

XenINFN

Distribuzione Xen per la
realizzazione di servizi sicuri

Riccardo.Veraldi@cnafe.infn.it
Massimo.Donatelli@cnafe.infn.it

Xen



- Virtual Machine Monitor che consente l'implementazione di macchine virtuali
- Supporto per HVM
 - Intel VT
 - AMD-V
- Supporto SMP e HyperThreading
- OS guest su disco virtuale (file)
 - Supporto file sparse
- Accesso a partizioni fisiche
- Possibilita' di migrare le macchine virtuali su un altro host fisico (xm migrate)
- Coesistenza di sistemi a 64 e 32 bit sullo stesso hw



- Distribuzione Scientific Linux based (x86_64) orientata all'implementazione di servizi su macchine virtuali
- Ambiente di virtualizzazione uniforme basato su Xen 3.1
- Possibilita' di creare e ridistribuire macchine virtuali
- Implementazione e distribuzioni di servizi sicuri pre-confezionati (INFN Security Group)
 - DNS
 - Web Server
 - WiFi TINO web portal
 - Radius server

Evoluzione di XenINFN

- rpm Xen 3.1.x costruite a partire dai sorgenti (mercurial)
- SL5.0 kernel-xen costruito ad hoc con patch red-hat e rpm Xen 3.1.1 personalizzate
 - Soluzione non scalabile, difficile da mantenere, problema delle security patch
- SL5.0 kernel-xen costruito ad hoc con patch red-hat e rpm Xen 3.1.2 personalizzate
 - Difficile applicare le patch di sicurezza al kernel-xen, mantenimento difficoltoso e molto impegnativo
- SL5.1 kernel-xen di default e rpm Xen 3.1.2 personalizzate (src xen-3.1-testing-15502)
 - Soluzione ottimale, RHEL5.1 supporta le hypercall di Xen 3.1 direttamente nel kernel di default.

