法联系 LDAP 服务器。
- 在 NIS 映射或 DIT 中找到的项与指定的映射不兼容。
- 尝试对 LDAP 服务器执行读写操作时返回错误。

解决方法: 检查 LDAP 服务器上的错误日志。请参见第 226 页中的 “常见的 LDAP 错误消息”。

NIS 操作产生意外的结果

描述: NIS 操作没有返回预期的结果，但是没有记录错误。

原因: LDAP 或 NIS 映射中可能存在不正确的项，这会导致映射无法按照预期的方式完成。

解决方法: 检查并纠正 LDAP DIT 中以及 N2L 版本的 NIS 映射中的项。

1. 检查 LDAP DIT 中的项是否正确，并根据需要更正这些项。

   如果使用的是 Oracle Directory Server Enterprise Edition，请运行 dsadm startconsole 命令启动管理控制台。

2. 检查 /var/yp 目录中 N2L 版本的 NIS 映射是否包含预期的项，方法是将新生成的映射与原来的映射进行比较。请根据需要更正这些项。

   ```
   # cd /var/yp/domainname
   # makedbm -u test.byname
   # makedbm -u test.byname
   ```

   检查映射的输出时请注意以下情况：

   - 在这两个文件中，各项的顺序可能不同。

     在对输出进行比较之前，请使用 sort 命令。

   - 在这两个文件中，空格的用法可能不同。

     在对输出进行比较之前，请使用 diff -b 命令。

NIS 映射的处理顺序

描述: 发生对象类违规。

原因: 当运行 ypserv -i 命令时，将读取每个 NIS 映射并将其内容写入到 DIT 中。同一个 DIT 对象的属性可以由多个映射创建。通常，通过一个映射来创建该对象的大部分属性，包括该对象的所有 MUST 属性。其他映射则负责创建其他 MAY 属性。

映射是按照 nisLDAPobjectDN 属性在 NISLDAPmapping 文件中的出现顺序来处理的。如果包含 MAY 属性的映射在包含 MUST 属性的映射之前处理，会发生对象类违规。要了解关于该错误的更多信息，请参见第 226 页中的 “常见的 LDAP 错误消息”中的错误 65。

解决方法: 将 nisLDAPobjectDN 属性重新排序，以便按照正确的顺序处理这些映射。

临时解决方法是多次重新运行 ypserv -i 命令。每次执行该命令，都会增加更多的 LDAP 项。

注 – 如果映射方式会导致不能从至少一个映射创建某个对象的所有 MUST 属性，则不支持以这种方式进行映射。

N2L 服务器超时问题

服务器超时。

原因: N2L 服务器在刷新映射时，可能会对 LDAP 目录进行大量访问。如果 Oracle Directory Server Enterprise Edition 的配置不正确，该操作可能会因超时而无法完成。

解决方法: 要避免目录服务器超时，请手动或者通过运行 idsconfig 命令修改 Oracle Directory Server Enterprise Edition 属性。有关详细消息，请参见第 226 页中的 “常见的 LDAP 错误消息”和第 223 页中的 “使用 Oracle Directory Server Enterprise Edition 进行 NIS 到 LDAP 转换的最佳做法”。

N2L 锁定文件问题

ypserv 命令启动，但未响应 NIS 请求。

原因: N2L 服务器锁文件没有正确同步对 NIS 映射的访问权限。这种情况绝对不应发生。

解决方法: 在 N2L 服务器上键入以下命令：

```
# svcadm disable network/nis/server:default
# rm /var/run/yp_maplock /var/run/yp_mapupdate
# svcadm enable network/nis/server:default
```

N2L 死锁问题

N2L 服务器死锁。

原因: 如果 hosts、ipnodes 或 ypserv 文件中未正确列出 N2L 主服务器和 LDAP 服务器的地址，则可能会出现死锁问题。请参见第 216 页中的 “NIS 到 LDAP 转换的先决条件”，了解关于 N2L 正确地址配置的详细信息。

有关死锁情况的示例，请考虑以下一系列事件：

1. 一台 NIS 客户机试图查找一个 IP 地址。
2. N2L 服务器发现 `hosts` 项已过时。
3. N2L 服务器尝试从 LDAP 更新 `hosts` 项。
4. N2L 服务器从 `ypserv` 获取其 LDAP 服务器的名称，然后使用 `libldap` 进行搜索。
5. `libldap` 尝试通过调用名称服务转换，将 LDAP 服务器名称转换为 IP 地址。
6. 名称服务转换可能会对 N2L 服务器进行 NIS 调用，而服务器死锁。

