

Bind

Bind ist der DNS-Server unter Linux. Hier nun die Basis-Einrichtung.

Installation

Bind kann mit folgenden Befehlen installiert werden:

```
sudo apt-get update
sudo apt-get install bind9
```

Zone

Nach dem Bind installiert ist, kann man die erste Zone anlegen. Eine Zone besteht aus zwei Dateien. <note warning>Die Domainnamen MÜSSEN immer mit einem Punkt abgeschlossen werden!</note>

Domainnamen

Die erste Datei beinhalte die Umwandlung von Domainnamen zu einer IP-Adresse. Am besten nutze man die Vorhandene Blanko-Datei.

```
sudo cp /etc/bind/db.empty /etc/bind/db.holzfeind.ch
```

Im nächsten Schritt muss die Datei den eigenen Bedürfnissen angepasst werden, hier nun ein Beispiel:

```
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL      86400
@   IN    SOA htpc.holzfeind.ch. root.localhost. (
```

```

                1      ; Serial
        604800    ; Refresh
                86400  ; Retry
        2419200  ; Expire
                86400 ) ; Negative Cache TTL
;
@ IN NS dns.holzfeind.ch.

htpc                IN      A      172.16.10.5
dns                 IN      A      172.16.10.5
vm                  IN      A      172.16.10.6
fw                  IN      A      172.16.10.1
sw                  IN      A      172.16.10.7

```

Revers

Als nächster Schritt wird die Revers-Datei erstellt, diese dient der Umwandlung von IP-Adressen in Domainnamen. Am besten nutzt man die Vorhandene Blanko-Datei.

```
sudo cp /etc/bind/db.empty /etc/bind/db.10.16.172
```

oder die zuvor erstellte Domainnamen-Datei

```
sudo cp /etc/bind/db.holzfeind.ch /etc/bind/db.10.16.172
```

Auch hier müssen die Daten den eigenen Bedürfnissen angepasst werden. Hier nun ein entsprechendes Beispiel:

```

; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL      86400
@ IN SOA htpc.holzfeind.ch. root.localhost. (
                1      ; Serial
        604800    ; Refresh
                86400  ; Retry
        2419200  ; Expire

```

```

        86400 ) ; Negative Cache TTL
;
@ IN NS dns.holzfeind.ch.

1 IN PTR fw.holzfeind.ch.
5 IN PTR dns.holzfeind.ch.
5 IN PTR htpc.holzfeind.ch.
6 IN PTR vm.holzfeind.ch.
7 IN PTR sw.holzfeind.ch.

```

Abschluss

Zum Abschluss müssen die zwei Zonen-Dateien noch dem DNS-Server bekannt gemacht werden, hier für erweitert man die Datei `/etc/bind/named.conf.local` um folgende Einträge:

```

zone "holzfeind.ch" {
    type master;
    file "/etc/bind/db.holzfeind.ch";
};
zone "10.16.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.10.16.172";
};

```

DNS-Cache

Sobald der DNS-Server läuft, besteht auch die Möglichkeit diesen als DNS-Cache zu konfigurieren. Hier für wird folgendes Vorgehen empfohlen:

1. DNS-Root-Server Informationen beziehen und speichern:

```
dig @A.ROOT-SERVERS.NET > /etc/bind/db.root
```

2. DNS-Root-Server-Eintrag erstellen (zum Teil auch schon vorhanden, `/etc/bind/named.conf.default-zones`).

```

zone "." {
    type hint;

```

```
file "/etc/bind/db.root";  
};
```

3. Update-Script erstellen (Pfad: `/etc/cron.weekly/`)

```
#!/bin/bash  
#  
# Aktualisierung der db.root  
#  
  
# Aktuelle Liste generieren  
dig @A.ROOT-SERVERS.NET > /etc/bind/db.root  
  
# Konfiguration Laden  
/usr/sbin/service bind9 reload
```

4. Script ausführbar machen.

```
chmod +x /etc/cron.weekly/bind-root-update.sh
```

5. Bind neustarten

```
service bind9 restart
```

Anfrage loggen

Um die Auflösung der Adressen zu loggen kann folgende Einstellung vorgenommen werden:

```
rndc querylog
```

Die Daten werden anschliessen in die Datei `/var/log/syslog` oder `/var/log/message` geschrieben.

Revision #1

Created 30 November 2023 10:45:43 by Gregor Holzfeind

Updated 30 November 2023 10:45:56 by Gregor Holzfeind