

Mail

Presented by: Nick Nelson

Introduction

- Hello, My name is Nick Nelson
- In this course, we will cover both the history of exim, how internet mail works, how cPanel integrates Exim, as well as advanced topics such a Exim Routers, Transports, and ACLs, as well as the differences of each.

Introduction of Exim

- Exim was written by Philip Hazel at the University of Cambridge in 1995.
- Written using the basic philosophy of Smail
- The name was derived from “Experimental Internet Mailer” as the outcome of the project at start was unknown.
- Exim is Open Source and distributed under the GNU General Public License (GPL)

How Internet Mail Works

- Exim is a **Mail Transfer Agent (MTA)**
- The program people most often use to send/receive mail are referred to as **Mail User Agents (MUAs)**. They exist to provide convenient mail interfaces for users. Examples are Outlook, Thunderbird, iMail, etc.
- The **MUA** simply sends the mail to the **MTA** which then transports the mail from host to host until it's delivered to a mailbox and retrieved using an **MTA**.

How Internet Mail Works

- Messages sent from one host to another use the Simple Mail Transfer Protocol (SMTP).
- SMTP listens on TCP port 25. Because of this, Exim must be run as a privileged program.
- Port 465 is reserved for SMTP over SSL. However, Exim employs Transport Layer Security (TLS) in order to not need a separate port for secure communications.

How Internet Mail Works

- RFC 2822 mandates the message format.
- A message consists of a header and a body. The header contains a number of lines as defined by RFC 2822.
- Headers are terminated with a blank white line.
- RFC 2822 allows many variations for addresses, such as :
To: example@example.com
John Doe <example@example.com>
example@example.com (John Doe)
- Text in Parenthese anywhere in the line are always comments.

How Internet Mail Works

- Many header lines are added by the MTA. In addition to the header and the body, the envelope is transmitted immediately prior to the headers using SMTP commands MAIL and RCPT.
- Envelope contains sender address and at least one recipient address. Always in form of <user@domain>
- Delivery is based completely on the envelope, not the To: or Cc: lines.
- Any message failures are always sent to the envelope from address, not the From: or Reply-to: address.

How Internet Mail Works

- Additional header lines are also added by the MUA and MTA.
- Before transmitting message, Date: and Message-ID: line always added by the MUA. Many other headers can also be added by MUA and MTA.
- SpamAssassin on cPanel servers add headers which are prefixed with X-Spam. Other headers can be added based on the Exim configuration.

How Internet Mail Works

- SMTP is a Simple command-reply protocol. Client host sends command and awaits a reply.
- All text is intended to be easily interpreted by humans.

- **SMTP Response Codes:**

2xx – The command was successful

3xx – Additional data required

4xx – Command suffered temporary error

5xx – Command suffered a permanent error

Exim only acts upon first number of code. The last line of text will omit the hyphen (-). All other lines include Hyphen. Such as:

550 – Host is not on relay list

550 – Message was not delivered

550 Relaying prohibited by administrator

How Internet Mail Works

- When an MUA connects to a MTA it must first await an initial success response such as:

220 ESMTP Ready

- Afterwards, you initialize the session by sending an EHLO command (Extended Hello) with the hostname, such as:

EHLO mail.example.com

- After the EHLO command is accepted, the client attempts to send mail. Each message is begun by a MAIL command.

MAIL FROM: <nick@example.com>

- Afterwards the destination is issued using the command:

RCPT TO: <mypal@invalid.com>

How Internet Mail Works

- After all recipients are transmitted, and at least one recipient is accepted, the client should send a DATA command and await a 354 response requesting further data (the message)
- Once the client has sent its whole message it ends the SMTP session with the QUIT command.
- You should remember that forging headers is very trivial as most mail hosts act as strangers to each other. Therefore, you should only look at the top Received: line to determine the IP that sent the email, any other Received: lines can be inserted by the MUA (often used for abuse purposes by spammers).

Exim Overview

- On cPanel servers, both `/usr/lib/sendmail` and `/usr/sbin/sendmail` are symlinks to the Exim binary.
- Most exim processes act separately and are short lived. The exception to this is:
 - 1) Process to listen on SMTP port for incoming TCP/IP connections
 - 2) Process to start up queue runner processes.
- Exim configuration file is stored at `/etc/exim.conf` on cPanel servers. However, all modifications to the `exim.conf` should be made through the Advanced Exim Configuration Editor in WHM.

