

Com muntar un servidor a casa

Roman Valls

20 de novembre de 2005

Motivacions

Disclaimer

Perquè vull un servidor ?

Mans a la obra

Ubicació

Hardware

Infraestructura

Gestió de discs

Hardware de comunicacions

Firewall

Serveis

Correu electrònic

Servidor Web

Gestió de Backups

VOIP

Què és VOIP ?

Conclusions

Conclusions

Disclaimer

- ▶ Amb aquesta xerrada pretenc donar a conèixer sistemes/programes que crec interessants.
- ▶ No es tracta d'un howto ni tutorial pas a pas.
- ▶ Pregunteu, atureu-me, discutiu !

Perquè vull un servidor ?

- ▶ Web
- ▶ Repositori de codi (demo!)
- ▶ Blog
- ▶ Àlbum de fotos
- ▶ Correu electrònic
- ▶ Disc i backups centralitzats
- ▶ Just for fun

Ubicació i acondicionament

- ▶ Important: Pensar bé el lloc
 - ▶ Ventilació adequada
 - ▶ Ens hem de resguardar del soroll !
- ▶ Protecció contra sobretensions o SAI
 - ▶ Offline
 - ▶ Online
- ▶ Relativament accessible per si volem fer upgrades

LCAC: La nevera del D6



- ▶ Aire acondicionat: (21°C constants)

Com ha de ser la màquina ?

- ▶ No té perque ser potent (dimensionat per casa)
- ▶ No cal invertir molts diners en hardware
- ▶ Memòria i CPU: "mínim" P133, 128MB RAM
- ▶ Si tenim restriccions d'espai, podem prescindir de la caixa

Com ha de ser la màquina ?

- ▶ No té perque ser potent (dimensionat per casa)
- ▶ No cal invertir molts diners en hardware
- ▶ Memòria i CPU: "mínim" P133, 128MB RAM
- ▶ Si tenim restriccions d'espai, podem prescindir de la caixa
- ▶ **Solució:** Useu hardware reciclat (pc's antics)!

RAID: Redundant Array of Independent/Inexpensive Disks

- ▶ RAID 0: Bit striping
- ▶ RAID 1: Mirroring
- ▶ RAID 5: Block striping + paritat distribuïda
- ▶ `mdadm -C /dev/md0 -level=raidX -raid-devices=N /dev/*`
- ▶ Altres nivells són relativament poc usats, per a més informació:
 - ▶ http://apc.gotdns.org/moodledata/3/moddata/assignment/34/21/RAID_-_Trabajo.pdf

LVM: Logical Volume Management

- ▶ Defineix una capa d'abstracció sobre dispositius d'emmagatzemament (guanyem amb flexibilitat)
- ▶ Si ens quedem sense espai, no cal moure dades !
- ▶ El sistema de fitxers creix a mesura que ho necessitem
- ▶ Podem donar noms explicatius als volums: "ventes" no "hda1", p.ex
- ▶ VG(PV=Dispositiu, LV=Filesystem)
- ▶ <http://tldp.org/HOWTO/LVM-HOWTO/>

LVM: Exemple d'ús

```
# pvcreate /dev/sda
# pvcreate /dev/sdb
# pvcreate /dev/sdc
# vgcreate my_volume_group /dev/sda /dev/sdb /dev/sdc/
# lvcreate -L1G -nmy_logical_volume my_volume_group
# mke2fs /dev/my_volume_group/my_logical_volume
# mount /dev/my_volume_group/my_logical_volume /mnt
(afegim nou HD)
# vgextend ops /dev/sdg1
```

EVMS: One app to bind them all

- ▶ EVMS (LVM2+RAID+...)
 - ▶ Enterprise Volume Management System
 - ▶ Abstracció d'emmagatzemament flexible i uniforme
 - ▶ Unifica mdadm i lv* en una sola aplicació
 - ▶ BBR i Snapshotting
 - ▶ Extensible: Permet (re)definir nous comportaments d'emmagatzematge

Exemple: evmsn

- ▶ “semi”-demo (screenshots)
- ▶ També hi ha GUI i CLI

Software adicional per a la gestió de discs

- ▶ UnionFS: `mount -t unionfs -o dirs=/user1,/user2 none /home`
- ▶ S.M.A.R.T: Self-Monitoring, Analysis and Reporting Technology (<http://smartmontools.sf.net>)
- ▶ Monitoritza paràmetres de funcionament dels HDD's:

