



Sendmail

Greg Baker – greg.baker@ifost.org.au



Back

Close



Some sendmail History



Back

Close



What is sendmail?

- The main mail transfer agent on the internet
- First release called “sendmail” in 1983.
- Is the default mail service on most versions of Unix



Back

Close



Sendmail's good features

- handles high loads well
- is extremely configurable to handle legacy protocols



Back

Close



Sendmail's bad features

- had an administrator-unfriendly configuration file
- a history of security problems
- a lot of legacy influences





Sendmail versions

v8.9 anti-spam

v8.10 Mail filter API

v8.11 LDAP, SMTP authentication, transport security

v8.12 no longer SUID root



Back

Close



What version am I running?

- `telnet localhost 25`
- `echo '$Z' | /usr/sbin/sendmail -bt -d0`



Back

Close

Exercise

What version are you running?



8/102



Back

Close



On the wire protocols



Back

Close



Method 1: Message Injection Protocol

- Runs on port 587
- Can do authentication of the end user
- Message may get rewritten
- Documented in rfc2476
- Otherwise, same as Method 2
- New (v8.11) – rarely used.



Back

Close



Method 2: SMTP on port 25

- Greet with **HELO**
- Announce the sender with **MAIL FROM:**
- Say who should receive it with **RCPT TO:**
- Send email body after **DATA**
- Finish with **.**
- Terminate with **QUIT**





Odd things about SMTP

1. The `From:` field in the **DATA** doesn't have to match the **MAIL FROM**
2. Neither does `To:` have to match **RCPT TO**
3. None of the header fields need to exist.



Back

Close

Exercise

Talking SMTP manually...



13/102



Back

Close



How spooled e-mail gets delivered

- The mail server does a DNS lookup for MX records for the domain name
- It gets several names back, each with a priority number
- Try delivering to the smallest number
- If it fails, it tries the next lowest
- If everything fails, try again later.
- Warn after 4 hours. Give up after 4 days.



Back

Close

Exercise

Walking through the lookup process...



15/102



Back

Close



The configuration file



Back

Close



sendmail.cf

- Only read at startup/SIGHUP time
- **Solaris** /etc/mail/sendmail.cf
HP-UX /etc/mail/sendmail.cf
***BSD** /etc/mail/sendmail.cf
Linux /etc/sendmail.cf
- Some versions of Unix still “freeze” it to a sendmail.fc





Configuration file format

- 14 different options
- Blank lines
- Comments begin with “#”
- Lines beginning with tab carry on from the previous line.



Back

Close



Some easy things to change

DS A smart relay host

DM What domain to masquerade as

Dj My hostname

O SmtpGreetingMessage What banner to give on connection.



Back

Close

Exercise



20/102

Modifying the sendmail configuration file...



Back

Close



Rewriting Rules



Back

Close



What is a ruleset?

- A “subroutine” for rewriting an address
- Can get applied to a source address
- Can get applied to a destination address
- Can get called from other rulesets
- Order doesn’t matter
- Is defined by Sname and then lots of R . . . lines



Back

Close



What import rule sets are there?

canonify=3 All addresses

Parse=0 How to send?

1 Process sender address

2 Process recipient address

final=4 Postprocess all addresses

localaddr=5 Rewrite unaliased

check_relay, check_mail, check_rcpt, check_compat Is this sender allowed to go to this recipient through our machine?



