

Linux kernel / CARNet kernel paket

/*-->*/

Općenito o CARNet kernel paketu

Kao što već znate, CARNetovi poslužitelji obično koriste unaprijed izgrađeni kernel-2.6-cn paket. On se temelji na stabilnoj Linux 2.6 jezgri (dostupna sa adrese <http://www.kernel.org/> [1]), razvojnim Grsecurity dodatcima (<http://www.grsecurity.net/~spender/> [2]) te L7-filter dodacima (<http://sourceforge.net/projects/l7-filter/files/> [3]). Stabilnom jezgrom smatramo onu major verziju koja je već otprije izdana te na kojoj se ne odvija intenzivni razvoj, ali koja ima pokrpane sve poznate probleme. Na primjer, trenutna razvojna verzija Linux jezgre je 2.6.24-rc4, a trenutna stabilna inačica je 2.6.23.9; dakle u 2.6.23 inačici je već 9 podverzija koje imaju ispravljene raznorazne greške, dok se znatnije promjene najranije očekuju u 2.6.24 inačici.

Ukratko navedimo što pojedini dodatak donosi:

- Grsecurity dodatak: ojačanja chroot poziva, zaštitu /tmp datotečnog sustava, djelomičnu zaštitu od različitih tipova napada preljeva spremnika u korisničkim aplikacijama (tzv. PaX) kao i u jezgri, randomizacija stoga, biblioteka i gomilišta, ograničenja /proc datotečnog sustava radi smanjenja curenja informacija, itd.
- L7-filter: riječ je o klasifikatoru paketa koji na aplikativnoj (OSI Layer 7) razini primjenjuje regularne izraze nad podacima i ustanovljava o kakvom je višem protokolu riječ. Klasifikator je vrlo složen i zahtjevan što se tiče sistemskih resursa, no vrlo koristan za slučajevne potrebe klasifikacije P2P i raznog drugog prometa koji ne koristi tipične odnosno uobičajene izvorišne i odredišne portove. Klasifikator pri tome nije u stanju sve protokole prepoznati sa jednako dobrom pouzdanošću, pa se najčešće ne koristi za blokiranje prometa, već kontrolu propusnosti kroz markiranje unutar jezgre i kasniji QoS na temelju oznaka.

Raspored CARNet kernel paketa

Sam izgled kernel-2.6-cn paketa možemo ukratko raščlaniti na:

- /boot direktorij koji sadrži:
 - vmlinuz datoteke, odnosno pojedinu komprimiranu (bzImage) izvršnu Linux jezgru u užem smislu,
 - System.map datoteke koje su tablice jezgrinih simbola (imena funkcija ili varijabli) prisutnih u pojedinoj jezgri i njihovih adresa. Primijetimo, System.map ne sadrži informacije o jezgrim modulima koji se učitavaju dinamički (po potrebi),
 - initrd datoteke su ramdisk datoteke, odnosno minimalni datotečni sustavi koji sadrže

dodatne jezgrine module koji trebaju poslužiti pri podizanju sustava. Tipična upotreba je za hardversku podršku različitim SCSI i SATA kontrolerima čime se omogućava jezgri da u nastavku podizanja sustava može pročitati osnovni (root) datotečni sustav,

- config datoteke koje sadrže konfiguraciju jezgre prilikom prevođenja što omogućava sistemcu da na osnovu takve konfiguracije uredi vlastitu i ponovno prevede,
- /lib/modules direktorij koji sadrži različite jezgrine module (LKM) koji se učitavaju po potrebi. Prisjetimo se, rečeni moduli mogu sadržavati podršku za različite datotečne sustave, hardver poput mrežnih kartica, SCSI ili SATA kontrolera, tračnih uređaja i sl.

