

## A Yum használata az RPM-frissítésekhez

A legtöbb ismert biztonsági kockázat elkerülhető, ha eltávolítjuk a nem használt programokat és naprakészen tartjuk a rendszerünket. Ehhez egy új eszközt mutatok be, amelyet már három népszerű Linux rendszer-csomag használ.

**A** rendszerünk sokszor a programhibák miatt válik sebezhetővé. Hogy az ebből eredő kockázatot csökkentsük, kiemelkedően fontos, hogy frissítsük a Linux rendszert minden alkalommal, ha egy új biztonsági javítócsomag válik elérhetővé. A kérdés súlyát jól mutatja, hogy annak idején hosszabb írást is szenteltem a témának, mind a Linux Journal oldalain („Staying Current without Going Insane”, 2002 júliusi szám), mind a könyvem (Building Secure Servers With Linux, Biztonságos kiszolgálók építése a Linux segítségével) 3. fejezetében.

A Debian és SuSE rendszerek frissítése az íráskor megjelenése óta eltelt két év alatt sem változott jelentősen, még mindig az **apt-get** és a **YaST** a feladat végrehajtására leginkább használt eszköz. A Red Hat világa azonban egy új és figyelemre méltó eszközzel lett gazdagabb, amit **Yum** néven emlegetnek (a **Yellow Dog Updater, Modified** kifejezés után). Ebben a hónapban azt fogom elmondani, hogy miképpen szerezhetjük be ezt a kis programot, hogyan helyezhetjük üzembe, és mi módon használhatjuk fel a Red Hat, Fedora vagy Mandrake rendszerünk naprakészen tartásában.

### A Yum legfontosabb vonásai

Ahogy a program neve is utal rá, a **Yellow Dog Updater, Modified** Yellow Dog Updater, vagyis Yúp program leszámoltja, amely a Macintosh gépekre írt Yellow Dog Linux Rendszer-csomag része. Noha a Yúp kizárólag csak a Yellow Dog (Macintosh) rendszereken fut, a Yum működik Red Hat, Fedora, Mandrake és Yellow Dog Linuxon, amelyekben a Yúp-ot váltotta fel. A Yum a Duke Egyetemen működő **Linux@DUKE** csapat projektje, mely csapat két legbefolyásosabb tagja **Seth Vidal** és **Michael Stenner**.

Pár szóban összefoglalva, a Yum az RPM-et használó rendszerekben azt a funkciót tölti be, amit az **apt-get** a Debianban, vagyis egy egyszerű parancsot biztosít, amelyet programcsomagok automatikus telepítésére vagy frissítésére használhatunk, miután önműködően megtörtént az összes olyan egyéb csomag telepítése és frissítése is, amelyek szükségesek a kívánt program függőségeinek kielégítésére. A Yum valójában két parancsból áll: a **yum** az ügyfél-oldali parancs, míg a **yum-arch** a kiszolgáló oldali utasítás, amellyel a Web- vagy FTP-kiszolgálóink Yum-tárra való alakításához szükséges fejérsz-állományokat hozhatjuk létre.

A **yum-arch** parancs ismertetése meghaladja ennek a cikknek a kereteit, de mindenképpen szükségünk lesz rá, ha nyilvános Yum-tárat szeretnénk létrehozni, saját Yum-tár kialakítását tervezzük a helyi rendszereink karbantartásához, vagy pedig egy nem hálózati Yum-tárat hozunk létre a merevlemezünkön. A **yum-arch** parancs használata egyszerű, és a **yum-arch(8)** man-oldal minden szükséges információval elátja a felhasználókat.

Az **apt-rpm** paranccsal szemben – amely az **apt-get** egy népszerű átültetése az RPM-alapú rendszer-csomagok kezelésére – a Yum kifejezetten az RPM-formátumú csomagokhoz lett létrehozva. Mindehhez **Michael Stenner** még azt is hozzáteszi, hogy „a Yum tervezése során elsődleges szempont az egyszerűség és megbízhatóság volt, s egyúttal nagyobb a hangsúly a biztonságon és megbízhatóságon, mint az ügyfél oldali testreszabás esetében.”

