Sometimes they come back...

Dieci anni di supporto Linux nelle sezioni:

alcune considerazioni sull'esperienza del

(fu?) Gruppo Linux,

un'indagine dal vivo ed una non-proposta.

(ovvero: molta filosofia e poca tecnica)

Luca Carbone – Sez. Milano Bicocca

Il Gruppo Linux

- Nasce nel ~99 con ~30 interessati/potenziali partecipanti, ridottisi quindi ufficialmente a 18 (per ~2FTE complessivi). Finalita' (*verbatim*):

•Creazione e manutenzione di una distribuzione di Linux per l'INFN che risponda ai requisiti fondamentali di sicurezza e facilita' di installazione e gestione. La distribuzione verra' progettata in relazione alle esigenze dell'Ente e sara' disponibile in varie taglie che, pur offrendo le medesime funzionalita' di base, si distingueranno per la ricchezza delle opzioni disponibili. Sara' inoltre compito del Gruppo aggiornare la distribuzione e curarne l'integrita' e la sicurezza (avvalendosi della collaborazione del Gruppo Security). La distribuzione verra' resa disponibile via AFS; per questo scopo verra' creato e mantenuto un albero apposito.

•Progettazione e sviluppo di procedure per l'installazione e la configurazione automatica di Linux; il Gruppo si concentrera' in particolare sulle procedure di installazione automatica (non assistita) e sulle tecniche di gestione e controllo remoti del parco installato.

•Definizione di una piattaforma hardware standard per l'installazione di Linux sulla quale verra' garantito il corretto funzionamento della distribuzione. Sulla base di prove effettuate nelle varie Sezioni partecipanti verra' stilata una lista di massima delle periferiche (schede di rete, schede video etc. etc.) di cui e' raccomandato l'acquisto.

•Gestione di una macchina pubblica (ad uso esclusivo dell'INFN) su cui installare e provare pacchetti software particolari (compilatori, ambienti di sviluppo, Suite di Office Automation) per valutarne l'utilita' e la rispondenza alle necessita' dell'Ente.

•Realizzazione e gestione di un sito Web sul quale raccogliere documentazione, informazioni, manuali, software di pubblica utilita' e FAQ realizzate dal gruppo stesso. Questo sito si propone come sorgente primaria e preferenziale di informazioni sulle procedure di installazione e gestione di Linux all'interno dell'INFN. Contestualmente al sito Web verra' creata una mailing list espressamente dedicata al Linux Management (lx-manager@infn.it).

•Studio dell'integrazione di Linux in servizi distribuiti di nuova generazione; ci si propone in particolare di verificare la possibilita' di utilizzare un DS (es.: LDAP) per i servizi base di autenticazione e gestione utenze (in stretta collaborazione con il gruppo sui Directory Services).

Modello proposto

- RedHat servita via rete (NFS, HTTP); installazione non assistita tramite kickstart con configurazione su floppy disk da consegnare all'utente;
- Distribuzione custom in varie taglie/sapori (small, medium, large, Sezione, Gruppo/EXP, ...), mantenuta centralmente ed aggiornata automaticamente sul server, comprensiva di pacchetti non standard di uso comune (CERNlib, root, Condor, AFS, acrobat reader, print client, ...);
- Configurazione completa della macchina 'chiavi in mano' orientata alla sicurezza (mostly closed: tcp_wrappers, solo servizi fondamentali/necessari attivi, iptables, ...); gestione account tramite DB centrale, prevista integrazione con DS;
- Gestione remota tramite ssh (installazione automatica di chiave pubblica di un management server centrale non accessibile dall'esterno); script (a-la cluster manager VMS) per aggiornamenti globali; no aggiornamenti automatici; syslog centralizzato;
- Test compatibilita' H/W & S/W su macchine dedicate gestite dal gruppo.

Cosa NON HA funzionato

- La distribuzione e' sbarcata ufficialmente (comunicazione in CCR) su AFS nel corso del 2001: **solo 1 (una) persona ha chiesto informazioni**, poi il gruppo e' stato sostanzialmente dimenticato (ma l'attivita' nelle singole sezione e' proseguita). Perche'?
  - Scarso interesse di base (e non solo)? Probabilmente il gruppo e' nato dalle esigenze pressanti di alcune sezioni le quali, una volta messo a punto uno strumento utilizzabile per la produzione, hanno iniziato ad usarlo con qualche soddisfazione (continuando a svilupparlo in qualche caso);
  - **Difficolta' oggettiva** nello sviluppo di soluzione standard;
  - **Diffidenza oggettiva** verso soluzione standard (meglio/piu' comodo utilizzare competenze locali - dove esistono - e strumenti sviluppati a misura della situazione locale): modello troppo generale? troppo specifico?
  - **Mancanza oggettiva di tempo e risorse per la produzione di documentazione**
    - ma disponibilita' – non sfruttata - a diffondere know-how ed esperienza...;
  - ... altro?