解决方法: 在 N2L 主服务器上的 `hosts` 或 `ipnodes` 文件中列出 N2L 主服务器和 LDAP 服务器的地址。必须将服务器地址列在 `hosts`、`ipnodes` 还是同时列在这两个文件中，取决于这些文件配置为以何种方式解析本地主机名。另外，请检查 `svc:/network/name-service/switch` 服务的 `config/hosts` 属性在查找顺序中是否将 `files` 列在了 `nis` 之前。

此死锁问题的另一种解决方案是在 `ypserv` 文件中列出 LDAP 服务器的地址，而不是其主机名。这意味着 LDAP 服务器地址将列在其他位置。因此，更改 LDAP 服务器或 N2L 服务器的地址会使工作量稍有增加。

恢复为 NIS

已使用 N2L 服务从 NIS 转换到 LDAP 的站点将会逐步使用 LDAP 命名服务客户机替换所有的 NIS 客户机。对 NIS 客户机的支持最终会成为多余。但是，N2L 服务提供了两种在必要时返回传统 NIS 的方法，如以下两个过程中所述。

提示 – 传统的 NIS 会忽略 N2L 版本的 NIS 映射（如果存在这些映射）。恢复为 NIS 之后，如果在服务器上保留 N2L 版本的这些映射，则 N2L 映射不会产生问题。因此，如果您以后决定重新启用 N2L，则保留 N2L 映射可能会非常有用。但是，这些映射确实会占用磁盘空间。

▼ 如何基于旧的源文件恢复到 NIS 映射

1 成为管理员。

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 停止 NIS 守护进程。

```
# svcadm disable network/nis/server:default
```

3 禁用 N2L。

此命令可备份并移动 N2L 映射文件。

```
# mv /var/yp/NISLDAPmapping backup_filename
```

4 设置 NOPUSH 环境变量，以便 ypmake 不会推送新映射。

```
# NOPUSH=1
```

5 创建一组基于旧源的新 NIS 映射。

```
# cd /var/yp
# make
```

6 （可选）删除 N2L 版本的 NIS 映射。

```
# rm /var/yp/domainname/LDAP_*
```

7 启动 DNS 和 NIS 服务。

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

▼ 如何基于当前的 DIT 内容恢复为 NIS 映射

执行此过程之前请先备份旧的 NIS 源文件。

1 成为管理员。

有关更多信息，请参见《Oracle Solaris 11.1 管理：安全服务》中的“如何使用指定给您的管理权限”。

2 停止 NIS 守护进程。

```
# svcadm disable network/nis/server:default
```

3 从 DIT 更新映射。

```
# ypserv -r
```

等待 ypserv 退出。

4 禁用 N2L。

此命令可备份并移动 N2L 映射文件。

```
# mv /var/yp/NISLDAPmapping backup_filename
```

5 重新生成 NIS 源文件。

```
# ypmap2src
```

6 手动检查重新生成的 NIS 源文件是否具有正确的内容和结构。

7 将重新生成的 NIS 源文件移到适当的目录中。

8 （可选）删除 N2L 版本的映射文件。

```
# rm /var/yp/domainname/LDAP_*
```

9 启动 DNS 和 NIS 服务。

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

词汇表

application-level naming service（应用程序级命名服务） 应用程序级命名服务包含在可提供文件、邮件和打印等服务的应用程序中。应用程序级命名服务绑定在企业级命名服务之下。企业级命名服务提供上下文，应用程序级命名服务的上下文可以绑定在该上下文中。

attribute（属性） 每个 LDAP 项都由许多命名**属性**组成，每个属性都具有一个或多个值。

另外，每个 N2L 服务映射和配置文件也包括许多命名**属性**。每个属性均具有一个或多个值。

authentication（验证） 服务器可以用来验证客户机的标识的手段。

baseDN 作为部分 DIT 的根元素的 DN。如果是 NIS 域项的 baseDN，它又称为**上下文**。

client-server model（客户机/服务器模型） 用来描述网络服务和这些服务的典型用户进程（程序）的一种常用方法。例如，**域名系统** *(Domain Name System, DNS)* 名称服务器/名称解析程序模式。另请参见 *client*（**客户机**）。

