Jailed template

ZFS alapú *jail*

Minden *jail* alapja egy olyan FreeBSD alaprendszer, amelyhez a későbbiekben nem igazán nyúlunk hozzá, leszámítva a biztonsági frissítéseket, illetve bosszantó hibák kijavítását. Mivel a hasonlóság nagyfokú, azért jól ki tudjuk használni a ZFS fájlrendszer klónozó képességét:

Parancssor

```
[root@freebsd:~]$ zfs create dpool/jails
[root@freebsd:~]$ zfs create dpool/jails/v8.1.0
[root@freebsd:~]$ zfs create dpool/jails/v8.1.0/template
[root@freebsd:~]$ zfs set compression=on dpool/jails/v8.1.0/template
[root@freebsd:~]$ df -h
Filesystem                              Size    Used   Avail Capacity  Mounted on
[...]
dpool/jails                             3.5G      0B    3.5G     0%    /dpool/jails
dpool/jails/v8.1.0                      3.5G      0B    3.5G     0%    /dpool/jails/v8.1.0
dpool/jails/v8.1.0/template             3.5G      0B    3.5G     0%    /dpool/jails/v8.1.0/template
```

Mint látni, létrehoztunk egy *template* jail könyvtárat, mégpedig a *jail*s fájlrendszer alá, a két fájlrendszer közé pedig egy v8.1.0 fájlrendszert, amely a *jail* **verziója**. A verzió mondja meg, hogy az adott *jail* 8.1-es alaprendszerbl készült, és az általunk "kiadott" els verzió. A *template* fájlrendszerbe a klasszikus módszerekkel beleteszünk egy alaprendszert:

Parancssor

```
[root@freebsd:~]$ cd /usr/src
[root@freebsd:/usr/src]$ make world DESTDIR=/dpool/jails/v8.1.0/template
--------------------------------------------------------------
>>> make world started on Wed Jan 14 11:54:34 CET 2009
--------------------------------------------------------------
--------------------------------------------------------------
>>> World build started on Wed Jan 14 11:54:35 CET 2009
--------------------------------------------------------------
[...]
--------------------------------------------------------------
>>> make world completed on Wed Jan 14 13:16:22 CET 2009
                  (started Wed Jan 14 11:54:34 CET 2009)
--------------------------------------------------------------
[root@freebsd:/usr/src]$ make distribution DESTDIR=/dpool/jails/v8.1.0/template
[...]
[root@freebsd:/usr/src]$ df -h
Filesystem                              Size    Used   Avail Capacity  Mounted on
[...]
dpool/jails/v8.1.0                      3.5G      0B    3.5G     0%    /dpool/jails/v8.1.0
dpool/jails/v8.1.0/template             3.5G     94M    3.5G     3%    /dpool/jails/v8.1.0/template
[root@freebsd:/usr/src]$ cp /etc/localtime /dpool/jails/v8.1.0/template/etc/
[root@freebsd:/usr/src]$ cp /etc/login.conf /dpool/jails/v8.1.0/template/etc/
[root@freebsd:/usr/src]$ cp /etc/make.conf /dpool/jails/v8.1.0/template/etc/
[root@freebsd:/usr/src]$ cp /etc/profile /dpool/jails/v8.1.0/template/etc/
[root@freebsd:/usr/src]$ cp /etc/resolv.conf /dpool/jails/v8.1.0/template/etc/
[root@freebsd:/usr/src]$ touch /dpool/jails/v8.1.0/template/etc/fstab
[root@freebsd:/usr/src]$ mkdir /dpool/jails/v8.1.0/template/usr/ports
[root@freebsd:/usr/src]$ echo 'keymap="hu.iso2.101keys"' >/dpool/jails/v8.1.0/template/etc/rc.conf
[root@freebsd:/usr/src]$ echo 'network_interfaces=""' >>/dpool/jails/v8.1.0/template/etc/rc.conf
[root@freebsd:/usr/src]$ echo 'rpcbind_enable="NO"' >>/dpool/jails/v8.1.0/template/etc/rc.conf
[root@freebsd:/usr/src]$ echo '' >>/dpool/jails/v8.1.0/template/etc/rc.conf
[root@freebsd:/usr/src]$ echo 'syslogd_enable="NO"' >>/dpool/jails/v8.1.0/template/etc/rc.conf
[root@freebsd:/usr/src]$ echo 'syslog_ng_enable="YES"' >>/dpool/jails/v8.1.0/template/etc/rc.conf
[root@freebsd:/usr/src]$ echo 'sendmail_enable="NO"' >>/dpool/jails/v8.1.0/template/etc/rc.conf
[root@freebsd:/usr/src]$ echo 'munin_node_enable="YES"' >>/dpool/jails/v8.1.0/template/etc/rc.conf
[root@freebsd:/usr/src]$ echo 'sshd_enable="YES"' >>/dpool/jails/v8.1.0/template/etc/rc.conf
[root@freebsd:/usr/src]$ echo '' >>/dpool/jails/v8.1.0/template/etc/rc.conf
```

