

Zoo di sistemi operativi: studio e realizzazione del supporto di macchine virtuali con accesso via Web

Mattia Gentilini

Relatore:
Renzo Davoli

Laurea Specialistica in Informatica — I Sessione — A.A. 2005/2006

12 luglio 2006

Sommario

Questa discussione presenterà un sistema di **virtualizzazione** per eseguire **sistemi operativi** diversi ed utilizzarli tramite il **World Wide Web**:

- Virtualizzazione: concetto ed esempi
- Lo **Zoo** di sistemi operativi: FreeOSZoo e FLOZ
- Implementazione di FLOZ
- Sviluppi futuri
- Conclusioni

Virtualizzazione: concetto

È ormai pratica diffusa ricorrere a meccanismi di **virtualizzazione** all'interno dei computer moderni, ossia utilizzare software che crei un ambiente (*Macchina virtuale* o VM) all'interno del quale eseguire altro software. Motivazioni diverse sono possibili:

- **Partizionamento** delle risorse in sottosistemi gestibili **independentemente**
- Mantenimento di **compatibilità** con altre architetture o sistemi operativi
- **Isolamento** di software o utenti per migliorare la **sicurezza** complessiva

Esistono molti esempi di virtualizzazione: se ne discutono brevemente tre, importanti in questo lavoro di tesi

QEMU, VDE e VNC

QEMU è probabilmente l'emulatore di **VM complete** con il maggior supporto di hardware e software e le migliori prestazioni.

- Può emulare un computer completo su cui eseguire un OS, oppure un processo Linux compilato per un certo processore su di un altro.
- Raggiunge ottime velocità, comparato con un sistema reale, e grazie a un modulo per il kernel Linux (QEMU Accelerator) può arrivare al pareggio.

VDE (*Virtual Distributed Ethernet*) è un emulatore di **reti Ethernet**. È composto da vari programmi che permettono, tra l'altro, di:

- Emulare switch, hub e cavi indipendenti dal sistema di trasporto
- Collegare le reti virtuali create a computer reali (tramite NAT o interfacce TUN/TAP) o virtuali (UML, QEMU, Bochs, MPS)

VNC (*Virtual Network Computing*) non è una virtualizzazione in senso stretto, ma consente di eseguire **applicazioni remote** come se fossero installate localmente

- A differenza dei prodotti concorrenti (che utilizzano oggetti), VNC trasmette *framebuffer*, ossia snapshot di porzioni di schermo
- Questo approccio è meno efficiente ma più portabile: per questo esistono server VNC per molti OS ed applicazioni, tra cui QEMU

Free Operating Systems Zoo (<http://www.oszoo.org/>)



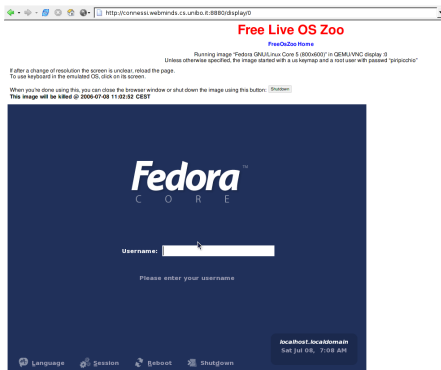
L'idea su cui si basa questo lavoro è quella sviluppata nel progetto **FreeOSZoo**

- Come uno zoo di animali, FreeOSZoo vuole far convivere più sistemi operativi FLOSS all'interno dello stesso ambiente reale, ricreando l'hardware per i quali i singoli OS sono progettati
- Lo scopo è quello di sperimentare sistemi operativi, impararli, studiarne la storia, creare ambienti di computing eterogenei con hardware omogeneo
- La versione attuale del progetto è una collezione di immagini di OS per QEMU, facilmente scaricabili ed eseguibili sul proprio computer

