Vorraussetzung: bind als caching only nameserver

Vorbereiten

systemd-resolvd

„systemd-resolved is not intended to be used on DNS servers. If you’re running a DNS server, you’ll need to disable systemd-resolved before setting up BIND or Unbound instead“

CentOS 7

Paket `caching-nameserver` deinstallieren

DNSSEC temporär abschalten

`/etc/named.conf` : CentOS (ab 6)

`/etc/bind/named.conf.options` : Debian (ab 7)

```
options {
…
        // In der Praxis ist DNSSEC eine gute Sache ... aber zum Lernen erst
mal aus:
        dnssec-enable no;
        dnssec-validation no;
        dnssec-lookaside no;
…
}
```

[1)]

```
named-checkconf
rndc reconfig
```

testen

Eine mit DNSSEC signierte Zone abfragen:

Ein validierender Nameserver sollte bei einer signierten Zone liefern:

```
dig www.posteo.de @1.1.1.1
```

```
flags: … ad
```

Unser Nameserver sollte das ad-Flag nicht setzen.

eigene Zonen in bind verwalten

Vorwärts-Zone

Zonendatei

Unter Debian und CentOS empfehlen wir ein entsprechendes Verzeichnis `master` für die Zonendateien noch anzulegen [2)]:

Debian :

```
mkdir /var/cache/bind/master
```

CentOS (ab 5) :

```
mkdir /var/named/master
```

`/var/named/master/linuxhotel.de` : (CentOS ab 5)

`/var/lib/named/master/linuxhotel.de` : (SuSE ab 10.0)

`/var/cache/bind/master/linuxhotel.de` : (Debian ab 3.1)

```
$ORIGIN . ; hilft Tippfehler (fehlender . am Ende) zu vermeiden
$TTL 2m   ; time to live: 2 Minuten, default wäre 2 Tage
linuxhotel.de. IN SOA notebook20.linuxhotel.de.
root.notebook20.linuxhotel.de. (
        1             ; Seriennummer
        1h20m         ; refresh      / 1 Stunde 20 Minuten
        1d12h         ; retry        / 1,5 Tage
        1w            ; expire       / 1 Woche
        60s           ; negative ttl / 60 Sekunden
)

; Nameserver:
linuxhotel.de.                  IN NS notebook20.linuxhotel.de.

; kanonische IP-Adressen:
notebook22.linuxhotel.de.       IN A 192.168.1.222
notebook05.linuxhotel.de.       IN A 192.168.1.205
notebook20.linuxhotel.de.       IN A 192.168.1.220
notebook06.linuxhotel.de.       IN A 192.168.1.206
notebook09.linuxhotel.de.       IN A 192.168.1.209

; Aliase:
peter.linuxhotel.de.            IN CNAME notebook09.linuxhotel.de.
lothar.linuxhotel.de.           IN CNAME notebook05.linuxhotel.de.
```

```
heribert.linuxhotel.de.          IN CNAME notebook06.linuxhotel.de.
bjoern.linuxhotel.de.            IN CNAME notebook20.linuxhotel.de.
admin.linuxhotel.de.             IN CNAME notebook22.linuxhotel.de.
```

Zonendatei überprüfen

CentOS (ab 5)

```
named-checkzone -D linuxhotel.de. /var/named/master/linuxhotel.de
```

SuSE (ab 10.0)

```
named-checkzone -D linuxhotel.de. /var/lib/named/master/linuxhotel.de
```

Debian (ab 3.1)

```
named-checkzone -D linuxhotel.de. /var/cache/bind/master/linuxhotel.de
```

Konfigurationsdatei

`/etc/named.conf` : (SuSE 10.2)

`/etc/named.conf` : (CentOS ab 5)

`/etc/bind/named.conf.local` : (Debian ab 5.0)

```
zone "linuxhotel.de" {
  type master;
  file "master/linuxhotel.de";
};
```

