# More Linux Core Command Practice

A good Linux admin can quickly parse huge log files from the command line (and jump tall buildings in a single bound.) The purpose of this lab is to show you just how powerful the command line can be, not necessarily to make you a log parsing guru.

The file, LinuxLab2LogFile, contains some SMTP (mail server) logs. The format of the file is:

Date Time SenderIPAddress SenderName ServiceName MailServerName MailServerIP Commands

We want to answer these questions:

1. how many separate senders sent mail?
2. how many messages did each sender send?
3. who sent the most messages?

Open a browser in you CentOS VM and go to Moodle. Download LinuxLab2LogFile. Open a terminal and change directory to ~/Downloads, which is where your browser puts things.

View the file from the command line:

less LinuxLab2LogFile.

First, some cleanup. On a few lines, the server tried to send binary data. Some of the bytes in the binary data looked like carriage returns, so there are extra lines of junk in the file. You can see some if you use less and page through the data (line 708 for example. While in less, type **g 708**). Without cleanup, our search for IP addresses will give us garbage like this:  
10.1.12.9  
192.168.12.2  
1C2M4GcUAVLS2tWtkcIkm4ZLMMknv+tLY7RJcLEf3SuNoHQHHOPxqvIdLl/euVBbkgZ/kKsQ  
afbXKyXPlrbNEdpYllweopBcXgZwLTeochTuC5GfSlt3nlu900Qi2JjGc5yf/rUAXKKKKAKu  
AUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFFFFABRRRQAUUUUAFF

Note that all of the valid lines start with the date, so the following command will remove any lines that don't start with 2014-. (The "^" means start at the beginning of the line. You could use a fancy regular expression in grep to match any line in the correct format no matter what the year, but we'll start simply.)

grep '^2014-' LinuxLab2LogFile > temp

[john@localhost Desktop]$ grep '^2014-' LinuxLab2LogFile > temp

Now, on to answering the questions. To do this, you'll have to find out how to use the command, cut. Use --help, man,or Google to do this.

## Question 1: How many separate senders (servers) sent mail?

Step 1: Cut the SenderIPAddress column from temp and save it to temp1. Use the command, less, to make sure it is correct.

We need to tell the cut command three things: which column we want, what character is in between the columns (delimiter), and where the input comes from. In this case we want column 3, the delimiter between columns is a space, and the file to get the input from is temp. We will redirect the output to temp1.

[john@localhost Desktop]$ cut -f3 -d" " temp > temp1

Step 2: Sort temp1 file so all the IP addresses are in order and output it to temp2. (Note: this is to help the uniq command work, and not to sort them into a human-nice format.)

[john@localhost Desktop]$ sort temp1 > temp2

Step 3: Use the uniq command to extract the unique IP addresses in temp2 and output them to temp3. Note, that this only works if you sorted the list first.

[john@localhost Desktop]$ uniq temp2 > temp3

Step 4: Use the wc command to count the number of lines in temp3. Note: I got 19.

Note that wc counts the lines, words, and bytes in the input it is given. In our case, each line only contains one word (no spaces), so the lines and words are both 19. If we only wanted lines, we could use wc –l.

[john@localhost Desktop]$ wc temp3  
 19 19 215 temp3

Step 5: Putting the commands on 5 different lines and using 4 different temporary files is pretty **klunky**, although it makes it easier for you to see what we are doing. Here's where the coolness of the pipe comes in. We can use it to do everything at once without using temp files.

Make a command that looks something like this:

grep '^2014-' LinuxLab2LogFile | [your cut command] | [your sort command] | [your uniq command] | [your wc command]

[john@localhost Desktop]$ grep '^2014' LinuxLab2LogFile | cut -f3 -d" " | sort | uniq | wc  
 19 19 215

**You'll leave out the "> temp" stuff, of course. We’re sending the output of one command directly to the input of the next command, no temp files required.**

Note: when you are making long strings of commands like this it may be helpful to take small steps. I will often pipe the output of the first command into less to see if I like the output. Then I pipe the first command to the second and then to less, and check again. I keep going this way until I finally have the entire command working correctly.

## Question 2: How many messages did each sender send?

Each message causes several lines in the log file, as the file records the EHLO, MAIL FROM, RCPT TO, DATA and QUIT commands that are part of the SMTP protocol. We'll assume that one DATA command means one message. Use the grep command to extract the lines containing "DATA". Then use cut and sort as before. The uniq command has an option to count the number of duplicates (messages in this case) it finds. The output will show the number of messages from each IP address.

Hint: your command will look something like this

grep '^2014-' LinuxLab2LogFile | [grep for DATA] |[same cut command as before] | [same sort] | [uniq with option to count]

[john@localhost Desktop]$ grep '^2014' LinuxLab2LogFile | grep "DATA" | cut -f3 -d" " | sort | uniq –c  
 3 10.1.10.11  
 3 10.1.10.123  
 5 10.1.10.181  
 4 10.1.10.203  
 1 10.1.10.229  
 5 10.1.10.233  
 1 10.1.10.242  
 73 10.1.10.34  
 376 10.1.10.35  
 2 10.1.10.4  
 2 10.1.10.5  
 3 10.1.10.93  
 3 10.1.11.215  
 4 10.1.11.37  
 5 10.1.11.55  
 15 10.1.11.69  
 12 10.1.12.32  
 6 10.1.12.9  
 1 192.168.12.2

## Question 3: who sent the most messages?

Since there are only 19 senders, you can just look at the output from the last question. If there were a huge number of senders, you could pipe the output into sort -rn and head, or sort -n and tail.

[john@localhost Desktop]$ grep '^2014' LinuxLab2LogFile | grep "DATA" | cut -f3 -d" " | sort | uniq -c | sort -nr | head  
 376 10.1.10.35  
 73 10.1.10.34  
 15 10.1.11.69  
 12 10.1.12.32  
 6 10.1.12.9  
 5 10.1.11.55  
 5 10.1.10.233  
 5 10.1.10.181  
 4 10.1.11.37

BTW If you'd like to get an idea of what's possible from the command line, look at the blog "Command Line Kung Fu".