Requisiti hw per XenINFN

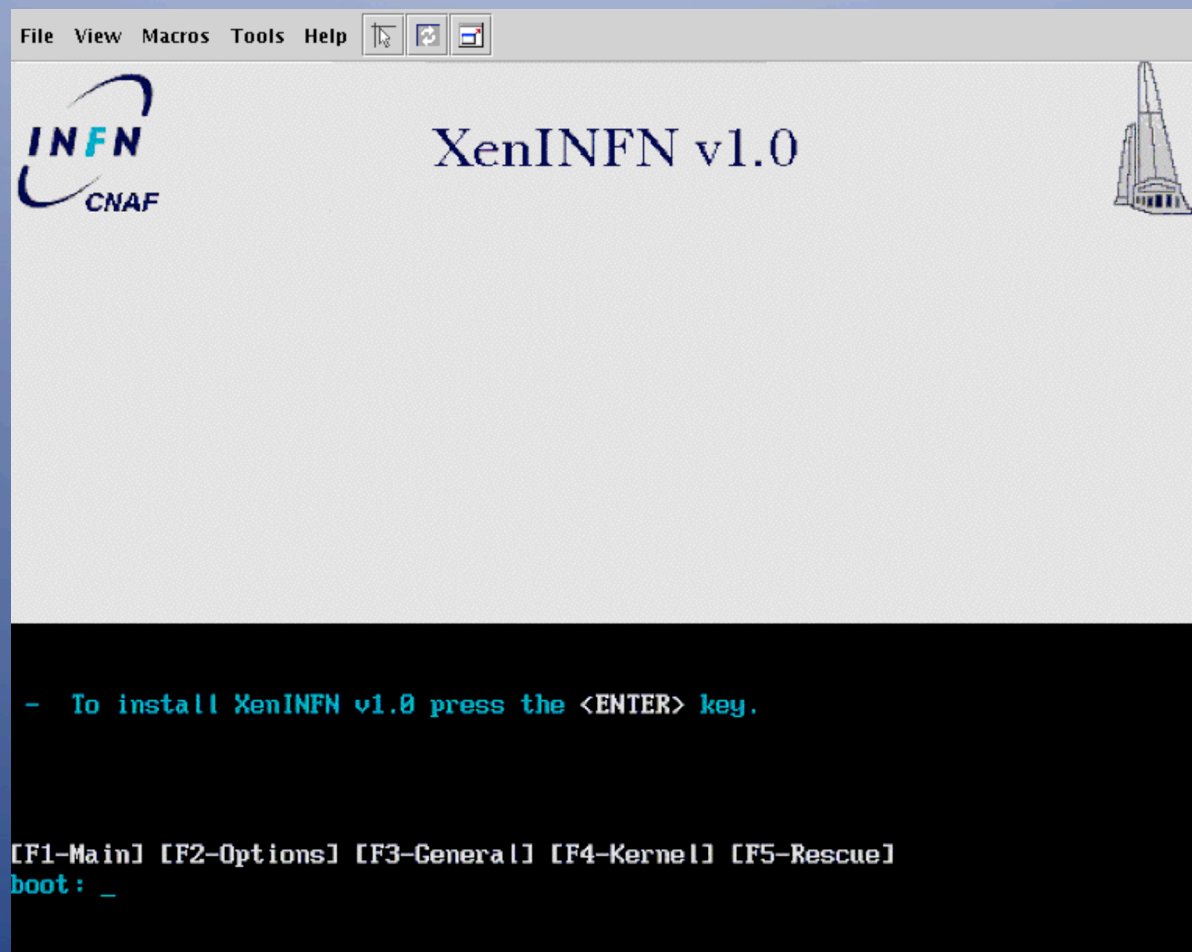


- CPU con architettura x86_64
- CPU con supporto hvm
 - Intel VT
 - AMD Pacifica Technology
- Almeno 1GB di RAM per Core
- Spazio su disco sufficiente per ospitare le macchine virtuali

