SelfLinux-0.13.1

Linux als Mailserver

Autor: Dirk Hebenstreit (*Dirk.Hebenstreit@epost.de*)
Formatierung: Johnny Graber (*selflinux@jgraber.ch*)
Lizenz: GFDL

Im INTERNET wie auch im INTRANET ist die elektronische Post inzwischen einer der wichtigsten Dienste geworden.

Hier werden die grundsätzlichen Verfahren des Mailaustausches sowie zwei typische Unix Mailer Server vorgestellt

Inhaltsverzeichnis

1 Grundlagen

Im INTERNET wie auch im INTRANET ist die elektronische Post inzwischen einer der wichtigsten Dienste geworden. Mit der zunehmenden Vernetzung von Arbeitsgruppen in den Unternehmen entstanden neben den INTERNET-Standards aber gleichzeitig diverse proprietäre Maildienste (MS-Mail, cc:Mail oder Notes), welche erst in der letzten Zeit wieder zusammenwachsen und sich hin zu den Standards des INTERNET bewegen. So kann mittlerweile jeder moderne Mailclient mit INTERNET-Nachrichten umgehen und die Mailserver der großen Softwareanbieter wie MS-Exchange oder Lotus Notes/Domino bieten die Möglichkeit, Daten auch zwischen INTRANET und INTERNET auszutauschen. Stellen wir also zuerst einmal fest, welche Standards im Zusammenhang mit elektronischer Post zu sehen sind:

* SMTP (Simple Message Transfer Protocol)
  Es ist das Übertragungsprotokoll der Server untereinander und wird von den Clients zun Einliefern der Post benutzt.
* POP (Post Office Protocol; derzeit aktuell in der Version 3)
  Die Clients benutzen es, um ihre Post vom Server abzuholen. Entgegen dem SMTP besteht dabei die Möglichkeit, die Mail auch teilweise auf dem Server zu verwalten (allerdings nur in beschränktem Maße).
* IMAP (Internet Mail Access Protocol; derzeit aktuell in der Version 4)
  IMAP wird wie POP 3 von den Clients benutzt, um Mail vom Server abzuholen. Es bietet aber gegenüber POP wesentlich mehr Flexibilität bei der Verwaltung der Post, so z.B. die Möglichkeit, Eingangskörbe auf dem Server zu verwalten und Roaming Users, also Anwender, die von verschieden Orten aus auf den Server zugreifen wollen.
* X.400
  Dieses Protokoll ist ein OSI-Standard und häufig im Behördenumfeld anzutreffen. Es ist, OSI üblich, sehr umfangreich und mächtig, aber es gibt kaum Anwendungen. Häufig werden POP/SMTP für den Zugriff durch die Clients benutzt und danach eine Umsetzung auf X.400 durch den Mailserver durchgeführt.
* X.500
  Ebenfalls ein OSI-Protokoll. Es beschreibt den Aufbau eines Verzeichnisdienstes der u.a. auch Mailadressen verwalten kann. X.400 nutzt in einer reinen OSI-Umgebung X.500 als Adressbuch.
* LDAP (Lightweight Directory Access Protocol)
  Eine ``leichte" Variante des DAP (Directory Access Protocol), welches von X.500 für den Zugriff auf die Datenbasis benutzt wird. LDAP wird derzeit von den neueren Mailclients (Outlook, Netscape) unterstützt, um auf globale Verzeichnisdienste zuzugreifen (Netcenter, VeriSign, Bigfoot etc.)