Konfigdatei und eingetragene Zonen überprüfen:

```
named-checkconf -z
```

bind die Änderung mitteilen

```
rndc reconfig
```

oder

openSuSE, centos (ab 7)

```
service named reload
```

Debian (ab 6)

```
service bind9 reload
```

im Log prüfen, ob es Fehler gab

Debian (ab 10)

```
journalctl -eu bind9.service
```

testen

```
host peter.linuxhotel.de 127.0.0.1
dig peter.linuxhotel.de @127.0.0.1 any
```

Zonendatei (kurze Schreibweise)

Das Format der Zonendatei [3] läßt es auch zu, diese Datei sehr viel kürzer zu schreiben:

```
$TTL 2h
@ IN SOA notebook20 root.notebook20 1999022301 1d 2h 5w 2d

; Nameserver:
                IN NS notebook20

; kanonische IP-Adressen:
notebook22      IN A 192.168.1.222
notebook05      IN A 192.168.1.205
notebook20      IN A 192.168.1.220
notebook06      IN A 192.168.1.206
notebook09      IN A 192.168.1.209

; Aliase:
peter           IN CNAME notebook09
lothar          IN CNAME notebook05
heribert        IN CNAME notebook06
bjoern          IN CNAME notebook20
admin           IN CNAME notebook22
```

Hier habe ich die Zeitangaben im SOA entsprechend der Empfehlungen des Ripe [4] gewählt.

Bei jeder Änderung der Zonendatei sollte die Seriennummer hochgezählt werden.

Zonendatei überprüfen

CentOS

```
named-checkzone -D linuxhotel.de. /var/named/master/linuxhotel.de
```

SuSE

```
named-checkzone -D linuxhotel.de. /var/lib/named/master/linuxhotel.de
```

Debian

```
named-checkzone -D linuxhotel.de. /var/cache/bind/master/linuxhotel.de
```

bind die Änderung mitteilen

```
rndc reload linuxhotel.de
```

Rückwärts-Zone

Zonendatei

/var/named/master/1.168.192.in-addr.arpa: (CentOS)

/var/lib/named/master/1.168.192.in-addr.arpa: (SuSE 10.0)

/var/cache/bind/master/1.168.192.in-addr.arpa: (Debian 3.1)

```
$TTL 2h
1.168.192.in-addr.arpa. IN SOA notebook20.linuxhotel.de.
root.notebook20.linuxhotel.de. (
    2005082401    ; serial
    3h            ; refresh
    1h            ; retry
    1w            ; expire
    1h            ; negative ttl
)
; Nameserver
1.168.192.in-addr.arpa. IN NS notebook20.linuxhotel.de.

; kanonische IP-Adressen
205.1.168.192.in-addr.arpa. IN PTR notebook05.linuxhotel.de.
220.1.168.192.in-addr.arpa. IN PTR notebook20.linuxhotel.de.
```

```
206.1.168.192.in-addr.arpa. IN PTR notebook06.linuxhotel.de.
209.1.168.192.in-addr.arpa. IN PTR notebook09.linuxhotel.de.
222.1.168.192.in-addr.arpa. IN PTR notebook22.linuxhotel.de.
```

testen

CentOS (ab 5)

```
named-checkzone -D linuxhotel.de. /var/named/master/linuxhotel.de
named-checkzone -D 1.168.192.in-addr.arpa. /var/named/master/1.168.192.in-
addr.arpa
```

SuSE (ab 10.0)

```
named-checkzone -D linuxhotel.de. /var/lib/named/master/linuxhotel.de
named-checkzone -D 1.168.192.in-addr.arpa.
/var/lib/named/master/1.168.192.in-addr.arpa
```

Debian (ab 3.1)

```
named-checkzone -D linuxhotel.de. /var/cache/bind/master/linuxhotel.de
named-checkzone -D 1.168.192.in-addr.arpa.
/var/cache/bind/master/1.168.192.in-addr.arpa
```

Konfigurationsdatei

`/etc/named.conf` : (SuSE 10.2)

