

Linux NIS(YP)/NYS/NIS+ HOGYAN

Thorsten Kukuk

Ez a dokumentáció elmagyarázza, hogyan kell a Linux rendszert NIS(YP) vagy NIS+ kliensként beállítani, és hogy kell NIS szerverként telepíteni.

Tartalomjegyzék

1. Bevezetés	3
1.1. A dokumentum új verziói	3
1.2. A felelősség teljes elhárítása	3
1.3. Visszajelzés és javítások	3
1.4. Köszönetnyilvánítás	4
1.5. Magyar fordítás	4
2. Összefoglalás és általános információ	4
2.1. Kifejezések összefoglalása	4
2.2. Néhány általános információ	6
3. NIS, NYS vagy NIS+?	6
3.1. libc 4/5 hagyományos NIS-el, vagy NYS ?	6
3.2. glibc 2 és NIS/NIS+	6
3.3. NIS vagy NIS+ ?	7
4. Hogyan működik?	7
4.1. Hogyan működik a NIS?	7
4.2. Hogyan működik a NIS+?	7
5. Az RPC Portmapper (Távoli Eljáráshívás kapuhozzárendelő)	8
6. Mire van szükség a NIS üzembe helyezéséhez?	8
6.1. Határozd meg, hogy géped szerver, szolga vagy kliens lesz.	8
6.2. A szoftver	9
7. A NIS kliens telepítése	9
7.1. Az ypbind démon	9
7.2. A NIS kliens beállítása hagyományos NIS használatával	11
7.3. NIS kliens beállítása NYS használatával	12
7.4. NIS kliens beállítása glibc 2.x segítségével	12
7.5. Az nsswitch.conf fájl	12
7.6. Árnycsapat jelszavak NIS-sel	13
8. Mire van szükség a NIS+ beállításához?	14
8.1. Szoftver	15
8.2. NIS+ kliens beállítása	15
8.3. NIS+, keylogin, bejelentkezés és PAM	16

8.4. Az nsswitch.conf fájl	16
9. NIS szerver beállítása	17
9.1. Az ypserv szerver-program	17
9.2. Az yps szerver program	19
9.3. Az rpc.ypxfrd program	20
9.4. Az rpc.yppasswdd program	20
10. A NIS/NYS telepítésének ellenőrzése	21
11. NIS térképek készítése és karbantartása	22
11.1. Új NIS térkép létrehozása	22
11.2. NIS térképek frissítése	22
11.3. A térképájl bejegyzéseinek hossza	23
12. Túlélőcsomag újraindítás esetére	23
12.1. A NIS indító (init) szkript	23
12.2. NIS domainnév	24
12.3. Linux-disztribúció specifikus megjegyzések.....	24
13. Jelszóváltás az rpasswd program segítségével	24
13.1. A szerver beállítása	25
13.2. A kliens beállítása	26
14. Általános, valamint NIS problémák elhárítása	26
15. Gyakran Ismételt Kérdések	27

1. Bevezetés

Egyre több linuxos gépet telepítenek hálózat részeként. A hálózati adminisztráció egyszerűsítéséhez, a legtöbb hálózatban (leginkább a Sun alapú hálózatokban) Hálózati Információs Szolgáltatást (Network Information Service, továbbiakban NIS) futtatnak. A Linux rendszerek teljes mértékben fel tudják használni a már meglévő NIS szolgáltatásokat, és ők maguk is képesek NIS szolgáltatásokat nyújtani. Mindemellett képesek teljes értékű NIS+ kliensként viselkedni, ez a támogatás egyelőre béta állapotban van.

Ez a dokumentáció megpróbál választ adni a NIS(YP) és NIS+ beállításával kapcsolatos kérdésekre, amik a Linux rendszeren felmerülhetnek. Ne felejtse el elolvasni "Az RPC Portmapper (Távoli Eljáráshívás kapuhozzárendelő)" fejezetet!

A NIS-HOGYANt szerkeszti, és karbantartja:

Thorsten Kukuk, <kukuk@suse.de>

Az első NIS-HOGYAN forrása az alábbi emberektől származik, akiknek eme dokumentáció első verzióit köszönhetjük:

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

1.1. A dokumentum új verziói

Mindig megtalálható a legfrissebb változatot, megnézheted a World Wide Web használatával a <http://www.linux-nis.org/nis-howto/HOWTO/NIS-HOWTO.html> honlapot.

A dokumentáció új verziói több linuxos WWW és FTP helyre felkerülnek, beleértve az LDP honlapot is.

A dokumentáció fordításaira mutató hivatkozásokat a <http://www.linux-nis.org/nis-howto/> honlapon találod.

1.2. A felelősség teljes elhárítása

Habár ezt a dokumentációt a legjobb tudásom szerint állítottam össze, lehet, sőt, szinte biztos, hogy tartalmaz hibákat. Kérlek, olvass el minden OLVASSEL (README) fájlt, ami ebben a dokumentációban leírtakhoz kapcsolódik, hogy még részletesebb, és pontosabb információkat szerezhess. Megpróbálok amennyire csak lehet hibátlanul tartani ezt a dokumentumot.

1.3. Visszajelzés és javítások

Ha kérdésed, vagy megjegyzésed van ezzel a dokumentummal kapcsolatban, kérlek ne habozz levelet küldeni Thorsten Kukuknak a kukuk@linux-nis.org (mailto:kukuk@linux-nis.org) e-mail címre. Örömmel fogadok bármilyen ötletet vagy kritikát. Ha hibát találnál e dokumentációban, kérlek értesíts, hogy ki tudjam javítani a következő változatban. Köszönöm.

Kérlek *ne* küldj nekem levelet a Linux disztribúciód belső problémáiról! Nem ismerem mindegyik Linux disztribúciót, de megpróbálom hozzáadni az összes megoldást, amit küldesz.

1.4. Köszönetnyilvánítás

Szeretnénk megköszönni mindenkinek, aki közreműködött (közvetlenül, vagy közvetve) eme dokumentum létrehozásában. ABC sorrendben:

Byron A Jeff	<byron@cc.gatech.edu>
Markus Rex	<msrex@suse.de>
Miquel van Smoorenburg	<miquels@cistron.nl>
Dan York	<dyork@lodestar2.com>
Christoffer Bromberg	<christoffer@web.de>

Theo de Raadt felelős az eredeti yp-kliensek kódjáért. Swen Thuemmler portolta az yp-kliensek kódját Linuxra, illetve az yp-rutinokat libc- be (szintén Theo munkájára alapozva). Thorsten Kukuk írta a NIS(YP) és NIS+ rutinokat GNU libc 2.x-re a semmiből.

1.5. Magyar fordítás

A magyar fordítást Bábos Balázs (mailto:bbk@swi.hu_NO_SPAM) készítette (?). A dokumentumot Völgyi Péter (mailto:petvolgyi@freemail.hu_NO_SPAM) frissítette (2003.02.28). A lektorálást Szilágyi Szilárd (mailto:sysop@szigetvar.partner.enternet.hu_NO_SPAM) végezte el (2003.09.04). Utoljára Daczi László (mailto:dacas@freemail.hu_NO_SPAM) frissítette (2003.10.14). A dokumentum legfrissebb változata megtalálható a Magyar Linux Dokumentációs Projekt (<http://tldp.fsf.hu/index.html>) honlapján.

2. Összefoglalás és általános információ

2.1. Kifejezések összefoglalása

Ebben a dokumentumban nagyon sok szakkifejezés található. Íme a legfontosabb szakkifejezések rövid magyarázata:

DBM

DataBase Management (adatbázis-menedzselés), egy könyvtárnyi függvény, amely kulcs-tartalom párokat kezelnek egy adatbázisban.

DLL

Dynamically Linked Library (dinamikusan láncolt programkönyvtár), futtatható programhoz futásidőben hozzákapcsolódó programkönyvtár.

domainname

A domain name (domain név) egy "kulcs", amit a NIS kliens arra használ, hogy megfelelő NIS szerveret találjon, ami ezt a domain név kulcsot szolgáltatja. Itt jegyezném meg, hogy ennek általában semmi köze sincs a gép(ek) DNS "domain nevéhez" (gép név).

