The Linux NIS(YP)/NYS/NIS+ HOWTO

Thorsten Kukuk, *kukuk@suse.de* <mailto:kukuk@suse.de>
Перевод на русский язык Виктор Вислобоков. 08.09.2000 v1.0, 9 March 1999

Этот документ описывает как настроить Linux в качестве NIS(YP) или NIS+ клиента и как установить NIS сервер.

Содержание

1 Введение

Все больше и больше Linux машин устанавливается для работы в сети. Для упрощения сетевого администрирования, во многих сетях (как правило в сетях на базе Sun) запущена Служба Сетевой Информации (Network Information Service). Linux машины могут либо полностью использовать существующую службу NIS, либо сами предоставлять ее. Linux машины также могут быть и клиентами NIS+, поддержка этой особенности находится в состоянии бета- тестирования.
Данный документ пытается ответить на вопросы об установке NIS(YP) и NIS+ на вашей Linux машине. Не забудьте прочитать секцию [5]The RPC Portmapper.
NIS-Howto редактируется и поддерживается

Thorsten Kukuk, *kukuk@suse.de* <mailto:kukuk@suse.de>

Основным источником информации для этого документа является начальный документ NIS-Howto, который создали:

- Andrea Dell'Amico *adellam@ZIA.ms.it* <mailto:adellam@ZIA.ms.it>
- Mitchum DSouza *Mitch.DSouza@NetComm.IE* <mailto:Mitch.DSouza@NetComm.IE>
- Erwin Embsen *erwin@nioz.nl* <mailto:erwin@nioz.nl>
- Peter Eriksson *peter@ifm.liu.se* <mailto:peter@ifm.liu.se>

и которым мы должны сказать спасибо.

1.1 Новые версии этого документа

Вы всегда можете найти последнюю версию этого документа в Интернет по адресу *http://www.suse.de/kukuk/linux/HOWTO/NIS-HOWTO.html* <http://www.suse.de/~kukuk/linux/HOWTO/NIS-HOWTO.html>.
Новые версии этого документа таже будут загружены на разные Linux WWW и FTP сайты, включая домашнюю страницу проекта LDP (Проект Документации Linux).
Ссылки на переводы этого документа могут быть найдены по адресу *http://www.suse.de/kukuk/linux/nis-howto.html* <http://www.suse.de/~kukuk/linux/nis-howto.html>.

1.2 Отречение

Так как этот документ был составлен на основе моих знаний, то он может и предположительно содержит ошибки. Пожалуйста прочтите все файлы README которые вы найдете в разных частях программного обеспечения, описываемого в данном документе для того, чтобы узнать больше подробностей и более точную информацию. Со своей стороны, я буду стараться, чтобы в этом документе содержалось как можно меньше ошибок.

1.3 Обратная связь и правки

Если у вас возникли вопросы или комментарии к данному документу, пожалуйста свободно обращайтесь ко мне Thorsten Kukuk по адресу *kukuk@suse.de.* <mailto:kukuk@suse.de.> Я приветствую любые советы или критику. Если вы найдете ошибки в этом документе, пожалуйста дайте мне знать о них, чтобы я мог их исправить в следующей версии. Заранее спасибо.
Пожалуйста не присылайте мне вопросы о специфических проблемах, связанных с вашим дистрибутивом Linux! Я не знаю каждый дистрибутив Linux. Но я попытаюсь добавить в документ каждое решение, которые вы мне пришлете.

1.4 Благодарности

Мы должны сказать большое спасибо всем людям, которые участвовали (напрямую или косвенно) в создании этого документа. В алфавитном порядке:

- Byron A Jeff *byron@cc.gatech.edu* <mailto:byron@cc.gatech.edu>
- Markus Rex *msrex@suse.de* <mailto:msrex@suse.de>
- Miquel van Smoorenburg *miquels@cistron.nl* <mailto:miquels@cistron.nl>

Theo de Raadt является создателем оригинального кода yp-клиента. Swen Thuemmler перенес код yp-клиента на Linux, а также перенес yp-подпрограммы в libc (снова базируясь на работе Theo). Thorsten Kukuk написал NIS(YP) и NIS+ подпрограммы для GNU libc 2.x "с нуля".

2 Глоссарий и основная информация

2.1 Глоссарий терминов

В данном документе используется большое число сокращений. Вот наиболее важные сокращения с коротким пояснением:

DBM

Управление базой данных (DataBase Management) - библиотека функций, которые управляют в базе данных парами ключ-значение.

DLL

Динамически связанная библиотека (Dynamically Linked Library) - библиотека, которая используется во время выполнения программы.

domainname

"Ключ"имени, который используется клиентами NIS для определения нужного сервера NIS, который обслуживает этот ключ имени домена. Пожалуйста, заметьте, что нет необходимости иметь что-нибудь типа DNS "домена"(имени машины) или машин(ы).

FTP

Протокол Приема/передачи файлов (File Transfer Protocol) - это протокол, используемый для обмена файлами между двумя компьютерами.

libnsl

Библиотека службы имен (Name services library) - библиотека, содержащая вызовы подпрограмм службы имен (getpwnam, getservbyname, и т.д.) в SVR4 Unix. Данные вызовы использует GNU libc для функций NIS (YP) и NIS+.

libsocket

Библиотека службы гнезд (Socket services library) - это библиотека, содержащая вызовы для работы с гнездами (socket, bind, listen, и т.д.) в SVR4 Unix.

NIS

Служба Сетевой Информации (Network Information Service) - служба, которая предоставляет информацию, которая может быть получена по сети для всех машин в сети. На Linux машинах со стандартной библиотекой libc имеется поддержка NIS, которая далее будет называться "традиционная NIS".

NIS+

Служба Сетевой Информации (Плюс :-), на основе NIS со стероидами. NIS+ разрабатывается фирмой Sun Microsystems Inc. как замена для NIS с улучшенной безопасностью и управлением _большими_ установками.

NYS

Это имя проекта для NIS+, YP и Switch, который возглавляет Peter Eriksson *peter@ifm.liu.se* <mailto:peter@ifm.liu.se>. Проект содержит вещи для полной замены/реализации кода NIS (= YP), который использует функциональность Name Services Switch библиотеки NYS.