2 Aufbau einer Mail-Umgebung

Das INTERNET stellt sich mit seiner Mail-Struktur vereinfacht folgendermaßen dar:
In den Domains der bei der IANA registrierten Netze stehen die Mail Transfer Agents (MTA), welche die Nachrichten annehmen und untereinander verteilen. Dabei wird in der Regel der direkte Austausch von MTA zu MTA bevorzugt, d.h., bevor eine Nachricht von A nach B geleitet wird, erfolgt ein Namensauflösung des Zielsystems B. Danach stellt der MTA A die Nachricht direkt an den MTA B zu.
Von dieser Verfahrenweise kann abgewichen werden, wenn die Konfiguration der MTAs dies festlegt, man spricht dann vom Mail-Routing. MTAs die nur als Zwischenstationen benutzt werden heißen Mail-Relay.
Um dem Anwender die Nachricht zustellen zu können, muß sich dieser mit einem User Agent (UA) an den MTA wenden. Er kann dann die Nachricht auf sein Zielsystem übertragen oder aber auf dem Server belassen und dort in einem Postfach verwalten. Hier kommen POP und IMAP ins Spiel.

3 Mail im INTRANET

Für das INTRANET gilt im Wesentlichen dasselbe wie für das INTERNET. Bleibt es bei einem lokalen Netz, so agiert der Mailserver als MTA und ggf. sogar als UA probieren Sie es aus:
Melden Sie sich an Ihrem Server an und starten Sie das Programm elm. Sie benutzen damit einen UA (elm) auf dem MTA). Wenn mehrere Standorte miteinander über ein WAN vernetzt sind, kommen häufig mehrere MTAs ins Spiel, welche die Nachrichten untereinander synchronisieren müssen. Die Art der darunterliegenden Netzverbindung ist dabei egal, Hauptsache, eine gleich wie geartete Datenübertragung ist möglich. Im INTERNET erfolgte dies am Anfang ausschließlich über das Protokoll/Verfahren UUCP (UNIX to UNIX copy), welches auf der Basis von Modem-Verbindungen die Nachrichten en Block austauschte. Heutzutage ist SMTP das Verfahren der Zeit, weshalb wir in diesem Kurs auf UUCP nicht weiter eingehen wollen.
Was benötige ich, um aus LINUX einen Mailserver zu machen? Nun, ich benötige einen MTA, also eine Software die Nachrichten entgegennimmt, weiterleitet und an die UAs zustellt, ferner Dämonen, welche die Protokolle POP und/oder IMAP zur Verfügung stellen.

4 Der MTA

Wie UNIX-üblich existieren verschiedene MTAs, so dass wir den uns genehmen auswählen können. Zur Disposition stehen an erster Stelle die Pakete

* Sendmail
* qmail

4.1 Sendmail

Das Paket `sendmail` ist eines der ältesten INTERNET-Programme und wohl auch das mit dem schlechtesten Ruf. Am Anfang war es aufgrund diverser Sicherheitslücken ein beliebtes Einfalltor für Hacker und Co., und bei den Administratoren ist es wegen seiner schwierigen Konfiguration gefürchtet. Dennoch hat es sich zum Standard für UNIX/LINUX-MTAs erhoben und verdient auf jeden Fall eine genauere Betrachtung.
Mit den Jahren ist `sendmail`, was die Sicherheit anbelangt, wesentlich besser geworden. Da es als OpenSource zur Verfügung steht, hatten Gott und die Welt Zeit und Muße, den Quellcode auf Fehler abzuklopfen und diese auszumerzen. Sendmail ist daher bei anständiger Konfiguration nicht unsicherer als andere Dienste auf einem UNIX-Server. Was die Konfiguration angeht, so haben sich die Programmierer die Kritik zu Herzen genommen und ein Tool entwickelt, welches die Arbeit erleichtert. Dieses Tool namens IDA ist bei SuSE im sendmail-Paket bereits enthalten und wird intern von YaST aufgerufen.

4.2 Qmail

Das Paket qmail entstand aus dem Frust heraus, einen sendmail-MTA administrieren zu müssen. Anfangs suchte der Autor einen einfachen Ersatz, doch mittlerweile ist qmail zu einem vollständigen MTA gewachsen, der in seiner Komplexität sendmail nicht mehr nachsteht. Wir verzichten in diesem Kurs auf die nähere Beschreibung, legen dem Leser aber nahe, sich mit dieser Software als Alternative auseinanderzusetzen. Die aktuelle Version findet sich unter www.qmail.org.