How Exim Delivers Mail...

- Exim delivers mail using drivers. There are three types of drivers, we'll focus first on routers and transports.
- The first router used by most `exim.conf` files (cPanel has a few misc. routers before this one for optimization purposes) is the `dnslookup` router.
- This router simply looks up the MX record for a domain. If the domain is in the `/etc/localdomains` file, exim is configured to skip this router.
- After this, cPanel uses “accept” routers, accept routers often have preconditions and simply accept ALL mail passed to it (mail goes through the preconditions first)

How Exim Delivers Mail...

- “accept” routers are used first as to accept any mail matching certain conditions prior to any filtering.
- After the “accept” router, mail is passed through a “redirect” router which is used to redirect mail based on user and system filters.
- Most routers have preconditions, once the precondition is met, the router often routes the mail to a suitable transport.
- For instance, when a dnslookup router is successful, it passes the message on to the remote_smtp transport to be delivered.
- Other transports include “pipe”, “appendfile”, and “smtp”

Exim Queue

- Every message handled by Exim is issued a unique Message-ID.
- The ID is 16 characters and separated into 3 parts by hyphens. Each part is actually a number, encoded in base 62.
- The first part is the unix time the message started to be received. The second part is the PID of the process that received it. The third part is used to distinguish between processes received by the same process at the very same moment.

Exim Queue

- The exim queue on cPanel servers is stored at /var/spool/exim/input
- On cPanel servers, we opt to split the queue into 62 subdirectories. ([a-z], [A-Z], and [0-9]). This causes all messages to be distributed to the separate subdirectories based on the 6th character in the message ID.
- This requires Exim to do more work when scanning the queue, but vastly improves the disk writing performance.
- You can manage the Exim queue from command line very easily.

Exim Queue

- To list the contents of the queue, you would simply use the command:
`exim -bp`
- To only give you the number of emails in the spool you simply add a 'c' to the end of the command:
`exim -bpc`
- You can examine the contents of a message in queue using the '`exim -Mvl`' command followed by the Message ID
- More frequently though, you will use the `eximstats` daemon to monitor your exim queue.

Eximstats

- Eximstats is a perl script which parses logs and creates a mysql database with many different statistics about Exim.
- Most of this information can be accessed through WHM using the “View Mail Statistics” option.
- To restart eximstats you would use /
scripts/restartsrv_eximstats

Troubleshooting Exim via Command Line

- There are many troubleshooting techniques you can use on the command line for Exim.
- To test how Exim would route a message you simply use the 'exim -bt' command, for instance:

```
exim -bt nick@example.com
```

- This will tell you which routers Exim would use to deliver a message to this address.

Exim Log Files

- There are three log files available for you to monitor the activities of Exim.
 - The main exim log file (`exim_mainlog`) records the arrival of each message as well as the delivery in a single logical line.
 - The reject log file (`exim_rejectlog`) records information about messages and addresses that are rejected based on policy.
 - The exim panic log (`exim_paniclog`) is only used when Exim suffers a disastrous error. (most often related to syntax errors in the log files)

Exim Configuration Editor

- The exim configuration editor should be used through WHM for modifying any aspect of the exim.conf
- This editor also allows you some simple configuration options such as:
 - Always set the Sender: header when the sender is changed from the actual sender. (Unchecking this will stop "On behalf of" data in Microsoft(R) Outlook, but may limit your ability to track abuse of the mail system.)
 - Verify the existance of email senders.
 - Use callouts to verify the existance of email senders.
 - Discard emails for users who have exceeded their quota instead of keeping them in the queue.

Maildir vs. Mbox

- The best advantage of Maildir over other mailbox formats is maildir does not require locks as it's all separate files.
- All mail is written to a tmp directory first, and then written to the 'new' directory.
- Once the MUA finds mail in the 'new' directory, it will move it to the 'cur' directory.
- All cPanel servers now come default using Maildir instead of mbox. However, for any old systems which have not yet been converted to maildir, you can simply use the script:

```
/scripts/convert2maildir
```

- Maildir is especially beneficial for servers that pass large volumes of mail.

Maildir vs. Mbox

<http://www.courier-mta.org/mbox-vs-maildir/>

Questions?