ID#1	ATTRIBUTE_NAME	FLAG	VALUE	WORST	THRESH	TYPE	UPDATED	WHEN_FAILED	RAW_VALUE
1	Raw_Read_Error_Rate	0x000f	007	001	046	Pre-fail	Always	FAILING_NOW	154618843423
2	Throughput_Performa	0x0005	100	100	020	Pre-fail	Offline	-	145
3	Spin_Up_Time	0x0003	094	083	025	Pre-fail	Always	-	24321
4	Start_Stop_Count	0x0032	097	097	000	Old_age	Always	-	1887
5	Reallocated_Sector_Ct	0x0033	099	099	024	Pre-fail	Always	-	1
7	Seek_Error_Rate	0x000f	100	100	047	Pre-fail	Always	-	458751
8	Seek_Time_Performance	0x0005	100	100	019	Pre-fail	Offline	-	0
9	Power_On_Seconds	0x0032	088	088	000	Old_age	Always	-	1819h+16m+52s
10	Spin_Retry_Count	0x0013	100	100	020	Pre-fail	Always	-	0
12	Power_Cycle_Count	0x0032	091	091	000	Old_age	Always	-	1467
194	Temperature_Celsius	0x0022	100	100	000	Old_age	Always	-	32
195	Hardware_ECC_Reco	0x001a	100	100	000	Old_age	Always	-	1221

LCAC: Sistema de disc

- ▶ 2 servidors Sun V240
- ▶ 1 Disk array Sun StorEdge 3150 FC
- ▶ 12 HDD's de 73GB
- ▶ 5HDD's per LD (logical drive), 2LD's
- ▶ 2 Global spares apagats
- ▶ Exporta el FS per NFS a totes les màquines
- ▶ Multipath: Camins redundants (backup)

Equips de xarxa

- ▶ Evitar els modems usb, usar routers
- ▶ Xarxa wired: switch, cablejar casa
- ▶ Xarxa wireless: tarja pci o pen usb
 - ▶ Seguretat: WEP, WPA, RADIUS...
 - ▶ També podem usar OpenVPN (túnel segur)
 - ▶ O usar portals captius: Chillispot, NoCat...

LCAC: Rack de comunicacions



- ▶ Capa d'accés
- ▶ Capa de distribució
- ▶ PSU's redundants
- ▶ Parc de mòdems

Regles del firewall

- ▶ Podem usar iptables
- ▶ O un bon frontend que ens simplifiqui/generi les regles: Shorewall, fwbuilder
- ▶ Si voleu filar prim amb les regles del firewall, teniu POM (Patch-O-Matic), alguns interessants:
 - ▶ Bits of string
 - ▶ Time-Based Rules
 - ▶ *-contrack: pathological protocols
 - ▶ TARPIT: frustrant atacants
 - ▶ <http://www.lowth.com/howto/iptables-treasures.php>

Script d'iptables (<http://www.netfilter.org>)

- ▶ Tutorial pràctic: <http://www.pello.info/filez/firewall/iptables.html>

```
Iptables:
#!/bin/sh
# Mi cortafuegos; 13/2/2004 1:49 AM, Daniel Clemente
# http://www.danielclemente.com
iptables -F INPUT
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -m state --state NEW -i lo -j ACCEPT
iptables -A INPUT -m state --state NEW -i eth0 -p tcp --dport 20 -j ACCEPT
iptables -A INPUT -m state --state NEW -i eth0 -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -m state --state NEW -i eth0 -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -m state --state NEW -i eth0 -s 172.26.0.2 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -m state --state NEW -i eth0 -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -m state --state NEW -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT
iptables -P INPUT DROP
iptables -F FORWARD
iptables -P FORWARD DROP
iptables -F OUTPUT
iptables -P OUTPUT ACCEPT
```

Script Shorewall (<http://www.shorewall.net>)

Shorewall:

fitxer zones:

inet	eth0	detect
loc	eth1	detect

fitxer policy:

loc	inet	ACCEPT
inet	all	DROP
all	all	REJECT

fitxer rules:

ACCEPT	inet	fw	tcp	20,21
ACCEPT	loc:172.26.0.2	fw	tcp	22
ACCEPT	inet	fw	tcp	80
ACCEPT	inet	fw	icmp	8 #icmp-request
ACCEPT	inet	fw	icmp	0 #icmp-reply

Postfix+Cyrus-IMAP+TLS+SASL+ClamAV+Amavis+...

- ▶ És un tema més complex del que sembla
- ▶ Consell: A poc a poc... muntar un sistema bàsic i anar afegint capacitats a mesura que funcionin correctament
- ▶ Estar ***MOLT*** atents al log i *provar* cada pas/modificació, per mínima que sembli

Exemple de com muntar-ho tot:

1. Postfix "pelat", sense *provar* enviament local i extern
2. Cyrus-IMAP: Crear compte d'exemple i *provar*
3. TLS: Generar certificats auto-signats i afegir la capacitat a Postfix i Cyrus, *provar*
4. SASL: Donar d'alta a sasldb i *provar*
5. Spamassassin: Fer les modificacions pertinents al postfix i *provar*
6. ClamAV: Afegir-hi suport a l'Spamassassin
7. ...així amb totes les millores que se'ns acudeixin: Greylisting, SPF, autenticació d'usuaris contra BBDD, etc...

