Használjunk FreeBSD-t!

Zahemszky Gábor

Magyar BSD Egyesület

Konfigurációs fájlok

- /boot/defaults/loader.conf - olvasandó
- /boot/loader.conf – szerkesztendő
- /etc/defaults/rc.conf - olvasandó
- /etc/rc.conf – szerkesztendő

  Ezeket a dhclient beállítja:
- /etc/nsswitch.conf
- /etc/resolv.conf

/boot/loader.conf

Pl. gyorsabb, színesebb boot

- autoboot_delay="1"
- loader_logo="beastie"
- loader_color="YES"
- beastie_disable="NO" # I like colourful Chuck!

Extra HW és SW használata

- snd_ich_load="YES"
- linux_load="YES"

  Intel 3945 Wifi használata
- if_wpi_load=”YES”
- legal.intel_wpi.license_ack=1

/etc/rc.conf – alap hálózat

- hostname="Lappantyu.Zahemszky.hu"
- ifconfig_fxp0="10.10.10.1"
- ifconfig_wpi0="WPA DHCP"

/etc/rc.conf – alap szoftverek

- sshd_enable=”YES” # Enable sshd
- syslogd_enable=”YES”
- syslogd_flags=”-s -s” # Flags to syslogd (if enabled).
- lpd_enable=”YES”
- lpd_flags=”-s”
- sendmail_enable=”NO”

/etc/rc.conf – extra szoftverek

- dbus_enable="YES"
- hald_enable="YES"
- avahi_daemon_enable="YES"
- avahi_dnsconfd_enable="YES"

Operációs rendszer frissítés/1

Bináris

- # freebsd-update fetch install

Operációs rendszer frissítés/2

Forrásból

- csup -h cvsup.freebsd.org /usr/share/examples/cvsup/standard-supfile
- cd /usr/src
- make KERNCONF=GENERIC buildworld buildkernel installkernel
- nextboot -o -s -k kernel
- shutdown -r now

Operációs rendszer frissítés/3

(single boot után)

- mount -a
- cd /usr/src
- make installword
- mergemaster
- nextboot -D && reboot now

Csomagtelepítés

Binárisan

- pkg_add -r nano

Forrásból

- cd /usr/ports/editors/nano
- make install clean

Csomagok frissítése

Telepítsünk plusz csomagot hozzá :-(!

- a portupgrade tud bináris frissítést IS
- a portmaster CSAK forrásalapút tud

Biztonsági ez-meg-az

- ACL-ek
- Csomagszűrők
- Jail-ek
- MAC-keretrendszer

ACL

A hagyományos jogosultságkezelés kevés ACL-lel extra felhasználóknak és/vagy extra csoportoknak adhatunk jogokat

- mount -u -o acls /mnt # vagy
- vi /etc/fstab # vagy

  /dev/akarmi /mnt ufs acls 0 1
- tunefs -a enable /mnt # a megoldás

- getfacl lo

  # file: lo

  # owner: zgabor

  # group: wheel

  user::rw-

  group::r--

  other::r--
- # setfacl -m u:nobody:r lo
- # setfacl -x u:nobody:r lo

- getfacl lo # megmaradt a "mask" ACL
- setfacl -x m::r lo
- getfacl lo # megmaradt a "mask" ACL
- setfacl -m u:nobody:--- lo
- setfacl -b lo
- getfacl lo # megmaradt a "mask" ACL
- setfacl -m u:nobody:--- lo
- setfacl -b -n lo # sikerült törölni!

Csomagszűrők

- ipfw - saját, néhány FreeBSD specifikum (pl. Jail-id alapú szabályok)
- ipf - Darren Reed-féle (multiplatform: Solaris, HP-UX, *BSD, stb.)
- pf - Daniel Hartmeier OpenBSD-ből -> NetBSD, FreeBSD, DragonFlyBSD

IPFW

- ipfw + natd
- ipfw2 beépített NAT mechanizmus
- dummynet – forgalomkorlátozás (traffic shaping)

- 0-31 szabályhalmazok
- 0 - alapértelmezett szabályhalmaz, ide kerülnek a saját szabályok alapból
- 31 - itt van a default DENY szabály (nem törölhető)

  ipfw set move 1 to 5

  ipfw set swap 8 13

Táblák 0 - 127

- ipfw table 1 add 192.168.1.0/24
- ipfw table 1 add 172.16.0.0/16
- ipfw table 2 delete
- ipfw table 3 flush
- ipfw table 1 list

Csövek és sorok

Hierarchiába szervezhető sebességkorlátozás

- ipfw pipe 1 config bw 10 MB
- ipfw queue 2 config weight 10 pipe 1
- ipfw queue 3 config weight 1 pipe 1

- kldload ipfw
- ipfw enable firewall
- ipfw disable firewall
- ipfw add allow ip from any to any 22 out via lnc0
- ipfw /szabalyokat/tartalmazo/file
- ipfw -S show
- ipfw set show

IPF

- kldload ipl # kernel modul betöltése, a név nem elírás!
- ipf -E # engedélyezés
- ipf -D # tiltás

