

使用 Oracle® Solaris 11.2 目录和命名服务： DNS 和 NIS

ORACLE®

文件号码 E53898
2014 年 7 月

使用 Oracle Solaris 11.2 目录和命名服务：DNS 和 NIS

Part No: E53898

Copyright © 2002, 2014, Oracle and/or its affiliates. All rights reserved.

本软件和相关文档是根据许可证协议提供的，该许可证协议中规定了关于使用和公开本软件和相关文档的各种限制，并受知识产权法的保护。除非在许可证协议中明确许可或适用法律明确授权，否则不得以任何形式、任何方式使用、拷贝、复制、翻译、广播、修改、授权、传播、分发、展示、执行、发布或显示本软件和相关文档的任何部分。除非法律要求实现互操作，否则严禁对本软件进行逆向工程设计、反汇编或反编译。

此文档所含信息可能随时被修改，恕不另行通知，我们不保证该信息没有错误。如果贵方发现任何问题，请书面通知我们。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，必须符合以下规定：

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

本软件或硬件是为了在各种信息管理应用领域内的一般使用而开发的。它不应被应用于任何存在危险或潜在危险的应用领域，也不是为此而开发的，其中包括可能会产生人身伤害的应用领域。如果在危险应用领域内使用本软件或硬件，贵方应负责采取所有适当的防范措施，包括备份、冗余和其它确保安全使用本软件或硬件的措施。对于因在危险应用领域内使用本软件或硬件所造成的一切损失或损害，Oracle Corporation 及其附属公司概不负责。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。其他名称可能是各自所有者的商标。

Intel 和 Intel Xeon 是 Intel Corporation 的商标或注册商标。所有 SPARC 商标均是 SPARC International, Inc 的商标或注册商标，并应按照许可证的规定使用。AMD、Opteron、AMD 徽标以及 AMD Opteron 徽标是 Advanced Micro Devices 的商标或注册商标。UNIX 是 The Open Group 的注册商标。

本软件或硬件以及文档可能提供了访问第三方内容、产品和服务的方式或有关这些内容、产品和服务的信息。对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的担保，亦不对其承担任何责任。对于因访问或使用第三方内容、产品或服务所造成的任何损失、成本或损害，Oracle Corporation 及其附属公司概不负责。

Référence: E53898

Copyright © 2002, 2014, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

目录

使用本文档	9
1 关于命名和目录服务	11
什么是命名服务？	11
Oracle Solaris 命名服务	15
命名服务和工具	15
DNS 命名服务的说明	15
多播 DNS 和服务搜索的说明	16
/etc 文件命名服务的说明	16
NIS 命名服务的说明	16
LDAP 命名服务的说明	17
名称服务转换的说明	17
命名服务：简要比较	17
Oracle Solaris 名称服务的 IPv6 扩展	18
DNS 的 IPv6 扩展	18
2 关于名称服务转换	19
名称服务转换概述	19
用于名称服务转换的数据库和源	19
名称服务转换中的 keyserv 和 publickey 项	23
配置名称服务交换机	23
▼ 如何更改数据库的源	24
▼ 如何为数据库配置搜索条件	24
▼ 如何为所有命名数据库更改源	25
▼ 如何使用传统的 nsswitch.conf 文件	26
名称服务转换和口令信息	26
3 管理域名系统	29
DNS 概述	29
多播 DNS	29

多播 DNS 服务搜索	29
有关 DNS 的相关资料	30
DNS 和服务管理工具	30
管理 DNS (任务)	31
▼ 如何安装 DNS 软件包	31
▼ 如何配置 DNS 服务器	32
▼ 如何创建 rndc.conf 文件	32
▼ 如何配置 DNS 服务器选项	33
▼ 如何作为替代用户运行 DNS 服务	34
▼ 如何启用 DNS 客户机	34
▼ 如何对 DNS 服务器启动问题进行故障排除	35
▼ 如何验证 DNS 配置	36
管理多播 DNS	37
▼ 如何启用 mDNS 和 DNS 服务搜索	37
为 DNS 通告资源	38
DNS 参考信息	38
DNS 文件	39
DNS 命令和守护进程	39
在生成 BIND 时使用的编译标志	40
4 设置 Oracle Solaris Active Directory 客户机	41
nss_ad 命名服务模块概述	41
▼ 如何配置 nss_ad 模块	42
口令更新	43
nss_ad 命名服务模块如何从 AD 检索数据	44
检索 passwd 信息	44
检索 shadow 信息	44
检索 group 信息	45
5 关于网络信息服务	47
NIS 简介	47
NIS 体系结构	47
NIS 计算机类型	48
NIS 服务器	49
NIS 客户机	49
NIS 元素	49
NIS 域	49
NIS 守护进程	50
NIS 命令	50

NIS 映射	51
NIS 绑定	54
服务器列表模式	55
广播模式	55
6 设置和配置网络信息服务	57
配置 NIS 任务列表	57
配置 NIS 之前的准备工作	58
NIS 和服务管理工具	58
规划 NIS 域	59
标识 NIS 服务器和客户机	60
准备主服务器	60
准备主服务器（任务列表）	60
源文件目录	60
passwd 文件和名称空间安全性	61
▼ 如何为转换准备源文件	61
准备 /var/yp/Makefile	63
▼ 如何安装 NIS 主服务器软件包	64
▼ 如何设置主服务器	64
▼ 如何在一台主服务器上支持多个 NIS 域	66
在 NIS 服务器上启动和停止 NIS 服务	66
在 NIS 服务器上启动和停止 NIS 服务（任务列表）	66
自动启动 NIS 服务	67
▼ 如何手动启动 NIS 服务器服务	67
▼ 如何禁用 NIS 服务器服务	67
▼ 如何刷新 NIS 服务器服务	68
设置 NIS 从属服务器	68
设置 NIS 从属服务器（任务列表）	68
准备从属服务器	69
▼ 如何设置从属服务器	69
▼ 如何在从属服务器上启动 NIS	70
▼ 如何添加新的从属服务器	71
管理 NIS 客户机	73
管理 NIS 客户机（任务列表）	73
▼ 如何在广播模式下配置 NIS 客户机	73
▼ 如何将 NIS 客户机配置为使用特定的 NIS 服务器	74
▼ 禁用 NIS 客户机服务	75
7 管理网络信息服务	77

口令文件和名称空间安全	77
管理 NIS 用户	78
▼ 如何向 NIS 域添加新 NIS 用户	78
设置用户口令	79
NIS 网络组	80
使用 NIS 映射	81
获取映射信息	81
更改映射的主服务器	82
修改配置文件	83
修改和使用 /var/yp/Makefile	84
修改 Makefile 项	85
更新和修改现有映射	87
▼ 如何更新随缺省集合提供的映射	87
维护更新后的映射	88
修改非缺省映射	90
使用 makedbm 命令修改非缺省映射	90
从文本文件创建新映射	90
向基于文件的映射中添加项	91
通过标准输入创建映射	91
修改通过标准输入创建的映射	91
使用 NIS 服务器	92
绑定到特定 NIS 服务器	92
▼ 如何设置计算机的 NIS 域名	92
▼ 如何配置通过 NIS 和 DNS 执行计算机主机名和地址查找	93
禁用 NIS 服务	94
8 网络信息系统故障排除	95
NIS 绑定问题	95
NIS 绑定问题的症状	95
影响一台客户机的 NIS 问题	96
影响多台客户机的 NIS 问题	99
术语表	103
索引	109

使用本文档

- 概述 - 介绍 DNS 和 NIS 命名服务、用于规划其使用的方法以及实施 DNS 和 NIS 的步骤。
- 目标读者 - 系统管理员。
- 必备知识 - 熟悉与 DNS 和 NIS 相关的命名服务概念和术语。

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。

关于命名和目录服务

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

本章包含以下主题：

- [“什么是命名服务？” \[11\]](#)
- [“Oracle Solaris 命名服务” \[15\]](#)
- [“命名服务：简要比较” \[17\]](#)

什么是命名服务？

命名服务执行对所存储的信息的查找工作，例如：

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

提供该信息是为了让用户能够登录到其主机、对资源进行访问以及被授予权限。名称服务信息可以存储在文件、映射或各种形式的数据库文件中。这些系统信息库可以位于系统本地或位于基于中央网络的系统信息库或数据库中。

如果没有中央命名服务，则每台主机都必须单独维护一份此信息的副本。如果集中存储所有数据，管理将变得更加轻松。

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

- 将名称与对象关联（绑定）
- 将名称解析为对象
- 删除绑定
- 列出名称
- 重命名信息

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

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



**Graphic Not Accessible
Check Declaration**

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



**Graphic Not Accessible
Check Declaration**

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

网络信息服务将网络信息存储在服务器上，可供任何系统查询。

这些系统被称作服务器的客户机。下图显示客户机/服务器布局。每次网络信息发生变化时，管理员将只更新网络信息服务存储的信息，而不更新每个客户机的本地文件。这样做可以减少错误、客户机之间的一致性以及任务的绝对工作量。



**Graphic Not Accessible
Check Declaration**

这种由服务器向网络中的客户机提供集中式服务的布局称为客户机/服务器计算。

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



**Graphic Not Accessible
Check Declaration**

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



**Graphic Not Accessible
Check Declaration**

可以将邮件发送到 example.com，而不是将邮件或其他网络通信发送到 198.168.0.0。可以无需输入 192.168.2.0 或 192.168.3.0 物理地址作为邮件或其他网络通信的地址，而是输入 sales.example.com 或 manf.example.com 作为地址。

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

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



**Graphic Not Accessible
Check Declaration**

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

表 1 example.com 网络的表示

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

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



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



因此，当组织更改时，其网络信息服务可以按此处所示更改其映射。



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

通过更改网络信息结构，无需重新组织网络结构，即可适应组织结构的后续更改。

Oracle Solaris 命名服务

Oracle Solaris 平台提供了以下命名服务：

- 域名系统 (Domain Name System, DNS) (请参见[“DNS 命名服务的说明” \[15\]](#))
- /etc 文件, 原始的 UNIX 命名系统 (请参见[“/etc 文件命名服务的说明” \[16\]](#))
- 网络信息服务 (Network Information Service, NIS) (请参见[“NIS 命名服务的说明” \[16\]](#))
- 轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP) (请参见 [《使用 Oracle Solaris 11.2 目录和命名服务：LDAP》](#))

大多数现代网络都组合使用这些服务中的两个或多个。名称服务转换可协调用于特定查找的命名服务。有关更多信息, 请参见[第 2 章 关于名称服务转换](#)。

命名服务和工具

在 Oracle Solaris 中, 所有命名服务现在都通过服务管理工具 (SMF) 管理。配置信息不再存储在配置文件中, 而是存储在 SMF 系统信息库中。有关 SMF 如何处理特定命名服务的更多信息, 请参阅本指南中的个别章节。

旧配置文件会保留在此 Oracle Solaris 发行版中, 但仅用于实现与以前的 Oracle Solaris 发行版兼容。它们的内容由与特定命名服务相关的 SMF 服务生成。不应再将这些文件用于命名服务配置。必须使用常规 SMF 命令 (例如 `svcs`、`svcadm` 和 `svccfg`) 取而代之。

在从 Oracle Solaris 10 升级到 Oracle Solaris 11 及其更新版本时, 系统的名称服务配置会自动迁移到 SMF。但是, 如有必要, 可以使用 `nscfg` 命令执行手动迁移。有关更多信息, 请参阅 [nscfg\(1M\)](#) 手册页。

DNS 命名服务的说明

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

DNS 客户机从一台或多台名称服务器请求关于主机名的信息并等待响应。DNS 服务器会响应来自从以下任何来源加载的信息高速缓存的请求：

- DNS 主服务器上的文件或第三方数据库
- 来自网络中协作 DNS 从属服务器的文件或第三方数据库
- 所存储的来自先前查询的信息

如果未找到响应并且服务器不负责有问题的域，则该服务将以递归方式从其他服务器请求主机名并缓存该响应（如果进行了相应的配置）。

多播 DNS 和服务搜索的说明

DNS 协议的两个扩展由 `svc:network/dns/multicast` 服务进行管理。多播 DNS (Multicast DNS, mDNS) 在未安装传统 DNS 服务器的小型网络中实施 DNS。DNS 服务搜索 (DNS Service Discovery, DNS-SD) 对多播 DNS 进行了扩展，使之还提供简单的服务搜索（网络浏览）。有关更多信息，请参见“[多播 DNS](#)” [29]和“[多播 DNS 服务搜索](#)” [29]。



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

/etc 文件命名服务的说明

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

NIS 命名服务的说明

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

NIS 名称空间信息存储在 NIS 映射中。NIS 映射旨在替换 UNIX `/etc` 文件以及其他配置文件。NIS 除了存储名称和地址外，还存储大量的其他信息。因此，NIS 名称空间存在大量映射。有关更多信息，请参见“[使用 NIS 映射](#)” [81]。