NSS

Переключатель службы имен (Name Service Switch). Это файл /etc/nsswitch.conf, который определяет порядок поиска, выполняемого когда требуются определенные куски информации.

RPC

Вызов Удаленной Процедуры (Remote Procedure Call) - подпрограммы RPC позволяющие программам на языке C выполнять вызовы процедур на других машинах сети. Когда кто-нибудь говорит об RPC, они часто имею в виду вариант Sun RPC.

YP

Желтые страницы (Yellow Pages(tm)) - зарегистрированная торговая марка в фирмы British Telecom plc в Великобритании.

TCP-IP

Протокол управления передачей данных/Интернет протокол (Transmission Control Protocol/Internet Protocol) - этот протокол очень часто используется на машинах с Unix.

2.2 Некоторая основная информация

Ниже приведены строки из Руководства Администратора Сети фирмы Sun(tm):

> "NIS сначала была известна как Sun Yellow Pages (YP), но имя Yellow Pages(tm) является зарегистрированной торговой маркой фирмы British Telecom plc в Великобритании и не может быть использовано без соответствующих прав."

NIS - это Службы Сетевой Информации. Цель NIS в том, чтобы предоставить нужную информацию по сети для всех машин в сети. Информация, которую предоставляет NIS это:

- имена для входа в систему/пароли/домашние каталоги (/etc/passwd)
- информация о группах (/etc/group)

Например, если ваш пароль записывается в базу данных паролей NIS, то вы получаете доступ ко всем машинам в сети, у которых запущена клиентская часть NIS.
Sun - это зарегистрированная торговая марка фирмы Sun Microsystems, Inc. лицензированная для фирмы SunSoft, Inc.

3 NIS, NYS или NIS+ ?

3.1 libc 4/5 с традиционной NIS или NYS ?

Различие между "традиционной NIS"и кодом NIS в библиотеке NYS состоит в различии между ленью и зрелостью против функциональности и любви к приключениям.
Код "традиционной NIS находится в стандартной библиотеке C и был там довольно долго, но иногда изменялся из-за требований времени и плохой функциональности.
Код NIS в библиотеке NYS требуется для перекомпиляции библиотеки libc, чтобы включить в нее код NYS (или может быть вы можете достать уже готовую версию libc куда уже включен NYS).
Другое отличие состоит в том, что код традиционной NIS имеет некоторую поддержку сетевых групп NIS, которую не имеет код NYS. В других случаях код NYS позволяет вам управлять прозрачно теневыми паролями. Код "традиционной NIS"не имеет поддержки теневых паролей через NIS.

3.2 glibc 2 и NIS/NIS+

Забудьте все это, если вы используете новую библиотеку GNU C Library 2.x (или libc6). Она имеет реальную поддержку NSS (службу переключения имен), которая делает ее очень удобной и содержит поддержку для следующих карт NIS/NIS+ : aliases, ethers, group, hosts, netgroups, networks, protocols, publickey, passwd, rpc, services и shadow. Библиотека GNU C не имеет проблем с теневыми паролями через NIS.

3.3 NIS или NIS+ ?

Выбор между NIS и NIS+ прост - используйте NIS, если вы не должны использовать NIS+ или если имеете проблемы с обеспечением безопастности. NIS+ _гораздо более_ проблематична для администрирования (она красиво и легко управляется на стороне клиента, но со стороны сервера отвратительно). Другая проблема состоит в поддержке NIS+ для Linux, которая находится в состоянии разработки - вам будет нужна последняя версия glibc 2.1.

4 Как это работает

4.1 Как работает NIS

В сети сервером NIS должна быть одна машина. Вы можете иметь несколько NIS серверов, каждый из которых будет обслуживать различные "домены"NIS - или вы можете иметь скооперированные серверы NISm где один сервер является мастер-сервером, а все другие являются подчиненными серверами (для определенного "домена"NIS) - или вы можете их смешивать...
Подчиненные серверы имеют только копии баз данных NIS и получают эти копии от мастер-сервера NIS, когда в базы данных на мастер-сервере вносятся изменения. В зависимости от количества машин в вашей сети и ее загруженности, вы можете установить один или более подчиненных серверов. Когда NIS сервер станет недоступен или будет слишком медленно отвечать на запросы, клиент NIS подключенный к этому серверу будет искать другой NIS сервер, который работает или который быстрее.
Базы данных NIS - это базы, в так называемом, DBM формате, который является производным от баз данных в ASCII. Например, файлы /etc/passwd и /etc/group могут быть преобразованы в формат DBM напрямую, через программу трансляции ASCII-to-DBM ("makedbm", поставляемую с сервером). Мастер-сервер NIS должен иметь как ASCII базы данных так и DBM базы данных.
Подчиненные серверы будут извещены об любых изменениях карт NIS, (через программу "yppush"), и автоматически получат необходимые изменения в порядке синхронизации их баз данных. Клиенты NIS не нуждаются в этом, так как они всегда говорят NIS серверу прочитать информацию, записанную у него в DBM базах данных.
Старые версии ypbind используют широковещательные запросы, чтобы найти NIS сервер. Это небезопасно, так как фактически любой может установить NIS сервер и отвечать на такие запросы. Новые версии ypbind (ypbind-3.3 или ypbind-mt) получают нужный сервер из файла с настройками - который не нежен для широковещательных запросов.

4.2 Как работает NIS+

NIS+ - это новая версия службы имен сетевой информации от Sun. Самое большое отличие между NIS и NIS+ это то, что NIS+ имеет поддержку шифрования данных и авторизацию через безопасный RPC.
Модель имен в NIS+ основывается на структуре дерева. Каждый узел в дереве соотвествует одному объекту NIS+ из шести типов: каталог, запись, группа, ссылка, таблица и личное.
Каталог NIS+ который формирует главное пространство имен NIS+, называется корневым каталогом. Имеется два специальных каталога NIS+: org_dir и groups_dir. Каталог org_dir содержит все административные таблицы, такие как passwd (пароли), hosts (узлы) и mail_aliases (почтовые псевдонимы). Каталог groups_dir содержит объекты групп NIS+, которые используются для управления доступом. Коллекция org_dir, groups_dir и их родительского каталога называется доменом NIS+.