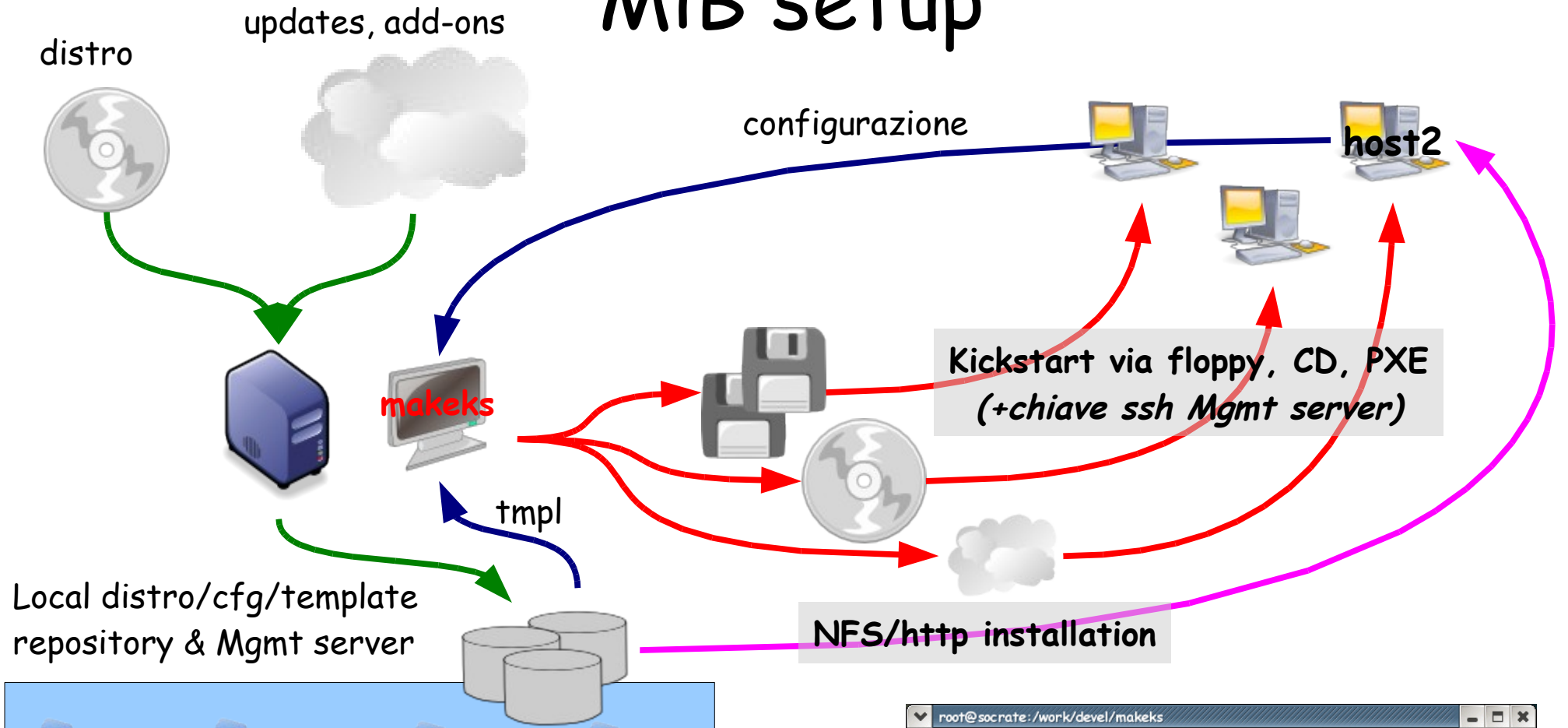
Cosa HA funzionato

- Una piccola indagine (limitata al campione – ristretto - delle sezioni allora presenti nel gruppo) ha rivelato che:
  - in alcune sezioni il modello delineato e' tuttora in produzione (kickstart via PXE da repository locale); la distribuzione ufficiale e' di norma SL; i portatili in genere vengono supportati (o sopportati) senza troppo entusiasmo - c'e' un certo interesse per Ubuntu;
  - dove la manodopera e' un problema (scarsita' di personale) il supporto e' su base best-effort, senza alcuna infrastruttura centrale attiva;
  - alcune sezioni lasciano completa liberta' di scelta all'utente (per via dell'assenza di uno standard de-facto); una offre supporto (con un modello di gestione simile a quello delineato) tramite personale part-time con contratto esterno;
  - In genere non e' previsto alcuno strumento di gestione centralizzata (tranne – in qualche caso - un syslog server per il controllo a l'analisi post-mortem)
- In sintesi: grande e' la confusione sotto al cielo – la situazione e' eccellente.

