

Huiswerk Linux: Instellen Smart Host

Zoals in de vorige opdracht beschreven is Sendmail een *Mail Transfer Agent* (MTA) en dus in staat om zelf de computers te vinden waar de e-mail uiteindelijk naartoe moet. We hebben dit in de vorige opdracht zelf met de hand uitprobeerde. De opdracht voor deze week is: stel de *Smart Host* voor je eigen mail server in.

Over e-mail forwarding

Normaal verstuurt Sendmail uitgaande e-mail via poort 25. Helaas hebben zowel ROC Leiden als ook de meeste internet providers (KPN, Ziggo, Online.nl) deze poort geblokkeerd omdat er teveel spam overheen wordt gestuurd. Gelukkig bieden de meeste providers ook gelijk de oplossing voor dit probleem. Zij hebben een interne mail server klaarstaan die de e-mail voor jouw doorstuurt. Dit doorsturen noemen we *forwarding* en de interne mail server noemen we een *Smart Host*.

Binnen ROC Leiden hebben we helaas geen smart host. We gaan dus mijn eigen mail server (**boland.xs4all.nl**) als smart host gebruiken. Deze ligt buiten het ROC netwerk en omdat binnen ROC *alle* poorten naar buiten geblokkeerd worden, moeten we bovendien uitwijken naar poort **21** (zie ook: *Huiswerksysteem*).

Het *sudo* mechanisme

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

Cygwin gebruikers	Andere Linux gebruikers
Sudo voor Cygwin gebruikers: rechts-klik op het icoon van de Cygwin terminal, en kies voor Als administrator uitvoeren . Zorg er ook voor dat de Sendmail daemon is gestart: service sendmail start	Sudo voor gebruikers van andere Linux-versies (<i>Ubuntu, Lubuntu, Kubuntu, Gentoo, Debian</i> , etc): start een terminal met de toetsencombinatie <Ctrl><Alt>-T . We gebruiken het commando <i>sudo</i> om in te loggen met het <i>su</i> (become Super User) commando. Daardoor blijven we ingelogd: sudo su

Smart Host instellen

Sendmail wordt geconfigureerd via het bestand */etc/mail/sendmail.cf*. Oorspronkelijk werd dit bestand met de hand gewijzigd. Maar in de loop der jaren zijn er zoveel opties bijgekomen, dat het nu meestal gedaan wordt via een zogenaamd *m4* script.

Het *m4* programma is een *tool* om ingewikkelde configuratiebestanden aan te maken (*general-purpose macro processor*). Via zogenaamde *directieven* kun je in één keer hele groepen van instellingen wijzigen.

Cygwin gebruikers	Andere Linux gebruikers
De <i>m4</i> scripts van Sendmail kun je vinden in de <i>cf</i> (config) directory van sendmail. Wissel naar deze directory met het <i>cd</i> (change directory) commando: cd /usr/share/sendmail/cf	Gebruikers van andere Linux-versies (<i>Debian, Ubuntu, Lubuntu, Kubuntu, Gentoo, Mint</i> , etc) kunnen de <i>m4</i> scripts vinden in de <i>/etc/mail</i> directory van sendmail. Wissel naar deze directory met het <i>cd</i> (change directory) commando: cd /etc/mail

Open het Sendmail *m4* script met de *vi* editor:

vi sendmail.mc

Het *m4* script voor Linux ziet er in iedere distributie anders uit, maar de instellingen zijn hetzelfde. Zoals je ziet zijn er verschillende *options* en *features* ingesteld. Ook kun je zien dat aan het begin van de meeste regels de letters *dnl* (delete until next line) staan. Hierdoor wordt alles tot aan de volgende regel genegeerd, vergelijkbaar met het hekje-symbool (#) in de Linux configuratiebestanden. Administrators kunnen deze *options* en *features* activeren door de letters *dnl* weg te halen.

