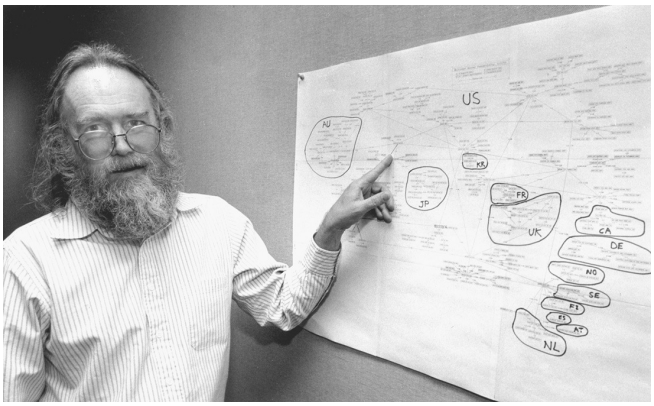
24. BIND DNS server installatie

In de komende serie lessen gaan we ons bezig houden met het Domeinnaam-Systeem (DNS). De meest gebruikte DNS server in de Linux-wereld heet *BIND* (Berkeley Internet Name Domain), geschreven door studenten van de Berkeley universiteit in Californië (USA). De opdracht voor deze week is: installeer en test de *BIND* DNS server.

Over DNS



Dit is Jon Postel in 1994. Jon Postel komt uit Amerika en je ziet dat hij wijst naar een kaart van het Internet. Het Internet was vroeger heel klein en gezellig. Alleen de computers van universiteiten in Amerika en Europa waren erop aangesloten. Postel hield de namen van deze computers bij in een tekstbestandje. Dit tekstbestandje werd regelmatig naar alle deelnemers gemaild en is een soort telefoonboek, waarin je het nummer van een computer kunt opzoeken, om hem te kunnen bellen.

Toen het internet groter werd, kon Postel het tekstbestandje niet meer alleen bijhouden. Om dit probleem op te lossen, schreven studenten van de *Berkeley Universiteit* in Amerika een programma, genaamd BIND. BIND is een domein naam systeem, afgekort DNS.

In het Domein Naam Systeem worden de namen en nummers van alle computers in het netwerk centraal bijgehouden. Het tekstbestandje bestaat nog steeds en je kunt het vinden onder de bestandsnaam */etc/hosts*. In de Windows-wereld wordt de DNS server ook wel de *Domain Controller* genoemd.

Het *sudo* mechanisme

Het configureren van Linux doen we namens de *super-user*. We moeten daarom tijdelijk inloggen als Administrator.

Cygwin gebruikers

Sudo voor Cygwin gebruikers: rechts-klik op het icoon van de Cygwin terminal, en kies voor **Als administrator uitvoeren**. Update eerst even de package-database:

```
apt-get update
```

Nu kunnen we de BIND DNS server installeren. Dit doen we met het *apt-get* programma:
apt-get install bind bind-utils

Debian

Sudo voor gebruikers van andere Linux-versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc): start een terminal met de toetsencombinatie **<Ctrl><Alt>-T**. We gebruiken het commando *sudo* om in te loggen met het *su* (become Super User) commando. Daardoor blijven we ingelogd:

```
sudo su
```

Update eerst even de package-database:
apt-get update Update eerst even de package-database:

```
apt-get update
```

Nu kunnen we de BIND name server software installeren. Dit doen we met het *apt-get* programma:
apt-get install bind9 dnsutils

Unprivileged user aanmaken

De BIND name daemon werkt namens een *unprivileged user*. Zoals al eerder uitgelegd, is dit een veiligheidsmaatregel om hackers buiten de deur te houden. Deze gebruiker bestaat op sommige Linux systemen nog niet. We moeten hem dus eerst aanmaken.

Cygwin gebruikers

Dit doen we met het commando *useradd*:

```
useradd -M -d /var/empty named
```

Debian

In andere Linux versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc) heet de unprivileged user *bind*:

```
useradd -M -d /var/empty bind
```

Via optie *M* geef je aan dat er geen *home-directory* voor de nieuwe gebruiker moet worden aangemaakt. Met optie *d* (directory) geven we aan dat */var/empty* de home-directory van de nieuwe gebruiker is. Als je geen foutmeldingen krijgt, is het commando succesvol uitgevoerd.

Cygwin gebruikers

Ook ontnemen we de nieuwe gebruiker de login-rechten. Dit doen we met het commando *usermod*:

```
usermod -L named
```

Debian

In andere Linux versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc) heet de unprivileged user *bind*:

```
usermod -L bind
```

Via optie *L* (lock) worden de nieuwe gebruiker de login-rechten ontnomen. Dit noemen we een *unprivileged user*.

DNSSEC uitzetten

Normaal wordt de domeininformatie tussen DNS servers onderling uitgewisseld in platte tekst. Middels *DNSSEC* (Secure DNS) wordt de domeininformatie versleuteld. Omdat wij niet over een geldig certficaat beschikken zullen we foutmeldingen krijgen. We kunnen dit oplossen door DNSSEC in onze server uit te zetten. De instellingen voor de BIND DNS server worden bijgehouden in het *named.conf* bestand.