FTP

File Transfer Protocol (fájl átviteli protokoll), fájlok két számítógép közötti átvitelére szolgáló protokoll.

libnsl

Name services library (név szolgáltató könyvtár), SVR4 Unixok névszolgáltatás-hívásainak (getpwnam, getservbyname, stb...) könyvtára. A GNU libc használja ezt a NIS(YP) és NIS+ függvényekhez.

libsocket

Socket services library (foglatat szolgáltatás könyvtár), SVR4 Unixok socket szolgáltatás-hívásainak (socket, bind, listen, stb.) programkönyvtára.

NIS

Network Information Service (hálózati információs szolgáltatás), a hálózat gépei számára olyan információt kínáló szolgáltatás, amit a teljes hálózatnak ismernie kell. A Linux általános libc könyvtára támogatást nyújt a NIS használatához, amire a következőkben "hagyományos NIS" néven fogunk hivatkozni.

NIS+

Network Information Service (Plus :-) (hálózati információs szolgáltatás plusz), alapvetően NIS szteroidokkal. A NIS+ szolgáltatást a Sun Microsystems Inc. tervezte a NIS-t lecserélendő, hogy nagy telepítések esetén biztonságosabb, és jobban kezelhető legyen.

NYS

Ez egy projekt neve, a NIS+-t, YP-t és a Switch (kapcsoló) rövidítése, Peter Eriksson >peter@ifm.liu.se< vezeti. Többek között a NYS könyvtár Name Services Switch (név szolgáltatás kapcsoló) funkcionalitását használó NIS (= YP) kód teljes újraírását foglalja magába.

NSS

Name Service Switch (név szolgáltatás kapcsoló), Az /etc/nsswitch.conf fájl határozza meg a különböző kért információ-darabok fellapozásának sorrendjét.

RPC

Remote Procedure Call (távoli eljárás-hívás). Az RPC rutinok lehetővé teszik C programok számára, hogy hálózaton keresztül más gépeken eljárásokat hívjanak meg. Amikor RPC-ről beszélünk, legtöbbször a Sun RPC változatára gondolunk.

YP

Yellow Pages(tm) (sárga oldalak(tm)), A United Kingdom of British Telecom plc bejegyzett védjegye.

TCP-IP

Transmission Control Protocol/Internet Protocol (átvitelirányító protokoll/internet protokoll), Unix gépeken leggyakrabban ezt az adatkommunikációs protokollt használják.

2.2. Néhány általános információ

A következő 4 sor idézet a Sun(tm) Rendszer- és hálózati adminisztráció kézikönyvéből:

```
"A NIS korábban Sun Yellow Pages (YP) néven volt ismert, de a Yellow Pages(tm) az United Kingdom of British Telecom plc bejegyzett védjegye, és tilos a beleegyezésük nélkül felhasználni."
```

A NIS a Hálózati Információs Szolgáltatás rövidítése. A célja az, hogy a hálózat gépei számára olyan információt kínáljon, amit a teljes hálózatnak ismernie kell. A NIS által szolgáltatott információk:

- felhasználói nevek/jelszavak/home könyvtárak (/etc/passwd)
- csoport információ (/etc/group)

Ha például a jelszavad bejegyzése szerepel a NIS jelszó adatbázisban, be tudsz jelentkezni a hálózat minden olyan gépére, amin fut a NIS kliens program.

A Sun a Sun Microsystems Inc. bejegyzett védjegye, amit a SunSoft Inc. számára licencelt.

3. NIS, NYS vagy NIS+?

3.1. libc 4/5 hagyományos NIS-el, vagy NYS ?

A választás a "hagyományos NIS" és a NYS könyvtár NIS kódja között olyan, mint a választás a lustaság és fejlettség, vagy a rugalmasság és a kaland imádata között.

A "hagyományos NIS" kód az általános C könyvtárban található már jó ideje, néha a korától és a rugalmatlanságától szenved.

A NYS könyvtár NIS kódjának használatához újra kell fordítanod a libc könyvtárat, és bele kell fordítani a NYS kódot (vagy legalábbis szerezned kell valakitől, aki már elkészítette egy előfordított libc változatot).

A másik különbség, hogy a hagyományos NIS kód tartalmaz némi NIS Netgroups (NIS Hálózati csoportok) támogatást, szemben a NYS kóddal. Másfelől a NYS kód lehetővé teszi, hogy árnyék jelszavakat (Shadow Password) használj teljesen átlátszó módon. A "hagyományos NIS" kód nem engedélyezi NIS feletti árnyék jelszavak használatát.

3.2. glibc 2 és NIS/NIS+

Ezt mind el is felejtethed, ha az új GNU C könyvtár 2.x-et (azaz libc6) használsz. Ebben valódi NSS (név kapcsolás szolgáltatás) támogatás van, ami nagyon rugalmassá teszi, valamint a következő NIS/NIS+ térképekre is tartalmaz

támogatást: aliases, ethers, group, hosts, netgroups, networks, protocols, publickey, passwd, rpc, services és shadow. A GNU C könyvtárnak nincs problémája a NIS feletti árnyék jelszavakkal.

3.3. NIS vagy NIS+ ?

A NIS és NIS+ közötti választás nagyon könnyű - használj NIS-t, ha nincs szükség a NIS+-ra, vagy ha komoly biztonsági szükségleteid vannak. NIS+-t sokkal körülményesebb adminisztrálni (nagyon könnyű kezelni a kliens oldalról, de a szerver oldalán szörnyű). Másik probléma, hogy a NIS+ Linux alatti támogatása sok hibát tartalmaz, és a fejlesztése is leállt.

4. Hogyan működik?

4.1. Hogyan működik a NIS?

Egy hálózaton belül legalább egy, NIS szerverként működő gépnek kell lennie. Lehet több NIS szerver is úgy, hogy mindegyik más NIS "körzetet" szolgál ki - vagy lehetnek együttműködő NIS szervereid is, ahol van egy mester NIS szerver, és a többi úgynevezett szolga NIS szerver (egy adott NIS "körzetedre" ez így is van) - vagy lehet vegyesen is...

A szolga szervereknek a NIS adatbázisról csak egy másolatuk van, és ezeket a másolatokat a mester NIS szervertől kapják, amikor abban változás történt. A hálózatod gépeinek számától és a hálózatod megbízhatóságától függően választhatsz, hogy egy vagy több szolga szervert telepítesz. Amikor egy NIS szerver lekapcsolódik, vagy túl lassan válaszol a kérésekre, a NIS kliens, ami ehhez a szerverhez kapcsolódik, megpróbál egy működő vagy gyorsabb szervert találni.

A NIS adatbázisok úgynevezett DBM formátumban tárolódnak, amik ASCII adatbázisból konvertálhatók. Például az /etc/passwd és az /etc/group fájlok közvetlenül átalakíthatók DBM formátumba ASCII-ből-DBM-be átalakító szoftverrel ("makedbm", amit a szerver szoftveréhez csatolnak). A mester NIS szerveren egyaránt kell ASCII és DBM adatbázisnak lennie.

A szolga szerverek minden a NIS térképben történt változásról értesülnek (az "yppush" program segítségével), és automatikusan megkapják az adatbázisok szinkronizálásához szükséges változásokat. A NIS klienseknek nem kell ezt megtenniük, hiszen ők folyamatosan a NIS szerverrel kommunikálnak, hogy a szerverek DBM adatbázisából megszerezzék a szükséges információkat.

A régi ypbind változatok üzenetszórással keresnek futó NIS szervert. Ez nem biztonságos, mert bárki telepíthet NIS szervert, és válaszolhat az üzenetszórással érkező üzenetekre. Az ypbind újabb változatai (ypbind-3.3 vagy ypbind-mt) képesek a szervert konfigurációs fájlból olvasni - tehát nincs szükség üzenetszórásra.

4.2. Hogyan működik a NIS+?

A NIS+ a Sun hálózati információs névszolgáltatásának új változata. A legnagyobb különbség a NIS és NIS+ között az, hogy a NIS+ támogatja az adattitkosítást és a biztonságos RPC hitelesítést.