Plaats de cursor aan het einde van het bestand met (hoofdletter) **G** en toets **i** (insert). We gaan dan naar de *INSERT* modus. Voeg nu de vetgedrukte regels in, zoals in het onderstaand voorbeeld:

```
divert(0)
VERSIONID(`$Id: generic-linux.mc,v 8.2 2014-08-13 20:51:08 dboland Exp $')
OSTYPE(linux)
DOMAIN(generic)
FEATURE(`virtusertable', `hash -o /etc/mail/virtusertable')
define(`confrun_as_user', `SYSTEM')
define(`confTO_IDENT', `0s')
dnl define(`ALIAS_FILE', `/etc/aliases')
define(`confLOG_LEVEL', `23')
dnl # Listen on localhost only
FEATURE(`no_default_msa')
DAEMON_OPTIONS(`Family=inet, Address=127.0.0.1, Port=25, Name=MTA-SMTP')
DAEMON_OPTIONS(`Family=inet, Address=127.0.0.1, Port=587, Name=MTA-SMTPA, M=Ea')
dnl # With STARTTLS (enables SMTPS port 587)
dnl define(`CERT_DIR', `MAIL_SETTINGS_DIR`certs')
dnl define(`confCACERT_PATH', `CERT_DIR')
dnl define(`confCACERT', `CERT_DIR/domain.pem')
dnl define(`confSERVER_CERT', `CERT_DIR/domain.pem')
dnl define(`confSERVER_KEY', `CERT_DIR/domain.pem')
dnl define(`confCLIENT_CERT', `CERT_DIR/domain.pem')
dnl define(`confCLIENT_KEY', `CERT_DIR/domain.pem')
dnl # With AUTH (enables SMTPSA port 465, disables SMTP port 25)
dnl # Also called 'Secure Password Authentication' by mail clients
dnl DAEMON_OPTIONS(`Family=inet, Address=0.0.0.0, Port=465, Name=MTA-SMTPSA, M=s')
dnl DAEMON_OPTIONS(`Family=inet6, Address=::, Port=465, Name=MTA-SMTPSA, M=s')
define(`SMART_HOST', `boland.xs4all.nl')dnl
define(`RELAY_MAILER_ARGS', `TCP $h 21')dnl
MAILER(local)
MAILER(smtp)
```

Let op: plaats nieuwe regels altijd voor de MAILER regels. Deze regels moeten altijd de laatste regels zijn.

Let goed op: Het format van deze instellingen is bizar. Als je goed kijkt lijkt het alsof de aanhalingstekens verkeerd worden gebruikt (**SMART_HOST**), maar het is toch correct!

Via de SMART_HOST instelling geven we aan dat alle uitgaande e-mail naar *boland.xs4all.nl* moet worden gestuurd. Deze server zoekt voor ons de MX-records op en stuurt de e-mail door naar de werkelijke bestemming. Middels de RELAY_MAILER_ARGS instelling geven we aan dat de communicatie via poort 21 moet plaatsvinden, omdat de SMTP poort 25 op school niet werkt.

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

```
:wq
```

Het *m4* bestand wordt nu opgeslagen en we zijn terug op de Linux command-line.

Configuratiebestand genereren

Nu kunnen we het *m4* script gebruiken om het Sendmail configuratiebestand te genereren.

Cygwin gebruikers

Cygwin gebruikers kunnen dit doen met het *make* programma:

```
make install-cf
```

Andere Linux gebruikers

Gebruikers van andere Linux-versies (*Debian, Ubuntu, Lubuntu, Kubuntu, Gentoo, Mint, etc*) gebruiken ook het *make* programma, maar op de volgende manier:

```
make
```

Via het programma *m4* zorgen we ervoor dat het *sendmail.cf* bestand opnieuw wordt aangemaakt en in de */etc/mail* directory geplaatst.

Het hoera-moment

Allereerst moeten we Sendmail herstarten, zodat de nieuwe instellingen worden ingelezen. Dit doen we met het *service* programma:

```
service sendmail restart
```

Om te zien of het werkt verstuur je een e-mail aan mijn privé-adres. We gebruiken daarvoor het *email* programma:

```
echo "Hallo wereld" | email -s "Relay test" -r localhost -p 25 dboland@xs4all.nl
```

Middels de optie *r* (relay) geven we aan dat we de e-mail via onze eigen mail server willen versturen. Deze luistert op de *localhost* (127.0.0.1). Via de optie *p* (port) geven we aan dat we de standaard smtp-poort (25) willen gebruiken.

