Toward an apt/yum-like NetBSD maintenance

Ken'ichi Fukamachi

http://www.nsrg.fml.org/

fukachan@fml.org k-fukama@photon.chitose.ac.jp

(obsoleted: kfuka@iij.ad.jp fukachan@sapporo.iij.ad.jp fukachan@phys.titech.ac.jp)

2018/03/09

Index

- Purpose
- Requirements
- Implementation
- TODOs

Purpose

provide a NetBSD maintenance like apt/yum.

- integrated automatic vulnerability check for both base system and pkgsrc.
- automatic update
  - replace (deinstall and install)
  - daemon restart if needed
    (preferrable not to forget after security update ;-)
- better for advocacy ?

[image]

```
% napt update
% napt upgrade
   ....
   deinstalling openssl
     installing openssl
      restaring postfix
      restaring bind99
   ...
```

Requirements

- a packaged base system
- daily updated base system delivery
- base-vulnerabilities database

Basepkg: What is it?

- split the NetBSD base system to 800+ archives.
- the archive format is same as pkgsrc one.
  - pkg_* can handle them.
  - more useful in using more clever tools such as pkgsrc/pkgtools/pkgin
- 1.4 released a few hours ago (2018/03/09 16:00)
- Next morning, Master Enomoto explains it :-)

Basepkg: Base package delivery system (work-in-progress)

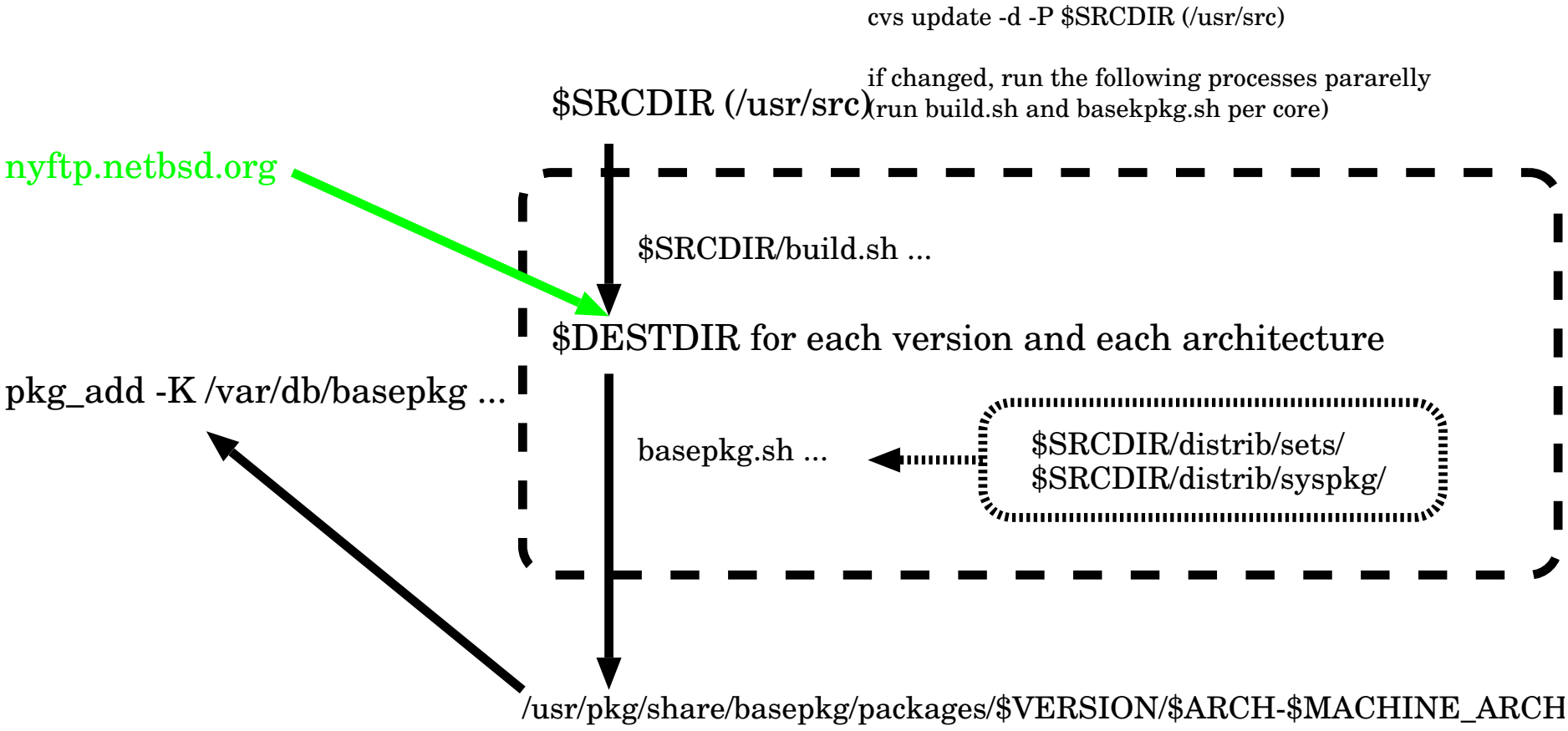
- (trial now)
- http://basepkg.netbsd.fml.org
- it has been running on SAKURA VPS(v3) 2G plan: 3 CORE CPU, 200GB storage, about 150 USD (16,745 JPY) per year

Basepkg: Base package delivery: plan 1

- just a web server
- update /usr/src
- build /usr/src per ARCH per CPU (5h per TARGET)
- run basepkg for all targets (20m per TARGET)
- too long ;-)

Basepkg: Base package delivery: plan 2

- get binaries from daily build system nycdn.netbsd.org (? mins)
- same steps above ...
- build may end within practical processing time.


cvs update -d -P $SRCDIR (/usr/src)
if changed, run the following processes pararelly
(run build.sh and basekpkg.sh per core)
$SRCDIR (/usr/src)
nyftp.netbsd.org
$SRCDIR/build.sh ...
$DESTDIR for each version and each architecture
pkg_add -K /var/db/basepkg ...
basepkg.sh ...
$SRCDIR/distrib/sets/
$SRCDIR/distrib/syspkg/
/usr/pkg/share/basepkg/packages/$VERSION/$ARCH-$MACHINE_ARCH

[image] vulnerability databases

- /var/db/pkg/pkg-vulnerabilities

```
[pkg-vulnerabilities]
openssl<1.0.2n  multiple-vulnerabilities

[base-vulnerabilies]
openssl<20180102 multiple-vulnerabilities
```

TODO

- more disk or more power or ... ? ;-)
- which version we support ?
- fool-proof user friendly tool
  based on pkgsrc/pkgtools/pkgin not pkg_*
- how to maintain base vulnerability databases
- integration with **vuls**

TODO: which version we support

It must be enough to support the daily updated packages for the following versions:

- Current
- netbsd-7 only

TODO: fool-proof utilities

- we need to provide a good UI to avoid critical mis-operations such as; overwrite files in /etc ....
- how to avoid invalid replacement of lib* blue-green deployment ?
  - install lib(new) not remove lib(old)
  - lib(new) and lib(old)
  - tune library search path

Extension: port a packaged base?

- **basepkg** is built on pkgsrc framework.
- we can split the system if the meta-data ready.
- ? we can port it to
  - MINIX 3.2
  - DragonflyBSD
  - OpenBSD