Electric Mail & Postfix

Yung-Zen Lai (yzlai@hotmail.com)
2004/08
Agenda

• Electric Mail Systems
  – Message Flow
    • MUA, MTA, MDA, (MSA, MAA)
  – Mail Addressing & DNS
  – Mail Header
  – Mail aliases, forwarding
  – Mailing list
  – MailBox, MailDir
  – Talking with MTA
Agenda (cont.)

- Postfix
  - Installation
  - Basic Configuration
  - Running Postfix
  - How It Works
  - Advanced Postfix
    - Virtual Domain/ Account
    - Mail Relay/ Transport
    - SMTPD Restrictions
    - Header/ Body Checks
    - Foreign Lookup Tables
    - Content Filtering
    - SASL Authentication
Part I: Electric Mail Systems

- Message Flow
  - MUA, MTA, MDA, (MSA, MAA)
- Mail Addressing & DNS
- Mail Header
- Mail aliases, forwarding
- Mailing list
- MailBox, MailDir
- Talking with MTA
Message Flow

UA: User Agent
TA: Transfer Agent
DA: Deliver Agent
SA: Submission Agent
AA: Access Agent
Related RFCs

- RFC 2821: Simple Mail Transfer Protocol
  - Reliable and Efficient
- RFC 2822: Internet Message Format
- RFC 1869: SMTP Service Extensions (ESMTP)
- RFC 1891: ESMTP for Delivery Status Notifications
- RFC 1894: An Extensible Message Format for DSNs
- RFC 2045: MIME Part I: Format of Internet Message Bodies
  - Multipurpose Internet Mail Extensions
- RFC 2476: Message Submission
- RFC 2554: ESMTP for Authentication
  - SASL: Simple Authentication and Security Layer
Mail Systems Agents

- **MUA**: Mail User Agent
  - Read and compose mail
  - mail, mutt, pine, elm, Outlook Express, Eudora, …, etc.

- **MTA**: Mail Transport Agent
  - Route messages among machines
  - SMTP (RFC 2821), ESMTP (RFCs 1869, 1870, …)
  - sendmail, qmail, postfix, smail, …, etc.

- **MDA**: Mail Delivery Agent
  - Place messages in a local message storage
  - /bin/mail, /bin/sh, mail.local, smrsh, procmail, …, etc.
  - To a person, a mailing list, a file or a program
Mail Systems Agents (cont.)

- MAA: Mail Access Agent (optional)
  - Connects the user agents to the message store
  - IMAP (Internet Message Access Protocol) or POP (Post Office Protocol)

- MSA: Mail Submission Agent
  - Split the mail submission agent from the MTA
  - Spread out the workload and maximize performance
Mail Addressing & DNS

• Route-based
  – UUCP address
    • mcvax!uunet!ucbvax!hao!boulder!lair!evi
    • evi@lair

• Location-independent
  – Internet Address
  – General form of Internet mail address
    • <user>@<host>
    • yzlai@hotmail.com
Mail Addressing & DNS (cont.)

• Mixed address
  – lair@evi@boulder.colorado.edu

• Route-based form of Internet address
  – <@ site1,@ site2,…,@ siteN:user@final-site>

• ARPANET
  – <user>%<host1>%<host2>@<host3>
  – <user>@<host1>
Mail Addressing & DNS (cont.)

- Domain Name Service
  - Mail eXchange Record (MX Record)
  - tp.edu.tw IN MX 0 smtp.tp.edu.tw.
  - Preference number
    - Lower value/ Higher Priority
  - Must be a host name, not IP Address
  - Must have valid A Record(s)
  - Can NOT be CNAME Record(s)
Mail Header

- Mail = Header + body
- Hidden by user agents
- We can add anything to mail header
- By convention, start with “X-”

```
Received: from 163.21.249.175
    by ms3.tp.edu.tw with Mail2000 ESMTP Server
V2.71N(254:0:AUTH_NONE)
    Fri, 06 Aug 2004 21:39:08 +0800 (CST);
    (envelope-from <epaper@games.epost.hinet.net>)
Return-Path: <epaper@games.epost.hinet.net>
Received: from sender.epost.hinet.net(enews.hinet.net[202.39.225.54])
    by smtp.tp.edu.tw (Postfix) with ESMTP
    id 5478F22CD57; Fri, 6 Aug 2004 21:39:04 +0800 (CST)
Message-ID: <10000519.842.ep-21@games.epost.hinet.net >
From: “HiNet 遊戲網” <epaper@games.epost.hinet.net>
To: “測試收件者” <netadm@tp.edu.tw>
Subject: HiNet遊戲網電子報20040807
Date: Fri, 6 Aug 2004 21:38:49 +0800 (CST)
X-Mailer: Microsoft Outlook Express 5.50.4522.1200
```
Mail aliases, forwarding