Podržani hardver u CARNet kernel paketu

- memorija: do 64GB (BigMem odnosno PAE podrška)
- procesori: svi IA32 (počevši od PIII procesora), x86_64 uključno sa EM64T procesorima PIII i viši (ali ne IA-64 arhitektura) u SMP i UP načinu rada
- matične ploče: sve standardne PC ploče za IA32 ili x86_64 arhitekturu
- PATA kontroleri: AMD AMD74xx, CMD64x, Highpoint HPT366, Intel PIIX/ICH, IT821x, Promise PDC202xx, ServerWorks, Silicon Image, SIS513, VIA82Cxxx, genericki PCI IDE, ITE 821x, Pacific Digital Corporation ADMA, Serverworks OSB4/CSB5/CSB6, Sil, SiS, VIA, Marvell
- SATA kontroleri: AHCI, Marvell, nVidia, Promise ATA TX2/TX4/TX4000, Pacific Digital Corporation QStor, Silicon Image, Silicon Image 3124/3132, Silicon Integrated Systems, K2, Promise, ULI, VIA, Vitesse VSC7174
- SCSI i SAS kontroleri: 3ware 9000, Dell PERC2, 2/Si, 3/Si, 3/Di, Adaptec Advanced Raid Products, HP NetRAID-4M, IBM ServeRAID, ICP SCSI, Adaptec AIC77xx/78xx/790x/94xx, HP Controller CCISS SA5xxx/SA6xxx, Adaptec I2O, IBM Power RAID, IBM ServeRAID, Emulex LightPulse Fibre Channel, LSI Logic MegaRAID, Fusion MPT, Qlogic ISP (QLA 1x80/1x160), QLogic Fibre Channel, NCR/Symbios/LSI 8xx/1010
- Ethernet kartice: 3Com 3c59x/3c9xx, RealTek RTL-8139, Broadcom NetXtreme II BCM5706/5708, Intel PRO/100, NE2000, PCNet32/PCnetPCI, RealTek RTL-8169, SiS sis190, SiS 900, SysKonnect, Digital 21x4x Tulip, 3Com Typhoon (3C990, 3CR990, itd), VIA Rhine, VIA Velocity, QLogic QLA3xxx
- podrška za ostalo: IPv4 i IPv6 Netfilter moduli, QoS pravila, raznorazni datotečni sustavi (NFSv3 client i server, XFS, Ext2/3, Minix), VLAN 802.1q, bridge 802.1d, USB EHCI/UHCI/OHCI, InfiniBand, Linux SoftRAID (append, MD0/1/5), LVM2, IPMI, i6300ESB watchdog, i8xx/Intel TCO watchdog, DeviceMapper, itd.

Instalacija CARNet kernel paketa

Do recentne i stabilne Linux jezgre najjednostavnije možete doći sa instalacijom CARNet Linux kernel paketa:

```
apt-get update
apt-get install kernel-2.6-cn
reboot
```

Prilikom same instalacije paketa, automatski se generira LILO konfiguracija (datoteka `/etc/lilo.conf`) i postavlja preporučena jezgrina konfiguracija (`/etc/sysctl.conf`). Također, paket kreira novu grupu "proc" sa GID-om 99. Osim root grupe, jedino rečena proc grupa ima privilegije čitanja potpunog `/proc` stabla; stoga se prakticira u tu grupu staviti specifične servise koji trebaju pristup `/proc` stablu - to su `snmpd`, `oidentd` i `sl`.

Vlastita kompilacija jezgre

Linux jezgra se relativno lako i bezbolno rekompilira. Nažalost, najveći problem je sama konfiguracija odnosno rekonfiguracija, ako koristite već pripremljenu config datoteku iz `kernel-2.6-cn` paketa. Tijekom vremena kako se razvijao računalni hardver i softver je vrlo narasla količina opcija koje je moguće podesiti (omogućiti ili onemogućiti). Shodno tome, prilikom rekonfiguracije potrebno je proći desetine menija i stotine opcija što je donekle zamoran posao. No još gore, očekuje se prilično dobro znanje o pojedinoj opciji i samom hardveru kojeg imate. Prije ikakvog postupka vlastite rekompilacije preporučamo pročitati par relevantnih dokumenata, poput <http://www.faqs.org/docs/Linux-HOWTO/Kernel-HOWTO.html> [4] te <http://www.digitalhermit.com/linux/Kernel-Build-HOWTO.html>.