NIS 使用与 DNS 类似的客户机/服务器布局。复制的 NIS 服务器可向 NIS 客户机提供服务。主要的服务器称为主服务器，为确保其可靠，主服务器还具有备份，即从属服务

器。主服务器和从属服务器都使用 NIS 检索软件，并且都存储 NIS 映射。有关 NIS 体系结构和 NIS 管理的更多信息，请参见第 6 章 [设置和配置网络信息服务](#) 和第 7 章 [管理网络信息服务](#)。

LDAP 命名服务的说明

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

Oracle Solaris OS 支持 LDAP 与 Oracle Directory Server Enterprise Edition (之前称为 Sun Java System Directory Server) 以及其他 LDAP 目录服务器结合使用。

LDAP 在 [《使用 Oracle Solaris 11.2 目录和命名服务：LDAP》](#) 中进行了介绍，其中包括了从 NIS 转换到 LDAP 的说明。

有关单点登录以及设置和维护 Kerberos 验证服务的信息，请参见 [《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务》](#) 中的第 2 章，“关于 Kerberos 服务”。

名称服务转换的说明

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

命名服务：简要比较

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

	DNS	NIS	LDAP	文件
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

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

Oracle Solaris 名称服务的 IPv6 扩展

本节介绍在实现 IPv6 时引入的命名更改。可以将 IPv6 地址存储在任何 Oracle Solaris 命名服务、NIS、LDAP、DNS 和文件中。还可以使用 NIS over IPv6 RPC 传输机制来检索任何 NIS 数据。

DNS 的 IPv6 扩展

AAAA 资源记录是 IPv6 特定的资源记录，它已在 RFC 1886 "*DNS Extensions to Support IP Version 6*" 中指定。该 AAAA 记录将主机名映射到 128 位 IPv6 地址。IPv6 仍使用 PTR（指针）记录将 IP 地址映射为主机名。系统为 IPv6 地址保留了 128 位地址中的 32 个半字节（四位）。每个半字节都转换为与其相对应的十六进制 ASCII 值，然后再附加 ip6.arpa。

关于名称服务转换

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

- “名称服务转换概述” [19]
- “配置名称服务交换机” [23]
- “名称服务转换和口令信息” [26]

名称服务转换概述

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

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

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

名称服务转换还控制客户机的 DNS 转发，如第 3 章 [管理域名系统](#) 中所述。DNS 转发允许客户机访问 Internet。

用于名称服务转换的数据库和源

使用 SMF 服务配置名称服务转换支持的数据库。要获取这些数据库的列表，可使用 `svcfg` 命令，如以下示例中所示。

```
# svccfg -s name-service/switch listprop config
config                               application
```

config/default	astring	files
config/password	astring	"files nis"
config/group	astring	"files nis"
config/host	astring	"files nis"
config/network	astring	"nis [NOTFOUND=return] files"
config/protocol	astring	"nis [NOTFOUND=return] files"
config/rpc	astring	"nis [NOTFOUND=return] files"
config/ether	astring	"nis [NOTFOUND=return] files"
config/netmask	astring	"files nis"
config/bootparam	astring	"nis [NOTFOUND=return] files"
config/publickey	astring	"nis [NOTFOUND=return] files"
config/netgroup	astring	nis
config/automount	astring	"files nis"
config/alias	astring	"files nis"
config/service	astring	"files nis"
config/printer	astring	"user nis"
config/auth_attr	astring	"files nis"
config/prof_attr	astring	"files nis"
config/project	astring	"files nis"

下表说明了每个数据库存储的信息类型。从 SMF 的角度来看，这些数据库均视为服务的可配置属性。

表 2 名称服务转换的数据库

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

此外，名称服务转换中的 `default` 属性定义了当未定义源字符串时用于任何数据库的源字符串。此属性的值设置为 `files`，表示所有数据库及其信息都是在 `/etc` 目录本地发现的。您可以根据表 3 “用于名称服务转换的信息源” 中列出的源为 `default` 属性设置不同配置。有关过程，请参见[如何为所有命名数据库更改源 \[25\]](#)。

通过 `default` 属性，您可以配置通用于数据库的源，而不是配置每个数据库的源。

下表介绍了在名称服务转换中可以为上面列出的数据库列出的源的种类。

表 3 用于名称服务转换的信息源

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

名称服务转换的源格式

以下搜索条件格式可用来选择一个或多个信息源，并可用来指定源的使用顺序。

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

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

用于名称服务转换的状态消息

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

表 4 用于名称服务转换的状态消息

状态消息	说明
SUCCESS	在指定的源中找到了所请求的项。
UNAVAIL	该源不响应或者不可用。换句话说，无法找到或访问数据库源。
NOTFOUND	该源给出 "No such entry" (该项不存在) 的响应。换句话说，已访问了数据库，但未找到所需的信息。
TRYAGAIN	该源正忙，下次可能会响应。换句话说，已找到了数据库但无法响应查询。

名称服务转换的转换操作选项

可以指示名称服务转换用下表中显示的两个操作之一来响应状态消息。

表 5 从名称服务转换对状态消息的响应

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

此外，对于 TRYAGAIN 状态消息，可以定义以下操作：

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

用于名称服务转换的缺省搜索条件

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

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

- SUCCESS=return. 停止查找信息。使用已经找到的信息以继续。
- UNAVAIL=continue. 转到下一个名称服务转换源并继续搜索。如果该源是最后一个源或唯一的源，将返回 NOTFOUND 状态。
- NOTFOUND=continue. 转到下一个名称服务转换源并继续搜索。如果该源是最后一个源或唯一的源，将返回 NOTFOUND 状态。
- TRYAGAIN=forever. 无限制地搜索当前名称服务转换源。
- TRYAGAIN=3. 搜索当前源三次。在用完三次重试后，TRYAGAIN 操作转换为 continue，并搜索下一个名称服务转换源。

可以通过使用前面列表中显示的 `STATUS=action` 语法显式指定某个其他条件来更改缺省搜索条件。有关过程，请参见[如何为数据库配置搜索条件 \[24\]](#)。

注 - 名称服务转换中的查找是按照项目的列出顺序执行的。但是，口令更新将以相反的顺序执行，除非使用 `passwd -r repository` 命令另行指定了更新顺序。有关更多信息，请参见[“名称服务转换和口令信息” \[26\]](#)。

语法有误时该怎么办？

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

auto_home 和 auto_master

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

timezone 和名称服务转换

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

名称服务转换中的 keyserv 和 publickey 项



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

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

配置名称服务交换机

配置名称服务转换时，请同时执行以下操作：

- 指定数据库的源。
- 如果数据库有多个源，请指定源的搜索顺序。
- 定义针对相应搜索状态（也称为转换条件）的转换操作。

名称服务转换数据库或属性配置有缺省值。以下步骤说明了以不同方式配置特定属性的步骤。

▼ 如何更改数据库的源

此过程说明了如何为 host 数据库指定不同的源。假设数据库的原始源配置是文件和 NIS，这意味着进行主机查找时，将首先搜索本地文件，然后再搜索 NIS。重新配置名称服务转换，使其在 host 查找中也使用 DNS。

您可将此过程作为模板，用于为其他名称服务转换数据库配置源。

开始之前 请确保名称服务转换配置反映您的系统中命名服务的实际设置。例如，如果您希望 DNS 成为 host 查找的源，则还必须配置 DNS。

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. （可选）显示 host 数据库的当前配置。

```
# svccfg -s name-service/switch listprop config/host
config                               application
config/host                          astring          "files nis"
```

3. 更改 host 数据库的源定义。

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

4. 刷新名称服务转换的服务。

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

▼ 如何为数据库配置搜索条件

名称服务转换具有缺省搜索条件，如“用于名称服务转换的缺省搜索条件” [22] 中所述。

在此过程中，您希望重新定义在第一个源中找不到信息时针对 host 数据库的搜索机制。搜索机制此时应停止，而不是继续搜索下一个源。

1. 成为管理员。
有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。
2. (可选) 显示 host 数据库的当前配置。

```
# svccfg -s name-service/switch listprop config/host
config                               application
config/network                       astring          "files dns nis"
```

3. 为 host 数据库查找创建一个新的搜索条件，用于在第一个源中找不到信息的情况。

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

通过此配置，针对 network 数据库的搜索机制对于 SUCCESS 状态和 UNAVAILABLE 状态将使用缺省搜索条件。但是，如果未找到信息，搜索将立即停止。

4. 刷新名称服务转换的服务。

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

▼ 如何为所有命名数据库更改源

使用此过程为名称服务用于进行查找的所有数据库定义通用源。缺省情况下，通用源为 files。在此过程中，您将添加其他源。

1. 成为管理员。
有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。
2. (可选) 显示 default 属性的当前配置。

```
# svccfg -s name-service/switch listprop config/default
config                               application
config/default                       astring          files
```

3. 添加 NIS 作为缺省源。

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

```
svc:/system/name-service/switch> quit
```

4. 刷新名称服务转换的服务。

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

▼ 如何使用传统的 nsswitch.conf 文件

如果现有命名转换配置仍然使用 nsswitch.conf 文件，则执行此过程。此过程将命名转换配置从该文件迁移至 SMF（这是在 Oracle Solaris 中配置命名转换的方法）。

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 将 nsswitch.conf 文件复制到新系统。

确保将文件命名为 /etc/nsswitch.conf。

3. 将信息从该文件装入到 SMF 系统信息库中。

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

4. 刷新名称服务转换的服务。

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

名称服务转换和口令信息

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



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

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

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

提示 - 将 files 列在首位将允许 root 用户在大多数情况下登录，甚至在系统遇到某些网络或命名服务问题时也同样如此。

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

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

管理域名系统

本章提供了关于 DNS 服务器和客户机服务的信息。本章包含以下主题：

- “DNS 概述” [29]
- “DNS 和服务管理工具” [30]
- “管理 DNS (任务)” [31]
- “管理多播 DNS” [37]
- “DNS 参考信息” [38]

DNS 概述

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

多播 DNS

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

多播 DNS 服务搜索

网络服务包括打印、文件传输、音乐共享、照片服务器、文档和其他文件共享，以及由其他本地设备提供的服务。Oracle Solaris 中的 DNS 服务搜索支持功能包括了来自 Apple Inc. 的开源框架和工具，使应用程序能够在本 Oracle Solaris 发行版中使用 DNS 来通告和搜索网络服务。

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

有关 DNS 的相关资料

有关 DNS 和 BIND 管理的信息，请参见下面的文档：

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

DNS 和服务管理工具

使用服务管理工具 (Service Management Facility, SMF) 管理 DNS 服务器守护进程 `named`。有关 SMF 的概述，请参阅《在 Oracle Solaris 11.2 中管理系统服务》中的第 1 章, “服务管理工具简介”。有关更多详细信息，另请参阅 `svcadm(1M)`、`svcs(1)` 和 `svccfg(1M)` 手册页。

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

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

提示 - 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。

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

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

- 下面是 `svcs -l` 命令的示例及其输出。

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

- 如果您需要以不同的选项启动 DNS 服务，请使用 `svccfg` 命令更改 `svc:/network/dns/server` 服务的属性。有关示例，请参见[如何配置 DNS 服务器选项 \[33\]](#)。

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

管理 DNS (任务)

本节介绍了以下任务：

- [如何安装 DNS 软件包 \[31\]](#)
- [如何配置 DNS 服务器 \[32\]](#)
- [如何创建 `rndc.conf` 文件 \[32\]](#)
- [如何配置 DNS 服务器选项 \[33\]](#)
- [如何作为替代用户运行 DNS 服务 \[34\]](#)
- [如何启用 DNS 客户机 \[34\]](#)
- [如何对 DNS 服务器启动问题进行故障排除 \[35\]](#)
- [如何验证 DNS 配置 \[36\]](#)

▼ 如何安装 DNS 软件包

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

1. 成为管理员。
有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。
2. 安装 DNS 软件包。

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

▼ 如何配置 DNS 服务器

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

1. 成为管理员。
有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

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

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

3. (可选) 创建 `rndc` 配置文件。
该文件用来配置 DNS 服务器的远程控制访问。请参见[如何创建 `rndc.conf` 文件 \[32\]](#)。
4. (可选) 更改 `dns/server` 服务的配置信息。
请参见[如何配置 DNS 服务器选项 \[33\]](#)。

5. 启动 DNS 服务。

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

▼ 如何创建 `rndc.conf` 文件

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

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 创建 `rndc` 配置文件。

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

3. (可选) 重新启动 DNS 服务。

如果要在 DNS 服务器配置过程中创建 `rndc.conf` 文件，则可以跳过重新启动 DNS 服务，直至所有 DNS 服务器配置均已完成。

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

▼ 如何配置 DNS 服务器选项

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

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 更改 `dns/server` 服务的配置信息。

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

注 - 可以通过单个命令更改配置信息。

```
# svccfg -s dns/server:default options/ip_interfaces=IPv4
```

3. 更新 SMF 系统信息库并启用 DNS 服务。

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

4. (可选) 验证更改。

```
# svccfg -s dns/server:default listprop options/ip_interfaces
options/ip_interfaces astring IPv4
```

▼ 如何作为替代用户运行 DNS 服务

此过程说明了如何为用户指定相关授权来管理 named 守护进程。

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 向替代用户提供相应的授权。

```
# useradd -c "Trusted DNS administrator user" -s /usr/bin/pfbash \  
-A solaris.smf.manage.bind USER
```

3. 设置用户的服务属性。

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

4. 为新的进程 ID 文件创建一个目录。

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

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

5. 更改配置以使用新目录。

将以下行添加到 named.conf 文件：

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

6. 更新 SMF 系统信息库并重新启动 DNS 服务。

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

▼ 如何启用 DNS 客户机

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 配置 DNS 域。

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

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

3. 更新名称服务转换信息以使用 DNS。

第一个命令更新 SMF 系统信息库中 DNS 配置信息。

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

4. 启动运行 DNS 客户机所需的服务。

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

▼ 如何对 DNS 服务器启动问题进行故障排除

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

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 检查 DNS 服务状态。

```
# svcs -x dns/server:default
svc:/network/dns/server:default (BIND DNS server)
State: online since Tue Oct 18 19:35:00 2011
See: named(1M)
See: /var/svc/log/network-dns-server:default.log
```

Impact: None.

