Understanding the maillog

Breakdowns of Typical Log Lines

Typical maillog line example

```
Sep 23 08:08:39 mta25 haraka[13424]: [NOTICE] [8BEF5192-4188-4824-B210-
A309BABC1897.1] [core] sender <alain.albert@woodoer.com> code=OK msg=""
```

Date/Time: `Sep 23 08:08:39`

Hostname: `mta25`

Process[Process ID]: `haraka[13424]:`

Log Severity: `[NOTICE]`

Haraka ID: `[8BEF5192-4188-4824-B210-A309BABC1897.1]`

Haraka Plugin (or core): `[core]`

Logged Message: `sender <alain.albert@woodoer.com> code=OK msg="" code=OK msg=""`

Haraka ID's

The example above cointains a Haraka UUID (Universally Unique Identifiers) for it's Session and Transaction ID's.

A 'Session' is from the start of the TCP connection to the end of the connection and the 'Transaction' relates to the SMTP transaction which starts whenever a sender sends an SMTP 'MAIL FROM' command. A host can send multiple Transactions in a single connection (Session). Note that Transactions may or may not yield a Message as a Transaction might be rejected before a message is sent.

```
8BEF5192-4188-4824-B210-A309BABC1897.1
---------- Session ID -------------- ^ Transaction ID
```

The transaction ID is simply a counter starting a 1 and incremented for each transaction. When searching through logs, you should use the Session ID to show the entire session unless you know there were a lot of transactions.

Haraka Log Levels

Haraka sends messages to the syslog based on the configured maximum severity which defaults to LOGNOTICE. This means that you will see NOTICE, WARN, ERROR, CRIT, ALERT and EMERG severity messages in the log.

```
LOGDATA          Most Verbose
LOGPROTOCOL           |
LOGDEBUG              |
LOGINFO               |
LOGNOTICE             |  < -- Default log level
LOGWARN               |
LOGERROR              |
LOGCRIT               |
LOGALERT              |
LOGEMERG        Least Verbose
```

To change the maximum severity level to increase the verbosity of the messages logged by Haraka - you simply write the desired level into /etc/haraka/config/loglevel e.g.:

```
echo LOGINFO > /etc/haraka/config/loglevel
```

Haraka will notice the change to the file almost immediately - so no restart is required. In production you should never increase the log level above LOGDEBUG as doing so will put considerable amounts of data into syslog and into the log files and will cause additional IO on the server.

Typical MailScanner log line example

```
Sep 23 08:08:45 mta25 MailScanner[31474]: Filename Checks: Allowing r8NBBN2j012991
msg-31474-155.txt
```

Date/Time: `Sep 23 08:08:45`

Hostname: `mta25`

Process[Process ID]: `MailScanner[31474]:`

Logged Message: `Filename Checks: Allowing r8NBBN2j012991 msg-31474-155.txt`

Typical sendmail log line example

```
Sep 23 08:08:40 mta25 sendmail[12991]: r8NBBN2j012991: to=<steve@swaney.com>,
delay=00:00:00, mailer=esmtp, pri=38403, stat=queued
```

Date/Time: `Sep 23 08:08:40`

Hostname: `mta25`

Process[Process ID]: `sendmail[12991]`

Logged Message: `r8NBBN2j012991: to=<steve@swaney.com>, delay=00:00:00, mailer=esmtp, pri=38403, stat=queued`

A typical email as seen by the maillog

The flow:

1. Haraka accepts the incoming connection and assigns a Message ID similar to: [8BEF5192-4188-4824-B210-A309BABC1897.1].
2. Haraka finishes processing the message and connects to sendmail listening on port 26 to forward the message
3. Sendmail assigns a new Queue ID similar to `r8NBBN2j012991` and places the message in /var/spool/mqueue.in.
4. Sendmail responds to Haraka saying that the message was successfully received and also returns the Queue ID back to Haraka. Haraka then responds back to the connected client with the same message and appends it's own Transaction ID to the end of the message to aid logging and debugging. The same output is sent to the syslog.
5. One of the MailScanner child processes picks up the message from /var/spool/mqueue.in and processes the message logging with the same Queue ID used by Sendmail, `r8NBBN2j012991`.
6. The MailScanner child finishes processing and passes the message to sendmail for final delivery with the Sendmail, Queue ID similar to `r8NBBN2j012991`.
7. If sendmail can't immediately deliver the message, the message is queued for later delivery attempts with the Sendmail, Queue ID similar to `r8NBBN2j012991`.