- ipf -f /szabaly/fajl
- ipf -f -

  pass in quick all

  pass in quick on lo0

  pass out quick on lo0

  pass in from any to any port = 22 keep state

  pass out from any to any port = 80 keep state
- ipf -r -f -

  pass in quick all

- ipmon -a # mindenféle logot olvasok
- ipmon -o NSI # NAT, state, filter log
- ipmon -a -O S # state logot nem
- ipmon /ide/menti # szöveges mentés
- ipmon -B /ide/menti # bináris log mentése
- ipmon -f /innen/olvas # -B -vel mentett olvasása
- ipmon -s -L facility # syslog (default local0)
- ipmon -N /dev/natlog # innen olvassa a NAT logokat
- ipmon -S /dev/statelog # state logs
- ipmon -f /dev/normallog # filterlogs

```
# ipf -f -

pass out log from 127.0.0.1/32 to any

log in proto tcp from 192.168.1.3/32 to
192.168.1.2/32 port = ftp

pass in log on em0 from 192.168.1.0 mask
255.255.255.0 to any

# ipmon -a

09/02/2009 17:47:20.747874 em0 @0:2 p
192.168.1.3,137 -> 192.168.1.255,137 PR udp
len 20 78 IN broadcast
```

PF

- kldload pf # kernelmodul betöltése
- pfctl -e # engedélyezés
- pfctl -d # tiltás

- pfctl -f /szabalyok/innen
- pfctl -f -

  pass in quick all

  pass in quick on lo0

  pass out quick on lo0

  pass in from any to any port = 22 keep state

  pass out from any to any port = 80 keep state

- Egyszerűsíthető

  pass quick on lo0

  pass in from any to any port = 22

  pass out from any to any port = 80

Táblákkal egyszerűsíthetők

table <private> const { 10/8, 172.16/12, 192.168/16 }

table <badhosts> persist

block on fxp0 from { <private>, <badhosts> } to any

pfctl -t badhosts -Tadd 204.92.77.111

JAIL

Jail készítés

mkdir -p /usr/jail/MASTER /usr/jail/dns /usr/jail/mail

setenv D /usr/jail/MASTER

(sh esetén: D=/usr/jail/MASTER; export D)

cd /usr/src

make DESTDIR=$D installworld

make DESTDIR=$D distribution

JAIL/2

```
# mount -t devfs devfs $D/dev

# ifconfig lo0 alias 172.16.1.1

# jail /usr/jail/MASTER dns.example.jail
172.16.1.1 sh /etc/rc

....

# jls

....
```

```
# jexec 1 /bin/sh
# sysctl security.jail.set_hostname_allowed=0
# jexec 1 /bin/sh
# jexec 1 /bin/sh /etc/rc.shutdown
# jexec 1 kill -15 -1
(vagy: # pkill -15 -j 1)
```

másik jail használata "loopback" mount segítségével

FreeBSD nullfs-mount-nak hívja

virtuális diszk készítés

truncate -s +100M /usr/jail/dnsdisk

mdconfig -a -t vnode -f /usr/jail/dnsdisk

mdconfig -l -v

mdconfig -d -u 0

vi rc.conf

mdconfig_md0="-t vnode -f /usr/jail/dnsdisk"

```
# sh /etc/rc.conf/mdconfig onestart
# bsdlabel -w /dev/md0   # régi neve: disklabel
# newfs -L dnsdisk /dev/md0a
# mount /dev/md0a /mnt
# jobb a "virtuális eszköznevek" használata
# mount /dev/ufs/dnsdisk /mnt
# umount /mnt
```

```
# pwd
/usr/jail/MASTER
# mkdir -p /usr/jail/skel/{home,distfiles}
# mv etc tmp var root /usr/jail/skel/
# mkdir s
# ln -s s/etc
# ln -s s/home
# ln -s s/root
# ln -s s/tmp
# ln -s s/var
# vi /usr/jail/skel/etc/make.conf
WRKDIRPREFIX?=  /s/portbuild
```

```
# mkdir /usr/jailskel

# cpdup /usr/jail/skel /usr/jailskel/dns

# mount -t nullfs -o ro /usr/jail/MASTER /usr/jail/
dns

# mount -t nullfs -o rw /usr/jailskel/dns
/usr/jail/dns/s

# mount /dev/ufs/dnsdisk /usr/jail/dns/home

# mount -t devfs devfs /usr/jail/dns/dev

# jail /usr/jail/dns dns.example.jail 172.16.1.1
/bin/sh /etc/rc
```

```
# vi /etc/fstab.dns
/usr/jail/MASTER /usr/jail/dns    nullfs  ro  0    0
/usr/jailskel/dns    /usr/jail/dns/s nullfs  rw  0    0
/dev/ufs/dnsdisk   /usr/jail/dns/home ufs  rw 0  1
```

```
# vi rc.conf:
jail_enable="YES"
jail_list="dns"
jail_dns_rootdir="/usr/jail/dns"
jail_dns_hostname="dns.example.jail"
jail_dns_ip="172.16.1.1"
jail_dns_interface="lo0"
jail_dns_mount_enable="YES"
jail_dns_devfs_enable="YES"
jail_dns_devfs_ruleset="dns_ruleset"
```