3. 检查 DNS 服务日志文件。

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

4. 检查系统日志消息。

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

5. 手动启动 `named` 守护进程。

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

```
# named -g
```

6. 在修复问题后，请清除“需要维护”状态。

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

▼ 如何验证 DNS 配置

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

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 根据需要更改配置文件。

在此示例中，更改了缺省目录。

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

3. 验证文件内容。

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

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

在此示例中，检查失败，因为 `/var/named` 目录尚未创建。

4. 更正报告的所有错误。

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

5. 重复步骤 3 和 4，直到不再报告错误。
6. (可选) 要在正在运行的服务中反映更改，请使用下面的方法之一：
 - 使用 `rndc` 命令和 `reload` 或 `reconfig` 选项来更新配置，具体取决于所做的更改。
 - 重新启动 `named` 服务。

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

管理多播 DNS

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

▼ 如何启用 mDNS 和 DNS 服务搜索

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

1. 成为管理员。
有关获取合适的权限来执行特定任务的更多信息，请参见 [《在 Oracle Solaris 11.2 中确保用户和进程的安全》](#) 中的“使用所指定的管理权限”。

2. 如果需要，安装 mDNS 软件包。

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

3. 更新名称服务转换信息。

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

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

4. 启用 mDNS 服务。

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

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

5. (可选) 如果需要，检查 mDNS 错误日志。

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

为 DNS 通告资源

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

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

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

下面是使用 DNS 服务搜索来通告服务的示例。

例 1 通告打印服务

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

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

要使此注册可用，必须在端口 515 上提供 LPR 服务。

例 2 通告 Web 页

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

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

DNS 参考信息

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

DNS 文件

下表介绍了与 DNS 服务关联的文件。

表 6 DNS 文件

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

DNS 命令和守护进程

下表介绍了与 DNS 服务关联的命令和守护进程。

表 7 DNS 命令和守护进程

文件名	功能
/usr/bin/dns-sd	查找或列出 mDNS 服务使用的资源。有关更多信息，请参见 dns-sd(1M) 手册页。
/usr/sbin/dig	从 DNS 服务器请求 DNS 响应。通常用于故障排除。有关更多信息，请参见 dig(1M) 手册页。
/usr/sbin/dnssec-dsfromkey	基于密钥文件生成 DS RR。有关更多信息，请参见 dnssec-dsfromkey(1M) 手册页。
/usr/sbin/dnssec-keyfromlabel	从加密设备检索选定的密钥并生成一个密钥文件。有关更多信息，请参见 dnssec-keygen(1M) 手册页。
/usr/sbin/dnssec-keygen	创建用于安全 DNS 和事务签名 (transaction signature, TSIG) 的密钥和密钥文件。有关更多信息，请参见 dnssec-keygen(1M) 手册页。
/usr/sbin/dnssec-signzone	对 DNS 区域进行签名。有关更多信息，请参见 dnssec-signzone(1M) 手册页。
/usr/sbin/host	执行简单的 DNS 查找，通常是将主机名转换为 IP 地址或者将 IP 地址转换为主机名。有关更多信息，请参见 host(1M) 手册页。
/usr/sbin/named	DNS 服务器守护进程，它响应来自客户机的信息请求。有关更多信息，请参见 named(1M) 手册页。
/usr/sbin/named-checkconf	检查 named.conf 文件的语法。有关更多信息，请参见 named(1M) 手册页。
/usr/sbin/named-checkzone	检查 DNS 区域文件的语法和完整性。有关更多信息，请参见 named-checkzone(1M) 手册页。
/usr/sbin/named-compilezone	转换 DNS 区域文件。有关更多信息，请参见 named-compilezone(1M) 手册页。

文件名	功能
/usr/sbin/nscfg	旧名称服务配置实用程序，可在旧名称服务配置文件与 SMF 系统信息库之间导入或导出名称服务配置。有关更多信息，请参见 nscfg(1M) 手册页。
/usr/sbin/nslookup	已过时：查询 DNS 服务器。请改用 dig 命令。
/usr/sbin/nsupdate	向 DNS 服务器提交 DNS 更新请求。有关更多信息，请参见 nsupdate(1M) 手册页。
/usr/sbin/rndc	提供对 DNS 服务器守护进程的远程控制。有关更多信息，请参见 rndc(1M) 手册页。
/usr/sbin/rndc-confgen	为 rndc 命令生成配置文件。有关更多信息，请参见 rndc-confgen(1M) 手册页。

在生成 BIND 时使用的编译标志

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

表 8 BIND 编译标志

标志名称	功能
<code>with-openssl</code>	使生成的 BIND 提供加密和安全套接字层 (Secure Sockets Layer, SSL) 支持，这是 DNSSEC 所必需的
<code>enable-threads</code>	启用多线程
<code>enable-devpoll</code>	使用 <code>/dev/poll</code> 驱动程序以快速轮询许多文件描述符
<code>disable-openssl-version-check</code>	禁用 OpenSSL 版本检查，因为 OpenSSL 是由一个单独的动态库提供的
<code>enable-fixed-rrset</code>	启用固定的资源记录集排序，这是实现向后兼容性所必需的
<code>with-pkcs11</code>	启用 OpenSSL 加密硬件支持

设置 Oracle Solaris Active Directory 客户机

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

- “nss_ad 命名服务模块概述” [41]
- “口令更新” [43]
- “nss_ad 命名服务模块如何从 AD 检索数据” [44]

nss_ad 命名服务模块概述

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

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

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

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

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

以下其他规则也适合 nss_ad 模块：

- 与 AD 一样，nss_ad 对用户名和组名执行不区分大小写的匹配。

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

▼ 如何配置 nss_ad 模块

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

1. 配置 DNS 服务。

有关说明，请参见[如何启用 DNS 客户机 \[34\]](#)。

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

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

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

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

2. 将 dns 添加到 hosts 的命名服务的列表中。

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

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

3. 确认 DNS 服务已启用且处于联机状态。

例如：

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

4. 使用 `kclient` 实用程序将系统加入 AD 域。

例如：

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

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

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

6. 启用 `idmap` 服务。

```
# svcadm enable idmap
```

7. 更新名称服务转换服务的 SMF 系统信息库。

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

注 - 每次刷新名称服务转换时，如有必要，`nscd` 模块都将自动重新启动。

8. 确认您可以访问 AD 中的 `user` 和 `group` 信息。

例如：

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

口令更新

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

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

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

nss_ad 命名服务模块如何从 AD 检索数据

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

检索 passwd 信息

以下语法显示了 passwd 项的正确格式：

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

有关更多信息，请参见 [passwd\(4\)](#) 手册页。

nss_ad 模块从 AD 检索 passwd 信息，如下所述：

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

检索 shadow 信息

以下语法显示了 shadow 项的正确格式：

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

有关更多信息，请参见 [shadow\(4\)](#) 手册页。

nss_ad 模块从 AD 检索 shadow 信息，如下所述：

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

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

检索 group 信息

以下语法显示了 group 项的正确格式：

groupname:password:gid:user-list

有关更多信息，请参见 [group\(4\)](#) 手册页。

nss_ad 模块从 AD 检索信息，如下所述：

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

关于网络信息服务

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

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

本章包含以下主题：

- “NIS 简介” [47]
- “NIS 计算机类型” [48]
- “NIS 元素” [49]
- “NIS 绑定” [54]

NIS 简介

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

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

注 - 在一些上下文中，计算机名称是指主机名或计算机名称。本讨论中使用计算机，但一些屏幕消息或 NIS 映射名中可能使用主机或计算机。

NIS 体系结构

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

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



**Graphic Not Accessible
Check Declaration**

因此，此物理网络将被编排为一个 NIS 域。



**Graphic Not Accessible
Check Declaration**

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

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

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

NIS 计算机类型

NIS 计算机有三种类型。

- 主服务器
- 从属服务器
- NIS 服务器的客户机

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

NIS 服务器

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

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

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

NIS 客户机

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

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

NIS 元素

NIS 命名服务由以下元素组成：

- 域（请参见“[NIS 域](#)” [49]）
- 守护进程（请参见“[NIS 守护进程](#)” [50]）
- 命令（请参见“[NIS 命令](#)” [50]）
- 映射（请参见“[NIS 映射](#)” [51]）

NIS 域

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

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

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

NIS 守护进程

NIS 服务是由下表中显示的守护进程提供的。NIS 服务由 SMF 进行管理。使用 `svcadm` 命令可以对此服务执行启用、禁用或重新启动等管理操作。有关 SMF 的概述，请参阅《在 Oracle Solaris 11.2 中管理系统服务》中的第 1 章, “服务管理工具简介”。有关更多详细信息，另请参阅 `svcadm(1M)` 和 `svcs(1)` 手册页。

表 9 NIS 守护进程

守护进程	功能
nscd	一项客户机服务，提供了一个用于大多数名称服务请求的高速缓存，该高速缓存由 <code>svc:/system/name-service/cache</code> 服务进行管理
rpc.yppasswdd	由 <code>svc:/network/nis/passwd</code> 服务管理的 NIS 口令更新守护进程 注 - <code>rpc.yppasswdd</code> 守护进程将所有以 <code>r</code> 开头的 shell 视为受限制的 shell。例如，如果您位于 <code>/bin/rksh</code> 中，将不允许从该 shell 更改到其他 shell 中。如果您有以 <code>r</code> 开头的 shell，但不想受到此类限制，请参阅第 8 章 网络信息系统故障排除 了解解决方法。
rpc.yppupdated	用于修改诸如 <code>publickey</code> 之类的映射的一个守护进程，由 <code>svc:/network/nis/update</code> 服务进行管理
yplibind	由 <code>svc:/network/nis/client</code> 服务管理的绑定进程
ypserv	由 <code>svc:/network/nis/server</code> 服务管理的服务器进程
ypxfrd	由 <code>svc:/network/nis/xfr</code> 服务管理的一个高速映射传送守护进程

NIS 命令

许多命令都支持 NIS 服务，下表中介绍了这些命令。

表 10 NIS 命令摘要

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

NIS 映射

NIS 映射中的信息以 `ndbm` 格式存储。[ypfiles\(4\)](#) 和 [ndbm\(3C\)](#) 手册页解释了映射文件的格式。

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

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

映射中进行查找。当服务器已知计算机的地址而需要查找其名称时，它将在 `hosts.byaddr` 映射中进行查找。

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

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

缺省 NIS 映射

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

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

下表介绍了缺省 NIS 映射并列出了每个映射的相应源文件名称。

表 11 NIS 映射说明

映射名	相应的源文件	说明
<code>audit_user</code>	<code>audit_user</code>	包含用户审计预选数据。
<code>auth_attr</code>	<code>auth_attr</code>	包含授权名称和说明。
<code>bootparams</code>	<code>bootparams</code>	包含客户机在引导期间所需文件的路径名： <code>root</code> 、 <code>swap</code> ，也可能是其他名称。
<code>ethers.byaddr</code>	<code>ethers</code>	包含计算机名和以太网地址。以太网地址是映射中的关键字。
<code>ethers.byname</code>	<code>ethers</code>	与 <code>ethers.byaddr</code> 相同，但关键字是计算机名而非以太网地址。
<code>exec_attr</code>	<code>exec_attr</code>	包含配置文件执行属性。
<code>group.bygid</code>	<code>group</code>	包含以组 ID 作为关键字的组安全信息。
<code>group.byname</code>	<code>group</code>	包含以组名作为关键字的组安全信息。
<code>hosts.byaddr</code>	<code>hosts</code>	包含计算机名和 IP 地址，以 IP 地址作为关键字。
<code>hosts.byname</code>	<code>hosts</code>	包含计算机名和 IP 地址，以计算机（主机）名作为关键字。
<code>mail.aliases</code>	<code>aliases</code>	包含别名和邮件地址，以别名作为关键字。
<code>mail.byaddr</code>	<code>aliases</code>	包含邮件地址和别名，以邮件地址作为关键字。
<code>netgroup.byhost</code>	<code>netgroup</code>	包含组名、用户名和计算机名。
<code>netgroup.byuser</code>	<code>netgroup</code>	与 <code>netgroup.byhost</code> 相同，但关键字为用户名。

