DNS reverse zone

Last edited time: June 27, 2022 18:58 AM
Reviewed: No

Waarden in dit scenario:
dns-server: dmz1.hgb.nl (10.2.0.10)
reverse zone voor ip-reeks: 10.1.0.0/16
voor visualisatie gebruik: https://www.youtube.com/watch?v=xUGSEdFV-W4

Een forward zone is het vertalen van naam naar ip, hiermee kan je dus directory1.hgb.nl pingen, dit wordt vertaald naar een IP-adres waar daadwerkelijk op gepinged wordt.
Een reverse zone is het vertalen van IP naar naam.

Forward zone

Om een reverse zone in te stellen moeten we eerst een forward zone hebben (gebruik BIPL DNS handleiding). In deze forward zone hebben we de volgende dns entries:

```
directory1      IN      A       10.1.0.100
directory2      IN      A       10.1.0.101

intern1         IN      A       10.1.1.100
intern2         IN      A       10.1.1.101
intern3         IN      A       10.1.1.102
```

Voor deze hosts gaan we dus de reverse zone maken

Reverse zone

bewerk het `/etc/named.conf` bestand en voeg een nieuwe zone toe onder de forward zone:

```
//dit is onze forward zone
zone "hgb.nl." IN {
        type master;
        file "hgb.nl";
};
```

```
//dit is onze reverse zone voor het 10.1.x.x netwerk
zone "1.10.in-addr.arpa" {
        type master;
        file "10.1.zone";
};
```

Ons 10.1.0.0 netwerk is een /16 netwerk, in het named.conf bestand zetten we alleen de netwerkgetallen en niet de hostgetallen. Deze getallen dienen in omgekeerde volgorde te staan (in ons geval is 10.1 omgedraaid 1.10).
We zetten in-addr.arpa erachter om te laten weten dat dit een reverse zone is.

Maak nu het 10.1.zone bestand aan in `/var/named` en plaats de volgende informatie in het bestand **let op: wijzig het NS en SOA record!**

```
$TTL 3h
@       IN      NS      dmz1.hgb.nl.
@       IN      SOA     hgb.nl. admin.hgb.nl. (
        2020042000; serial
        10800;          refresh
        3600;           retry
        604800;         expire
        86400;          default ttl
)
```

Voeg nu de volgende regel toe aan het 10.1.zone bestand waarmee je het linkt aan de zone in /var/named.conf

```
$ORIGIN 1.10.in-addr.arpa.
```

Voeg nu de reverse DNS entries toe **letop, de hostgetallen zijn net als de netwerkgetallen omgedraaid**

```
100.0   IN      PTR             directory1.hgb.nl.
101.0   IN      PTR             directory2.hgb.nl.

100.1   IN      PTR             intern1.hgb.nl.
101.1   IN      PTR             intern2.hgb.nl.
102.1   IN      PTR             intern3.hgb.nl.
```

vergelijk nu het 10.1.zone bestand met het forward zone bestand, je zult vergelijkingen tegekomen qua naam-IP combinatie

restart nu de DNS service met `sudo systemctl restart named`

Testen

Je kan de werking van de reverse DNS zone testen met `dig -x 10.1.0.100`

```
; <<>> DiG 9.11.36-RedHat-9.11.36-3.el8 <<>> -x 10.1.0.100
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65033
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 5f59f95231eff56b4fd69e7c62ba2ec6072b53ad4fa1e08c (good)
;; QUESTION SECTION:
;100.0.1.10.in-addr.arpa.       IN      PTR

;; ANSWER SECTION:
100.0.1.10.in-addr.arpa. 10800  IN      PTR     directory1.hgb.nl.

;; AUTHORITY SECTION:
1.10.in-addr.arpa.      10800   IN      NS      dmz1.hgb.nl.

;; ADDITIONAL SECTION:
dmz1.hgb.nl.            10800   IN      A       10.2.0.10

;; Query time: 2 msec
;; SERVER: 10.2.0.10#53(10.2.0.10)
;; WHEN: Tue Jun 28 00:27:18 CEST 2022
;; MSG SIZE  rcvd: 146
```

Je ziet dat 10.1.0.100 vertaald wordt naar directory1.hgb.nl, en dat de vertaling is gedaan door dmz1.hgb.nl.