5 RPC Portmapper

Чтобы запустить любую программу из описанных выше вам понадобится запустить программу /usr/sbin/portmap. Некоторые дистрибутивы Linux уже имеют сценарий для запуска этого демона в каталогах /sbin/init.d/ или /etc/rc.d/. Все что вам нужно сделать - это активизировать этот сценарий и перегрузить вашу Linux машину. Прочтите документацию по вашему дистрибутиву Linux, чтобы узнать как это сделать.
RPC portmapper (portmap(8)) - это сервер, который преобразует номера программ RPC в номер портов протоколов TCP/IP (или UDP/IP). Он должен быть запущен, чтобы можно было выполнять вызовы RPC (которые использует клиентская часть NIS/NIS+) для серверов RPC (таких как NIS или NIS+) на нужной машине. Когда запускается сервер RPC, он будет говорить portmap, какой номер порта нужно слушать и какие номера RPC программ он подготавливает для обслуживания. Когда

клиент хочет сделать вызов RPC для заданного номера, он будет сперва связываться с portmap на машине-сервере для определения номера порта, куда должны быть отправлены пакеты RPC.
Обычно, стандартные сервера RPC запускаются через inetd(8), так что portmap должен быть запущен перед запуском inetd.
Из соображений безопастности RPC, portmapper'у нужна служба Времени. Убедитесь, что служба Time в /etc/inetd.conf разрешена для всех узлов:

```
#
# Time service is used for clock syncronization.
#
<tag/ ime    stream  tcp     nowait  root    internal /<p>
<tag/ ime    dgram   udp     wait    root    internal /<p>
```

ВАЖНО: Не забудьте перезапустить inetd после внесения изменений в его конфигурационный файл!

6 Что нужно сделать для настройки NIS?

6.1 Определите что вам нужно: сервер, подчиненный сервер или клиент.

Чтобы ответить на этот вопросы вы должны рассмотреть два случая:

1. Ваша машина входит в сеть, где уже есть NIS серверы
2. Вы пока не имеете никаких NIS серверов в сети

В первом случае, вам нужны только клиентские программы (ypbind, ypwhich, ypcat, yppoll, ypmatch). Самой важной программой является ypbind. Эта программа должна быть запущена всегда, она должна всегда быть в списке процессов. Эта программа является демоном и должна запускаться при старте системы (например из файлов /etc/init.d/nis, /sbin/init.d/ypclient, /etc/rc.d/init.d/ypbind, /etc/rc.local). Как только демон ypbind запущен в вашей системе, она становится клиентом NIS.
Во втором случае, если вы не имеете NIS серверов, то вам таже понадобится и NIS сервер (программа обычно называется ypserv). Секция Установка Сервера NIS описывает как установить сервер NIS на вашей Linux машине, используя реализацию "ypserv"авторов Peter Eriksson и Thorsten Kukuk. Заметим что начиная с версии 0.14 данная реализация поддерживает концепцию мастер-подчиненный о которой мы говорили в секции 4.1.
Имеется также другая свободная реализация сервера NIS, называемая "yps", которую написал Tobias Reber из Germany и которая не поддерживает концепцию мастер-подчиненный и имеет другие ограничения и уже давно не поддерживается.

6.2 Программное обеспечение

Системная библиотека "/usr/lib/libc.a"(версии 4.4.2 и выше) или динамическая библиотека "/lib/libc.so.x"содержит все необходимые системные вызовы для успешной компиляции клиента и сервера NIS. Для библиотеки GNU C 2 (glibc 2.x), также нужна библиотека /lib/libnsl.so.1.
Некоторые люди говорят, что NIS работает только с "/usr/lib/libc.a"версии 4.5.21 м выше, так что если вы хотите, чтобы все было хорошо сразу, не используйте старые версии. Клиент NIS может быть получен отсюда:

Site	Directory	File Name
ftp.kernel.org	/pub/linux/utils/net/NIS	yp-tools-2.2.tar.gz
ftp.kernel.org	/pub/linux/utils/net/NIS	ypbind-mt-1.4.tar.gz
ftp.kernel.org	/pub/linux/utils/net/NIS	ypbind-3.3.tar.gz
ftp.kernel.org	/pub/linux/utils/net/NIS	ypbind-3.3-glibc5.diff.gz
ftp.uni-paderborn.de	/linux/local/yp	yp-clients-2.2.tar.gz

Когда вы получили клиента, пожалуйста следуйте инструкциям, которые идут с клиентом. yp-clients 2.2 может использоваться как с libc4 так и с libc5 до версии 5.4.20. Для libc 5.4.21 и glibc 2.x нужны yp-tools версии 1.4.1 или выше. Новые yp-tools 2.2 должны работать с любым Linux libc. Так как в более ранних версиях libc, в коде NIS был найдена ошибка, вам не нужны версии libc 5.4.21-5.4.35. Используйте libc 5.4.36 или выше вместо них или большинство программ YP работать не будут. ypbind 3.3 также будет работать со всеми библиотеками. Если вы используете gcc 2.8.x или выше, egcs или glibc 2.x, вы должны добавить исправления ypbind-3.3-glibc5.diff для ypbind 3.3. Пожалуйста никогда не используйте ypbind от yp-clients 2.2. ypbind-mt - это новый демон, использующий нити (треды). Ему нужно ядро Linux версии 2.2 и glibc 2.1 или выше.

