

System operacyjny Linux

Paweł Rajba

pawel.rajba@continent.pl

<http://kursy24.eu/>

Zawartość modułu 13

- NFS
 - Wprowadzenie
 - Konfiguracja
 - Polecenie exportfs
 - Problemy
 - Podłączanie zasobów sieciowych
 - Dwie uwagi na koniec

Wprowadzenie

- Co to jest?
 - udostępnianie zasobów
 - model klient-serwer
- Uruchamianie demonów
 - /etc/init.d/nfsserver – włącza, wyłącza i sprawdza stan udostępniania zasobów
 - /etc/init.d/nfs – montuje/odmontowuje zasoby zdefiniowane w /etc/fstab
- Inne sprawdzenie, czy demon nfs działa
 - `# rpcinfo -p | grep nfs`

Konfiguracja

- Jest zawarta w pliku `/etc/exports`
- Każdy wiersz jest postaci
 - `/katalog host(uprawnienia) host(uprawnienia) ...`
- Nazwą hosta może być
 - nazwa komputera np. `zeus`, `zeus.olimp.gr`, `88.1.2.3`
 - grupa w domenie NIS np. `@grupa`
 - adresy sieci postaci `adres/maska` np. `192.168.0.0/255.255.255.0`, `10.5.5.0/24`

Konfiguracja

- Uprawnienia
 - ro, rw — tylko do odczytu, do odczytu i zapisu,
 - async — zwiększa wydajność, ale w przypadku niepoprawnego restartu serwera dane mogą ulec uszkodzeniu,
 - sync — zapewnia wyższy poziom bezpieczeństwa w transmisji danych,
 - root_squash — przy żądaniu użytkownika root zamienia jego identyfikator na identyfikator użytkownika anonimowego, czyli inaczej mówiąc odmawia dostępu użytkownikowi root,

Konfiguracja

- **Uprawnienia**
 - `no_root_squash` — pozwala na dostęp użytkownikowi `root` (przeciwnie do `root_squash`),
 - `all_squash` — przy zadaniu zamienia identyfikator każdego użytkownika na identyfikator użytkownika anonimowego (odmawia dostępu wszystkim użytkowników); ma zastosowanie przy dostępie do plików np. przez `ftp`,

Konfiguracja

- Uprawnienia
 - `squash_uids`, `squash_gids` — określamy uid i gid użytkowników, których identyfikatory będą wymieniane na identyfikator użytkownika anonimowego, np. `squash_uids=0-15,20,25-50` (określamy, komu odmawiamy),
 - `anonuid`, `anongid` — ustawia uid i gid użytkownika anonimowego; przydatne, jeśli publicznie udostępniamy zasoby i chcemy mieć wszystkie zadania od jednego użytkownika.

Konfiguracja

- Przykłady
 - / master(rw) trusty(rw,no_root_squash)
 - /projects proj*.local.domain(rw)
 - /usr *.local.domain(ro) @trusted(rw)
 - /home/joe
pc001(rw,all_squash,anonuid=150,anongid=100)
 - /pub (ro,insecure,all_squash)

Polecenie `exportfs`

- Polecenie służy do wyeksportowania zasobu (włączenie udostępniania)
- Jest ono wykorzystywane przez skrypt `/etc/init.d/nfsserver`
- Po edycji pliku `/etc/exports` należy
 - albo wykonać skrypt `nfsserver` z opcją `restart`
 - albo ręcznie za pomocą polecenia `exportfs` nanieść zmiany

Polecenie `exportfs`

- Składnia

- `# exportfs [-avi] [-o opcja, ...] [host:/sciezka ...]`
- `# exportfs -r [-v]`
- `# exportfs [-av] -u [host:/sciezka ...]`
- `# exportfs [-v]`

- Opcje

- `-a` — eksportuje lub wyłącza eksportowanie wszystkich katalogów,
- `-o` — podajemy opcje eksportowanego katalogu (takie jak w pliku `/etc/exports`),

Polecenie `exportfs`

- Opcje
 - `-i` — pomijana jest zawartosc pliku `/etc/exports`,
 - `-r` — ponowne wyeksportowanie; synchronizacja z plikiem `/etc/exports`,
 - `-u` — wyłączenie eksportowania katalogu(ów),
 - `-v` — wersja gadatliwa drukujaca dodatkowe komunikaty,
 - `host:/sciezka` — eksportujemy katalog `/sciezka` dla hosta `host`.

