

*Server di rete
multifunzionali e modulari:
la soluzione Open Source Linux*

Elio Tondo

Seminario Open Source
Roma 7 aprile 2008

Elio Tondo

- Consulente IT, architettura dei sistemi e delle infrastrutture e applicazioni di rete
- Primi contatti con la telematica nel 1974, alla "tenera età" di 16 anni (connessione via terminale da Livorno al CNUCE di Pisa)
- Laurea in Ingegneria Elettronica nel 1982 (non esisteva ancora ingegneria informatica)
- Conoscenza del s.o. Unix durante l'attività di tesi (1981)
- Tecnologie di rete e sistemi operativi come filo conduttore durante tutta l'attività professionale
- Attività su Internet dal 1988 (prima della nascita del Web)
- Attività in ambito Open Source da inizio anni '90

Socio Mensa Italia dal 1985

Sistemi operativi e modularità (1)

Caratteristiche distintive di Unix fin dalle origini (1970):

- multiutente e multitasking
- interfaccia utente a riga comando "ricca" e programmabile (shell)
- comandi "esterni" alla shell numerosi, semplici ma potenti, combinabili tra loro
- uso generalizzato di flussi di dati di input/output e relative redirezioni
- dispositivi di ingresso/uscita "visti" come file
- protocolli di comunicazione in rete (TCP/IP si è diffuso tramite Unix)
- servizi di sistema come processi distaccati da console (esecuzione in background)
- interfaccia grafica (se utilizzata) vista come un servizio di sistema, non intimamente legata ad esso

Queste caratteristiche rendono i s.o. di tipo Unix particolarmente adatti per l'implementazione di servizi di rete, anche per la facilità nella realizzazione di procedure di amministrazione automatizzate e replicabili

Sistemi operativi e modularità (2)

Sistemi operativi "proprietary" (in particolare quelli di produzione Microsoft):

MS-DOS (inizio anni '80):

- monoutente e monotasking
- interprete dei comandi molto limitato
- pochi comandi esterni non combinabili tra loro
- uso limitato delle redirezioni
- dispositivi di ingresso/uscita gestiti in modo non omogeneo

Windows 3.x (inizio anni '90):

- interfaccia grafica e rudimentale multitasking per applicazioni native e MS-DOS
- supporto di rete limitato (TCP/IP inizialmente non disponibile)

Windows NT 3.5 (1993):

- prima versione a 32 bit non basata su MS-DOS
- somiglianze con VMS di Digital Equipment Corporation
- interfaccia grafica strettamente connessa con il kernel del sistema
- networking integrato, orientamento a servizi di rete locale

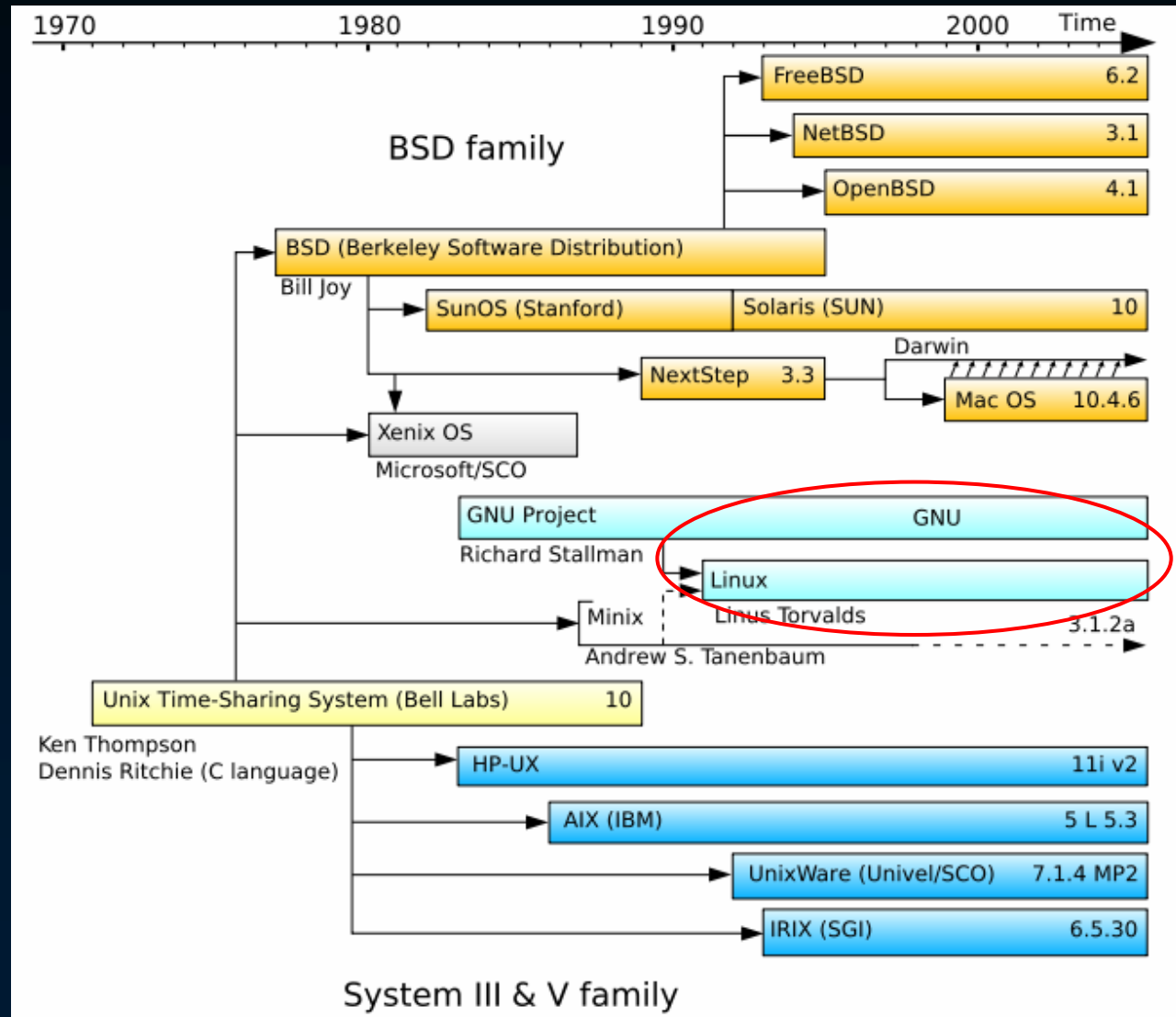
Anche le versioni successive (NT4, 2000, 2003 Server...) hanno una struttura poco modulare e una forte integrazione tra kernel e interfaccia grafica, rendendo complessa l'automazione della configurazione e dell'amministrazione del sistema

