jail初心者が作るjail構築講座

Echigo BSD Users Group
神保道夫

jailとは

- jailとは、FreeBSDに標準的に備わっている、仮想マシンを実現する機能です。chrootコマンドを拡張して、ネットワーク・プロセス等も隔離できるようにしたFreeBSD(とその派生OSも含む)特有の機能です。

きっかけは・・・

- 私が普段利用しているマシンが、Pentium3 800MHzなので、make buildkernelや、bsfilterによる処理が結構遅くて苦痛になってきた。それに、耐用年数もちょっと不安なのでリプレースしたい。
- サーバーの台数を減らしたい(電力消費の問題)
- そろそろjailコマンドを覚えようかな(単純な動機)
- 上記マシンはRELENG_6_1で動いており、バージョンアップしたい。

とりあえず調べてみる

- http://www.otsune.com/bsd/jail/fulljail.html あたりがヒットした。
- jpmanもとりあえず参考にしてみよう

運用ポリシーを決める

- 常用マシンのリプレースなので、ネットワーク系のコマンド(pingやtraceroute)が使えないと困る →/etc/sysctl.confに security.jail.allow_raw_sockets=1を指定
- sshdも起動
- IPv6アドレスもつけたいところだが、jailでは対応していないので今回は諦める(;_;)
- 自分だけしか使わないホストだが、元のサーバーではanonymous FTPを扱っていたので、それはホストOSに引越しさせる。

jail環境の構築(1)

- 前述したとおり、常用環境のリプレースなので、fat jail(フルツリー)で構築する。
- ディレクトリは、/home/jail/casper内に構築。
- システムのビルド。(今回はホストのsrcから作る)
- mkdir -p /home/jail/casper
- make installworld DESTDIR=/home/jail/casper

jail環境の構築(2)

- make distributibutition DESTDIR=/home/jail/casper
- mount_devfs devfs /home/jail/casper/dev
- chroot /home/jail/casper/dev
- touch /etc/fstab
- newaliases
- /etc/resolv.confを編集
- passwd root で、rootのパスワードを編集
- touch /etc/wall_cmos_clock

jail環境の構築(3)

- ln -s /usr/share/zoneinfo/Asia/Tokyo /etc/localtime
- /etc/syslog.confの、/dev/consoleへの出力をコメントアウトする
- /etc/crontabの、adjkerntzの実行をコメントアウトする
- /etc/rc.conf を作成する
- /etc/make.conf に、WITHOUT_IPV6="YES"を追加する。
- ホストOSに戻り、/etc/rc.conf のネットワークインターフェースにaliasでIPアドレスを振る。
- /etc/rc.confに、jailの設定を追加する。

jail環境の構築(4)

- jail_jail1_rootdir="/home/jail/casper"
- jail_jail1_hostname="casper.jinbo.jp"
- jail_jail1_ip="210.229.61.xxx"
- jail_jail1_interface=""
- jail_jail1_exec_start="/bin/sh /etc/rc"
- jail_jail1_exec_stop="/bin/sh /etc/rc.shutdown"
- jail_jail1_devfs_enable="YES"
- jail_jail1_fdescfs_enable="NO"
- jail_jail1_procfs_enable="YES"
- jail_jail1_mount_enable="NO"
- jail_jail1_devfs_ruleset="ruleset_name"
- jail_jail1_fstab=""
- jail_jail1_flags="-l -U root"

jail環境の構築(5)

- ここまでできたら、/etc/rc.d/jail start してみて、うまく動くことを確認してみる。
- jail内のportsは、jail内で管理することにしたので、csup等で取ってきて、別途makeする。

Jail環境のupdate

- FreeBSD SAなどが出た際に、ホストOSとゲストOSをいっぺんに更新したいときがある。その際は以下の様な形でupdateすると良い。
  make installworld DESTDIR=/home/jail/casper
  mergemaster -D /home/jail/casper

まとめ

- Jail環境に移行することにより、本来の目的である、マシンの高速化が実現できた。ただし、マシンのディスクが破損した場合は被害が2台分になるので、RAID1などを組むなど、それなりの対策を取る必要があるだろう。