HowTo -- Nameserver auf Router einrichten: bind9

Moderatoren: knecht, gulliver, supporter

neues Thema | antworten **Seite 1 von 1** [11 Beiträge]

Druckansicht Vorheriges Thema | Nächstes Thema

Autor	Nachricht
knecht	**Betreff des Beitrags:** HowTo -- Nameserver auf Router einrichten: bind9 **Verfasst:** 30.11.2004, 10:58

offline

Administrator

Registriert: 29.03.2004, 20:53
Beiträge: 4506
Wohnort: Berlin

Ich gehe davon aus das jeder weiß was ein Nameserver ist, wir Beschäftigen uns jetzt mit dem installieren und einrichten eines **Bind9** Nameservers unter Debian (bei anderen Distributionen ist das Prinzip das selbe nur liegen die Konfigurationsdateien an anderen Orten.

Jetzt erstmal zur Therorie der Namensauflösung und Grundlagen der Netzwerk Konfigurationsdateien

/etc/hostname enthält den Hostnamen des Systems

Code:

```
myself@himself: -> cat /etc/hostname
himself
myself@himself:~> su
Password:
himself:/home/myself #
```

Als normaler User steht der Hostname hinter dem Namen, als root steht der Hostname am Anfang , das nur zur Info!

/etc/hosts Lokale Rechnernamen-Datenbank

Code:

```
himself:~# cat /etc/hosts
127.0.0.1       localhost
192.168.0.1     himself.knecht     himself

# The following lines are desirable for IPv6 capable hosts
# (added automatically by netbase upgrade)

::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

unter dem Eintrag **127.0.0.1 localhost** muß hier die eigene IP gefolgt vom Domainnamen und Nicknamen stehen. Domain- und Nickname sind frei wählbar, solange man nicht einen bestehenden Domainnamen verwendet. (z.b **ichbins.debian.org** gehen nicht)
Hier im Beispiel ist der lokale Rechner in der Domain **.knecht** und hat den Namen **himself**

/etc/hosts.conf Diese Datei definiert die Reihenfolge der Dienste, die zur Namensauflösung angefragt werden.

Code:

```
himself:~# cat /etc/host.conf
order hosts,bind
multi on
```

die erste Zeile sagt, das er als erstes unter hosts (**/etc/hosts**) schauen soll ob dort die Domain aufgelöst werden kann, danach soll er **bind** benutzen, auch wenn Momentan noch gar kein Bind Nameserver installiert ist!(das ist der Standart). Möglich wäre noch **nis** (Network Information System), das der vollständigkeit halber.
multi on steht dafür, das mehrere Namen (Domains) für einen Rechner in der **/etc/hosts** möglich sein sollen. **multi off** würde das dann verbieten.

/etc/nsswitch.conf (Name Service Switch) Diese Datei hat einen ähnlichen Zweck wie die Datei **/etc/hosts.conf**, und ist von mehr Diensten benutzt als **hosts.conf** (wird in naher Zukunft dieselbige ersetzen).

Code:

```
localhost:~# cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat
group:          compat
shadow:         compat

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Die Erklärung dieser Datei spare ich mir jetzt, und verweise auf **man 5 nsswitch.conf**

/etc/resolv.conf Diese Datei definiert welche DNS-Server für die Namensauflösung benutzt wird. Normalerweise stehen darin externe DNS Adressen, wenn wir **bind9** installiert haben schreiben wir darin folgendes:

Code:

```
localhost:~# cat /etc/resolv.conf
nameserver 127.0.0.1
```

Also lenken wir alle Anfragen wieder auf den localhost, wo dann später unser lokaler Nameserver alles weitere übernimmt.

Es gibt einige Dienste, die die **resolv.conf** regelmässig wieder mit anderen Nameservern vollschreibt. Das können 2 Dienste sein.
1.
Deinstalliert das Programm **resolvconf**

Code:

```
apt-get remove resolvconf
```

2.
Versichert euch das in der Datei **/etc/ppp/peers/dsl-provider**
folgender Eintrag auskommentiert ist

Code:

```
#usepeerdns
```

Hört auf euch bis in den Schlaf zu verbeugen!

Zuletzt geändert von **knecht** am 30.08.2005, 21:20, insgesamt 6-mal geändert.