További jail-eket ugyanígy lehet csinálni

truncate -s +100M /usr/jail/maildisk

bsdlabel -w /dev/md1

newfs -L maildisk /dev/md1a

mount /dev/md1a /tmp/maildisk

mount /dev/ufs/maildisk /tmp/maildisk

vi rc.conf:

- mdconfig_md1="-t vnode -f /usr/jail/maildisk"

folytatás:

- jail_enable="YES"
- jail_list="dns mail"
- jail_set_hostname_allow="NO"
- jail_interface="lo0"
- jail_mount_enable="YES"
- jail_devfs_enable="YES"
- jail_dns_rootdir="/usr/jail/dns"
- jail_dns_hostname="dns.example.jail"
- jail_dns_ip="172.16.1.1"
- jail_mail_rootdir="/usr/jail/mail"
- jail_mail_hostname="mail.example.jail"
- jail_mail_ip="172.16.2.1"

```
# vi /etc/fstab.mail
/usr/jail/MASTER /usr/jail/mail    nullfs  ro   0  0
/usr/jailskel/mail   /usr/jail/mail/s nullfs  rw  0  0
/dev/ufs/maildisk  /usr/jail/mail/home ufs rw 0  1
```

MAC

- mac_bsdextended
- mac_ifoff
- mac_partition
- mac_portacl
- mac_seeotheruids

  (nem beszélünk róla, HANDBOOK v. man)
- mac_biba
- mac_lomac
- mac_mls

Cimkék

BIBA, MLS, LOMAC és Partition használ cimkét, többi nem

Cimke:

- szubjektum (user/processz)
- policy/alapszint:rekesz1+r2+r3(alsószint:rX+rY-felsőszint:rI+rJ+rK+rL)
- objektum (fájl/netif)
- policy/szint:rA+rB+rC

Cimke beállítása

- # setpmac POLICY process parameter1 parameter2 ...
- USER: (kb processz)

  /etc/login.conf:

  label=LABEL,LABEL,LABEL
- FÁJLRENDSZER (FS):

  # setfmac POLICY file1 file2 dir1 dir2

  # setfsmac -f filelist POLICY
- INTERFÉSZ:

  # ifconfig ... maclabel ...

MAC_BSDEXTENDED

- FS-firewall, sysctl paranccsal szabályozható
- security.mac.bsdextended.enabled=1
- security.mac.bsdextended.rule_count=256
  # ennyi szabály van (ez a max)
- security.mac.bsdextended.rule_slots=XYZ
  # használatban levők száma
- security.mac.bsdextended.firstmatch_enabled=
  1 # első találat nyer
- security.mac.bsdextended.logging=1
  # syslog AUTHPRIV logolás be

- Szabályokat az ugidfw -vel állítjuk be:

- ugidfw add subject uid UID1:UID2 object ! gid GID1:GID2 type fdl mode rw
- ugidfw list
- ugidfw remove

MAC_IFOFF

Hálózati forgalom kikapcsolása

- security.mac.ifoff.lo_enabled=1
  # loopback engedélyezett
- security.mac.ifoff.other_enabled=0
  # minden más is
- security.mac.ifoff.bpfrecv_enabled=0
  # BPF mehet :-)

MAC_PARTITION

Processzek szeparálása

- setpmac partition/1 apache
- setpmac partition/2 ftpd
- setpmac partition/3 sendmail
- ezek után nem látjak egymást/egymás adatait, "mini jail"
- # ps axZ - partício cimkéje

MAC_PORTACL

- security.mac.portacl.enabled=1 # kell
- security.mac.portacl.port_high=1023
  # eddig érdekes a portacl (default)
- security.mac.portacl.rules=szabályok
  # ezek döntik el
- security.mac.portacl.suser_exempt=1
  # root kimarad a korlátozásból
- security.mac.portacl.autoport_exempt=1
  # port 0 kivétel (socket bind-nál érdekes)

Szabályok

- "uid" | "gid" : ID : "tcp" | "udp" : port , ... , ...

  pl:

  security.mac.portacl.rules=uid:80:tcp:80,

  uid:53:udp:53,uid:53:tcp:53

  Szokványos fenntartott portoknak:
- net.inet.ip.portrange.reservedlow: 0
- net.inet.ip.portrange.reservedhigh: 1023 -> 0 !!!!

  nem szabad beleesniük a portacl tartományba!

MAC_SEEOTHERUIDS

Nem láthatják egymás processzeit/socketeit

- security.mac.seeotheruids.enabled=1
- security.mac.seeotheruids.suser_privileged=1
  # root nem érdekes
- security.mac.seeotheruids.primarygroup_enabled=1
  # a saját csoportomat láthatom
- security.mac.seeotheruids.specificgid_enabled=1
  # van kitüntetett csoport
- security.mac.seeotheruids.specificgid=GID
  # ez a csoport az