A NIS+ névmodellje fa-struktúrán alapul. Minden levél a fában egy NIS+ objektumnak felel meg. Az objektumok hat típusa: könyvtár, bejegyzés, csoport, hivatkozás, tábla és privát.

A NIS+ névterület gyökerét alkotó NIS+ könyvtárat gyökér könyvtárnak hívják. Két különleges NIS+ könyvtár létezik: `org_dir` és `groups_dir`. Az `org_dir` (`org=organization`: szervezet, `dir=directory`: könyvtár) könyvtár tartalmazza az összes adminisztrációs táblát, olyanokat mint a `passwd` (`passwd=password`: jelszó), `hosts` (`hosts`: gépnevek) és a `mail_aliases` (`mail aliases`: levél álnevek). A `groups_dir` (`groups`: csoportok) könyvtár tartalmazza a hozzáférés vezérlésére szolgáló NIS+ csoport objektumokat. Az `org_dir`, `groups_dir` és a szülő könyvtárak együttesét NIS+ körzetnek nevezzük (NIS+ domain).

5. Az RPC Portmapper (Távoli Eljáráshívás kapuhozzárendelő)

A lentebb említésre kerülő programok futtatásához el kell indítanod az `/sbin/portmap` programot. Néhány Linux disztribúció már tartalmazza a kódot e démon futtatásához az `/sbin/init.d/` vagy `/etc/rc.d/` könyvtárakban. Csak annyit kell tenned, hogy aktiváld és újraindítd a Linux gépedet. Olvasd el a Linux disztribúció dokumentációjában ennek menetét.

Az RPC portmapper (`portmap(8)`) egy RPC program számokat TCP/IP (vagy UDP/IP) protokoll port számokká alakító szerver. Ennek futnia kell ahhoz, hogy RPC hívásokat (mint amilyeneket a NIS/NIS+ kliens szoftver is nyújt) adhass RPC szervereknek (mint amilyen a NIS vagy NIS+ szerver) azon a gépen. Amikor egy RPC szerver elindul, megmondja a `portmap`-nek hogy melyik porton hallgat, és milyen RPC program számok kiszolgáltatására van felkészítve. Amikor egy kliens RPC hívást szeretne tenni egy adott programszámra, először kapcsolatot teremt a szerver `portmap`-jével, hogy megállapítsa, melyik portcímre küldje az RPC csomagokat.

Szabványosan, az általános RPC szerveret az `inetd(8)` indítja, így a `portmap`-nek már az `inetd` indulása előtt el kell indulnia.

A biztonságos RPC-hez a portmapper-nek szüksége van az idő szolgáltatásra (Time service). Győződj meg arról, hogy engedélyezted az idő szolgáltatást az `/etc/inetd.conf`-ban minden gépre:

```
#
# Az idő szolgáltatás óra egyeztetésre használatos.
#
time    stream  tcp      nowait  root    internal
time    dgram   udp      wait    root    internal
```

FONTOS: Ne feledkezz el a konfigurációs fájlok változtatása után az `inetd` újraindításáról!

6. Mire van szükség a NIS üzembe helyezéséhez?

6.1. Határozd meg, hogy géped szerver, szolga vagy kliens lesz.

Ennek eldöntéséhez két esetet kell megvizsgálni:

1. A géped egy már NIS szervereket tartalmazó hálózat része lesz.
2. Még nincs NIS szervered a hálózatban.

Az első esetben csak a kliens programokra van szükség (ypbind, ypwhich, ypcat, yppoll, ypmatch). A legfontosabb program az ypbind. Ennek a programnak állandóan futnia kell, ami azt jelenti, hogy mindig szerepelnie kell a folyamatok listájában (list of processes). Ez egy démon folyamat, és a rendszerindító fájljából kell indítani (például /etc/init.d/nis, /sbin/init.d/ypclient, /etc/rc.d/init.d/ypbind, /etc/rc.local). Amint fut az ypbind, a géped máris NIS klienssé válik.

A második esetben, ha még nincs NIS szervered, akkor a NIS szerver programokra is szükség lesz (általában ypserv-nek hívják). A "NIS szerver beállítása" fejezet mutatja be, hogy hogyan kell a Linux gépedre NIS szervert telepíteni, használva az **ypserv** demont.

6.2. A szoftver

A NIS kliens és szerver szoftver sikeres lefordításához minden szükséges rendszerhívás megtalálható az "/usr/lib/libc.a" (v.4.4.2 és újabb) rendszerkönyvtárban, vagy a "/lib/libc.so.x" oszott könyvtárban. A GNU C könyvtár 2-höz (glibc 2.x), a /lib/libnsl.so.1 is szükséges.

Néhányan jelezték, hogy a NIS csak 4.5.21 és újabb "/usr/lib/libc.a" változatokkal működik, tehát ha biztonságosan szeretnéd használni, ne használj régebbi libc-eket. A NIS kliens szoftver beszerezhető az alábbi helyekről:

Hely	Könyvtár	Fájl neve
ftp.kernel.org	/pub/linux/utils/net/NIS	yp-tools-2.8.tar.gz
ftp.kernel.org	/pub/linux/utils/net/NIS	ypbind-mt-1.13.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

Amint megszerezted a szoftvert, kérlek, kövesd a szoftverrel kapott utasításokat. Az yp-clients-2.2 libc4-el és libc5-el használható 5.4.20-ig. A libc5.4.21-hez és glibc 2.x-hez yp-tools-1.4.1-re vagy újabbra lesz szükséged. Az új yp-tools-2.4-nek minden Linux libc-vel működnie kell. Mivel volt egy hiba a NIS kódban, ne használj libc-5.4.21-5.4.35 közötti változatot. Használj inkább 5.4.36-os vagy frissebb libc könyvtárat helyette, vagy a legtöbb YP program nem fog működni. Az ypbind 3.3 is működni fog minden könyvtárral. Ha gcc-2.8.x-et vagy újabbat használsz, egcs-t vagy glibc-2.x-t, hozzá kell adnod az ypbind-3.3-glibc5.diff foltot (patch) az ypbind-3.3-hoz. Ha lehetséges ne használj az ypbind 3.3-as verzióját, biztonsági hiányosságokból kifolyólag. Az ypbind-mt egy új, többszálú démon. 2.2-es Linux kernel kell hozzá, és 2.1-es vagy újabb glibc.

7. A NIS kliens telepítése

7.1. Az ypbind démon

Miután sikeresen lefordítottad a szoftvert, készen állsz a telepítésére. Az ypbind démon számára megfelelő hely az /usr/sbin könyvtár. Néhányan mondhatnák, hogy nincs szükséged ypbind-re NYS-t tartalmazó rendszerben. Tévednek. ypwhich-re és ypcat-ra mindig szükség van.

Ezt természetesen root felhasználóként kell elvégezned. A többi binárist (ypwhich, ypcat, yppasswd, yppoll, ypmatch) olyan könyvtárba kell tenni, ami minden felhasználó számára elérhető, általában az /usr/bin könyvtárba.

Újabb ypbind változatok /etc/yp.conf nevű konfigurációs fájlal rendelkeznek. Bedrótozhatsz ide egy NIS szervert - további információkért nézd meg az ypbind(8) kézikönyv oldalt. Erre az fájlra NYS esetén is szükséged van. Például:

```
ypserver 10.10.0.1
ypserver 10.0.100.8
ypserver 10.3.1.1
```

Ha a rendszer fel tudja oldani a gépneveket NIS nélkül, használhatsz gépnevet, különben IP címet kell használnod. Az ypbind-3.3-ban van egy hiba, és csak a legutolsó bejegyzést használja (a példában ypserver 10.3.1.1). Minden más bejegyzést figyelmen kívül hagy. Az ypbind-mt helyesen kezeli ezt, és azt használja, amelyik először válaszol.

Jó ötlet kipróbálni az ypbind-et, mielőtt beleteszed az indítófájlokba. Az ypbind kipróbálásához a következőket kell tenned:

- Győződj meg róla, hogy van YP-körzet név beállításod. Ha ez nincs beállítva, akkor add ki a következő utasítást:

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

ahol a `nis.domain` olyan szöveg, aminek általában SEMMI köze a géped DNS-körzet nevéhez. Ez azért van így, hogy a külső betörők számára megnehezítse a NIS szerveredből a jelszó adatbázis megszerzését. Ha nem tudod, hogy mi a NIS körzet neve a hálózaton, kérdezd meg a rendszergazdát/hálózati adminisztrátort.

