BIND Nameserver

Mit BIND[1] richten wir uns für unser SOHO[2]-LAN ein Domain-Name-System-Server oder kurz DNS[3]ein. DNS wurde in den beiden RFC 1034 und RFC 1035 definiert und bekam von der Internet Assigned Numbers Authority die beiden Ports 53/UDP und 53/TCP.

Installation

Zu erst installieren wir uns die beiden Pakete **bind** und **bind-chroot**. Letzters hilft uns, unseren DNS in einem chroot[4]-Umgebung laufen zu lassen. Hierzu reicht quasi die installation von **bind-chroot**, da **bind** auf Grund der Abhängigkeiten bei Bedarf automatisch mit installiert wird.

```
yum install bind-chroot
```

Konfiguration

named.conf

Als erstes erstellen wir uns unsere Serverkonfigurationsdatei:

```
# vim /var/named/chroot/etc/named.conf
```

```
// Red Hat BIND Configuration Tool
//
// Default initial "Caching Only" name server configuration
//

options {
allow-query {
        127.0.0.1;
        192.168.100.0/24;
};



query-source address 192.168.100.1 port *
   ;
forwarders {    212.18.3.5;
        212.18.0.5;
};

random-device "/dev/random";
directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
```

```
        statistics-file "/var/named/data/named_stats.txt";
        /*
         * 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 uses an unprivileged
         * port by default.
         */
         // query-source address * port 53;
};

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

zone "localdomain." IN {
        type master;
        file "localdomain.zone";
        allow-update { none; };
};

zone "localhost." IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa." IN {
        type master;
        file "named.local";
        allow-update { none; };
};

zone
"0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa." IN
{
        type master;
        file "named.ip6.local";
        allow-update { none; };
};

zone "255.in-addr.arpa." IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
};

zone "0.in-addr.arpa." IN {
        type master;
        file "named.zero";
```

```
        allow-update { none; };
};

zone "nausch.org" IN {
        type master;
        file "nausch.org";
};

zone "10.168.192.in-addr.arpa" IN {
        type master;
        file "10.168.192.in-addr.arpa";
};

include "/etc/rndc.key";
```

Forward-Auflösung

Als nächstes legen wir uns für die *Forward-Auflösung* die entsprechende Konfigurationsdatei passend für unsere Domäne **nausch.org** an.

```
vim /var/named/chroot/var/named/nausch.org
$TTL    86400
@                                       IN      SOA     nss.nausch.org.
root.nausch.org. (
                                                        2008110701      ;
serial
                                                        3H              ;
refresh
                                                        15M             ;
retry
                                                        1W              ;
expiry
                                                        1D )            ;
minimum

                                        IN      NS      nss.nausch.org.
                                        IN      MX  10  nss

ldap                                    IN      CNAME   nss
time                                    IN      CNAME   nss

nausch.org.                             IN      A       192.168.100.1
*.nausch.org.                           IN      A       192.168.100.1

nss                                     IN      A       192.168.100.1

GXP-2000                                IN      A       192.168.100.50
ST-100                                  IN      A       192.168.100.51
SPA-2100-1                              IN      A       192.168.100.52
SPA-2100-2                              IN      A       192.168.100.53
```

```
snom360                                 IN      A       192.168.100.54
snom320                                 IN      A       192.168.100.55
snom300-1                               IN      A       192.168.100.56
snom300-2                               IN      A       192.168.100.57
snom300-3                               IN      A       192.168.100.58
snom-m3                                 IN      A       192.168.100.59
```

Reverse-Auflösung

Für die *Reverse-Auflösung*, also für die Ermittlung des Namens zu einer vorgegebenen IP-Adresse, legen wird entsprechend unserem IP-Adresspools folgende Konfigurationsdatei **100.168.192.in-addr.arpa** an.

```
vim /var/named/chroot/var/named/10.168.192.in-addr.arpa
$TTL 2D
@                               IN SOA          nss.nausch.org.
root.nss.nausch.org. (
                                2008110701      ; serial
                                3H              ; refresh
                                1H              ; retry
                                1W              ; expiry
                                1D )            ; minimum

@                               IN NS           1.100.168.192.in-addr.arpa.

1                               IN PTR          nss.nausch.org.
50                              IN PTR          GXP-2000.nausch.org.
51                              IN PTR          ST-100.nausch.org.
52                              IN PTR          SPA-2100-1.nausch.org.
53                              IN PTR          SPA-2100-2.nausch.org.
54                              IN PTR          snom360.nausch.org.
55                              IN PTR          snom320.nausch.org.
56                              IN PTR          snom300-1.nausch.org.
57                              IN PTR          snom300-2.nausch.org.
58                              IN PTR          snom300-3.nausch.org.
59                              IN PTR          snom-m3.nausch.org.
```

Weiter legen wir uns noch folgende Dateien an

localdomain.zone

```
$TTL    86400
@               IN SOA  localhost root.localhost (
                                        42              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

```
                IN NS           localhost
localhost       IN A            127.0.0.1
```

localhost.zone

```
$TTL    86400
@               IN SOA  @       root (
                                        42              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                IN NS           @
                IN A            127.0.0.1
                IN AAAA         ::1
```

named.broadcast

```
$TTL    86400
@               IN SOA  localhost.      root.localhost. (
                                        42              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
        IN      NS      localhost.
```

named.ip6.local