La nascita di Linux (1)

All'inizio degli anni '90, dalla convergenza di parte degli sviluppi del progetto GNU della Free Software Foundation



e di un nuovo kernel di tipo Unix sviluppato dallo studente finlandese Linus Torvalds nasce il sistema operativo Linux



La nascita di Linux (2)

Da <http://it.wikipedia.org/wiki/Linux> e voci correlate:

«Linux vede la luce nel 1991 grazie al giovane studente finlandese Linus Torvalds che, appassionato di programmazione, era insoddisfatto del sistema operativo Minix (sistema operativo unix-like destinato alla didattica, scritto da Andrew Tanenbaum, professore ordinario di Sistemi di Rete all'università di Amsterdam), poiché supportava male la nuova architettura i386 a 32bit, all'epoca tanto economica e popolare. Così Linus decise di creare un kernel unix con lo scopo di divertirsi e studiare il funzionamento del suo nuovo computer, che era appunto un 80386.



Torvalds e altri sviluppatori della prima ora di Linux adattarono il loro kernel perché funzionasse con i componenti GNU ed i programmi in user-space per creare un sistema operativo completo, pienamente funzionante e libero.

Nella primavera del 1992 l'hacker Orest Zborowski riuscì a rendere eseguibile il server X sulla versione 0.13 di Linux. Per far ciò Orest dovette implementare tutta la struttura degli Unix Domain Socket indispensabili a X Window e quindi un primo livello socket sul quale venne poi costruita tutta l'infrastruttura di rete di Linux.»

La nascita di Linux (3)

«Il 14 marzo 1994 il 16° livello di patch del kernel 0.99 divenne Linux 1.0. Fu lo stesso Linus Torvalds a presentare la prima versione stabile della sua creatura presso l'Università di Helsinki.

Oggi Torvalds continua a dirigere lo sviluppo dei kernel, mentre altre parti del sistema, come le componenti GNU, sono sviluppate separatamente. Il compito di fornire un sistema integrato, che combina tutte le componenti di base con le interfacce grafiche (come per esempio GNOME o KDE, che a loro volta si basano sulla presenza dell'X Window System) e con il software applicativo, viene ora svolto dalle distribuzioni [...] create da comunità di sviluppatori o società, che preparano e scelgono i pacchetti da includere.

Tutte le distribuzioni condividono il kernel di Linux, mentre si differenziano tra loro per il cosiddetto "parco software", cioè i pacchetti preparati e/o selezionati dagli sviluppatori per la distribuzione stessa, per il sistema di gestione del software e per i servizi di assistenza/manutenzione offerti.»

La figura successiva mostra lo sviluppo delle distribuzioni Linux dalle origini a oggi.