`/etc/named.conf` : (CentOS)

`/etc/bind/named.conf.local` : (Debian 3.1)

```
zone "1.168.192.in-addr.arpa" {
      type master;
      file "master/1.168.192.in-addr.arpa";
};
```

testen

```
named-checkconf -z
```

bind die Änderung mitteilen

```
rndc reconfig
```

testen

```
host 192.168.1.222 127.0.0.1
dig -x 192.168.1.222 @127.0.0.1
```

Zonendateien mit nsupdate bearbeiten

bind konfigurieren

`/etc/named.conf` : (SuSE, CentOS)

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

```
acl "nsupdate" {
  127.0.0.1;
};

zone "linuxhotel.de" {
        type master;
        allow-update { "nsupdate"; };
        file "master/linuxhotel.de";
};

zone "1.168.192.in-addr.arpa" {
        type master;
        allow-update { "nsupdate"; };
        file "master/1.168.192.in-addr.arpa";
};
```

bind Konfigurationsdatei prüfen

```
named-checkconf
```

bind Schreibzugriff auf Master-Zonendateien geben

Debian:

```
chown -R bind /var/cache/bind/master
```

Testen: Eintrag hinzufügen

```
nsupdate <<EOT

server localhost

update add notebook23.linuxhotel.de 43200 IN A 192.168.1.223

update add 223.1.168.192.in-addr.arpa 43200 IN PTR notebook23.linuxhotel.de

EOT
```

Trotz nsupdate Zonen mit Editor bearbeiten

```
rndc freeze linuxhotel.de
vim linuxhotel.de
rndc reload linuxhotel.de
rndc thaw linuxhotel.de
```

Hilfreich ist vielleicht:

`~/.bashrc` :

```
function zvi {
  cd /var/cache/bind/master
  rndc freeze $1
  vim $1
  rndc reload $1
  rndc thaw $1
  cd -
}
```

bind als slave einrichten

Mittlerweile** (Version) **sind auch die Begriffe primary und secondary als Ersatz für master und slave möglich

Master konfigurieren

Erst müssen die Slave-Nameserver in der Zonendatei des Masters eingetragen werden:

```
linuxhotel.de. IN NS notebook04.linuxhotel.de.
```

Bei SuSE muß noch der Eintrag

```
notify yes;
```

in der Datei `/etc/named.conf` eingetragen werden, oder die Zeile ganz entfernt oder auskommentiert werden.

testen: funktioniert der Master

openSuSE 12.3

```
named-checkzone -i local -D linuxhotel.de
/var/lib/named/master/linuxhotel.de
rndc reload linuxhotel.de
tail /var/log/messages
dig @127.0.0.1 linuxhotel.de NS
```

debian 8

```
named-checkzone -i local -D linuxhotel.de
/var/cache/bind/master/linuxhotel.de
rndc reload linuxhotel.de
journalctl -eu bind9
dig @127.0.0.1 linuxhotel.de NS
```

Slave konfigurieren

Vorraussetzung: Master funktioniert

```
dig @<IP-des-Masters> linuxhotel.de AXFR
```

Ausgabe muss mindestens 2 NS Records enthalten:

1. den eigenen Rechner
2. den Master

`/etc/named.conf` : (CentOS 5.3)

```
zone "linuxhotel.de" {
        type slave;
        file "slaves/linuxhotel.de";
        masters { 192.168.1.220; };
};
zone "1.168.192.in-addr.arpa" {
        type slave;
        file "slaves/1.168.192.in-addr.arpa";
        masters { 192.168.1.220; };
```

```
};
```

`/etc/named.conf` : (SuSE 10.0)

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

```
zone "linuxhotel.de" {
        type slave;
        file "slave/linuxhotel.de";
        masters { 192.168.1.220; };
};
zone "1.168.192.in-addr.arpa" {
        type slave;
        file "slave/1.168.192.in-addr.arpa";
        masters { 192.168.1.220; };
};
```

Zonendateien im Binärformat kann man mit:

```
named-checkzone -D -f raw linuxhotel.de slave/linuxhotel.de
```

anzeigen. Wenn man die Zonenfiles **lieber im Textformat statt im Binärformat** haben will, kann man in die Zone eintragen:

```
zone "…" {
  …
  masterfile-format text;
  …
```

bind Schreibzugriff auf Slave-Zonendateien geben

Debian:

```
mkdir /var/cache/bind/slave
chown bind /var/cache/bind/slave
```

testen: funktioniert der Slave?

