使用 Oracle® Solaris 11.2 目录和命名服务：LDAP

文件号码 E53903
2014 年 7 月

ORACLE

目录

使用此文档

- **概述** – 介绍 LDAP 命名服务、规划其使用的方法以及实施 LDAP 的步骤。
- **目标读者** – 系统管理员。
- **必要知识** – 熟悉与 LDAP 相关的概念和术语。

产品文档库

有关本产品的最新信息和已知问题均包含在文档库中，网址为：http://www.oracle.com/pls/topic/lookup?ctx=E36784。

获得 Oracle 支持

Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

反馈

可以在 http://www.oracle.com/goto/docfeedback 上提供有关此文档的反馈。

♦ ♦ ♦ 第 1 章

1 LDAP 命名服务简介

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。

注 - LDAP 这一术语更多指的是命名服务而非该协议本身。本书中，术语 LDAP 用于指服务而非协议。

有关背景阅读资料，请参见以下来源：

- *Oracle Directory Server Enterprise Edition*
- *Oracle Directory Server Enterprise Edition Administration Guide*
- 所用 Oracle Directory Server Enterprise Edition 版本的安装指南

本章对 LDAP 服务进行了概述。

此 Oracle Solaris 发行版中的 LDAP

在 Oracle Solaris 11.2 中，在现有的 Oracle Solaris RBAC 架构中添加了 `SolarisQualifiedUserAttr` 对象类。此类具有可为其指定多个值的属性，从而增强了当前的 `SolarisUserQualifier` 类。要查看具有新对象类的修改后 RBAC 架构，请参阅“基于角色的访问控制和执行配置文件架构” [86]。

如果在推出 `SolarisQualifiedUserAttr` 类之前您已经有了现成的 LDAP 配置，则可通过使用 `ldapadd` 命令将该类添加到该配置中。

LDAP 命名服务的概述

Oracle Solaris 支持将 LDAP 与 Oracle Directory Server Enterprise Edition（以前称为 Sun Java System Directory Server）结合使用。但是，任何常规目录服务器都可充当 LDAP 服务器。本书中，术语目录服务器和 *LDAP* 服务器同义，可互换使用。

LDAP 命名服务是 Oracle Solaris 中支持的不同命名服务之一。《使用 Oracle Solaris 11.2 目录和命名服务：DNS 和 NIS》 介绍了其他命名服务。有关 Oracle Solaris 中不同命名服务的比较，请参见“比较：LDAP 命名服务与其他命名服务” [11]。

LDAP 可执行以下服务：

- 命名服务 – LDAP 可根据客户机请求提供命名数据。例如，在解析主机名时，LDAP 类似于 DNS，可提供全限定域名。假设域名为 `west.example.net`。如果应用程序使用 `gethostbyname()` 或 `getnameinfo()` 请求主机名，则 LDAP 将返回值 *server*`.west.example.net`。
- 验证服务 – LDAP 管理并提供有关客户机标识、验证和帐户的信息。因此，LDAP 将实施安全措施，以便仅向授权请求者提供信息。

LDAP 命名服务具有以下优点：

- 通过替代特定于应用程序的数据库，整合了信息，减少了要管理的独立数据库数量。
- 数据可由不同的命名服务共享。
- 使用了集中的系统信息库来存储数据。
- 可在主服务器和副本服务器之间更频繁地执行数据同步。
- LDAP 可兼容多种平台以及由多个供应商提供的产品。

LDAP 命名服务具有以下限制：

- LDAP 服务器不能作为其自身的客户机。
- 客户机不能同时是 NIS 和 LDAP 的客户机。

注 - 由于缺少限制，设置和管理 LDAP 命名服务比较复杂，需要仔细规划。

LDAP 如何存储信息

LDAP 所提供的信息存储在目录信息树 (Directory Information Tree, DIT) 中。数据本身采用 LDAP 数据交换格式 (LDAP Data Interchange Format, LDIF)。DIT 由多个具有层次结构的信息容器组成，这些信息容器使用定义的 LDAP 架构。

通常，大多数 DIT 所使用的缺省架构可满足使用 LDAP 的大多数网络的要求。但是，DIT 非常灵活。您可以通过在客户机配置文件中指定搜索描述符来覆盖 DIT 的缺省结构。有关搜索描述符的更多讨论，请参见“服务搜索描述符和架构映射” [32]。

下表显示了 DIT 的容器以及每个容器存储的信息类型。

表 1-1 缺省 DIT 容器中的信息类型

缺省容器	信息类型
`ou=Ethers`	`bootparams`、`ethers`

缺省容器	信息类型
ou=Group	group
ou=Hosts	hosts、ipnodes、publickey（对于主机）
ou=Aliases	aliases
ou=Netgroup	netgroup
ou=Networks	networks, netmasks
ou=People	passwd、shadow、user_attr、audit_user、publickey（对于用户）
ou=Protocols	protocols
ou=Rpc	rpc
ou=Services	services
ou=SolarisAuthAttr	auth_attr
ou=SolarisProfAttr	prof_attr, exec_attr
ou=projects	project
automountMap=auto_*	auto_*（自动挂载映射）

比较：LDAP 命名服务与其他命名服务

除了 LDAP 命名服务，还会经常使用其他类型的命名服务。

下表显示了每种命名服务的功能比较。这些服务在 Oracle Solaris 中均受支持。

表 1-2 命名服务的功能比较

	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	全部	全部	全部

LDAP 命令

Oracle Solaris OS 提供两个与 LDAP 相关的命令集。第一个命令集由常规 LDAP 命令组成，需要配置 LDAP 命名服务。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。

在以下各节中，在列出命令时也指明了其对应的手册页。

常规 LDAP 命令

常规 LDAP 命令可在任意系统上运行，无需在系统中配置 LDAP 命名服务。LDAP 命令行工具支持一组通用选项（包括验证和绑定参数）。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)。您可以使用以下命令直接处理目录项：

命令	说明	手册页
`ldapsearch`	在 LDAP 架构中搜索指定的项。	`ldapsearch(1)`
`ldapmodify`	修改架构中的 LDAP 项。	`ldapmodify(1)`
`ldapadd`	添加架构中的 LDAP 项。	`ldapadd(1)`
`ldapdelete`	从架构中删除 LDAP 项。	`ldapdelete(1)`

特定于 LDAP 操作的 LDAP 命令

下表列出了可配置客户机系统或要求客户机系统进行配置的 LDAP 命令。

命令	说明	手册页
`ldapaddent`	在来自相应 `/etc` 文件的架构中创建 LDAP 项。	`ldapaddent(1M)`
`ldaplist`	显示从 LDAP 服务器中检索的信息。	`ldaplist(1)`
`idsconfig`	向 DIT 置备数据以为客户机提供服务。	`idsconfig(1M)`
`ldapclient`	初始化 LDAP 客户机。	`ldapclient(1M)`

♦ ♦ ♦ 第 2 章

2 LDAP 和验证服务

LDAP 命名服务能够以两种方式使用 LDAP 系统信息库。

- 同时用作命名服务和验证服务的源
- 仅限于作为命名数据的源

本章专门讨论了 LDAP 的验证服务，并涵盖以下主题：

LDAP 命名服务安全模型

LDAP 支持验证和受控制访问等安全功能，以确保客户机所获取的信息的完整性和保密性。

要访问 LDAP 系统信息库中的信息，客户机首先要向目录服务器表明其身份。该身份可以是匿名的，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身份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。

验证可以是以下两种类型之一：

- 代理验证，意味着身份基于生成请求的主机。在主机通过验证后，该主机上的所有用户都可以访问目录服务器。
- 每用户验证，意味着身份基于每个用户。每个用户都必须通过验证才能访问目录服务器并发出各种 LDAP 请求。

可插拔验证模块 (pluggable authentication module, PAM) 服务用于确定用户登录是否成功。验证的基础因所使用的 PAM 模块而异，如以下列表所示：

- pam_krb5 模块 – Kerberos 服务器是验证的基础。有关此模块的更多信息，请参见 pam_krb5(5) 手册页。另请参见《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务》，其中对 Kerberos 的讨论比本指南更为广泛。
- pam_ldap 模块 – LDAP 服务器和本地主机用作验证的基础。有关此模块的更多信息，请参见 pam_ldap(5) 手册页。要使用 pam_ldap 模块，请参见 “LDAP 帐户管理” [23]。
- pam_unix_* 等效模块 – 信息由主机提供，验证由本地确定。

注 - pam_unix 模块已被删除，Oracle Solaris 将不再支持该模块。该模块已由一组功能相同或功能更强的其他服务模块所取代。在本指南中，pam_unix 是指提供相同功能的模块，而非 pam_unix 模块本身。

如果使用的是 pam_ldap，命名服务和验证服务将以不同的方式访问目录。

- 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。
- 验证服务将使用 LDAP 服务器验证用户名和口令，以确定是否已指定了正确的口令。

可以同时使用 Kerberos 和 LDAP 向网络提供验证服务和命名服务。通过 Kerberos，可以在您的企业中支持单点登录 (single sign on, SSO) 环境。同一个 Kerberos 标识系统也可用于基于每个用户或基于每个主机来查询 LDAP 命名数据。

如果使用 Kerberos 执行验证，则根据每用户模式的要求，也必须启用 LDAP 命名服务。然后 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