Aree di utilizzo di Linux

Attualmente Linux viene utilizzato praticamente su ogni classe di dispositivo hardware programmabile: soluzioni embedded (cellulari, palmari, router), laptop e desktop, server dipartimentali ed enterprise, cluster ad elevata affidabilità, mainframe, supercomputer.

Anche se oggi Linux è ormai maturo per un utilizzo generalizzato per applicazioni di produttività personale, storicamente l'area di maggior utilizzo è sempre stata quella dei server. A fine 2006 Netcraft riportava l'utilizzo di Linux sui web server di otto tra le dieci società di hosting più affidabili.

Linux è la base della piattaforma di hosting più diffusa, denominata LAMP (Linux, Apache, MySQL, PHP [/Perl/Python]) la cui popolarità tra gli sviluppatori ha portato al rilascio di molti prodotti Open Source nell'area della gestione dei contenuti e delle applicazioni web in genere.

Riguardo al segmento dei supercomputer, a fine 2007 oltre l'85% dei 500 sistemi più potenti utilizzava Linux.

Caratteristiche auspicabili di una distribuzione per server (1)

Le distribuzioni sono costituite da un elevato numero di pacchetti di installazione dei vari moduli e applicazioni software; i pacchetti contengono file binari compilati per la piattaforma hardware target (Linux ha ereditato da Unix l'approccio "multi-piattaforma") e corrispondenti ai sorgenti liberamente disponibili.

Per rispettare la licenza GNU GPL chi prepara e pubblica una distribuzione deve rendere disponibili anche i sorgenti di tutte le applicazioni, in un formato adeguato a riprodurre le applicazioni stesse; la disponibilità di pacchetti in formato binario è però fondamentale per rendere veloce e affidabile l'installazione.

La ricchezza del corredo di applicazioni precompilate e la loro varietà (ampia gamma di ambiti applicativi) è una caratteristica molto importante a favore della scelta di una distribuzione, perché rende raro il caso in cui è necessario installare pacchetti "generici" non appartenenti alla distribuzione, o compilarli in proprio partendo dai sorgenti. E' anche importante che le applicazioni vengano preconfigurate con default "ragionevoli" in modo da minimizzare l'esigenza di modificare le configurazioni per avere un sistema realmente utilizzabile.

Caratteristiche auspicabili di una distribuzione per server (2)

La community che sta dietro a una distribuzione non commerciale è un altro fattore fondamentale: se è numerosa, ben organizzata e motivata si può prevedere un'evoluzione nel tempo della distribuzione tale da mantenerla aggiornata e quindi sempre adeguata agli usi per cui si è scelta.

Un'altra esigenza fondamentale è la garanzia di aggiornamenti frequenti dei pacchetti di installazione, sia a seguito di rilasci di nuove versioni e di bug fixing sia soprattutto ogni qual volta emerga un security advisory tale da rendere possibile la compromissione di un sistema non aggiornato.

La produzione di pacchetti aggiornati e la loro distribuzione efficiente tramite mirror su scala geografica (tale da soddisfare senza attese la base di utenza) è un punto critico, perché richiede sia risorse umane (persone dedicate alla manutenzione dei pacchetti) sia risorse materiali (infrastrutture in termini di server e reti di comunicazione).

Una distribuzione che lascia all'utente la responsabilità di curare in proprio la ricerca e l'installazione degli aggiornamenti di sicurezza può essere un utile strumento didattico o un hobby per un appassionato, ma è da rifuggire in ambienti di produzione.

Perché Fedora (1)

da <http://fedoraproject.org>

«*Fedora è un sistema operativo basato su Linux che presenta gli ultimissimi software liberi ed open source. L'uso, la modifica e la distribuzione di Fedora è sempre libero per chiunque. E' creato da persone in tutto il mondo che lavorano assieme come una comunità: il Fedora Project. Il Fedora Project è aperto a chiunque e di chiunque è benvenuta la partecipazione.*»



La distribuzione Fedora nasce nel 2003 da una “costola” di Red Hat, una delle più note distribuzioni commerciali, che fino a quel momento aveva mantenuto una versione di libera distribuzione. La nascita di Fedora (inizialmente “Fedora Core”) segna la diversificazione tra il prodotto commerciale RHEL (Red Hat Enterprise Linux) e la distribuzione libera, sviluppata e mantenuta dalla community denominata “Fedora Project”.