6.3 Демон ypbind

После того как вы успешно скомпилировали программное обеспечение, вы готовы установить его. Наилучшее место для демона ypbind - это каталог /usr/sbin. Некоторые люди могу сказать вам, что вам не нужен ypbind в системе с NYS. Это неверно. Он нужен для ypwhich и ypcat.
Разумеется вы должны устанавливать демон с правами суперпользователя root. Другие программы (ypwhich, ypcat, yppasswd, yppoll, ypmatch) должны быть в каталогах доступных всем пользователям, обычно в /usr/bin.
Новые версии ypbind имеют файл с настройками, называемый /etc/yp.conf. С помощью него вы можете настроить NIS сервер - для подробностей смотрите страницу руководства man ypbind(8). Это файл вам также понадобится для NYS. Пример:

```
ypserver voyager
ypserver defiant
ypserver ds9
```

Если система может получить имена узлов (отрезолвить) без NIS, то вы можете использовать имя, в противном случае вы должны использовать IP адрес. ypbind 3.3 имеет ошибку и будет использовать только последнюю запись (запись ypserver ds9 в примере выше). Все другие записи игнорируются. ypbind-mt управляет записями корректно и использует ту, сервер прописанный в которой отвечает первым.
Хорошо бы протестировать ypbind перед тем как включить его в работу при старте системы. Для тестирования ypbind надо сделать следующее:

- Убедитесь, что вы задали имена YP-доменов. Если вы это не сделали, то выполните команду

  ```
  /bin/domainname nis.domain
  ```

  где nis.domain должен быть некоторой строкой обычно _НЕ_ соответствующей имени DNS-домена вашей машины! Причина этого в том, что при одинаковых именах доменов, хакерам снаружи предоставляется маленькая возможность получить базу данных паролей с ваших серверов NIS. Если вы не знаете какое имя NIS-домена в вашей сети, спросите у вашего администратора системы/сети.

- Запустите "/usr/sbin/portmap", если он уже не запущен.

- Создайте каталог "/var/yp", если он не существует.

- Запустите "/usr/sbin/ypbind"

- Используйте команду "rpcinfo -p localhost"чтобы проверить, что ypbind доступа регистрация своей службы с portmapper. Вы должны получить:

  ```
  program vers proto   port
   100000    2   tcp    111  portmapper
   100000    2   udp    111  portmapper
   100007    2   udp    637  ypbind
   100007    2   tcp    639  ypbind
  ```

или

```
program vers proto   port
 100000    2   tcp    111  portmapper
 100000    2   udp    111  portmapper
 100007    2   udp    758  ypbind
 100007    1   udp    758  ypbind
 100007    2   tcp    761  ypbind
 100007    1   tcp    761  ypbind
```

В зависимости от версии ypbind которую вы используете.

- Вы можете также запустить "rpcinfo -u localhost ypbind". Эта команда должна выдать следующее:

```
program 100007 version 2 ready and waiting
```

или

```
program 100007 version 1 ready and waiting
program 100007 version 2 ready and waiting
```

в зависимости от версии ypbind, которая установлена. Важным является только сообщение "version 2".

После этого вам должно быть доступно использование клиентских программ NIS, таких как ypcat, и т.д. Например, "ypcat passwd.byname"даст вам базу данных паролей NIS.
ВАЖНО: Если вы пропустите процедуру тестирования, то убедитесь что вы задали имя домена и создали каталог

```
/var/yp
```

Данный каталог ДОЛЖЕН существовать для того, чтобы запуск ypbind был успешен.
Для проверки корректности установки имени домена, используйте /bin/ypdomainname из yp-tools 2.2. Эта программа использует функцию yp_get_default_domain(), которая более ограничена. Она не позволяет например задавать имя домена "(none)", которое устанавливается по умолчанию в Linux и может создать большое количество проблем.
Если тест работает, то вы можете теперь захотеть изменить ваши файлы старта системы таким образом, чтобы ypbind запускался во время загрузки и ваша система становилась клиентом NIS. Убедитесь, что имя домена установлено перед тем как запускать ypbind.
Хорошо. Теперь перегрузите машину и смотрите сообщения, выдаваемые при загрузке, чтобы увидеть, что ypbind действительно запустился.

6.4 Установка клиента NIS используя традиционоык OIS

Для поиска узлов вы должны установить (или добавить) запись "nis"в строку lookup order в файле /etc/host.conf. Пожалуйста прочтите станицу руководства man "resolv+(8)"для подробностей.
Добавьте следующую строку в файл /etc/passwd на машинах NIS-клиентах:

```
+::::::
```

Вы можете также использовать символы + и - для добавления/исключения или изменения пользователей. Если вы хотите исключить пользователя guest, то просто добавьте -guest в файл /etc/passwd file. Вы хотите использовать другой интерпретатор команд (например ksh) для пользователя "linux"? Нет проблем, просто добавьте "+linux::::::/bin/ksh"(без кавычек) в файл /etc/passwd. Поля, которые вам не нужно изменять вы должны оставить пустыми. Вы можете также использовать Netgroups для управления пользователем.
Например, для того, чтобы разрешить вход в систему только пользователям miquels, dth и ed, и всем членам сетевой группы sysadmin, но при этом чтобы была доступна информация о всех других пользователях, используйте:

```
+miquels:::::::
+ed:::::::
+dth:::::::
+@sysadmins:::::::
-ftp
+:*::::::/etc/NoShell
```

Заметим, что в Linux вы можете также перекрыть поле пароля, как мы делали в этом примере. Мы также удалили имя "ftp", так что оно стало неизвестным и anonymous ftp работать не будет.
Сетевая группа может выглядеть так

```
sysadmins (-,software,) (-,kukuk,)
```

ВАЖНО: Возможность работы с сетевой группой реализуется начиная с libc 4.5.26. Если вы имеете версию libc младше 4.5.26, каждый пользователь в базе данных паролей NIS может иметь доступ к вашей linux машине, если вы запустили "ypbind"!

6.5 Установка клиента NIS используя NYS

Все что требуется - это файл с настройками NIS (/etc/yp.conf) с корректной информацией о сервере (серверах). Также, должен быть корректно установлен файл с настройками Переключателя Служб Имен (/etc/nsswitch.conf).
Вы должны установить ypbind. Это не требует libc, но требуется для утилит NIS(YP).
Если вы желаете использовать возможности добавления/удаления пользователя (+/-guest/+@admins), вы должны использовать "passwd: compat"и "group: compat"в файле nsswitch.conf. Заметим, что там нет строчки "shadow: compat"! Вы должны использовать "shadow: files nis"в этом случае.
Исходные тексты NYS являются частью исходных текстов libc 5. Когда вы запускаете configure, сперва скажите "NO"на вопрос "Values correct", затем "YES"на вопрос "Build a NYS libc from nys".