可以使用传输层安全 (transport layer security, TLS) 来保护 LDAP 客户机与目录服务器之间的通信安全，从而确保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。但是，使用 SSL 会增加目录服务器和客户机的负荷。

以下列出了使用 TLS 的各种要求：

- 为 SSL 配置目录服务器和 LDAP 客户机。

  要为 SSL 配置 Oracle Directory Server Enterprise Edition，请参见您使用的 Oracle Directory Server Enterprise Edition 版本的管理指南。
- 安装必要的安全数据库，特别是证书和密钥数据库文件。
  - 如果您使用来自 Netscape Communicator 的较旧的数据库格式，请安装 cert7.db 和 key3.db。

- 如果您使用来自 Mozilla 的较新的数据库格式，请安装 `cert8.db`、`key3.db` 和 `secmod.db`。

`cert*` 文件包含可信证书。`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，也必须安装 `key3.db` 文件。`secmod.db` 文件中包含安全模块，如 `PKCS#11` 模块。

要设置 TLS 安全性，请参见“设置 TLS 安全性” [64]。

客户机凭证级别

LDAP 服务器将根据客户机凭证级别验证 LDAP 客户机。可以为 LDAP 客户机指定以下凭证级别之一：

`anonymous`

使用 `anonymous` 凭证级别，仅可以访问对所有人可用的数据。不会发生 LDAP BIND 操作。

anonymous 凭证级别的安全风险很高。任何客户机都可以更改 DIT 中的、客户机对其具有写入权限的信息，包括其他用户的口令或其自己的身份。另外，`anonymous` 级别会使所有客户机对所有 LDAP 命名服务和属性具有读取权限。

注 - Oracle Directory Server Enterprise Edition 使您能够基于 IP 地址、DNS 名称、验证方法和一天中的时段对访问进行限制。这样，您就可以实施安全措施。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”。

`proxy`

使用 `proxy` 凭证级别，客户机将绑定到一组共享的 LDAP 绑定凭证。共享的一组凭证也称为代理帐户。此代理帐户可以是任何允许绑定到目录的条目。此帐户需要有足够的访问权限以在 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，这意味着使用代理访问权限登录到系统的用户（包括 root 用户）都将看到相同的信息。您必须在使用 `proxy` 凭证级别的每个客户机系统上配置 `proxyDN` 和 `proxyPassword` 属性。另外，`proxyDN` 必须在所有服务器上具有相同的 `proxyPassword`。

经过加密的 `proxyPassword` 存储在客户机本地。如果某个代理用户的口令发生了更改，您必须在使用该代理用户的每个客户机系统上更新该口令。此外，如果您对 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。

您可以为不同的客户机组设置不同的代理。例如，您可以配置一个代理，限制所有销售客户机只能访问公司范围内可访问的目录和销售目录。禁止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。

如果计划为不同的客户机设置多个代理，请仔细考虑各种选择。代理太少可能会限制您对用户的资源访问权限的控制能力。但是，代理太多，又会增大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“LDAP 客户机的凭证存储” [17]。

proxy 凭证级别适用于任何特定系统上的所有用户和进程。需要使用不同命名策略的用户必须登录到不同的系统，或使用每用户验证模型。

`proxy anonymous`

`proxy anonymous` 凭证级别是一个多值条目，它定义了多个凭证级别。使用此级别时，指定的客户机将首先尝试使用其代理标识进行验证。如果验证失败，例如由于用户锁定或口令失效，则客户机将使用匿名访问方式。根据目录的配置情况，不同的凭证级别可能会与不同的服务级别相关联。

`self`

`self` 凭证级别也称为每用户模式。此模式使用 Kerberos 标识（称为主体）针对每个系统或用户执行查找，以进行验证。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。

要使用每用户验证模式，必须具备以下条件：

- 部署 Kerberos 单点登录服务
- 支持在一个或多个目录服务器中使用 SASL 和 SASL/GSSAPI 验证机制
- 配置 DNS，Kerberos 将结合使用 DNS 和文件来执行主机名查找
- 启用 `nscd` 守护进程

`enableShadowUpdate` 开关

如果在客户机上 `enableShadowUpdate` 开关设置为 `true`，则将使用管理员凭证来更新影子数据。阴影数据存储在目录服务器上的 `shadowAccount` 对象类中。管理员凭证是由 `adminDN` 和 `adminPassword` 属性的值定义的，如“定义本地客户机属性” [59]中所述。

管理员凭证具有与 `proxy` 凭证类似的属性。但是，对于管理员凭证，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。

注意 - 管理员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`)。

具有管理员凭证的条目必须具有足够的访问权限才能读取影子数据并将其写入目录。此条目是一个按系统共享的资源。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。特定系统上的所有用户和进程都将使用管理员凭证来读取和更新影子数据。

LDAP 客户机的凭证存储

在当前 LDAP 实现中，初始化期间设置的代理凭证存储在 SMF 系统信息库中，而非客户机配置文件中。这种实现方式提高了针对代理的标识名 (distinguished name, DN) 和口令信息的安全性。

SMF 系统信息库为 svc:/network/ldap/client。它存储着使用代理标识的客户机的代理信息。同样，凭证级别不是 self 的客户机的影子数据更新也将保存在此系统信息库中。

对于使用每用户验证模式的客户机，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。目录服务器将 Kerberos 主体映射到一个 DN，并使用 Kerberos 凭证向该 DN 证明身份。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。

在此环境中，Kerberos 票证信息用于向目录服务器证明身份。系统不存储验证 DN 或口令。因此，当使用 ldapclient 命令初始化客户机时，无需设置 adminDN 和 adminPassword 属性。

LDAP 命名服务的验证方法

为客户机指定 proxy 或 proxy-anonymous 凭证级别时，还必须选择对代理进行验证的方法。缺省情况下，验证方法是 none，它表示匿名访问。验证方法可能还有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。在这种情况下，可以按如下方式配置 authenticationMethod 属性：tls:simple;sasl/digest-MD5。

LDAP 命名服务支持某些简单验证和安全层 (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，请在 IETF Web 站点 (http://datatracker.ietf.org/)中搜索 RFC 4422。

支持的验证机制如下所示：

none　　客户机不向目录证明身份。此方法等效于 anonymous 凭证级别。

`simple` 客户机系统通过以明文形式发送用户口令，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。`digest-MD5` 的主要优点在于，在验证期间，口令不会以明文形式发送，比 `simple` 验证方法更安全。有关 `digest-MD5` 的信息，请在 IETF Web 站点 (http://datatracker.ietf.org/)中搜索 RFC 2831。`digest-MD5` 是 `cram-MD5` 的改进。

使用 `sasl/digest-MD5` 时，验证过程是安全的，但会话不受保护。

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` LDAP 会话不会加密，但是客户机的口令在验证期间会受到保护。不要使用这种过时的验证方法。

`sasl/GSSAPI` 此验证方法与“每用户”模式一起使用可启用“每用户”查找。使用客户机凭证的每用户模式的 `nscd` 会话将通过使用 `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，且会话将加密。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 - 要使用 `digest-MD5`，Oracle Directory Server Enterprise Edition 要求口令以未加密的形式存储。使用 `sasl/digest-MD5` 或 `tls:sasl/digest-MD5` 验证方法的代理用户的口令必须以未加密的形式存储。在这种情况下，请为 `userPassword` 属性配置正确的 ACI 以防止其可读。

下表概述了各种验证方法及其各自的特征。

表 2-1 验证方法

方法	绑定	线路上的口令	Oracle Directory Server Enterprise Edition 上的口令	会话
`none`	否	不适用	不适用	无加密

方法	绑定	线路上的口令	Oracle Directory Server Enterprise Edition 上的口令	会话
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	不适用	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	不适用	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

serviceAuthenticationMethod 属性确定针对特定服务的验证方法。如果没有为服务设置此属性，则将使用 authenticationMethod 属性的值。

如果 enableShadowUpdate 开关设置为 true，ldap_cachemgr 守护进程也将遵循相同的顺序来绑定到 LDAP 服务器：如果未配置 serviceAuthenticationMethod 属性，则使用 authenticationMethod 属性的值。守护进程不会使用 none 验证方法。

您可以为以下服务选择验证方法：

- passwd-cmd – 由 passwd 命令用来更改登录口令和口令属性。有关详细信息，请参见 passwd(1) 手册页。
- keyserv – 由 chkey 和 newkey 实用程序用来创建和更改用户的 Diffie-Hellman 密钥对。有关详细信息，请参阅 chkey(1) 和 newkey(1M) 手册页。
- pam_ldap – 用于验证使用 pam_ldap 服务的用户。pam_ldap 支持帐户管理。

注 - 在每用户模式下，Kerberos 服务模块用作验证服务并且无需使用 ServiceAuthenticationMethod。

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 来向目录服务器证明身份，但会使用 SSL 会话更改口令。

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

可插拔验证方法

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。

要使用每用户验证，则必须启用 pam_krb5。但是，即使没有指定每用户凭证级别，仍可以使用 pam_krb5 验证。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来限制对目录数据的访问。

如果选择了 anonymous 或 proxy 验证，请使用 pam_ldap 模块而非等效的 pam_unix_* 模块。pam_ldap 模块更灵活，支持更强的验证方法并可以执行帐户管理。