Cygwin gebruikers

Open het configuratiebestand met de *vi* editor:

```
vi /etc/named.conf
```

Debian

In andere Linux versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc) staat het bestand in de */etc/bind* directory. Open het configuratiebestand met de *vi* editor:

```
vi /etc/bind/named.conf.options
```

Je krijgt ongeveer het volgende te zien. De inhoud van het bestand is op iedere computer anders, maar de instellingen zijn hetzelfde. Toets **i** (insert), zodat we naar de *INSERT* modus gaan en voeg de vetgedrukte regel toe:

```
options {
     version "";     // remove this to allow version queries
     directory "/var/named";
     listen-on    { 127.0.0.1; };
     dnssec-enable no;
     listen-on-v6 { none; };
     allow-recursion { clients; };
     dnssec-validation no;
};
```

Middels de optie *dnssec-validation* kunnen we aangeven of de domeininformatie versleuteld moet worden. We zetten deze optie op *no* omdat we geen geldig certificaat hebben.

Toets **<Esc>** om uit de *INSERT* modus te komen en geef de *w* (write) en *q* (quit) commando's:

```
:wq
```

Het bestand wordt opgeslagen en we zijn terug in de Linux command line.

Het hoera-moment

Nu kunnen we de BIND name daemon testen. Herstart allereerst de server, zodat de instellingen opnieuw worden ingelezen. Dit doen we met met het *service* programma:

Cygwin gebruikers

Herstart de BIND nameserver:

```
service bind restart
```

Debian

In andere Linux versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc) heet de service *bind9*:

```
service bind9 restart
```

Testen doen we via het uitvoeren van een zogenaamde *query*. Dit doen we met het *nslookup* programma:

```
nslookup localhost.
```

Let op: de punt (".") aan het eind is belangrijk. Zonder punt zoekt de *resolver* alle mogelijke domeinnamen op (bijvoorbeeld: localhost.intra.rocleiden.nl). Dat is niet wat we willen.

De output moet er ongeveer alsvolgt uitzien. Als het goed is staat achter de veldnaam *Server* het IP-adres van je localhost (127.0.0.1). Dit betekent dat de query via je eigen DNS is uitgevoerd:

```
Server:      127.0.0.1
Address:       127.0.0.1#53

Name:   localhost
Address: 127.0.0.1
```

Huiswerk opsturen

Zoals je weet, kun je de opdracht aftekenen door een e-mail met daarin de output van het *history* commando te versturen. Dit doen we met een pijpleiding tussen de commando's *nslookup* en *email*. Zorg dat het onderwerp van de e-mail tussen aanhalingstekens staat:

```
nslookup localhost. | email -s "Installatie BIND" docent@localhost
```

Als je geen foutmelding ziet is de e-mail succesvol verstuurd.

Administrator uitloggen

We hebben de BIND DNS server geïnstalleerd en getest, maar we zijn nog steeds ingelogd als Administrator (*root*).

Geef tot slot **<Ctrl>-D** om de Administrator uit te loggen.

Problemen oplossen

Als je in bovenstaande output een foutmelding krijgt, kijk dan in het logbestand van de Linux *daemons* (programma's die in de achtergrond draaien). Hier worden eventuele foutmeldingen bijgeschreven:

tail /var/log/daemon

Let op: in sommige Linux systemen heet het algemene logbestand **/var/log/daemon.log**. De output van een correct geïnstalleerde DNS server ziet er ongeveer alsvolgt uit:

```
Apr 17 20:20:12 optiplex named: PID 2644: command channel listening on 127.0.0.1#953
Apr 17 20:20:12 optiplex named: PID 2644: all zones loaded
Apr 17 20:20:12 optiplex named: PID 2644: running
```

Server wordt niet gebruikt

Het kan zijn dat je in de output van *nslookup* een ander IP-adres ziet staan. Dit betekent dat je nieuwe DNS server niet gebruikt is. Op een Linux machine kunnen domeinnamen op verschillende manieren worden opgezocht. De meest bekende zijn via het */etc/hosts* bestand (de 'mini-dns') en via een aparte DNS name-server. Dit mechanisme is vastgelegd in de Linux kernel en wordt in de Linux-wereld ook wel de *resolver* genoemd. De instellingen van de resolver worden bijgehouden in het bestand *resolv.conf*. Controleer of het configuratie-bestand correct is aangemaakt. Dit doen we met het cat commando:

cat /etc/resolv.conf

Je zou ongeveer de volgende output moeten kunnen zien:

```
# Generated by resolvconf
domain sassenheim.dmz
nameserver 127.0.0.1
```

In veel Linux distributies wordt het programma *resolvconf* gebruikt om de resolver te configureren, maar is vaak niet geactiveerd. Om het te activeren kunnen we de BIND opstartinstellingen controleren:

vi /etc/default/bind9

Je ziet de volgende instelling. Zorg ervoor dat deze op *yes* staat en sla het bestand op:

```
# run resolvconf?
RESOLVCONF=yes
```

Probeer het dan nog een keer.