映射名	相应的源文件	说明
netgroup	netgroup	与 netgroup.byhost 相同，但关键字为组名。
netid.byname	passwd, hosts group	用于 UNIX 形式的验证。包含计算机名和邮件地址（包括域名）。如果存在可用的 netid 文件，则除了查询通过其他文件提供的数据外，还会查询该文件。
publickey.byname	publickey	包含安全 RPC 使用的公钥数据库。
netmasks.byaddr	netmasks	包含要与 IP 一起提交的网络掩码，以地址作为关键字。
networks.byaddr	networks	包含系统已知的网络的名称及其 IP 地址，以地址作为关键字。
networks.byname	networks	与 networks.byaddr 相同，但关键字为网络的名称。
passwd.adjunct.byname	passwd 和 shadow	包含 C2 客户机的审计信息和隐藏的口令信息。
passwd.byname	passwd 和 shadow	包含以用户名作为关键字的口令信息。
passwd.byuid	passwd 和 shadow	与 passwd.byname 相同，但关键字为用户 ID。
prof_attr	prof_attr	包含执行配置文件的属性。
protocols.byname	protocols	包含网络可识别的网络协议。
protocols.bynumber	protocols	与 protocols.byname 相同，但关键字为协议编号。
rpc.bynumber	rpc	包含系统可识别的 RPC 的程序编号和名称。关键字为 RPC 程序编号。
services.byname	services	列出网络可识别的 Internet 服务。关键字为端口或协议。
services.byservice	services	列出网络可识别的 Internet 服务。关键字为服务名。
user_attr	user_attr	包含用户和角色的扩展属性。
ypservers	不适用	列出网络可识别的 NIS 服务器。

当实现了 NIS 到 LDAP 转换时，ageing.byname 映射包含 yppasswdd 守护进程用来在目录信息树 (directory information tree, DIT) 中读写口令生命期信息的信息。如果不使用口令生命期，可以将其从映射文件中注释掉。有关 NIS 到 LDAP 转换的更多信息，请参见《使用 Oracle Solaris 11.2 目录和命名服务：LDAP》中的第 8 章，“从 NIS 转换为 LDAP”。

使用 NIS 映射

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

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

例如，向运行 NIS 的网络中添加新用户时，只需要更新主服务器中的输入文件并运行 `make` 命令即可。此命令将自动更新 `passwd.byname` 和 `passwd.byuid` 映射。然后，这些映射将传送给从属服务器，并可供域中所有客户机及其程序使用。当客户机或应用程序通过用户名或 UID 来请求信息时，NIS 服务器将相应地引用 `passwd.byname` 或 `passwd.byuid` 映射，并将所请求的信息发送到客户机。

您可以使用 `ypcat` 命令显示映射中的值。`ypcat` 基本格式为：

```
% ypcat mapname
```

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

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

```
% ypwhich -m mapname
```

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

NIS 映射昵称

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

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

NIS 绑定

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

- 服务器列表 – 在服务器列表模式下，`ybind` 进程查询 `svc:/network/nis/domain` 服务来获取域中所有 NIS 服务器的名称。`ybind` 进程只绑定到此文件中的服务器。可以通过使用 `svccfg` 命令添加 NIS 服务器。它们将添加到 `svc:/network/nis/domain` 服务中的 `config/ypservers` 属性。每个属性值都代表一台特定的 NIS 服务器。此外，在 `svc:/network/nis/domain` 服务中指定的任何服务器名称在 `/etc/inet/hosts` 文件中都必须有一个对应的项，NIS 绑定功能才能工作。

- 广播 - ypbind 进程还可以使用 RPC 广播来启动绑定。因为广播只是不会进一步路由的本地子网事件，所以必须至少有一台服务器（主服务器或从属服务器）与客户机位于同一个子网中。服务器本身可能会存在于不同的子网中，因为映射传播可跨越子网边界。在子网环境中，一种常用方法是使子网路由器成为 NIS 服务器。这样，域服务器便可为任何一个子网接口上的客户机提供服务。

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

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

要确定当前正在为特定客户机提供服务的 NIS 服务器，请使用以下命令。

```
% ypwhich machinename
```

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

服务器列表模式

在服务器列表模式下，绑定进程的工作过程如下：

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

广播模式

在广播模式下，绑定进程的工作过程如下：

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

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

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

设置和配置网络信息服务

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

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

本章包含以下主题：

- “配置 NIS 任务列表” [57]
- “配置 NIS 之前的准备工作” [58]
- “规划 NIS 域” [59]
- “准备主服务器” [60]
- “在 NIS 服务器上启动和停止 NIS 服务” [66]
- “设置 NIS 从属服务器” [68]
- “管理 NIS 客户机” [73]

配置 NIS 任务列表

任务	说明	有关指导
为转换准备源文件。	在基于本地 /etc 文件生成 NIS 映射之前，您需要整理这些文件。	如何为转换准备源文件 [61]
设置主服务器。	创建一台主服务器，这是 NIS 信息的主要来源。	如何设置主服务器 [64]
在主服务器上启动 NIS。	开始从 NIS 服务器提供 NIS 信息。	“在 NIS 服务器上启动和停止 NIS 服务” [66]
设置从属服务器。	创建一台从属服务器，这是 NIS 信息的次要来源。	如何设置从属服务器 [69]
设置 NIS 客户机。	使客户机能够使用 NIS 信息。	“管理 NIS 客户机” [73]

配置 NIS 之前的准备工作

在配置 NIS 名称空间之前，必须执行以下操作。

- 规划 NIS 域。有关详细信息，请参见“[规划 NIS 域](#)” [59]。
- 在将使用 NIS 的所有计算机上安装正确配置的名称服务转换信息。有关详细信息，请参见[第 2 章 关于名称服务转换](#)。

NIS 和服务管理工具

NIS 服务由服务管理工具管理。有关 SMF 的概述，请参见《[在 Oracle Solaris 11.2 中管理系统服务](#)》中的第 1 章，“[服务管理工具简介](#)”。有关更多详细信息，另请参阅 [svcadm\(1M\)](#) 和 [svcs\(1\)](#) 手册页。

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

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

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

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

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

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

- 以下是 `svcs -l` 命令及其输出的示例：

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

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

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

规划 NIS 域

在将计算机配置为 NIS 服务器或客户机之前，必须规划 NIS 域。

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

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

部，则可将其中一个域命名为 sales.example.com，将另一个域命名为 manf.example.com。

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

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

标识 NIS 服务器和客户机

选择一台计算机作为主服务器。决定哪些计算机将作为从属服务器。

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

准备主服务器

以下各节介绍如何为主服务器准备源文件和 passwd 文件。

准备主服务器（任务列表）

下表列出了准备 NIS 主服务器的任务。

任务	说明	有关指导
准备用于转换的源文件。	准备用于转换到 NIS 映射的源文件。	如何为转换准备源文件 [61]
安装 NIS 主服务器软件包。	安装 NIS 主服务器软件包。	如何安装 NIS 主服务器软件包 [64]
设置主服务器。	配置 NIS 主服务器并在主服务器上创建 NIS 映射。	如何设置主服务器 [64]
支持多个 NIS 域。	设置 NIS 主服务器以支持多个域。	如何在一台主服务器上支持多个 NIS 域 [66]

源文件目录

源文件通常位于主服务器上的 /etc 目录中。但是，将源文件存储在 /etc 中并不合适，因为这样映射中的内容将与主服务器上的本地文件中的内容相同。这是 passwd 和

shadow 文件的一个特殊问题，因为所有用户都具有对主服务器映射的访问权限，并且 root 口令将通过 passwd 映射传递到所有 NIS 客户机。有关其他信息，请参见“passwd 文件和名称空间安全性” [61]。

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

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

passwd 文件和名称空间安全性

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

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



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

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

▼ 如何为转换准备源文件

此过程说明了如何为转换到 NIS 映射准备源文件。

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 检查主服务器上的源文件以确保它们反映了您的系统。

检查以下文件：

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

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

该源目录是在 `/var/yp/Makefile` 中通过 `DIR` 宏定义的。

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

口令源目录是在 `Makefile` 中通过 `PWDIR` 宏定义的。

5. 将 **audit_user**、**auth_attr**、**exec_attr** 和 **prof_attr** 文件复制到选择的权限源目录。

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



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

6. 检查 `/etc/mail/aliases` 文件。

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

注 - 通过将 `/var/yp/Makefile` 中的 `ALIASES = /etc/mail/aliases` 项指向其他位置，可以添加特定于 NIS 的邮件别名文件。然后当您运行 `make` 命令时，`ALIASES` 项将创建一个 `mail.aliases` 映射。当 `/etc/nsswitch.conf` 文件正确地将 `files` 和 `nis` 作为目标时，`sendmail` 服务除了使用 `/etc/mail/aliases` 文件，还使用此映射。请参阅“[修改和使用 /var/yp/Makefile](#)” [84]。

7. 清除源文件中的所有注释以及其他多余的行和信息。
这些操作可以通过一个 `sed` 或 `awk` 脚本或者使用文本编辑器来执行。`/var/yp/Makefile` 会自动为您执行某些文件清理，但最好在运行 `make` 命令之前手动检查并清理这些文件。
8. 确保所有源文件中的数据都具有正确的格式。
对于该特定文件，源文件数据的格式必须是正确的。请检查各文件对应的手册页，以确保每个文件都具有正确格式。

准备 `/var/yp/Makefile`

检查源文件并将其复制到源文件目录之后，您现在需要将这些源文件转换为 NIS 服务使用的 `ndbm` 格式的映射。在主服务器上调用 `ypinit` 时，它会自动执行此操作，如[如何设置主服务器](#) [64]中所述。

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

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

- 非缺省映射
如果创建了自己的非缺省源文件并想将其转换为 NIS 映射，必须将这些源文件添加到 `Makefile`。
- DIR 值
如果希望 `Makefile` 使用 `/etc` 目录以外的其他目录中存储的源文件（如“[源文件目录](#)” [60]中所述），必须将 `Makefile` 中的 `DIR` 的值更改为希望使用的目录。更改 `Makefile` 中的该值时，请勿使行缩进。
- PWDIR 值
如果希望 `Makefile` 使用 `/etc` 目录以外的其他目录中存储的 `passwd`、`shadow` 和 `adjunct` 源文件，必须将 `Makefile` 中 `PWDIR` 的值更改为希望使用的目录。更改 `Makefile` 中的该值时，请勿使行缩进。

- RBACDIR 值

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

- 域名解析程序

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

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

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

▼ 如何安装 NIS 主服务器软件包

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

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 安装 NIS 主服务器软件包。

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

▼ 如何设置主服务器

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

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

1. 成为 NIS 主服务器的管理员。

有关更多信息，请参见《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. 编辑 /etc/inet/hosts 文件。

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

例如：

```
172.16.0.1 master.example.com master
172.16.0.2 slave1.example.com slave1
172.16.0.3 slave2.example.com slave2
```

3. 在主服务器上生成新的映射。

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

4. 键入 NIS 服务器的名称。

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

5. 确认已设置了 NIS 域名。

```
# domainname
example.com
```

6. 如果发生了非致命错误，请键入 `y` 以选择停止进程。

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

注 - 当某些映射文件不存在时，会出现非致命错误。此错误不会影响 NIS 的功能。如果未自动创建这些映射，可能需要手动添加。有关所有缺省 NIS 映射的说明，请参阅[“缺省 NIS 映射” \[52\]](#)。

7. 选择是否应删除源文件。

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

8. ypinit 命令构造服务器列表之后，将调用 `make` 命令。

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

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

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

此命令会将 passwd 映射推送到目标域，而不是主服务器所属的域。

9. 如果需要，对名称服务转换进行更改。
请参见“[配置名称服务交换机](#)” [23]。

▼ 如何在一台主服务器上支持多个 NIS 域

通常，NIS 主服务器仅支持一个 NIS 域。但是，如果要使用一台主服务器来支持多个域，则在设置服务器为更多域提供服务时，必须对[如何设置主服务器](#) [64]中所述的步骤稍做修改。

1. 成为 NIS 主服务器的管理员。
有关更多信息，请参见《[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. 更改 NIS 域名。

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

3. 生成 NIS 文件。

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

在 NIS 服务器上启动和停止 NIS 服务

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

下面是在服务器中启动或停止 NIS 服务的三种方法：

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

在 NIS 服务器上启动和停止 NIS 服务（任务列表）

下表列出了通过使用 svcadm 命令启动和停止 NIS 服务的任务。

任务	说明	有关指导
手动启用 NIS 服务器服务。	使用 <code>svcadm enable</code> 命令可启用 NIS 服务器服务。	如何手动启动 NIS 服务器服务 [67]
禁用 NIS 服务器服务。	使用 <code>svcadm disable</code> 命令可禁用 NIS 服务器服务。	如何禁用 NIS 服务器服务 [67]
刷新 NIS 服务器服务。	使用 <code>svcadm refresh</code> 命令可刷新 NIS 服务。	如何刷新 NIS 服务器服务 [68]