- Indítsd el az `"/sbin/portmap"` programot, ha még nem fut.
- Készíts egy `/var/yp` nevű könyvtárat, ha még nem létezik.
- Indítsd el az `/usr/sbin/ypbind` programot.
- Ellenőrizd a `rpcinfo -p localhost` utasítással, hogy az ypbind be tudta-e regisztrálni a szolgáltatását a portmapper-be. A kimenetnek ilyesminek kell lennie:

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

vagy

```
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
```

az általad használt ypbind változattól függően.

- Elindíthatod az `rpcinfo -u localhost ypbind` programot is. Ez az utasítás valami ehhez hasonlót fog eredményezni:

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

vagy

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

A kimenet attól függ, hogy melyik ypbind változatot telepítetted. Csak a "version 2" üzenet fontos.

Ettől a ponttól kezdve használhatod az olyan NIS kliens programokat, mint például az ypcat, stb... Például az **ypcat passwd.byname** visszaadja neked a teljes NIS jelszó-adatbázist.

FONTOS: Ha kihagytd a tesztelő eljárást, győződj meg róla, hogy beállítottad a körzet nevét, és létrehoztd a következő könyvtárat:

```
/var/yp
```

Ennek a könyvtárnak léteznie KELL az ypbind sikeres elindulásához.

A körzetnév helyességének ellenőrzésére használd a **/bin/ypdomainname** programot az yp-tools-2.2-ből. Ez az yp_get_default_domain() függvényt használja, ami sokkal szigorúbb. Nem engedélyezi például a "(semmi)" körzetnevet, ami az alapértelmezett Linux alatt, és sok probléma okozója.

Ha a teszt működik, most érdemes megváltoztatnod a démonokat indító fájlokat, hogy az ypbind a rendszer indulásakor indulhasson, és a rendszered NIS kliensként viselkedjen. Győződj meg róla, hogy a körzetnév az ypbind indítása előtt beállításra kerül!

Nos, ennyi. Indítsd újra a géped, és nézd meg a rendszerüzeneteket, hogy az ypbind elindult-e.

7.2. A NIS kliens beállítása hagyományos NIS használatával

Gépnév feloldáshoz be kell állítanod (vagy hozzá kell adnod) a "nis"-t a feloldási sorrend sorához az `/etc/host.conf` fájlban. Nézd meg a "resolv+.8" kézikönyv oldalt a részletes leírásért.

Add hozzá a NIS kliens az `/etc/passwd` fájlhoz a következő sort:

```
+:::~:
```

Használhatod a + és a - karaktereket felhasználó hozzáadásához/kizárásához vagy megváltoztatásához. Ha a vendég felhasználót szeretnéd kizárni, csak add hozzá az `/etc/passwd` fájlhoz a "-guest" kapcsolót. Más parancsértelmezőt (például ksh) szeretnél használtatni a "linux" felhasználóval? Nem probléma, egyszerűen add hozzá a "+linux:::::/bin/ksh" (idézőjelek nélkül) sort az `/etc/passwd` fájlhoz. Azokat a mezőket, amelyeket nem akarsz használni, üresen kell hagyni. Használhatod a Netgroups-t a felhasználó szabályozáshoz.

Például ahhoz hogy csak miquels, dth és ed, valamint a sysadmin hálózati csoport számára engedélyezd a bejelentkezés-hozzáférést, és a többiek számára megmaradjon az azonosító, a következőket kell megadnod:

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

Jegyezzük meg, hogy Linux rendszerben a jelszó mezőt is felül lehet bírálni ugyanúgy, ahogy ebben a példában tettük. Eltávolítottuk az "ftp" felhasználót is, tehát itt többé nem létezik, azaz az anonymous ftp nem fog többé működni.

A hálózati csoport így fog kinézni:

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

FONTOS: A hálózati csoport (netgroup) beállítási lehetőség a 4.5.26-os libc változattól kezdve használható. Ha 4.5.26-os libc-nél korábbi változatod van, minden NIS jelszó-adatbázisban szereplő felhasználó hozzáférhet a Linux gépedhez, ha "ypbind"-et futtatsz!

7.3. NIS kliens beállítása NYS használatával

Mindössze arra van szükség, hogy a NIS konfigurációs fájl (/etc/yp.conf) a helyes szerver(ek)re mutasson. Ezen kívül a Névszolgáltatás Kapcsoló (Name Services Switch) konfigurációs fájl (/etc/nsswitch.conf) helyesen be kell állítani.

Az ypbind-et fel kell még telepítened. Erre nem a libc-nek, hanem a NIS(YP) tools-nak van szüksége.

Ha szeretnéd használni a felhasználók hozzáadása/kizárása jellemzőt (+/-guest/+@admins), a "passwd: compat"-t és "group: compat" sort be kell az nsswitch.conf fájlba tenned. Jegyezzük meg, hogy nincs "shadow: compat"! "shadow: files nis" bejegyzést kell használnod ebben az esetben.

A NYS források nem részei az 5-ös libc forrásnak. Ha a configure szkriptet futtatod, válaszd első alkalommal "NO"-t a "Values correct" kérdésre, és utána "YES"-t a "Build a NYS libc from nys" kérdésre.

7.4. NIS kliens beállítása glibc 2.x segítségével

A glibc a "hagyományos NIS"-t használja, tehát el kell indítanod az ypbind-et. A Név Szolgáltatás Kapcsoló konfigurációs (Name Services Switch) fájl (/etc/nsswitch.conf) helyesen be kell állítani. Ha a compat módot használod a passwd-hez, shadow-hoz vagy a group-hoz, hozzá kell adnod ezen fájlok végéhez a "+"-t, és használhatod a felhasználó hozzáadás/kizárás jellemzőt. A beállítás ugyanilyen Solaris 2.x esetén is.

7.5. Az nsswitch.conf fájl

A Hálózati Szolgáltatások (Network Services) beállítási fájl (/etc/nsswitch.conf) határozza meg egy meghatározott információcsoport lekérdezésekor a feloldások sorrendjét, hasonlóan ahogy az /etc/host.conf fájl meghatározza, hogy milyen módon történjen a gépnév feloldása. Például a

```
hosts: files nis dns
```

sor meghatározza, hogy a gépnév feloldás függvény először a helyi /etc/hosts fájlt nézze, majd NIS feloldás kövesse, végül a körzetnév szolgáltatáson keresztül oldja fel (/etc/resolv.conf és named). Ennél a pontnál, ha nincs találat, hibával tér vissza. Ezt az fájlt minden felhasználó számára olvashatóvá kell tenni! További információt találsz erről az nsswitch.5, vagy az nsswitch.conf.5 kézikönyv oldalakban.

Egy NIS számára használható /etc/nsswitch.conf fájl:

```

#
# /etc/nsswitch.conf
#
# Egy példa Név Szolgáltatás Kapcsoló (Name Service Switch) beállítási
# fájl. Ezt a fájlt úgy kell rendezni, hogy a leginkább használt
# szolgáltatás kerüljön az elejére.
#
# A '[NOTFOUND=return]' bejegyzés azt jelenti, hogy egy bejegyzés
# keresése be kell, hogy fejeződjön, ha az előző bejegyzés keresése
# nem adott vissza semmit. Jegyezzük meg, hogy ha a keresés más
# okból hibás (mondjuk nem válaszol NIS szerver), akkor a keresés
# folytatódik a következő bejegyzéssel.
#
# Lehetséges bejegyzések:
#
# nisplus Használj NIS+ -t (NIS 3-as verzió)
# nis Használj NIS-t (NIS 2-es verzió), YP-nek is hívják
# dns Használj DNS-t (Domain Name Service: Körzet |Név Szolgáltatás)
# files Használd a helyi fájlokat
# db Használd a /var/db adatbázist
# [NOTFOUND=return] Hagyd abba a keresést, ha nem találsz
#

passwd:      compat
group:       compat
# libc5 esetén shadow: files nis -t kell használnod
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

```

A `passwd_compat`, `group_compat` és `shadow_compat` csak `glibc 2.x` alatt támogatott. Ha nincs `shadow` szabály az `/etc/nsswitch.conf` fájlban, a `glibc` a `passwd` szabályt fogja alkalmazni a feloldáshoz. Van még néhány feloldó modul a `glibc`-hez, mint például a `hesoid`. További információért olvasd el a `glibc` dokumentációját.