Alapveten kész vagyunk, elkészült az els *jail* fájlrendszere, amelyet nem fogunk használni, hanem egyszeren klónozni fogjuk ezt, de eltte megtöltjük kényelmes csomagokkal, amelyeket már megismertünk az alaprendszer használata közben. Ehhez fel kell csatolnunk a *ports* fájlrendszert, amelyet eltte célszer frissíteni:

Parancssor

```
[root@freebsd:/usr/src]$ zfs create dpool/jails/ports
[root@freebsd:/usr/src]$ zfs set compression=on dpool/jails/ports
[root@freebsd:/usr/src]$ portsnap fetch extract -p /dpool/jails/ports/
Looking up portsnap.FreeBSD.org mirrors... 2 mirrors found.
Fetching snapshot tag from portsnap1.FreeBSD.org... done.
Fetching snapshot metadata... done.
Updating from Wed Jan 14 14:59:46 CET 2009 to Wed Jan 14 16:09:42 CET 2009.
[...]
Building new INDEX files... done.
[root@freebsd:/usr/src]$ zfs set mountpoint=/dpool/jails/v8.1.0/template/usr/ports/ dpool/jails/ports
[root@freebsd:/usr/src]$ ln -s /tmp /dpool/jails/v8.1.0/template/usr/ports/distfiles
[root@freebsd:/usr/src]$ ls -l /dpool/jails/v8.1.0/template/usr/ports/distfiles
lrwxr-xr-x  1 root  wheel  4 Jan 14 17:31 /dpool/jails/v8.1.0/template/usr/ports/distfiles -> /tmp
```

A *jail* elindítása egyszer dolog, a *jail* parancsot tudjuk használni, s értelemszeren a megfelel paramétereket (*jail* könyvtára, a *jail host* neve, a *jail* IP címe illetve a használandó *shell*):

Parancssor

```
[root@freebsd:/usr/src]$ cd ~
[root@freebsd:~]$ mount -t devfs devfs /dpool/jails/v8.1.0/template/dev
[root@freebsd:~]$ ifconfig bge1 alias 192.168.2.1 netmask 255.255.255.0
[root@freebsd:~]$ jail /dpool/jails/v8.1.0/template template 192.168.2.1 /bin/csh
template# df -h
Filesystem                    Size    Used   Avail Capacity  Mounted on
dpool/jails/v8.1.0/template    3.7G     94M    3.6G     3%    /
template# ps aux
USER   PID %CPU %MEM   VSZ   RSS  TT  STAT STARTED      TIME COMMAND
root 22015  0.0  0.0  7056  1820  p0  SJ    7:04PM   0:00.02 /bin/csh
root 22508  0.0  0.0  6788   820  p0  R+J   7:05PM   0:00.00 ps aux
template# exit
```

A *jail* IP címének léteznie kell, a fenti esetben a *192.168.2.1* a gép egyik létez interfészére felhúzott IP cím alias.