LDAP 服务模块

如前文所述，如果定义了 serviceAuthenticationMethod 属性，则该属性将确定用户绑定到 LDAP 服务器的方式。否则，将使用 authenticationMethod 属性。使用用户标识和所提供的口令将 pam_ldap 模块成功绑定到服务器之后，该模块将对用户进行验证。

注 - 以前在使用 pam_ldap 帐户管理时，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 等工具进行非基于口令的登录将失败。

在用户登录时，您现在可以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制为 1.3.6.1.4.1.42.2.27.9.5.8。缺省情况下，此控制处于启用状态。要修改缺省控制配置，请在目录服务器上添加访问控制指令 (access control instruction, ACI)。例如：

```
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 模块不读取 userPassword 属性。如果没有客户机使用 UNIX 验证，则无需授予对 userPassword 属性的读取权限。同样，该模块不支持将 none 作为验证方法。

注意 - 如果使用 simple 验证方法，userPassword 属性可能会以未加密的方式被第三方读取。

下表汇总了各种验证机制之间的主要区别。

表 2-2 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
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。口令不以未加密形式存储。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) 手册页和 Kerberos V5 帐户管理模块。

pam_unix_* 服务模块

如果未配置 /etc/pam.conf 文件，则缺省情况下会启用 UNIX 验证。

注 - pam_unix 模块已被删除，Oracle Solaris 将不再支持该模块。该模块已由一组功能相同或功能更强的其他服务模块所取代。在本指南中，pam_unix 是指提供相同功能的模块，而非 pam_unix 模块本身。

以下模块提供了与原始 pam_unix 模块相同的功能。这些模块是使用其对应的手册页列出的。

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 验证模式：

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。

pam_unix_* 模块具有以下限制：

- 口令必须以 UNIX crypt 格式存储。
- 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/digest-MD5 验证方法不兼容。在 Oracle Directory Server Enterprise Edition 中，要使用 digest-MD5，口令必须以未加密的形式存储。UNIX 验证要求口令以 crypt 格式存储。

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。对于 enableShadowUpdate 模式中的 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。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

在以下来源中广泛地讨论了 Kerberos：

- pam_krb5(5) 手册页。
- 《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务》

PAM 和更改口令

使用 passwd 命令更改口令。如果未启用 enableShadowUpdate 开关，则 userPassword 属性对于用户和管理员凭证必须是可写的。对于此操作，passwd-cmd 的

serviceAuthenticationMethod 会覆盖 authenticationMethod。根据验证方法，当前口令可能是未加密的。

在 UNIX 验证中，新的 userPassword 属性将使用 UNIX crypt 格式来加密。该属性将加上标记，然后写入 LDAP。因此，无论使用哪种验证方法绑定到服务器，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。

如果已启用 enableShadowUpdate 开关，则当用户口令更改时，pam_unix_* 模块也将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 模块对口令更新的支持功能已由使用 server_policy 选项的 pam_authtok_store 模块所替换。使用 pam_authtok_store 时，新口令将以未加密形式发送到 LDAP 服务器。为了确保保密性，请使用 TLS。否则，新 userPassword 将很容易被窥探。

如果您为 Oracle Directory Server Enterprise Edition 设置了未标记的口令，则该软件会使用 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。

如果使用 UNIX 验证的 NIS 或任何其他客户机将 LDAP 用作系统信息库，则必须使用 crypt 配置 passwordStorageScheme 属性。此外，如果对 Oracle Directory Server Enterprise Edition 使用 sasl/digest-MD5 LDAP 验证，则必须将 passwordStorageScheme 配置为明文。

LDAP 帐户管理

使用 pam_krb5 执行帐户和口令管理时，Kerberos 环境将管理所有的帐户、口令、帐户锁定和其他帐户管理详细信息。

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。可以将 pam_ldap 配置为支持用户帐户管理。通过正确的 PAM 配置，passwd 命令将强制执行 Oracle Directory Server Enterprise Edition 口令策略所设置的口令语法规则。但是，不要启用对 proxy 帐户的帐户管理。

以下帐户管理功能受 pam_ldap 支持。这些功能取决于 Oracle Directory Server Enterprise Edition 的口令和帐户锁定策略配置。您可以启用其中的任意多个功能。

- 口令生命期和失效通知 – 用户必须根据预定的时间更改其口令。否则，口令将失效，用户验证将失败。

  在过期警告期间内登录时，用户每次都会收到警告。警告包含口令失效前的剩余时间。

- 口令语法检查 – 新口令必须符合口令的最低长度要求。口令不得与用户目录条目中的 uid、cn、sn 或 mail 属性的值相同。
- 历史记录检查中的口令 – 用户无法重用口令。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 - 这些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“使用 pam_ldap 模块进行帐户管理的示例 pam_conf 文件” [24]。

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版本的 LDAP 客户机用于 pam_ldap 帐户管理。此外，确保客户机具有正确配置的 pam.conf 文件。否则，当 proxy 或用户口令到期后，LDAP 命名服务将失败。

使用 pam_unix_* 模块管理 LDAP 帐户

如果已启用 enableShadowUpdate 开关，帐户管理功能将可用于本地帐户和 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 开关可为在文件中和 LDAP 范围内定义的用户实现一致的帐户管理。

pam_ldap 和 pam_unix_* 模块不兼容。pam_ldap 模块要求口令可由用户修改。pam_unix_* 模块的要求则相反。因此，无法在同一个 LDAP 命名域中同时使用这两个模块。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。由于这一限制，您可能需要使用专用的 LDAP 服务器，以防出现例如 Web 或电子邮件应用程序可能会要求用户在 LDAP 服务器上更改其自身口令的情况。

实施 enableShadowUpdate 还要求将管理员凭证（adminDN 和 adminPassword）存储在每台客户机本地的 svc:/network/ldap/client 服务中。

使用 pam_unix_* 模块进行帐户管理无需更改 /etc/pam.conf 文件。使用缺省的 /etc/pam.conf 文件足以满足要求。

使用 pam_ldap 模块进行帐户管理的示例 pam_conf 文件

本节包含一个示例 pam_conf 文件。