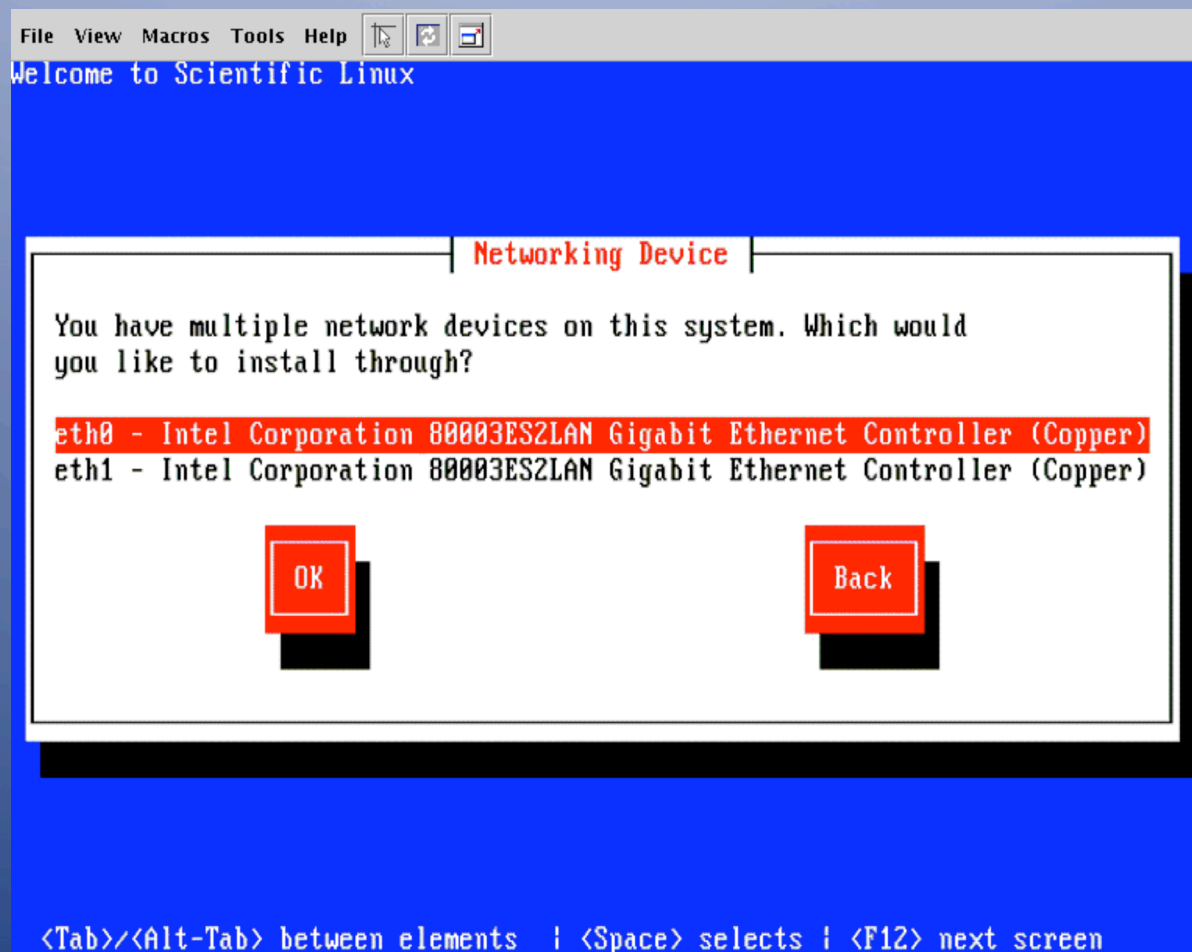
Installazione di XenINFN v1.0

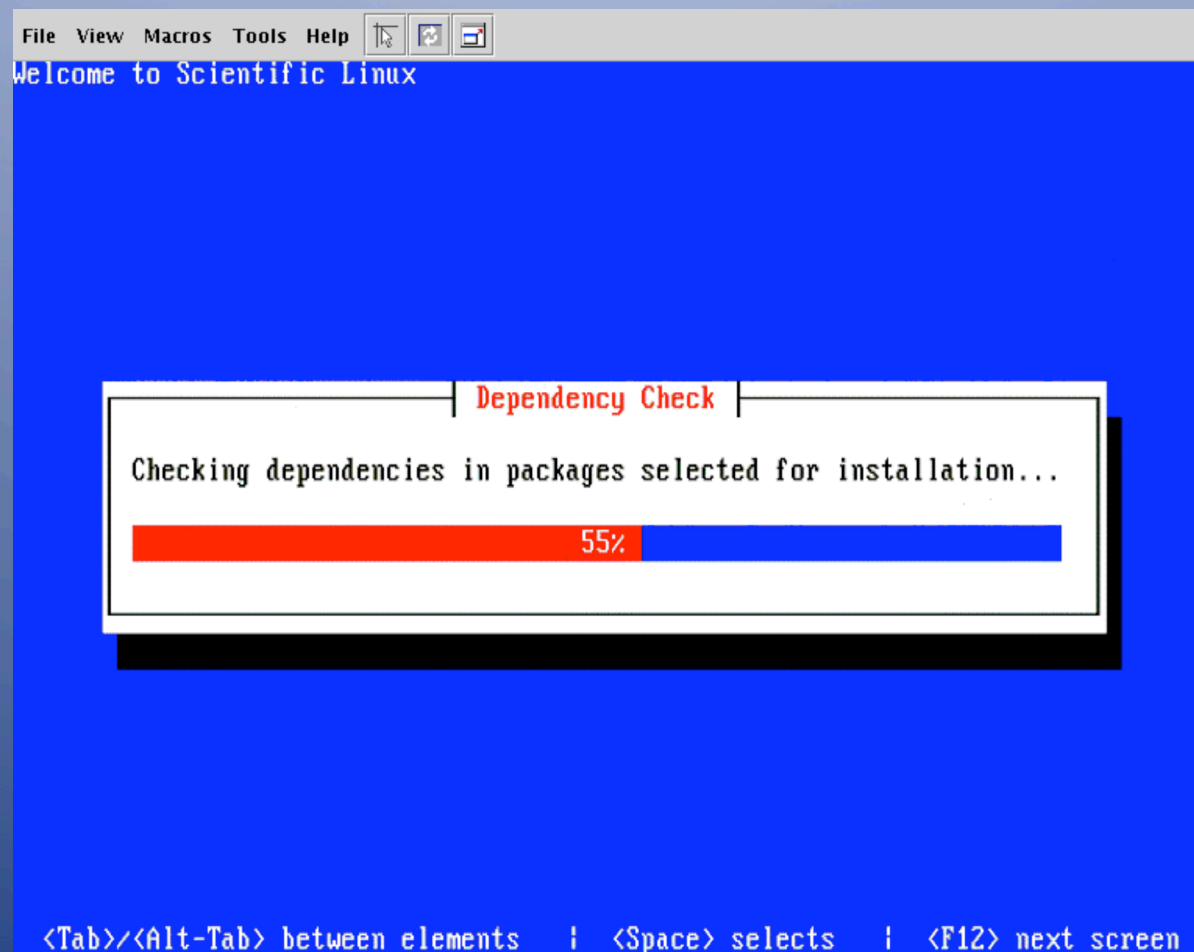


- Boot CD
 - XenINFNnet.iso
- Network install (<http>)
- Kickstart
 - SL5.1 base
 - Installazione componenti virtualizzazione
 - Security update
 - Installazione rpm Xen-3.1.2 personalizzate
 - xen-3.1.2-0.1.cug.x86_64.rpm
 - xen-libs-3.1.2-0.1.cug.x86_64.rpm
 - Post configurazione di Xen
- Reboot

