

Bind9 DNS on CentOS7

Deze installatie resulteert in een DNS met IP nr 192.168.1.100 en hostname dns.voorbeeld.lan die lookups serveert voor het domein voorbeeld.lan Als de DNS in zijn zone files geen record kan vinden word de lookup geforward naar de google DNS.

Install software

installeer de nodige software: `yum install bind bind-utils`

Configuration

named conf files

Pas de volgende zaken aan in de hoofd configuratie aan: `vi /etc/named.conf`:

Zet het trusted acl voor het netwerk van de servers die de DNS moeten kunnen gebruiken:

```
acl "trusted" {  
    192.168.1.0/24; #hele netwerk  
};
```

pas het options{} deel aan:

listen-on, luister ook op het externe IP, maar niet op IPv6

```
option {  
  
    listen-on port 53 { 127.0.0.1; 192.168.1.100; }; #added own IP  
#    listen-on-v6 port 53 { ::1; }; # commented out
```

allow-query, pas deze aan naar trusted als we niet de hele wereld willen serveren maar alleen de servers in ons netwerk.

```
allow-query { trusted; }; #changed to trusted
```

forwarders, stel in waar de DNS naar antwoorden gaat zoeken mocht hij ze zelf niet vinden. In dit geval forwarden we naar de DNS van google, je zou ook de upstream DNS in je netwerk kunnen gebruiken of die van je ISP of OpenDNS.

```
#added forwarders to googleDNS  
forwarders {  
    8.8.8.8;  
    8.8.4.4;  
};
```

allow-recursion altijd een goed idee.

```
recursion yes;  
allow-recursion { trusted; }; #added
```

En voeg tenslotte na het options deel een `include` statement toe voor onze configuratie. Je zou de configuratie rechtstreeks hier kunnen toevoegen, maar bij een situatie waar er een aantal domains zijn wordt het al snel onoverzichtelijk.

```
# toegevoegd  
include "/etc/named/named.conf.voorbeeld.lan";
```

Vervolgens maken we de top configuratie voor ons domein aan: `vi /etc/named/named.conf.voorbeeld.lan`

zet hierin de forward lookup zone file:

```
zone "voorbeeld.lan" {  
    type master;  
    file "/etc/named/zones/db.voorbeeld.lan";  
};
```

en de reverse lookup zone file:

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

named zone files

De domain configuratie file verwijst naar de zone files. Maak eerst de directory aan:

```
mkdir /etc/named/zones
```

forwards zone file

```
vi /etc/named/zones/db.voorbeeld.lan
```

```
@    IN      SOA      dns.voorbeeld.lan. admin.voorbeeld.lan. (  
                                1      ; Serial  
                                604800 ; Refresh  
                                86400  ; Retry  
                                2419200 ; Expire  
                                604800 ) ; Negative Cache TTL
```

```

; name servers - NS records
    IN      NS      dns.voorbeeld.lan.

; name servers - A records
dns.voorbeeld.lan.      IN      A      192.168.1.100

; 192.168.122.0/24 - A records
server1.voorbeeld.lan.  IN      A      192.168.1.101
webserver.voorbeeld.lan.  IN      A      192.168.1.102
server2.voorbeeld.lan.  IN      A      192.168.1.200
jansPC.voorbeeld.lan.   IN      A      192.168.1.220

```

reverse zone file

```
vi /etc/named/zones/db.1.168.192
```

```

$TTL      604800
@      IN      SOA      dns.voorbeeld.lan. admin.voorbeeld.lan. (
                        1      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL

; name servers - NS records
    IN      NS      dns.voorbeeld.lan.

; PTR Records
100 IN      PTR      dns.voorbeeld.lan.
101      IN      PTR      server1.voorbeeld.lan.
102      IN      PTR      webserver.voorbeeld.lan.
200      IN      PTR      server2.voorbeeld.lan.
220      IN      PTR      jansPC.voorbeeld.lan.

```

Check configuratie en start named

Check de configuratie files:

```
named-checkconf
```

Check de zone files:

```
named-checkzone voorbeeld.lan /etc/named/zones/db.voorbeeld.lan
```

```
named-checkzone 1.168.192.in-addr.arpa /etc/named/zones/db.1.168.192
```

Zet de firewall open:

```
firewall-cmd --permanent --add-service=dns
```

```
firewall-cmd --reload
```

enable en start name daemon:

```
systemctl enable named
```

```
systemctl start named
```

Linux Servers naar deze DNS laten resolvable

Log in op de betreffende server en pas de resolving aan door vi /etc/resolv.conf en zet hier in:

```
domain lan  
search lan voorbeeld.lan  
nameserver 192.168.1.100
```

Aanpassen van de zone file met een draaiende DNS

Volg [deze instructies](#) om de zonefiles uit te breiden als er bijvoorbeeld een server bij komt of verdwijnt.

From:
<https://wiki.auriel.nl/> -

Permanent link:
https://wiki.auriel.nl/doku.php?id=installatie_handleidingen:bind_9_dns_configureren&rev=1520340469 

Last update: **2018/03/06 13:47**