7.6. Árnyék jelszavak NIS-sel

A NIS feletti árnyék jelszavak használata mindig rossz ötlet. Elveszted az árnyék által biztosított biztonságot, és csak néhány Linux C könyvtár támogatja. Egy jó módszer a NIS feletti árnyék jelszavak használatának elkerülésére az, hogy csak a helyi felhasználók esetén használj árnyékjelszót az `/etc/shadow` fájlban. Vedd ki a NIS felhasználó bejegyzéseket az árnyék adatbázisból, és tedd vissza a jelszót a `passwd` fájlba. Így tehát használhatod az árnyék jelszót a root bejelentkezéshez, és a hagyományos `passwd`-t a NIS felhasználóhoz. Ennek a módszernek megvan az az előnye, hogy minden NIS kliens esetén működni fog.

7.6.1. Linux

Az egyetlen Linux libc, amely támogatja az árnyék jelszavak NIS feletti használatát a GNU C 2.x könyvtár. A Linux libc5-ben nincs ehhez támogatás. A Linux libc5 engedélyezett NYS-sel lefordítva tartalmaz némi kódot hozzá. Azonban ez a kód néhány esetben hibásan működik, és nem működik minden árnyék bejegyzéssel helyesen.

7.6.2. Solaris

A Solaris nem támogatja a NIS feletti árnyék jelszavakat.

7.6.3. PAM

A Linux-PAM 0.75 és újabb verzói támogatják a NIS feletti árnyék jelszavakat, amennyiben `pam_unix.so` modult használsz, vagy telepíted a `pam_unix2.so` modult. Régi rendszereknél (például RedHat 5.x), melyek még a `pam_pwdb/libpwdb`-t használják, meg kell változtatnod az `/etc/pam.d/*` bejegyzéseket. Cseréld ki az `összed pam_pwdb` szabályt a `pam_unix_*` modulokban.

Az `/etc/pam.d/login` fájl például így néz ki:

```

#%PAM-1.0
auth    requisite    pam_unix2.so          nullok #set_secrcp
auth    required     pam_securetty.so
auth    required     pam_nologin.so
auth    required     pam_env.so
auth    required     pam_mail.so
account required     pam_unix2.so
password required     pam_pwcheck.so       nullok
password required     pam_unix2.so         nullok use_first_pass use_authok
session required     pam_unix2.so         none # debug or trace
session required     pam_limits.so

```

8. Mire van szükség a NIS+ beállításához?

8.1. Szoftver

A Linux NIS+ kliens kódot a GNU C 2-es könyvtárhoz fejlesztették ki. Vagy Linux libc5-höz is egy változat, hiszen a legtöbb kereskedelmi alkalmazást ehhez a könyvtárhoz fordítják és nem tudod őket glibc használatához újrafordítani. Problémák vannak a libc5 és NIS együttes használatában: statikus programokat nem lehet ehhez fordítani, és az e könyvtárhoz fordított programok nem fognak más libc5 változatokkal működni.

Ha olyan disztribúció van, amelyikben nincs 2.11-es vagy újabb glibc, akkor be kell szerezned egyet, vagy frissítened kell a rendszered glibc-jét. Alaprendszerként, szükséged lesz egy glibc alapú disztribúcióra, mint például a Debian, RedHat, vagy SuSE Linux.

A NIS+ kliens szoftvert megszerezheted az alábbi címekről:

Hely	Könyvtár	Fájl neve
ftp.gnu.org	/pub/gnu/glibc	glibc-2.3.2.tar.gz, glibc-linuxthreads-2.3.2.tar.gz
ftp.kernel.org	/pub/linux/utils/net/NIS+	nis-utils-1.4.1.tar.gz

Nézz körül a <http://www.linux-nis.org/nisplus/> webhelyen további információkért, és a legfrissebb forrásokért.

8.2. NIS+ kliens beállítása

FONTOS: NIS+ kliens beállításához olvasd el a Solaris NIS+ dokumentációkat, abban van leírva mit kell tenni a szerver oldalán! Ez a dokumentáció csak a kliens oldali teendőket írja le!

Miután feltelepítetted az új libc-t és NIS-eszközöket, elkészítheted az új kliens megbízólevelét (credential) a NIS+ szerveren. Győződj meg róla, hogy a portmap fut. Ezután ellenőrizd, hogy a Linux géped ideje megegyezik a NIS+ szerverével. Biztonságos RPC használatakor legfeljebb 3 perces ablak áll rendelkezésre, amíg a megbízások érvényesek. Jó ötlet minden gépen az xntpd futtatása. Mindezek után futtasd a következőket:

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

az indítófájlok beállításához. Olvasd el az nisinit kézikönyv oldalt a többi lehetőségért. Győződj meg róla, hogy a körzetnév minden újraindítás után beállítódik-e. Ha nem tudod, hogy mi a hálózatod NIS+ körzetneve, kérdezd meg a redszergazdát/hálózati adminisztrátort.

Most célszerű megváltoztatnod az /etc/nsswitch.conf fájlt. Bizonyosodj meg arról, hogy a publickey szolgáltatás utáni egyetlen szolgáltatás a nisplus ("publickey: nisplus"), és semmi más!

Ezután indítsd el a keyserv-et, és nézd meg, hogy minden induláskor ez az első elinduló démon a portmap után. Futtasd a

```
keylogin -r
```

parancsot a rendszered root titkos kulcsának eltárolásához. (Remélem hozzáadtad az új gép nyilvános kulcsát a NIS+ szerveren?).

A `niscat passwd.org_dir` parancsnak ekkor már meg kell mutatnia a passwd adatbázisod összes bejegyzését.

8.3. NIS+, keylogin, bejelentkezés és PAM

Amikor a felhasználó bejelentkezik, meg kell adnia a titkos kulcsát a keyserv-nek. Ezt a "keylogin" parancs hívásával teszi meg. Az árnyék (shadow) csomagban lévő login megteszi ezt a felhasználónak, ha glibc-2.1-el volt lefordítva. A PAM alapú bejelentkezéshez fel kell telepíteni a pam_keylogin-1.2.tar.gz csomagot, és meg kell változtatni az `/etc/pam.d/login` fájlt úgy, hogy a pam_unix_auth-ot használja, ne a pwdb-t, ami nem támogatja a NIS+ -t. Például:

```

#%PAM-1.0
auth        required /lib/security/pam_securetty.so
auth        required /lib/security/pam_unix2.so          set_secrpc
auth        required /lib/security/pam_nologin.so
account     required /lib/security/pam_unix2.so
password    required /lib/security/pam_unix2.so
session     required /lib/security/pam_unix2.so

```

8.4. Az nsswitch.conf fájl

A Hálózati Szolgáltatások (Network Services) beállítási fájl (`/etc/nsswitch.conf`) megadja, hogy milyen sorrendben történjenek a kérés-feloldások, ha egy bizonyos információkérés történt, hasonlóan ahogyan az `/etc/host.conf` fájl meghatározza a gépnév feloldásának menetét. Például a

```
hosts: files nisplus dns
```

sor meghatározza, hogy a gépnév feloldó függvény először a helyi `/etc/hosts` fájlt nézze, amit egy NIS+ feloldás kövessen, végül a körzetrév szolgáltatást kérdezze (`/etc/resolv.conf` és `named`), ami után ha nincs találat, akkor hibával tér vissza.