Perché Fedora (2)

Il legame tra le due linee di attività resta comunque molto stretto, come si legge su <http://fedoraproject.org/wiki/Overview>

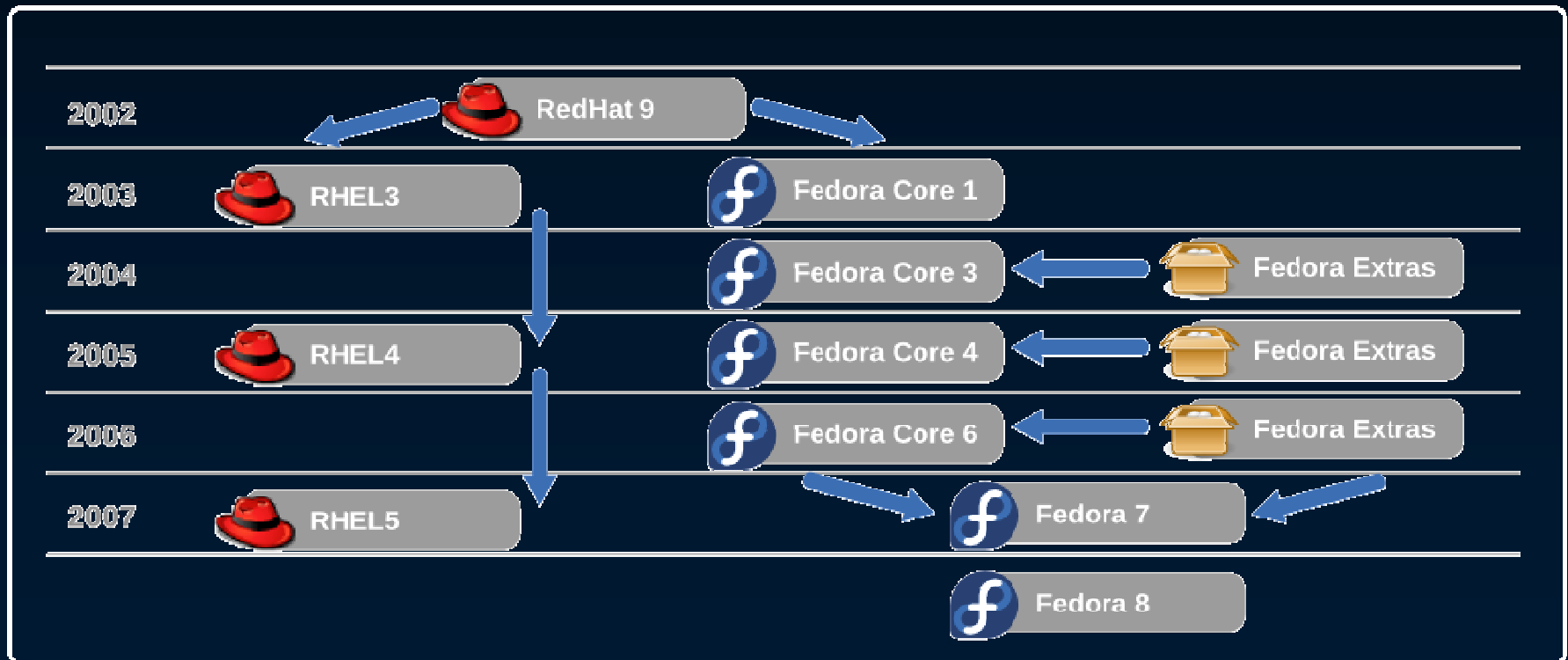
«Gli sviluppatori di Fedora contribuiscono attivamente a diverse centinaia di progetti software open source, tra cui elementi essenziali di Linux e componenti free software. Questi elementi comprendono il kernel di Linux, la libreria glibc, GNOME e molte altre librerie di sistema e infrastrutture amministrative. Red Hat, lo sponsor di Fedora Project, continua a investire milioni di dollari non solo sviluppando free software ma anche acquistando prodotti nati con licenze proprietarie e donandoli alla comunità del software open source.»

La collaborazione tra Red Hat e Fedora Project fornisce benefici reciproci: Fedora Project ha il supporto di un'azienda commerciale con risorse finanziarie e infrastrutturali utili allo sviluppo, all'aggiornamento e alla distribuzione di un vasto corredo software, mentre Red Hat utilizza la community di Fedora come un laboratorio di sviluppo e un incubatore di nuove tecnologie, con un'organizzazione snella e tempi di risposta rapidi.

Questo è anche evidenziato dai diversi cicli di vita dei rispettivi prodotti: RHEL viene rilasciato ogni due anni e viene supportato per sette anni, mentre Fedora viene rilasciato ogni sei mesi e viene supportato per poco più di un anno.

Perché Fedora (3)

Scegliere Fedora significa quindi avere un sistema costantemente aggiornato e con la disponibilità di un corredo software comprendente anche pacchetti di recentissimo rilascio, al "costo" di un aggiornamento almeno annuale dell'installazione, che comunque può anche essere svolto in modo semiautomatico, senza fermare i servizi e da remoto.