5 Installation von sendmail

In der SuSE-Distribution ist `sendmail` in der Serie n enthalten, es wird daher am einfachsten über YaST installiert:

> Installation festlegen/starten ->
> Konfiguration ändern/erstellen ->
> Netzwerk-Support

Nach der Installation kann `sendmail` dann wieder über `YaST` mit seiner Konfigurationsdatei (sendmail.cf) versehen werden. Hierfür ruft man in `YaST` das Menü

> Administration des Systems ->
> Netzwerk konfigurieren ->
> Sendmail konfigurieren

auf.

Wählen Sie Konfiguration mit Zugriff über einen Nameserver, um `sendmail` über eine ppp-Verbindung auf den Provider zugreifen zu lassen. Wenn der Server ausschließlich lokal betrieben wird ist die Auswahl beliebig, kann bei einem späteren INTERNET-Anschluß aber jederzeit geändert werden. Im Verzeichnis /etc wird jetzt die Konfigurationsdatei angelegt. Ferner schreibt die Installation in das Verzeichnis /sbin/init.d das Start-/Stopscript sendmail und legt in /etc/rc.d/rc2.d die symbolischen Verweise S20sendmail und K20sendmail an. Um sendmail jetzt zu starten geben Sie an der Kommandozeile den Befehl

```
root@linux ~/ # sh /etc/rc.d/sendmail start
```

ein. Das Kommando ps sollte uns jetzt folgende Ausgabe liefern:

```
root@linux ~/ # ps ax| grep sendmail
  22432  ?  S    0:00 sendmail: accepting connections on port 25
```

Wie man erkennen kann, benutzt `sendmail` jetzt den Port 25 (SMTP) für ein- und ausgehende Verbindungen. Um im laufenden Betrieb einen Neustart des Dienstes zu erreichen genügt ein `sh /etc/rc.d/sendmail reload`

5.1 Einträge in /etc/rc.config

Das Verhalten von `sendmail`kann UNIX-üblich über Kommandozeilenparameter beeinflußt werden. SuSE hat hierfür in das Start-/Stopscript Variable aufgenommen, welche in der Datei /etc/rc.config gesetzt werden.
Diese sind:

-SENDMAIL_TYPE="yes"

> bestimmt, dass die Konfiguration von sendmail.cf über rc.config und YaST erfolgen soll. Bei ``no" müssen wir diese selber editieren.

-SENDMAIL_SMARTHOST=""

Bei Verbindung über UUCP wird hier der sog. ``smarthost'' (der Kommunikationspartner) eingetragen.

-SENDMAIL_LOCALHOST="localhost"

Die hier aufgeführten Namen werden als Aliasnamen für den eigenen Rechner betrachtet. Es unterbleibt die DNS-Anfrage!

-SENDMAIL_RELAY=""

Sendmail liefert keine Nachrichten lokal aus, sondern übergibt diese an das Relay. Damit kann ein Relay-Verbund aufgebaut werden.

-SENDMAIL_ARGS="-bd -q30m -om"

Hier werden `sendmail` seine Startparameter übergeben. Die komplette Liste erhält man mit `man sendmail`, die hier aufgeführten Werte bedeuten: -bd: `sendmail` startet als Daemon und geht in den Hintergrund -q30m: die Nachrichten in der Warteschlange werden alle 30 Minuten abgearbeitet -om: die Option ``m'' wird gesetzt (s. Installations- und Betriebshandbuch ;-))

SENDMAIL_EXPENSIVE="yes"

Mit dieser Einstellung schreibt `sendmail` die Nachrichten nur in seine Messagequeue und stellt sie erst beim Aufruf `sendmail -q` zu. Dies wird benötigt, wenn man den Server mittels ISDN-Wählverbindung an das INTERNET gehängt hat und nicht will, dass jede ausgehende Mail eine Verbindung zum Provider aufbaut. Stattdessen ruft man `sendmail -q` per crontab z.B. in den Nachtstunden auf und holt bzw. sendet die Mail in einem Rutsch (Polling). Alternativ kann der Eintrag auch in das PPP-Startscript aufgenommen werden, so dass bei jedem Verbindungsaufbau auch ein Mailaustausch stattfindet.1.1