- **Mail aliases**
  - 1. In a user agent’s configuration file
    - .muttrc
  - 2. In system-wide aliases
    - /etc/aliases, NIS map
      - admin: jdtsai, yzlai
      - help: :include:/ etc/ help-bounce
      - nobody: “/ dev/ null”
      - nhelp: "| / bin/ mail2news tp. help"
  - 3. In a user’s forwarding
    - ~/.forward

- The order to lookup
  - 1 Ë 2 Ë 3
Mailing list

- Conventions in the aliases file:
  - mylist: :include: / etc/ mail/ include/ mylist
  - mylist-request: “| mailing-list-program”
- Majordomo: http://www.greatcircle.com
- GNU Mailman: http://www.list.org
- ListProc: http://www.cren.net
- LISTSERV: http://www.lsoft.com
MailBox, MailDir

- MailBox (mbox)
  - All messages store in a single file for each user
    - Usually Spool Directory: /var/mail or /var/spool/mail

- MailDir
  - Using Directory Structure to store messages.
    - Avoid file locking and improve reliability
    - Usually have three sub-directory (tmp/, new/, cur/) under user’s home directory
Talking with MTA

telnet smtp.tp.edu.tw 25
220 smtp.tp.edu.tw ESMTP TpEduNet(1) Official MX
EHLO smtp.ntnu.edu.tw
250-smtp.tp.edu.tw
250-PIPELINING
250-SIZE 50000000
250-ETRN
250 8BITMIME
MAIL FROM: <yzlai@hotmail.com>
250 Ok
RCPT TO: <netadm@tp.edu.tw>
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Mail Headers
<space line>
Mail Body
.
250 Ok: queued as 505D322987C
QUIT
221 Bye
SMTP Reply Codes

- 1yz
  - Positive Preliminary reply

- 2yz
  - Positive Completion reply

- 3yz
  - Positive Intermediate reply

- 4yz
  - Transient Negative Completion reply

- 5yz
  - Permanent Negative Completion reply
Part II: Postfix

• Installation
• Basic Configuration
• Running Postfix
• How It Works
• Advanced Postfix
  – Virtual Domain/ Account
  – Mail Relay/ Transport
  – SMTPD Restrictions
  – Header/ Body Checks
  – Foreign Lookup Tables
  – Content Filtering
  – SASL Authentication
Introduction to Postfix

- To be fast, easy to administer and secure
- Build from over a dozen litter programs
  - Each perform only one specific task
- [http://www.postfix.org](http://www.postfix.org)
  - Postfix 2.1.4 (Postfix 2.1 Patchlevel 4)


Installation

• From FreeBSD ports
  – mail/ postfix
    • make install

• From tarball
  – Download from [http://www.postfix.org/download.html](http://www.postfix.org/download.html)
  – make; make install

• Post-install on FreeBSD
  – Edit /etc/rc.conf: sendmail_enable="NONE"
  – Edit /etc/periodic.conf

• Post-install on Linux
  – Stop Original Mail Service (usually sendmail)
## Basic Configuration Files

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>main.cf</td>
<td>Main configuration file. Hundreds parameters with sensible default values</td>
</tr>
<tr>
<td>master.cf</td>
<td>How a mailer component program should be run</td>
</tr>
<tr>
<td>access</td>
<td>The same as /etc/mail/access (for access control)</td>
</tr>
<tr>
<td>aliases</td>
<td>The same as /etc/mail/aliases</td>
</tr>
<tr>
<td>canonical</td>
<td>(recursive) address mapping/rewriting table</td>
</tr>
<tr>
<td>header_checks</td>
<td>Access list of mail headers</td>
</tr>
<tr>
<td>mynetworks</td>
<td>SMTP client lists</td>
</tr>
<tr>
<td>transport</td>
<td>Email addresses to message delivery transports and/or relay hosts mappings</td>
</tr>
<tr>
<td>virtual</td>
<td>Address aliases for arbitrary local or non-local recipient</td>
</tr>
<tr>
<td>relay_domains</td>
<td>Who treat this host as their MX (Mail eXchange)</td>
</tr>
</tbody>
</table>
main.cf

- parameter = value
- other_parameter = $parameter
- My own hostname
  myhostname
- My own domain name
  mydomain
- What domain name to use in outbound mail
  myorigin = $myhostname ( "user@myhostname" )
  myorigin = $mydomain ( "user@mydomain" )
main.cf (cont.)