Perché Fedora (4)

Chiaramente troverete nel mondo Linux chi vi dirà che altre distribuzioni, sia commerciali sia libere, sono migliori per una serie di ragioni certamente motivate. La scelta della distribuzione è in buona parte frutto della propria esperienza personale e dell'importanza relativa che ciascuno specialista dà ai vari aspetti del sistema.

E' bene comunque non perdere mai di vista le "caratteristiche auspicabili" che ho elencato in precedenza. La garanzia di aggiornamenti costanti, soprattutto quando è in gioco la sicurezza, è un punto irrinunciabile, e la chiarezza di idee nella linea di sviluppo e il suo mantenimento nel tempo è un'altra caratteristica che preserva gli investimenti fatti nel comprendere i dettagli della configurazione dei vari servizi da gestire.

Un altro punto fondamentale è la ricchezza del parco software disponibile: se la distribuzione che avete scelto vi costringe a gestire in proprio la compilazione, l'installazione e il costante aggiornamento nel tempo anche "solo" di cinque pacchetti software perché non forniti dalla distribuzione stessa (o disponibili in versioni meno che correnti), allora non avete scelto la distribuzione adatta per approntare uno o più server e gestirli in modo semplice e affidabile nel tempo.

Perché Fedora (5)

← → ↻ × 🏠  http://fedoraproject.org/wiki/ElioTondo


fedora
wiki

Search Titoli Testo

[ElioTondo](#)

Elio Tondo

I live in Livorno (Tuscany - center of Italy). I hold a degree in Electronic Engineering from the University of Pisa (1982). I am currently working as a consultant in the areas of networking, system administration, architecture of IT systems. I began using Unix (V7) before graduating (1981) on a Zilog Z8000 development system. I am using Internet since 1988, before the birth of the Web: I was working for Olivetti, the major Italian IT company at the time, and they had a private link with their R&D group in Cupertino, CA. Later I switched to Linux (from the early times of kernel 0.98 without TCP/IP, using the SLS distro at the beginning, and later Slackware). Years later I switched to Red Hat, then Mandrake, and finally Fedora (Core 3). I am currently using Fedora on all the servers I manage, and I recommend Fedora to everybody is currently using other distributions. I especially like the availability of updates whenever they are required, the ease to install them automatically and the ability to do a major version upgrade remotely through yum. I have also experience in programming (C, PHP) and in the use and integration of open source software.



Contact

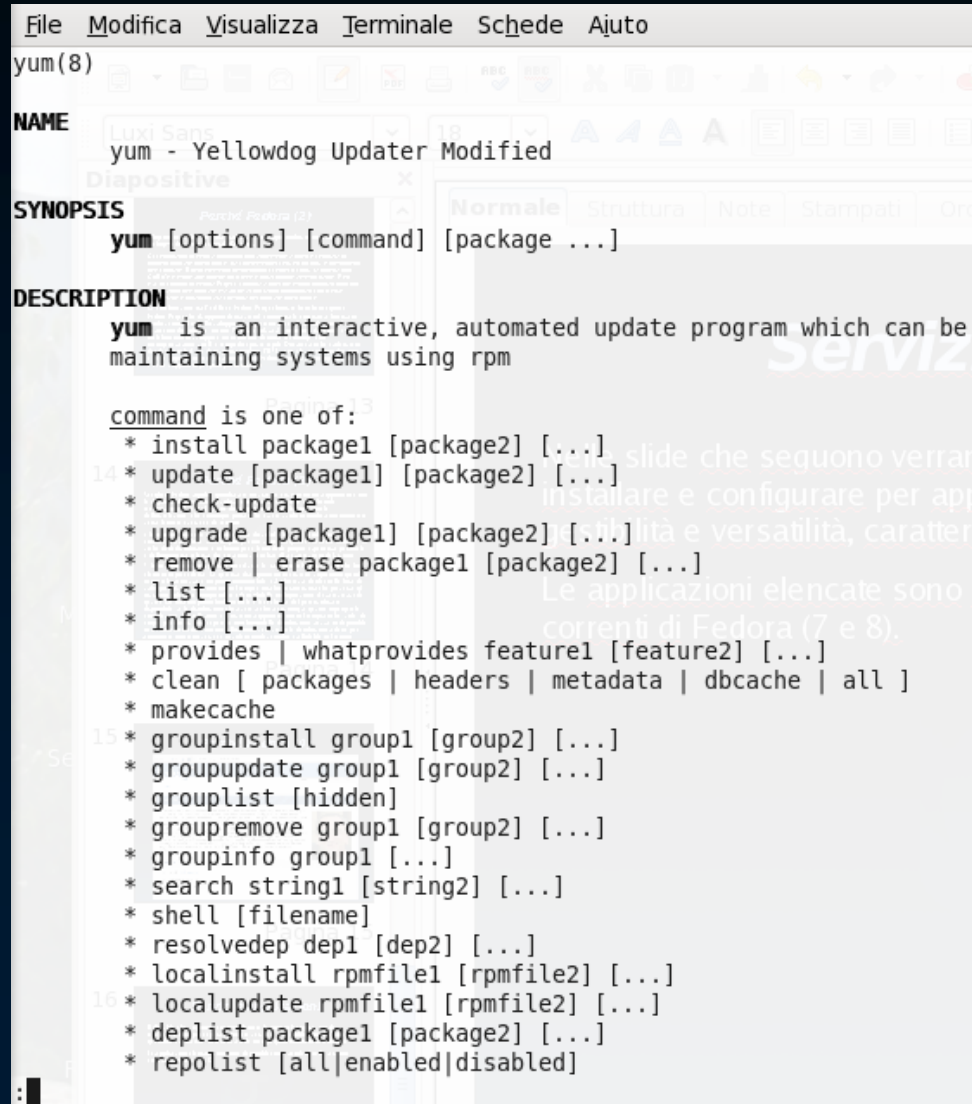
- ◉ **Email:** elio@tondo.it
- ◉ **GPG key:** CB019EF6
- ◉ **Fedora Account:** eliotondo
- ◉ **Skype:** eliotondo