Egy használható NIS+ `/etc/nsswitch.conf` fájl:

```

#
# /etc/nsswitch.conf
#
# Egy példa Név Szolgáltatás Kapcsoló (Name Service Switch) beállítási fájl.
# Ezt a fájlt úgy kell rendezni, hogy a legtöbbször használt szolgáltatás
# kerüljön az elejére.
#
# A '[NOTFOUND=return]' bejegyzés azt jelenti, hogy egy bejegyzés
# keresése fejeződjön be, ha az előző bejegyzés keresése
# nem adott vissza semmit. Jegyezzük meg, hogy ha a keresés más
# okból hibás (mondjuk nem válaszol NIS szerver), akkor a keresés
# folytatódik a következő bejegyzéssel.
#

```

```

# Lehetséges bejegyzések:
#
# nisplus Használj NIS+ -t (NIS 3-as verzió)
# nis Használj NIS-t (NIS 2-es verzió), YP-nek is hívják
# dns Használj DNS-t (Domain Name Service: Körzet Név Szolgáltatás)
# files Használd a helyi fájlokat
# db Használd a /var/db adatbázist
# [NOTFOUND=return] Hagyd abba a keresést, ha nem találsz
#

passwd:      compat
group:       compat
shadow:      compat

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

```

9. NIS szerver beállítása

9.1. Az ypserv szerver-program

Ez a dokumentáció csak az "ypserv" NIS szerver beállítását tartalmazza.

A NIS szerver szoftvert megtalálsz a

Hely	Könyvtár	Fájl neve
ftp.kernel.org	/pub/linux/utils/net/NIS	ypserv-2.9.tar.gz
ftp.kernel.org	/pub/linux/utils/net/NIS	ypserv-2.9.tar.bz2

helyen.

Bővebb információkat találsz még a <http://www.linux-nis.org/nis/> webhelyen.

A hagyományos NIS és a NYS szerver beállítása megegyezik.

Az **ypserv** és **makedbm** programok elkészítéséhez fordítsd le a szoftvert. Beállíthatod az ypserv-et securenets fájlok vagy tcp_wrapper-ek használatára.

Ha a szerveredet mesterként futtatsz, határozd meg, hogy melyik fájlokat kell NIS-en keresztül elérhetővé tenned, és add hozzá vagy vedd ki a megfelelő bejegyzéseket az "all" szabálynál a `/var/yp/Makefile` fájlban. Mindig célszerű megnézned, és megfelelően szerkeszteni az Opciókat (Options) a Makefile elején.

Nagy váltás volt az ypserv 1.1 és az 1.2 között. Az 1.2-es verzió óta az fájlkezelők cache-ben tárolódnak. Ez azt jelenti, hogy ha új map-eket készítesz, mindig a `-c` kapcsolóval kell meghívnod a makedbm-et. Győződj meg róla, hogy az ypserv 1.2-ből, vagy újabból származó `/var/yp/Makefile`-t használod, vagy add hozzá a `-c` kapcsolót a makedbm-hez a Makefile-ban. Ha ezt nem teszed meg, az ypserv nem fogja tovább használni a régi map-eket, és a frissítetteket sem.

Most átszerkesztheted a `/var/yp/securenets` és a `/etc/ypserv.conf` fájlokat. Bővebb információkért olvasd el az ypserv(8) és az ypserv.conf(5) kézikönyv oldalakat.

Bizonyosodj meg róla, hogy a portmapper (portmap(8)) fut, és indítsd el az **ypserv** szerveret. A

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

utasítás kimenete hasonló lesz ehhez:

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

A "version 1" sor lehet, hogy hiányzik, az ypserv verziójától függően, és attól függően, hogy milyen konfigurációs fájlt használsz. Csak akkor lényeges, ha régi SunOS 4.x-es klienseket használsz.

Most készítsük el a NIS (YP) adatbázist. A mesteren futtasd a

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

parancsot. A szolgán nézd meg, hogy működik-e az **ypwhich -m**. Mielőtt a

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

parancs kiadásával beüzemelned a gépet NIS szolgának, NIS kliensként kell beállítani

Nos, a szervered kész van és működik.

Ha nagyobb problémáid vannak, elindíthatod az **ypserv** és **ypbind** programokat nyomkövető üzemmódban is, különböző xterm-ekben. A nyomkövetés kimenetének mutatnia kell, hogy mi működik rosszul.

Ha map-et kell frissítened, futtasd a NIS mester szerveren a **make**-et a `/var/yp` könyvtárban. Ez frissíteni fogja a map-et, ha a forrásfájl frissebb, majd át is adja a szolga szervereknek is. Kérlek ne használj a map frissítéshez `/var/yp-et`.

Esetleg átszerkesztheted a root crontabját `*a szolga*` szerveren és hozzáadni a következő sorokat:

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

Ez biztosítani fogja, hogy a legtöbb NIS map frissüljön, még ha ki is maradt egy frissítés, ha a mester szerver frissítésekor a szolga le volt kapcsolva.

A későbbiekben bármikor hozzáadhatsz új szolgát. Először biztosítsd, hogy az új szolga szervernek legyen jogosultsága a NIS mester szerverhez kapcsolódni, majd futtasd a

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

programot az új szolgán. A mester szerveren add hozzá a `/var/yp/ypservers`-hez az új szolga szerver nevét és futtasd a **make**-et a `/var/yp` könyvtárban a map frissítéséhez.

Ha korlátozni szeretnéd a felhasználók hozzáférését a NIS szerveredhez, a NIS szerveredet kliensként is üzemeltetned kell úgy, hogy elindítod az `ypbind`-et, és hozzáadod az `/etc/passwd` jelszó fájlhoz `_félúton_` a plusz bejegyzéseket. A könyvtár függvények figyelmen kívül hagyják a hagyományos bejegyzéseket az első NIS bejegyzés után és a többi NIS-en keresztül szerzik meg. Így a NIS hozzáférés-szabályok karbantartottak. Például:

```
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
```

Bár a "tester" felhasználó létezik, a parancsértelmezője azonban az `/etc/NoShell`. `miquels`-nek rendes hozzáférése lesz.

Alternatívaként átszerkesztheted a `/var/yp/Makefile` fájlt és beállíthatod, hogy a NIS másik jelszó forrás fájlt használjon. Nagy rendszereken a NIS jelszó és csoport fájlok általában az `/etc/yp/` könyvtárban vannak. Ha a hagyományos eszközöket nem használhatók a `passwd`, `chfn`, `adduser` fájlokat adminisztrálására. Ehhez saját készítésű programokra lesz szükséged.

Habár az `yppasswd`, `ypchsh` és az `ypchfn` természetesen működni fog.

9.2. Az yps szerver program

Az "yps" NIS szerver beállításához tanulmányozd az előző fejezetet. Az "yps" szerver beállítása hasonló, `_de_` nem pontosan ugyanolyan, tehát légy óvatos, mielőtt megpróbárod az "ypserv" utasításait az "yps"-re alkalmazni! Az "yps"-t nem támogatja egyik szerző sem, és néhány biztonsági rést is tartalmaz. Tényleg nem kellene használnod!

Az "yps" NIS szerver szoftvert megtalálsz az alábbi címeken:

Hely	Könyvtár	Fájl neve
<code>ftp.lysator.liu.se</code>	<code>/pub/NYS/servers</code>	<code>yps-0.21.tar.gz</code>
<code>ftp.kernel.org</code>	<code>/pub/linux/utills/net/NIS</code>	<code>yps-0.21.tar.gz</code>

9.3. Az rpc.ypxfrd program

Az `rpc.ypxfrd`-t nagyon nagy NIS map fájlok esetén használjuk a mester és szolga NIS szerverek közötti adatátvitel gyorsítására. Ha egy NIS szolga szerver olyan üzenetet kap, hogy új map készült, elindítja az `ypxfr`-t, hogy letöltse azt. Az `ypxfr` elolvasa a mester szerver map-jét az `yp_all()` függvény segítségével. Ez a folyamat több percet is igénybe vehet, ha nagyon nagy map fájlokról van szó, amit az adatbázis könyvtárban kell tárolni.

Az `rpc.ypxfrd` szerver úgy gyorsítja az átvitel folyamatát, hogy a NIS szolga szervereknek engedélyezi, hogy egyszerűen lemásolják a szerver map fájlait, és ne kelljen újra felépíteniük a sajátjukat. Az `rpc.ypxfrd` RPC-alapú fájl átviteli protokollt használ, tehát nincs szükség új map építésére.