6.6 Установка клиента NIS Client используя glibc 2.x

glibc использует "традиционную NIS", так что вам нужно просто запустить ypbind. Файл с настройками Переключателя Служб Имен (/etc/nsswitch.conf) должен быть корректно установлен. Если вы используете режим compat для passwd, shadow или group, вы должны добавить "+"в конец этих файлов и вы можете использовать возможность добавления/исключения пользователей. Настройка точно такая же как в Solaris 2.x.

6.7 Файл nsswitch.conf

Файл Переключателя Служб Имен /etc/nsswitch.conf определяет порядок поиска, который выполняется когда требуется определенный кусок информации, также как файл /etc/host.conf, который определяет способ выполнения поиска узлов. Например, строка

```
hosts: files nis dns
```

говорит, что функции поиска узлов должны сперва смотреть в локальный файл /etc/hosts, затем производить поиск через NIS и наконец использовать службу доменных имен (/etc/resolv.conf и демон named), и если нужный узел не найден, возвратить ошибку. Данный файл должен быть доступен на чтение для любого пользователя! Вы можете найти больше информации на станице руководства nsswitch(5) или nsswitch.conf(5).
Хороший файл /etc/nsswitch.conf для NIS это:

```
#
# /etc/nsswitch.conf
#
```

```
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Legal entries are:
#
#       nisplus                 Use NIS+ (NIS version 3)
#       nis                     Use NIS (NIS version 2), also called YP
#       dns                     Use DNS (Domain Name Service)
#       files                   Use the local files
#       db                      Use the /var/db databases
#       [NOTFOUND=return]       Stop searching if not found so far
#

passwd:     compat
group:      compat
# For libc5, you must use shadow: files nis
shadow:     compat

passwd_compat: nis
group_compat: nis
shadow_compat: nis

hosts:      nis files dns

services:   nis [NOTFOUND=return] files
networks:   nis [NOTFOUND=return] files
protocols:  nis [NOTFOUND=return] files
rpc:        nis [NOTFOUND=return] files
ethers:     nis [NOTFOUND=return] files
netmasks:   nis [NOTFOUND=return] files
netgroup:   nis
bootparams: nis [NOTFOUND=return] files
publickey:  nis [NOTFOUND=return] files
automount:  files
aliases:    nis [NOTFOUND=return] files
```

passwd_compat, group_compat и shadow_compat поддерживаются только glibc 2.x. Если в файле /etc/nsswitch.conf нет правил для shadow, glibc будет использовать для поиска правило passwd. Для glibc имеет несколько больше модулей для поиска таких как hesoid. Для подробностей смотрите документацию на glibc.

6.8 Теневые пароли в NIS

Теневые пароли через NIS всегда плохая идея. Вы теряете безопасность, которую дают вам теневые пароли и кроме того такая возможность поддерживается только некоторыми библиотеками C в Linux. Хорошая идея в использовании теневых паролей с NIS состоит в том, чтобы поместить в /etc/shadow только локальных системных пользователей. Удалите записи о пользователях NIS из базы данных теневых паролей или поместите пароли обратно в файл /etc/passwd. Вы можете использовать теневой пароль для пользователя root и обычный пароль для пользователя NIS. Это будет работать с любым клиентом NIS.

Linux

Только библиотека GNU C 2.x в Linux поддерживает теневые пароли через NIS. Linux libc5 скомпилированная с NYS также имеет возможности для этого. Но код в ней плохо работает в некоторых случаях и может работать не всегда корректно.

Solaris

Solaris не имеет поддержку теневых паролей через NIS.

PAM

PAM не поддерживает теневых паролей через NIS, особенно pam_pwdb/libpwdb. Это большая проблема для пользователей RedHat 5.x. Если вы имеете glibc и PAM, вам нужно изменить значения /etc/pam.d/*. Замените все правила pam_pwdb на pam_unix_* модули. Но из-за ошибки в pam_unix_auth.so это не всегда работает.

Пример файла /etc/pam.d/login:

```
#%PAM-1.0
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_unix_auth.so
auth       required     /lib/security/pam_nologin.so
account    required     /lib/security/pam_unix_acct.so
password   required     /lib/security/pam_unix_passwd.so
session    required     /lib/security/pam_unix_session.so
```

Для auth вам нужно использовать модуль pam_unix_auth.so, для account модуль pam_unix_acct.so, для password модуль pam_unix_passwd.so и для session модуль pam_unix_session.so.

7 Что мне нужно для установки NIS+ ?

7.1 Программное обеспечение

Код клиента Linux NIS+ был разработан для GNU C library 2. Также имеется порт для версии Linux libc5, так как многие коммерческие приложения собраны с этой библиотекой и не могут быть перекомпилированы для использования glibc. Имеется несколько проблем с libc5 и NIS+: статические программы не могут быть связаны с ней и программы скомпилированные с этой библиотекой не работают с другими версиями libc5.
Вам нужно получить и скомпилировать библиотеку GNU C Library 2.1 для платформы Intel или GNU C Library 2.1.1 для 64bit платформ. В качестве базовой системы вам понадобится основанный на glibc дистрибутив Linux, такой как Debian 2.x, RedHat 5.x или SuSE Linux 6.x.
Для других дистрибутивов вам понадобится перекомпилировать компилятор gcc/g++, libstdc++ и ncurses. Для Redhat, вам понадобится сделать большое количество изменений в настройках PAM. Для SuSE Linux 6.0, вам понадобится перекомпилировать пакет shadow.
Клиент NIS+ может быть получен отсюда:

Site	Directory	File Name
ftp.funet.fi	/pub/gnu/funet	libc-*, glibc-crypt-*, glibc-linuxthreads-*
ftp.kernel.org	/pub/linux/utils/net/NIS+	nis-utils-19990223.tar.gz
ftp.kernel.org	/pub/linux/utils/net/NIS+	pam_keylogin-1.2.tar.gz

Дистрибутивы основанные на glibc могут быть получены отсюда:

Site	Directory
ftp.debian.org	/pub/debian/dists/slink
ftp.redhat.com	/pub/redhat/redhat-5.2
ftp.suse.de	/pub/SuSE-Linux/6.0

Для компиляции библиотеки GNU C пожалуйста следуйте инструкциям, которые идут вместе с исходными текстами. Вы можете найти исправленную версию libc5, основанную на NYS, и исходные тексты как замену стандартной libc5 здесь:

```
Site              Directory                  File Name

ftp.kernel.org    /pub/linux/utils/net/NIS+  libc-5.4.44-nsl-0.4.10.tar.gz
```

Вы должны также посмотреть *http://www.suse.de/~kukuk/linux/nisplus.html* <http://www.suse.de/~kukuk/linux/nisplus.html> для подробной информации и последних версиях исходных текстов.