Servizi e applicazioni

Nelle slide che seguono verranno elencate le principali applicazioni da installare e configurare per approntare server di rete multifunzionali di ottima gestibilità e versatilità, caratterizzati da un impegno amministrativo minimo.

Le applicazioni elencate sono tutte disponibili come standard nelle versioni correnti di Fedora (7 e 8).

Per la loro installazione è opportuno utilizzare il comando `yum`, che gestisce automaticamente la risoluzione delle dipendenze tra i vari pacchetti e può essere utilizzato anche per gli aggiornamenti.



```
File Modifica Visualizza Terminale Schede Aiuto
yum(8)
NAME
    yum - Yellowdog Updater Modified
SYNOPSIS
    yum [options] [command] [package ...]
DESCRIPTION
    yum is an interactive, automated update program which can be
    maintaining systems using rpm

    command is one of:
    * install package1 [package2] [...]
    * update [package1] [package2] [...]
    * check-update
    * upgrade [package1] [package2] [...]
    * remove | erase package1 [package2] [...]
    * list [...]
    * info [...]
    * provides | whatprovides feature1 [feature2] [...]
    * clean [packages | headers | metadata | dbcache | all ]
    * makecache
    * groupinstall group1 [group2] [...]
    * groupupdate group1 [group2] [...]
    * grouplist [hidden]
    * groupremove group1 [group2] [...]
    * groupinfo group1 [...]
    * search string1 [string2] [...]
    * shell [filename]
    * resolvedep dep1 [dep2] [...]
    * localinstall rpmfile1 [rpmfile2] [...]
    * localupdate rpmfile1 [rpmfile2] [...]
    * deplist package1 [package2] [...]
    * repolist [all|enabled|disabled]
```

Servizi e applicazioni Web & application server

httpd

Apache web server

php

Linguaggio di scripting

mysql (+ phpMyAdmin)

Database server e interfaccia di amministrazione

tomcat5

Java application server

awstats

Statistiche accessi web

vsftpd

FTP server



http://www

Servizi e applicazioni Firewall e sicurezza

shorewall

Firewall basato su iptables

denyhosts

Protezione contro attacchi brute-force

selinux

Controlli di accesso alle risorse

snort

Intrusion Detection System

yum-cron

Installazione automatica di aggiornamenti



Servizi e applicazioni

Rete locale e directory services

samba

*Server di rete SMB/CIFS
(interoperabilità Windows)*

cups

Common Unix Printing System

squid

Web & FTP proxy

amanda

*Backup (Advanced Maryland
Automatic Network Disk
Archiver)*

dhcpcd

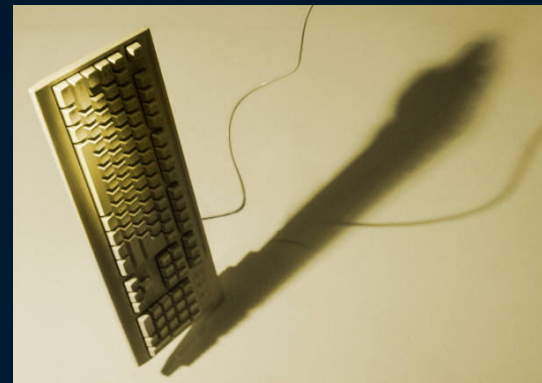
*Assegnazione automatica
indirizzi di rete*