Nach oben Profil E-Mail

knecht

offline

Administrator

Registriert: 29.03.2004, 20:53

Betreff des Beitrags: **Verfasst:** 30.11.2004, 11:54

Installation und Konfiguration von bind9

Jetzt erstmal warum wir das Ding überhaupt installieren, und welche Aufgaben es übernimmt. Jeder Client der noch im selben Netzwerk ist sollte als Nameserver die IP des Routers eingetragen haben (nichts sonst !). Wenn nun ein Client eine DNS Anfrage an den Router stellt, soll er, wenn er ihn kennt, sofort Antwort geben, wenn nicht soll er auf externe Nameserver verweisen. Ein lokaler DNS hat den Vorteil das Anfragen gecached werden, d.h. für ein www.google.com fragt er nur einmal einen externen DNS nach der IP, und kann dann (sehr viel schneller) bei der zweiten Anfrage der gleichen URL aus seinem Cache antworten. Dadurch das solche Anfragen ohne eine Anfrage ins Internet beantwortet werden können, beschleunigt sich das Surfen im Internet.

Also dann schreiten wir zur Tat:

Beiträge: 4506
Wohnort: Berlin

Code:

```
apt-get install bind9
```

Das wäre das installieren, nun noch die Konfiguration:

Im Ordner **/etc/bind/** befinden sich alle wichtigen Dateien, die mit bind zu tun haben:

Code:

```
himself:~# ls -l /etc/bind
total 48
-rw-r--r--  1 root root  237 Sep 23 17:25 db.0
-rw-r--r--  1 root root  271 Sep 23 17:25 db.127
-rw-r--r--  1 root root  237 Sep 23 17:25 db.255
-rw-r--r--  1 root root  353 Sep 23 17:25 db.empty
-rw-r--r--  1 root root  256 Sep 23 17:25 db.local
-rw-r--r--  1 root root 1507 Sep 23 17:25 db.root
-rw-r--r--  1 root bind 1611 Sep 23 17:25 named.conf
-rw-r--r--  1 root bind  228 Nov 30 10:17 named.conf.local
-rw-r--r--  1 root bind  700 Nov 29 14:12 named.conf.options
-rw-r-----  1 bind bind   77 Nov 29 12:01 rndc.key
-rw-r--r--  1 root root 1316 Nov 30 09:05 zones.rfc1918
```

Uns interessiert vorerst die Datei **named.conf.options**:

Code:

```
localhost:~# cat /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you might need to uncomment the query-source
        // directive below.  Previous versions of BIND always asked
        // questions using port 53, but BIND 8.1 and later use an unprivileged
        // port by default.

        // query-source address * port 53;

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
        145.253.2.75;
        145.253.2.11;
        217.237.149.161;
};

        auth-nxdomain no;    # conform to RFC1035

};
```

Der Eintrag **forwarders** steht für die Nameserver, die er bei einer Anfrage, die er lokal nicht auflösen kann, befragt werden. Normalerweise ist dieser Eintrag leer oder fehlt ganz. Das muß jetzt wie im Beispiel geändert werden, damit bind weiß wenn er fragen soll . Benutzt am besten Nameserver aus euerer jeweiligen Gegend, die oberen stehen in Berlin (145.253 = arcor) und Hamburg (217.237... = Telekom).
Falls ihr keine kennt
http://www.atelier89.de/users/dirk/t-o/010.html#liste

Ist das gemacht muß man nun noch bind neustarten, damit es die neuen Konfigurationen übernimmt.

Code:

```
/etc/init.d/bind9 restart
```

Damit ist der Nameserver schon fertig eingerichtet und von Clients benutzbar. Steht zwischen Client und Router eine Firewall muß der Router den Port 53 offen haben, damit er die Anfragen erhält.

Hört auf euch bis in den Schlaf zu verbeugen!

Zuletzt geändert von **knecht** am 30.11.2004, 12:32, insgesamt 1-mal geändert.