Automatikusan nem lesz hálózatuk a *jail_ben, ehhez egy NAT-ot kell beállítanunk, ezt (meglepen beszédes formában) a _/etc/ipnat.rules* fájlban tudjuk megtenni (a *bge1* az interfész neve, a *91.83.48.130* pedig a gépünk küls – publikus – IP címe):

/etc/ipnat.rules

```
map bge1 192.168.2.0/24 -> 91.83.48.130/32
```

Ezek után indítsuk el az *ipnat* programot:

Parancssor

```
[root@freebsd:~]$ echo 'ipnat_enable="YES"' >>/etc/rc.conf
[root@freebsd:~]$ /etc/rc.d/ipnat start
Installing NAT rules.
0 entries flushed from NAT table
0 entries flushed from NAT list
```

Lépjünk bele a *jail*-be és próbaképpen telepítsünk fel egy *portupgrade* csomagot:

Parancssor

```
template# cd /usr/ports/ports-mgmt/portupgrade
template# make && make install && make clean
[...]
===>   Registering installation for portupgrade-2.4.6,2
===>  Cleaning for ruby-1.8.6.287,1
===>  Cleaning for ruby18-bdb-0.6.4
===>  Cleaning for db41-4.1.25_4
===>  Cleaning for portupgrade-2.4.6,2
template# df -h
Filesystem                     Size    Used   Avail Capacity  Mounted on
dpool/jails/v8.1.0/template    3.7G    110M    3.6G     3%    /
```

Tegyünk fel néhány fontosabb csomagot, ezek nem fognak túl sok helyet elfoglalni, hiszen ezeket is klónozzuk majd. Mindenkinek saját elvárásai vannak a rendszerrel kapcsolatban, de az alábbi csomagok szinte mindenkinek jó szolgálatot tesznek:

- shells/bash
- java/jdk16
- www/links
- misc/mc
- sysutils/munin-node
- databases/mysql51-client
- security/nmap
- net/openldap24-client
- ports-mgmt/portaudit
- databases/postgresql83-client
- sysutils/screen
- sysutils/syslog-ng2
- archivers/unzip
- ftp/wget
- archivers/zip

Parancssor

```
template# df -h
Filesystem                     Size    Used   Avail Capacity  Mounted on
dpool/jails/v8.1.0/template    3.7G    584M    3.1G    16%    /
template# exit
```

Picit felhízott a *jail*, amit részben az okoz, hogy a fenti 15 csomagot telepítettünk fel (amelyek jó része függség okán feltelepített további csomagokat, amelyek úgyis kellenek majd az egyedi csomagok fordításához), másrészt az okoz, hogy a /tmp alá linkeltük a /usr/ports/distfiles könyvtárat, érdemes pár dolgot kitakarítani, mielőtt klónozzuk a *jail* fájlrendszerét:

Parancssor

```
[root@freebsd:~]$ rm -Rf /dpool/jails/v8.1.0/template/tmp/*
[root@freebsd:~]$ rm /dpool/jails/v8.1.0/template/root/.history
[root@freebsd:~]$ rm /dpool/jails/v8.1.0/template/root/.cshrc
[root@freebsd:~]$ rm /dpool/jails/v8.1.0/template/root/.profile
[root@freebsd:~]$ zfs list
NAME                                  USED  AVAIL  REFER  MOUNTPOINT
[...]
dpool/jails/ports                     156M  3.41G   156M  /dpool/jails/v8.1.0/template/usr/ports/
dpool/jails/v8.1.0                    254M  3.41G    19K  /dpool/jails/v8.1.0
dpool/jails/v8.1.0/template           254M  3.41G   254M  /dpool/jails/v8.1.0/template
```

Elkészítettünk egy közel 250MBájt helyet foglaló *jail* mintát, amelyet klónozva kevés helyet foglaló - különféle szolgáltatásokat futtató - *jail* rendszereket fogunk készíteni.