7.2 Установка клиента NIS+

ВАЖНО: Для установки клиента NIS+ прочтите вашу документацию Solaris NIS+ которая говорит о стороне сервера. Этот документ описывает только то, что нужно сделать на стороне клиента!
После установки новой libc и nis-tools, создайте мандат для нового клиента на сервере NIS+. Убедитесь, что запущен portmap. Затем проверьте, чтобы ваш Linux PC имел то же самое время как и NIS+ сервер. По соображениям безопастности RPC, вы имеете только маленькое окно около 3-х минут, в котором созданные вами мандаты разрешены. Хорошо бы запустить xntpd на каждый узел. После этого, выполните команды

```
domainname nisplus.domain.
nisinit -c -H <NIS+ server>
```

для инициализации файла холодного старта. Прочтите страницу руководства по nisinit на предмет опций. Убедитесь, что имя домена будет всегда установлено после перезагрузки. Если вы не знаете какое у вас в сети имя домена NIS+, спросите у администратора вашей системы/сети.
Теперь вы должны изменить ваш файл /etc/nsswitch.conf. Убедитесь, что только после publickey стоит nisplus ("publickey: nisplus"), и ничего другого!
Затем запустите keyserv и убедитесь, что он будет всегда запускаться во время загрузки как первый демон после portmap. Запустите

```
keylogin -r
```

для записи root secretkey на вашей системе. (Я надеюсь, что вы добавили publickey для нового узла в NIS+ сервер?).
Команда "niscat passwd.org_dir"должна выдать вам все ваши записи в базе данных паролей.

7.3 NIS+, keylogin, login и PAM

Когда пользователь входит в систему, ему нужно установить его secretkey для keyserv. Это делается вызовом "keylogin". login из пакета shadow будет делать это для пользователя, если он был скомпилирован для glibc 2.1. Для login, основанном на PAM, вы должны установить pam_keylogin-1.2.tar.gz и изменить файл /etc/pam.d/login для использования pam_unix_auth, а не pwdb, который не поддерживает NIS+. Например:

```
#%PAM-1.0
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_keylogin.so
auth       required     /lib/security/pam_unix_auth.so
auth       required     /lib/security/pam_nologin.so
account    required     /lib/security/pam_unix_acct.so
password   required     /lib/security/pam_unix_passwd.so
session    required     /lib/security/pam_unix_session.so
```

7.4 Файл nsswitch.conf

Файл Переключателя Служб Имен /etc/nsswitch.conf определяет порядок поиска, который выполняется когда требуется определенный кусок информации, также как файл /etc/host.conf, который определяет способ выполнения поиска узлов. Например, строка

```
hosts: files nis dns
```

говорит, что функции поиска узлов должны сперва смотреть в локальный файл /etc/hosts, затем производить поиск через NIS+ и наконец использовать службу доменных имен (/etc/resolv.conf и демон named), и если нужный узел не найден, возвратить ошибку. Данный файл должен быть доступен на чтение для любого пользователя! Вы можете найти больше информации на станице руководства nsswitch(5) или nsswitch.conf(5).
Хороший файл /etc/nsswitch.conf для NIS+ это:

```
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Legal entries are:
#
#       nisplus                 Use NIS+ (NIS version 3)
#       nis                     Use NIS (NIS version 2), also called YP
#       dns                     Use DNS (Domain Name Service)
#       files                   Use the local files
#       db                      Use the /var/db databases
#       [NOTFOUND=return]       Stop searching if not found so far
#

passwd:     compat
# for libc5: passwd: files nisplus
group:      compat
# for libc5: group: files nisplus
shadow:     compat
# for libc5: shadow: files nisplus

passwd_compat: nisplus
group_compat:  nisplus
shadow_compat: nisplus

hosts:      nisplus files dns

services:   nisplus [NOTFOUND=return] files
networks:   nisplus [NOTFOUND=return] files
protocols:  nisplus [NOTFOUND=return] files
rpc:        nisplus [NOTFOUND=return] files
ethers:     nisplus [NOTFOUND=return] files
netmasks:   nisplus [NOTFOUND=return] files
netgroup:   nisplus
bootparams: nisplus [NOTFOUND=return] files
```

```
publickey:  nisplus
automount:  files
aliases:    nisplus [NOTFOUND=return] files
```

8 Установка сервера NIS

8.1 Программа-сервер ypserv

Данный документ описывает только установку сервера NIS "ypserv".
Сам сервер может быть найден здесь:

```
Site              Directory                    File Name

ftp.kernel.org    /pub/linux/utils/net/NIS     ypserv-1.3.6.tar.gz
```