```
#
# 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.
#
```

♦ ♦ ♦ 第 3 章

3 LDAP 命名服务的规划要求

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 规划主要包括确定向 LDAP 客户机配置文件中放入哪些信息。客户机使用配置文件中的配置信息集合从 LDAP 服务器访问命名服务信息。在 LDAP 服务器上生成配置文件时可以指定配置信息。服务器设置期间，系统会提示您输入该信息。提示输入的某些信息是必需的，而其他信息则是可选信息。在大多数情况下，将会接受已提供的缺省值。提示输入的配置文件的各类信息称为**客户机属性**。

随着配置文件的配置信息越来越多，可以使用“用于配置 LDAP 的空核对表 ” [35]上的模板核对表。您可以在设置 LDAP 服务器时将这些核对表用作参考信息。

下表显示了 LDAP 客户机配置文件属性。

表 3-1 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。

属性	说明
	注 - 如果要使用主机名同时定义 defaultServerList 和 preferred ServerList，则不得将 LDAP 用于主机服务器查找搜索。不要将 svc:/network/name-service/switch 服务的 config/host 属性值配置为 ldap。
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 preferred ServerList 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 属性来覆盖该值。
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。缺省值为单级别搜索。
authenticationMethod	标识了客户机使用的验证方法。缺省值为 none (anonymous)。有关更多信息，请参见“LDAP 命名服务的验证方法” [17]。
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，不定义任何 attributeMap。
objectclassMap	客户机使用的对象类映射。缺省情况下，未定义任何 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（秒）。该值不会影响在 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（秒）。缺省值为 30 秒。
followReferrals	指定客户机是否应遵循 LDAP 引用。可能的值包括 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。

当您在服务器上运行 idsconfig 命令时，将自动设置这些属性。

其他客户机属性可通过使用 ldapclient 命令在客户机系统本地进行设置。有关这些属性的更多信息，请参见“定义本地客户机属性” [59]。

规划 LDAP 客户机配置文件的配置

要正确设置 LDAP 命名服务，必须先规划 LDAP 客户机配置文件的配置。配置文件属性的缺省值可满足大多数网络的要求。但是，根据您自己的网络拓扑，可能要为某些配置文件属性指定非缺省值。本节介绍了您可能要配置的不同属性。

LDAP 网络模型

规划 LDAP 网络模型是指确定要为LDAP 命名服务部署的物理服务器。要确保可用性和性能，网络的每个子网都必须有一个 LDAP 服务器来为该子网中的客户机提供服务。规划该模型时，您应考虑以下事项：

- 要部署为 LDAP 服务器的系统数量

  哪些服务器指定为主服务器，哪些服务器是用作备份的副本服务器？
- 访问服务器的方式

  所有的 LDAP 服务器是否都对客户机请求的访问具有同等的优先级？还是服务器具有不同的优先级，会首先访问具有较高优先级的服务器？如果访问服务器的优先级不同，则列出访问这些服务器的顺序。

  指定的信息由 `defaultServerList` 和 `preferredServerList` 属性进行管理。
- 超时因素

  按如下所示确定超时值：

  - `bindTimeLimit` 属性用于确定在丢弃请求之前，TCP 连接请求持续的时间。
  - `searchTimeLimit` 属性用于确定在取消搜索之前，LDAP 搜索操作持续的时间。
  - `profileTTL` 属性确定客户机从服务器下载配置文件的频率。

  例如，在速度较慢的网络中，您可以增加搜索和 TCP 连接请求所持续的时间长度。在开发环境中，您可以限制客户机下载配置文件的频率。

目录信息树

LDAP 命名服务使用缺省目录信息树 (directory information tree, DIT) 存储信息。DIT 本身基于 LDAP 架构。

DIT 由多个具有层次结构的信息容器组成。该结构使用 RFC 2307 (http://tools.ietf.org/html/rfc2307) 和 RFC 4876 (http://tools.ietf.org/html/rfc4876) 中所述的标准 LDAP 架构。

DIT 的缺省结构可满足大多数网络设置实施 LDAP 的要求。使用缺省结构时，您只需确定以下内容：

- 命名服务将从中搜索特定域相关信息的树的基本节点标识名 (distinguished name, DN)。基本节点信息由 `defaultSearchBase` 属性进行管理。
- 命名服务查找功能应执行的搜索的范围。该范围可以只涵盖 DN 以下的一个级别，也可以涵盖 DN 以下的整个子树。此信息由属性 `defaultSearchScope` 进行管理

DIT 还可以用更为复杂的结构来存储数据。例如，用户帐户相关的数据可存储在 DIT 的不同部分。您应确定如何定制搜索操作的行为（如基本 DN、搜索范围和过滤器），以使用其覆盖缺省搜索序列。定制的搜索序列信息由属性 `serviceSearchDescriptor`、`attributeMap` 和 `objectclassMap` 进行管理。有关定制搜索序列操作的详细说明，请参见“服务搜索描述符和架构映射” [32]。

多个服务器可为单个 DIT 提供服务。在此设置中，DIT 的子树可分布在多个服务器中。因此，您必须进一步配置 LDAP 服务器，以将客户机请求正确重定向到可提供所请求信息的相应 LDAP 服务器。有关如何将客户机请求重定向到正确服务器的信息由 `followReferrals` 属性进行管理。

通常建议的设置是使用单个 LDAP 服务器向特定域提供所有命名数据。但是，即使在此示例中，您仍可以将 `followReferrals` 属性配置用于特定目的。通过引用，您可以针对大多数信息请求，将客户机定向到只读副本服务器。仅在少数例外情况下，才提供对主服务器的访问权限以执行读写操作。通过引用配置，您可以防止主服务器过载。

安全注意事项

对于处理目录信息请求的LDAP 操作的安全性，您需要考虑以下事项：

- 客户机标识自身以访问信息的方式。标识的方式由为客户机指定的凭证级别确定。凭证级别通过 `credentialLevel` 属性管理，可向其指定以下值之一：
  - `anonymous`
  - `proxy`
  - `proxy anonymous`
  - `self`

  有关其中某个值的详细说明，请参见“客户机凭证级别” [15]。
- 验证客户机的方法。您指定的方法由 `authenticationMethod` 属性进行管理。可通过指定以下任一选项来指定验证方法：
  - `none`
  - `simple`
  - `sasl/digest-MD5`
  - `sasl/cram-MD5`
  - `sasl/GSSAPI`
  - `tls:simple`
  - `tls:sasl/cram-MD5`

- `tls:sasl/digest-MD5`

有关其中某个值的详细说明，请参见“LDAP 命名服务的验证方法” [17]。

除了要分配给客户机的凭证级别以及要使用的验证方法，还应考虑以下事项：

- 是否要使用 Kerberos 和“每用户”验证
- 要为服务器的 `passwordStorageScheme` 属性指定的值
- 是否设置访问控制信息？

  有关 ACI 的更多信息，请查阅所用 Oracle Directory Server Enterprise Edition 版本的管理指南。
- 将使用 `pam_unix_*` 还是 `pam_ldap` 模块来执行 LDAP 帐户管理

  此注意事项与 LDAP 命名服务是否与 NIS 兼容有关。

规划 LDAP 主服务器和副本服务器的部署

主服务器和副本服务器可通过以下方式进行部署：

- 单主复制
- 浮动主复制
- 多主复制

下表比较了部署 LDAP 主服务器和副本服务器的三个策略。

表 3-2 LDAP 主服务器和副本服务器

策略	说明	风险
单主复制	特定网络或子网存在一个主服务器。主服务器存储目录的可写副本。副本数据库存储只读副本。只有主服务器才可执行写操作。	单点故障。如果主服务器变为不可用，则任何其他服务器都不可执行写操作。
浮动主复制	与单主复制类似。但是，如果主服务器变为不可用，另一台副本服务器可执行写操作。可基于算法选择接管写操作的副本服务器。	针对网络配置更改的策略不具有灵活性。例如，网络细分为子网。两个子网上的副本服务器都将成为主服务器。如果子网随后在一段时间内重新连接，则使用浮动主复制策略重新部署服务器的重新配置过程将变得很复杂。
多主复制	多个主服务器存储同一目录的读写副本。	可能出现在不同的主服务器中更新同一目录的冲突。如果采用此策略，则必须建立更新冲突的解决策略，如“以最后写入者为准”。

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

规划 LDAP 数据置备

在为 LDAP 服务器配置了正确的 DIT 和架构后，需要向 DIT 置备数据。数据源是多个系统中的 /etc 文件。您需要考虑使用何种方法置备 DIT：

- 将某种特定数据类型的 /etc 文件合并到该数据类型的单个文件，例如将不同系统中的所有 /etc/passwd 文件合并到单个 /etc/passwd 文件中。然后，从存储所有合并的 /etc 文件的该单个主机填充服务器。
- 通过从每个访问目录服务器的客户机系统发出相应的命令来置备服务器。

有关填充目录服务器的步骤，请参见“使用数据置备 LDAP 服务器” [48]。

服务搜索描述符和架构映射

如上所述，LDAP 命名服务要求 DIT 具有某种特定结构。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。有关缺省过滤器列表，请使用以下命令：

```
ldaplist -v
```

注 - “LDAP 命名服务使用的缺省过滤器” [97]中也列出了缺省过滤器。

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）。

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，其后跟一个或多个用分号分隔的 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 中执行单级搜索，然后在 ou=east,dc=example,dc=com 中执

行单级搜索。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。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。

您可能会发现想要在现有目录服务器中映射属性的情况下，使用架构映射十分有用。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
```