自动启动 NIS 服务

如果启用了 `svc:/network/nis/server` 服务，则 `ypserv` 守护进程在引导时会自动启动。有关更多信息，请参见[如何设置主服务器 \[64\]](#)。

▼ 如何手动启动 NIS 服务器服务

在使用 `svcadm` 命令时，只有当运行了该服务的多个实例时，实例名称才是必需的。有关更多信息，请参见[“NIS 和服务管理工具” \[58\]](#)或 `svcadm(1M)` 手册页。

1. 成为管理员。
有关获取合适的权限来执行特定任务的更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“使用所指定的管理权限”。
2. 启动所需的 NIS 服务器服务。

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

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

▼ 如何禁用 NIS 服务器服务

在使用 `svcadm` 命令时，只有当运行了该服务的多个实例时，特定实例名称才是必需的。有关更多信息，请参见[“NIS 和服务管理工具” \[58\]](#)或 `svcadm(1M)` 手册页。

1. 成为管理员。
有关获取合适的权限来执行特定任务的更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“使用所指定的管理权限”。
2. 禁用所需的 NIS 服务器服务。

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

注 - 还可以使用 `ypstop` 命令禁用 NIS 服务。

▼ 如何刷新 NIS 服务器服务

此过程说明了在进行配置更改后如何刷新 NIS 服务器服务。

在使用 `svcadm` 命令时，只有当运行了该服务的多个实例时，特定实例名称才是必需的。有关更多信息，请参见“[NIS 和服务管理工具](#)” [58]或 [svcadm\(1M\)](#) 手册页。

1. 成为管理员。
有关获取合适的权限来执行特定任务的更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“[使用所指定的管理权限](#)”。
2. 刷新所需的 NIS 服务器服务。

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

设置 NIS 从属服务器

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

设置 NIS 从属服务器（任务列表）

下表列出了设置 NIS 从属服务器的任务。

任务	说明	有关指导
设置从属服务器。	将系统配置为 NIS 从属服务器。	如何设置从属服务器 [69]
在从属服务器上启动 NIS。	使用 <code>svcadm</code> 命令可启动 NIS 客户机和服务器服务。	如何在从属服务器上启动 NIS [70]
添加新的从属服务器。	在启动 NIS 服务后配置新的从属服务器。	如何添加新的从属服务器 [71]

准备从属服务器

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

注 - 虽然 DNS 域名不区分大小写，但 NIS 域名区分大小写。

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

▼ 如何设置从属服务器

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

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 编辑 `/etc/inet/hosts` 文件。

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

例如：

```
172.16.0.1 master.example.com master
172.16.0.2 slave1.example.com slave1
172.16.0.3 slave2.example.com slave2
```

3. 在从属服务器上，将目录转至 `/var/yp`。

注 - 必须先将新的从属服务器配置为 NIS 客户机，它才能首次从主服务器中获取 NIS 映射。有关详细信息，请参见“管理 NIS 客户机” [73]。在更改了 NIS 主映射后，可使用 `yppush` 命令将新的映射传播至 NIS 从属服务器。有关传播 NIS 映射的信息，请参见“更新和修改现有映射” [87]。

4. 将从属服务器初始化为 NIS 客户机。

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

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

5. 确定客户机服务是否正在运行，然后根据需要启动或重新启动这些服务。

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

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

- a. 如果客户机服务正在运行，请重新启动客户机服务。

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

- b. 如果客户机服务未在运行，请启动客户机服务。

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

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

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

- a. 如果主 NIS 服务器正在运行，请重新启动该服务。

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

- b. 如果主 NIS 服务器未在运行，请启动该服务。

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

7. 将此计算机初始化为从属服务器。

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

其中，*master* 是现有的 NIS 主服务器的计算机名。

▼ 如何在从属服务器上启动 NIS

以下过程说明了如何在从属服务器上启动 NIS。

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

- 重新启动客户机服务并启动所有 NIS 服务器进程。

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

▼ 如何添加新的从属服务器

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

- 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”。

- 转至 NIS 域目录。

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

- 反汇编 `ypservers` 文件。

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

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

- 编辑 `/tmp/temp_file` 文件。

将新的从属服务器的名称添加到服务器列表中。然后，保存并关闭该文件。

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

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

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

- 验证 `ypservers` 映射是否正确。

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

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

`makedbm` 命令会在屏幕上显示 `ypservers` 中的每项。

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

- 成为新的 NIS 从属服务器上的管理员。

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”。

8. 确认已设置了 NIS 域名。

```
# domainname
example.com
```

9. 设置新从属服务器的 NIS 域目录。

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

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

10. 将此计算机初始化为从属服务器。

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

其中，`ypmaster` 是现有的 NIS 主服务器的计算机名。

11. 停止作为 NIS 客户机运行的计算机。

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

12. 确定客户机服务是否正在运行，然后根据需要启动或重新启动这些服务。

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

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

- a. 如果客户机服务正在运行，请重新启动客户机服务。

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

- b. 如果客户机服务未在运行，请启动客户机服务。

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

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

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

- a. 如果 NFS 服务器正在运行，请重新启动该服务。

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

- b. 如果 NIS 服务器未在运行，请启动该服务。

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

管理 NIS 客户机

本节介绍了两种配置客户机使用 NIS 作为其命名服务的方法。

注 - Oracle Solaris OS 不支持 NIS 客户机与本地 LDAP 客户机共存于同一客户机中的配置。

- 广播模式 - 用于将客户机配置为使用 NIS 的首选方法。有关说明，请参见[如何在广播模式下配置 NIS 客户机 \[73\]](#)。
- 服务器列表方法 - 用于配置客户机的另一种方法，它使用 `ypinit` 命令来指定服务器。有关说明，请参见[如何将 NIS 客户机配置为使用特定的 NIS 服务器 \[74\]](#)。

管理 NIS 客户机（任务列表）

下表列出了管理 NIS 客户机的任务。

任务	说明	有关指导
在广播模式下配置 NIS 客户机。	通过搜索本地子网上存在的 NIS 服务器来配置 NIS 客户机。	如何在广播模式下配置 NIS 客户机 [73]
使用特定的 NIS 服务器配置 NIS 客户机。	使用特定的 NIS 主服务器和从属服务器配置 NIS 客户机。	如何将 NIS 客户机配置为使用特定的 NIS 服务器 [74]
禁用 NIS 客户机服务。	使用 <code>svcadm</code> 命令可禁用 NIS 客户机服务。	禁用 NIS 客户机服务 [75]

▼ 如何在广播模式下配置 NIS 客户机

这是用于建立 NIS 客户机的首选方法。

当您启动 `nis/client` 服务时，该服务运行 `ybind` 命令，该命令在本地子网中搜索 NIS 服务器。如果找到了一个子网，则 `ybind` 将绑定到该子网。这种搜索被称为广播。如果在客户机的本地子网中不存在 NIS 服务器，则 `ybind` 将无法绑定，并且客户机无法从 NIS 服务获取名称空间数据。有关说明，请参见[如何将 NIS 客户机配置为使用特定的 NIS 服务器 \[74\]](#)。

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“使用所指定的管理权限”。

2. 设置 NIS 域名。

```
# domainname  
  
example.com
```

3. 如果需要，对名称服务转换进行更改。

请参见[“配置名称服务交换机” \[23\]](#)。

4. 启动 NIS 客户机服务。

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

▼ 如何将 NIS 客户机配置为使用特定的 NIS 服务器

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

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“使用所指定的管理权限”。

2. 设置 NIS 域名。

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

3. 运行客户机配置脚本。

```
# ypinit -c
```

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

▼ 禁用 NIS 客户机服务

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 禁用 NIS 客户机服务。

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


管理网络信息服务

本章介绍了如何管理 NIS。本章包含以下主题：

- “口令文件和名称空间安全” [77]
- “管理 NIS 用户” [78]
- “使用 NIS 映射” [81]
- “更新和修改现有映射” [87]
- “使用 NIS 服务器” [92]

注 - NIS 服务由服务管理工具管理。使用 `svcadm` 命令可以对此服务执行启用、禁用或重新启动等管理操作。有关将 SMF 与 NIS 结合使用的更多信息，请参见“[NIS 和服务管理工具](#)” [58]。有关 SMF 的概述，请参见《[在 Oracle Solaris 11.2 中管理系统服务](#)》中的第 1 章，“[服务管理工具简介](#)”。有关更多详细信息，另请参阅 [svcadm\(1M\)](#) 和 [svcs\(1\)](#) 手册页。

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

口令文件和名称空间安全

出于安全原因，请遵循以下原则。

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

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

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

管理 NIS 用户

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

▼ 如何向 NIS 域添加新 NIS 用户

1. 成为 NIS 主服务器的管理员。

有关更多信息，请参见《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 `useradd` 命令创建新用户的登录 ID。

```
# useradd userID
```

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

3. 创建新用户的初始口令。

要创建新用户可用来登录的初始口令，请运行 `passwd` 命令。

```
# passwd userID
```

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

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

4. 将新项复制到主服务器的 `passwd` 映射输入文件中。

主服务器上的映射源文件应位于 `/etc` 之外的某个目录中。从 `/etc/passwd` 和 `/etc/shadow` 文件复制新行并将其粘贴到服务器上的 `passwd` 映射输入文件中。有关其他信息，请参见“[口令文件和名称空间安全](#)” [77]。

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

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

要从 `/etc/shadow` 中复制的有关 `brown` 的行将如下所示：

```
brown:$5$YiFpYwXb$6jJKG/gKdfkKtLTbemORnbeH.qsv09MwBD3ulTihq9B:6445:::~:~:~
```

5. 确保 `Makefile` 正确指定了口令输入文件所在的目录。
6. 从 `/etc/passwd` 和 `/etc/shadow` 输入文件中删除新用户的项。
出于安全原因，请不要在 NIS 主服务器的 `/etc/passwd` 和 `/etc/shadow` 文件中保留用户项。在将新用户的项复制到其他某个目录中存储的 NIS 映射源文件后，请在主服务器上使用 `userdel` 命令删除新用户。

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

```
# userdel brown
```

有关 `userdel` 的更多信息，请参见 [userdel\(1M\)](#) 手册页。

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

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

8. 通知新用户已为其登录 ID 指定的初始口令。
登录后，新用户随时可以通过运行 `passwd` 设置不同口令。

设置用户口令

用户可以运行 `passwd` 来更改自己的口令。

```
% passwd username
```

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

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

NIS 网络组

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

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

每个网络组都有一个网络组名。网络组不直接设置权限或访问权限。而是由其他 NIS 映射在通常使用用户名或计算机名的地方使用网络组名。例如，假设您创建了一个由网络管理员组成的网络组，名为 `netadmins`。要向 `netadmins` 网络组的所有成员授予对给定计算机的访问权限，只需向该计算机的 `/etc/passwd` 文件中添加一个 `netadmin` 项即可。网络组名也可以添加到 `/etc/netgroup` 文件中并传播到 NIS `netgroup` 映射。有关使用网络组的更多详细信息，请参见 [netgroup\(4\)](#) 手册页。

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

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

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

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

下面是两个 `netgroup` 输入文件项样例，每个样例都创建了一个名为 `admins` 的网络组，网络组由用户 `hauri` 和 `juanita`（后者在远程域 `sales` 中）以及计算机 `altair` 和 `sirius` 组成。

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

各种程序在登录、远程挂载、远程登录以及远程创建 `shell` 期间会使用 NIS 映射进行权限检查。这些程序包括 `mountd` 和 `login`。`login` 命令在 `passwd` 数据库中遇到网络组名时，会在网络组映射中查询用户分类。`mountd` 守护进程在 `/etc/dfs/dfstab` 文件中遇到网络组名时，会在网络组映射中查询用户分类。实际上，如果使用 `ruserok` 接口的任何

程序遇到了 `/etc/hosts.equiv` 或 `.rhosts` 文件中的网络组名称，它们都将在网络组映射中查找计算机和用户分类。

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

使用 NIS 映射

本节包含以下信息：

- “获取映射信息” [81]
- “更改映射的主服务器” [82]
- “修改配置文件” [83]
- “修改和使用 `/var/yp/Makefile`” [84]

