Giải thích log của lệnh sendmail

Published: Sat, 02 Nov 2019 23:04:22 | Last modified: Sat, 02 Nov 2019 23:04:22

MỤC LỤC

Bài này sẽ dịch lại một phần của trang: **http://sendmail.org/~ca/email/doc8.12/op-sh-2.html** Về nội dung liên quan đến `format` log của `sendmail` cũng ý nghĩa của từng trường.

0. Sendmail là gì

- Một phần mềm chạy trên hệ thống `Linux` (hoặc là *Nix).
- Có nhiệm vụ gửi `mail` - ta nên dùng từ `phân phối` (delivery) thì sẽ chuẩn xác hơn.
- Gửi mail (hay phân phối mail) nói đơn giản là sử dụng kết nối mạng (có thể là `internet` hoặc không) thực hiện gửi nội dung `có định dạng` bằng giao thức như SMTP,... đến máy chứa tài khoản người nhận.
- Nội dung mail sẽ được máy chủ phía nhận phân phối đến đúng user ta đã gửi.
- Nó chẳng khác gì một ứng dụng mạng bằng `Socket` mà nhiều người vẫn học.
- Nó chỉ khác là có các giao thức cụ thể để gửi dữ liệu (là các mail) đi thôi.
- Thường sẽ có 2 hình thức: `Gửi trực tiếp` và `Gửi gián tiếp`.
- `Gửi trực tiếp` : Gửi mail từ máy đang chạy phần mềm `sendmail` đến máy chủ của người nhận mail, một phát đến luôn.
- `Gửi gián tiếp` : Chuyển mail đến một máy khác và nhờ máy đó đại diện gửi đến máy chủ của người nhận mail.
  - Ví dụ: ta có thể gửi mail thông qua server của Google mail (tất nhiên là có thông tin tài khoản Google rồi) đến một địa chỉ bất kì ta muốn.
  - Khi đó, mail đó sẽ giống như ta gửi trực tiếp từ tài khoản Google Mail trên web thôi.
  - Tức là gửi 1 mail từ máy chạy `sendmail` đến máy chủ của người nhận thông qua `Google Mail` server.

1. Nói về syslog

- Hệ thống log hệ thống trong Linux được `quản lý` (thực ra là được vận chuyển) bởi phần mềm có tên `syslog`.
- Sẽ có một chương trình chạy ngầm (dạng `daemon`) gọi là `syslogd`.
- Chương trình này sẽ tiếp nhận hầu hết các log được `đẩy ra` từ các phần mềm `hệ thống` đang chạy rồi đẩy ra một đầu ra khác (thường luôn là `file`)
- Log của phần mềm `sendmail` cũng vậy.

2. Format

- Mỗi dòng log cho ứng dụng `sendmail` trong hệ thống gồm : `timestamp`, tên của máy đã tạo ra nó (để phân biệt với trường hợp log được tạo từ máy khác trong mạng), từ `sendmail:`, và một message đi kèm. Hầu hết các message bao gồm một dãy các cặp `name = value`.

- Có 2 loại log phổ biến nhất khi các message (tức là log mà `sendmail` log ra ấy) được đưa ra.

2.1 Đầu tiên là log nhận

- Mỗi message chỉ có 1 dòng log. Một số trường có thể được bỏ qua nếu chúng không chứa thông tin hữu ích. Các trường của message này:

Tên trường	Ý nghĩa
from	Địa chỉ của phía gửi trên phong thư
size	Kích thước (theo byte) của message
class	Class của message
pri	Độ ưu tiên ban đầu của message (sử dụng cho việc sắp xếp trong hàng đợi).
nrcpts	Số lượng phong thư của phía nhận (sau khi aliasing và forwarding).
msgid	Id của message (từ header).
proto	Giao thức được sử dụng để nhận message (ví dụ: ESMTP or UUCP)
daemon	Tên của chương trình chạy ngầm lấy từ giá trị **DaemonPortOptions** .
relay	Cái máy mà message sẽ được nhận

2.2 Log dành cho mỗi lần cố gắng gửi (phân phối)

- Có thể mỗi message có thể có nhiều log cho mỗi phân phối mail.
- Mỗi dòng sẽ tương ứng với 1 lần
- Các trường đó là:

Tên trường	Ý nghĩa
to	Danh sách người nhận được phân cách bởi dấu phảy (,).
ctladdr	Là `Controlling user` (user điều khiển), đó là tên của user được sử dụng để xác thực khi phân phối mail.
delay	Khoảng thời gian giữa khi message được nhận và thời điểm nó bị đẩy đi.
xdelay	Khoảng thời gian cần để phân phối message (thông thường biểu thị tốc độ của kết nối internet).
mailer	Tên của `mailer` được sử dụng để phân phối mail đến phía nhận.
relay	Tên của `host` (có thể hiểu là máy chủ) thực sự chấp nhận (hoặc từ chối) địa chỉ người nhận.
dsn	Mã lỗi bổ sung (RFC2034) nếu có
stat	Trạng thái kết quả phân phối.

Không phải lúc nào cũng có đủ các trường ở trên; ví dụ, relay thường không xuất hiện khi phân phối đến mạng cục bộ.

SENDMAIL LOG