DNS mit Bind9

von

Martin „Venty“ Ebnöther

Was ist das Domain Name System?

- Eine netzweit verteilte Datenbank
- Hierarchischer Aufbau
- Beliebig skalierbar

Wie funktioniert DNS?

Clients schauen in /etc/hosts nach und fragen „ihren“ Nameserver gemäss /etc/resolv.conf.

Weiss der Nameserver die Antwort selber (Cache oder verwaltet Zone), schickt er die Antwort an den Client.

Andernfalls fragt der Nameserver sich „von oben nach unten“ durch, bis er eine Antwort bekommt. Also zuerst einen Rootserver (für „.“), der ihn an einen Server für die TLD (für „.ch“) weiterleitet. Der TLD-Server weiss, welcher Nameserver für die Domain (für „blumfrub.ch“) zuständig ist und verweist an diesen.

Warum ein Domain Name System?

- Namen sind sich einfacher zu merken als Zahlen (IP-Adressen)
- Werbewirksamer (www.sieht-besser-aus.ch)
- Virtuelle Hosts sind nur dank DNS möglich

Gibt es Alternativen?

- IP-Adressen auswendig lernen
- /etc/hosts

Einen eigenen Nameserver für DNS-Abfragen einrichten (caching-only)

Download der Software von ftp://ftp.isc.org/isc/bind9/
Eventuell auch Installation über ein Package-Management
Aktuell bei Bind9 ist zur Zeit die Version 9.2.4. Die unstable Version ist 9.3.0.

named.conf

```
options {
        directory "/etc/namedb";
};

zone "." IN {
        type hint;
        file "named.root";
};
```

named.root

Download per FTP von ftp://ftp.internic.net/domain/named.root (ftp://192.0.34.27/domain/named.root)

named.root enthält die IP-Adressen der Root-Server. (Auszug):

```
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     192.228.79.201
;
; formerly C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
;
; formerly TERP.UMD.EDU
;
```

In /etc/resolv.conf muss der Nameserver eingetragen werden:

```
nameserver 127.0.0.1
```

Es können auch mehrere Nameserver eingetragen werden. Diese werden der Reihe nach abgefragt, bis eine Antwort erhalten worden ist. Um den Server anschliessend zu testen, lassen wir aber mal nur unseren Nameserver eingetragen.

Dann den Nameserver starten:

```
# named
#
```

Testen der Installation:

```
# host www.symlink.ch
host www.symlink.ch
www.symlink.ch has address 129.132.189.110
```

Es klappt!

Falls nicht:

```
host www.symlink.ch
Host www.symlink.ch not found: 3(NXDOMAIN)
```

Unbedingt aber mit mehreren Domains testen. Es könnte ja auch ein Problem auf der Zielseite sein!

Check: Läuft der Nameserver?
ps ax ¦ grep named (BSD/Linux-Systeme)
ps -ef | grep named (Solaris, IRIX)
Was steht im Syslog?

Die eigene Domain

Eine eigene Domain ist heutzutage kein Luxus mehr. Man denkt sich einen coolen Namen aus und registriert diesen bei der Registrierstelle für die entsprechende Top-Level-Domain (TLD). Für .ch und .li ist das die Switch http://www.switch.ch/

Um eine Domain selber zu hosten braucht man zwei Nameserver, einen Master (Primary) und einen Slave (Secondary). Diese müssen fixe IP-Adressen aufweisen und in unterschiedlichen Subnetzen stehen.

Eine Domain kann man aktiv oder inaktiv registrieren. Um eine Domain inaktiv zu registrieren braucht es keine Vorbereitung.

Wir möchten unsere Domain jedoch gleich aktiv benutzen.
Als Beispiel soll unsere Domain „blumfrub.ch“ heissen.

Zuerst richten wir unsere Domain auf unserem Nameserver ein.

Konfiguration des Bind9 Masters für die eigene Domain

Die Zonendatei

named.blumfrub.ch

```
; Authoritative data for Berkeley.EDU (ORIGIN assumed Berkeley.EDU)
;
$TTL 2592000
@       IN          SOA dns1.blumfrub.ch.  root.dns1.blumfrub.ch. (
                                2002012401     ; Serial
                                10800          ; Refresh 3 hours
                                3600           ; Retry   1 hour
                                604800         ; Expire  1000 hours
                                86400)         ; Minimum 24 hours
;
                IN      NS          dns1.blumfrub.ch.
                IN      NS          dns2.der-is-woanders.ch.
;
localhost       IN      A           127.0.0.1
dns1            IN      A           195.162.162.160
;
blumfrub.ch.    IN      MX  0       mail.blumfrub.ch.
;

www             IN      A           195.162.162.160
ftp             IN      CNAME       www

mail            IN      A           195.162.162.160
```

```
smtp            IN      CNAME       mail
pop             IN      CNAME       mail
;
```