Также неплохо посмотреть страничку *http://www.suse.de/kukuk/linux/nis.html* <http://www.suse.de/~kukuk/linux/nis.html> для подробностей.
Установка сервера одна и та же как для традиционной NIS так и для NYS.
Скомпилируйте программное обеспечение, чтобы получить программы ypserv и makedbm. Вы можете настроить ypserv для использования файла securenet или с использованием tcp_wrapper. tcp_wrapper является более удобным, но большое количество людей имеют с ним проблемы. И некоторые файлы с настройками для tcp_wrappers могут привести к нехватке памяти. Если у вас проблемы с ypserv скомпилированным для tcp_wrapper, перекомпилируйте его для использования с файлом securenets. Команда ypserv –version скажет вам, какую версию вы имеете.
Если вы запустили ваш сервер как мастер, определите какие файлы нужны вам для доступа через NIS и затем добавьте или удалите соответствующие записи в правиле "all"в /var/yp/Makefile. Вы всегда должны просматривать Makefile и править Options в начале этого файла.
Есть одно большое различие между ypserv 1.1 и ypserv 1.2. Начиная с версии 1.2, дескрипторы файлов кэшируются. Это приводит к тому, что вы должны вызывать makedbm всегда с опцией -c, если вы создаете новые карты. Убедитесь, что вы используете новый /var/yp/Makefile от ypserv 1.2 или выше или добавьте флаг -c для makedbm в Makefile. Если вы этого не сделаете, ypserv будет продолжать использовать старые карты и не будет их обновлять.
Теперь отредактируйте /var/yp/securenets и /etc/ypserv.conf. Для подробностей, прочтите страницы руководства man на ypserv(8) и ypserv.conf(5).
Убедитесь, что portmapper (portmap(8)) запущен и запустите сервер ypserv. Команда

```
% rpcinfo -u localhost ypserv
```

должна выдать примерно следующее

```
program 100004 version 1 ready and waiting
program 100004 version 2 ready and waiting
```

Строка "version 1"может быть опущена в зависимости от версии ypserv и настроек, которые вы используете. Она необходима только если вы имеете старых клиентов NIS от SunOS 4.x.
Теперь сгенерируйте базу данных NIS (YP). На мастер-сервере запустите команду

```
% /usr/lib/yp/ypinit -m
```

На подчиненном сервере убедитесь, что ypwhich -m работает. Это означает, что ваш подчиненный сервер должен быть настроен как клиент NIS перед тем как вы запустите команду

```
% /usr/lib/yp/ypinit -s masterhost
```

для установки этого узла как подчиненного сервера NIS.
Вот теперь ваш сервер запущен.
Если вы имеете проблемы, вы можете запустить ypserv и ypbind в режиме отладки в другом терминале. Отладочные сообщения должны показать вам где произошла ошибка.
Если вам нужно обновить карту, запустите make в каталоге /var/yp на вашем мастер-сервере. Это приведет к обновлению карты и ее выталкиванию на подчиненные серверы, если ее исходный файл имеет более свежую дату. Пожалуйста не используйте команду ypinit для обновления карты.
Может быть вы захотите исправить crontab пользователя root *на подчиненном* сервере и добавить туда следующие строки:

```
20 *    * * *    /usr/lib/yp/ypxfr_1perhour
40 6    * * *    /usr/lib/yp/ypxfr_1perday
55 6,18 * * *    /usr/lib/yp/ypxfr_2perday
```

Тогда вы будете уверены, что большинство карт NIS обновлены, даже если какое-нибудь обновление утеряно, потому что подчиненный сервер был выключен во время выполнения обновления на мастер-сервере.
Вы можете добавить подчиненный сервер позднее. Во первых, убедитесь, что новый подчиненный сервер имеет права на подключение к мастер-серверу NIS. Затем запустите

```
% /usr/lib/yp/ypinit -s masterhost
```

на новом подчиненном сервере. На мастер-сервере добавьте имя нового подчиненного сервера в файл /var/yp/ypservers и запустите make в каталоге /var/yp для обновления карты.
Если вы хотите ограничить доступ пользователей к вашему серверу NIS, вы должны установить NIS сервер как клиент, запустив ypbind и добавить записи со знаком плюс в /etc/passwd _halfway_. Функции библиотеки будут игнорировать все обычные записи после первой записи NIS и будут получать остаток информации от NIS. Это способ обслуживания правил доступа NIS. Пример:

```
root:x:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:
bin:*:2:2:bin:/bin:
sys:*:3:3:sys:/dev:
sync:*:4:100:sync:/bin:/bin/sync
games:*:5:100:games:/usr/games:
man:*:6:100:man:/var/catman:
lp:*:7:7:lp:/var/spool/lpd:
mail:*:8:8:mail:/var/spool/mail:
news:*:9:9:news:/var/spool/news:
uucp:*:10:50:uucp:/var/spool/uucp:
nobody:*:65534:65534:noone at all,,,,:/dev/null:
+miquels::::::
+:*:::::/etc/NoShell
[ All normal users AFTER this line! ]
tester:*:299:10:Just a test account:/tmp:
miquels:1234567890123:101:10:Miquel van Smoorenburg:/home/miquels:/bin/zsh
```

Пользователь "tester"будет существовать, но у его интерпретатором команд будет /etc/NoShell. Пользователь miquels будет иметь нормальный доступ.
В противоположность этому, вы можете отредактировать файл /var/yp/Makefile и настроить NIS для использования другого файла паролей. На больших системах, файлы паролей и групп NIS обычно записываются в /etc/yp/. Если вы делаете это, то обычные инструменты администратора, которые работают с файлом паролей passwd, такие как chfn, adduser не будут работать корректно и вам понадобятся специальные инструменты.
Однако, yppasswd, ypchsh и ypchfn конечно же работать будут.

8.2 Программа-сервер yps

Для установки сервера NIS "yps"пожалуйста вернитесь к предыдущему параграфу. Сервер "yps"устанавливается сходным образом, _но_ он к нему нельзя применить те же инструкции в точности. "yps"не поддерживается автором и содержит некоторые дырки в безопастности. Лучше бы вам его не использовать.
Вы можете найти программное обеспечение "yps"по адресу:

```
Site                  Directory                   File Name

ftp.lysator.liu.se    /pub/NYS/servers            yps-0.21.tar.gz
ftp.kernel.org        /pub/linux/utils/net/NIS    yps-0.21.tar.gz
```

8.3 Программа rpc.ypxfrd

rpc.ypxfrd - используется для увеличения скорости передачи очень больших карт NIS от мастер-сервера NIS к подчиненным серверам. Если подчиненный сервер NIS получает сообщение, что имеется новая карта, то он запускает pxfr для того чтобы ее получить. ypxfr будет читать содержимое карты от мастер-сервера, используя функцию yp_all(). Этот процесс может занять несколько минут, когда карты очень большие.
Сервер rpc.ypxfrd увеличивает скорость процесса передачи путем предоставления подчиненным серверам NIS возможности просто копировать файлы карт с мастер-сервера вместо того, чтобы строить свои собственные карты "с нуля". rpc.ypxfrd использует основанный на RPC протокол передачи файлов, так что подчиненные сервера не нуждаются в построении новых карт.
rpc.ypxfrd может быть запущен через inetd. Но таким образом он запускается очень медленно, он должен бы запускаться ypserv. Запуск rpc.ypxfrd будет вам нужен только на мастер-сервере NIS.