client（客户机） (1) 客户机是从命名服务器请求命名服务的主体（计算机或用户）。

(2) 在用于文件系统的客户机/服务器模型中，客户机是远程访问计算服务器资源（如计算能力和大容量内存）的计算机。

(3) 在客户机/服务器模型中，客户机是从“服务器进程”访问服务的**应用程序**。在该模型中，客户机和服务器可以在同一台计算机上运行，也可以在不同的计算机上运行。

context（上下文） 对于 N2L 服务，上下文是 NIS 域通常映射到其下的某种环境。另请参见 baseDN。

credentials（凭证） 客户机软件随每个请求一起发送到命名服务器的验证信息。这些信息用于验证用户或计算机的身份。

data encrypting key（数据加密密钥） 用于对数据进行加密和解密的密钥，适用于执行加密的程序。与**密钥加密密钥**相对。

data encryption standard, DES（数据加密标准） 一种极其复杂的常用算法，由美国国家标准局开发，用于对数据进行加密和解密。另请参见 SUN-DES-1。

databaseID 对于 N2L 服务，databaseID 是包含具有相同格式的 NIS 条目（具有到 LDAP 的相同映射）的映射组的别名。映射可能具有不同的密钥。

DBM DBM（数据库管理）是一种数据库，最初用于存储 NIS 映射。

decimal dotted notation（点分十进制表示法） 32 位整数的语法表示形式，它包含四个以 10 进制表示的 8 位数字，数字之间用句点（点）分隔。用于将 Internet 中的 IP 地址表示为类似于 192.67.67.20 的形式。

DES 请参见 *data encryption standard, DES*（**数据加密标准**）。

directory cache（目录高速缓存） 一个本地文件，用于存储与目录对象相关联的数据。

directory information tree（目录信息树） DIT 是指给定网络的分布式目录结构。缺省情况下，客户机在访问信息时会假设 DIT 具有给定的结构。LDAP 服务器支持的每个域都有一个具有假设结构的假设子树。

directory（目录） (1) LDAP 目录是 LDAP 对象的容器。在 UNIX 中，目录是文件和子目录的容器。

distinguished name（标识名） 标识名是 X.500 目录信息库 (directory information base, DIB) 中的项，由沿根目录直至指定项的路径，从树中每一项选择的属性组成。

DIT 请参见 directory information tree（目录信息树）。

DN LDAP 中的一个标识名。LDAP 目录的树状结构化寻址方案，它赋予每个 LDAP 项一个唯一的名称。

DNS 请参见 *Domain Name System*（**域名系统**）。

DNS-forwarding（DNS 转发） NIS 服务器将它无法应答的请求转发到 DNS 服务器。

DNS zone files（DNS 区域文件） 一组文件，DNS 软件将域中所有工作站的名称和 IP 地址存储在其中。

DNS zones（DNS 区域） 网络域中的管理范围，通常由一个或多个子域组成。

domain name（域名） 指定给本地网络上一组共享 DNS 管理文件的系统的名称。必须要有域名，网络信息服务数据库才能正常工作。另请参见 *domain*（**域**）。

Domain naming service, DNS（域名服务） 一种服务，它提供的命名策略和机制用于将域名和计算机名映射为企业外部地址（如 Internet 上的地址）。DNS 是由 Internet 使用的网络信息服务。

domain（域） (1) 在 Internet 中，命名分层结构的一部分通常对应于一个局域网 (Local Area Network, LAN) 或广域网 (Wide Area Network, WAN) 或这类网络的一部分。从语法上来说，Internet 域名由一系列用句点（点）分隔的名称（标签）组成。例如，`sales.example.com`。