Cosa HA funzionato: Mi e MiB

- In produzione dal ~2000: qualche centinaio di macchine (server, ws, portatili) installate con personalizzazioni per gruppo/utente (anche dual-boot) e gestite con basso impegno e pochissimi problemi di sicurezza;
- Distribuzioni supportate nel tempo (a volte contemporaneamente) con la medesima architettura di base:
  - RedHat 5.2, 6.2, 7.2-7.3, 8, 9; Fedora Core 1, 3, 4, 6, 7, 8; CentOS 5, 5.1; SLC 3.05, 4.4, 5.1.
- Creazione kickstart mediante perl script template-driven (per gruppo o esperimento o distribuzione); archivio permanente configurazioni; inizialmente auth *distribuita a mano* (*poor man LDAP*: passwd/group centrali -> db utenze), in seguito supporto LDAP; media di installazione: floppy -> CD R/RW -> PXE;
- Gestione parco mediante distribuzione chiave SSH di un server di mgmt centrale; syslog centralizzato; aggiornamenti semi-automatici
- Strumenti di gestione/aggiornamento delle distribuzioni sviluppati ad hoc.
- No piattaforma H/W standard, ma consulenza acquisto e piccolo magazzino di parti supportate (schede video, rete, audio) e pezzi di ricambio (PSU, dischi, ...).

MiB setup




```
root@socrate:/work/devel/makeks
File  Edit  View  Terminal  Tabs  Help
[root@socrate makeks]# ./nmakeks --help
Usage: makeks [OPTIONS] <hostname|filename> [ <hostname|filename> ...]
Create kickstart configuration file

       --force     force delete old .cfg & .img files
       --cgi       for use in CGI scripts
       --ldap      get user/group info from LDAP server
       --config    create host config tree
       --split     create 'split' ks file
       --stdin     read host config options from stdin
       --iso       create an ISO9660 bootable KS image
       --nolookup  don't perform DNS lookup

[root@socrate makeks]#
```

makeks

Lavori in corso

- Nonostante nel complesso l'architettura sviluppata abbia dato buona prova di se' in termini di flessibilita', efficienza e comodita', alcuni suoi punti deboli (ad es. il ciclo di gestione delle distribuzioni, rimasto piuttosto rozzo) ci hanno spinto a pensare come migliorarla.
- Redhat, dopo avere pressoche' ignorato per anni uno strumento potente come il kickstart, ha iniziato a sviluppare e rendere disponibili una serie di tool particolarmente interessanti:
  - **Cobbler/Koan**: OS provisioning and profile management
  - **Func**: a secure, scriptable remote control framework & API
  - **Augeas**: a configuration editing tool and API
  - **FreeIPA**: an integrated security information management solution combining Linux, Fedora DS, MIT Kerberos, DNS, ...

