

# QEMU



Relatore: Michele Asciutti

Autori: Michele Asciutti e  
MajaGLUG

Evento: Linux Day 2006

Location: Genzano – RM Biblioteca  
Comunale

# QEMU

- Da Wikipedia:
- Qemu è un software che implementa un particolare sistema di emulazione che permette di ottenere un'architettura nuova e disgiunta in un'altra che si occuperà di ospitarla; Qemu è stato ideato ed è coordinato da Fabrice Bellard.

# QEMU

- Questo software è conosciuto grazie alla sua velocità di emulazione ottenuta grazie alla tecnica della traslazione dinamica. È simile a Bochs, VMWare Workstation, Virtual PC ma più veloce nell'emulazione delle architetture x86.

# QEMU

- Qemu è formato da due parti: la prima si occupa dell'emulazione vera e propria (convertire, ad esempio, le istruzioni da 32 bit a 64) permettendo quindi di eseguire programmi compilati su architetture diverse; la seconda parte è l'emulatore di sistema: utilizzando la prima parte, è capace di creare un nuovo sistema completamente separato da quello ospitante (i file, quindi, sono separati).

# Storia

- Qemu, inizialmente, era un progetto che si prefiggeva di emulare solo il microprocessore x86 su un sistema GNU/Linux. L'intento iniziale era di eseguire Wine anche sulle macchine con architetture diverse dall'x86 (ad esempio i PowerPC, l'architettura dei Macintosh). Lo scopo fu raggiunto e si constatò che la tecnica della traslazione dinamica era più che valida; si iniziò, quindi, a cercare di creare un intero sistema di virtualizzazione per ottenere una macchina virtuale equiparabile ad un sistema x86 completo. Il risultato ottenuto fu più che positivo.

# Stato attuale

- Tuttora, Qemu è in grado di simulare sistemi x86, amd64, PowerPC e arm.
- Bellard ideò anche un modulo per i kernel Linux (KQemu) capace di aumentare notevolmente le prestazioni della macchina simulata; il codice, però, non è stato ancora rilasciato ed è distribuito come programma Freeware. Qemu ha trovato adesioni nella comunità dei programmatori che si occupano di migliorarlo; tra i vari progetti esistenti, risalta quello di FreeOsZoo che si occupano di fornire immagini dei dischi di Qemu dei più noti sistemi operativi liberi.

# Difetti

- Supporto parziale per Microsoft Windows e altri sistemi operativi
- Nessun supporto per le applicazioni multimediali: viene emulato una scheda grafica Cirrus Logic

# Utilizzo

- Per creare un disco virtuale di 500MB in Qemu utilizzando qcow:
- `qemu-img create -f qcow c.img 500M`
- l'opzione -f del comando serve a specificare il tipo di formato del disco virtuale. Sono supportati i tipi raw, qcow, cow, vmdk e cloop.

# Utilizzo

- Il comando farà partire l'emulazione su una macchina con 128MB di Ram utilizzando il disco c.img creato prima e farà il boot dall'immagine del CD salvata nel file linux.iso. La macchina emulata avrà il supporto audio e l'ora sarà sincronizzata con quella del pc host.
- ```
qemu -hda c.img -cdrom linux.iso  
-boot d -m 128 -soundhw sb16  
-localtime
```

# Utilizzo

- Per utilizzare una macchina virtuale con 64Mb di Ram avente come CD-Rom quello del sistema ospitante, di dovrà digitare
- `qemu -hda c.img -cdrom /dev/cdrom -boot c -m 64 -full-screen`

# Utilizzo

- Quando la macchina virtuale è avviata, con la combinazione Control-Alt-2 si accederà alla console di controllo di Qemu per effettuare alcune operazioni semplici (caricare un nuovo discoimmagine, riavviarlo, sospenderlo o uscire dal programma).
- Con la combinazione Control-Alt-1, invece, si ritornerà alla macchina emulata.

# Funzionamento

- Vediamo ora in pratica come funziona qemu, e quali usi è possibile fare dell'emulatore:
- Test rete, uso applicativi, installazione sistemi su dischi esterni ecc.