Bind absichern

rekursive Abfragen abschalten

```
options {
  recursion no;
};
```

rekursive Abfragen verbieten

`/etc/bind/named.conf.options` (Debian)

`/etc/bind/named.conf` (SuSE)

```
acl friendly {
  192.168.1.0/24;
};

options {
  allow-recursion { friendly; };
};
```

1)

2)

Zonentransfer verbieten

`/etc/bind/named.conf.options` (Debian)

`/etc/bind/named.conf` (SuSE)

```
acl internal {
  127.0.0.1/32;           // localhost
};

acl friendly {
  internal;
  192.168.1.204;          // slave DNS
};

options {
  allow-transfer { friendly; };
};
```

Oder, alternativ, nur für eine Zone:

`/etc/bind/named.conf.local` (Debian)

`/etc/bind/named.conf` (SuSE)

```
zone "linuxhotel.de" {
    type master;
    file "master/linuxhotel.de";
    allow-transfer { friendly; };
};
```

IPv6 ausschalten

`/etc/bind/named.options` : (Debian 4.0)

```
options {
…
        listen-on-v6 { none; };
…
};
```

bind in chroot

- Bei SuSE ist das automatisch so,
- bei RedHat 6 gibt es ein Paket `bind-chroot`,
- bei debian sarge muß man noch etwas Hand anlegen:

`/etc/default/bind9`:

```
CHROOT="/var/lib/bind"
OPTIONS="-u bind -t $CHROOT"

test -d $CHROOT/var/run         || mkdir -p $CHROOT/var/run
test -d $CHROOT/var/run/bind    || mv /var/run/bind $CHROOT/var/run
test -e /var/run/bind           || ln -s $CHROOT/var/run/bind /var/run/bind

test -d $CHROOT/var/cache       || mkdir -p $CHROOT/var/cache
test -d $CHROOT/var/cache/bind  || mv /var/cache/bind $CHROOT/var/cache
test -e /var/cache/bind         || ln -s $CHROOT/var/cache/bind
/var/cache/bind

test -d $CHROOT/dev             || mkdir -p $CHROOT/dev
test -c $CHROOT/dev/null        || mknod $CHROOT/dev/null c 1 3
test -c $CHROOT/dev/random      || mknod $CHROOT/dev/random c 1 8
chmod 666 $CHROOT/dev/random $CHROOT/dev/null

test -d $CHROOT/etc             || mkdir -p $CHROOT/etc
```

```
test -d $CHROOT/etc/bind       && rm -r $CHROOT/etc/bind
cp -a /etc/bind $CHROOT/etc
```

Ab Debian lenny reicht:

`/etc/default/bind9` :

```
OPTIONS="-u bind -t /var/lib/named"
```

Beim nächsten restart läuft bind in einer chroot-Umgebung. Überprüfen: [3)]

```
/etc/init.d/bind9 restart
ls /proc/`pgrep named`/root
```

[1)]
oder, wenn man einen hidden primary Nameserver betreibt sogar:

```
options {
  allow-query { friendly; };
};
```

[2)]
`allow-query-cache` muss nicht zusätzlich eingeschränkt werden, da es per default den Wert von `allow-recursion` übernimmt.
[3)]
Anders als in manchen HowTos beschrieben ist es nicht notwendig `/dev/log` ins chroot zu legen und den Syslog anzupassen. `named` macht erst einen `connect` mit `/dev/log` und erst danach `chroot`.