FLOZ: Free Live OS Zoo

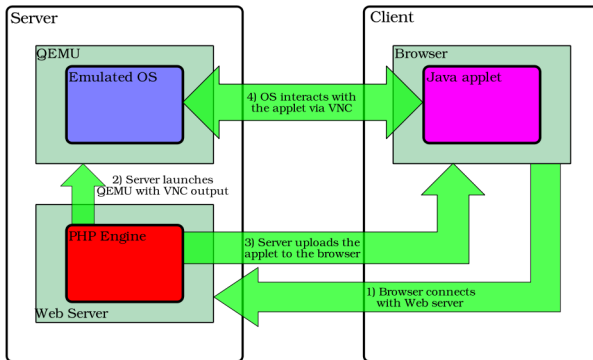
FLOZ rende FreeOSZoo utilizzabile “on-the-fly”, permettendo di eseguire le immagini da esso fornite senza scaricarle e senza installare QEMU

- L'utente si collega ad un server WWW e sceglie quale OS avviare
- Il server lancia QEMU con l'immagine dell'OS desiderato
- Il browser interagisce con QEMU tramite un'applet Java



Implementazione di FLOZ

FLOZ ha tre componenti: il server Web con gli script PHP di gestione, il sistema emulato attraverso QEMU, l'applet del client che interagisce con esso



Prestazioni e problemi noti

Le **prestazioni** sono incoraggianti, grazie alle potenzialità di QEMU e di VNC

- I tempi di trasferimento su connessione ADSL sono accettabili (aggiornamento completo dello schermo in circa 1 secondo, risposta di mouse e tastiera attorno al mezzo secondo). È possibile avere tempi maggiori in caso di cambio di modalità video
- L'emulazione è veloce, soprattutto con quelle immagini per le quali è possibile utilizzare QEMU Accelerator

Vi sono alcuni **problemi**, dovuti al fatto che il supporto VNC di QEMU è stato introdotto da poco tempo

- La tastiera non è emulata completamente, per cui alcuni tasti speciali (come le lettere accentate) possono non funzionare
- Il puntatore del mouse emulato può apparire accelerato rispetto a quello reale, a seconda delle impostazioni dell'OS emulato
- L'aggiornamento dello schermo può non essere perfetto



FLOZ per il fornitore di contenuti

Il software di FLOZ è facilmente portabile su sistemi dotati di OS POSIX, server Web e interprete PHP

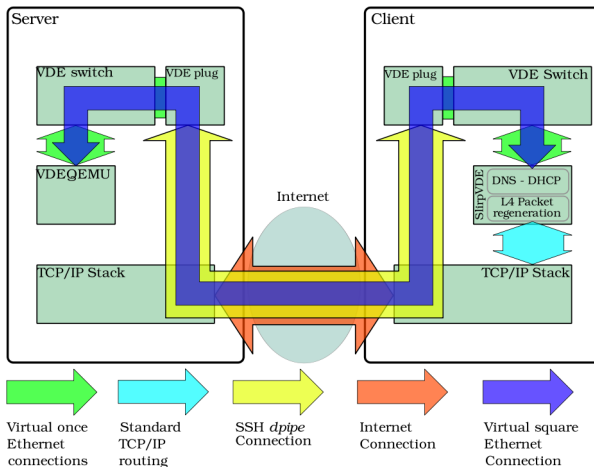
- Dover eseguire un'istanza di QEMU per ogni utente impone elevati requisiti hardware
- Esiste un'interfaccia Web dedicata alla configurazione delle singole immagini
- Ogni modifica alle immagini è persa a fine uso
- È possibile definire un tempo massimo di uso, dopo il quale QEMU viene terminato, e rilevare se il browser si è disconnesso



Il supporto di rete

Questa caratteristica di FLOZ ha come scopo quello di far passare il traffico di rete dell'OS emulato dal network stack dell'utente

La figura mostra il sistema finora testato, che richiede VDE installato sul client; questo requisito è penalizzante e andrà eliminato