Nach oben

Profil E-Mail

knecht

offline

Administrator

Registriert: 29.03.2004, 20:53
Beiträge: 4506
Wohnort: Berlin

Betreff des Beitrags:

Verfasst: 30.11.2004, 12:31

Einrichten von lokalen Domainnamen:

Das eigendlich schöne und nützliche an einem eigenen Nameserver ist die Möglichkeit sogenannte "zones" im lokalen Netzwerk zu definieren. Praktisch bedeutet das, das wenn ich z.B. im Netzwerk die Zone **.knecht** erstellt habe, und **matthias** als Teilnehmer dieser Zone definiert habe (und seine IP 192.168.0.2 hinter diesem Namen hinterlegt habe), ist das dann ein im ganzen lokalen Netzwerk gültiger Domainname (alle Client müßen natürlich auch den Router als Nameserver eingetragen haben!!).
Also kann ich dann anstatt **ping 192.168.0.2** auch ein **ping matthias.knecht**

Genau das werde ich jetzt beschreiben. Wie im Beitrag vorher haben wir ja schon **forwarders** unter **/etc/bind /named.conf.options** eingetragen.

Jetzt definieren wir die zone "knecht".

Code:

```
localhost:/etc/bind# cat named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "knecht"  { type master; file "/etc/bind/db.knechtnet"; };
```

Die Datei enthält normalerweiße keinen Eintrag. Die letzte Zeile definiert unsere neue Zone "knecht", und wir sagen ihm das die Datei die die Informationen über diese Zone enthält die Datei **/etc/bind/db.knechtnet** ist.
Diese Datei mußen wir jetzt erstmal erstellen, dazu kopieren wir einfach eine vorhandene Datei nach **db.knechtnet**:

Code:

```
himself:~# cp /etc/bind/db.local /etc/bind/db.knechtnet
```

Und diese Editieren wir nun:

Code:

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
```

Nach dem editieren sollte sie so aussehen:

Code:

```
himself:~# cat /etc/bind/db.knechtnet
;
; BIND data file for local loopback interface
;
$TTL    604800
knecht.         IN      SOA     himself.knecht. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
                        NS      himself
himself         IN      A       192.168.0.1
sebastian       IN      A       192.168.0.6
```

```
matthias        IN      A       192.168.0.2
```

$TTL steht für "time to life" in Sekunden. Halt wie lange eine Domain im Cache bleibt bevor er sie aktualisiert.

die Zeile darunter:
Zonenname (**knecht.**), dann **IN SOA** (start of authority, wer ist zuständiger Nameserver für diese Zone) und der Name des Routers (**himself.knecht.**). Das **root.localhost.** ist dann noch die EMailadresse, an die er Meldungen schicken soll (steht für root@localhost, also lokale Mailzustellung unter **/var/mail/root**)

dann ist erst **NS himself** wieder wichtig, gibt nochmal den Hostnamen des Nameservers (NS) im lokalen Netz an. Diesen Hostnamen müßen wir natürlich auch erstmal erstellen, und eine IP hinterlegen, damit er diesen auch finden kann. Dafür die folgenden Zeilen, mit dem Syntax:
[HOSTNAME] IN A [IP]
Jetzt legt man für jeden Rechner im Netz einen Hostnamen und die dazugehörige IP in einer Zeile fest.

Ist das gemacht muß man nun noch bind neustarten, damit es die Konfiguration übernimmt.

Code:

```
/etc/init.d/bind9 restart
```

Nun zum Überprüfen ob er auch alles richtig macht:

Code:

```
localhost:~# host matthias.knecht
matthias.knecht has address 192.168.0.2
localhost:~# host himself.knecht
himself.knecht has address 192.168.0.1
localhost:~# ping himself.knecht
PING himself.knecht (192.168.0.1) 56(84) bytes of data.
64 bytes from himself.knecht.site (192.168.0.1): icmp_seq=1 ttl=64 time=0.179 ms
64 bytes from himself.knecht.site (192.168.0.1): icmp_seq=2 ttl=64 time=0.193 ms
```

auch ein schönes Tool zum Domain Testen ist **dig**

Code:

```
localhost:~# dig himself.knecht

; <<>> DiG 9.2.4 <<>> himself.knecht
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 57632
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;himself.knecht.                        IN      A

;; AUTHORITY SECTION:
.                       3600    IN      SOA     A.ROOT-SERVERS.NET. NSTLD.VERISIGN-GRS.COM. 2004120901 1800
900 604800 86400

