NIS Debian HOWTO

Miquels, miquels@cistron.nl v3.2.1-3, 2 Mar 1998

이범석shinsuk@ai-cse.sch.ac.kr 12 Dec 1998

이 HOWTO는 다음에 대해 설명합니다.

목 차

제 1 절 지역 NIS 클라이언트를 어떻게 설정하는가

1. netbase, netstd, nis 패키지를 설치합니다.
2. 설치 과정에서 NIS domainname을 묻습니다. 이것은 NIS를 사용할 시스템들의 그룹을 나타내는 이름으로 hostname과는 다릅니다.
3. 만약 NIS 서버가 지역 네트워크 안에 있지 않으면 몇 가지 미세조정이 필요합니다. ypbind 프로세스는 /etc/yp.conf 라는 설정 파일을 가지고 있습니다. 여기에 NIS 서버의 이름을 적습니다. - 더 자세한 정보는 ypbind(8) 매뉴얼을 보십시오.
4. NIS를 시작합니다.

```
/etc/init.d/nis stop
/etc/init.d/nis start
```

제 2 절 NIS를 통해 자원을 어떻게 이용하는가

1. FOR libc6

   /etc/nsswitch.conf 파일의 passwd, group, shadow, netgroup 엔트리를 다음과 같이 바꿉니다.

```
passwd:   compat
group:    compat
shadow:   compat

netgroup: nis
```

libc6은 파일로부터 netgroup 정보를 읽는데 몇 가지 문제를 가지고 있습니다. 그러니 netgroup 엔트리에 "db"나 "files"를 쓰지 마십시오. 모든 netgroup 정보는 NIS 서버를 통해 얻어지게 됩니다.

2. USERS: NIS clients의 /etc/passwd에 다음 줄을 추가합니다.

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

사용자(user)의 포함/차단을 위해 +와 - 기호를 사용할 수 있습니다. 사용자 guest를 제외하려면 /etc/passwd 파일에 -guest를 추가합니다. 사용자 linux가 다른 쉘(e.g. ksg)을 사용하길 원한다면 /etc/passwd에 +linux::::::/bin/ksh를 추가해 주면 됩니다. 변경을 원하지 않는 필드는 빈채로 놔둡니다.

예로, miquels, dth, ed만 로그인을 허락하고 다른 사용자의 계정 정보만을 유지하려면:

```
+miguels::::::
+ed::::::
+dth::::::
+:*::::::/etc/NoShell
```

예에서와 같이 리눅스에서는 패스워드 필드도 override할 수 있습니다.

3. GROUPS: /etc/group에 다음 줄을 추가합니다.

```
+:::
```

4. HOSTS:

보통 NIS를 통해 host lookup은 하지 않고 DNS를 사용합니다. 꼭 NIS를 통해 해야 한다면 여기서 하십시오.

- For libc5 applications: NIS 서버의 NIS host 맵을 사용하려면 /etc/host.conf를 수정해야 합니다. 다음과 같이 order 줄에 nis라는 단어를 추가합니다:

```
order hosts,nis
multi on
```

- For libc6 applications: /etc/nsswitch.conf의 hosts 엔트리를 수정합니다:

```
hosts: nis files
```

제 3 절 NIS master 서버를 어떻게 설정하는가

1. nis 패키지를 설치합니다. RPC daemon들(rpc.portmap)을 설치하기 위해 netbase와 netstd도 설치해야 합니다.

2. master, slave 구분없이 NIS 서버로 사용될 모든 시스템의 이름이 /etc/hosts 파일내에 있어야 합니다. 각 IP 주소 뒤에 첫 번째 hostname이 FQDN(Fully Qualified Domain Name)이어야 하고, 그에 이어 domainname을 제외한 hostname만을 기입합니다. 예를 들면:

```
192.168.88.10    troi.cistron.nl troi
```

NIS는 DNS를 사용하지 않기 때문에 NIS server 내의 NIS host file(보통 /etc/hosts)도 이 설정을 해야 합니다.

3. /etc/defaultdomain에 NIS domain을 설정합니다. NIS domain은 NIS를 사용하는 시스템들의 그룹을 나타내는 이름으로 hostname과는 다릅니다. 이것은 보통 DNS domainname을 이것에도 사용합니다.

   이것은 많은 사람들에 의해 보안 위험을 지적되고 있습니다. domainname을 아는 것만으로 원격지에서 NIS server에 query를 보내고 NIS 맵들을 받을 가능성이 있기 때문입니다. 이것을 막기위해 모호한 domainname을 선택해서는 안됩니다. 단지 지역 네트워크 이외에서 NIS 서버에 접근할 수 없도록 하면 됩니다.

4. /etc/init.d/nis 파일 내의 ypserv를 master로 (ypserv=master) 설정합니다.

5. 위에서 말한 것과 같이, 지역 네트워크 번호를 /etc/ypserv.securenets에 추가합니다. 기본값으로 모든 시스템이 NIS server에 접근할 수 있도록 되어 있지만 이렇게 하지 않는 것을 권장합니다. 보안의 강화를 위해 /etc/ypserv.conf 파일을 수정하여 password를 나오지 않도록(mangle)할 수 있습니다. (네트워크 내에 데비안이 아닌 slave server들이 있을 때에는 이것을 사용해서는 안됩니다.)

6. "/usr/lib/yp/ypinit -m"을 입력하여 서버를 설정합니다.

7. 다음을 입력하여 서버를 시작합니다.