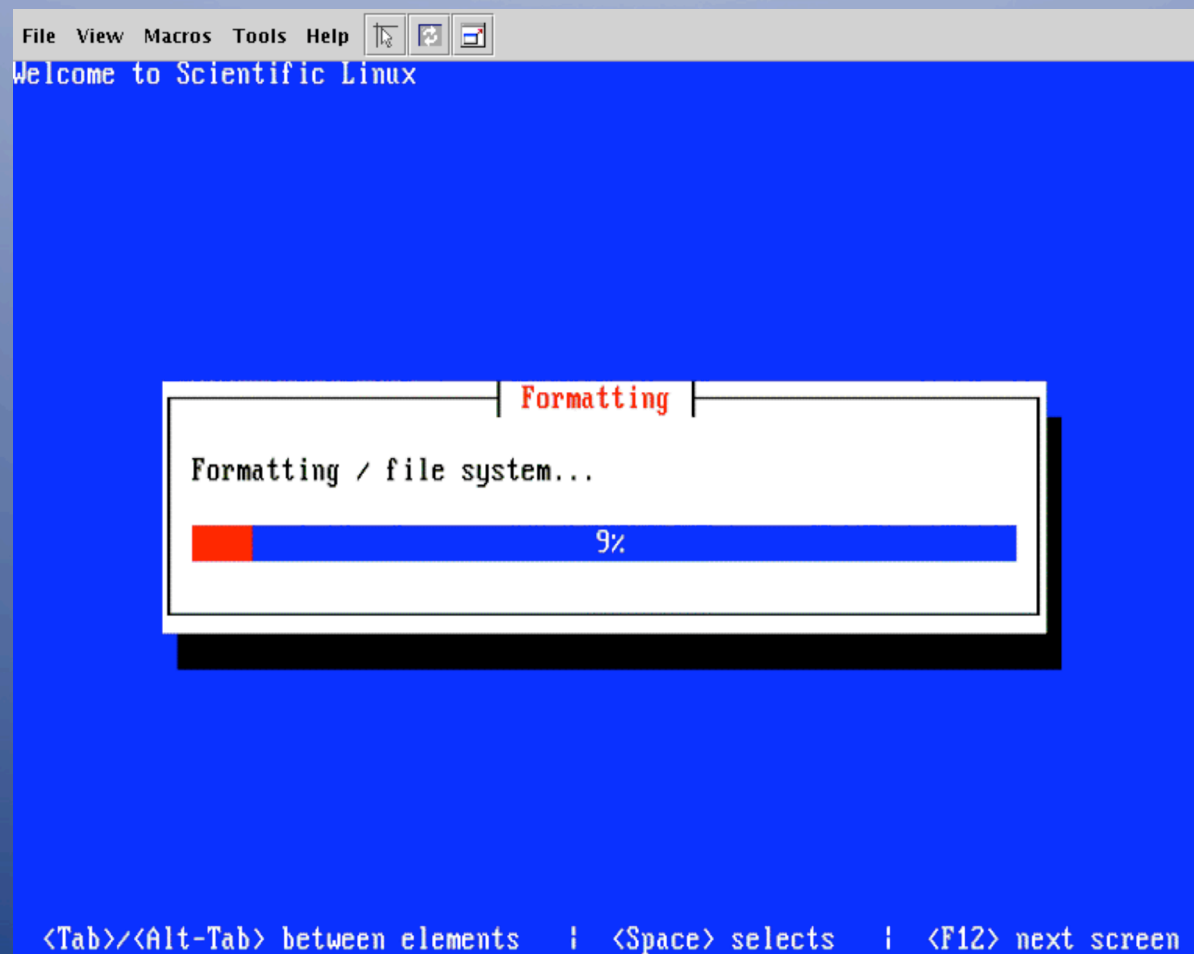


XenINFN (network install)





XenINFN (creazione partizioni)





File View Macros Tools Help

Welcome to Scientific Linux

Package Installation

Name : nss-3.11.7-1.3.el5-i386
 Size : 1885k
 Summary: Network Security Services

Status:

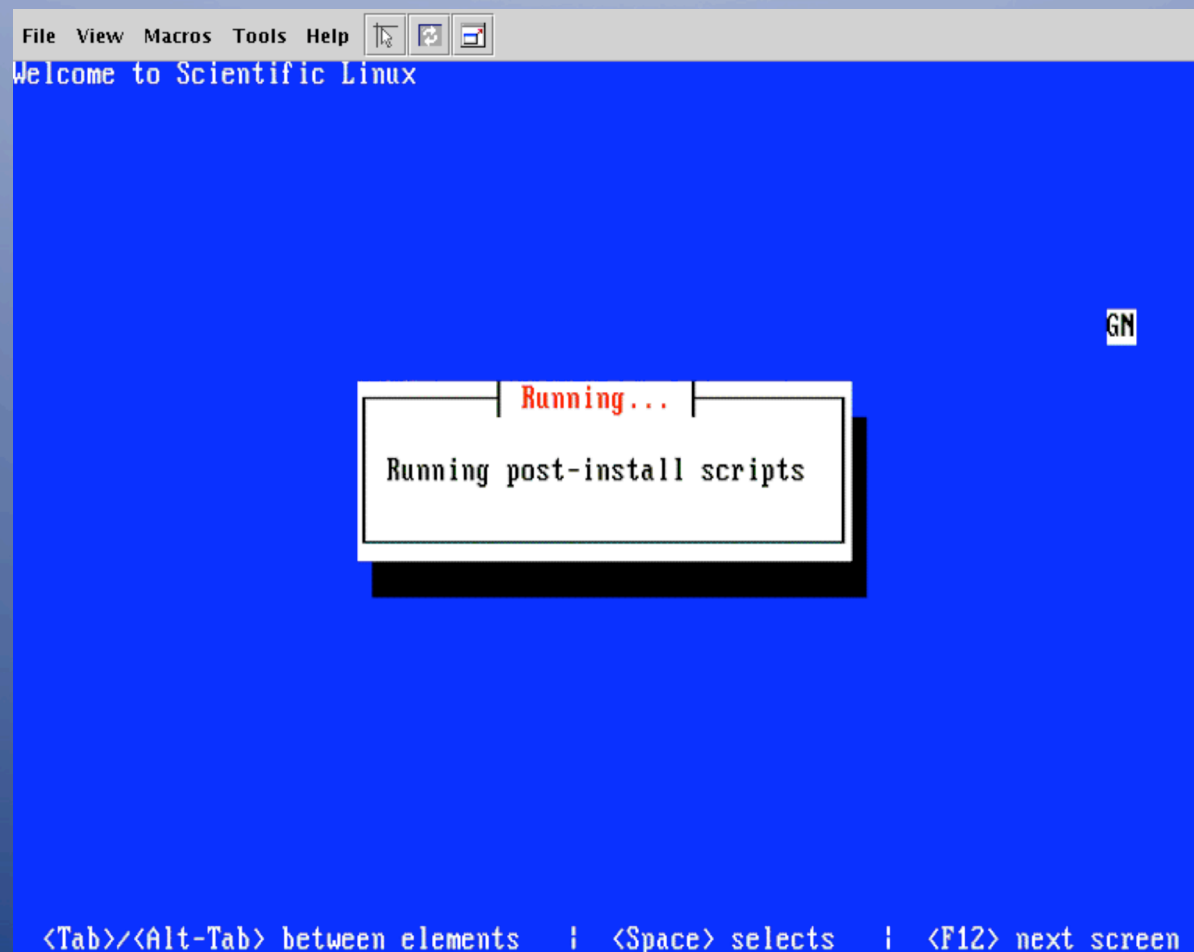
100%

	Packages	Bytes	Time
Total :	468	790M	0:01:40
Completed:	74	181M	0:00:22
Remaining:	394	609M	0:01:17