### A Yum beszerzése

A Yum letöltését kínáló Weboldal (amelynek címét a Kapcsolódó címek részben találhatjuk meg) elmagyarázza, hogy az egyes Red Hat vagy Fedora változatok esetén a Yum melyik változatát érdemes letöltenünk. Ha a Fedorát használjuk, a Yumot a Fedora Core 1 tartalmazza, a **yum-2.0.4-2.noarch.rpm** csomag pedig megtalálható a Fedora 1-es számú telepítőcd-jén. Amennyiben az általunk használt rendszer a Mandrake 9.2, a **yum-2.0.1-1mdk.noarch.rpm** csomagot a telepítőcsomag **contrib/i586** könyvtára tartalmazza.

A Yum teljes egészében Python nyelven íródott, ezért ahhoz, hogy a Yum RPM-csomagjait telepíteni tudjuk, szükségünk van a Fedora/Red Hat **python**, **gettext**, **rpm-python** és **libxml2-python** csomagjainak (vagy ezek Mandrake-megfelelőinek) feltelepítésére. Jó eséllyel ezek a csomagok már korábban a rendszerünkre kerültek.

### Hol találhatóunk Yum-tárhelyeket?

Honnan tudja a Yum az RPM-csomagokat letölteni? Az erre alkalmas hely rendszerint a Világháló valamelyik távoli szöglete. Mivel a biztonsági kérdéseket igen fontosnak tartom, innentől kezdve a Yum-ot a biztonsági foltok letöltésének szemszögéből fogom vizsgálni. A cikk hátralévő részének fókuszában a hálózaton keresztül történő frissítések

## 1. lista A Fedora Core 1 /etc/yum.conf állománya

```
[main]
cachedir=/var/cache/yum
debuglevel=2
logfile=/var/log/yum.log
pkgpolicy=newest
distroverpkg=fedora-release
tolerant=1
exactarch=1

[base]
name=Fedora Core $releasever - $basearch - Base
baseurl=http://fedora.redhat.com/releases/fedora-core-$releasever

[updates-released]
name=Fedora Core $releasever - $basearch - Released Updates
baseurl=http://fedora.redhat.com/updates/release
d/fedora-core-$releasever

#[updates-testing]
#name=Fedora Core $releasever - $basearch - Unreleased Updates
#baseurl=http://fedora.redhat.com/updates/testing/fedora-core-$releasever
```

## 2. lista A testre szabott [base] szakasz

```
[base]
name=Fedora Core $releasever - $basearch - Base
baseurl=http://mirror.eas.muohio.edu/fedora/
↳ linux/core/$releasever/$basearch/os/baseurl=
↳ http://fedora.redhat.com/releases/
↳ fedora-core-$releasever
gpgcheck=1
failovermethod=priority
```

állnak, de a teljesség érdekében meg kell jegyezni, hogy a Yum képes az RPM-csomagok helyi, vagy olyan, látszólag helyi fájlrendszeréből való olvasására is, mint amilyen az NFS.

Akár távoli, akár helyi kiszolgálóról van szó, az RPM-csomagoknak egy Yum-tárat kell alkotniuk. Ennek tartalmaznia kell egy *headers* nevű könyvtárat, amely magában foglalja a Yum számára az RPM-csomagok függőség-ellenőrzéséhez és megfeleltetéséhez szükséges információkat. Ez az oka annak, hogy nem választhatunk ki tetszésünk szerint egy régebbi Red Hat tükrözést vagy Mandrake CD-ROM-ot. Amennyiben a Fedora Core 1 vagy 1.90 változatot használjuk, lehetőségünk van a Yum-ot bármelyik Fedora tükrözésre ráirányítani. Mivel a Yum a Fedora hivatalosan is támogatott frissítő eljárása, a tükrözések már eleve Yum-tárhelyként is szolgálnak.

Hallottunk már a Fedora Legacy Project-ről? A Fedora erőfeszítéseinek ez a vonulata a korábbi Red Hat rendszercsomagokhoz kínál biztonsági frissítéseket, jelenleg a Red Hat 7.3, 8.0 és 9.0 változatokhoz. Ebből következik, hogy sok Fedora-tükrözés Red Hat frissítéseket is tartalmaz Yum-tárhely formátumban.