Back

Close

Rewrites rule OK

1. Rleft hand side tokens `tab` replacements
2. Rleft hand side tokens `tab` \$: replacements
3. Rleft hand side tokens `tab` \$@ final result
4. Rleft hand side tokens `tab` \$# delivery mechanism, host and user





Things on the left hand side

\$ | Meta-separator

\$* Match zero or more tokens

\$+ Match one or more tokens

\$- Exactly one token

\$=x Match any phrase in class x

\$~x Match any word not in class x

\$@ Match nothing



Back

Close



Things on the right hand side

$\$n$ The n th thing that was matched on the left

$\$[name\$]$ Canonicalize *name*

$\$(map\ key\ \$@arguments\ \$:default\ \$)$ Find *key* in *map*, otherwise *default*

$\$>n$ Call ruleset n with the rest of the line

Letters, symbols, numbers, $\$$ | Just substitute it



Back

Close



More things on the right hand side

Extra TAB Everything following is a comment

\$#mechanism \$@ host \$: user Only in rule-set 0 or check_rcpt or similar

\$#error \$@ number \$: error string Die with the error given (including SMTP error code number)



Back

Close

Example Ruleset



28/102

Sappend_domainname

```
R$@ tab $#error $@ 5.7.1 $: "550 Arrgl
```

```
R$* @ $* tab $@ $1 @ $2
```

```
R$* tab $: $1 @ ifost.org.au
```



Back

Close

How to test

sendmail -bt

```
ADDRESS TEST MODE (ruleset 3 NOT automatically invoked)
Enter <ruleset> <address>
> append_domainname gregb
append_domainnam input:  gregb
append_domainnam returns:  gregb @ ifost .  org .  au
```



29/102



Back

Close

Exercises

Making your own rewrites...



30/102



Back

Close



31/102

Classes and Maps



Back

Close



Class definitions

- CM
- Cw localhost loghost
- FR-o /etc/mail/relay-domains



Back

Close



Some examples

From Canonify2=96:

```
R$* < @ $=M > $* tab $: $1 < @ $2 . > $3
```

From Relay_ok

```
R$=R $* tab $@ RELAY tab relayable IP address
```



Back

Close



Other class tricks

- `FL/etc/passwd %[^ :]`
- `Fg | /some/program`



Back

Close

Exercise

Playing with classes...



35/102



Back

Close



Problems with classes

- Only read at *sendmail* startup time
- Can only copy unchanged to the the right hand side
- A little inflexible



Back

Close



What is a map?

A lookup from something to something else:

- a username → GECOS field
- Query DNS, NIS/NIS+ or LDAP
- Find an entry in a flat file or indexed file
- A regular expression
- Run a program with an argument



Back

Close



How do I use a hash map?

1. Create a text file `myfile`
2. Make a hash from it `/etc/stuff`
3. Put `Kmyhash /etc/stuff` in `sendmail.cf`
4. Make a rule `R$* tab $(myhash $1 $)`



Back

Close

Exercise

Making and using simple hash maps...



39/102



Back

Close



Common special flags

- ax** append *x* for successful matches
- Tx** append *x* for temporary failures
- o** Optional
- h,-b** LDAP server hostname / basename



Back

Close



Classy maps

- `F{VirtHosts}@ldap:-k (&(objectClass=virtHosts)-v host`
- `F{MyClass}foo@hash:/etc/mail/classes`



Back

Close



Delivery Mechanisms



Back

Close

M sent me

```
Mprocmail, Path=/usr/local/bin/procmail,  
Flags=mSDFMhun, S=11, R=21, Argv=procmail  
-m $h $g $u
```



43/102



Back

Close



Flags

- Expand aliases?
- Hidden dot method?
- “/” means file or X500?
- Email addresses with comments?



Back

Close



Special mailers

local Delivery locally

error Refuse to send

discard Silently drop the message

prog Deliver via program

file Deliver to a file

smtp/esmtp/smtp8/esmtp8 TCP protocols

relay Forward to something else

procmail Delivery via `procmail`



Back

Close



Message flow Part 1

- Recipient address tidied by ruleset 3
- Remember this tidy result
- Which mailer to use from ruleset 0
- ...



Back

Close



Message flow Part 2

- Send the tidy address through 2
- Send the result through the delivery agent's
R= ruleset
- Ruleset 4



Back

Close



Message Flow Part 3

Take the *sender* address through rulesets:

- 3
- 1
- The delivery agent's $S =$ ruleset
- 4



Back

Close



Message Flow Part 4

Check flags (F=) on mailer:

- A flag? Check recipient `/etc/mail/aliases`.
- 5 flag and alias didn't work? Try ruleset 5
- w flag? Try recipient `.forward` file

Run the mailer!