- What domain to receive mail for
  mydestination
- What clients to relay mail from
  mynetwork_style
  mynetworks
- What destination to relay mail to
  relay_domains
- What delivery method: direct or indirect
  relayhost
main.cf (cont.)

- All main.cf parameters can be found
  - [http://www.postfix.org/postconf.5.html](http://www.postfix.org/postconf.5.html)
  - `postconf`

- What you need to know about Postfix logging
  - `/etc/syslog.conf`
    - mail.err / dev/ console
    - mail.debug / some/ log/ file
    - egrep 'reject| warning| error| fatal| panic):' / some/ log/ file
Running Postfix

- **postfix**
  - start
  - stop
  - reload (Re-read configuration files/ Re-run postfix after minor upgrade)
  - flush (Attempt to deliver every message in the deferred mail queue)
  - check

- **postqueue**
  - -p (same as `mailq`)
  - -f (same as `postfix flush`)
  - -s <site>

- **postsuper**
  - -d
  - -h
  - -H
How Postfix receives mail

Local

sendmail → postdrop

postdrop

postdrop

pickup

cleanup

Network

smtpd → trivial-rewrite

incoming

How Postfix delivers mail

- Active
- Deferred
- Hold
- Qmgr
- Trivial-rewrite
- Smtplib
- Lsmtp
- Local
- Virtual
- Pipe

Network, File, Command
Virtual Domain/ Account

- shared/ separate domains
- system/ virtual account
- shared domain with system account
  
  \[
  \text{mydestination} = $\text{myhostname}, \ a.edu.tw, \ b.edu.tw
  \]

- separate domain with system account

  \[
  \text{virtual\_alias\_domains} = a.edu.tw, \ b.edu.tw
  \]

  \[
  \text{virtual\_alias\_maps} = \text{hash:/ some/ dir/ virtual\_alias}
  \]

  \[
  \begin{align*}
  \text{qoo@a.edu.tw} & \quad qoo.a@localhost \\
  \text{test@b.edu.tw} & \quad \text{test@some.where.on.earch}
  \end{align*}
  \]
Virtual Domain/ Account (cont.)

• separate domain with virtual account
  – Cons
    • Nologin
    • Need POP/IMAP server with virtual account support
  – Pros
    • No UID limit
    • Ease to management

virtual_mailbox_domains = a.edu.tw, b.edu.tw
virtual_mailbox_base = /var/vmail
virtual_mailbox_maps = hash:/some/dir/virtual
  qoo@a.edu.tw a/qoo
  test@b.edu.tw b/test
Mail Relay

- relay_domains
  163.21.0.0/16, /some/dir/relay_domains

- relay_recipients
  hash:/some/dir/relay_recipients
  qoo@a.edu.tw any_value
  test@b.edu.tw any_value
  @c.edu.tw catchall.c@localhost
Transport

- Change the default message delivery transport
- transport_maps = hash:/some/dir/transport
  
  host/domain transport:nexthop
  
  tp.edu.tw smtp:mail.tp.edu.tw
  slhs.tp.edu.tw smtp:[ms.slhs.tp.edu.tw]
  cc.ntnu.edu.tw smtp:[cc.ntnu.edu.tw]:10025
  .mailserver.idv.tw devnull:
  zdl.net devnull:

- master.cf
  devnull unix - n n - - pipe
  user=nobody argv=/bin/cat /dev/null
SMTPD Restrictions

- `smtpd_client_restrictions`
  - Usually check IP/host/domain
- `smtpd_helo_restrictions`
- `smtpd_sender_restrictions`
  - MAIL FROM
- `smtpd_recipient_restrictions`
  - RCPT TO
- `smtpd_data_restrictions`
SMTPD Restrictions (cont.)

- smtpd_client_restrictions
  - reject_unknown_client
  - reject_rbl_client
  - reject_unknown_client
  - reject_non_fqdn_hostname
  - check_client_access type:mapname
  - permit_mynetworks
SMTPD Restrictions (cont.)

- **smtpd_helo_restrictions**
  - check_helo_access type: mapname

- **smtpd_sender_restrictions**
  - reject_non fqdn_sender
  - reject_unknown_sender_domain
  - check_sender_mx_access type: mapname
  - check_sender_access type: mapname

- **smtpd_recipient_restrictions**
  - reject_unknown_recipient_domain
  - check_recipient_access type: mapname
SMTPD Restrictions (cont.)