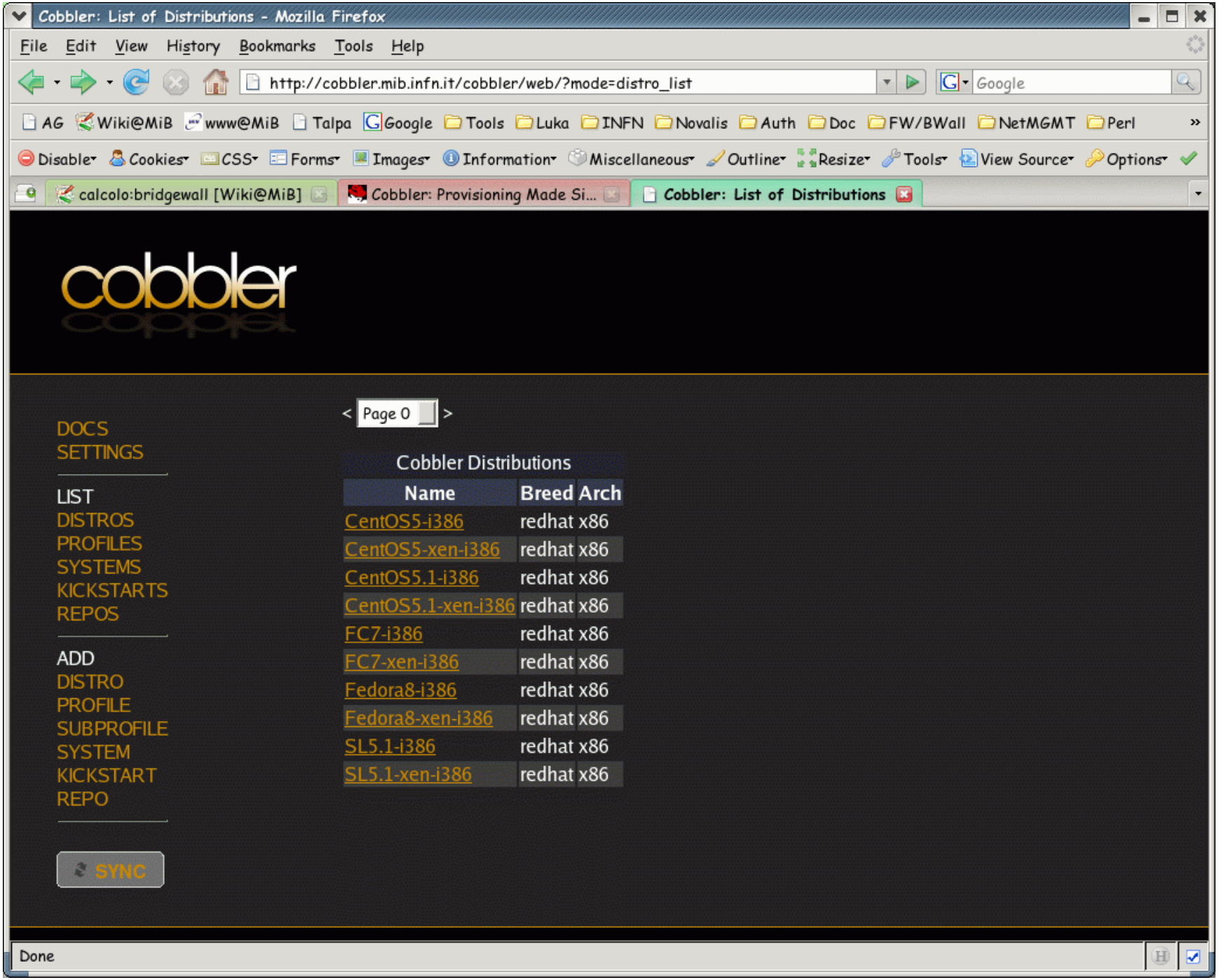
COBBLER: provisioning made simple

(eravamo in anticipo sui tempi...)

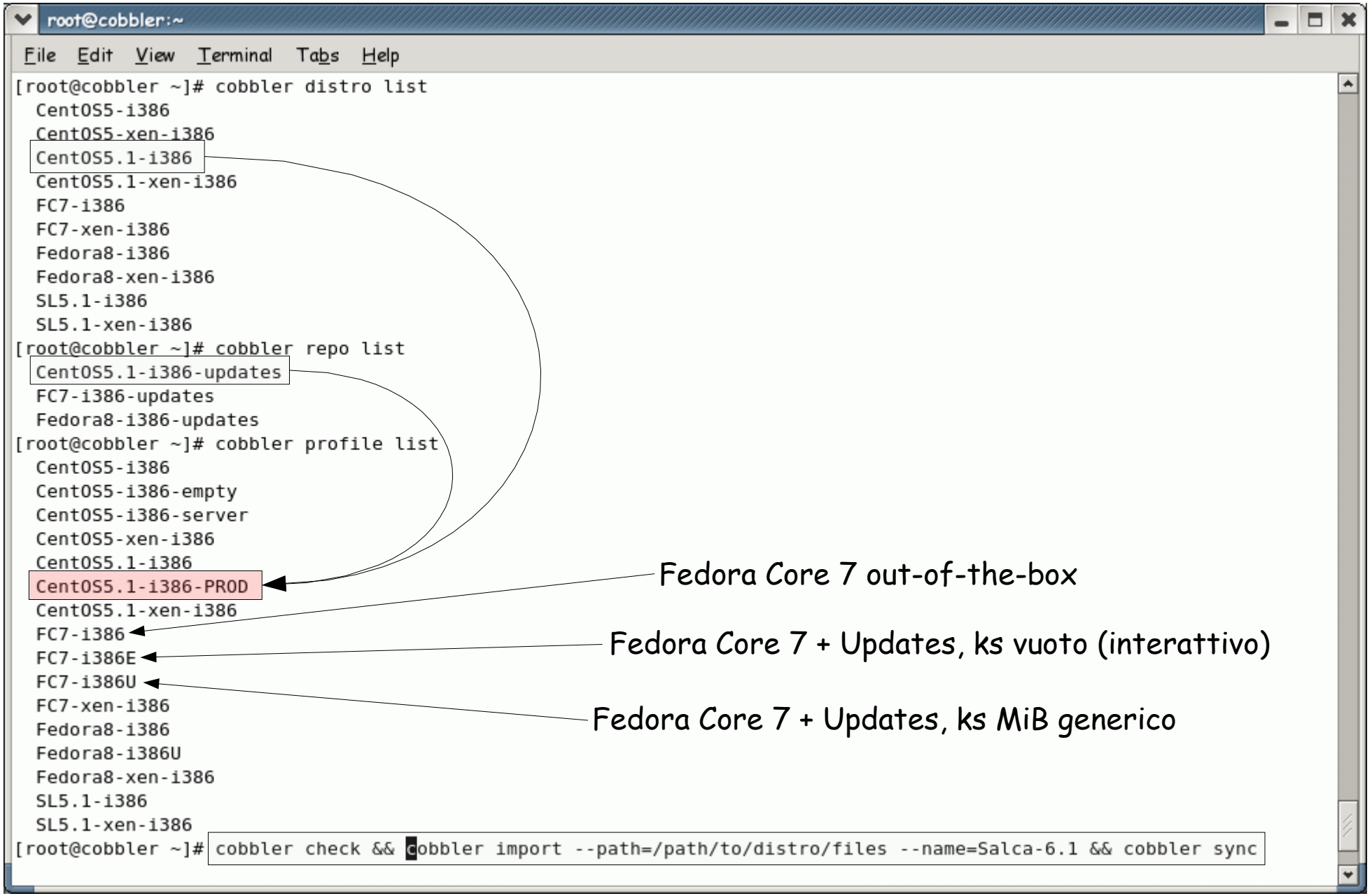
About Cobbler *(from http://cobbler.et.redhat.com/)*