SENDMAIL_NOCANONIFY="no"

Sendmail versucht nicht mehr, bei jeder Mail den vollen Namen der Mailadresse per DNS aufzulösen. Diese Einstellung ist ebenfalls bei ISDN-Dialup-Verbindungen wichtig um zu verhindern, dass auch lokale Adressen über den DNS des Providers aufgelöst werden. Alternativ kann auch ein lokaler DNS dies unterbinden (s. Aufbau eines DNS-Servers)

5.2 Ein kurzer Blick in sendmail.cf

Um zu verstehen, warum `sendmail` als ``Konfigurationsmonster'' gilt, hier ein kleiner Ausschnitt aus der Datei sendmail.cf:

sendmail.cf

```
Cwlocalhost
# my official domain name

# ... define this only if sendmail cannot automatically
determine your domain

#Dj$w.Foo.COM
CP.

# "Smart" relay host (may be null)
DS

# place to which unknown users should be forwarded

#Kuser user -m -a<>

#DLname_of_luser_relay

# operators that cannot be in local usernames (i.e., network indicators)

CO @ % !

# a class with just dot (for identifying canonical names)

C..

# a class with just a left bracket (for identifying domain literals)

C[[

# Mailer table (overriding domains)

Kmailertable hash -o /etc/mail/mailertable.db

# Domain table (adding domains)

#Kdomaintable dbm /etc/domaintable

# Generics table (mapping outgoing addresses)

Kgenerics hash -o /etc/mail/genericstable.db
```

5.3 mailertable

Die Datei mailertable legt fest, auf welchem Wege die Mail für bestimmte Zielsysteme zugestellt werden soll. Sie wird standardmäßig bei SuSE nicht angelegt, was zu Problemen führen kann, wenn man nicht das von SuSE gelieferte rpm-Paket installiert, sondern `sendmail` aus den Sourcen heraus selbst übersetzt. Am besten, man legt die Datei mit dem Befehl

```
root@linux ~/ # touch /etc/mailertable
```

an und läßt sie leer. Wenn man sie jedoch einsetzten will hat sie folgenden Aufbau:

/etc/mailertable

```
# /etc/mailertable
# Legt fest, wie ein Host zu erreichen ist

# Zuerst die Zustellung in der eigenen Domain über smtp.
# %1 wird dabei durch die eMail-Adresse des Empfängers ersetzt
# Hinweis: Der Domainname muß aufgelöst werden können!

.my.domain     smtp:%1

my.domain      smtp:%1

# Der Rechner somebody ist über relay.my.domain erreichbar
somebody       smtp:[relay.my.domain]

# Für den Rechner number soll kein DNS genutzt werden
 number         smtp:[192.168.1.56]
```

Um diese mailertable dem Programm `sendmail` bekannt zu machen muß sie mit dem Befehl `makemap` in ein DBM-Format übersetzt werden. Neustarten des `sendmail` nicht vergessen!

5.4 aliases

Die Datei /etc/aliases ermöglicht es, einer realen Mailadresse verschiedene Pseudonyme zuzuordnen. So existiert auf Webservern in der Regel dein Aliasname für den Systemverantwortlichen als webmaster@my.domain, das NetNews-System benutzt das Synonym news@my.domain um Fehlermeldungen zuzustellen. Um nicht für jede dieser Kennungen echte Accounts anlegen zu müssen, können diese einem oder mehreren User-Accounts zugeordnet werden.