Az `rpc.ypxfrd` indítható az `inetd`-ből, azonban mivel nagyon lassan indul el, célszerű az `ypserv` segítségével indítani. Az `rpc.ypxfrd`-t csak a mester NIS szerveren kell elindítanod.

9.4. Az rpc.yppasswdd program

Amikor a felhasználók megváltoztatják a jelszavukat, a NIS jelszó adatbázis, és feltehetőleg az összes, ettől a NIS jelszó adatbázistól függő többi adatbázis frissítésre szorul. Az "rpc.yppasswdd" program egy olyan szerver, ami a jelszóváltozásokat kezeli, és gondoskodik arról, hogy a NIS információ helyesen frissüljön. Az `rpc.yppasswdd` már az `ypserv` része. Nincs szükséged régi, különálló `yppasswd-0.9.tar.gz`-re, vagy `yppasswd-0.10.tar.gz`-re, és nem is javallott a továbbiakban használatuk.

Az `rpc.yppasswdd` démon csak a mester NIS szerveren kell elindítanod. Alapértelmezés szerint a felhasználók nem változtathatják meg a teljes nevüket, illetve a parancsértelmezőjüket. Engedélyezheted ezek megváltoztatását a `-e chfn` vagy `-e chsh` kapcsolókkal.

Ha a jelszó vagy az árnyékfájlok nem az `/etc` könyvtárban vannak, a `-D` kapcsolót is használnod kell. Például ha minden forrásfájl az `/etc/yp` könyvtárba tettél, és szeretnéd engedélyezni a felhasználók számára, hogy megváltoztathassák a parancsértelmezőjüket, a következő paraméterekkel kell indítanod az `rpc.yppasswdd` démon:

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

vagy

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

Nincs más tennivaló, már csak meg kell győződnöd róla, hogy az `rpc.yppasswdd` ugyanazt az fájlt használja, mint a `/var/yp/Makefile`. A hibákat a `syslog` naplózza.

10. A NIS/NYS telepítésének ellenőrzése

Ha minden rendben (ahogy lennie kellene), néhány egyszerű utasítással ellenőrizheted a telepítést. Feltételezve, hogy például a jelszó fájlodat a NIS adja, a

```
% ypcat passwd
```

utasításnak vissza kell adnia a NIS jelszófájlod tartalmát. A

```
% ypmatch userid passwd
```

utasítás (ahol a `userid` egy találmra választott felhasználó azonosítója) vissza kell, hogy adja a felhasználó NIS jelszó fájlban lévő bejegyzését. Az `"ypcat"` és az `"ypmatch"` programokat a hagyományos NIS vagy NYS disztribúcióod tartalmazza.

Ha egy felhasználó nem tud bejelentkezni, indítsd el a következő programot a kliensen:

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

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

    if(argc != 2)
    {
        fprintf(stderr, "Használat: getwpmam felhasználónév\n");
        exit(1);
    }

    pwd=getpwnam(argv[1]);

    if(pwd != NULL)
    {
        printf("név.....: [%s]\n", pwd->pw_name);
        printf("jelszó...: [%s]\n", pwd->pw_passwd);
        printf("felh. id.: [%d]\n", pwd->pw_uid);
        printf("csoport id: [%d]\n", pwd->pw_gid);
        printf("gecos....: [%s]\n", pwd->pw_gecos);
    }
}
```

```

    printf("könyvtár.: [%s]\n",pwd->pw_dir);
    printf("shell....: [%s]\n",pwd->pw_shell);
}
else
    fprintf(stderr,"Az \"%s\" felhasználó nem található!\n",argv[1]);

exit(0);
}

```

Ezt a programot futtatva a felhasználó nevével, mint paraméterrel, kiírja mindazt az információt, amit a `getpwnam` függvény ad vissza erre a felhasználóra. Ennek meg kell mutatnia, hogy melyik bejegyzés hibás. A leggyakoribb probléma az, hogy a jelszó mező "*" -al felül lett írva.

A GNU C 2.1-es könyvtár (glibc 2.1) tartalmaz egy `getent` eszközt. Ezt használhatod a fenti program helyett egy ilyen rendszeren. Kipróbálhatod:

```
getent passwd
```

vagy

```
getent passwd login
```

11. NIS térképek készítése és karbantartása

11.1. Új NIS térkép létrehozása

Az első NIS térképek a

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

parancs futtatásával hozhatók létre. Ezt a NIS mester szerver létrehozásakor kell tenni. A "NIS szerver beállítása" fejezetben bővebben olvashatsz erről. Új térkép hozzáadása, illetve egy régi eltávolítása, a `/var/yp/Makefile` szerkesztésével lehetséges: meg kell változtatnod az `all:` kezdetű sort. Add hozzá vagy távolítsd el a szükséges/szükségtelen szabály nevét.

Ha eltávolítasz egy térkép bejegyzést, a hozzá tartozó fájlokat is törölnöd kell.

A változtatások után már csak a

```
% make -C /var/yp
```

parancsot kell futtatnod és elkészülnek a térképeid.

11.2. NIS térképek frissítése

Ha megváltoztatod a NIS térképek forrásadatait, (mondjuk egy új felhasználót veszel fel a `passwd` fájlba) akkor újra kell generálnod a NIS térképet is. Ezt egyszerűen a

```
% make -C /var/yp
```

parancs kiadásával érheted el. Ez az utasítás megnézi mely források változtak, elkészíti az új téképeket és tudatja az ypserv-vel a változásokat.

11.3. A térképájl bejegyzéseinek hossza

A NIS protokoll 1024 karakterre korlátozza egy-egy bejegyzés hosszát. Nem lehet tehát csak úgy megváltoztatni ezt az értéket, és újrafordítani a rendszert. Minden NIS v2-t használó rendszer 1024 byte-nál rövidebb kulcs és adatértékeket vár; ha hirtelen megnöveled a kliens és szerver YPMAXRECORD változójának méretét, megszakad az átjárhatóság a NIS-t használó rendszereid között. Ahhoz, hogy ez így működjön, el kellene menned minden szoftvergyártóhoz, akik rendszerei támogatják a NIS-t és rá kellene vened őket, hogy változtassák már meg az 1024 byte-os méretet, méghozzá egyszerre, és egyformán... elég csekély a valószínűsége annak, hogy eredményes lesz az utad.

A glibc 2.1-től kezdve a glibc NIS alkalmazásain ez a korlát megszűnt. Vagyis lehetségessé vált, hogy Linux rendszereken használhassunk hosszabb bejegyzéseket is, de csak ha nincs más típusú kliens, vagy szerver a rendszerben.

Ahhoz, hogy hosszabb bejegyzéseket használhass a NIS térképeken, hozzá kell adnod a `/var/yp/Makefile`-ban levő `makedbm` bejegyzéshez a `--no-limit-check` opciót.

Az eredmény valami ilyesmi:

```
DBLOAD = $(YPBINDIR)/makedbm -c -m '$(YPBINDIR)/yphelper --hostname' --no-limit-check
```

FIGYELEM! Ez törést okoz a NIS protokollban, és bár a Linux támogatja, nem minden Linux alatt futó program tud a változásokkal együtt dolgozni.

Van egy másik útja is a probléma megoldásának. Ken Cameron ötletéből ered és a `/etc/group` fájl bejegyzéseit érinti:

1. A bejegyzést több sorban helyezzük el úgy, hogy minden csoport egymástól kissé eltérő nevekkel szerepeljen.
2. A GID maradjon ugyanaz minden csoportnál
3. Legyen az első bejegyzés a jó csoportnév és GID
(Én nem teszek felhasználónevet ide)

Amikor aztán a program felhasználó szerint haladva elolvassa a GID-et, majd visszafelé haladva megáll az első egyező GID-nél és beolvassa a hozzá tartozó felhasználónevet. Ronda, de működik!

12. Túlélőcsomag újraindítás esetére

Ha egyszer beállítottad és működőképpé tetted a NIS rendszered, mind a kliens, mind pedig a szerver oldalról, meg kell győződnöd arról is, hogy ez az állapot fennmarad-e a rendszer újraindításakor is.

Két elkülönülő dolgot kell ellenőrizned: Az indító szkript meglétét, és a NIS domainnév helyes tárolását.

12.1. A NIS indító (init) szkript

A Linux disztribúció szerinti init-szkript könyvtárban (leggyakrabban: `/etc/init.d`, `/etc/rc.d/init.d`, `/sbin/init.d`) ellenőrizd, hogy megvan-e a NIS indításához szükséges szkript. Általában `ypbind` vagy `ypclient` néven találod meg.

12.2. NIS domainnév

Talán az egyik legfontosabb kérdés, ami néhányunknál felmerülhet a NIS-sel kapcsolatban, hogy a NIS domain újraindítás után elérhető-e vagy sem. Solaris 2.x rendszereknél a NIS domain a `taz`

