네임데몬을 nobody로 운영하기

Scott Wunsch, *scott@wunsch.org* <mailto:scott@wunsch.org>

번역자 임승환*kilhan@kldp.org* <mailto:kilhan@kldp.org>

v1.0, 13 March 2000

 개념을 정리하기 보다는 실제적으로 유용하게 쓰일수 있도록 설치를 지원해주는 문서로 작성하였습니다.

목 차

제 1 절 BIND설치준비

1.1 어떻게?

이 문서는 BIND패키지를 설치 할때 추가적인 보안사항에 대하여 설명한다. 그것은 bind패키지가 'chroot'외부로 읽거나 다른 허가권을 가질수 없도록 설정하는것을 의미한다. 또한 이것은 'root'(시스템 관리자)이외의 사용자로서 설정할수 있도록 할것이다. chroot에 뒤의 이 과정은 간단하다. BIND나 다른 어떤 process도 chroot 에서 수행되도록 하면 chroot 이외를 보거나 다른 filesystem을 읽는것은 불가능하다. 예를 들면 이 문서 안에서 BIND를 디렉토리/chroot/named에 chrooted되게 설정할 것이다. 그렇게 된다면 BIND로써는 이 문서가 있는 현재 디렉토리를 / 으로 알게된다.즉 chroot 외의 디렉토리에 대한 허가권이 없어지는것이다. 아마 Anonymous FTP로 서비스 하는곳에 로그인 하였다면 chroot에 대해서 알것이다.

1.2 왜?

chroot로 BIND를 운영하는 것은 악의적인 사용자들로부터 BIND를 운영시 발생할수 있는 위험을 제한 하기 위함이다. 같은 이유로 BIND를 root(시스템 운영자)가 아닌 사용자로부터 운영하고자 한다.

1.3 어디서?

문서의 최근은 다음에서 얻을수 있다. `www.losurs.org/docs/howto/Chroot-BIND.html` BIND는 the Internet Software Consortium 에서 즉`www.isc.org/bind.html` 에서 얻을수 있고 최근의 가장 최신 버전은 8.2.2_P5 이다. *1.4와 1.5는 생략합니다.*

1.4 How?

wrote this document based on my experiences in setting BIND up in a chroot environment. In my case, I already had an existing BIND installation in the form of a package that came with my Linux distribution. I'll assume that most of you are probably in the same situation, and will simply be transferring over and modifying the configuration files from your existing BIND installation, and then removing the package before installing the new one. Don't remove the package yet, though; we may want some files from it first. If this is not the case for you, you should still be able to follow this document. The only difference is that, where I refer to copying an existing file, you first have to create it yourself. The DNS HOWTO may be helpful for this.

1.5 Disclaimer

These steps worked for me, on my system. Your mileage may vary. This is but one way to approach this; there are other ways to set the same thing up (although the general approach will be the same). My BIND experience to date has been installing on Linux servers. However, most of the instructions in this document should be easily applicable to other flavours of UNIX as well, and I shall try to point out differences of which I am aware.

제 2 절 Preparing the Jail (chroot를 위한 준비)

2.1 사용자를 추가합니다.

(원본글에서는 named 사용자를 추가하였습니다. 번역글에서는 nobody를 사용하기에 대부분의 계정에서는 이미 생성되어 있을것 입니다.) /etc/passwd 에 다음을 추가한다. named:x:200:200:Nameserver:/chroot/named:/bin/false /etc/group 에 다음을 추가한다. named:x:200: 셸을 /bin/false를 준것은 로그온 하지 못하게 하기 위함이다.

2.2 디렉토리 구조

다음과 같은 디렉토리 구조를 만들자.

```
/chroot
  +-- named
       +-- bin +-- dev +-- etc |     +-- namedb +-- lib +-- var
            +-- run
```

2.3 기존의 BIND정보를 옮겨 오자.