22%

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

XenINFN post install



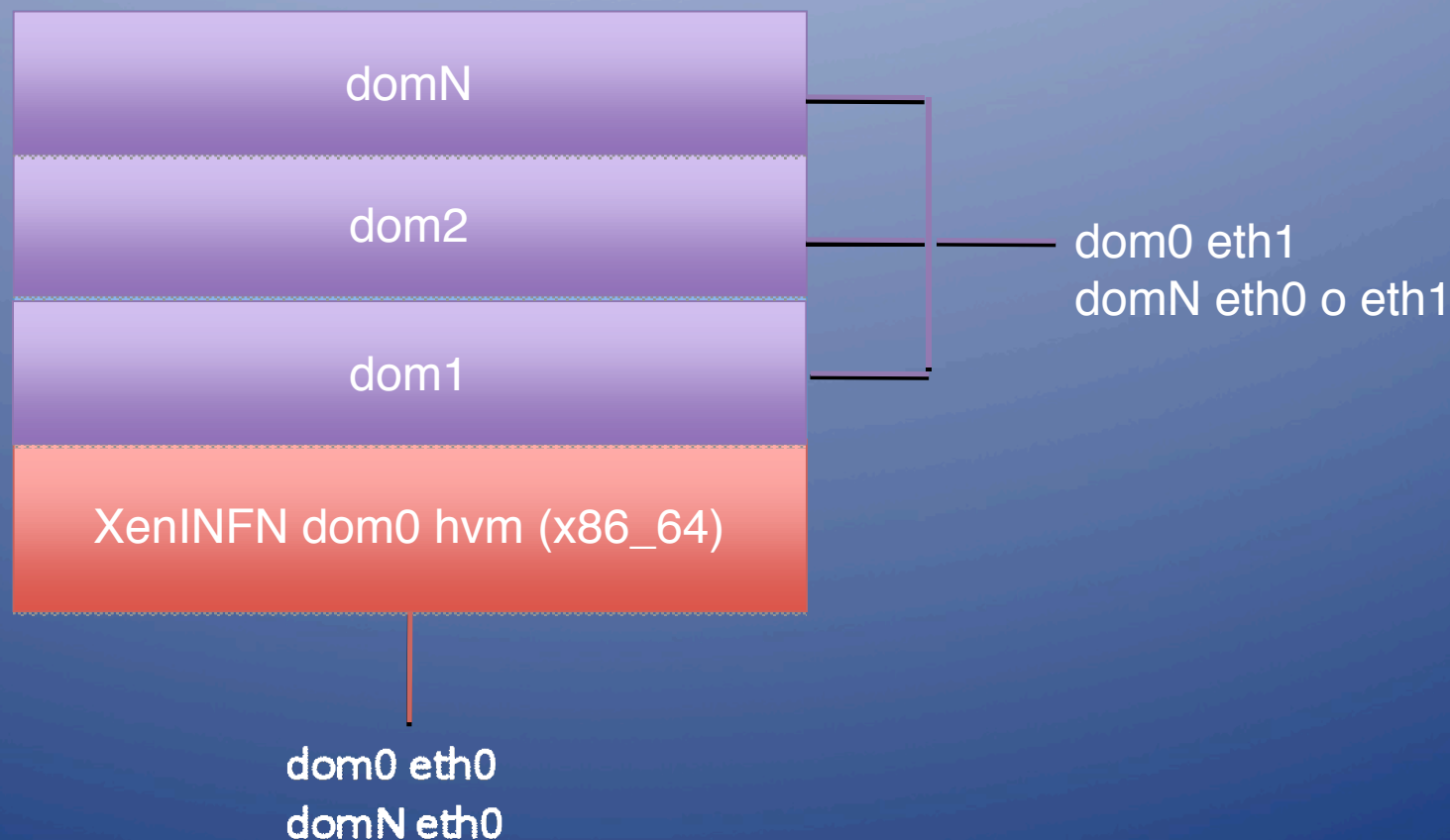
XenINFN post install



- Rimozione di alcuni servizi inutili
- Installazione delle rpm di Xen 3.1.2
- Cambiamento della configurazione di Xen di default (xend-config.sxp)
 - Creazione di 2 network bridge

bridge name	bridge id	STP enabled	interfaces
xenbr0	8000.feffffffffffno		peth0 vif0.0
xenbr1	8000.feffffffffffno		peth1 vif0.1

XenINFN default NIC config



Xen network overbust



- Bisogna compilare i moduli sulla macchina guest

`xen-3.1-testing-15502/unmodified_drivers/linux-2.6`

- `xen-vnif.ko` (netfront)
- `xen-platform-pci.ko`
- `xen-vbd.ko`
- `xen-balloon.ko`
- Caricare i moduli al boot della macchina guest
- Modificare il template Xen per la macchina virtuale in modo da utilizzare Netfront

XenINFN in produzione

Mail server @CNAF (iris)



- Dom0 XenINFN v1.0
- Utilizzo driver di rete netfront sulla macchina guest (mail server)
- Utilizzo di un file sparse per le partizioni di sistema operativo
- Utilizzo di partizioni fisiche del dom0 per le mailbox e per lo swap

Xen iris template file



```
name = "iris"
builder = "hvm"
memory = "3500"
disk = [ 'file:/domU/iris.img,hda,w', 'phy:/dev/sdb2,hdb,w', 'phy:/dev/sdb3,hdc,w' ]
vif = [ 'type=netfront, mac=00:16:3e:65:b1:db, bridge=xenbr0', ]
#vif = [ 'type=ioemu, mac=00:16:3e:65:b1:db, bridge=xenbr0', ]
device_model = "/usr/lib64/xen/bin/qemu-dm"
kernel = "/usr/lib/xen/boot/hvmloader"
vfb = [ 'type=vnc' ]
vnc=1
vncunused=1
apic=1
acpi=1
pae=1

vcpus=4
#serial = "pty" # enable serial console
on_reboot    = 'restart'
on_crash     = 'restart'
```

Xen in produzione



- Disk I/O: 98MB/sec
- Network I/O: 930Mbit/sec
- CPU performance: analoghe alla macchina reale (senza CPU overbooking)
- Stabilità: guest mai andato in crash (x86_64)
- Backup semplice, basta copiare 1 file (iris.img)
- Facile ripartire in caso di disastro, tutto il sistema e' su 1 file

XenINFN: 32bit e 64bit guest



- x86_64 guest funzionano senza problemi
- i386 guest hanno qualche problema con ACPI
 - Non si riesce a fare il restart della macchina virtuale in modo automatico
 - Occorre spegnere la macchina con “xm destroy” una volta effettuato lo shutdown
 - Il tempo di boot del guest aumenta a causa di problemi di gestione di ACPI
 - Per il resto anche le macchine a 32 bit sono stabili e funzionano
 - Workaround: disabilitare ACPI

ToDo



- Aggiornare <https://calcolo.infn.it/wiki> con info dettagliate sull'installazione e utilizzo di XenINFN
- XenINFN v1.1
 - Integrazione con Xen 3.1.4
- XenINFN v2.0
 - Integrazione con Xen 3.2.1