bind

DNS server

openldap - fds

LDAP server



Servizi e applicazioni

Posta elettronica

postfix

Server SMTP

amavisd-new

*Interfaccia con antivirus e
antispam*

spamassassin

Antispam

clamav

Antivirus

sqlgrey

Greylisting (antispam)

dovecot

Server POP3 e IMAP

squirrelmail

Webmail

mailman

Gestore di mailing list



Servizi e applicazioni VoIP e messaggistica

asterisk

Centralino software VoIP

ser

SIP Express Router

ekiga

SIP softphone

jabberd

Server messaggistica Jabber



Servizi e applicazioni Virtualizzazione

xen

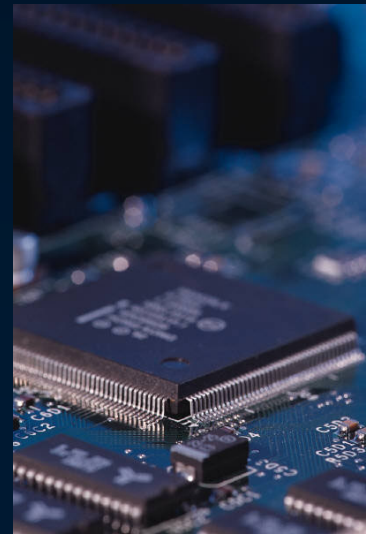
Xen Hypervisor

kvm

Kernel-based Virtual Machine

qemu

Processor emulator



Esempi di configurazione (1)

httpd

```
patch -l -p0 << "EoF"
--- /etc/httpd/conf/httpd.conf.00      2006-07-26 17:13:40.000000000 +0200
+++ /etc/httpd/conf/httpd.conf        2006-09-21 16:17:08.000000000 +0200
@@ -71,7 +71,7 @@
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
-KeepAlive Off
+KeepAlive On

#
# MaxKeepAliveRequests: The maximum number of requests to allow
@@ -323,7 +323,7 @@
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
-   AllowOverride None
+   AllowOverride All

#
# Controls who can get stuff from this server.
@@ -743,7 +743,7 @@
# in HTML content to override this choice, comment out this
# directive:
#
-AddDefaultCharset UTF-8
+#AddDefaultCharset UTF-8

#
# AddType allows you to add to or override the MIME configuration
@@ -988,3 +988,5 @@
#   ErrorLog logs/dummy-host.example.com-error_log
#   CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
+
+Include /etc/httpd/conf/vhost.conf
EOF
```

Esempi di configurazione (2)

shorewall

```
patch -l -p0 << "EOF"
--- shorewall-4.0.8-1.fc8/zones 2008-01-28 00:31:57.000000000 +0100
+++ shorewall/zones 2008-04-05 09:21:51.000000000 +0200
@@ -10,4 +10,5 @@
#ZONE TYPE OPTIONS IN OUT
# OPTIONS OPTIONS
fw firewall
+net
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
--- shorewall-4.0.8-1.fc8/interfaces 2008-01-28 00:31:57.000000000 +0100
+++ shorewall/interfaces 2008-04-05 09:22:07.000000000 +0200
@@ -8,4 +8,5 @@
#
#####
#ZONE INTERFACE BROADCAST OPTIONS
+net eth0 detect nosmurf, norfc1918
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
--- shorewall-4.0.8-1.fc8/policy 2008-01-28 00:31:57.000000000 +0100
+++ shorewall/policy 2008-04-05 09:22:20.000000000 +0200
@@ -9,4 +9,7 @@
#####
#SOURCE DEST POLICY LOG LIMIT: BURST
# LEVEL
+fw net ACCEPT
+net all DROP info
+all all REJECT info
#LAST LINE -- DO NOT REMOVE
--- shorewall-4.0.8-1.fc8/rules 2008-01-28 00:31:57.000000000 +0100
+++ shorewall/rules 2008-02-07 18:14:05.000000000 +0100
@@ -12,4 +12,16 @@
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
+ACCEPT net fw icmp
+ACCEPT net fw tcp ssh
+ACCEPT net fw tcp smtp
+ACCEPT net fw tcp pop3
+ACCEPT net fw tcp imap
+ACCEPT net fw tcp www
+ACCEPT net fw tcp https
+ACCEPT net fw tcp ftp
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
EOF
```