Ha kétségeink lennének, a különböző rendszercsomagok számára készült Yum-tárhelyek egy kicsi, de jól használható listáját találjuk a Kapcsolódó címek szakaszban. A listában szereplő hivatkozások mindegyike egy szövegblokkot is tartalmaz, amelyet közvetlenül az */etc/yum.conf* fájlunkba is átírhatunk – erről hamarosan részletesen is szó lesz. Ha más megoldást nem találunk, írjuk be a Google-be a rendszercsomagunk nevét és a Yum repository (Yum-tár) kifejezést, így szintén rábukkanhatunk a megfelelő helyekre.

## A Yum beállításai

A Yum beállítása meglehetősen egyszerű, mindössze egyetlen fájl szerkesztéséről van szó, amelynek a neve – ahogyan megjósolható – */etc/yum.c*. Az 1. lista azt az alapértelmezett */etc/yum.conf* fájlt mutatja be, amely a Fedora Core 1 Yum RPM csomagban juthat el a felhasználóhoz.

Amint látható, ez a fájl globális változók beállításának listájából áll, amelyet egy vagy több [server] blokk követ ([base] és [updates-released] az 1. listán). Ezek mindegyike különböző típusú RPM-csoportok beállításait határozza meg. Nem szándékozom az összes lehetséges globális illetve kiszolgáló-blokk beállítást ismertetni, erre használhatjuk a *yum.conf(5) man*-oldalt is, de vizsgáljunk meg néhányat a legfontosabbak közül.

Az általános (global) szakaszban a *debuglevel* azt határozza meg, hogy a Yum kimenete mennyire legyen bőbeszédű. Ennek az értéke 0-tól (nincs semmilyen kimenet) a 10-es értékig (a legrészletesebb kimenet) terjedhet. Az 1. listán látható az alapértelmezett beállítás, amelynek értéke 2.

Amennyire én tudom, ez a *debuglevel* értéke csak a szabványos kimenetet érinti, vagyis nincs hatással a Yum napló-fájljára, amelynek a helyét a *logfile* értéke határozza meg. Most ezt az értéket mégis 4-re szeretném állítani, amely értéket úgy kaptam meg, hogy egy kicsit eljártam a *yum* parancs *-d* paraméterével. Például a *(yum -d 4 yum-parancsok)* utasítással ugyanazt a hatást érhetjük el és ez a beállítás felülbírálja a *debuglevel* értékét.

Szintén az általános szakaszban találjuk a *pkgpolicy* változót, amely azt határozza meg, hogy egy adott csomag melyik változatát használja a program, amikor az több [server] blokkban is előfordul. A *distroverpkg* változó a helyi kiadás-fájl csomag (*release file package*) nevét adja meg a kiadás fájl, amely például */etc/fedora-release* vagy */etc/redhat-release* lehet, a Linux rendszercsomagunk nevét és változatszámát tartalmazza.

Minden egyes [server] blokk egy RPM-halmazt határoz meg. Jobban örülnék neki, ha ezeket inkább [package-type] blokkoknak neveznék, ugyanis nem a kiszolgáló, hanem az RPM-csoport az, ami ezeket megkülönbözteti. Egyetlen blokk is tartalmazhat több kiszolgálóra mutató URL-t. Az 1. listában a [base] blokk egyetlen URL-t tartalmaz, amely a fő Fedora tárhelyre, a <http://www.fedora.redhat.com> címre mutat. Azok a Fedora-tükrözések, amelyek ugyanezeket az RPM-gyűjteményeket tartalmazzák, további sorokban adhatóak

meg ugyanebben a szakaszban. A [server] blokk bármely sorában használható két változó: a \$releasever, amely a használt Linux rendszercsomag verziószámát adja meg, és a \$basearch, amely a rendszerünk processzorát sorolja a megfelelő processzorcsaládba. A processzorcsaládok itt a legáltalánosabb értelemben szerepelnek, ebben az összefüggésben például az Athlon processzorok az i386 család tagjai. Lehet, hogy a Yum RPM-ünk által telepített `/etc/yum.conf` fájl rendben működik, de az 1. listában látható alapértelmezett `http://fedora.redhat.com...` hivatkozásokat legalább egy tüköroldalra mutató hivatkozással kell kibővítenünk. Ezzel minimálisra csökkenthető a veszély, hogy egy kiszolgáló elérési problémái miatt a frissítési folyamatunk nem sikerül. Ne feledjük a böngészőprogramunkkal ellenőrizni, hogy a `yum.com` fájlhoz hozzáadott hivatkozások mindegyike egy olyan könyvtárra mutat, amely tartalmaz egy `headers` nevű könyvtárt is. Arra is ügyeljünk, hogy a megadott URL végére kitegyük a záró perjelet.