Back

Close



About aliases

- Normally in `/etc/mail/aliases.db`
- In DBM format (usually)
- Created by running `newaliases` manually
- `newaliases` reads from `/etc/mail/aliases`
- Should redirect *postmaster* and any system accounts.



Exercises

Confusing users terribly...



51/102



Back

Close



Oddities



Back

Close



Forwarding

- ForwardPath
- Normally just `$z/.forward`
- Consider `/var/mail/forwards/$z`
- Checks for stale NFS



Back

Close



Non-standard delivery

`/etc/mail/aliases` and `.forward` can contain:

- `\user`
- `|program`
- `/some/file`
- `:include:/some/file`
- Local addresses
- Remote addresses



Back

Close



Fun ideas

- `ForwardPath=$z/.forward.$w`
- `ForwardPath=$z/.forward.$s`
- `somealias+extra: |program`
- `somealias+*: /else/where2`
- `owner-list: root`



Back

Close



Vacation

- Program for auto-responding to emails
- Run from `.forward`
- Looks for a file (with headers) called `.vacation`
- Will reply only once per address per week
- Keeps track in `.vacation.db`



Back

Close

Exercises

Mailing lists and missing users



57/102



Back

Close



Header rewriting



Back

Close



Why modify headers?

- Because RFC822 demands it
- To include disclaimers
- To flag possible spam
- To reject messages



Back

Close



A simple header addition

```
Hx-Our-Extra-Stuff:  Flumph gloop
```

```
Hx-Long-Stuff:     Garble warble
```

```
tab farble
```



Back

Close

Exercise

Add in your own header...



61/102



Back

Close



Headers and macros

- HX-Size: `#{msg_size}`
- HX-Received-Using: `$?rProto r .`



Back

Close



Conditional headers

- `H?x?Full-Name: $x`
- Is `x` in the *flags* of the mailer handling this message?



Back

Close

Exercise

Flags and headers



64/102



Back

Close

Complaining about headers

```
HMessage-Id:    $>CheckMsgId
```

```
...
```

```
SCheckMsgId
```

```
R< $+ @ $+ > tab $@ OK
```

```
R$* tab $#error $: 553 Header Err
```



Exercise

Enabling simple censorship...



66/102



Back

Close



67/102

Simplifying everything



Back

Close



Don't edit `sendmail.cf`!

- Find your `.mc` files
- Change it
- Rerun `m4`
- Restart/HUP *sendmail*



Back

Close



69/102

A simple .mc file

```
VERSIONID('Client -- sends mail elsewhere')
```

```
OSTYPE(openbsd)
```

```
FEATURE('nullclient', 'mailhub.ifost.org')
```



Back

Close

Exercise

Autogenerating .cf files ...



70/102



Back

Close



Things in a .mc file

VERSIONID Turns into a comment in sendmail

OSTYPE Where files are found

FEATURE Turn on something

define Set a configuration option

dn1 Delete to end of newline (comment)

MASQUERADE_AS



Back

Close



VERSIONID

- Usually `$RCS: rcs id$`
- Can be anything
- Becomes a comment
- Keep in quotes ‘ and ’



Back

Close



OSTYPE

- Essential
- Defines where files go
- Not all operating systems defined
- Look in `ostype` for complete list





Famous FEATURES

use_cw_file Read an `/etc/mail/local-host-`

redirect Control users who have moved

virtusertable Handle virtual domains

local_procmail Use `procmail` as a local
mailer

dnsbl Stop known spammers



Back

Close

MASQUERADING

- MASQUERADE_AS('company.com')
- MASQUERADE_DOMAIN('oldcompanyname.com')
- MASQUERADE_DOMAIN_FILE('filename')