请注意，您可以将 passwd 服务的 gecos 属性映射到多个属性，如以下示例所示：

```
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，便会使用 myUnixAccount 对象类：

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

摘要：用于准备实施 LDAP 的缺省客户机配置文件属性

以下列表确定了您通常会配置以实施 LDAP 命名服务的重要属性。请注意，并非所有这些属性都需要配置。在列出的属性中，只有 cn、defaultServerList 和 defaultSearchBase 要求您提供值。对于其他属性，您可以接受缺省值，或保留其他属性而不进行任何配置。

- cn
- defaultServerList
- preferredServerList
- bindTimeLimit
- searchTimeLimit
- profileTTL
- defaultSearchBase
- defaultSearchScope
- serviceSearchDescriptor
- attributeMap
- objectclassMap
- followReferrals
- credentialLevel
- authenticationMethod
- serviceCredentialLevel
- serviceAuthenticationMethod

用于配置 LDAP 的空核对表

表 3-3 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 number*：*port number*）	
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（秒）	
为每个搜索请求返回的最多项数	

表 3-4 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。可能的值包括 '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？（引用是当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（秒）。缺省值为 `30` 秒。	
与服务器进行联系时的绑定时间限制（秒）。缺省值为 `30` 秒。	
验证方法。缺省值为 `none`。	

♦ ♦ ♦ 第 4 章

设置 Oracle Directory Server Enterprise Edition 和 LDAP 客户机

本章介绍了如何配置 Oracle Directory Server Enterprise Edition 以支持 LDAP 客户机。本章中的信息特定于 Oracle Directory Server Enterprise Edition。

注 - 必须已安装和配置 Oracle Directory Server Enterprise Edition，然后才能配置其与 LDAP 客户机一起使用。本章并不介绍 Oracle Directory Server Enterprise Edition 的所有功能。有关更多的详细信息，请参阅您所拥有的特定目录服务器的文档。

本章包含以下主题：

准备用于配置目录服务器的信息

要为 LDAP 命名服务配置目录服务器，您必须具备两组信息：服务器信息和客户机配置文件信息。

LDAP 的服务器信息

配置目录服务器时，系统会提示您提供有关该服务器的以下信息：

- 目录服务器实例的端口号。缺省情况下，端口号为 389。
- 服务器名称。
- 副本服务器的 IP 地址和端口号。
- 目录管理器，由变量 `cn` 表示。缺省情况下，`cn` 设置为 `directory manager`。
- 要为其提供服务的域名。
- 在请求超时之前处理客户机请求的最长时间（秒）。
- 为每个搜索请求提供的最大记录信息数。

有关服务器的某些信息是在“规划 LDAP 客户机配置文件的配置” [29]中介绍的 LDAP 客户机配置文件的一些属性。

为方便准备服务器信息，请使用“用于配置 LDAP 的空核对表 ” [35]中的样例核对表，该核对表列出了这些变量以及要分配的对应值。

LDAP 的客户机配置文件信息

必须具备有关 LDAP 客户机配置文件属性的信息。请求相关信息时，这些属性会控制客户机对服务器的访问。有关这些属性的说明，请参见“规划 LDAP 客户机配置文件的配置” [29]。

- 客户机配置文件的名称。
- LDAP 服务器的列表。
- 访问服务器的首选顺序。

  通常，服务器列表及其访问顺序由服务器的 IP 地址组成。或者，您可以指定服务器的主机名。但是，如果使用主机名，则务必不要使用 LDAP 进行主机查找操作。因此，一定不要配置 `svc:/network/name-service/switch` 服务的 `config/host` 属性中的 `ldap`。有关 LDAP 和服务管理工具 (Service Management Facility, SMF) 的信息，请参见“LDAP 和服务管理工具” [57]。
- 在目录树上搜索的范围。缺省值为 `one`，但您可以指定 `sub`。
- 访问服务器的凭证
- 对其他 LDAP 服务器的引用，假如目录中的信息分布在多个服务器中的话。值为 `No`（缺省值）或 `Yes`。
- 在超时之前，接收服务器对请求的响应的等待时间。
- 在超时之前与服务器进行联系的最长时间。
- 验证方法。

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。

为方便准备客户机配置文件信息，请使用“用于配置 LDAP 的空核对表 ” [35]中的样例核对表，该核对表列出了这些变量以及要分配的对应值。

使用浏览索引

Oracle Directory Server Enterprise Edition 的浏览索引功能称为虚拟列表视图 (Virtual List View, VLV)。借助 VLV，客户机可以从一长串的列表中查看选择的条目子集，从而可以缩短每个客户机的搜索时间。

在为树创建 VLV 的过程的最后会创建目录信息树。屏幕中提供了在创建 VLV 时所发出的命令的说明。必须在目录服务器上发出这些命令。

创建目录树定义

收集必要的服务器和客户机配置文件信息后，请为 LDAP 设置 Oracle Directory Server Enterprise Edition。使用 `idsconfig` 可依据核对表上的定义来生成目录信息树。

使用 `idsconfig` 命令创建 DIT 时，实际上是在构建客户机配置文件及其属性（如表 3-1 “LDAP 客户机配置文件属性” 中列出的内容）。客户机配置文件存储在 LDAP 服务器上的一个众所周知的位置中。在服务器上使用单一配置文件的优点是，可以针对使用该服务器的所有客户机来定义配置。配置文件属性之后的任何更改都会自动传播到客户机。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。

可以从网络的任何 Oracle Solaris 系统上创建目录定义。但是，在这种情况下，`idsconfig` 命令的输出将以明文形式包含目录管理器的口令。作为避免公开口令的备选方法，请由目录服务器本身发出命令。

有关 `idsconfig` 命令的更多信息，请参见 `idsconfig(1M)` 命令手册页。

注 - 您可以在创建目录树的同时，创建服务搜索描述符 (Service Search Descriptors, SSD)。通过同一个命令（`idsconfig` 命令）可同时启动这两个操作。但是，如果愿意，您可以在单独的操作中创建 SSD。有关 SSD 及其用途的说明，请参见“服务搜索描述符和架构映射” [32]。

▼ 如何为 LDAP 命名服务配置 Oracle Directory Server Enterprise Edition

1. 确保目标 Oracle Directory Server Enterprise Edition 正在运行。
2. 生成目录信息树。

   ```
   # /usr/lib/ldap/idsconfig
   ```

3. 根据系统提示提供信息。
4. 按照屏幕上的说明来生成 VLV 索引。

   在创建 DIT 过程结束时，将通过单独的操作来生成 VLV 索引。屏幕提供了相应的命令语法。请确保在服务器上执行这些说明。在 `idsconfig` 进程完成时，说明将显示如下：

   ```
   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.
```

有关运行 idsconfig 命令时的完整输出，请参见“生成目录信息树” [40]中的屏幕示例。

LDAP 的服务器配置示例

本节提供了 Oracle Directory Server Enterprise Edition 在使用 LDAP 命名服务时，其系统配置的各个方面的示例。示例演示了一家在全国各地设有分支机构的公司 Example, Inc.。具体来说，示例侧重于公司西海岸分部的 LDAP 配置，其中域名为 west.example.com。

生成目录信息树

下表列出了 west.example.com 的服务器信息。

表 4-1 为 west.example.com 域定义的服务器变量

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 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（秒）	1
为每个搜索请求返回的最多项数	1

下表列出了客户机配置文件信息。

表 4-2 为 west.example.com 域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
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

变量	针对示例网络的定义
搜索范围（沿着目录树 one（缺省）或 sub 向下查找的层数）	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

根据上述信息，您可以创建目录树。

```
# 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 ...
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
 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
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.
```

以下屏幕包含要完成 `idsconfig` 设置需要遵循的其他说明。

```
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
```

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`

可以使用 `idsconfig` 实用程序在为新配置文件生成 DIT 时启用影子更新。要启用影子更新，必须在提示 `Do you want to enable shadow update (y/n/h)? [n]` 时键入 **`y`**。必须在提示 `Enter passwd for the administrator:` 时键入管理员口令。

以下示例显示了如何使用 `idsconfig` 实用程序启用影子更新。

```
# 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 ...
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] y
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
 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          : TRUE
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:proxy-password
Re-enter passwd:proxy-password
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:admin-password
Re-enter passwd:admin-password
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. Administrator identity cn=admin,ou=profile,dc=west,dc=example,dc=com added.
15. Give cn=admin,ou=profile,dc=west,dc=example,dc=com read/write access to\
    shadow data.
16. Non-Admin access to shadow data denied.
17. Generated client profile and loaded on server.
18. 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.
19. Processing eq,pres,sub indexes:
ipHostNumber (eq,pres,sub)   Finished indexing.
membernisnetgroup (eq,pres,sub)   Finished indexing.
nisnetgrouptriple (eq,pres,sub)   Finished indexing.
20. Processing VLV indexes:
west.example.com.getgrent vlv_index   Entry created
west.example.com.gethostent vlv_index   Entry created
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.
```

有关如何初始化 LDAP 客户机以启用影子更新的信息，请参阅“初始化 LDAP 客户机” [60]。在初始化 LDAP 客户机时，必须使用与在生成 DIT 时提供的域名和管理员口令相同的域名和管理员口令。

定义服务搜索描述符

在 Example, Inc. 中，上一个 LDAP 配置将用户信息存储在目录树的 `ou=Users` 容器中。在本手册介绍的 Oracle Solaris 发行版中，假定用户项均存储在 `ou=People` 容器中。因此，如果搜索到 `passwd` 服务，且客户机搜索的是 `ou=People` 容器，则无法获取信息。

为避免重新创建公司现有目录信息树的复杂性及可能对其他操作产生的影响，您可以改为创建服务搜索描述符 (Service Search Descriptors, SSD)。这些 SSD 将指导 LDAP 客户机从 `ou=Users` 容器（而不是缺省容器）查找用户信息。

有关搜索描述符的信息，请参见“服务搜索描述符和架构映射” [32]。

要创建 SSD，也可以使用 `idsconfig` 命令。引用 SSD 的提示行如下所示：

```
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
```

使用数据置备 LDAP 服务器

创建 DIT 之后，需要使用数据置备信息树。数据来源于包含 `/etc` 文件的所有系统。因此，必须在这些系统（而不是服务器）上执行此任务。置备信息树的方式取决于在“规划 LDAP 数据置备” [32]中所描述的规划。

以下是其中数据可填充信息树的文件示例：

- `aliases`
- `auto_*`
- `bootparams`
- `ethers`
- `group`
- `hosts`

类似地，`/etc` 中权限相关文件中的信息也会添加到信息树中，如 `user_attr`、`~/security/auth_attr`、`~/security/prof_attr` 和 `~/security/exec_attr` 等。

要置备信息树，可以使用 ldapaddent 命令。还可以指定要将其数据加载到树中的 /etc 文件或数据库。某些文件必须按顺序加载才能获得更好的性能。文件及其加载顺序如下所示：

1. passwd
2. shadow
3. networks
4. netmasks
5. bootparams
6. ethers

请注意，在加载自动挂载程序信息时，文件或数据库名称将使用 auto_* 命名格式，如 auto_home。

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。有关采用 UNIX crypt 格式设置口令的详细信息，请参见 Oracle Directory Server Enterprise Edition 文档。有关 ldapaddent 命令的详细信息，请参见 ldapaddent(1M) 手册页。

▼ 如何使用数据置备服务器

本过程说明了使用来自客户机系统的 /etc 文件中的数据置备服务器上的信息树的步骤。此任务假定来自不同客户机系统的 /etc 文件不会合并成单个文件。您必须在包含用于置备服务器的源 /etc 文件的每个系统上执行此任务。

此任务使用域 west.example.com，该域用于准备 “LDAP 的服务器配置示例” [40]中的客户机配置文件。

开始之前 确保 Oracle Directory Server Enterprise Edition 已设置。具体来说，请确保目录信息树已使用 idsconfig 命令进行配置，如如何为 LDAP 命名服务配置 Oracle Directory Server Enterprise Edition [39]中所述。

1. **成为管理员。**

   有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

2. **使用来自 /etc 中的各个文件或数据库中的数据置备服务器。**

   ```
   # ldapaddent -D "cn=directory manager" -f /etc/filename container
   ```

   其中 *container* 与 *filename* 具有相同的名称，如 passwd。

其他目录服务器配置任务

在服务器上创建 DIT 并按需要定义 SSD 之后，您可以执行以下其他任务。

使用 Member 属性指定组成员关系

RFC 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，组项可以具有以标识名 (Distinguished Names, 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

使用带有 genprofile 选项的 ldapclient 命令基于所指定的属性创建配置文件的 LDIF（LDAP Data Interchange Format，LDAP 数据交换格式）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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

2. 使用带 genprofile 的 ldapclient 命令。