Cobbler is a Linux provisioning server that allows for rapid setup of network installation environments. With a simple series of commands, network installs can be configured for PXE, reinstallations, and virtualized installs using Xen or KVM. Cobbler uses a helper program called 'Koan' (which interacts with Cobbler) for reinstallation and virtualization support.

- Focus on:
  - **DISTRO**: distribuzioni
  - **REPO**: repository aggiuntive (uptades, add-ons, ...)
  - **PROFILE**: configurazioni/profili personalizzati (per gruppi di macchine)
  - **SYSTEM**: configurazioni per i singoli sistemi
  - **KICKSTART**: file associati ai vari profili/sistemi (w/templates system)
- Gestione integrata DHCP server (volendo DNS) con installazione one-shot
- Ora alla versione 1.0, e' estremamemente comodo, efficiente e veloce.


Cobbler: List of Distributions - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://cobbler.mib.infn.it/cobbler/web/?mode=distro_list
Google
AG Wiki@MiB www@MiB Talpa Google Tools Luka INFN Novalis Auth Doc FW/BWall NetMGMT Perl
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
calcolo:bridgewall [Wiki@MiB]
Cobbler: Provisioning Made Si...
Cobbler: List of Distributions
cobbler
DOCS
SETTINGS
LIST
DISTROS
PROFILES
SYSTEMS
KICKSTARTS
REPOS
ADD
DISTRO
PROFILE
SUBPROFILE
SYSTEM
KICKSTART
REPO
SYNC
< Page 0 >
Cobbler Distributions
Name Breed Arch
CentOS5-i386 redhat x86
CentOS5-xen-i386 redhat x86
CentOS5.1-i386 redhat x86
CentOS5.1-xen-i386 redhat x86
FC7-i386 redhat x86
FC7-xen-i386 redhat x86
Fedora8-i386 redhat x86
Fedora8-xen-i386 redhat x86
SL5.1-i386 redhat x86
SL5.1-xen-i386 redhat x86
Done