Esempi di configurazione (3)

postfix

```
patch -l -p0 << "EoF"
--- /etc/postfix/main.cf.00  2006-09-01 18:47:45.000000000 +0200
+++ /etc/postfix/main.cf    2006-11-17 11:26:46.000000000 +0100
@@ -665,3 +665,33 @@
 # readme_directory: The location of the Postfix README files.
 #
 readme_directory = /usr/share/doc/postfix-2.4.5/README_FILES
+
+owner_request_special = no
+virtual_maps = hash:/etc/postfix/virtual
+
+header_checks = regexp:/etc/postfix/header_checks
+
+smtpd_client_restrictions =
+
+smtpd_helo_required = yes
+smtpd_helo_restrictions =
+
+smtpd_sender_restrictions =
+
+smtpd_recipient_restrictions = permit_mynetworks,
+ permit_sasl_authenticated,
+ reject_unauth_destination,
+ reject_invalid_hostname,
+ reject_unauth_pipelining,
+ reject_non_fqdn_sender,
+ reject_unknown_sender_domain,
+ reject_non_fqdn_recipient,
+ reject_unknown_recipient_domain,
+ reject_rbl_client sbl-xbl.spamhaus.org,
+ reject_rbl_client list.dsbl.org,
+ check_policy_service inet:127.0.0.1:2501
+
+smtpd_sasl_auth_enable = yes
+smtpd_sasl_security_options = noanonymous
+broken_sasl_auth_clients = yes
+
EoF
```

Conclusione

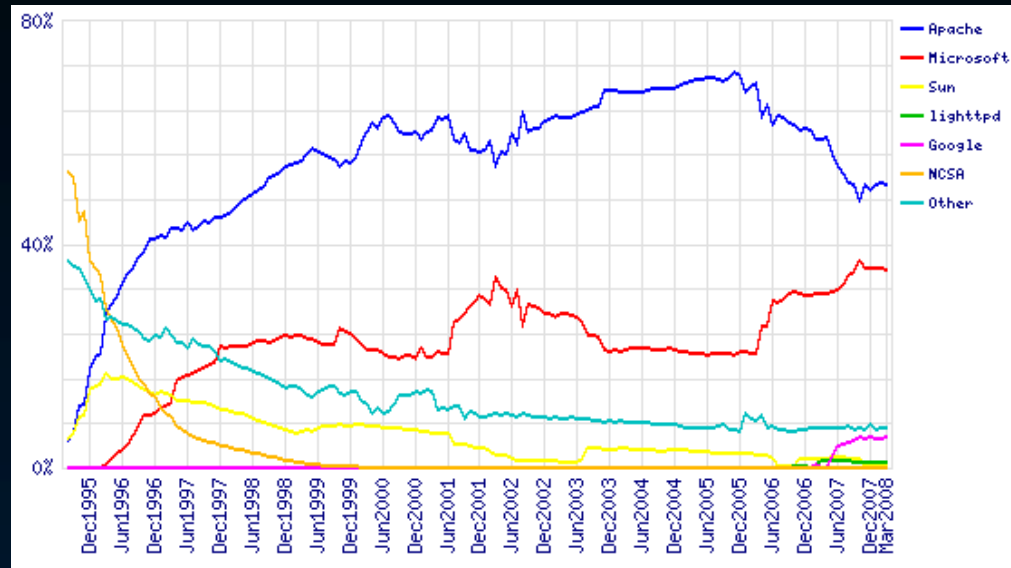
Dovrebbe essere chiaro, a questo punto, che le soluzioni Open Source consentono di approntare server di rete multifunzionali a costo zero come licenze software e con caratteristiche estremamente competitive.

Un esempio per tutti: il "market share" del web server Apache

(fonte *Netcraft Web Server Survey*: <http://news.netcraft.com>)

Spesso, quando si espongono questi argomenti, si tende a partire dalla considerazione che il primo aspetto appetibile è il fatto di non avere costi di licenze, e si prosegue cercando di convincere l'interlocutore che, malgrado questo, si riesce comunque a ottenere sistemi validissimi e affidabili. Questo approccio "difensivo" sminuisce i meriti dell'Open Source.

E allora, diciamo chiaramente come stanno le cose...



Microsoft just gives
you Windows...



Linux gives you the
whole house.

You never own a copy of Windows. You simply license it from Microsoft. But with Open Source Linux, you OWN your operating system! You can copy, sell, and install Linux as many times as you want, for free. And of course, you're getting the finest Operating System out there because people can see the code behind Linux, and suggest changes to make your experience better.

With Windows, you need to buy software like Microsoft Office. Why spend hard earned cash on Office when you can get a powerful, intuitive open source projects like Open Office? Use built-in Linux software catalogues like Ubuntu's Synaptic to find over 20,000 free pieces of safe software for the Linux desktop.



Think Free
Think Linux



fedora

*Grazie per
l'attenzione*

elio.tondo@mensa.it