75/102



Back

Close



A better example

```
VERSIONID('A genuine configuration')  
OSTYPE(openbsd)  
FEATURE(nouucp, 'reject')  
FEATURE(virtusertable)  
FEATURE('masquerade_envelope')  
MAILER(local)  
MAILER(smtp)  
MASQUERADE_AS('ifost.org.au')
```



Back

Close

Exercise

Real-life .mc files



77/102



Back

Close



Tweaking Rulesets

- Rulesets 0 - 5 call “local” rulesets
- “Local” rulesets can be modified
- Use the name of the main ruleset



Back

Close

LOCAL_CONFIG

- Introducing other classes or maps ...



79/102



Back

Close

Exercise

A sense of déjà vu...



80/102



Back

Close



Configuration Options

confPRIVACY_FLAGS Allow EXPN, VRFY?

confSMTP_LOGIN_MSG Option SmtplGreeting

confMIN_FREE_BLOCKS Full filesystem
– stop receiving mail!

confMAX_MESSAGE_SIZE Defaults to in-
finite

confMATCH_GECOS From /etc/passwd



Back

Close

MAILERS

You probably want:

- MAILER(local)
- MAILER(smtp)



Back

Close

DOMAINS

- For big sites only
- Centralises names for relay servers
- Not necessary at all





Reducing SPAM



Back

Close

Statistics for my servers

1078	Total rejected messages
147	HELO failures
269	Non-existent domains
469	Common invalid mailboxes
190	Other non-existent names
2	Yahoo oddity
1	Misconfiguration



85/102



Back

Close



What sendmail does automatically

- Reject unresolvable domains
- Reject unqualified names (user, but no domain)
- Reject invalid HELOs



Back

Close



Blacklists

- A DNS domain
- Keeps track of IP addresses that send SPAM
- Many organisations maintain blacklists



Back

Close



Using a blacklist manually

- You get a connect from IP address A . B . C . D
- Look up the A record for D . C . B . A . *relays.ordb.c*
- If you get a response – it's a SPAM domain, see TXT record for the reason
- If you don't get a response, it's not a known spammer



Back

Close

Very quick blacklist exercise

Slightly contrived, but helpful



89/102



Back

Close



Lists I use / have used

Subdomain

Purpose

relays.ordb.org

Open relay servers

opm.blitzed.org

Open proxies

lists.dsbl.org

Unsecure servers

spl.spamhaus.org

Known spammers

cbl.abuseat.org

Worms, trojans, etc.



Back

Close



Configuring

- `FEATURE('dnsbl')`
- `FEATURE('dnsbl','relays.ordb.org')`
- `FEATURE('dnsbl','opm.blitzed.org', "451
Temporarily rejected from proxy list")`



Back

Close

More information

The whole scoop from `cf/README`



92/102



Back

Close

Anti-spam exercises

Using a blacklist



93/102



Back

Close



Integration with other services



Back

Close



IMAP, POP – Plan 1

- *sendmail* delivers into `/var/mail` files or equivalent
- POP/IMAP server needs to read from there
- Both WU-IMAP and Dovecot can do this
- Run `imapd` and/or `pop3d` from `inetd`



Back

Close



Plan 1 problems

- `imapd` has to re-read and re-write the user's whole mail file.
- No support for folders
- Still OK for `pop3d` though.



Back

Close

IMAP, POP – Plan 2

- Deliver via `procmail` into a `maildir`
- Use `courier-imap` and `courier-pop3d`



97/102



Back

Close



Web-based mail

- IMP or many alternatives.
- Talks to IMAP server



Back

Close

Exercises

Just a quick demonstration of integration...



99/102



Back

Close



Milters



Back

Close



What is a milter?

- A filter for mail
- Every message gets sent through all milters
- Can do virus or spam checks
- Connected to *sendmail* via sockets



Back

Close



How to use milters

- `InputMailFilters` gives order
- X configuration line



Back

Close