```
# ldapclient genprofile \
-a profileName=myprofile \
-a defaultSearchBase=dc=west,dc=example,dc=com \
-a "defaultServerList=xxx.xxx.x.x yyy.yyy.y.y:portnum" \> myprofile.ldif
```

3. 将新配置文件上载到服务器。

```
# ldapadd -h xxx.xxx.x.x -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。

使用 pam_ldap 模块的客户机的帐户管理

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。有关具体过程和更多信息，请参见您所用 Oracle Directory Server Enterprise Edition 版本的管理指南中的“用户帐户管理”一章。

注 - 以前在使用 pam_ldap 帐户管理时，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 等工具进行非基于口令的登录将失败。

在用户登录时，您现在可以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制为 1.3.6.1.4.1.42.2.27.9.5.8。缺省情况下，此控制处于启用状态。要修改缺省控制配置，请在目录服务器上添加访问控制指令 (access control instruction, ACI)。例如：

```
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与帐户过期信息。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。

使用 pam_unix_* 模块的客户机的帐户管理

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。所有配置均可运行 idsconfig 实用程序来执行。

下面的示例显示了两个 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 5 章

5 设置 NIS 客户机

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：

准备 LDAP 客户机设置

以下是 Oracle Solaris 客户机使用 LDAP 作为命令服务的要求：

- 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参数。
- `ldap_cachemgr` 必须正在客户机上运行。
- 必需至少有一台要为其配置客户机的服务器正在运行。

`ldapclient` 实用程序将执行除启动服务器之外的所有已列出的配置步骤。本章举例说明如何使用 `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。

LDAP 和服务管理工具

Oracle Solaris 服务管理工具 (Service Management Facility, SMF) 用于管理 LDAP 客户机服务。有关 SMF 的更多信息，请参阅《在 Oracle Solaris 11.2 中管理系统服务 》。有关详细信息，另请参见 `svcadm(1M)` 和 `svcs(1)` 手册页。

以下列表重点列出了与管理 LDAP 客户机服务相关的 SMF 功能。

- svcadm 命令用于启用、禁用或重新启动 LDAP 客户机服务。

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。

- 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。
- svcs 命令用于查询 LDAP 客户机和 ldap_cachemgr 守护进程的状态。
  - 以下示例显示 svcs 命令及其输出：

```
# svcs \*ldap\*
STATE          STIME    FMRI
online         15:43:46 svc:/network/ldap/client:default
```

  - 以下示例显示在 FMRI 中使用实例名称时的 svcs -l 命令及其输出。

```
# 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 ldapsearch 命令：

```
# ldapsearch -h server-name -b "" -s base "objectclass=*" |grep -i context
namingContexts: dc=example,dc=com
```

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。

定义本地客户机属性

第 3 章 LDAP 命名服务的规划要求描述了为配置 LDAP 服务器而定义的 LDAP 客户机配置文件的属性。使用 idsconfig 命令可以在服务器上设置具有那些属性的配置文件。

通过使用 ldapclient 命令可以在本地设置其他客户机属性。下表列出了这些属性。

表 5-1 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，且 credentialLevel 的值不是 self，则必须指定 adminDN。
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 设置为 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 设置为 "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。

管理 LDAP 客户机

本节介绍如何使用 ldapclient 命令来初始化以及修订 LDAP 客户机配置。

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，所以当前 Oracle Solaris 发行版不支持 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。

初始化 LDAP 客户机

使用 ldapclient 可以通过以下两种方式之一来初始化 LDAP 客户机：

- 使用配置文件

  发出 ldapclient 命令时，必须至少指定配置文件和域的服务器地址。如果未指定配置文件，则假定为缺省配置文件。服务器提供了配置文件中除代理和证书数据库信息之外的其余所需信息。

  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“客户机凭证级别” [15]。要启用影子数据更新，您必须提供管理员的凭证（adminDN 和 adminPassword）。

  使用配置文件可降低 LDAP 配置的复杂性，尤其是在企业环境中。
- 在一个命令行中定义所有参数

  不存在任何配置文件。因此，客户机将自己创建配置文件。通过此方法，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。

您可以通过使用 ldapclient 命令的不同命令语法来初始化客户机。

- 通过使用已配置了缺省值的配置文件来初始化客户机。例如：

```
# ldapclient init -a profilename=new -a domainname=west.example.com 192.168.0.1
System successfully configured
```

- 初始化一个客户机，其配置文件配置为使用每用户凭证和 sasl/GSSAPI 验证方法。

  示例假定当您使用 idsconfig 命令生成 DIT 时，已指定适当的验证方法和凭证级别，例如，凭证级别为 self，验证方法为 sasl/GSSAPI。查看以下 idsconfig 命令的部分输出，其中每用户凭证信息是在服务器上创建的。

```
# /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
```

配置文件的名称为 gssapi_EXAMPLE.COM。以示例中显示的方式创建配置文件之后，您可以发出 ldapclient 命令，使用每用户配置文件来初始化客户机。

```
# ldapclient init -a profilename=gssapi_EXAMPLE.COM -a \
domainname=example.com 9.9.9.50
```

注 - 当您初始化配置有每用户凭证的客户机时，必须满足几个要求，如使用 LDAP 所需的 Kerberos 配置和 DNS 服务器配置。有关 Kerberos 的信息，请参见《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务》。有关 DNS 配置的信息，请参见《使用 Oracle Solaris 11.2 目录和命名服务：DNS 和 NIS》中的第 3 章 “管理域名系统”。有关验证的信息，请参见第 2 章 LDAP 和验证服务；有关生成 DIT 的信息，请参见第 3 章 LDAP 命名服务的规划要求。

- 初始化使用代理凭证的客户机。例如：

```
# 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
```

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。

- 初始化客户机以启用要更新的影子数据。例如：

```
# 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 \
-a enableShadowUpdate=TRUE \
192.168.0.1
System successfully configured
```

修改 LDAP 客户机配置

使用 ldapclient 命令可以在没有配置文件的情况下修改客户机配置。通常情况下，修改仅会影响有限数量的客户机属性，因此只需要一个命令行就足以修改所有选定的属性。

- 将 LDAP 客户机修改为使用简单的验证方法。例如：

```
# ldapclient mod -a authenticationMethod=simple
```

- 修改配置的 LDAP 客户机以启用影子数据更新。例如：

```
# ldapclient mod -a enableShadowUpdate=TRUE \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
System successfully configured
```

取消初始化 LDAP 客户机

取消初始化 LDAP 客户机意味着将客户机名称服务恢复到在上一次发出带有 `init`、`modify` 或 `manual` 选项的 `ldapclient` 命令之前的状态。换句话说，命令的 `-uninit` 选项会取消由 `ldapclient` 命令的其他选项所做出的上一次更改。例如，如果将客户机配置为使用 `profile1`，然后更改为使用 `profile2`，则使用 `ldapclient uninit` 将使客户机恢复使用 `profile1`。

要取消初始化 LDAP 客户机，请使用以下命令语法：

```
# ldapclient uninit
System successfully recovered.
```

使用 LDAP 进行客户机验证

本节介绍使用 LDAP 验证服务的各种配置任务。

配置 PAM

`pam_ldap` 模块是 LDAP 用于验证客户机和执行帐户管理的 PAM 模块选项。如果已将客户机配置文件的验证模式配置为 `simple`，且凭证级别配置为 `self`，则还必须启用 `pam_krb` 模块。

请参阅以下资源：

- `pam_ldap(5)` 手册页
- `pam_krb5(5)` 手册页
- 《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务》

配置 PAM 以使用 UNIX policy

/etc/pam.conf 文件可用作 PAM 使用 UNIX policy 时的缺省配置文件。通常，您不需要对此文件做出更改。

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。有关初始化 LDAP 客户机以启用影子数据更新的示例，请参见"初始化 LDAP 客户机" [60]。

有关配置文件的详细信息，请参见 pam.conf(4) 手册页。

配置 PAM 以使用 LDAP server_policy

要配置 PAM 以使用 LDAP server_policy，请参阅"使用 pam_ldap 模块进行帐户管理的示例 pam_conf 文件" [24]。要使用该示例文件，请执行以下附加步骤：

- 向客户机的 /etc/pam.conf 文件中添加包含 pam_ldap.so.1 的行。
- 如果样例文件中的任何 PAM 模块指定了 binding 标志和 server_policy 选项，请在客户机的 /etc/pam.conf 文件中为对应的模块使用相同的标志和选项。

