Instalacja emulatora qemu w wersji 0.8.2, wraz z akceleratorem kqemu w wersji 1.3.9pre.

Wojciech Kwedlo
Wydział Informatyki PB

1. Kompilacja emulatora qemu. Do kompilacji qemu potrzebny jest pakiet gcc, z tym że nie wolno używać wersji 4.x.x !. Kompilacja i instalacja przebiegają w trzech krokach:

```
cd katalog_w_którym_rozpakowano_plik_tar.gz
./configure --prefix=katalog_gdzie_zostanie umieszczony_qemu
make
make install
```

ostatni krok wymagać może uprawnień superużytkownika.

2. Uruchomienie emulatora.

```
qemu -hda hd0.img -hdb hd1.img -M isapc -m 32
```

W przypadku gdy kompilacja przeprowadzona została na architekturze x86_64 (wymagany Athlon 64, najnowsze procesory Intela + 64-bitowa dystrybucja) należy posłużyć się poleceniem `qemu-system-x86_64`. Aby umożliwić emulatorowi precyzyjne odmierzanie czasu, warto dodać linijkę:

```
echo 1024 > /proc/sys/dev/rtc/max-user-freq
```

do jednego z systemowych plików startowych np. rc.local.

3. Dostęp do plików na emulowanej maszynie.
Aby uzyskać dostęp do plików na emulowanej maszynie należy posłużyć się urządzeniem „loop". Dokonujemy tego przy pomocy następujących komend (zakładamy, że w systemie stworzono katalog /mnt/loop):

```
modprobe loop
losetup /dev/loop0 -o 32256 hd0.img
mount /dev/loop0 /mnt/loop
```

Spowodują one, że dane z głównego systemu plików zostaną zamontowane w katalogu /mnt/loop. Jeżeli nie mamy uprawnień superużytkownika, to proponuję do przegrywania plików wykorzystać katalog /tmp. W takiej sytuacji przegrywając pliki z emulowanej maszyny, należy pamiętać o ustawieniu uprawnienia do czytania dla wszystkich. Bardzo ważne: podczas przegrywania plików emulator qemu nie może pracować. W przeciwnym wypadku system plików na emulowanym dysku hd0.img na pewno straci spójność!!! Jeżeli zatem chcemy ponownie uruchomić emulator należy wykonać polecenie:

```
umount /dev/loop0
```

odmontowujące system plików emulatora.

4. Kompilacja akceleratora kqemu.
Akcelerator kqemu pozwala na bardzo szybką pracę emulatora (1.5 – 2 razy wolniej niż na maszynie gospodarza, bez kqemu nawet 10 razy wolniej). W związku z tym jest polecany, jeżeli chcemy na emulowanej maszynie kompilować jądro systemu, co jest bardzo pracochłonną czynnością. Po rozpakowaniu akcelerator kqemu kompilujemy i instalujemy podobnie jak qemu

```
./configure
make
make install
```

Ostatniego polecenia należy użyć z uprawnieniami superużytkownika (instalowany jest moduł jądra). Moduł ten należy ładować każdorazowo przy starcie systemu poprzez `modprobe kqemu`. Kqemu wymaga do pracy pliku urządzenia /dev/kqemu (domyślnie urządzenie o numerze 250) W związku z tym w dystrybucjach opartych na na mechanizmie udev należy moduł jądra nieco inaczej: `modprobe kqemu major=0`, co automatycznie przydzieli numer i utworzy plik specjalny. Ponadto należy ustalić prawa dostępu tego pliku dla wszystkich użytkowników, poprzez dodanie linii do odpowiedniego pliku (w Fedora Core 5 jest to `/etc/udev/50-udev.rules`).

```
DEVPATH==”/class/misc/kqemu”, MODE=666
```