Az 1. listával kapcsolatos másik említésre méltó dolog, hogy hiányzik egy fontos [server] szakaszbeli beállítás, mégpedig a `pgpcheck`. A 2. listán láthatunk egy javított [base] blokkot, amely használja ezt a lehetőséget.

A `pgpcheck=1` beállítással azt érjük el, hogy a Yum minden letöltött RPM-csomagban ellenőrzi a GnuPG aláírást.

Ahhoz, hogy ez működjön, szükségünk van a megfelelő GnuPG-kulcsok RPM-adatbázisunkba történő befoglalására. A Fedora Core 1 rendszereknél ezek a kulcsok a `fedora-release` csomag részeként már a rendszerünkre települtek. Ezeknek az RPM-adatbázisba történő másolásához a következő parancsot kell futtatnunk:

```
rpm --import /usr/share/doc/fedora-release-1/
➔ RPM-GPG*
```

Az `rpm --import` parancs URL-t is elfogad paraméterként, így ha a Yum-forrásunk GnuPG-kulcsa a hálózaton keresztül hozzáférhető, az alábbi formát használhatjuk:

```
rpm --import
http://your.distro.homepage/GPGsignature
```

amelyben a `http://your.distro.homepage/GPGsignature` részt a megfelelő valós hivatkozással kell helyettesítenünk. Úgy tűnhet, hogy ezzel csak bonyolítjuk a dolgot, pedig érdemes használni ezt a beállítást. Az évek során számos Linux-terjesztéssel foglalkozó oldalról töltöttek le a gyánútlan felhasználók trójai programokkal vagy egyéb „finomsággal” fertőzött programcsomagokat. Ezeknek a kivédésére a legmegfelelőbb eszköz az RPM GnuPG aláírást támogató tulajdonságának a kihasználása.

A 2. listában eszközölt másik említésre méltó változtatás, a `failovermethod=priority` változó megadása, amely arra utasítja a Yum-ot, hogy a listában felsorolt URL-eket sorrendben, a legfelsőtől lefelé haladva próbálja felhasználni. Az alapértelmezett viselkedés a `failovermethod=roundrobin`, amely beállítás hatására a Yum a felsorolt hivatkozások közül véletlenszerűen választ ki egyet. Én személy szerint a prioritásos működést részesítem előnyben, mert így lehetőségem van arra, hogy a közelebbi, gyorsabb tükörzéseket tegyem az elsődleges helyekké.

3. lista Frissítések ellenőrzése (a kimenet az olvashatóság érdekében enyhén rövidítve és formázva lett)

```
[root@iwazaru-fedora etc]# yum check-update
Gathering header information file(s) from
server(s)
Server: Fedora Core 1 - i386 - Base
Server: Fedora Core 1 - i386 - Released Updates
Finding updated packages
Downloading needed headers
getting /var/cache/yum/updates-released/headers/
➔ coreutils-0-5.0-34.1.i386.hdr
coreutils-0-5.0-34.1.i386 100% |=====|
➔ 13 kB 00:01
```

Name	Arch	Version	Repo
XFree86	i386	4.3.0-55	updates-released
XFree86-100dpi-fonts	i386	4.3.0-55	updates-released
XFree86-75dpi-fonts	i386	4.3.0-55	updates-released
XFree86-Mesa-libGL	i386	4.3.0-55	updates-released