Sviluppi futuri

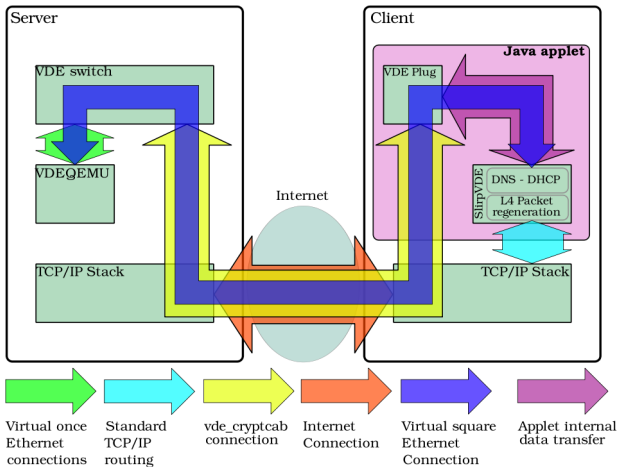
FLOZ, anche per motivi di tempo, non è un progetto completo; alcune cose vanno migliorate, ed altre funzionalità possono essere aggiunte

- Integrare il supporto di rete nell'applet Java
- Migliorare la sicurezza
- Gestire il carico del server
- Connessioni di rete tra le immagini
- Amministrazione delle immagini



Integrare il supporto di rete nell'applet Java

È il miglioramento più importante, poiché permette di ridurre al minimo i vincoli per il client anche con il supporto di rete attivato



Migliorare la sicurezza e gestire il carico del server

È necessario gestire la **sicurezza** delle connessioni

- **Manca un controllo sulle porte VNC e del canale di connessione.** Se per ogni istanza di QEMU si utilizzano porte diverse, è sufficiente modificare al volo le regole del firewall
- **La connessione VNC non è cifrata.** Si può estendere il server VNC di QEMU aggiungendovi un protocollo simmetrico (AES, Blowfish, Twofish); inoltre si può utilizzare una sessione HTTP sicura (con autenticazione e/o HTTPS) per trasferire le chiavi di cifratura

Controllare il **consumo di risorse** di FLOZ migliora la scalabilità; le due misure da tenere sotto controllo sono la RAM utilizzata e il *load average*

- Va determinato il numero massimo di immagini avviabili contemporaneamente, impostando la quantità di memoria necessaria ad ogni immagine
- Per ridurre il carico medio si può prevenire l'esecuzione di nuove immagini quando si superano certi valori e/o implementare politiche di distribuzione su più server



Connettere tra loro ed amministrare le immagini

- Si può permettere alla propria immagine attiva di collegarsi ad altre, per sperimentare firewall, NAT od altro, attivando più NIC o consentendo altre connessioni al proprio switch
- Per ambienti “di produzione”, per imparare al meglio l'uso di un sistema operativo, per testare sistemi potenzialmente pericolosi, può essere interessante permettere modifiche persistenti alle immagini
- Oltre all'accesso remoto consentito dalla connessione tra immagini, si può permettere un accesso locale, sviluppando politiche di gestione della connessione VNC



Conclusioni

Tre obiettivi hanno guidato lo sviluppo di FLOZ

- Portabilità dell'interfaccia client
- Ridurre i vincoli sugli OS utilizzabili nell'emulatore
- Uso di software libero ed open source, per libertà di sviluppo e apertura alla collaborazione

Questi obiettivi hanno reso la scelta del software abbastanza obbligata, ed a parte il supporto di rete di QEMU sono stati pienamente raggiunti con lo sviluppo attuale

Il supporto di rete incentrato sul client, caratteristica innovativa rispetto ad altri sistemi esistenti, è probabilmente il punto di forza di FLOZ e la base del lavoro futuro



Ringraziamenti e prova

FLOZ e questa tesi esistono anche grazie a:
Renzo Davoli, Fabrice Bellard, Anthony Liguori,
<garden>, <gaspa> e <danielinux>
Grazie!

Una versione di FLOZ è correntemente attiva su
<http://connessi.webminds.cs.unibo.it:8880/>
Verrà ora mostrato brevemente FLOZ in azione