```
$TTL    86400
@       IN      SOA     localhost. root.localhost.  (
                                      42         ; Serial
                                      28800      ; Refresh
                                      14400      ; Retry
                                      3600000    ; Expire
                                      86400 )    ; Minimum
       IN      NS      localhost.
1      IN      PTR     localhost.
```

named.local

```
$TTL    86400
@       IN      SOA     localhost. root.localhost.  (
                                      42         ; Serial
                                      28800      ; Refresh
```

```
                                        14400      ; Retry
                                        3600000    ; Expire
                                        86400 )    ; Minimum
        IN      NS      localhost.
1       IN      PTR     localhost.
```

named.root

```
; root "." zone hints file, queried of a.root-servers.net. by system-config-
bind
; version of root zone: 2007082400
.                       518400  IN      NS      H.ROOT-SERVERS.NET.
.                       518400  IN      NS      I.ROOT-SERVERS.NET.
.                       518400  IN      NS      J.ROOT-SERVERS.NET.
.                       518400  IN      NS      K.ROOT-SERVERS.NET.
.                       518400  IN      NS      L.ROOT-SERVERS.NET.
.                       518400  IN      NS      M.ROOT-SERVERS.NET.
.                       518400  IN      NS      A.ROOT-SERVERS.NET.
.                       518400  IN      NS      B.ROOT-SERVERS.NET.
.                       518400  IN      NS      C.ROOT-SERVERS.NET.
.                       518400  IN      NS      D.ROOT-SERVERS.NET.
.                       518400  IN      NS      E.ROOT-SERVERS.NET.
.                       518400  IN      NS      F.ROOT-SERVERS.NET.
.                       518400  IN      NS      G.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000 IN      A       198.41.0.4
B.ROOT-SERVERS.NET.     3600000 IN      A       192.228.79.201
C.ROOT-SERVERS.NET.     3600000 IN      A       192.33.4.12
D.ROOT-SERVERS.NET.     3600000 IN      A       128.8.10.90
E.ROOT-SERVERS.NET.     3600000 IN      A       192.203.230.10
F.ROOT-SERVERS.NET.     3600000 IN      A       192.5.5.241
G.ROOT-SERVERS.NET.     3600000 IN      A       192.112.36.4
H.ROOT-SERVERS.NET.     3600000 IN      A       128.63.2.53
I.ROOT-SERVERS.NET.     3600000 IN      A       192.36.148.17
J.ROOT-SERVERS.NET.     3600000 IN      A       192.58.128.30
K.ROOT-SERVERS.NET.     3600000 IN      A       193.0.14.129
L.ROOT-SERVERS.NET.     3600000 IN      A       198.32.64.12
M.ROOT-SERVERS.NET.     3600000 IN      A       202.12.27.33
```

named.zero

```
$TTL    86400
@               IN SOA  localhost.      root.localhost. (
                                        42              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

```
        IN      NS      localhost.
```

Nameserver starten

Den ersten Start unseres DNS-Servers nehmen wir wie folgt vor.

```
service named start
named starten:                                             [  OK  ]
```

Im syslog wird der erfolgreiche Start entsprechend quittiert:

```
Nov  7 21:40:17 mnss named[17041]: starting BIND 9.3.4-P1 -u named -t
/var/named/chroot
Nov  7 21:40:17 mnss named[17041]: found 2 CPUs, using 2 worker threads
Nov  7 21:40:17 mnss named[17041]: loading configuration from
'/etc/named.conf'
Nov  7 21:40:17 mnss named[17041]: listening on IPv4 interface lo,
127.0.0.1#53
Nov  7 21:40:17 mnss named[17041]: listening on IPv4 interface eth0,
192.168.100.2#53
Nov  7 21:40:17 mnss named[17041]: command channel listening on
127.0.0.1#953
Nov  7 21:40:17 mnss named[17041]: command channel listening on ::1#953
Nov  7 21:40:17 mnss named[17041]: zone 0.in-addr.arpa/IN: loaded serial 42
Nov  7 21:40:17 mnss named[17041]: zone 0.0.127.in-addr.arpa/IN: loaded
serial 42
Nov  7 21:40:17 mnss named[17041]: zone 100.168.192.in-addr.arpa/IN: loaded
serial 2008110701
Nov  7 21:40:17 mnss named[17041]: zone 255.in-addr.arpa/IN: loaded serial
42
Nov  7 21:40:17 mnss named[17041]: zone
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN:
loaded serial 42
Nov  7 21:40:17 mnss named[17041]: zone localdomain/IN: loaded serial 42
Nov  7 21:40:17 mnss named[17041]: zone localhost/IN: loaded serial 42
Nov  7 21:40:17 mnss named[17041]: zone nausch.org/IN: loaded serial
2008110701
Nov  7 21:40:17 mnss named[17041]: running
Nov  7 21:40:17 mnss named[17041]: zone 10.168.192.in-addr.arpa/IN: sending
notifies (serial 2008110701)
```

automatisches Starten des Dienste beim Systemstart

Damit nun unser DNS-Server beim Booten automatisch gestartet wird, nehmen wir noch folgende Konfigurationsschritte vor.

```
chkconfig named on
```

Anschließend überprüfen wir noch unsere Änderung:

```
chkconfig --list | grep named
named           0:Aus   1:Aus   2:Ein   3:Ein   4:Ein   5:Ein   6:Aus
```

Links

- **Zurück zu Projekte und Themenkapitel**
- **Zurück zur Startseite**

1)
Berkeley Internet Name Domain
2)
SmallOfficeHomeOffice
3)
Domain Name System
4)
change root directory