이미 기존의 BIND를 설치하거나 운영해오고 있을 경우 named.conf나 zone화일이 있을경우 chroot 복사(이동)로 복사느 이동을 한다. /etc/named.conf 는 /chroot/named/etc 로 zone화일은 /chroot/named/etc/namedb로 옮긴다. 예를 들면 다음과 같다.

```
# cp -p /etc/named.conf /chroot/named/etc/ # cp -a /var/named/*
/chroot/named/etc/namedb/
```

만약 master가 아닌 slave로 bind를 운영하고자 하거나 기타 여러가지 이유로 BIND가 zone화일에 허가권이 있어야 할것이다. 다음예와 같이 소유권을 바꾸자 # chown -R named:named /chroot/named/etc/namedb (참고로 본인은 nobody로 운영하기를 원했으므로 # chown -R nobody:nobody /chroot/named/etc/namedb 해주었습니다.) BIND는 또한 /var/run에 pid화일과 ndc에서 사용하는 socket를 적을수 있는 허가권이 필요 합니다. 따라서 다음예와 같이 소유권을 줍니다. # chown named:named /chroot/named/var/run (참고로 본인은 nobody로 운영하기를 원했으므로 # chown -R nobody:nobody /chroot/named/var/run 해주었습니다.)

2.4 시스템에서 필요한 화일 추가

BIND를 chroot에서 운영하게 되면 chroot외에는 허가권이 없기 때문에 몇개의 화일들(특히 시스템 라이브러리) 이 필요 합니다. 아래의 명령어는 필요한 라이브러리를 chroot안에서 읽을수 있도록 해주는 작업입니다. 보통의 LINUX머쉰에서는 작동될것 입니다.

```
# cd /chroot/named/lib # cp -p /lib/libc-2.*.so .  # ln -s libc-2.*.so
libc.so.6 # cp -p /lib/ld-2.*.so .  # ln -s ld-2.*.so ld-linux.so.2
```

BIND가 chroot로 운영될때는 chroot안에 /dev/null이 있어야 합니다. /dev/MKDEV 의 메뉴얼이나 mknod의 메뉴얼을 확인해 보십시요. 아래의 명령행은 보통의 LINUX머쉰에서는 작동될것 입니다. # mknod /chroot/named/dev/null c 1 3 마지막으로 /etc 디렉토리를 chroot안에 역시 만들어야 합니다. 그리고 /etc/localtime화일을 chroot안으로 복사 해야만 BIND log가 정확한 시간에 기록될것입니다. 또한 간단한 group화일을 생성해야할것 입니다. 다음의 명령행을 참고 하세요 # cp /etc/localtime /chroot/named/etc/ # echo 'named:x:200:' > /chroot/named/etc/group (처음에 만들때 원본에서 GID 200을 준것을 주의 하십시요 저는 nobody로 생성하기 때문에 echo 'nobody:x:99:' > /chroot/named/etc/group 하였습니다)

2.5 로그생성

sysclogd를 통하여 로그를 생성하는 방법은 두가지가 있다고 합니다. 이것은 시스템 마다 설정이 다를수 있기 때문에 RedHat에서 사용하는 첫번째 방법만 설명하겠습니다. 보통 syslogd는 다음의 화일을 통하여 운영됩니다. /etc/rc.d/init.d/syslog 이 화일을 아래 부분은 고쳐 주십시요 daemon syslogd -m 0 을 이렇게 daemon syslogd -m 0 -a /chroot/named/dev/log 고쳤으니 데몬을 재구동 하십시요.

```
# /etc/rc.d/init.d/syslog stop
#/etc/rc.d/init.d/syslog start
```

아래와 같은 화일이 발견되면 정상적인것입니다.

```
  /chroot/named/dev
srw-rw-rw-   1 root     root            0 Mar 13 20:58 log
다른 방법은..  If you have an older syslogd, then you'll have to find
another way to do your logging. There are a couple programs out there,
such as holelogd, which are designed to help by acting as a ``proxy''
and accepting log entries from the chrooted BIND and passing them out
to the regular /dev/log socket.  입니다.
```

제 3 절 BIND를 컴파일 합니다.

www.isc.org/bind.html <http://www.isc.org/bind.html> 나 다른 미러 싸이트에 가서 최신의 bind를 구합니다.

3.1 경로를 수정해 줍니다.

(confusing할수 있다고 합니다. ^^) 기본 디렉토리는 /var/run이고 이것은 chroot안에 위치시켜야 합니다. ndc또한 다른 디렉토리에 위치하기 때문에 수정해주어야 합니다. 리눅스 시스템이라고 가정하고 다음 화일을 다음과 같이 수정해 줍니다. src/port/linux/Makefile.set 의 화일내부의 DESTRUN=/var/run 을 DESTRUN=/chroot/named/var/run 으로 수정해 줍니다. (While you're in there, you may want to change the other destination paths from /usr to /usr/local.) 네임 데몬만 빼고는 모두 chroot안에서 좀더 수정해 줍니다. src/bin/named/named.h 화일은 #include "pathnames.h" 을 #define _PATH_NDCSOCK "/var/run/ndc" 으로 수정해 줍니다.