```
/etc/defaultdomain
```

fájlban kell tárolni. A legtöbb Linux disztribúció nem használja ezt a fájlt.

12.3. Linux-disztribúció specifikus megjegyzések

Mostanáig a következő információk állnak rendelkezésre a Linux disztribúciók NIS domainnév tárolásával kapcsolatban:

12.3.1. Caldera 2.x

A Caldera az `/etc/nis.conf` fájlt használja, formátuma a normál `/etc/yp.conf`-val megegyező.

12.3.2. Debian

A Debian a Sun-os `/etc/defaultdomain`-t használja.

12.3.3. Red Hat Linux 6.x and 7.x, 8x és 9

Az `/etc/sysconfig/network` fájlban található **NISDOMAIN** változóval állíthatjuk be a körzetnevet.

12.3.4. SuSE Linux 6.x and 7.x

Az `/etc/rc.config` fájlban az **YP_DOMAINNAME** változót módosíthatod, majd futtatni kell a **SuSEconfig**-ot.

12.3.5. SuSE Linux 8.x és későbbi

A 8.0-tól kezdve a SuSE is a SUN-os rendszert követi, vagyis `/etc/defaultdomain`.

13. Jelszóváltás az rpasswd program segítségével

A NIS jelszó megváltoztatásának általános módja az **yppasswd** program meghívása, ez néhány rendszeren ez mindössze a **passwd** program alias neve. Ez a parancs az **yppasswd** protokollt használja, emellett szükséges az

rpc.yppasswdd folyamatnak futnia a NIS master szerveren. A protokoll eléggé idejétmúlt, a régi jelszót sima szöveggként küldi át a hálózaton. Ez nem problémás, amennyiben a jelszó sikeresen megváltozik. Abban az esetben a régi jelszót felváltja egy új. De ha a jelszóváltás sikertelen, úgy egy támadó használhatja a helyes jelszót, és beléphet a felhasználó nevében. Még rosszabb, ha a rendszeradminisztrátor változtatja meg egy másik felhasználó jelszavát, ekkor a NIS master szerver root jelszava továbbítódik sima szöveggként a hálózaton. És az ebben az esetben nem fog megváltozni.

Egyfajta megoldás az, ha nem az yppasswd programot használod jelszóváltásra. Ehelyett jól használható az **rpasswd** parancs a `pwdutils` csomagból.

Webhely	Könyvtár	Fájl neve
ftp.kernel.org	/pub/linux/utils/net/NIS	pwdutils-2.3.tar.gz
ftp.suse.com	/pub/people/kukuk/pam/pam_pwcheck	pam_pwcheck-2.2.tar.bz2
ftp.suse.com	/pub/people/kukuk/pam/pam_unix2	pam_unix2-1.16.tar.bz2

Az **rpasswd** biztonságos SSL kapcsolaton keresztül megváltoztatja egy felhasználó jelszavát egy távoli szerveren. Egy átlagos felhasználó csak a saját jelszavát változtathatja meg, ha az adminisztrátor jelszavát is tudja, akkor pedig bárkiét, ha meghívja az **rpasswd** programot az `-a` kapcsolóval.

13.1. A szerver beállítása

A szervernek az elsősorban tanúsítványra van szüksége, annak alapértelmezett fájlneve az `/etc/rpasswd.pem`. Ezt a következő paranccsal hozhatod létre:

```
openssl req -new -x509 -nodes -days 730 -out /etc/rpasswd.pem -keyout /etc/rpasswd.pem
```

Egy PAM beállítófájlra is szüksége van az **rpasswd** programnak. Ha a NIS felhasználói jelszavak az `/etc/passwd` fájlban vannak, a következő példa jó kiindulási alapot nyújt a beállításhoz:

```
##PAM-1.0
auth      required      pam_unix2.so
account   required      pam_unix2.so
password  required      pam_pwcheck.so
password  required      pam_unix2.so   use_first_pass use_authtok
password  required      pam_make.so    /var/yp
session   required      pam_unix2.so
```

Ha a NIS jelszótérképek forrása másutt tárolódik (például `/etc/yp`), úgy a `pam_unix2 nisdir` kapcsolója használható a forrásfájl megkeresésére:

```
##PAM-1.0
auth      required      pam_unix2.so
account   required      pam_unix2.so
password  required      pam_pwcheck.so nisdir=/etc/yp
password  required      pam_unix2.so   nisdir=/etc/yp use_first_pass use_authtok
password  required      pam_make.so    /var/yp
```

```
session required      pam_unix2.so
```

Most indítsd el az **rpasswd** démonot a NIS mester szerveren.

A PAM modulokban történt jelszóbeállítás után az **rpasswd** is használható jelszováltásra NIS+, LDAP vagy más, a PAM modul által támogatott szolgáltatásokhoz.

13.2. A kliens beállítása

Minden egyes kliensen csak az `/etc/rpasswd.conf` fájlban vannak a szükséges szerverek nevei. Ha a szerver nem az alapértelmezett portot használja, akkor azt be kell állítani:

```
# az rpasswd az master.example.com gépen fut
server master.example.com
# Port 774 az alapértelmezett
port 774
```

14. Általános, valamint NIS problémák elhárítása

Íme néhány általános, felhasználók által jelzett probléma:

1. A 4.5.19-eshez szállított programkönyvtárak hibásak. A NIS nem működik vele.
2. Ha a 4.5.19-es könyvtárakat 4.5.24-re frissíted, akkor a su program megszakad. Meg kell szerezned a su programot az 1.2.0-s slackware-ből. Minő véletlen, hogy pont ugyaninnen szerezheted be a frissített programkönyvtárakat is.
3. Amikor egy NIS szerveret lekapcsolnak, majd újra bekapcsolnak, az ypbind a következő üzenettel indul:

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

és a bejelentkezéseket megtagadja azoknak, akik a NIS adatbázisban regisztrálva vannak. Megpróbálkozhatsz root felhasználóként bejelentkezni, és legyilkolni az ypbind-et, majd újra elindítani. Egy 3.3-as, vagy újabb verziójú ypbind frissítés is segíthet.

4. Miután a libc-t 5.4.20-asnál magasabb verziósámra frissítetted, az YP eszközök nem működnek tovább. 1.2-es, vagy frissebb yp-tools-ra lesz szükséged az 5.4.21-es, vagy frissebb libc-hez és a glibc 2.x-hez. Korábbi libc verziójú libc-hez 2.2-es yp-clients kell. Az yp- tools 2.x-nek minden programkönyvtárral működnie kell.
5. A 5.4.21 - 5.4.35 számú libc-ben az yp_maplist hibás, 5.4.36-es, vagy frissebb változatra van szükséged, vagy néhány YP program, mint például az ypwhich segfault hibával leáll.
6. A libc 5 hagyományos NIS-el nem támogatja a NIS feletti árnyék jelszavakat. libc5+NYS-re vagy glibc 2.x-re van szükséged.
7. Az ypcat shadow nem mutatja a shadow map-et. Ez így helyes, az árnyék térkép neve shadow.byname, nem shadow.

8. A Solaris nem mindig használ privilegizált kapukat, tehát ne használj password mangling-et ha Solaris kliensed is van.

15. Gyakran Ismételt Kérdések

Mostanra a legtöbb kérdésedre válasz kellett kapnod. Ha még mindig lenne megválaszolatlan kérdésed, küldj egy üzenetet a

`comp.os.linux.networking`

hírcsoportba.