An Example of a typical message being received

Haraka log entries

```
Sep 23 08:08:39 mta25 haraka[13424]: [NOTICE] [8BEF5192-4188-4824-B210-
A309BABC1897.1] [core] sender <alain.albert@woodoer.com> code=OK msg=""
```

Incoming message; sender is alain.albert@woodoer.com

```
Sep 23 08:08:40 mta25 haraka[13424]: [NOTICE] [8BEF5192-4188-4824-B210-
A309BABC1897.1] [core] recipient <steve@swaney.com> code=OK msg=""
```

Incoming message; recipient is steve@swaney.com

```
Sep 23 08:08:40 mta25 haraka[13424]: [NOTICE] [8BEF5192-4188-4824-B210-
A309BABC1897.1] [core] message
mid="<CANgkz+H8GUUaaM3LMzxwPYZhm4cAOwGNDYWJ9r3QpBkuT03p0A@mail.gmail.com>"
size=6946 rcpts=1/0/0 delay=0.319 code=CONT msg=""
```

Incoming message;
Gmail Message ID: CANgkz+H8GUUaaM3LMzxwPYZhm4cAOwGNDYWJ9r3QpBkuT03p0A@mail.gmail.com
Size is 6946 bytes, one recipient accepted, 0 recipients temp failed, 0 recipients rejected, message took 0.319 seconds to process and processing continues

```
Sep 23 08:08:40 mta25 haraka[13424]: [NOTICE] [8BEF5192-4188-4824-B210-
A309BABC1897.1] [core] queue code=CONT msg="2.0.0 r8NBBN2j012991 Message accepted
for delivery (8BEF5192-4188-4824-B210-A309BABC1897.1)"
```

Message was accepted by Sendmail and assigned Sendmail Queue ID r8NBBN2j012991

Haraka log entries (cont.)

```
Sep 23 08:08:40 mta25 haraka[13424]: [NOTICE] [8BEF5192-4188-4824-B210-
A309BABC1897.1] [core] disconnect ip=209.85.215.48 rdns="mail-la0-f48.google.com"
helo="mail-la0-f48.google.com" relay=N early=N esmtp=Y tls=Y pipe=N txns=1
rcpts=1/0/0 msgs=1/0/0 bytes=6946 lr="" time=2.273
```

The sending server mail-la0-f48.google.com disconnected
relay=N : the host is not allowed to relay
rdns="mail-la0-f48.google.com" : The rDNS entry for the host
helo="mail-la0-f48.google.com" : The response to the HELO command
esmtp=Y ; ESMTP was requested by the sender
tls=Y : Session was encrypted using TLS
early=N pipe=N :
early is short for earlytalker; which means the host tried to pipeline commands in the wrong SMTP state.
pipe is short for pipelining; which means the host pipelined commands correctly.
txns=1 : txns shows the number of transactions in this session.
rcpts=1/0/0 : Recipient counters, reas as accepted/tempfailed/rejected
msgs=1/0/0 : Message counters accepted/tempfailed/rejected
bytes=6946 : Message size in bytes
lr="" : Last rejection sent to sending MTA
time=2.273: Total connection (session) time was 2.273 seconds