Da bi uopće mogli kompilirati jezgru, potrebno vam je minimalno C razvojno okruženje. Ono je dobavljivo na sljedeći način:

```
apt-get update
apt-get install build-essential libncurses5-dev patch
```

Najjednostavnije je početi od već poznate i ispravne konfiguracije poput one iz `kernel-2.6-cn` paketa. Samu jezgru možete preuzeti bilo instalacijom `kernel-2.6-source-cn` paketa (pa će se pojaviti u `/usr/src/linux-2.6` direktoriju) bilo direktnim skidanjem sa izvornog mjesta, a to je <https://www.kernel.org/> [1]. U prvom slučaju dobivate sve dodatke integrirane s jezgrom, a u drugom slučaju potrebno je to ručno odraditi. Dakle, pokažimo prvi način - instalaciju već priređenog izvornog koda za CARNet `kernel-2.6-cn` paket:

```
apt-get update
```

```
apt-get install kernel-2.6-source-cn
cd /usr/src/linux-2.6
make menuconfig
```

Druga varijanta je tek neznatno kompliciranija: prvo ćemo dohvatiti svježju jezgru (koja je aktualna uvijek možete provjeriti na <https://www.kernel.org> [1]):

```
mkdir -p /usr/src/linux-custom
cd /usr/src/linux-custom
wget ftp://ftp.hr.kernel.org/pub/linux/kernel/v2.6/linux-2.6.23.9.tar.bz2
tar xjf linux-2.6.23.9.tar.bz2
chown -Rh root:root linux-2.6.23.9
```

Dohvatimo i posljednji Grsecurity dodatak, uvijek dostupan u razvojnom direktoriju samog autora (<http://www.grsecurity.net/~spender/> [2]). Pazite, verzija u Grsecurity dodatku mora odgovarati verziji jezgre koju ste skinuli:

```
wget http://www.grsecurity.net/~spender/grsecurity-2.1.11-2.6.23.9-200712101800.patch
cd linux-2.6.23.9
patch -p1 < ../grsecurity-2.1.11-2.6.23.9-200712101800.patch
```

Izvorni kod je spreman za rekompilaciju, sad možemo iskoristiti postojeću konfiguraciju iz kernel-2.6-cn paketa:

```
cp /boot/config-2.6.22.9-grsec .config
make oldconfig menuconfig
```

Nakon završenog konfiguriranja (postupak nadalje vrijedi za obje varijante pribavljanja izvornog koda), potrebno je prevesti jezgru i module:

```
make -j2 bzImage modules
```

Te instalirati na pravo mjesto:

```
make install modules_install  
reboot
```

Jasno, prije kompilacije je moguće skinuti i po volji dodati raznorazne druge dodatke, što se najčešće obavlja naredbom patch.

- [Logirajte](#) [5] se za dodavanje komentara

pon, 2007-12-24 16:35 - Dinko Korunić **Kuharice:** [Linux](#) [6]

Kategorije: [Software](#) [7]

Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: <https://sysportal.carnet.hr/node/339>

Links

[1] <https://www.kernel.org/>

[2] <http://www.grsecurity.net/~spender/>

[3] <http://sourceforge.net/projects/l7-filter/files/>

[4] <http://www.faqs.org/docs/Linux-HOWTO/Kernel-HOWTO.html>

[5] <https://sysportal.carnet.hr/sysportallogin>

[6] <https://sysportal.carnet.hr/taxonomy/term/17>

[7] <https://sysportal.carnet.hr/taxonomy/term/25>