   ```
   /etc/init.d/nis stop
   /etc/init.d/nis start
   ```

   서버(ypserv)와 패스워드 데몬(yppasswdd)이 시작됩니다.

   NIS 서버에의 접근을 제한하기를 원하면 NIS 서버를 클라이언트와 마찬가지로 ypbind를 실행하고 /etc/passwd 파일의 중간에 plus-entries를 추가하여 설정합니다. 라이브러리 함수는 첫 번째 NIS entry 후의 모든 normal entries를 무시하고, 나머지를 NIS를 통해 얻게 됩니다. 이 방법은 NIS에의 접근 규칙을 관리하는 방법입니다.

   예:

   ```
   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 Smooreburg:/home/miquels:/bin/zsh
   ```

   사용자 tester는 존재하지만, 쉘이 /etc/NoShell로 지정되어 있고, miguels는 보통 접근을 갖게 됩니다.

   다른 방법으로, /var/yp/Makefile을 수정하고 NIS가 다른 패스워드 파일을 사용하도록 설정할 수 있습니다. 큰 시스템에서는, NIS 패스워드와 그룹파일을 일반적으로 /var/yp/ypfiles/에 저장합니다. 이것을 사용할 경우엔 패스워드 파일을 관리하는 "passwd", "chfn", "adduser"등의 일반 관리 도구를 더 이상 사용할 수 없게 되어 특별한 도구를 직접 만들어 사용해야 합니다.

   그러나 yppasswd, ypchsh, ypchfn은 yppasswdd를 -D 옵션으로 NIS 패스워드와 쉐도우의 위치를 지정하면 사용할 수 있습니다. 이 유틸리티들과 yppasswdd 데몬의 데비안 버전은 비표준 확장을 가지

고 있습니다. "Root"는 root 패스워드를 사용하여 다른 사람들의 패스워드, finger 정보와 쉘을 변경할 수 있습니다.

NIS 패스워드 파일을 직접 수정하거나 표준 /etc/passwd 파일을 사용한다면, NIS 소스 파일이 이 중의 하나라도 변경된 후 /var/yp 디렉토리에서 make를 실행시켜 NIS 맵을 갱신해야 하는 것을 기억하십시오. 이것은 cron으로 밤에 수행시켜 최신의 NIS 맵을 유지하도록 하는 것이 적당합니다.

제 4 절 SHADOW PASSWORDS

리눅스 libc5는 쉐도우 NIS 맵을 지원하지 않습니다. libc5에 종속적인 응용 프로그램을 사용할 경우엔 쉐도우 NIS 맵을 사용해서는 안됩니다. 대신 다음의 방법들을 사용할 수 있습니다.

1. SHADOW-LIKE SECURITY NIS가 패스워드를 찾는 것을 "mangling"하여 쉐도우와 비슷한 보안을 제공할 수 있습니다. "ypserv.conf" 맨페이지와 /etc/ypserv.conf의 주석을 읽어보십시오.

2. REAL SHADOW SUPPORT libc6은 NIS 내에 쉐도우 지원이 포함되어 있습니다. 이것은 당신이 원하는 것과 같이 동작할 것입니다; NIS 서버로부터 쉐도우를 받아 사용하기만 하면 됩니다. 쉐도우 맵은 makedbm에 옵션 "-s"(secure)를 주면 만들어 집니다. 이것은 현재의 모든 /var/yp/Makefile내에서 자동으로 수행됩니다. 주)쉐도우 패스워드를 사용하고 있다면 2.2와 같은 "plus" entries를 /etc/passwd와 /etc/shadow 모두에 추가시킬 필요가 있습니다. 올바른 형태로 추가하십시오; passwd와 shadow파일은 다른 필드들을 가지고 있습니다.

제 5 절 HOW TO SETUP A NIS SLAVE SERVER

1. 먼저, 시스템을 NIS 클라이언트로 설정하십시오(1을 보십시오).

2. 이어서 위에 설명한데로 3.1부터 3.5까지 설정하되, 3.4에서 /etc/init.d/nis 파일내의 ypserv를 slave(ypserv=slave)로 설정하십시오.

3. 데몬을 실행하고 초기화하십시오.

```
/etc/init.d/nis stop
/etc/init.d/nis start
/usr/lib/yp/ypinit -s <주 NIS 서버 이름>
```

4. 이제 주 NIS 서버에 종 NIS 서버 지원을 설정합니다. 먼저 주 NIS 서버에 있는 NIS Makefile을 조정하여 앞으로의 모든 갱신된 정보를 자동으로 종 NIS 서버에 전달하도록 합니다. /var/yp/Makefile내의 NOPUSH 변수를 다음과 같이 설정하십시오.

```
NOPUSH="false"
```

이제 주 서버는 "/usr/lib/yp/ypinit -m" 명령 실행으로 종 서버들의 정보를 전달합니다. 종 서버들의 이름을 입력하십시오. 맵을 다시 만들어 종 서버로 자료를 전달합니다.

5. 종 서버의 루트 crontab에 다음을 추가합니다. (crontab -e)

```
20 *     * * * /usr/lib/yp/ypxfr_1perhour
40 5     * * * /usr/lib/yp/ypxfr_1perday
55 6, 18 * * * /usr/lib/yp/ypxfr_2perday
```

이것은 모든 NIS 맵들이 최신 정보로 갱신되도록 하며, 정보 갱신시 종 서버의 다운으로 빠진 정보도 갱신됩니다.