获取映射信息

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

要列出映射中的所有值，请键入以下命令：

```
% ypcat mapname
```

要同时列出映射中的关键字和值（如果有），请键入以下命令：

```
% ypcat -k mapname
```

要列出所有映射昵称，请键入以下任何命令：

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

要列出所有可用映射及其主服务器，请键入以下命令：

```
% ypwhich -m
```

要列出特定映射的主服务器，请键入以下命令：

```
% ypwhich -m mapname
```

要使映射中的项与关键字匹配，请键入以下命令：

```
% ypmatch key mapname
```

如果要查找的项不是映射中的关键字，请键入以下命令：

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

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

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

更改映射的主服务器

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

▼ 如何更改映射的主服务器

1. 成为 NIS 主服务器的管理员。

有关更多信息，请参见《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. 更改目录。

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

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

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

4. 要更新映射或重新进行映射，请键入以下命令：

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

5. 如果旧的主服务器仍为 NIS 服务器，请远程登录 (ssh) 到该旧的主服务器并编辑 `/var/yp/Makefile`。
确保注释掉 Makefile 中创建 `sites.byname` 映射的部分，以便不再创建映射。
6. 如果 `sites.byname` 仅作为 `ndbm` 文件存在，请新的主服务器上重新创建映射。
首先，通过使用 `yycat` 命令反汇编 `sites.byname` 文件的副本。然后，通过 `makedbm` 运行反汇编的版本。

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

新的主服务器上创建映射后，必须向其他从属服务器发送新映射的副本。不要使用 `yypush`，因为其他从属服务器会试图从旧的主服务器（而不是新的主服务器）中获取新副本。解决此问题的一个典型方法是从新的主服务器向旧的主服务器传送一份映射的副本。为此，请在旧的主服务器上成为超级用户或承担等效角色，并键入以下命令。

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

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

如果此方法失败，可以使用 `root` 用户身份登录每台 NIS 服务器并执行其上所示的 `yycfr` 命令。

修改配置文件

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

进行以下任何一项操作时，请使用本节中的过程：

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

▼ 如何修改配置文件

请牢记以下几点。

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

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 停止 NIS 服务器。

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

3. 对文件进行必要的更改。

4. 启动 NIS 服务器。

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

修改和使用 /var/yp/Makefile

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

提示 - 请保留原始的 Makefile 的未修改副本，以供将来参考。

使用 Makefile

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

通常，会使用 awk、sed 或 grep 对可读的文本文件进行过滤，以使其适合输入到 makedbm。有关示例，请参阅缺省的 Makefile。有关 make 命令的常规信息，请参见 [make\(1S\)](#)。

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

向 Makefile 中添加项涉及以下步骤。

- 向 all 规则中添加数据库名称
- 编写 time 规则

- 为数据库添加规则

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

要将这些映射添加到 NIS 数据库，需要修改 Makefile。

更改 Makefile 宏/变量

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

这些变量如下所示：

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

修改 Makefile 项

以下过程介绍如何在 Makefile 中添加和删除数据库。

▼ 如何修改 /var/yp/Makefile 以使用特定数据库

此过程要求您已配置了一台 NIS 主服务器。

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 通过添加要添加的数据库的名称来修改以单词 `all` 开头的行：

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

各项的顺序不相关，但连续行开头的空白处必须为制表符，而不是空格。

3. 在 Makefile 的末尾添加以下行：

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

4. 在该文件中间添加 `auto_direct.time` 项。

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

其中

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

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

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

5. 运行 `make` 命令。

```
# make mapname
```

其中，`mapname` 是要创建的映射的名称。

▼ 如何修改 Makefile 以删除数据库

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

1. 从 `all` 规则中删除数据库的名称。
2. 为要删除的数据库删除或注释掉数据库规则。
例如，要删除 `hosts` 数据库，应删除 `hosts.time` 项。
3. 删除 `time` 规则。

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

4. 从主服务器和从属服务器中删除映射。

更新和修改现有映射

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

如“[缺省 NIS 映射](#)” [52]中所述，缺省 NIS 映射的缺省位置是主服务器上的 /var/yp/domainname，其中 domainname 是 NIS 域的名称。当您更新某个映射时，可以根据该映射是否为缺省映射来使用两个更新过程之一。

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

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

▼ 如何更新随缺省集合提供的映射

使用以下过程可以更新随缺省集合提供的映射。

1. 成为 NIS 主服务器的管理员。
有关更多信息，请参见《[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. 编辑您要更改的映射的源文件。
该文件可能位于 /etc 或您选择的某个其他目录中。
3. 运行 make 命令。

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

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

维护更新后的映射

以下各节介绍完成更新随缺省集合提供的映射之后进行的其他过程。

传播 NIS 映射

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

svc:/network/rpc/bind 服务的 config/local_only 属性必须设置为 false。否则，NIS 主服务器无法通过使用 yppush 命令将更新后的 NIS 主服务器版本映射到 NIS 从属服务器。

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

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

使用 cron 命令进行映射传送

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

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

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

将 Shell 脚本用于 cron 和 ypxfr

作为为每个映射创建单独的 crontab 项的备选方法，您可能更喜欢让根 crontab 命令运行 shell 脚本来定期更新所有映射。用于更新映射的 shell 脚本样例位于

`/usr/lib/netsvc/yp` 目录中。这些脚本名为 `ypxfr_1perday`、`ypxfr_1perhour` 和 `ypxfr_2perday`。您可以修改或替换这些 shell 脚本来满足站点需要。以下示例显示的是缺省 `ypxfr_1perday` shell 脚本。

例 3 ypxfr_1perday Shell 脚本

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

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

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

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

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

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

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

直接调用 ypxfr 命令

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

记录 ypxfrr 活动

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

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

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

修改非缺省映射

要更新非缺省映射，必须执行下列操作：

1. 创建或编辑对应的文本文件。
2. 生成（或重新生成）新映射或更新的映射。生成映射的方法有两种。
 - 使用 `Makefile`。使用 `Makefile` 是生成非缺省映射的首选方法。如果映射在 `Makefile` 中具有一个项，请运行 `make name`，其中 `name` 是要生成的映射的名称。如果映射中没有 `Makefile` 项，请尝试按照“[修改和使用 /var/yp/Makefile](#)” [84] 中的说明创建一个项。
 - 使用 `/usr/sbin/makedbm` 程序。[makedbm\(1M\)](#) 手册页全面介绍了此命令。

使用 `makedbm` 命令修改非缺省映射

如果您没有输入文件，可通过两种不同的方法使用 `makedbm` 来修改映射：

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

从文本文件创建新映射

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

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

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

向基于文件的映射中添加项

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

通过标准输入创建映射

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

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

修改通过标准输入创建的映射

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

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

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

要更新映射，请键入以下命令将修改过的临时文件的名称提供给 *makedbm*：

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

然后，成为 *root* 用户并键入下列命令，将映射传播到从属服务器。

```
# yppush mymap
```

前面的段落解释了如何使用 *makedbm* 创建映射。但是，您实际上必须执行的所有操作均可通过使用 *ypinit* 命令和 */var/yp/Makefile* 来完成，除非在系统已启动并运行后向数据库添加非缺省映射或更改 NIS 服务器集。

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

使用 NIS 服务器

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

绑定到特定 NIS 服务器

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

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

```
# domainname
example.com
```

3. 提示输入 NIS 服务器主机名。

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

4. 执行以下步骤以重新启动 NIS 服务：

- 对于在系统重新引导后持续有效的服务，请运行 `svcadm` 命令。

```
# svcadm enable svc:/network/nis/client
```

- 对于仅在重新引导之前持续有效的服务，请运行 `ypstop` 和 `ypstart` 命令。

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

▼ 如何设置计算机的 NIS 域名

要更改计算机的 NIS 域名，请执行以下过程。

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“使用所指定的管理权限”。

2. 定义 NIS 域名。

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

3. 更新并运行域名服务。

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

4. 将计算机设置为 NIS 客户机、从属服务器或主服务器。
有关详细信息，请参见第 6 章 [设置和配置网络信息服务](#)。

▼ 如何配置通过 NIS 和 DNS 执行计算机主机名和地址查找

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

1. 成为管理员。

有关获取合适的权限来执行特定任务的更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“使用所指定的管理权限”。

2. 添加 `YP_INTERDOMAIN` 关键字。

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

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

更改为

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

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

3. 运行 `make` 命令，以重新生成映射。

```
# make hosts
```

4. 检查是否正确设置了 DNS 名称服务器。

以下命令列出了 DNS 名称服务器的所有 IP 地址：

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

5. 要启用 DNS 转发，请重新启动每台服务器。

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

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

禁用 NIS 服务

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

- 要禁用客户机上的 NIS，请键入以下命令：

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

- 要禁用特定从属服务器或主服务器上的 NIS，请在服务器上键入以下命令：

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

网络信息系统故障排除

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

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

注 - NIS 服务由服务管理工具管理。使用 `svcadm` 命令可以对此服务执行启用、禁用或重新启动等管理操作。有关将 SMF 与 NIS 结合使用的更多信息，请参见“[NIS 和服务管理工具](#)” [58]。有关 SMF 的概述，请参阅《[在 Oracle Solaris 11.2 中管理系统服务](#)》中的第 1 章，“[服务管理工具简介](#)”。有关更多详细信息，另请参阅 [svcadm\(1M\)](#) 和 [svcs\(1\)](#) 手册页。

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

NIS 绑定问题

NIS 绑定问题的症状

NIS 绑定问题具有以下常见症状。

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

影响一台客户机的 NIS 问题

如果只有一两台客户机出现了表明 NIS 绑定问题的症状，则可能是这些客户机存在问题。如果许多 NIS 客户机都无法正确绑定，则可能是一台或多台 NIS 服务器存在问题。请参见[“影响多台客户机的 NIS 问题” \[99\]](#)。

ypbind 未在客户机上运行

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

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

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

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

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

缺少域名或域名不正确

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

在该客户机上，运行 `domainname` 命令，查看它设置了哪个域名。

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

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

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

```
drwx----- 2 root example.com
```

如果在计算机上运行 `domainname` 所返回的域名与 `/var/yp` 中作为目录列出的服务器域名不同，则计算机的 `/etc/defaultdomain` 文件中指定的域名不正确。请按[如何设置计算机的 NIS 域名 \[92\]](#)中所示重新设置 NIS 域名。

注 - NIS 域名区分大小写。

客户机未绑定到服务器

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

没有可用的服务器

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

- 客户机是否具有 `/var/yp/binding/domainname/ypservers` 文件（该文件包含要绑定到的服务器的列表）？如果没有该文件，请运行 `ypinit -c` 并按优先级顺序指定客户机应绑定到的服务器。
- 如果客户机具有 `/var/yp/binding/domainname/ypservers` 文件，该文件中列出的服务器数量是否足以应对一台或两台服务器不可用时的情况？如果没有足够多的服务器，请运行 `ypinit -c` 向列表中添加更多服务器。
- 选定的 NIS 服务器在 `/etc/inet/hosts` 文件中是否有相应项？要查看选定的 NIS 服务器，请使用 `svcprop -p config/ypservers nis/domain` 命令。如果这些主机不在本地 `/etc/inet/hosts` 文件中，请将服务器添加到 `hosts` NIS 映射并通过运行 `ypinit -c` 或 `ypinit -s` 命令重新生成您的映射，如[“使用 NIS 映射” \[81\]](#)中所述。
- 是否已将名称服务转换设置为除了检查 NIS 外还检查计算机的本地 `hosts` 文件？有关该转换的更多信息，请参见[第 2 章 关于名称服务转换](#)。
- 是否已将名称服务转换设置为首先在 `files` 中检查 `services` 和 `rpc`？有关该转换的更多信息，请参见[第 2 章 关于名称服务转换](#)。

ypwhich 显示不一致

在同一客户机上多次使用 `ypwhich` 时，所显示的结果会随 NIS 服务器的更改而有所不同。这是正常的。当网络或 NIS 服务器繁忙时，NIS 客户机到 NIS 服务器的绑定会不时发生变化。只要可以进行绑定，网络便会在某一时间稳定，所有客户机在此期间从 NIS

服务器获取可接受的响应时间。只要您的客户机能够获得 NIS 服务，服务来源无关紧要。例如，一台 NIS 服务器计算机可以从网络中的其他 NIS 服务器获取其 NIS 服务。

当无法进行服务器绑定时

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

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

有关其他方法，请参见“[绑定到特定 NIS 服务器](#)” [92]。



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

要重新启动 `ypbind` 守护进程，请按以下方式使用 SMF：

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

ypbind 崩溃

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

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

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

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

```
% rpcinfo client
```

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

```
program version netid address service owner
...
100007 3 udp6 :::191.161 ypbind 1
100007 3 tcp6 :::135.200 ypbind 1
```

```

100007 3  udp      0.0.0.0.240.221  ypbind  1
100007 2  udp      0.0.0.0.240.221  ypbind  1
100007 1  udp      0.0.0.0.240.221  ypbind  1
100007 3  tcp      0.0.0.0.250.107  ypbind  1
100007 2  tcp      0.0.0.0.250.107  ypbind  1
100007 1  tcp      0.0.0.0.250.107  ypbind  1
100007 3  ticlts   2\000\000\000    ypbind  1
100007 2  ticlts   2\000\000\000    ypbind  1
100007 3  ticotsord 9\000\000\000    ypbind  1
100007 2  ticotsord 9\000\000\000    ypbind  1
100007 3  ticots   @\000\000\000    ypbind  1
...