Greylisting ? SPF ?

- ▶ Greylisting: El soft usat per spammers no compleix amb els estàndars (RFC821)

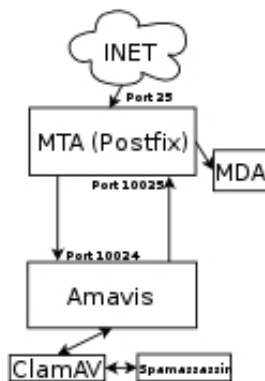
```
Nov 19 12:35:49 nopcode postfix/smtp[8495]: A428117989:  
to=<somebody@netbsd.org>, relay=mail.netbsd.org[204.152.190.11], delay=4,  
status=deferred (host mail.netbsd.org[204.152.190.11]  
said: 450 <somebody@netbsd.org>: Recipient address rejected:  
Greylisting in action, please try later (in reply to RCPT TO command))  
-----
```

```
Nov 19 13:05:05 nopcode postfix/smtp[8922]: A428117989:  
to=<somebody@netbsd.org>, relay=mail.netbsd.org[204.152.190.11],  
delay=1760, status=sent
```

- ▶ SPF: Sender Policy Framework
- ▶ S'usa per validar l'identitat/validesa de l'origen mitjançant registres DNS (TXT)

Exemple de configuració: Postfix (main.cf)

```
smtpd_banner = $myhostname NO UCE ESMTX
# anti-UCE
smtpd_helo_required = yes
disable_vrfy_command = yes
(...)
smtpd_recipient_restrictions =
  permit_sasl_authenticated,
  permit_mynetworks,
  reject_non_fqdn_sender,
  reject_non_fqdn_recipient,
  reject_unauth_destination
(...)
smtpd_use_tls = yes
smtpd_tls_key_file = /path/a/clau_privada.key
smtpd_tls_cert_file = /path/a/certificat.crt
smtpd_tls_CAfile = /path/a/CA.pem
content_filter = smtp-amavis:[127.0.0.1]:10024
```



Connexió de Postfix amb Amavis (master.cf)

```
127.0.0.1:10025 inet      n      (...)  smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=
permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes
```

Exemple de configuració: Amavisd-new

```
$inet_socket_port = 10024;           # accept SMTP on this local TCP port
                                     # (default is undef, i.e. disabled)
@inet_acl = qw(127.0.0.1 [::1]);     # allow SMTP access only from localhost IP
                                     # (default is qw(127.0.0.1 [::1]) )

(...)
[qr'^(bulkmail|offers|cheapbenefits|earnmoney|foryou)@'i      => 5.0],
[qr'^(greatcasino|investments|lose_weight_today|market\.alert)@'i=> 5.0],
[qr'^(money2you|MyGreenCard|new\.tld\.registry|opt-out|opt-in)@'i=> 5.0],
[qr'^(optin|saveonlsmoking2002k|specialoffer|specialoffers)@'i  => 5.0],
(...)
@av_scanners = (

# ### http://www.clamav.net/
['ClamAV-clamd',
 \&ask_daemon, ["CONTSCAN {}]\n", "/var/run/clamav/clamd"],
 qr/\bOK$/, qr/\bFOUND$/,
 qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
```

Headers d'un correu filtrat per Amavis

```
# zcat /var/amavis/quarantine/spam-Qv44SxSN1FBr.gz

X-Spam-Status: Yes, score=19.901 tag=2 tag2=5.4 kill=5.4
tests=[FORGED_RCVD_HELO=0.05, INFO_TLD=0.481,
RCVD_IN_BL_SPAMCOP_NET=1.832, RCVD_IN_DSBL=2.765,
RCVD_IN_NJABL_DUL=1.655, RCVD_IN_XBL=2.511,
URIBL_AB_SURBL=2.007, URIBL_JP_SURBL=1.539,
URIBL_OB_SURBL=1.996, URIBL_SBL=0.629,
URIBL_SC_SURBL=3.897, URIBL_WS_SURBL=0.539]
X-Spam-Score: 19.901
X-Spam-Level: *****
X-Spam-Flag: YES
```

Headers d'un correu filtrat amb Amavis (II)

X-Spam-Report:

Content analysis details: (19.9 points, 5.0 required)

pts	rule name	description
0.1	FORGED_RCVD_HELO	Received: contains a forged HELO
0.5	INFO_TLD	URI: Contains an URL in the INFO TLD
2.8	RCVD_IN_DSBL	RBL: Received via a relay in list.dsbl.org [< http://dsbl.org/listing?194.144.29.115 >]
1.8	RCVD_IN_BL_SPAMCOP_NET	RBL: Received via a relay in bl.spamcop.net [Blocked - see < http://www.spamcop.net/bl.shtml?194.144.29.115 >]
2.5	RCVD_IN_XBL	RBL: Received via a relay in Spamhaus XBL [194.144.29.115 listed in sbl-xbl.spamhaus.org]
1.7	RCVD_IN_NJABL_DUL	RBL: NJABL: dialup sender did non-local SMTP [194.144.29.115 listed in combined.njabl.org]
2.0	URIBL_AB_SURBL	Contains an URL listed in the AB SURBL blocklist [URIs: matedesign.info raremate.info]

Extenent el sistema de correu

- ▶ Exemple: Hylafax
 - ▶ Simplement enviem un correu a `alguntelefon@blabla.fax`
 - ▶ Els faxes entrants podem adjuntar-los en pdf i que els rebi un(s) usuari(s).
 - ▶ Millor usar modems que suporten CID
- ▶ El límit està en la imaginació, però compte amb l'entrada de l'usuari !

Apache (<http://www.apache.org>)

- ▶ Tot i ser el servidor web més consolidat avui en dia, no hem d'oblidar alternatives
 - ▶ thttpd, Tux, screws, mini-httpd ...
- ▶ Amb apache tenim la possibilitat d'experimentar amb la gran quantitat de plugins que disposa
 - ▶ mod_php, mod_deflate, mod_perl, mod_security ...
- ▶ Si tenim més d'un domini, podem fer servir virtual hosting
- ▶ Podem usar certificats SSL si volem un site segur (<http://www.cacert.org>)

Backups per casa (i empresa)

- ▶ S'han vist les opcions de sempre: tar,dump-restore,etc...
- ▶ Existeixen altres solucions més completes, que faciliten la gestió de backups:
 - ▶ Backuppc: Amb interface web i amb estalvi considerable d'espai
 - ▶ Bacula: "It comes by night and sucks the vital essence from your computers"
 - ▶ rdiff-backup: backups molt fàcils
 - ▶ duplicity: backups xifrats: GnuPG
 - ▶ flexbackup: flexibilitat
 - ▶ amanda: Ideal per cintes, tot i que funciona perfecte amb altres suports

LCAC: Backup en cintes DLT i LTO

▶ DLT: 20-30GB



▶ LTO: 300-400GB



VOIP: Voice Over IP

- ▶ Enrutat de veu sobre paquets IP en comptes de commutació de circuits (telefonía tradicional)
- ▶ Tots coneixem skype i d'altres sistemes VOIP, però no ténen la potència que ens ofereix un PBX
- ▶ Possibilitat de disposar de teléfans software o hardware (tradicionals)
- ▶ Més interessant: Poder hibridar tecnologies de telefonía: POTS, INET, GSM ... per tal de trucar amb la ruta més econòmica :-)

Asterisk PBX: La centraleta telefònica software

- ▶ Permet fer trucades a través d'internet per evitar tarifes locals
- ▶ És software, podeu programar vosaltres mateixos les extensions ...
- ▶ ...IVR (Interactive Voice Response), MultiRing, Contestador automàtic ...
- ▶ Enorme quantitat de configuracions/possibilitats.
- ▶ No us perdeu: http://pof.eslack.org/writings/ESILUX_Asterisk.pdf

Conclusions

- ▶ El sysadmin ha d'estar sempre al dia de totes les novetats
 - ▶ Llegir/subscriu-re's/muntar un blog ajuda molt avui en dia
 - ▶ Llistes de correu sobre el software que useu
 - ▶ Bookmarks col·laboratius: <http://del.icio.us>
 - ▶ Revistes, llibres, e-zines
 - ▶ Xerrades, conferències, LUG's, etc...
- ▶ Abans d'implementar una solució, provar-la a consciència (devel-producció)

Conclusions (II)

- ▶ No hem d'oblidar mai la part humana, s'ha de saber tractar bé als usuaris !
 - ▶ Resoldre els dubtes de forma entenedora i clara, sense entrar amb tecnicismes
 - ▶ Preguntar SEMPRE abans d'accedir a dades privades
 - ▶ En cas de detectar activitats sospitoses d'un usuari, tenir tacte en comunicar-ho
 - ▶ Saber reconèixer els propis errors
 - ▶ etc... (és qüestió de trobar-se amb la situació)