Debian

```
named-checkconf -z
rndc reconfig
journalctl -eu bind9
ls /var/cache/bind/slave/{linuxhotel.de,1.168.192.in-addr.arpa}
dig @127.0.0.1 linuxhotel.de AXFR
```

OpenSuSE 12.3

```
named-checkconf -z
rcnamed restart
tail /var/log/messages
ls /var/lib/named/slave/{linuxhotel.de,1.168.192.in-addr.arpa}
dig @127.0.0.1 linuxhotel.de AXFR
```

testen: funktionieren alle verantwortlichen Nameserver?

```
dig @141.1.1.1 linuxhotel.de +nssearch
```

Subdomains delegieren

Übergeordneter DNS

`/etc/named.conf.local` : (Debian ab 5.0)

`/etc/named.conf` : (CentOS ab 5)

```
zone "linuxhotel.de" IN {
        type master;
        file "master/linuxhotel.de";
        forwarders      { };
};
```

Fallstrick: Unbedingt an **forwarders** denken! Und **alle** dnssec Optionen ausschalten

`/var/named/master` : (CentOS 5)

```
sub05.linuxhotel.de.        IN NS ns1.sub05.linuxhotel.de.
ns1.sub05.linuxhotel.de.    IN A 192.168.150.110
```

Fallstrick: Seit bind 9.9 werden die empty zones automatisch „aufgefüllt“. Dadurch werden aber PTR-RR für nicht eigene Netze nicht mehr geforwarded

`/etc/named.conf.options` : (Debian 8)

```
disable-empty-zone "168.192.in-addr.arpa";
```

Das muss auch auf jedem Delegaten konfiguriert werden

```
named-checkzone -i local -D linuxhotel.de /var/named/master/linuxhotel.de
```

Subdomain DNS

Wie oben, unter „eigene Zonen in bind verwalten“

Zonendatei für Subnetz per Skript erzeugen

```
#!/bin/bash
NAMESERVER=$(hostname -f)
SUBNET=192.168.1

cat <<HEAD
\$TTL 2h
@ IN SOA $NAMESERVER. root.$NAMESERVER. (
        $(date '+%Y%m%d')01             ; Seriennummer
        3h              ; refresh
        1h              ; retry
        1w              ; expire
        1h              ; negative ttl
)

  IN NS $NAMESERVER.

HEAD

for ip in $(seq 1 254)
do
  getent hosts $SUBNET.$ip | ( read ip name && echo -e "$name.\tIN\tA\t$ip"
| expand -t '34 37 43 ' )
done
```

Dokus & Links

- Bind Buch "DNS for Rocket Scientists"
- Howto zu Bind und DHCP unter SuSE
- bind und Active Directory
- DNS Root Server System
- Zusammenspiel Windows NS und Bind
- Beispiel einer Windows AD unter Bind

1)

mehr zu `allow-query` weiter unten im Kapitel „Bind absichern“ und natürlich unter

```
man named.conf
```

2)

oder man legt die Zonendateien direkt in /var/cache/bind bzw. /var/named ab

3)

rfc1035

4)

https://www.ripe.net/publications/docs/ripe-203

```
example.com.  3600  SOA  dns.example.com. hostmaster.example.com. (
                         1999022301   ; serial YYYYMMDDnn
                         86400        ; refresh (  24 hours)
                         7200         ; retry   (   2 hours)
                         3600000      ; expire  (1000 hours)
                         172800 )     ; minimum (   2 days)
```