```

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

影响多台客户机的 NIS 问题

如果只有一两台客户机出现了表明 NIS 绑定问题的症状，则可能是这些客户机存在问题。请参见“[影响一台客户机的 NIS 问题](#)” [96]。如果许多 NIS 客户机都无法正确绑定，则可能是一台或多台 NIS 服务器存在问题。

rpc.yppasswdd 将以 r 开头的非受限 Shell 视为受限制

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

无法访问网络或服务器

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

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

服务器运转异常

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

NIS 守护进程未运行

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

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

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

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

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

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

服务器具有不同版本的 NIS 映射

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

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

如果服务器和路由器运行正常，请检查以下各项：

- 检查 `ypxfr` 日志输出：请参见[“记录 ypxfr 输出” \[100\]](#)。
- 检查 `svc:/network/nis/xfr:default` 日志文件以查找错误。
- 检查控制文件。请参见[“检查 crontab 文件和 ypxfr Shell 脚本” \[101\]](#)。
- 检查主服务器上的 `ypservers` 映射。请参见[“检查 ypservers 映射” \[101\]](#)。

记录 ypxfr 输出

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

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

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

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

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

检查 `crontab` 文件和 `ypxfr` Shell 脚本

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

检查 `ypservers` 映射

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

在有故障的从属服务器上更新映射的解决方法

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

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

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

`ypserv` 崩溃

如果 `ypserv` 进程几乎总是在启动后的瞬间崩溃，并且即使重复启动也无法持续运行，则基本上可按照“`ypbind` 崩溃” [98]中所述的过程进行调试。首先，运行以下命令来查看是否会报告任何错误：

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

如下所示，检查是否存在 rpcbind 守护进程：

```
# ptree |grep rpcbind
```

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

```
% rpcinfo -p ypserver

% program vers proto port service
100000 4 tcp 111 portmapper
100000 3 tcp 111 portmapper
100068 2 udp 32813 cmsd
...
100007 1 tcp 34900 ypbind
100004 2 udp 731 ypserv
100004 1 udp 731 ypserv
100004 1 tcp 732 ypserv
100004 2 tcp 32772 ypserv
```

您的计算机可能具有不同的端口号。表示 ypserv 进程的四个项如下所示：

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

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

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

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

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)	<p>每个 LDAP 项均由多个有名称的属性组成，每个属性都具有一个或多个值。</p> <p>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。</p>
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 (<i>Domain Name System, DNS</i>) 名称服务器/名称解析程序模式。另请参见 <i>client</i> (客户机)。
client (客户机)	<p>(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)。</p> <p>(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。</p> <p>(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。</p>
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 项（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 <i>data encryption standard, DES</i> (数据加密标准)。
directory cache (目录高速缓存)	一个本地文件，用于存储与目录对象相关联的数据。
directory information tree (目录信息树)	DIT 是指给定网络的分布式目录结构。缺省情况下，客户机在访问信息时会假设 DIT 具有给定的结构。LDAP 服务器支持的每个域都有一个具有假设结构的假设子树。
directory (目录)	(1) LDAP 目录是 LDAP 对象的容器。在 UNIX 中，目录是文件和子目录的容器。
distinguished name (标识名)	标识名是 X.500 目录信息库 (directory information base, DIB) 中的项，由沿根目录直至指定项的路径，从树中每一项选择的属性组成。
DIT	请参见 <i>directory information tree</i> (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 <i>Domain Name System</i> (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 地址存储在它们之中。
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 (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 <i>domain</i> (域)。
Domain naming service, DNS (域名服务)	一种服务，它提供的命名策略和机制用于将域名和计算机名映射为企业外部地址 (如 Internet 上的地址)。DNS 是由 Internet 使用的网络信息服务。
domain (域)	(1) 在 Internet 中，命名分层结构的一部分通常对应于一个局域网 (Local Area Network, LAN) 或广域网 (Wide Area Network, WAN) 或这

	<p>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。</p> <p>(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。</p>
encryption key (加密密钥)	请参见 <i>data encrypting key</i> (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 <i>group ID</i> (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 <i>TCP/IP</i> 的主机的 32 位地址。请参见 <i>decimal dotted notation</i> (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 <i>data encrypting key</i> (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其中获取其网络信息的源。
namespace (名称空间)	(1) 名称空间存储着用户、工作站和应用程序在网络中进行通信时必须使用的信息。 (2) 命名系统中所有名称的集合。
naming service (命名服务)	一项网络服务，用于处理计算机、用户、打印机、域、路由器名称以及其他网络名称和地址。
NDBM	NDBM (新数据库管理) 是 DBM 的改进版本。
network mask (网络掩码)	一个数字，软件用它将本地子网地址与给定 Internet 协议地址的其余部分分开。
network password (网络口令)	请参见 Secure RPC password (安全 RPC 口令)。
NIS	一种分布式网络信息服务，其中包含有关网络上的系统和用户的关键信息。NIS 数据库存储在主服务器和全部副本服务器或从属服务器上。
NIS maps (NIS 映射)	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 <code>client_info</code> 表或一个 <code>client_info</code> 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 <i>entry</i> (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 <i>Transport Control Protocol, TCP</i> (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 <i>Internet</i> 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

A

- 安全 RPC 口令
 - 定义, 107
- 安全套接字层 见 SSL
- 安全性
 - NIS, 60, 61
 - NIS 映射中的 root, 77
 - NIS, 和, 77
- 安装
 - DNS 客户机, 34
 - DNS 软件包, 31
- AAAA 记录, 18
- Active Directory
 - AD 命名服务, 41
 - 更新口令, 43
 - 检索
 - group 信息, 45
 - passwd 信息, 44
 - shadow 信息, 44
 - 设置客户机, 41
 - 配置 nss_ad, 42
- adjunct 文件, 63
- aliases 文件, 62
- audit_attr 映射
 - 描述, 52
- audit_user 映射
 - 描述, 52
- auto_direct.time 映射, 85
- auto_home 表
 - 名称服务转换和, 23
- auto_home.time 映射, 85
- auto_master 表
 - 名称服务转换和, 23

B

- 编译标志
 - DNS, 40
- 标识名
 - 定义, 104
- baseDN
 - 定义, 103
- bootparams 映射
 - 描述, 52

C

- 传输层安全
 - 定义, 108
- 传输控制协议
 - 定义, 108
- 创建
 - rndc.conf 文件, 32
- 从属服务器
 - 定义, 108
- CHKPIPE, 86
- crontab 文件
 - NIS 问题和, 101
 - ypxfr 和, 88

D

- 点分十进制表示法
 - 定义, 104
- 多播 DNS 见 mDNS
- databaseID
 - 定义, 104
- dbm 文件, 91, 92
- DES
 - 定义, 104, 104
- dig 命令

- 说明, 39
 - DIR 目录, 62
 - DIT 见 目录信息树
 - DN
 - 定义, 104
 - DNS
 - FMRI, 30
 - NIS 和, 47, 48, 93
 - SMF 和, 30
 - 任务, 31
 - 名称服务转换和, 19
 - 命令, 39
 - 守护进程, 39
 - 定义, 104, 104
 - 文件, 39
 - 概述, 15, 29
 - 用户授权, 34
 - 相关信息, 30
 - 编译标志, 40
 - 通告资源, 38
 - DNS 服务器
 - 故障排除, 35
 - 配置, 32
 - 配置选项, 33
 - DNS 服务搜索
 - 概述, 16, 29
 - 配置, 37
 - DNS 客户机
 - 安装, 34
 - DNS 区域
 - 定义, 104
 - DNS 区域文件
 - 定义, 104
 - DNS 软件包
 - 安装, 31
 - DNS 转发
 - 定义, 104
 - dns-sd 命令
 - 说明, 39
 - 通告资源, 38
 - dnssec-dsfromkey 命令
 - 说明, 39
 - dnssec-keyfromlabel 命令
 - 说明, 39
 - dnssec-keygen 命令
 - 说明, 39
 - dnssec-signzone 命令
 - 说明, 39
 - DOM 变量, 65, 66
 - domainname 命令
 - NIS 和, 97
- ## E
- /etc 文件, 51
 - 命名和, 15
 - /etc/inet/hosts 文件, 12
 - NIS 从属服务器和, 69
 - /etc/mail 目录, 63
 - /etc/mail/aliases 文件, 62
 - /etc/named.conf 文件
 - DNS 用户授权, 34
 - 说明, 39
 - 验证配置, 36
 - /etc/rndc.conf 文件
 - 说明, 39
 - ethers.byaddr 映射
 - 描述, 52
 - ethers.byname 映射
 - 描述, 52
 - exec_attr 映射
 - 描述, 52
- ## F
- 反向解析
 - 定义, 107
 - 服务管理工具 见 SMF
 - 服务管理工具 (Service Management Facility, SMF)
 - 和 Oracle Solaris 命名服务, 15
 - 服务器
 - NIS 从属设置, 68, 69
 - ypservers 文件, 71
 - 不可用 (NIS), 97
 - 准备 NIS 服务器, 60
 - 定义, 107
 - 服务器列表
 - NIS 绑定, 54
 - 定义, 107

服务搜索 见 DNS 服务搜索

FMRI

- DNS, 30
- mDNS, 37
- NIS, 58

G

公钥

- 定义, 107

故障排除

- DNS 服务器, 35

广播

- NIS 绑定, 55

getaddrinfo ()

- 名称服务转换和, 19

gethostbyname ()

- 名称服务转换和, 19

getpwnam ()

- 名称服务转换和, 19

getpwuid ()

