

NIS - informacje ogólne

Położenie: (nie dotyczy)

© Imagine Studio 2005, <http://myGentoo.tk>

NIS (*Network Information Service*), znany także jako *Yellow Pages*, opiera się na protokole RPC2 (NIS+ obsługuje szyfrowane RPC3) i może być serwerem haseł (*/etc/passwd*), grup (*/etc/group*), ale także np. pliku */etc/hosts*. To, jakie informacje (pliki) NIS ma serwować, określamy w */var/yp/Makefile*.

Bezpieczeństwo NIS

Każdy użytkownik sieci LAN może uzyskać zawartość pliku */etc/passwd* z głównego serwera NIS (polecenie **ypcat passwd**). Następnie za pomocą programów crackerskich oraz słownika może próbować złamać hasło (jeśli było banalne).

Hasła w */etc/shadow* zostały wymyślone po to, aby zwykli użytkownicy nie mieli dostępu do zaszyfrowanej postaci haseł (rw-----). Ale gdy udostępnimy mapy *shadow*, to użytkownicy będą mieć dostęp do zawartości tego pliku (teoretycznie, w praktyce raczej nie). Lepiej więc nie budować map *shadow*. Na kliencie powinno być tylko konto roota, natomiast wszystkie inne konta użytkowników na serwerze. Aby pozwolić na korzystanie z NIS tylko komputerom z sieci lokalnej, należy uczynić następujące wpisy:

ypserv: 192.168.0. (w pliku */etc/hosts.allow*)

ypserv: ALL (w pliku */etc/hosts.deny*)

Odpowiednie wpisy należy także poczynić w pliku */var/yp/securenets.default* (lub */etc/ypserv.securenets*).

Konfiguracja serwera NIS

Na serwerze musi być zainstalowany pakiet **ypserv** (obecnie w jego skład wchodzi także program *rpc.ypxfrd*, który służy do przyspieszania przesyłu bardzo dużych map z serwera *master* na *slave* oraz program *rpc.yppasswdd*, który jest serwerem odpowiedzialnym za zmiany haseł i uaktualnianie baz danych NIS). Operacje:

- **# domainname imagine** (utworzenie nazwy domeny NIS)
- Sprawdzić czy plik */etc/nisdomainname* zawiera wpis "imagine" (tylko w *Gentoo*).
- W pliku */etc/conf.d/ypserv* dodać wpis: *YP_DOMAIN=imagine*. (W innych dystrybucjach, np. *Mandrake* lub *Red Hat*, wpisu dokonuje się w pliku */etc/sysconfig/network* i ma on postać: *NISDOMAIN="imagine"*).
- Skonfigurować plik */var/yp/Makefile* (określić m. in. które pliki ma serwować NIS).
- Skonfigurować plik */etc/ypserv.conf* (konfiguracja serwera NIS).
- Skonfigurować plik */var/yp/securenets.default* określający, które komputery będą mieć dostęp do serwera NIS (w innych dystrybucjach może to być */etc/securenets* lub *etc/ypserv.securenets*).
- Uruchomić demony: *network*, *portmap*, *ypserv*, *rpc.yppasswdd*.
- **# rc-update add portmap default** (ustawienie automatycznego uruchamiania demonów)
- **# rc-update add ypserv default**
- **# rc-update add rpc.yppasswdd default**
- Zrestartować komputer (czasami ten krok jest ważny, inaczej występują problemy).
- **# /usr/lib/yp/ypinit -m** (ustalamy na ilu komputerach będzie działał serwer NIS; innymi słowy czy będą zapasowe serwery NIS)
- **# cd /var/yp**
- **# make** (tworzymy tzw. mapy udostępnionych przez NIS plików)

Uwaga: Jeśli zmieniamy zawartość udostępnionych plików (np. zmieniamy hasło, dodajemy wpis do */etc/hosts* lub dodajemy użytkownika), musimy za każdym razem powtórzyć dwa ostatnie kroki.