  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。然后，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)。
- 将 server_policy 选项添加到包含服务模块 pam_authtok_store.so.1 的行中。

注 - 以前在使用 pam_ldap 帐户管理时，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 等工具进行非基于口令的登录将失败。

在用户登录时，您现在可以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制为 1.3.6.1.4.1.42.2.27.9.5.8。缺省情况下，此控制处于启用状态。要修改缺省控制配置，请在目录服务器上添加访问控制指令 (access control instruction, ACI)。例如：

```
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
```

设置 TLS 安全性

注 - PEM 证书文件必须可供任何人读取。请勿加密或限制对这些文件的读取权限。否则，ldaplist 等工具将无法工作。

如果您使用的是传输层安全 (Transport Layer Security, TLS)，则必须安装必要的 PEM 证书文件。具体而言，所有自签名的服务器证书和 CA 证书文件都是必需的，这些文件用于验证 LDAP 服务器，还可能用于验证客户机对服务器的访问。例如，如果已拥有 PEM CA 证书 certdb.pem，则必须确保此文件已添加且可通过证书路径来读取。

注 - 如果使用的是 TLS，则首先安装在本节中介绍的所需 PEM 证书文件，然后再运行 ldapclient。

有关如何创建和管理 PEM 格式证书的信息，请在所用 Oracle Directory Server Enterprise Edition 版本的管理指南中，参见“管理 SSL”一章中有关配置 LDAP 客户机以使用 SSL 的一节。配置完成后，这些文件必须存储在 LDAP 命名服务客户机所需的位置。certificatePath 属性确定此位置。缺省情况下，此位置位于 /var/ldap 中。

例如，创建必需的 PEM 证书文件（如 certdb.pem）后，请将该文件复制到如下所示的缺省位置：

```
# cp certdb.pem /var/ldap
```

然后，向所有人授予读取访问权限。

```
# chmod 444 /var/ldap/certdb.pem
```

注 - 多个证书文件可能位于该证书路径中。此外，任何给定的 PEM 证书文件可能包含多个串联在一起的 PEM 格式证书。有关更多的详细信息，请参阅服务器文档。如果将这些证书文件用于 LDAP 命名服务客户机，则必须存储在本地文件系统中。

♦ ♦ ♦ 第 6 章

6 LDAP 故障排除

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。本章包含以下主题：

监视 LDAP 客户机状态

本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，另请参见相关的手册页。

有关服务管理工具 (Service Management Facility, SMF) 的信息，请参阅《在 Oracle Solaris 11.2 中管理系统服务》。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。您可以通过以下几种方式确定 LDAP 客户机服务是否处于联机状态：

- 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 -l 选项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)
```

- 向 `-ldap_cachemgr` 传递 `g` 选项。

  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
```

如果 `ldap_cachemgr` 守护进程已禁用，则通过以下命令将其启用：

```
# svcadm enable network/ldap/client
```

有关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

要查看当前配置文件信息，成为超级用户或承担等效角色，然后运行带有 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
```

除 ldapclient list 命令之外，还可以使用 svccfg 或 svcprop 命令获取当前配置文件信息。

验证基本的客户机/服务器通信

要验证 LDAP 客户机和 LDAP 服务器之间是否存在通信，请使用 ldaplist 命令。

- 使用无选项的 ldaplist 命令将在服务器上显示 DIT 的所有容器。
- 使用 ldaplist *database* 命令将显示特定数据库的内容。例如，ldaplist passwd *username* 或 ldaplist host *hostname*。

从非客户机检查服务器数据

要查看无现成 LDAP 客户机的系统的相关信息，可使用 ldapsearch 命令。显示的信息取决于搜索时使用的过滤器。以下示例列出了 DIT 中的所有容器：

```
# ldapsearch -h server1 -b "dc=west,dc=example,dc=com" -s one "objectclass=*"
```

有关可与 ldapsearch 命令一起使用的选项和过滤器的列表，请参见ldapsearch(1) 手册页。

LDAP 配置问题及解决方案

本节介绍了可能出现的 LDAP 配置问题和建议的解决方案。

未解析的主机名

LDAP 客户机软件针对主机查找返回全限定主机名，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），则客户机软件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 域名与 LDAP 域名不同，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：

- `ldap` 未与名称服务转换中的 `passwd` 数据库相关联。
- 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。
- 代理可能没有正确的口令。
- 该项没有 `shadowAccount` 对象类。
- 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。如果您使用不带有 `-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。
- 没有可访问的 LDAP 服务器。

检查服务器的状态。

```
# /usr/lib/ldap/ldap_cachemgr -g
```

- pam.conf 的配置有误。
- 没有在 LDAP 名称空间中定义该用户。
- 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。
- 口令没有以 crypt 格式存储。
- 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。
  - 用户尝试使用非基于口令的程序（例如 ssh 或 sftp）进行登录。
- 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 配置设置有误。有关解决这些问题的详细信息，请参阅《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务》。

查找速度过慢

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。LDAP 文档（来自 Oracle 和其他供应商）包含一组应当编制索引的常用属性。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 命令无法初始化客户机。失败的可能原因包括：

- 命令行上指定的域名有误。
- 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。
- 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。
- 向 ldapclient 命令传递的服务器地址有误。请使用 ldapsearch 命令验证服务器地址。
- 向 ldapclient 命令传递的配置文件名称有误。请使用 ldapsearch 命令验证 DIT 中的配置文件名称。

作为用于故障排除的帮助手段，可以对客户机网络接口使用 snoop，以查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

通过 -g 选项运行 ldap_cachemgr 守护进程，以查看有助于调试的当前客户机配置和统计信息。

此命令将按上面提到的那样，在标准输出中显示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。在此情况下，请与服务器管理员核实，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。

解决使用每用户凭证时的问题

使用每用户凭证需要更多配置，如 Kerberos 设置等。配置每用户配置文件时请参阅以下说明。

syslog 文件指示 82 Local Error

syslog 文件可能包含以下错误消息：

```
libsldap: Status: 7 Mesg: openConnection: GSSSAPI bind failed -82 Local error
```

Kerberos 可能未初始化或其票证已过期。发出 klist 命令以进行浏览。发出 kinit -p 命令或 kinit -R 命令以重新初始化 Kerberos。

Kerberos 不会自动初始化

要使 kinit 命令在您每次登录时自动运行，请将 pam_krb5.so.1 添加到 /etc/pam.conf 文件中。例如：

```
login      auth optional pam_krb5.so.1
rlogin     auth optional pam_krb5.so.1
other      auth optional pam_krb5.so.1
```

syslog 文件指示无效凭证

发出 kinit 命令之后，syslog 文件可能包含 Invalid credential。这可能是下列某一原因造成的：

- LDAP 目录中不包含 root 主机项或用户项。
- 映射规则不正确。

ldapclient init 命令在转换检查中失败

发出 ldapclient init 命令时，将检查 LDAP 配置文件是否存在 self/sasl/GSSAPI 配置。如果转换检查失败，错误通常在于 DNS 未用作主机数据库搜索条件。

- 发出以下两个命令检查 DNS 服务的状态并将其启用。

```
# svcs -l dns/client
# svcadm enable dns/client
```

- 如果 sasl/GSSAPI 的绑定操作中出现故障，则检查 syslog 文件以确定问题。

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 实用程序列出了 LDAP 服务器中的命名信息，该信息格式为 LDIF，对于故障排除非常有用。有关详细信息，请参见 ldaplist(1)。

列出所有 LDAP 容器

ldaplist 命令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。

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，ldaplist 将列出在当前搜索 baseDN 下的所有项。

以下示例显示了 ldaplist 输出样例。

```
# 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），请使用 getent 命令。例如：

```
# getent passwd user1
user1::30641:10:Joe Q. User:/home/user1:/bin/csh
```

您还可以使用 getent 命令在数据库中执行自动挂载表中列出的查找，例如，getent automount/*map* [*key*]。例如：

```
# getent automount/auto_home user1
user1 server-name:/home/user1
```

在之前示例中，auto_home 是自动挂载映射的名称，user1 是搜索关键字。如果不指定任何搜索关键字，则将列出指定自动挂载映射的全部内容。

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
```

♦ ♦ ♦ 第 7 章

7 LDAP 命名服务（参考信息）

本章包含以下主题：

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 是 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 )

( 2.16.840.1.113894.1009.2.100.1.1 NAME 'SolarisUserAttrEntry'
  DESC 'user_attr file format without username'
  EQUALITY caseExactIA5Match
  SYNTAX  'IA5String'  )


( 2.16.840.1.113894.1009.2.100.1.2 NAME 'SolarisUserType'
  DESC 'specifies whether a normal user or a role'
  EQUALITY caseExactIA5Match
  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 ) )

( 2.16.840.1.113894.1009.2.100.2.1 NAME 'SolarisQualifiedUserAttr'
  SUP top AUXILIARY
  DESC 'Host or netgroup qualified user attributes'
  MAY ( SolarisUserAttrEntry $ SolarisUserType ) )
```

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 7-1 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))
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))

过滤器	定义
authName	(&(objectClass=SolarisAuthAttr)(cn=%s))
auditUserByName	(&(objectClass=SolarisAuditUser)(uid=%s))
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 7-2 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 8 章