- 名称服务转换和, 19

getXbyY () 接口

- 名称服务转换和, 19

group.bygid 映射

- 描述, 52

group.byname 映射

- 描述, 52

H

后缀

- 定义, 108

host 命令

- 说明, 39

host.byaddr 映射

- 描述, 52

host.byname 映射

- 描述, 52

hosts 数据库, 86

hosts 文件

- NIS 从属服务器和, 69

hosts.byaddr 映射, 51

hosts.byname 映射, 51

I

Internet

- NIS 和, 48

Internet 地址

- 定义, 105

Internet 访问

- 名称服务转换和, 19

IP

- 定义, 105

IP 地址

- 定义, 105

J

基于文件的命名, 16

记录

- 定义, 107

加密

- 定义, 105

加密密钥

- 定义, 105, 105

架构

- 定义, 107

检验

- /etc/named.conf 文件, 36

节点名称

- 设置, 60

K

客户机

- NIS, 49
- NIS 设置, 73
- 定义, 103

客户机/服务器模型

- 定义, 103

口令

- NIS, 79
- rpc.yppasswdd 守护进程, 79

口令数据

- NIS, 60, 61
- NIS 映射中的 root, 77
- NIS, 和, 77
- 名称服务转换, 26

key serv

- 名称服务转换和, 23

L

LAN

- 定义, 106

LDAP

- 定义, 105

M

密钥服务器

- 定义, 105

名称服务器

- 定义, 106

名称服务转换

- auto_home 表, 23

- auto_master 表, 23

- DNS 与, 19

- Internet 访问, 19

- keyserv 服务, 23

- mDNS 和, 37

- NIS, 48

- NOTFOUND=continue 搜索条件, 22

- publickey 属性, 23

- SMF 属性, 19

- SUCCESS=return 搜索条件, 22

- timezone 表和, 23

- TRYAGAIN=3 搜索条件, 22

- TRYAGAIN=forever 搜索条件, 22

- UNAVAIL=continue 搜索条件, 22

- 从 nsswitch.conf 文件进行迁移, 26

- 修改, 23

- 口令信息, 26

- 口令数据和, 26

- 定义, 106

- 搜索条件, 22

- 操作, 22

- 数据库, 19

- 消息, 21

- 源格式, 21

- 状态消息, 21, 22

- 简介, 19

- 选项, 22

配置

- 搜索条件, 24

- 数据库的源, 24

- 缺省源, 25

名称解析

- 定义, 106

名称空间

- 定义, 106

命令

- DNS, 39

- NIS, 50

命名

- DNS, 17

- IPv6 扩展, 18

- LDAP, 17

- NIS, 16

- Oracle Solaris 命名服务, 15

- 基于文件, 16

- 概述, 11

- 比较, 17

命名服务

- 定义, 106

目录

- 定义, 104

目录高速缓存

- 定义, 104

目录信息树

- 定义, 104

mail.aliases 映射

- 描述, 52

mail.byaddr 映射

- 描述, 52

make 命令

- Makefile 语法, 84

- NIS 映射, 54

- ypinit 和, 65

- 更新映射后, 87

- 说明, 51

makedbm 命令

- make 命令和, 52

- Makefile 和, 64

- ypinit 和, 65

- 更改映射服务器, 83

- 添加从属服务器, 71

- 说明, 51

- 非缺省映射和, 90

Makefile 文件

- NIS, 52

- NIS 安全, 77

- passwd 映射和, 64
 - 准备, 63
 - 到 NIS 的转换和, 63
 - 映射
 - 支持的列表, 83
 - 更改映射的主服务器, 82
 - 更改源目录, 60, 63
 - 自动挂载程序映射和, 85
 - 设置主服务器, 65
 - 非缺省映射
 - 修改, 90
 - Makefile 中的 NOPUSH, 86
 - mapname.dir 文件, 64
 - mapname.pag 文件, 64
 - mDNS
 - 概述, 16, 29
 - 配置, 37
 - 错误日志, 38
 - MIS
 - 定义, 106
- N**
- “不响应”消息 (NIS), 95
 - named 守护进程
 - SMF 和, 30
 - 对其进行故障排除, 35
 - 显示编译标志, 40
 - 用户授权和, 34
 - 说明, 39
 - 配置文件
 - 说明, 39
 - named-checkconf 命令
 - 说明, 39
 - 配置 DNS 服务器, 32
 - 验证 /etc/named.conf 文件, 36
 - named-checkzone 命令
 - 说明, 39
 - named-compilezone 命令
 - 说明, 39
 - named.conf 文件 见 /etc/named.conf 文件
 - ndbm 格式, 63
 - NIS 映射和, 51
 - netgroup 映射
 - 概述, 80
 - 项, 80
 - netgroup.byhost 映射
 - 描述, 52
 - 概述, 80
 - netgroup.byuser 映射
 - 描述, 52
 - 概述, 80
 - netid.byname 映射
 - 描述, 53
 - netmasks.byaddr 映射
 - 描述, 53
 - networks.byaddr 映射
 - 描述, 53
 - networks.byname 映射
 - 描述, 53
 - nicknames 文件, 54
 - NIS, 16
 - /var/yp/domainname 目录和, 52
 - DNS 和, 48, 93
 - Internet 和, 48
 - Makefile, 52
 - Makefile 准备工作, 63
 - Makefile 过滤, 84
 - ndbm 格式, 51
 - passwd 映射自动更新, 88
 - root 项, 77
 - rpc.yppasswdd 守护进程, 79
 - SMF 和, 58
 - useradd, 78
 - userdel, 79
 - ypbind 失败, 98
 - ypbind 守护进程, 55
 - ypbind“无法”消息, 95
 - ypinit, 65
 - ypservers 文件, 71
 - ypwhich, 55
 - ypwhich 显示不一致, 97
 - “不可用”消息, 95
 - “不响应”消息, 95
 - 主服务器, 49
 - 从属服务器, 49
 - 从属服务器设置, 68, 69
 - 体系结构, 47
 - 修改配置文件, 83
 - 停止, 94, 94

- 准备工作, 58
- 口令数据, 60, 61
- 启动守护进程, 66
- 命令, 50
- 命令挂起, 95
- 域, 48, 49
- 域名, 59
- 多个域, 66
- 守护进程, 50
- 安全性, 77
- 定义, 106
- 客户机, 48, 49
- 客户机设置, 73
- 客户机问题, 96
- 广播绑定, 55
- 手动绑定, 92
- 无法进行服务器绑定, 98
- 更新 passwd 映射, 79
- 服务器, 48, 49
- 服务器, 映射不同版本, 100
- 服务器不可用, 97
- 服务器列表绑定, 55
- 源文件, 60, 61
- 用户, 管理, 78
- 用户口令, 79
- 用户口令已锁定, 78
- 简介, 47
- 组件, 49
- 绑定, 54
- 结构, 47
- 网络组, 80, 80
- 自动启动, 67
- 设置准备工作, 60
- 过载的服务器, 99
- 问题, 95
- NIS 从属服务器
 - 初始化, 72
 - 添加, 71
- NIS 服务器
 - 运转异常, 99
- NIS 客户机
 - 未绑定到服务器, 97
- NIS 守护进程
 - 未在运行, 100
- NIS 映射
 - `/var/yp/domainname` 目录和, 52
 - Makefile DIR 变量, 85
 - Makefile DOM 变量, 85
 - Makefile PWDIR 变量, 85
 - Makefile 中的 CHKPIPE, 86
 - Makefile 中的 NOPUSH, 86
 - Makefile 中的 yppush, 86
 - Makefile 以及, 84
 - Makefile 过滤, 84
 - ndbm 格式, 51
 - 从文件创建, 90
 - 从键盘创建, 91
 - 使用, 53
 - 修改配置文件, 83
 - 列表, 52
 - 创建, 54
 - 定义, 106
 - 昵称, 54
 - 显示内容, 54, 81
 - 更改 Makefile 变量, 85
 - 更改 Makefile 宏, 85
 - 更改服务器, 82
 - 更新, 53
 - 查找, 54
 - 管理, 81
 - 缺省, 52
 - 非缺省, 87
- NIS 域
 - 更改, 92
- NIS 域名
 - 不正确, 96
 - 缺少, 96
- NIS 主机
 - 更改域, 92
- NOTFOUND=continue 搜索条件
 - 名称服务转换和, 22
- nscd 守护进程
 - 说明, 50
- nscfg 命令
 - 说明, 40
- nslookup 命令
 - 说明, 40
- nsswitch.conf
 - 迁移至 SMF, 26
- nsupdate 命令
 - 说明, 40

O

Oracle Solaris 命名服务, 15
 和服务管理工具 (Service Management Facility, SMF), 15

P

配置

DNS 服务器, 32
 DNS 服务器选项, 33

凭证

定义, 103

/PWDIR/shadow 文件, 64

/PWDR/security/passwd.adjunct, 64

\$PWDIR/security/passwd.adjunct, 83

passwd

NIS 映射已自动更新, 88

passwd 命令, 79

passwd 文件

Solaris 1.x 格式, 78

passwd 映射, 61

用户, 添加, 78

passwd.adjunct 文件, 64, 83

passwd.adjunct.byname 映射

描述, 53

passwd.byname 映射

描述, 53

passwd.byuid 映射

描述, 53

prof_attr 映射

描述, 53

protocols.byname 映射

描述, 53

protocols.bynumber 映射

描述, 53

publickey.byname 映射

描述, 53

PWDIR, 61

Q

企业级网络

定义, 105

启动

NIS 守护进程, 66

轻量目录访问协议 见 LDAP

全局命名服务

定义, 105

R

任务

DNS, 31

rndc 命令

说明, 40

配置文件

说明, 39

rndc-confgen 命令

创建 rndc.conf 文件, 32

说明, 40

配置 DNS 服务器, 32

rndc.conf 文件

创建, 32

RPC

定义, 107, 107

rpc.bynumber 映射

描述, 53

rpc.yppasswdd 守护进程

NIS 口令和, 79

passwd 命令更新映射, 88

说明, 50

rpc.yupdated 守护进程

说明, 50

S

上下文

定义, 103

设置

NIS Makefile, 63

NIS 从属服务器, 68, 69

NIS 客户机, 73

多个 NIS 域, 66

针对 NIS 的准备工作, 58, 60

守护进程

DNS, 39

NIS, 50

未在运行, 100

属性

- 定义, 103
- 数据加密标准 见 DES
- 数据加密密钥
 - 定义, 103
- 私钥
 - 定义, 107
- 索引名
 - 定义, 105
- SASL
 - 定义, 107
- searchTriple
 - 定义, 107
- services.byname 映射
 - 描述, 53
- services.byservice 映射
 - 描述, 53
- shadow 文件, 64
 - Solaris 1.x 格式, 78
- sites.byname 映射
 - 更改映射服务器, 83
- SMF, 66
 - DNS 和, 30
 - NIS 和, 58
- SSL
 - 定义, 108
- SUCCESS=return 搜索条件
 - 名称服务转换和, 22
- svc:/network/dns/client
 - 描述, 30
- svc:/network/dns/server
 - 描述, 30
- svcadm
 - 与 NIS, 72

T

- 停止
 - NIS 守护进程, 66
- TCP 见 传输控制协议
- TCP/IP
 - 定义, 108
- timezone 表, 23
- TLS 见 传输层安全

U

- “不可用”消息 (NIS), 95
- /usr/bin/dns-sd 命令
 - 说明, 39
- /usr/sbin/dig 命令
 - 说明, 39
- /usr/sbin/dnssec-dsfromkey 命令
 - 说明, 39
- /usr/sbin/dnssec-keyfromlabel 命令
 - 说明, 39
- /usr/sbin/dnssec-keygen 命令
 - 说明, 39
- /usr/sbin/dnssec-signzone 命令
 - 说明, 39
- /usr/sbin/host 命令
 - 说明, 39
- /usr/sbin/makedbm 命令
 - 修改非缺省映射, 90
- /usr/sbin/named 守护进程
 - 说明, 39
- /usr/sbin/named-checkconf 命令
 - 说明, 39
- /usr/sbin/named-checkzone 命令
 - 说明, 39
- /usr/sbin/named-compilezone 命令
 - 说明, 39
- /usr/sbin/nscfg 命令
 - 说明, 40
- /usr/sbin/nslookup 命令
 - 说明, 40
- /usr/sbin/nsupdate 命令
 - 说明, 40
- /usr/sbin/rndc 命令
 - 说明, 40
- /usr/sbin/rndc-configgen 命令
 - 说明, 40
- UNAVAIL=continue 搜索条件
 - 名称服务转换和, 22
- user_attr 映射
 - 描述, 53
- useradd, 78
 - 口令已锁定, 78
- userdel, 79, 79
- usermod 命令
 - DNS 用户授权, 34

V

- /var/spool/cron/crontabs/root 文件
 - NIS 问题和, 101
- /var/svc/log/network-dns-multicast:default.log 文件, 38
- /var/svc/log/network-dns-server:default.log 文件
 - 故障排除, 35
- /var/yp 目录
 - NIS 安全, 77
- /var/yp/binding/domainname/ypservers 文件, 97
- /var/yp/domainname 目录, 52
- /var/yp/Makefile, 65
 - 映射
 - 支持的列表, 83
- /var/yp/mymap.asc 文件, 91
- /var/yp/nicknames 文件, 54

W

- 网络服务
 - DNS 和, 29
- 网络口令 见 安全 RPC 口令
- 网络掩码
 - 定义, 106
- 文件
 - DNS, 39
- WAN
 - 定义, 108

X

- 项
 - 定义, 105
- X.500
 - 定义, 108

Y

- 验证
 - 定义, 103
- 映射过程
 - 定义, 106
- 用户

- NIS, 78
- NIS 口令, 79
 - useradd, 78
 - userdel (NIS), 79
 - 更新 passwd 映射, 79
 - 网络组, 80, 80
- 用户授权
 - 针对 DNS, 34
- 邮件交换记录
 - 定义, 106
- 邮件主机
 - 定义, 106
- 域
 - NIS, 48, 49, 59
 - 多个 NIS, 66
 - 定义, 104
- 域名
 - NIS 从属服务器和, 69
 - 定义, 104
 - 设置, 60
- 域名系统 见 DNS
- 域名系统 (Domain Name System, DNS)
 - 针对 IPv6 的扩展, 18
- 源
 - 定义, 108
- yp
 - 定义, 108
- ypbind 守护进程, 66
 - “无法”消息, 95
 - 失败, 98
 - 客户机未绑定, 97
 - 广播模式, 55, 73
 - 服务器列表模式, 55
 - 添加从属服务器, 72
 - 说明, 50
 - 过载的服务器和, 99
- ypcat 命令, 54
 - 说明, 51
- ypinit 命令
 - make 命令和, 65
 - Makefile 文件和, 63
 - 主服务器设置, 64
 - 从属服务器和, 69
 - 初始化从属服务器, 69
 - 启动 ypserv, 67

- 客户机设置, 73
- 添加从属服务器, 72
- 缺省映射, 87
- 说明, 51
- ypmatch 命令
 - 说明, 51
- yppush 命令
 - Makefile 和, 86
 - NIS 问题, 101
 - 更改映射服务器, 83
 - 说明, 51
- ypserv 守护进程, 55, 66
 - 广播模式, 56
 - 故障, 101
 - 说明, 50
 - 过载的服务器和, 99
- ypservers 文件
 - NIS 故障排除, 97
 - 创建, 71
 - 添加从属服务器, 71
- ypservers 映射
 - NIS 问题, 101
 - 描述, 53
- ypset 命令
 - 说明, 51
- ypwhich 命令
 - 显示不一致, 97
 - 识别主服务器, 54
 - 识别绑定服务器, 55
 - 说明, 51
- ypxfr 命令
 - crontab 文件, 88
 - shell 脚本, 101
 - 将新映射分布到从属服务器中, 91
 - 更改映射服务器, 83
 - 记录输出, 100
 - 说明, 51
- ypxfrd 守护进程
 - 说明, 50
- NIS 客户机, 48
- NIS 服务器, 48
- 更改 NIS 域, 92
- 主机名
 - 设置, 60
- 字段
 - 定义, 105
- 子网
 - 定义, 108
- 组
 - 网络组 (NIS), 80, 80
- 组 ID
 - 定义, 105

Z

- 主服务器
 - 定义, 106
- 主机 (计算机)