3.2 화일을 생성합니다.

INSTALL화일을 읽어 보고 보통 설치를 하나 이 곳에서는 만들기만 하지 설치를 하지는 않습니다. 물론 이것도 INSTALL화일에 적혀있는 것과 다르지 않습니다. 아래와 같이 보통 명령행을 입력해 줍니다.

```
#make clean #make depend #make
```

제 4 절 새롭게 만들어진 BIND를 설치 합니다.

보통 이전에 rpm이나 기타 다른것으로 설치되어 있는것이 있다면 제거 해도 좋습니다. RedHat을 사용하는 Linux라면 bind, bind-utils, bind-devel, caching-nameserver이 설치되어 있을것입니다. /etc/rc.d/init.d/named 스크립트가 있다면 지우기전에 보관하는것이 좋을것입니다.

4.1 chroot밖에서의 설치

This is the easy part :-). /usr/local/sbin/named 데몬을 실수 방지를 위해 권한을 000줍니다. #chmod 000 /usr/local/sbin/named

4.2 chroot안에서의 설치

named daemon 화일과 named-xfer(zone trandfer를 위한 화일)을 보통 복사 합니다.

```
 # cp src/bin/named/named /chroot/named/bin
# cp src/bin/named-xfer/named-xfer /chroot/named/bin
```

4.3 시작 스크립트를 작성합니다.

보통 RedHat 6.0 system에서는 다음과 같습니다. -u 는 실행된 후에 네인서버의 변경될 사용자 ID를 말합니다. -g 는 실행된 후에 네인서버의 변경될 사용자 group를 말합니다. -t 는 chroot를 적용할 디렉토리를 말합니다. >>>>daemon /chroot/named/bin/named -u named -g named -t /chroot/named 원본에는 위와 같았으나 저는 아래같이 수정하였습니다. >>>>daemon /chroot/named/bin/named -u nobody -g nobody -t /chroot/named

아래 스크립트는 /etc/rc.d/init.d/named 에 저장 합니다.

```
 #!/bin/sh #
#named           This shell script takes care of starting and stopping #
named (BIND DNS server).  # # chkconfig: 345 55 45 # description: named
(BIND) is a Domain Name Server (DNS) \ # that is used to resolve host
names to IP addresses.  # probe: true
# Source function library.  . /etc/rc.d/init.d/functions
# Source networking configuration.  . /etc/sysconfig/network
# Check that networking is up.  [ ${NETWORKING} = "no" ] && exit 0
[ -f /chroot/named/bin/named ] || exit 0
[ -f /chroot/named/etc/named.conf ] || exit 0
# See how we were called.  case "$1" in
  start)
        # Start daemons.  echo -n "Starting named: " daemon
        /chroot/named/bin/named -u named -g named -t /chroot/named echo
        touch /var/lock/subsys/named ;;
  stop)
        # Stop daemons.  echo -n "Shutting down named: " killproc named
        rm -f /var/lock/subsys/named echo ;;
  status)
        /usr/local/sbin/ndc status exit $?  ;;
  restart)
        /usr/local/sbin/ndc restart exit $?  ;;
  reload)
        /usr/local/sbin/ndc reload exit $?  ;;
  probe)
        # named knows how to reload intelligently; we don't want linuxconf
        # to offer to restart every time /usr/local/sbin/ndc reload
        >/dev/null 2>&1 || echo start exit 0 ;;
  *)
```

```
        echo "Usage: named {start|stop|status|restart}" exit 1
esac
exit 0
```

4.4 설정 변경

named.conf 에 적용된 설정 몇개를 변경해야 할지도 모릅니다. 변경해야 할것들은 아래예들 등입니다.

```
directory "/etc/namedb"; pid-file "/var/run/named.pid"; named-xfer
"/bin/named-xfer";
```

(%주의%) 절대 directory 안에다가 /chroot/named/etc으로 적지 마십시요 /chroot가 /라고 생각하므로 위에 설정대로 진행하였다면 보통 /etc/namedb 이렇게 될것 입니다.

제 5 절 BIND를 실행합니다.

보통 RedHat 6.0 system에서는 다음과 같습니다. /etc/rc.d/init.d/named start 예전 버전이나 이미 시작되어 있던것이 작동하는것이 아닌지 주의 하십시요 제대로 되지 않았다면 log나 설정을 살피십시오. 언제나 그렇듯이 무소식이 희소식입니다.^^