Om te controleren of de e-mail correct is verstuurd, kunnen we in het maillog kijken. Dit doen we met het *tail* commando:

```
tail /var/log/maillog
```

Let op: op sommige Linux systemen heet het log-bestand */var/log/mail.log*. De output van een succesvolle verzending ziet er ongeveer als volgt uit (*Message accepted for delivery*):

```
Aug 11 20:49:07 optiplex sm-mta: PID 2132: t7BIn7Au002132: from=<d.boland@rocleiden.nl>,
size=383, class=0, nrcpts=1,
msgid=<201508111849.t7BIn7Au002132@optiplex.sassenheim.dmz>, proto=ESMTP, daemon=MTA,
relay=localhost [127.0.0.1]
Aug 11 20:49:08 optiplex sm-mta: PID 3800: STARTTLS=client, relay=boland.xs4all.nl.,
version=TLSv1/SSLv3, verify=FAIL, cipher=DHE-RSA-AES256-SHA, bits=256/256
Aug 11 20:49:08 optiplex sm-mta: PID 3800: t7BIn7Au002132: to=<dboland@xs4all.nl>,
delay=00:00:01, xdelay=00:00:00, mailer=relay, pri=120383,
relay=boland.xs4all.nl. [83.162.146.149], dsn=2.0.0, stat=Sent (t7BJrNAg020740
Message accepted for delivery)
```

Huiswerk opsturen

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

```
cat /var/log/maillog | email -s "Configuratie Smart Host" docent@localhost
```

Let op: op sommige Linux systemen heet het log-bestand */var/log/mail.log*. Als je geen foutmelding ziet is de e-mail succesvol verstuurd.

Administrator uitloggen

We hebben Sendmail als Smart Host geconfigureerd, maar we zijn nog steeds ingelogd als Administrator (*root*).

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

Problemen oplossen

Het kan zijn dat je in bovenstaande test een foutmelding krijgt. Het lijkt alsof het gelukt is, want de laatste regel geeft aan dat de e-mail is verstuurd (*Sent*):

```
Aug 11 23:09:48 optiplex sm-mta: PID 2320: t7BL9mIW002320: to=<d.boland@rocleiden.nl>,
    delay=00:00:00, xdelay=00:00:00, mailer=relay, pri=31660, relay=smtp.boland.nl.,
    dsn=5.7.1, stat=User unknown
Aug 11 23:09:48 optiplex sm-mta: PID 2320: t7BL9mIW002320: t7BL9mIX002320: return to
    sender: User unknown
Aug 11 23:09:49 optiplex sm-mta: PID 2320: t7BL9mIX002320: to=root, delay=00:00:01,
    xdelay=00:00:01, mailer=local, pri=32684, dsn=2.0.0, stat=Sent
```

Maar als we naar de regel erboven kijken, dan zien we de foutmelding *User unknown*. De *Sent*-regel geeft in dit geval aan dat de *root* user de complete foutmelding heeft ontvangen. Deze kunnen we opvragen met de mutt e-mail client:

```
mutt -f /var/spool/mail/root
```

Middels de optie *f* (file) geven we aan dat we in de INBOX van de *root* user willen kijken. Je kunt de laatst ontvangen e-mail bekijken door hem te selecteren en **<Enter>** te geven. Je ziet onder andere het volgende:

```
----- Transcript of session follows -----
... while talking to smtp.boland.nl.:
>>> DATA
<<< 550 5.7.1 <d.boland@rocleiden.nl>... Relaying denied. Proper authentication required.
550 5.1.1 <d.boland@rocleiden.nl>... User unknown
<<< 503 5.0.0 Need RCPT (recipient)
```

Mijn mail-server (smtp.boland.nl) weigert de e-mail door te sturen (*Relaying denied*) en wenst authenticatie, maar kan de user d.boland@rocleiden.nl (mijn afzender-adres) niet in de wachtwoorden-database vinden. Dit gebeurt als je de test niet vanuit school uitvoert.

Toch kunnen we dit als een hoera-moment beschouwen, want onze eigen *Mail Transfer Agent* heeft de e-mail succesvol weten te versturen naar de *Mail Exchanger* (smtp.boland.nl).