8.4 Программа rpc.yppasswdd

Когда пользователи изменяют собственные пароли, база данных паролей NIS и предположительно другие базы данных NIS, которые зависят от нее должны быть обновлены. Программа "rpc.yppasswdd"это сервер, который управляет изменением паролей и гарантирует, что информация NIS будет вовремя обновлена. В настоящий момент rpc.yppasswdd интегрирован в ypserv. Теперь вам не нужны отдельные yppasswd-0.9.tar.gz или yppasswd-0.10.tar.gz, и вы больше не должны их использовать. rpc.yppasswdd в ypserv 1.3.2 имеет полную поддержку теневых паролей. yppasswd теперь часть yp-tools-2.2.tar.gz.
Запуск rpc.yppasswdd нужен вам только на мастер-сервере NIS. По умолчанию, пользователям не разрешается изменять их собственные имена или интерпретатор команд. Вы можете позволить им это используя опции -e chfn или -e chsh.
Если ваши файлы passwd и shadow находятся в каталоге отличном от /etc, то вам нужно использовать опцию -D. Например, если вы поместили их в каталог /etc/yp и хотите разрешить пользователям изменять их интерпретаторы команд, то вы должны запустить rpc.yppasswdd со следующими параметрами:

```
rpc.yppasswdd -D /etc/yp -e chsh
```

or

```
rpc.yppasswdd -s /etc/yp/shadow -p /etc/yp/passwd -e chsh
```

Больше ничего делать не надо. Вы только должны убедится, что rpc.yppasswdd использует те же файлы что и /var/yp/Makefile. Ошибки будут протоколироваться в syslog.

9 Проверка NIS/NYS

Если все хорошо (как должно быть), то вы можете проверить ваши настройки несколькими простыми командами. Просмотрите, например, ваш файл паролей для использования с NIS, командой

```
% ypcat passwd
```

которая должна вам выдать содержимое файла паролей NIS. Команда

```
% ypmatch userid passwd
```

(где userid это имя для входа в систему соответствующего пользователя) должна выдать вам запись про соответствующего пользователя в файле паролей NIS. Программы "ypcat"и "ypmatch"должны быть включены в ваш дистрибутив традиционной NIS или NYS.
Если пользователь не может войти в систему, запустите на клиентской машине следующую программу:

```
#include <stdio.h>
#include <pwd.h>
#include <sys/types.h>

int
main(int argc, char *argv[])
{
 struct passwd *pwd;

 if(argc != 2)
   {
     fprintf(stderr,"Usage: getwpnam username\n");
     exit(1);
   }

 pwd=getpwnam(argv[1]);

 if(pwd != NULL)
   {
     printf("name.....: [%s]\n",pwd->pw_name);
     printf("password.: [%s]\n",pwd->pw_passwd);
     printf("user id..: [%d]\n", pwd->pw_uid);
     printf("group id.: [%d]\n",pwd->pw_gid);
     printf("gecos....: [%s]\n",pwd->pw_gecos);
     printf("directory: [%s]\n",pwd->pw_dir);
     printf("shell....: [%s]\n",pwd->pw_shell);
   }
 else
   fprintf(stderr,"User \"%s\" not found!\n",argv[1]);

 exit(0);
}
```

Запуск этой программы с именем пользователя в качестве параметра выдаст всю информацию функции getpwnam для этого пользователя. Это должно показать вам, что запись пользователя корректна. Большинство проблем связано с тем, что поле пароля перекрывается символом "*".
GNU C Library 2.1 (glibc 2.1) поставляется с инструментом, называемым getent. Используйте эту программу вместо данной выше. Вы можете попытаться выполнить:

```
 getent passwd
```

или

```
 getent passwd login
```

10 Общий проблемы и неисправности NIS

Здесь изложен ряд проблем, о которых нам сообщили разные пользователи:

1. Библиотеки до версии 4.5.19 содержат ошибку. NIS не будет с ними работать.
2. Если вы обновили библиотеки с версии 4.5.19 до 4.5.24 то команда su не работает. Вам нужно взять команду su из дистрибутива slackware 1.2.0.
3. Когда сервер NIS становится недоступен и затем снова становится доступен, ypbind выдает сообщение об ошибке вида:

   ```
   yp_match: clnt_call:
                RPC: Unable to receive; errno = Connection refused
   ```

   и вход в систему для тех, кто в ней зарегистрирован в базе данных NIS, становится невозможен. Попытайтесь войти в систему как root, убить ypbind и запустить его снова. Также може помочь обновление ypbind до версии 3.3 или выше.
4. После обновления libc до версии выше 5.4.20, инструменты YP не будут работать. Вам понадобятся yp-tools 1.2 или выше для libc >= 5.4.21 и glibc 2.x. Для более ранних версий libc вам нужны yp-clients 2.2. yp-tools 2.x будут работать со всеми библиотеками.
5. В libc 5.4.21 - 5.4.35 yp_maplist работает некорректно, вам нужна версия 5.4.36 или выше, иначе некоторые программы YP такие как ypwhich будут падать.
6. libc 5 с традиционным NIS не поддерживает теневые пароли в NIS. Вам нужна libc5 + NYS или glibc 2.x.
7. ypcat shadow не показывает карту shadow. Это правильно, так как имя карты shadow - это shadow.byname, а не shadow.
8. Solaris не всегда использует привилигированные порты. Так что не используйте password mangling если у вас клиент Solaris.

11 Frequently Asked Questions

Ответы на большинство ваших вопросов уже есть. Если у вас есть вопрос, который еще не рассматривался, пошлите сообщение в группу новостей

```
comp.os.linux.networking
```