Mail Administration from the Command-line

We’ll start by learning to read the log files and mail headers, and then continue onto troubleshooting issues like mail delivery and spam.

**By the end of this course, you'll be able to..**

* Read the **mail-related logs** to determine the origin, path, and end point of a message.
* Find users with **excessive mail usage**.
* Identify issues caused by **firewalls** (both on and off the server).
* Determine the destination of “**missing**” **mail**.
* Manually test **usernames** and **passwords**.
* Manage the **exim queue**.

Before you start troubleshooting, you probably want to know what Exim is currently processing. There are several ways to determine this.

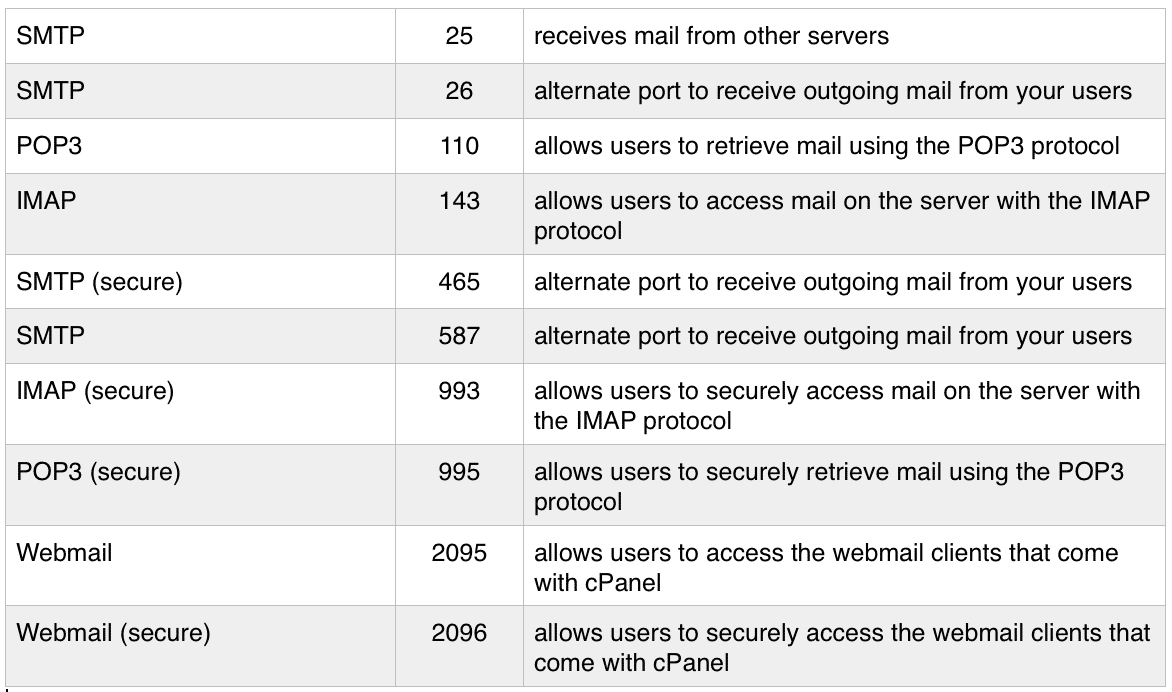
The three most common ways in order of usefulness, from our perspective, are as follows:

• exiwhat - This command shows active connections being handled.

• ps -C exim wwwu - This command shows a list of all running exim processes

•lsof -c exim - This command shows a list of files being accessed by Exim.

If you want to keep your mail flowing - and most administrators probably do - you'll want to take note of the following ports that are needed for specific types of mail traffic.



**Manual Testing**

One of the first tests that you can do is to ensure that Dovecot is authenticating and responding properly. Using telnet allows you to send the commands by hand so that you can observe exactly what's going on.

You should test from a remote location because Dovecot considers all local connections to be innately secure. Telnet should be installed on most servers, but if it’s not, you can install it with “yum install telnet”. Next, we'll take a look at a demonstration of the testing process.

**Need more information?**  
This article from **linuxquestions.org** goes over the IMAP telnet testing process in detail and breaks down each component.

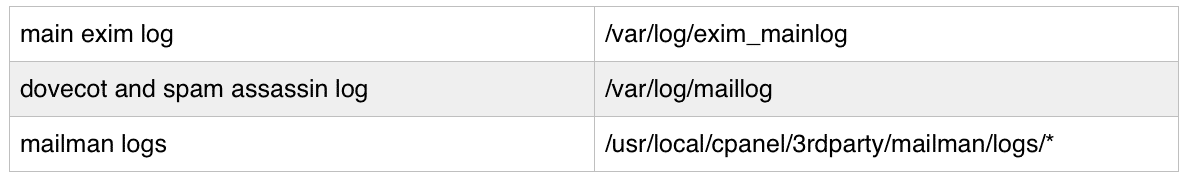
**Testing IMAP with OpenSSL**

While telnet is the tried and true standby for manually testing IMAP connections, plain text communications are increasingly frowned upon, even for testing.

It is also possible to test IMAP securely, using OpenSSL’s secure client command:

openssl s\_client -connect IP:port

The next important thing you’ll need to do is to check the log files. Unit 1 covers reading the logs, but here’s a chart to help you find the ones we’ll be discussing in this course:



**Reading Mail Logs and Headers**

This is generally not done on the server, but rather through the user’s mail client. Each mail client will have different instructions for how to view the full email headers.

Tools:

**zcat** is a tool to let you view zipped files without unzipping them.

It prints output to STDOUT (standard output), so you can redirect it to tools like grep to obtain only the information you need from the file.

**exigrep** is a special command-line utility for searching the Exim logs.

It works just like grep, but shows you all the log entries related to your search

**The Exim Main Log**

The log exim\_mainlog is Exim’s primary log, and the log we will be looking at. However, you should know that Exim does have other log files it writes to. These are Exim’s three logs:

/var/log/exim\_mainlog

Logs message arrival and delivery attempts; output is controlled by the log\_selector option

/var/log/exim\_rejectlog

Logs delivery rejections based on policy (e.g. ACL)

/var/log/exim\_paniclog

Logs severe errors, such as those that cause Exim to crash, or those that cause a message to never be delivered; should be empty, or nearly empty

**Message Status Indicators**

Exim logs have a clear format. One thing that is useful to know when looking at these logs are the status indicators that you might run across. The status indicators can be thought of as arrows pointing in and out of the Exim ID for arrival and delivery, respectively.

**Status Indicators**

<= Indicates message arrival

Example: *2015-03-13 09:20:29 1YWQRx-0008D8-LD <= root@hw1-x86.tech.cpanel.net ...*

=> Indicates successful delivery

Example: *2015-03-11 10:35:36 1YVifY-0004Dw-KL => mary@cpanel.net ...*

== Indicates a "deferred" message, generally meaning delayed.

Example: 2015-03-11 10:40:13 1YVik1-0004RW-Ef == root@hw1-x86.tech.cpanel.net ...

\*\* Indicates a delivery failure.

Example: 2015-03-11 10:40:13 1YVik1-0004RW-Ef \*\* root@hw1-x86.tech.cpanel.net ...

<https://exams.cpanel.net/unit/view/id:2078>