从 NIS 转换为 LDAP

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“LDAP 命名服务的概述” [9]。

本章包含以下主题：

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。如第 1 章 LDAP 命名服务简介中所述，该目录使用目录管理工具进行管理。

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“LDAP 和服务管理工具” [57]和《使用 Oracle Solaris 11.2 目录和命名服务：DNS 和 NIS 》中的“NIS 和服务管理工具”。有关 SMF 的信息，请参阅《在 Oracle Solaris 11.2 中管理系统服务 》。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，请参见以下章节：

- 有关 NIS 的概述，请参见《使用 Oracle Solaris 11.2 目录和命名服务：DNS 和 NIS 》中的第 5 章 “关于网络信息服务”
- 第 1 章 LDAP 命名服务简介（提供 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：

- 未不计划在 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

  在此类环境中，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

仅安装与 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 手册页发生一些变化且其中会增加 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 配置文件将在 N2L 服务器上安装。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 服务器会将更新的 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。此行为与连接到 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。 如果您尝试在 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 8-1 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 maps（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。“支持的标准映射” [105]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 service 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

两个实用程序、两个配置文件和一个映射与 N2L 转换相关联。

表 8-2 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。

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 服务支持以下提供的映射列表，以及 RFC 2307、RFC 2307bis 及其后续版本的 LDAP 项。这些标准映射不需要手动修改映射文件。系统上任何未在列表中列出的映射都被视为定制映射，且需要手动修改。

N2L 服务还支持对 auto.* 映射进行自动映射。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。

标准映射有：

```
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	有关指导
完成所有先决条件。	请确保您已正确配置了 NIS 服务器和 Oracle Directory Server Enterprise Edition（LDAP 服务器）。	“NIS 到 LDAP 转换的先决条件” [106]
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	如何使用标准映射设置 N2L 服务 [108]
	定制映射或非标准映射	如何使用定制映射或非标准映射设置 N2L 服务 [109]
定制映射。	查看如何为 N2L 转换创建定制映射的示例。	“定制映射的示例” [112]
通过 N2L 配置 Oracle Directory Server Enterprise Edition。	根据 LDAP 服务器配置并调整 Oracle Directory Server Enterprise Edition，以进行 N2L 转换。	“通过 Oracle Directory Server Enterprise Edition 实现 NIS 到 LDAP 转换的最佳方法” [113]
对系统进行故障排除。	确定和解决常见的 N2L 问题。	“NIS 到 LDAP 故障排除” [116]
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	如何基于旧的源文件恢复到 NIS 映射 [121]
	基于当前 DIT 的映射	如何基于当前的 DIT 内容恢复为 NIS 映射 [122]

NIS 到 LDAP 转换的先决条件

在实现 N2L 服务之前，必须检查或完成以下各项操作：

- 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 迁移工具支持 Oracle Directory Server Enterprise Edition 和 Oracle 提供的兼容版本的目录服务器。如果使用 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 4 章 设置 Oracle Directory Server Enterprise Edition 和 LDAP 客户机和 `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。由于 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

您可以按照本节中的过程中的说明，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。有关需要提供的信息类型的说明，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（秒）
- LDAP 搜索操作的超时值（秒）
- LDAP 修改操作的超时值（秒）
- LDAP 添加操作的超时值（秒）
- LDAP 删除操作的超时值（秒）
- LDAP 服务器上搜索操作的时间限制（秒）
- LDAP 服务器上搜索操作的大小限制（字节）
- 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（秒）
- 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（秒）
- 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“支持的标准映射” [105]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，请参见如何使用定制映射或非标准映射设置 N2L 服务 [109]。

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“NIS 到 LDAP 转换的先决条件” [106]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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

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“设置 NIS 到 LDAP 转换服务” [107]。

   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 DIT 已完全初始化，则跳过步骤 5 并转到 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
```

N2L 服务当前使用标准映射进行设置。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“支持的标准映射” [105]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“NIS 到 LDAP 转换的先决条件” [106]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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

   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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的第 3 章 “在 Oracle Solaris 中指定权限”。

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“设置 NIS 到 LDAP 转换服务” [107]。

   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“定制映射的示例” [112]。

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 DIT 已完全初始化，请跳过步骤 6。

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“恢复为 NIS” [121]。

定制映射的示例

本节中的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 1 章 LDAP 命名服务简介中的 LDAP 命名服务信息。

例 8-1 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。
```

例 8-2 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 \
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), ",")
```

通过 Oracle Directory Server Enterprise Edition 实现 NIS 到 LDAP 转换的最佳方法

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，则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。要进行增强，必须对 Oracle Directory Server Enterprise Edition 具有 LDAP 管理员特权。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。Sun Java System Directory Server Enterprise Edition 6.2 Web 站点上提

供了 Oracle Directory Server Enterprise Edition 文档。（使用您最常用的搜索引擎搜索 "oracle.com: sun java system directory server enterprise edition"。）

通过 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。有关在 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 VLV 与 Oracle Directory Server Enterprise Edition 结合使用，则 LDAP 服务器和 N2L 服务器必须能够处理此大小的传送。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` 属性设置为大于或等于 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，通过在 Oracle Directory Server Enterprise Edition 服务器上运行带有 `vlvindex` 选项的 `dsadm` 将索引激活。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：

- 您使用的是 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，则必须手动创建新的 Oracle Directory Server Enterprise Edition VLV 用于映射，或者复制和修改现有 VLV 索引：

- 您使用的是 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 出现服务器超时状况

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，则必须手动或者通过运行 `idsconfig` 命令来修改 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（秒），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。

有关使用 LDAP 配置 Oracle Directory Server Enterprise Edition 的更多信息，请参见本书的第 4 章 设置 Oracle Directory Server Enterprise Edition 和 LDAP 客户机。

避免 Oracle Directory Server Enterprise Edition 出现缓冲区溢出状况

要避免缓冲区溢出，请手动或者通过运行 `idsconfig` 命令来修改 Oracle Directory Server Enterprise Edition 属性。

- 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
  ```

- 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Creating Virtual List View Indexes With Oracle Directory Server Enterprise Edition中的定义设置 “通过 Oracle Directory Server Enterprise Edition 创建虚拟列表视图索引” [114] 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。

有关使用 LDAP 配置 Oracle Directory Server Enterprise Edition 的更多信息，请参见第 4 章 设置 Oracle Directory Server Enterprise Edition 和 LDAP 客户机。

NIS 到 LDAP 转换限制

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 故障排除

本节包括两个方面的故障排除：

- “常见的 LDAP 错误消息” [116]
- “NIS 到 LDAP 转换问题” [118]

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。

本节介绍了一些在实现 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
```

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此错误：

- 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：81

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`
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。

`ypserv -ir`（或 `-Ir`）运行时显示控制台消息

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: `ypserv` 或其他 NIS 守护进程运行时，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“常见的 LDAP 错误消息” [116]中的 LDAP 错误说明。

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，并根据需要修复这些项。

   如果您使用的是 Oracle Directory Server Enterprise Edition，则通过运行 `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。请根据需要修复这些项。

   ```
   # 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“常见的 LDAP 错误消息” [116]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。每次执行命令时，LDAP 项接近完成状态。

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，可能会对大型 LDAP 目录进行单一访问。如果 Oracle Directory Server Enterprise Edition 的配置不正确，此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` 命令来修改 Oracle Directory Server Enterprise Edition 属性。有关详细消息，请参见“常见的 LDAP 错误消息” [116]和“通过 Oracle Directory Server Enterprise Edition 实现 NIS 到 LDAP 转换的最佳方法” [113]。

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来描述操作：

```
# 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“NIS 到 LDAP 转换的先决条件” [106]，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。由于 LDAP 服务器地址将在其他位置中列出，所以更改 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，如本节中的过程中所述。

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，保留 N2L 映射将会有用，以防您稍后需要重新启用 N2L。但是，请注意，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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

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/domain-name/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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

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/domain-name/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 DIT 部件的根元素的 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，客户机是访问某个“服务器进程”提供的服务的应用程序。在此模型中，客户机和服务器可以运行在同一台计算机上，也可以运行在不同的计算机上。
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 192.168.67.20 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, DIT（目录信息树）	DIT 是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）	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, DN（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 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。
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。
Domain Name System, DNS（域名系统）	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 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（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）	用来保护数据的保密性的手段。
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。这种全球范围内链接在一起的网络的集合称为 "Internet"。除了对网络进行命名外，全局命名服务还标识给定网络内的各个计算机和用户。
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）	用于标识网络中每台主机的唯一数字。
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（映射过程）	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、域、路由器以及其他网络的名称和地址。
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）	NIS 用于存储特定类型的信息（例如，网络上所有用户的口令项或者网络上所有主机的名称）的文件。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的公共部分，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。在面向窗口系统的客户机-服务器模型中，服务器是向应用程序或“客户机进程”提供窗口服务的进程。在此模型中，客户机和服务器可以运行在同一台计算机上，也可以运行在不同的计算机上。 (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）	为了简化路由而将单个逻辑网络划分为较小物理网络的一种解决方案。
suffix（后缀）	在 LDAP 中，后缀是 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。它又称作 *Internet* 协议套件。缺省情况下，Oracle Solaris 网络使用 TCP/IP 运行。
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

Z