Sendmail log entries

```
Sep 23 08:08:40 mta25 sendmail[12991]: r8NBBN2j012991:
from=<alain.albert@woodoer.com>, size=8403, class=0, nrcpts=1,
msgid=<WM!f1493998dd0a3ea4267275ff51f3d612291064b1f19466b2606fb69665fd916dba1fde2d1
834142435aea02f9bc8bcf6, proto=ESMTP, daemon=MTA, relay=localhost.localdomain
[127.0.0.1]
```

Sendmail accepts the message from Haraka on port 26

```
Sep 23 08:08:40 mta25 sendmail[12991]: r8NBBN2j012991: to=<steve@swaney.com>,
delay=00:00:00, mailer=esmtp, pri=38403, stat=queued
```

Sendmail queues the message to /var/spool/mqueue.in for pickup and processing

MailScanner log entries

```
Sep 23 08:08:45 mta25 MailScanner[31474]: Message r8NBBN2j012991 from 209.85.215.48
(alain.albert@woodoer.com) to swaney.com is not spam, SpamAssassin (not cached,
score=-1.897, required 4, BAYES_00 -1.90, DI_A_WILDCARD 0.00, HARAKA_FCRDNS 0.00,
HTML_MESSAGE 0.00)
```

MailScanner has processed and scored the message using Spamassassin

```
Sep 23 08:08:45 mta25 MailScanner[31474]: Filename Checks: Allowing r8NBBN2j012991
msg-31474-155.txt
```

Attachment msg-31474-155.txt is allowed

```
Sep 23 08:08:45 mta25 MailScanner[31474]: Filetype Checks: Allowing r8NBBN2j012991
msg-31474-156.html
```

Attachment msg-31474-156 is allowed

MailScanner log entries (cont.)

```
Sep 23 08:08:46 mta25 MailScanner[31474]: <A> tag found in message r8NBBN2j012991
from alain.albert@woodoer.com
```

Content scanning found an HTML <A> in the message

```
Sep 23 08:08:46 mta25 MailScanner[31474]: r8NBBN2j012991: Logged to MailWatch
```

Message has been passed to sendmail and logged to the Postgres maillog Database

Sendmail log entries

```
Sep 23 08:08:46 mta25 sendmail[28376]: r8NBBN2j012991: to=<steve@swaney.com>,
delay=00:00:06, xdelay=00:00:00, mailer=esmtp, pri=128403, relay=mail1.sgmhost.com.
[173.0.137.147], dsn=2.0.0, stat=Sent (ok 1379944860 qp 28965)
```

The message has been successfully delivered by sendmail to mail1.sgmhost.com and assigned Message ID "1379944860 qp 28965" by the receiving MTA.

Searching the maillog using fgrep

1. Find a Haraka or MailScanner Message ID:
   a. From the message headers
   b. Using the BarricadeMX Plus web interface Reports >> Run Reports or Reports >> SMTP log Search
   c. Search the maillog (with the proper date) for the From or To address:
      ```
      fgrep steve@swaney.com /var/log/maillog | more
      ```
2. Use the Haraka Message ID to locate all of the Haraka maillog entries for the message:
   ```
   fgrep 8BEF5192-4188-4824-B210-A309BABC1897 /var/log/maillog
   ```
   Or

   Use the MailScanner Queue ID to locate all of the MailScanner and Sendmail maillog entries:
   ```
   fgrep /var/log/maillog r8NBBN2j012991
   ```

Note:

1. You will need to manually run two searches of the mail log to find all of the log entries for any message.
2. The maillog is typically configured to start a new log early every Sunday Morning. Be sure and search the right maillog or maillogs for the dates that message you are looking for might be contained in.

References

syslog configuration:

syslog Configuration | Linux Journal
Creating a Centralized Syslog Server

log rotation:

Rotating Linux Log Files - Part 1: syslog - MDLog:/sysadmin
Rotating Linux Log Files - Part 2: logrotate - MDLog:/sysadmin

sendmail logging:

read sendmail entries in the system log

fgrep:

HowTo: Use grep Command In Linux / UNIX – Examples
Linux and Unix fgrep command

smtpf logs:

Smtpf log messages