/etc/aliases

```
# /etc/aliases
# Zuordnung von Aliasnamen zu realen Accounts
# Erst die Systemkennungen:

news:             pmeier, \news
newsadmin:        pmeier
newsadm:          pmeier
webmaster:        rschulz
postmaster:       sschmidt
mail:             sschmidt
root:             nkrueger, \root
# ``sprechende'' Aliasnamen für die Accounts

pmeier:           peter.meier
rschulz:          robert.schulz
sschmidt:         stefan.schmidt
nkrueger:         norbert.krueger
```

Die Syntax ist damit recht einleuchtend, interessant sind die Einträge news: pmeier, \news und root: nkrueger, \root. Damit wird sichergestellt, dass die an die Kennungen news und root adressierten Nachrichten nicht nur an den realen Benutzer pmeier, sondern auch an die Systemkennungen news bzw. root zugestellt werden. Damit erzeugt man quasi ein Mailarchiv für diese Kennungen und kann darin auch noch nach Meldungen suchen, wenn nkrueger sie bereits in seinem Eingangskorb gelöscht hat.

In der zweiten Hälfte der Datei werden die heute recht gebräuchlichen eMail-Adressen der Form mein.name@my.domain erzeugt. Dieser Abschnitt will allerdings auf einem Produktivsystem mit häufig wechselnden Accounts gepflegt sein!
Bevor die Aliasnamen eingesetzt werden können, muß mit dem Befehl `newaliases` erst wieder eine DBM-Datei erzeugt werden. Auch hier schadet es nichts, `sendmail` neu zu starten!

6 POP3-Server

Für das Abholen der Mail auf dem Server wird in der Regel das Protokol POP (Post Office Protocol) in der Version 3 verwendet. Bei SuSE ist der hierfür notwendige Daemon leicht installiert, er findet sich in der Serie n als pop. Nach der Installation über YaST ist in der Datei /etc/inetd.conf der Eintrag

/etc/inetd.conf

```
pop3    stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/popper -s
```

durch Entfernen des Kommentarzeichens # zu aktivieren. Damit wird das Programm /usr/sbin/popper mit dem Parameter -s über das Programm tcpd (dem tcp-Wrapper) gestartet. Dieser doppelte Aufruf ist notwendig, um Zugriffsbeschränkungen für die zu startenden Dämonen zu realisieren und den Zugriff selber mittels syslog zu protokollieren. Näheres zum tcp-Wrapper s. man tcpd.
Nach den Änderungen in inetd.conf ist dies dem inetd-Prozeß mitzuteilen:

```
root@linux /root/ # killall -HUP inetd
```

Um sich davon zu überzeugen, dass unser POP-Dämon jetzt aufrufbereit ist gebe man ein:

```
root@linux /root/ # netstat -a | grep pop
 tcp        0      0 *:pop3          *:*             LISTEN
```

Der Eintrag LISTEN zeigt, dass unser POP-Server erfolgreich registriert wurde.

7 IMAP-Server

Der IMAP-Dämon wird nach demselben Schema eingerichtet wie POP3. Zuerst sucht man in der Datei /etc/inetd.conf den Eintrag

/etc/inetd.conf

```
imap2   stream  tcp     nowait  root    /usr/sbin/tcpd  imapd
```

und entfernt das Kommentarzeichen (#). Danach folgt wieder

```
root@linux /root/ # killall -HUP inetd
```

und die Kontrolle mit

```
root@linux /root/ # netstat -a | grep imap
 tcp        0      0 *:imap2       *:*             LISTEN
```

Jetzt können wird die Clients für den Zugriff über POP oder IMAP auf unseren Server einrichten.

8 Konfiguration von Netscape als Mailclient

Die Einstellungen für den Mailzugriff erfolgen bei Netscape unter dem Punkt

Edit -> Preferences

Für das Versenden der Mail ist der SMTP-Server und der Benutzername einzutragen. Der Server für den Maileingang ist im Feld ``Mail Server'' zu konfigurieren, nachdem man ihn mit ``Add'' angelegt hat. In der folgenden Registerkarten können wir unseren POP-Zugriff definieren:

Der IMAP-Zugriff ermöglicht eine wesentlich vielfältigere Konfiguration:

Die Verwaltung anderer Mailclients (z.B. Outlook) erfolgt ähnlich.