(2) 在国际标准化组织的开放系统互连 (open systems interconnection, OSI) 中，“域”通常用作复杂分布式系统的管理分区，正如在 MHS 专用管理域 (private management domain, PRMD) 和目录管理域 (directory management domain, DMD) 中一样。

encryption key（加密密钥） 请参见 *data encrypting key*（**数据加密密钥**）。

encryption（加密） 用来保护数据的私密性的手段。

enterprise-level network（企业级网络） “企业级”网络可以是通过电缆、红外线光束或无线电广播进行通信的单个局域网 (Local Area Network, LAN)；也可以是通过电缆或直接电话连线链接到一起的两个或多个 LAN 的群集。在企业级网络中，每台计算机都能在不引用全局命名服务（如 DNS 或 X.500/LDAP）的情况下与任何其他计算机进行通信。

entry（项） 数据库表中的一行数据，如 DIT 中的一个 LDAP 元素。

field（字段） 一个 NIS 映射项可能由许多组成部分和分隔符组成。在 N2L 服务映射过程中，该项将首先被分解为许多命名**字段**。

GID 请参见 *group ID*（**组** *ID*）。

global naming service（全局命名服务） 全局命名服务标识全球的企业级网络，这些网络通过电话、卫星或其他通信系统连接在一起。这个连接在一起的全球网络集合称为 "Internet"。除了命名网络，全局命名服务还可标识给定网络内的单台计算机和单个用户。

group ID（组 ID） 一个数字，用于标识用户的缺省**组**。

indexed name（索引名） 用于标识表中的项的命名格式。

Internet address（Internet 地址） 指定给使用 *TCP/IP* 的主机的 32 位地址。请参见 *decimal dotted notation*（**点分十进制表示法**）。

IP Internet 协议。Internet 协议套件的**网络层**协议。

IP address（IP 地址） 用于标识网络中的每台主机的一个唯一数字。

key (encrypting)（加密密钥） 用于对其他密钥进行加密和解密的密钥，它是密钥管理和分发系统的一部分。与 *data encrypting key*（**数据加密密钥**）相对。

key server（密钥服务器） 用于存储私钥的 Oracle Solaris 操作环境进程。

LDAP 轻量目录访问协议是一种标准的、可扩展的目录访问协议，它由 LDAP 命名服务客户机和服务器用于进行相互通信。

local-area network, LAN（局域网） 位于同一地理位置的多个系统，为了共享和交换数据及软件而连接在一起。

mail exchange records（邮件交换记录） 一些文件，其中包含 DNS 域名及其对应邮件主机的列表。

mail hosts（邮件主机） 一个工作站，充当站点的电子邮件路由器和接收器。

mapping（映射） 将 NIS 项与 DIT 项相互转换的过程。此过程由**映射**文件控制。

master server（主服务器） 维护着特定域的网络信息服务数据库主副本的服务器。名称空间更改总是针对由域的主服务器保存的命名服务数据库进行。每个域都只有**一台**主服务器。

MIS 管理信息系统（或服务）。

N2L server（N2L 服务器） NIS 到 LDAP 转换服务器。已使用 N2L 服务重新配置为 N2L 服务器的 NIS 主服务器。重新配置过程包括替换 NIS 守护进程和添加新配置文件。

name resolution（名称解析） 将工作站名称或用户名转换为地址的过程。

name server（名称服务器） 运行一个或多个网络命名服务的服务器。

name service switch（名称服务转换） `svc:/system/name-service/switch` 服务，它定义了命名客户机可以从中获取其网络信息的源。

namespace（名称空间） (1) 名称空间存储着用户、工作站和应用程序在网络中进行通信时必须使用的信息。

(2) 命名系统中所有名称的集合。

naming service（命名服务） 一项网络服务，用于处理计算机、用户、打印机、域、路由器名称以及其他网络名称和地址。

NDBM NDBM（新数据库管理）是 DBM 的改进版本。

network mask（网络掩码） 一个数字，软件用它将本地子网地址与给定 Internet 协议地址的其余部分分开。

network password（网络口令） 请参见 Secure RPC password（安全 RPC 口令）。

NIS 一种分布式网络信息服务，其中包含有关网络上的系统和用户的关键信息。NIS 数据库存储在**主服务器**和全部**副本服务器**或**从属服务器**上。

NIS maps（NIS 映射） 供 NIS 使用的一个文件，它包含特定类型的信息，例如，网络上的所有用户的口令项或网络上的所有主机的名称。作为 NIS 服务一部分的程序会查询这些映射。另请参见 *NIS*。

preferred server list（首选服务器列表） 一个 `client_info` 表或一个 `client_info` 文件。首选服务器列表为客户机或域指定首选服务器。

private key（私钥） 以数学方法生成的一对数字中的专用部分，在与私钥合并时，可生成 DES 密钥。DES 密钥又可用于对信息进行编码和解码。发件人的私钥只能由密钥的所有者使用。每个用户或每台计算机都有其各自的公钥/私钥对。

public key（公钥） 以数学方法生成的一对数字中的公用部分，在与私钥合并时，可生成 DES 密钥。DES 密钥又可用于对信息进行编码和解码。公钥对所有的用户和计算机公开。每个用户或每台计算机都有其各自的公钥/私钥对。