- Actions in check_xxxxxx_access
  - Permit, OK
  - Reject [optional text]
  - [45]yz text
  - Hold [optional text]
  - Discard [optional text]
  - Filter transport:destination
Header/ Body Checks

- header_checks = regexp:/some/dir/header Checks
  / match pattern/ ACTION
- body_checks = regexp:/some/dir/body Checks
- Actions
  - Ignore (*)
  - Permit, OK
  - Reject [optional text]
  - [45]yz text
  - Hold [optional text]
  - Discard [optional text]
  - Filter transport:destination
Header/ Body Checks (cont.)

/ ^From: [a-z][0-9]{7,}@yahoo.com/ Reject Illegal mail header.
/ ^From: [a-z][0-9]{7,}@hotmail.com/ Reject Illegal mail header.
/ ^To: .*\.txt/ Reject Illegal mail header.
/ ^Received: from tp.edu.tw/ Reject Illegal mail header.
/ ^From: .*\<[a-zA-Z0-9]*@msa.hinet.net\>/> Reject User unknown.
/ ^From: .*\<.+\..+@ms[a-zA-Z0-9]+.hinet.net\>/> Reject User unknown.
/ ^X--Mailer: ([0-9A-Za-z]{15,})/ Reject Mailer $1 is unacceptable.
/ ^X--Library: Dynamailer/ Reject Dynamailer is unacceptable.
/ ^X--Library: Indy/ Reject Indy is unacceptable.
/ ^Content-Disposition: Multipart message/ Reject mail MAY contain the SirCam virus.
/ ^Subject: new photos from my party!/ Reject mail MAY contain the MyParty virus.
/ ^Subject: Re: Your password!$/ Reject mail MAY contain the Frethem virus.
/ ^Message-ID: <[a-zA-Z]{19}\>@/ Reject mail MAY contain the Bagle virus.
Foreign Lookup Tables

- Postfix Supports Berkeley DB, MySQL, LDAP, and PostgreSQL as his foreign tables.
- Virtual account/ Large dynamic data, IP,…

- `smtpd_client_restrictions = check_client_access mysql:/some/dir/check_client.cf`
SELECT action FROM check_client_access_table
WHERE client_ip = '10.1.2.3' AND status = 'abcd'

/ some/ dir/ check_client.cf
host = 192.168.169.170
user = netadm
password = Godknows
dbname = for_postfix_20040816_introduce
table = check_client_access_table
select_field = action
where_field = client_ip
additional_conditions = and status = 'abcd'
Content Filtering

- Usually for Virus/Spam Scanning
  - External-program filtering
Content Filtering (cont.)

- Daemon-based filtering
  - more efficient
Content Filtering (cont.)

- **main.cf**
  
  ```
  content-filter = smtp-filter:[127.0.0.1]:10024
  ```

- **master.cf**
  
  ```
  smtp-filter   unix    -   n   -   10    smtp
  -o myhostname=localhost
  localhost:10025   inet    n   -   n   -   10    smtpd
  -o content_filter=
  -o mynetworks=127.0.0.0/ 8
  -o smtpd_client_restrictions=permit_mynetworks, reject
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=
  -o header_checks=
  ```
Content Filtering (cont.)

- **Anti-Virus**
  - AMaViS / AMaViSd
    - McAfee VirusScan
    - Sophos Anti-Virus
    - Trend InterScan
    - Sophie + SAVI
  - Central Command Vexira MailArmor
  - Avpcheck
- **Spam-Detection**
  - SpamAssassin
- **Amavisd-new + Razor + Spamassassin**
SASL Authentication

- Simple Authentication and Security Layer
- Cyrus SASL
SASL Authentication (cont.)

telnet smtp.tp.edu.tw 25
220 smtp.tp.edu.tw ESMTP TpEduNet(1) Official MX
EHLO smtp.ntnu.edu.tw
250-smtp.tp.edu.tw
250-PIPELINING
250-SIZE 50000000
250-ETRN
250-AUTH DIGEST-MD 5 PLAIN CRAM-MD 5
250 8BITMIME
AUTH PLAIN dGVzdAB0ZXN0AHRlc3RwYXNz
235 Authentication successful
MAIL FROM: <yzlai@hotmail.com>
SASL Authentication (cont.)

- **main.cf**
  
  ```
  smtpd_sasl_auth_enable = yes
  smtpd_recipient_restrictions =
      permit_sasl_authenticated
  smtpd_sasl_security_options =
      noplaintext, noactive, nodictionary, noanonymous
  ```

- **smtpd.conf (sasl)**
  
  ```
  pwcheck_method:
      saslauthd (unix password)
      auxprop (sasl dedicate password, `man saslpasswd2`)
  ```
The End

Thank you!