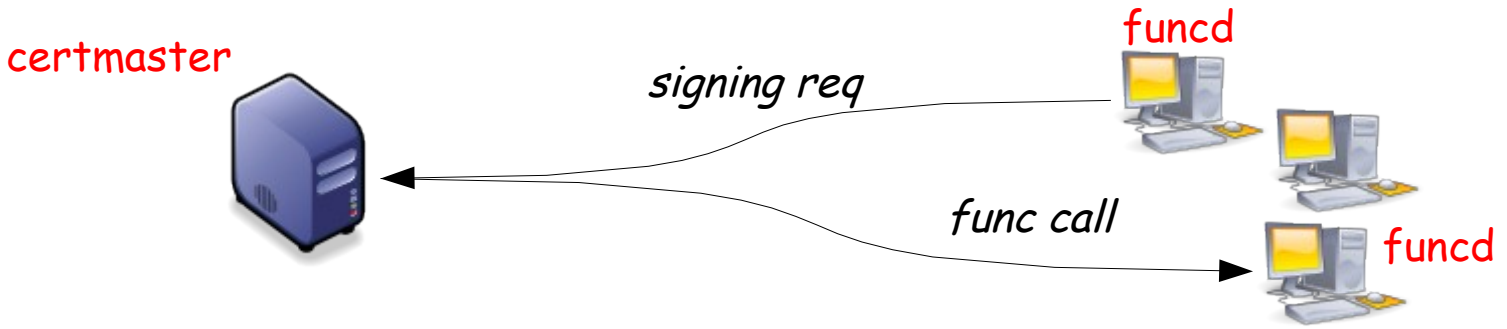
Cobbler via command-line



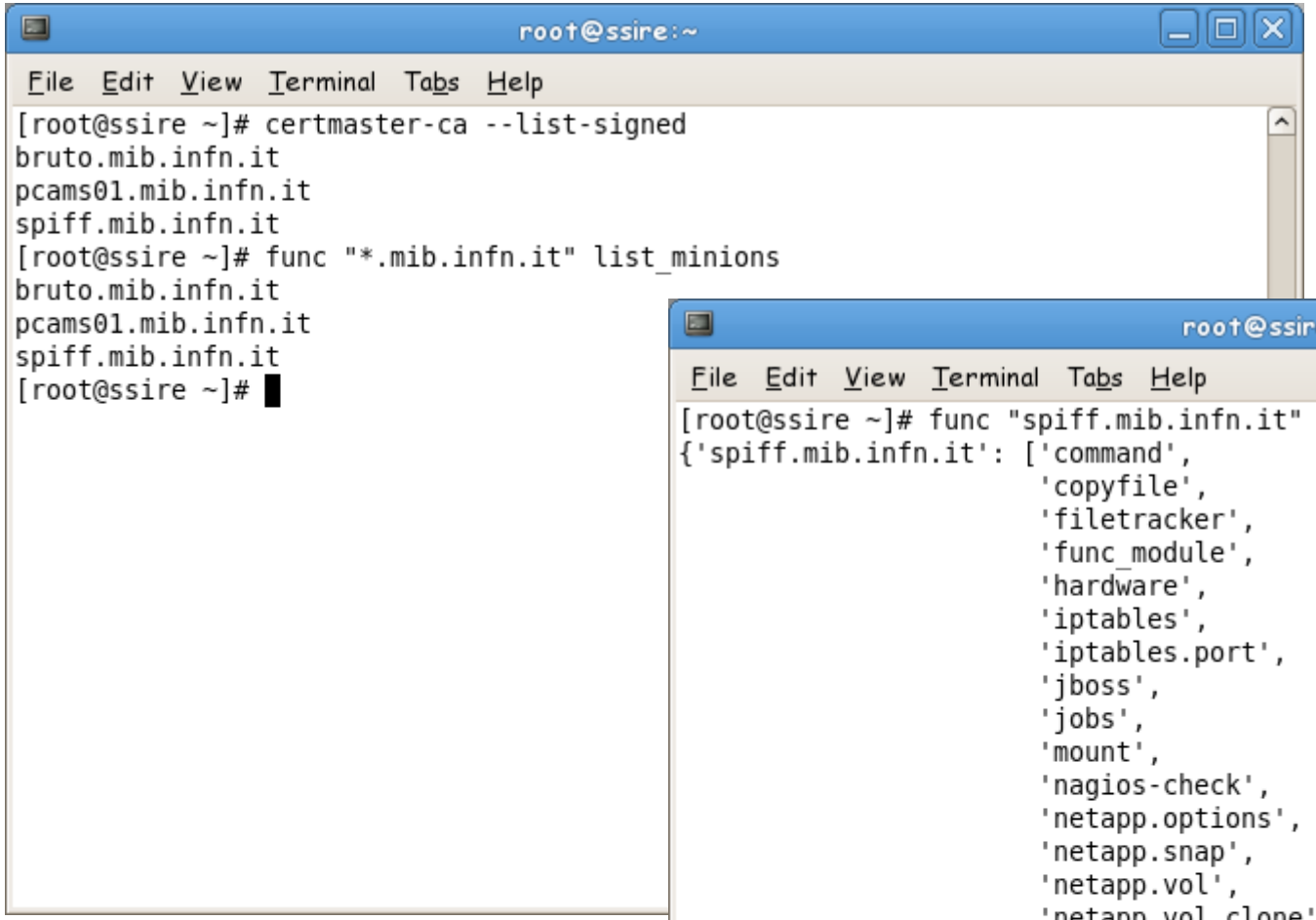
func: fedora unified network controller

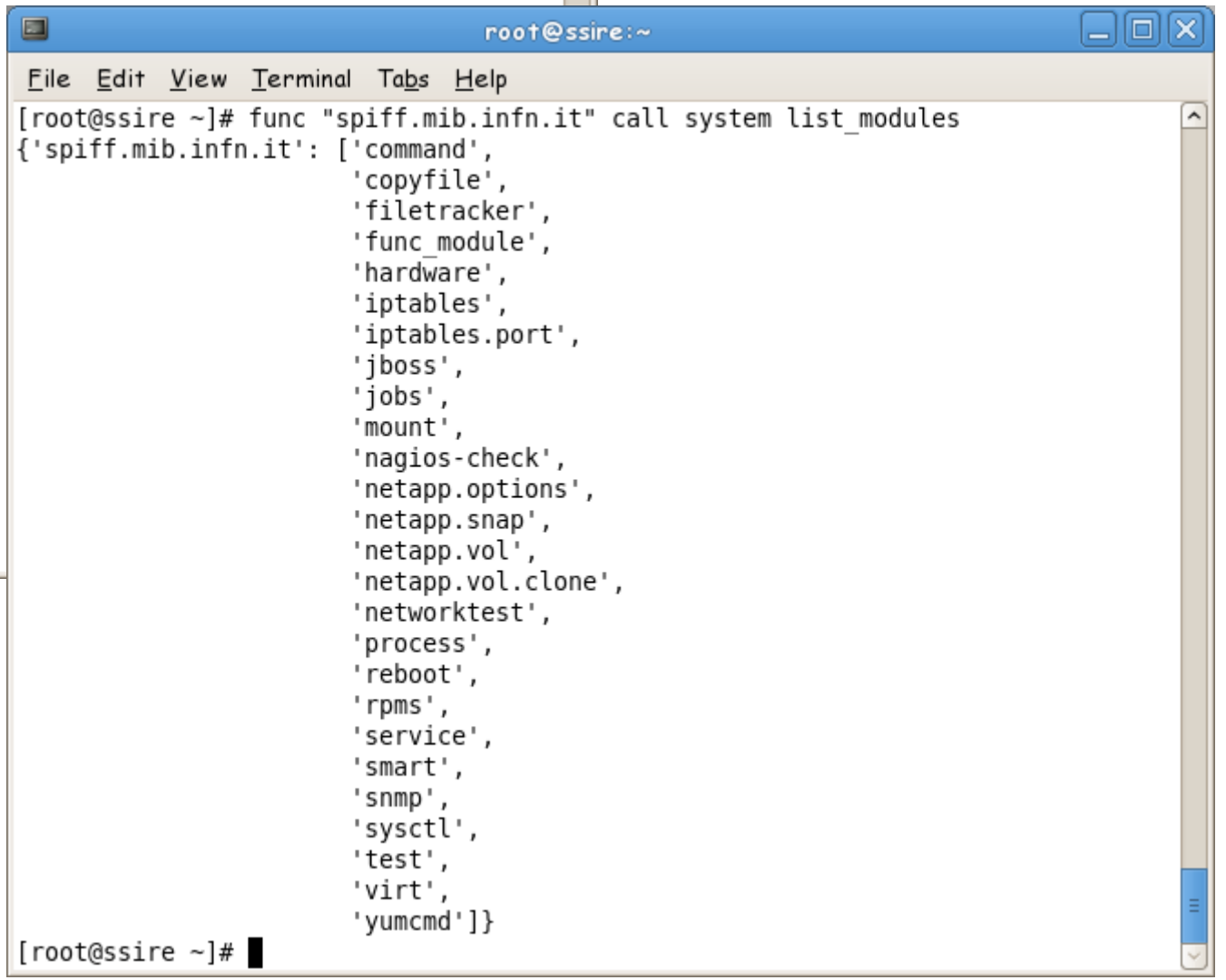
A lot of programs, systems, and tools need some way to communicate. Func provides a two-way authenticated system for generically doing these sort of things. You can build your own applications on top of it, and easily expand func by adding in additional modules, whether you want these to work through the func command line or by means of some other application. If you just want to use the func command line, that's great. If you want to build apps on the func tools, that's great too. If this sounds generically vague, it's only because it really is that expandable.

- L'autenticazione tra server e client avviene mediante scambio di certificati gestito da **certmaster** (altro tool sviluppato da Redhat) – la firma di un *client certificate* da parte del server puo' essere automatica o manuale;
- Scritto in Python, nasce gia' con una nutrita serie di moduli di interesse generale (H/W, mgmt, iptables, yum, network test, command, ...), e' espandibile a piacere, utilizzabile dalla command-line o in uno script;
- Gira su Fedora, Redhat, Centos, probabilmente SL; e' facilmente integrabile nel ks.



func in azione





Possibile evoluzione della struttura di gestione

- cobbler come repository manager/provisioning server:
  - A MiB e' in semi *produzione* da ~1 anno con buoni risultati; la completa integrazione nella struttura attuale e' in corso (si sta valutando se replicarla, o se utilizzare viceversa le ricche funzionalita' native di cobbler);
- func/certmaster come strumento di gestione sicura centralizzata:
  - La sua struttura modulare sembra ideale per la creazione di moduli di gestione manuale/automatizzata di uso comune.