RDN 相对标识名。DN 的一部分。

record（记录） 请参见 *entry*（**项**）。

remote procedure call, RPC（远程过程调用） 一种易于使用的常见模式，用于实现客户机/服务器分布式计算模型。使用所提供的参数向远程系统发送请求，以执行指定的过程，结果将返回到调用者。

reverse resolution（反向解析） 使用 DNS 软件将工作站 IP 地址转换为工作站名称的过程。

RFC 2307 RFC 的一部分，指定将信息从标准 NIS 映射映射到 DIT 项。缺省情况下，N2L 服务实现更新版本 RFC 2307bis 中指定的映射。

RPC 请参见 remote procedure call, RPC（远程过程调用）。

SASL 简单验证和安全层。用于在应用层协议中协商验证和安全层语义的框架。

schema（架构） 一个规则集合，它定义了在任意给定的 LDAP DIT 中可以存储什么类型的数据。

searchTriple 一种说明，描述从 DIT 中的什么位置查找给定属性。searchTriple 由“基本 DN”、“范围”和“过滤器”组成。这是在 RFC 2255 中定义的 LDAP URL 格式的一部分。

Secure RPC password（安全 RPC 口令） 安全 RPC 协议所需的口令。此口令用于对私钥进行加密。此口令应当始终与用户的登录口令相同。

server list（服务器列表） 请参见 *preferred server list*（**首选服务器列表**）。

server（服务器） (1) 在 NIS、DNS 和 LDAP 系统中，它是为网络提供命名服务的主机。

(2) 在用于文件系统的**客户机/服务器模型**中，服务器是具有大容量内存和计算资源的计算机（有时称为计算服务器）。客户机可以远程访问和使用这些资源。在用于窗口系统的客户机/服务器模型中，服务器是为应用程序提供窗口服务的进程或“客户机进程”。在该模型中，客户机和服务器可以在同一台计算机上运行，也可以在不同的计算机上运行。

(3) 实际负责提供文件的**守护进程**。

slave server（从属服务器） 用于维护 NIS 数据库副本的服务器系统。它包含磁盘以及操作环境的完整副本。

source（源） NIS 源文件

SSL SSL 是指安全套接字层协议。它是通用的传输层安全机制，旨在使应用协议（如 LDAP）更加安全。

subnet（子网） 一种工作方案，它将单个逻辑网络划分为较小的物理网络以简化路由。

suffix（后缀） 在 LDAP 中，为 DIT 的标识名 (distinguished name, DN)。

TCP 请参见 *Transport Control Protocol, TCP*（**传输控制协议**）。

TCP/IP 传输控制协议/接口程序 (Transport Control Protocol/Interface Program) 的首字母缩略词。最初为 Internet 开发的协议套件。它还称作 *Internet* 协议套件。Oracle Solaris 网络缺省情况下运行 TCP/IP 协议。

Transport Control Protocol, TCP（传输控制协议） Internet 协议套件中的主要传输协议，用于提供可靠的、面向连接的全双工数据流。使用 IP 传送信息。请参见 TCP/IP。

Transport Layer Security, TLS（传输层安全性）	TLS 保护 LDAP 客户机与目录服务器之间的通信的安全，提供保密性和数据完整性。TLS 协议是一组绝佳的安全套接字层 (Secure Sockets Layer, SSL) 协议。
wide-area network, WAN（广域网）	一种网络，通过电话、光纤或卫星链路连接位于不同地理位置的多个局域网 (local-area network, LAN) 或系统。
X.500	由开放系统互连 (Open Systems Interconnection, OSI) 标准定义的全局级目录服务。LDAP 的前身。
yp	黄页。NIS 的旧名，仍用在 NIS 代码中。

索引

I

K

L

M

O

P

R

邮

域

源

帐

主

子

字

组