Polecenie `exportfs`

- Plik `/var/lib/nfs/xtab` zawiera informacje o aktualnie wyeksportowanych zasobach
- Przykłady
 - `# exportfs -a`
 - `# exportfs -ua`
 - `# exportfs -r`
 - `# exportfs -o async,no_root_squash komputer:/pub/`

Problemy

- Serwer NFS może zamieniać adres łączącego się klienta na pełną nazwę domenową, podczas gdy w pliku `/etc/exports` znajduje się tylko sama nazwa hosta; klientowi nie uda się wtedy podłączyć zasobu.
- Serwer NFS może nie eksportować katalogów, jeśli nie może zamienić IP hosta na nazwę. Może tak być, jeśli serwer DNS nie działa prawidłowo, lub brakuje odpowiedniego wpisu w pliku `/etc/hosts`.

Podłączanie zasobów sieciowych

- Służy do tego polecenie mount
 - Składnia
mount -t nfs [-o opcje] zdalny_host:zdalny_katalog
 lokalny_katalog
 - Opcje
 - rsize=n — wielkość bloku odczytu; domyślnie 1024, chociaż ustawienie tej wartości na 8192 zwykle zwiększa wydajność,
 - wsize=n — wielkość bloku zapisu; domyślnie 1024, chociaż ustawienie tej wartości na 8192 zwykle zwiększa wydajność,

Podłączanie zasobów sieciowych

- Polecenie mount
 - Opcje c.d.
 - bg — połączenie w tle; zalecane przy wpisie do pliku /etc/fstab,
 - fg — dualne do bg i domyslne,
 - soft — miękkie połączenie; oznacza, że jeśli jest ustawiony limit czasowy operacji, to przy nieudanych próbach połączenie zostanie przerwane z błędem,
 - hard — twarde połączenie; połączenie będzie powtarzane do skutku,
 - timeo=n — określa, po ilu sekundach będzie wysłane ponowne zadanie połączenia (timeout),

Podłączanie zasobów sieciowych

- Polecenie mount
 - Opcje c.d.
 - retrans=n — określa, ile razy timeout musi zostać przekroczony (ile razy będzie wysłane zadanie podłączenia), aby podłączanie zostało przerwane z błędem (musi być ustawiona opcja soft)
 - tcp, udp — nakazuje użycie protokołu tcp lub udp; domyślnie jest to udp i większość serwerów NFS nie obsługuje protokołu tcp.
- Znaczenie kombinacji opcji:
 - timeo, retrans, soft

Podłączanie zasobów sieciowych

- Polecenie mount, przykłady
 - # mount -t nfs oskarek:/pub /mnt/pub
 - # mount -t nfs -o soft,timeo=4,retrans=5 komp:/pub /mnt/pub
- Zamiast wykonywać polecenie mount ręcznie, warto rozważyć dokonanie odpowiednich wpisów do pliku /etc/fstab, np.
 - server:/usr/local/pub /pub nfs rsize=8192,wsiz=8192 0 0
- Przykład
 - udostępnienie /pub i zamontowanie tego katalogu do /mnt/pub (na tym samym komputerze)

Dwie uwagi na koniec

- Kwestia uprawnień
 - Uprawnienia są przydzielane na podstawie adresu IP
 - Zły może podszyć się pod inny komputer (jesli jest rootem)
 - Serwer NFS dokonuje uwierzytelnienia tylko przy pierwszym żądaniu
 - Zły mógłby przechwycić (podśluchać) lub sfalszować uchwyt i nielegalnie skorzystać z zasobów
- Automontowanie