Konfiguracja klienta NIS

Na kliencie muszą być zainstalowane dwa pakiety:

- **ypbind**
- **yp-tools** (który zawiera m. in. klienta *yppasswd*)

Pliki konfiguracyjne klienta to:

- */etc/nsswitch.conf* (*Name Service Switch*)
- */etc/yp.conf*

W lokalnym pliku */etc/passwd* powinien znajdować się tylko *root* (ewentualnie *anonim* jako konto awaryjne), natomiast wszyscy inni użytkownicy, na serwerze NIS.

Procedura:

- # **domainname imagine**
- Dodać do pliku `/etc/sysconfig/network` wpis: `NISDOMAIN="imagine"` (tylko w *Mandrake* i *RedHat*).
- Dodać do pliku `/etc/hosts` wpis: `192.168.0.1 ypserver`.
- Skonfigurować plik `/etc/yp.conf`.
- Skonfigurować plik `/etc/nsswitch.conf`. (Uwaga: Jeśli opcja `passwd` zostanie ustawiona jako `passwd=nisplus`, nie będzie możliwe logowanie w ogóle; jeśli `passwd=nisplus nis`, wtedy możliwe będzie logowanie tylko użytkowników zwykłych, nie `roota`, i tylko w trybie tekstowym, bowiem mapa haseł `roota` nie jest budowana w NIS! Należy także zwrócić uwagę, że plik ten nie należy tylko do NIS i jest niezbędny do działania systemu w ogóle).
- Uruchomić demony i ustawić, aby uruchamiały się przy starcie: `network`, `portmap`, `ypbind`.
- Restart maszyny (niby bezsensowne, ale czasami pomaga przy różnych problemach)
- # **ypcat passwd** (testujemy działanie klienta; pokazuje zawartość zdalnego pliku `/etc/passwd`);
- # **ypcat group** (pokazuje zdalny plik `/etc/group`)
- # **ypcat hosts** (pokazuje zdalny plik `/etc/hosts`)
- # **ypmatch użytkownik passwd** (pokazuje wpis dotyczący wybranego użytkownika ze zdalnego pliku `/etc/passwd`)
- # **ypcat shadow** (nie powinien tego pokazywać!)

Istnieje także możliwość zmiany haseł w NIS przez każdego użytkownika zdalnego systemu za pomocą komendy:

yppasswd użytkownik

Hasło jest wtedy zmieniane zarówno w mapach NIS, jak i `/etc/passwd` na serwerze.

W niektórych manualach jest także zalecane dodawanie wpisów (na klientach NIS):

+ `użytkownik :::` (w pliku `/etc/passwd` oraz w pliku `/etc/shadow`)

+`:::` (w pliku `/etc/group`)

Ale być może dotyczy to jakis starszych wersji (w każdym razie u mnie to nie działa i w ogóle zdaje się nie mieć znaczenia).

Udostępnianie \$home

mount -t smb 192.168.0.1:/home /home

Teraz musimy dopisać polecenie montowania do skryptów startowych (najlepiej w pliku umieszczonym w `/etc/init.d` klienta i z dowiązaniem do niego w `/etc/rcS.d`)

Na serwerze *Samby* (ale tylko wtedy, gdy jest ona głównym kontrolorem domen) należy także ustawić opcję `nis homedir`. Można także użyć `automount` do montowania zdalnych `$homes`. (Zob. R. S h a r p e , T. P o t t e r , J. M o r r i s , *Samba dla każdego*, wyd. Helion, Gliwice 2002, s. 560)

Jeśli z różnych przyczyn nie chcemy udostępniać `$home`, możemy utworzyć je na zdalnym komputerze za pomocą `ssh`:

ssh root@klient

mkdir /home/katalog

chown -R użytkownik.grupa /home/katalog

chmod 0700 /home/katalog

Problemy

Problemy mogą wystąpić, gdy id użytkowników będzie różny w lokalnym `/etc/passwd` i w zdalnych mapach NIS. Należy to poprawić.

Pomoc

B. B a l l , D. P i t t s , *Red Hat Linux 7.1. Księga Eksperta*, wyd. Helion, Gliwice 2002, s. 452.

Ostatnia aktualizacja: 13 maj 2005.