;; Query time: 137 msec
;; SERVER: 145.253.2.75#53(145.253.2.75)
;; WHEN: Fri Dec 10 12:41:27 2004
;; MSG SIZE  rcvd: 107
```

Also hab ich jetzt im lokalen Netz die Zone **.knecht** erstellt, und dazu die drei Subdomains himself, matthias und sebastian.

Reverse lookup Zone

Nun haben wir alles getan, damit ein Domainname in eine IP umgesetzt wird, aber das ganze gibt es auch umgedreht . . . also das Auflösen einer IP in einem Domainnamen. Dazu liegt unter **/etc/bind9/** die Datei **zones.rfc1918**. Darin deklariert man den Verweis auf eine Reverse Lookup Zone. So ein Eintrag sieht für die Addressen 192.168.0.xx wie folgt aus:

Code:

```
zone "0.168.192.in-addr.arpa" { type master; file "/etc/bind/db.192"; };
```

Hier ist die ReverseZone Datei **/etc/bind/db.192**, diese Datei muß dann wie folgt aussehen:

Code:

```
;
; BIND reverse data file for 192.168.0
;
$TTL    1d
@       IN      SOA     himself.knecht. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      himself

7       IN      PTR     labslave.knecht.
1       IN      PTR     himself.knecht.
2       IN      PTR     matthias.knecht.
6       IN      PTR     sebastian.knecht.
22      IN      PTR    ibook.knecht.
```

nun kann man auch IP Adressen auflösen, wieder mit **host** oder **nslookup**

Code:

```
myself@stupidslave:~$ host 192.168.0.6
6.0.168.192.in-addr.arpa domain name pointer sebastian.knecht.
```

Damit ist die Konfiguration einer Zone mit ReverseZone abgeschlossen

_____
Hört auf euch bis in den Schlaf zu verbeugen!

Zuletzt geändert von **knecht** am 29.10.2005, 17:51, insgesamt 1-mal geändert.

Nach oben Profil E-Mail

rak64

offline

nicht viel Schreiber

Registriert: 22.06.2005, 14:31
Beiträge: 1
Wohnort: N/A

Betreff des Beitrags: **Verfasst:** 22.06.2005, 14:43

Code:

```
;; SERVER: 145.253.2.75#53(145.253.2.75)
```

sollte da nicht

Code:

```
;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Jun 22 15:23:33 2005
```

stehen?
Ich glaube, die obige Konfiguration nutzt denn localen bind9-Dienst garnicht. Dig gibt erst die Benutzung des localen Bind-server zu, wenn ich die resolv.conf editiere. Bei mir wird der Eintrag nameserver 127.0.01 in der /etc/resonv.conf regelmäßig gelöscht, obwohl ich das Paket resolvconf deinstalliert habe. Ich beziehe meine IP-Nummer über DHCP und pump. Auch ist die resolv.conf für root readonly.

Nach oben Profil

knecht

offline

Administrator

Betreff des Beitrags: **Verfasst:** 22.06.2005, 15:26

Zitat:

;; SERVER: 145.253.2.75#53(145.253.2.75)

Das ist die Addresse meines Servers im Internet, und nicht die lokale. Meine DNS Auflösung funktioniert intern auch wunderbar. Warum DIG meine ppp0 IP anzeigte weiß ich nicht.

Zitat:

Bei mir wird der Eintrag nameserver 127.0.01 in der /etc/resonv.conf regelmäßig gelöscht, obwohl ich das Paket resolvconf

Registriert: 29.03.2004, 20:53
Beiträge: 4506
Wohnort: Berlin

> deinstalliert habe. Ich beziehe meine IP-Nummer über DHCP und pump. Auch ist die resolv.conf für root readonly.

Da gibts anscheinend mehr als ein Programm das die **resolv.conf** überschreiben will, bei mir warens **PPPOE** und das Paket **resolvconf**. Ich denke das wird das DHCP machen, aber wie man das behebt weiß ich nicht. Irgendwie müßte man dem DHCP Client doch sagen können, er soll den Nameserver nicht holen.

Bei mir daheim ist der DHCP Server auch der DNS Server, also kriegen meine Clients eben die Serveraddresse als DNS, so wie es sein soll . . . und auf dem Server warens wie schon geschrieben PPPOE und resolvconf

_____
Hört auf euch bis in den Schlaf zu verbeugen!

Nach oben Profil E-Mail

kbdcalls **Betreff des Beitrags:** **Verfasst:** 22.06.2005, 20:38

offline

Backbone

Registriert: 26.05.2005, 14:39
Beiträge: 619
Wohnort: 44287 (Dortmund)

In der dhclient.conf

prepend domain-name-servers 127.0.0.1;

Und den richtigen DNS eintragen. Zwei werden durch Komma getrennt.

Nach oben Profil E-Mail

Guest **Betreff des Beitrags:** **Verfasst:** 17.07.2005, 13:43

was mich jetzt nur noch interessieren würde, ist die sache mit nem alias

da ich etwas schreibfaul bin, möchte ich beispielsweise bei nem ping oder nslookup nicht immer noch den zonennamen anhängen

ich habe einen host1 in zone1, und möchte nun nicht auf host1.zone1 pingen sondern nur auf host1

müsste theoretisch wie praktisch kein problem sein, nur wie realisiert man das

Nach oben

knecht **Betreff des Beitrags:** **Verfasst:** 17.07.2005, 20:52

offline

Administrator

Registriert: 29.03.2004, 20:53
Beiträge: 4506
Wohnort: Berlin

Was du meinst geht, hat aber nichts mit der konfiguration des BIND Servers zu tun.

Ich habe bei mir im internen Netz die Zone **.knecht**, **sebastian.knecht** ist mein PC in den Netzwerk.
Damit man einfach per

Code:
```
ping sebastian
```

meinen Rechner erreichen kann muß auf dem Rechner, auf dem das Ping ausgeführt wird, in der **/etc/resolv.conf** folgende Zeile stehen:

Code:
```
search knecht
```

dann ist folgendes möglich:

Code:
```
himself:~# ping sebastian
PING sebastian.knecht (192.168.0.6) 56(84) bytes of data.
64 bytes from sebastian.knecht (192.168.0.6): icmp_seq=1 ttl=64 time=0.388 ms
64 bytes from sebastian.knecht (192.168.0.6): icmp_seq=2 ttl=64 time=0.282 ms
```

Es ist also eine Einstellung des Clients, nicht des BIND Servers die sowas ermöglicht, auch unter Windows gibts diese **search** Option irgendwo, wo genau weiß ich aber nicht . . .

gruss
Sebastian

_____
Hört auf euch bis in den Schlaf zu verbeugen!

Nach oben Profil E-Mail

Guest **Betreff des Beitrags:** **Verfasst:** 18.07.2005, 15:11

ahh oke, danke für den tipp mit der resolv.conf

hatte auf dem ugly wintendo nur vergessen, nach dem setzen des primary dns suffix neuzustarten

Nach oben

Gast **Betreff des Beitrags:** Re: HowTo -- Nameserver auf Router einrichten: bind9 **Verfasst:** 30.08.2005, 20:53

> **knecht hat geschrieben:**
>
> **Code:**
> ```
> himself:~# cat /etc/hosts
> 192.168.0.1     himself.knecht     knecht
> ```
>
> Hier im Beispiel ist der lokale Rechner in der Domain **.knecht** und hat den Namen **himself**

deshalb sollte es:

Code:
```
192.168.0.1     himself.knecht        himself
```

heissen, sonst ist man im weiteren verlauf vielleicht verwirrt.

herrchen

Nach oben

knecht **Betreff des Beitrags:** **Verfasst:** 30.08.2005, 21:20

offline

Administrator

Ist geändert, vielen Dank für den Hinweis

_____
Hört auf euch bis in den Schlaf zu verbeugen!

Registriert: 29.03.2004, 20:53
Beiträge: 4506
Wohnort: Berlin

Nach oben Profil E-Mail

Beiträge der letzten Zeit anzeigen: Alle Beiträge Sortiere nach Erstellungsdatum Aufsteigend Los

neues Thema antworten **Seite 1 von 1** [11 Beiträge]

Wer ist online?

Mitglieder in diesem Forum: 0 Mitglieder und 1 Gast

Du darfst **keine** neuen Themen in diesem Forum erstellen.
Du darfst **keine** Antworten zu Themen in diesem Forum erstellen.
Du darfst deine Beiträge in diesem Forum **nicht** ändern.
Du darfst deine Beiträge in diesem Forum **nicht** löschen.
Du darfst **keine** Dateianhänge in diesem Forum erstellen.

Suche nach: Los Gehe zu: Netzwerk Los