### A Yum önműködő futtatása

Elérkeztünk a könnyű részhez, a yum parancs használatához. A Yum futtatásának két módja létezik, az egyik, hogy kézzel elindítjuk a parancssorból, a másik pedig, hogy az `/etc/init.d/yum` indító parancsfájl segítségével önműködővé tesszük az indítást. Ha engedélyezett – ezt a `chkconfig --add yum` parancs futtatásával magunknak kell megtennünk –, akkor ez a parancsfájl egyszerűen ellenőrzi a futtatófájlt, amely a `/var/lock/subsys/yum` fájl, s amelyet a `cron.daily` feladat, a `yum.cron` vizsgál meg. Ha a parancsfájl engedélyezett, vagyis ha a futtatófájl létezik, a cron-feladat először is futtatja a Yum parancsot a frissített Yumcsomag ellenőrzésének és telepítésének céljából, ezután pedig ellenőrzi az összes többi csomag esetleges frissítését, és szükség esetén telepíti is azokat. Mindeközben a Yum a háttérben önműködően felold minden fontos függőséget. Ha egy frissített csomag függ egy másik csomagtól, a Yum kikeresi és telepíti az a csomagot, még akkor is, ha korábban ez nem történt meg. A legtöbb felhasználó jó hasznát veheti ennek a hatékony parancsfájlnak. Ellenben ha a környezetünk megkívánja a minden részletre kiterjedő változás-ellenőrzést, és nem szeretnénk, hogy bármilyen új program önműködően a rendszerünkre kerüljön, kézzel kell futtatnunk a Yum-ot.

### A Yum manuális indítása

Ha csak egy listát szeretnénk kapni az elérhető frissítésekről anélkül, hogy bármit is feltelepítenénk, használjuk a `yum check-update` parancsot (3. lista).

Egyetlen frissítés telepítéséhez az összes olyan frissítés végrehajtásához, amire a függőségek miatt szükség van, a yum update csomagnev parancsot használhatjuk, például yum update yum.

Ezzel valójában csak magát a Yum csomagot frissítjük. Ha tényleg elérhető a Yum egy frissített csomagja, a rendszer a folytatásra és telepítésre buzdít. Amennyiben a Yum-ot egy parancsfájlból hívjuk, és azt szeretnénk, ha az összes feltett kérdésre önműködően -y legyen a válasz, használjuk a -y kapcsolót:

```
yum -y update yum
```

A check-update parancs, vagyis a Yum parancs megfelelő formájának futtatása, nem kötelező a frissítések telepítése előtt. Ha úgy tetszik, használhatjuk közvetlenül a yum update parancsot is – ez ugyanazokat az ellenőrzéseket végrehajtja, mint a yum check-update.

Az utolsó mintaként bemutatott parancsban egyetlen frissítendő csomagot, a yum-ot adtuk meg. A rendszerünkön lévő összes telepített csomag frissítésének kezdeményezéséhez mindössze el kell hagynunk az utolsó paramétert, a csomag-meghatározást: yum update.

Miután a Yum ellenőriz minden frissítési lehetőséget, és kiszámolja a függőségeket, bemutat egy listát azokról a frissítésekről, amelyeket le szeretne tölteni. Ha nem használtuk a -y lehetőséget, kérdést kapunk, hogy tényleg le szeretnénk-e tölteni és telepíteni az összes felsorolt csomagot. A teljesség kedvéért íme egy jutalomtipp: új csomagokat

is telepíthetünk a Yum segítségével – mint ahogy erre esetleg már rá is jöttünk. Bármelyik csomag esetében, amelyet tartalmaz az */etc/yum.conf* fájlban felsorolt források valamelyike, használhatjuk a yum install csomagnev parancsot a kérdéses csomag legfrissebb változatának telepítéséhez, kiegészítve azokkal, amelyektől függő helyzetben van. Például a *vsftpd* nevű FTP-kiszolgáló csomag telepítéséhez a következő parancsot futtatnánk: yum install vsftpd.

### További információk

Amennyiben a Yum használatával kapcsolatban bármilyen problémánk adódna, a hálózaton keresztül bőséges leírás – köztük két kitűnő GYIK áll rendelkezésre. Erre vonatkozóan lásd a hálózaton keresztül elérhető források jegyzékét. Ha az on-line dokumentáció sem segít, rendelkezésünkre áll a Yum levelezőlistája is. Mielőtt azonban feladnánk egy kérdést, ne mulasszunk el a problémánkra vonatkozóan egy-két keresést feladni a Google keresőben. E cikk írása közben számos olyan kérdéssel találkoztam a Yum levelezőlistáján, amit a Google segítségével meg tudtam oldani.

*Linux Journal* 2004. június, 122. szám



**Mick Bauer** (mick@visi.com)

Biztonsági szakember, a *Linux Journal* biztonsági témákkal foglalkozó szerkesztője, biztonsági tanácsadó a Minnesota állambeli Minneapolisban található Upstream Solutions LLC Inc.-nél.

