Bind-Chroot-Howto (Debian)

Version 1.0

Author: Falko Timme

Last edited 02/03/2005

This document describes how to install the DNS server Bind on Debian so that it runs out of a chroot jail for security reasons.

This howto is meant as a practical guide; it does not cover the theoretical backgrounds. They are treated in a lot of other documents in the web.

This document comes without warranty of any kind!

Install Bind And Chroot It

apt-get install bind9

For security reasons we want to run BIND chrooted so we have to do the following steps:

/etc/init.d/bind9 stop

Edit the startup script /etc/init.d/bind9 so that the daemon will run as the unprivileged user 'nobody', chrooted to /var/lib/named. Modify the line: OPTS="" so that it reads OPTS="-u nobody -t /var/lib/named":

```sh
#!/bin/sh
PATH=/sbin:/bin:/usr/sbin:/usr/bin
# for a chrooted server: "-u nobody -t /var/lib/named"
OPTS="-u nobody -t /var/lib/named"
test -x /usr/sbin/named || exit 0
case "$1" in
    start)
        echo -n "Starting domain name service: named"
        start-stop-daemon --start --quiet
                --pidfile /var/run/named.pid --exec /usr/sbin/named -- $OPTS
        echo "."
    ;;
    stop)
        echo -n "Stopping domain name service: named"
        /usr/sbin/rndc stop
        echo "."
    ;;
    reload)
        /usr/sbin/rndc reload
    ;;
    restart|force-reload)
        $0 stop
        sleep 2
        $0 start
    ;;
    *)
        echo "Usage: /etc/init.d/bind {start|stop|reload|restart|force-reload}"
>&2
        exit 1
    ;;
esac
```

```
exit 0
```

Create the necessary directories under /var/lib:

```
mkdir -p /var/lib/named/etc
mkdir /var/lib/named/dev
mkdir -p /var/lib/named/var/cache/bind
mkdir /var/lib/named/var/run
```

Then move the config directory from /etc to /var/lib/named/etc:

```
mv /etc/bind /var/lib/named/etc
```

Create a symlink to the new config directory from the old location (to avoid problems when bind is upgraded in the future):

```
ln -s /var/lib/named/etc/bind /etc/bind
```

Make null and random devices, and fix permissions of the directories:

```
mknod /var/lib/named/dev/null c 1 3
mknod /var/lib/named/dev/random c 1 8
chmod 666 /var/lib/named/dev/null /var/lib/named/dev/random
chown -R nobody:nogroup /var/lib/named/var/*
chown -R nobody:nogroup /var/lib/named/etc/bind
```

We need to modify the startup script /etc/init.d/sysklogd of sysklogd so that we can still get important messages logged to the system logs. Modify the line: SYSLOGD="" so that it reads: SYSLOGD="-a /var/lib/named/dev/log":

```
#! /bin/sh
# /etc/init.d/sysklogd: start the system log daemon.
PATH=/bin:/usr/bin:/sbin:/usr/sbin
pidfile=/var/run/syslogd.pid
binpath=/sbin/syslogd
test -x $binpath || exit 0
# Options for start/restart the daemons
#   For remote UDP logging use SYSLOGD="-r"
#
SYSLOGD="-a /var/lib/named/dev/log"
create_xconsole()
{
    if [ ! -e /dev/xconsole ]; then
        mknod -m 640 /dev/xconsole p
    else
        chmod 0640 /dev/xconsole
    fi
    chown root.adm /dev/xconsole
}
running()
{
    # No pidfile, probably no daemon present
    #
```

```
    if [ ! -f $pidfile ]
    then
        return 1
    fi
    pid=`cat $pidfile`
    # No pid, probably no daemon present
    #
    if [ -z "$pid" ]
    then
        return 1
    fi
    cmd=`cat /proc/$pid/cmdline | tr "\000" "
"|head -1`
    # No syslogd?
    #
    if [ "$cmd" != "$binpath" ]
    then
        return 1
    fi
    return 0
}
case "$1" in
  start)
    echo -n "Starting system log daemon: syslogd"
    create_xconsole
    start-stop-daemon --start --quiet --exec $binpath -- $SYSLOGD
    echo "."
    ;;
  stop)
    echo -n "Stopping system log daemon: syslogd"
        start-stop-daemon  --stop  --quiet  --exec  $binpath  --pidfile  $pidfile
    echo "."
    ;;
  reload|force-reload)
    start-stop-daemon --stop --quiet --signal 1 --exec $binpath --pidfile $pidfile
    ;;
  restart)
    echo -n "Stopping system log daemon: syslogd"
        start-stop-daemon  --stop  --quiet  --exec  $binpath  --pidfile  $pidfile
    echo "."
    sleep 1
    echo -n "Starting system log daemon: syslogd"
    start-stop-daemon --start --quiet --exec $binpath -- $SYSLOGD
    echo "."
    ;;
  reload-or-restart)
    if running
    then
          start-stop-daemon --stop --quiet --signal 1 --exec $binpath --pidfile
$pidfile
    else
                start-stop-daemon  --start  --quiet  --exec  $binpath  --  $SYSLOGD
    fi
    ;;
  *)
```

```
    echo "Usage: /etc/init.d/sysklogd
{start|stop|reload|restart|force-reload|reload-or-restart}"
    exit 1
esac
exit 0
```

Restart the logging daemon:

```
/etc/init.d/sysklogd restart
```

Start up BIND, and check /var/log/syslog for any errors:

```
/etc/init.d/bind9 start
```

Good luck!

From http://www.falkotimme.com/howtos/debian_bind_chroot/index.php

current rating:

image:rdf newsfeed / //static.linuxhowtos.org/data/rdf.png (null)
 |
image:rss newsfeed / //static.linuxhowtos.org/data/rss.png (null)
 |
image:Atom newsfeed / //static.linuxhowtos.org/data/atom.png (null)
- Powered by
image:LeopardCMS / //static.linuxhowtos.org/data/leopardcms.png (null)
 - Running on
image:Gentoo / //static.linuxhowtos.org/data/gentoo.png (null)
 -
Copyright 2004-2020 Sascha Nitsch Unternehmensberatung GmbH
image:Valid XHTML1.1 / //static.linuxhowtos.org/data/xhtml.png (null)
 :
image:Valid CSS / //static.linuxhowtos.org/data/css.png (null)
 :
image:buttonmaker / //static.linuxhowtos.org/data/buttonmaker.png (null)
- Level Triple-A Conformance to Web Content Accessibility Guidelines 1.0 -
- Copyright and legal notices -
Time to create this page: ms
<!--
image:system status display / /status/output.jpg (null)
-->