

A NIS és az NFS (1. rész)

A központi felhasználókezelés két segédeszköze

Ekét hárombetűs, bűvös rövidítés több ponton is hasonlít egymásra. Az első és legszembevetőbb apróságon túl lépve (miszerint ugyanazzal a betűvel kezdődnek), észreveheted, hogy mind a kettő mögött ugyanaz a cég áll, név szerint a Sun. Továbbá mindkettő ugyanazt a célt hivatott szolgálni: adatokat oszthatasz meg velük a hálózaton. Ha már hallottál róluk, most biztosan morogsz, amiért együtt említem őket, hiszen úgy vélheted, semmi közük egymáshoz. Igaz: a két rendszernél az állományok megosztásának módja nem ugyanolyan, viszont remélem, e kétrészes cikk végére kiderül, milyen remekül kiegészíti egymást a két rendszer. Vágjunk bele!

Mire jó a NIS?

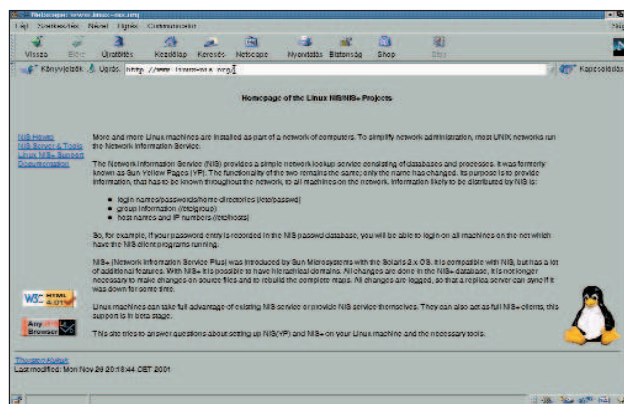
A NIS (Network Information Service) arra szolgál, hogy dbm formátumú adatbázisokat oszthass meg számítógépek között. Egy ilyen adatbázis rendkívül egyszerű felépítésű. Minden rekord egy kulcs- és egy értékpárból áll. Ezeket az adatbázisokat egyszerű szöveges állományokból készítheted a csomaghoz mellékelt segédprogrammal, a `makeidbm`-mel. Ahhoz, hogy eloszlassam a témát körülölgő homályt, ismertetek egy egyszerű példát. Tegyük fel, létezik egy linuxos háló, ahol azt szeretnéd, ha a felhasználókat központilag lehetne felügyelni. Örülnél, ha nem kellene az összes gép `/etc/passwd` állományát módosítanod, amennyiben egy új felhasználót fel szeretnél venni a rendszerbe. Ebben az esetben a NIS a megoldás. Csak a központi gépen veszed fel a `/etc/passwd`-be a felhasználókat, elkészítesz egy adatbázist, majd a NIS-sel megosztod. Ilyen egyszerű!

NIS, NIS+ és YP

Elnézést kérek mindenkitől a sok rövidítésért, tudom, hogy ezeket fel kell dolgozni, de egyedül ilyen „csúnya” szavakkal van tele az összes fellelhető leírás. Mivel ez a cikk nem lépheti túl a szabott keretet, kénytelen leszel hozzászokni ezekhez a „mozaikszavakhoz”. A NIS és az YP ugyanaz. Az YP (Yellow Pages – Sárga oldalak) a régebben használatos kifejezés. Mindaddig így hívták a NIS-t, amíg a British Telecom be nem jegyeztette az YP-t. A NIS+ pedig a NIS egy továbbfejlesztett változata. Minden megtalálható benne, amit a NIS-ből valaha is hiányolhattál: titkosított fájlátvitel, a faszervezeteknek köszönhetően a nagy hálózatok rugalmas és megbízható kezelése. Akad azonban egy kis gond is a NIS+-szal: kiszolgálórésze Linux alá még csak próbaváltozatban létezik, így közel sem mondható üzembiztosnak. Másrészt a NISHOWTO is azt ajánlja, hogy a borzalmas kiszolgálóoldali beállítását gyötrelmeitől lehetőleg kíméljük meg magunkat, és használjunk NIS-t, ahol csak lehet.

Az RPC

Ha még nem barátkoztál meg a `portmap`-pal, itt az ideje, hiszen ez a NIS egyik alapköve. Az RPC (Remote Procedure Call) egy C-programozói könyvtár, amely lehetővé teszi, hogy egy folyamat egy függvényt egy másik számítógépen hívjon meg. Amikor az RPC-ről beszélünk, legtöbbször a Sun-féle



<http://www.linux-nis.org/>

megvalósításra gondolunk, más néven a `sunrpc`-re. Amennyiben akad olyan kiszolgáló, amely távoli függvényhívást tesz lehetővé, először a `portmap`-hez fordul, és „elmondja”, hogy milyen számon és melyik kapun érhető el. Amikor az ügyfél kapcsolódik, a `portmap`-tól tudja meg, hogy az adott számú kiszolgáló éppen melyik kapun csücsül. Az egyetlen állandó kapu így a `portmap`-é, ami a 111-es, az összes RPC-kiszolgáló kapuja változhat. Összefoglalva: a `portmap` nem tesz mást, mint hogy azokat az egyedi számokat, amelyeken a függvények elérhetők, kapuszámokra fordítja. Ez a kialakítás természetesen azt is jelenti, hogy a `portmap`-nak kell legelőször elindulnia – még mielőtt bármilyen RPC-kiszolgálót indíthatnál a gépeden. Debian alatt például futási szinttől függetlenül a rendszerindítás után önműködően elindul a `portmap`. Amennyiben a `portmap` meghal, az összes RPC-kiszolgálót újra kell indítani. Meg kell jegyezni, hogy velem ez még sosem fordult elő, de ki tudja, mit hoz a jövő. A biztonságmániásoknak jegyezném meg, hogy a `portmap` használja a `tcp_wrapper` függvénykönyvtárat, így a `/etc/hosts.allow`, illetve a `/etc/hosts.deny` állományokkal kényelmesen behatárolható azoknak a gépeknek a köre, amelyeknek engedélyezett a használat (lásd még: `portmap(8)`).

A NIS-tartományok

Egy NIS-re épülő hálózat több tartományból áll, de legalább egy szükséges. Ezt a tartományt még véletlenül sem szabad összetéveszteni a DNS-sel. Amennyiben a hálózaton NIS és `named` is található, tartományként mindenképpen valamilyen a DNS-től különböző nevet válassz, ezzel is megnehezítve az esetleges külső behatolókat. A tartománynevet a `domainname` paranccsal bármikor lekérdezheted és beállíthatod (lásd később). Ebben a tartományban lennie kell legalább egy úgynevezett fő (master) kiszolgálónak, ami a megosztandó adatbázisokat tartalmazza. Ezt tükrözheti egy vagy több alkiszolgáló (slave), amelyek a fő gép adatbázisairól mindig pillanatnyi másolatot tartanak fenn, és ha nagyon leterhelt lenne, ők is kiszolgálhatják az ügyfeleket.