named.conf des Masters

```
options {
//        directory "/var/named";
         pid-file "named.pid";
         max-transfer-time-in 60;
         allow-transfer {
        130.59.1.80;
        130.59.211.10;
        192.16.202.11;
        128.112.129.15;
        147.28.0.39;
        200.16.97.77;
        194.42.48.120;
        203.37.255.97;
        164.128.36.32/27;
        195.162.161.182;      Unser Secondary Nameserver
         };
         query-source address * port 53;
};




zone "." in {
         type hint;
```

```
        file "named.root";
};

zone ".blumfrub.ch" in {
        type master;
        file "named.blumfrub.ch";
};
```

Dann den Nameserver neustarten oder kill -1 <pid>.

Test

```
# host www.blumfrub.ch
www.blumfrub.ch has address 195.162.162.160
```

Es klappt.

Falls nicht, schreibt Bind ins Syslog, was ihm nicht passt.

Konfiguration des Bind9 Slaves für die eigene Domain

named.conf

```
zone "blumfrub.ch" {
```

```
        type slave;
        file "secondary-blumfrub.ch";
        masters {
                195.162.162.160;
        };
};
```

Danach muss hier ebenfalls Bind neu gestartet werden, damit er die geänderte Konfiguration einliest.

Die Reverse-Einträge

Hat man einen eigenen IP-Range, so kann man für die IPs sog. reverse Einträge machen.

Hierfür existiert eine eigene Toplevel-Domain: in-addr.arpa
Auch für Reverse-Einträge benutzt man Zonendateien.

Beispiel anhand dem C-Klasse Netz 84.241.64.0/24:
64.241.84.in-addr.arpa

```
$TTL 2592000
@       IN      SOA     ns1.kfn-ag.ch.   noc.as8833.net. (
                                2004100601      ; Serial
                                10800   ; Refresh 3 hours
                                3600    ; Retry   1 hour
                                604800  ; Expire  1000 hours
                                86400 ) ; Minimum 24 hours
;
                IN      NS      ns1.kfn-ag.ch.
                IN      NS      ns2.kfn-ag.ch.
;
;
        IN      A       255.255.255.0   ; subnet mask
;
$GENERATE 1-255 $ PTR dyn-cable-customer.$.64.241.84.customer.kfn-ag.ch.
```

Oder einzelne Einträge:

```
3       1D      IN      PTR     mail.pilatus-aircraft.com
```

```
4       1D      IN      PTR     fixip.pilatus.kfn-ag.ch.
5       1D      IN      PTR     fixip.pilatus.kfn-ag.ch.
```

Eine interne Domain zur bestehenden Domain hinzufügen:

named.blumfrub.ch anfügen

```
$ORIGIN int.blumfrub.ch.
border1    IN          A       192.168.1.1
intranet       IN          A       192.168.1.2

; DHCP-Range 192.168.1.128/25

$GENERATE 128-254  dhcp$      A   192.168.1.$
```

Eine Subdomain delegieren

Anstatt mit $ORIGIN die Subdomain im Zonenfile anzugeben kann man diese auch an einen anderen (evt. internen) Nameserver delegieren.

In der Zonendatei von blumfrub.ch delegieren wir die Subdomain int.blumfrub.ch an einen anderen Nameserver:

```
int             IN      NS              border1
int             IN      NS              intranet

border1         IN      A               192.168.1.1
intranet        IN      A               192.168.1.2
```

Auf border1.blumfrub.ch richten wir nun die interne Domain als Master und auf intranet als Slave ein, wie oben beschrieben.

Uebersicht der gebräuchlichen Record-Typen

A <IP>	Authoritativ Record IPv4
AAAA <IPv6>	Authoritativ Record IPv6
A6 <IPv6>	Authoritativ Record IPv6
NS <hostname>	Nameserver Record
MX <prio> <hostname>	Mail Exchanger
CNAME <hostname>	Canonical Name
SOA <Domain>	Start Of Authority
PTR <hostname>	Pointer für Reverse-DNS

Seltener benutzte Record-Typen

HINFO <Text>	Host-Info, Angaben zur Hardware, OS, Standort etc
TXT <Text>	Freier Text
RP <Text>	Responsible Person, Name der zuständigen Person

Experimentelle oder nicht mehr gebräuchliche Record-Typen

ISDN <Telnummer>	ISDN Nummer
MINFO <resp-mbox>	Mailbox oder Mailinglisten Information
NULL <irgendwas>	Tut nichts