I portatili

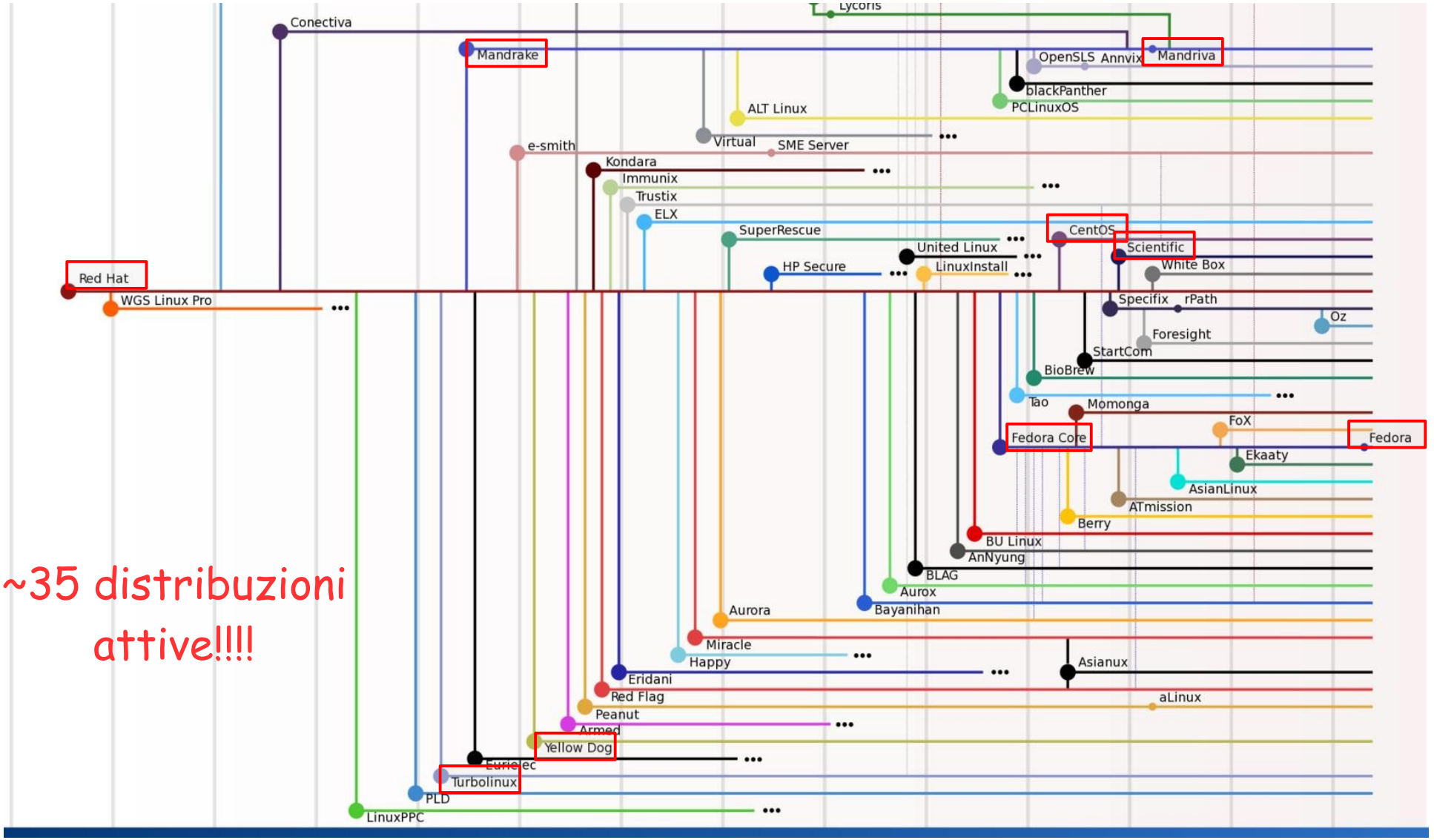
- A MiB vengono gestiti piu' o meno come i table-top, ma:
  - H/W esotico: necessitano quasi sempre delle distribuzioni (o dei kernel) piu' recenti per il supporto di tutte le periferiche (video, wireless, audio, suspend/hibernate) – esempio: sino a Fedora 8 il NetworkManager non era in grado di gestire il meccanismo di autenticazione di INFN-dot1x; con altre distribuzioni?
  - Dual-boot: oramai e' richiesto solo per questa classe di macchine, ed il rapporto con Vista pare piuttosto problematico; e' possibile definire un tool di virtualizzazione facile e comodo di uso comune? VirtualBox sembra una soluzione soddisfacente;
  - Fondamentale la circolazione delle informazioni: sarebbe utile raccoglierle ordinatamente in un sito centrale?

Conclusioni
(e piccolo questionario dal vivo...)

- In alcune sezioni sono in produzione da anni infrastrutture di installazione non assistita e gestione centralizzata di nutriti parchi macchine linux: l'esperienza accumulata puo' essere ancora interessante per l'INFN?
  - Quanti supportano pienamente Linux?
  - Quanti (al netto di PD, BO, MI, MIB, ROMA1) usano strumenti di installazione non assistita e gestione centralizzata del parco Linux?
  - Quali problemi/obbiettivi del '99 possono ancora essere considerati attuali? *(molti: scelta distribuzione, standardizzazione, sicurezza,...)*
  - **E' un'esigenza ancora sentita?**

Linux oggi: RedHat e famiglia

(mancano Debian/Ubuntu & Slackware/SuSe...)



~35 distribuzioni attive!!!!

Come eravamo: linuxbox.mi.infn.it