Google IT Support Certificate: Course 3: Operating Systems and You

Week 6: Operating Systems in Practice

Quiz: Using Logs to Help You Track Down an Issue in Linux

Introduction

In this lab, you'll use logs to help you troubleshoot and track down an issue. As an IT Support Specialist, it's crucial that you know how to troubleshoot and "follow the cookie crumbs." There are five different issues that you'll need to resolve, using the skills you've learned so far in this course.

What you'll do

- Familiarize yourself with the process of changing permissions within a file and folder in Linux
- Change the ownership of a specific file and folder

The scenario

Your computer is having some issues, and you can't seem to figure out what's wrong. Argh! Dig through the logs to figure out how to fix these issues.

You'll use logs to identify issues on a Linux VM, which you'll then fix using the knowledge you've gained from the other labs that you've completed.

What you should already know

This lab focuses on looking at logs that indicate issues that need to be fixed. These issues can be resolved using the skills you've gained in previous labs, so detailed instructions won't be included here. You're on your own...but you've got this!

Here are the concepts you need to be familiar with before taking this lab:

- Updating software that's out-of-date
- Finding and deleting files
- Modifying file permissions
- Finding and terminating specific processes

Viewing logs on Linux

On Linux machines, logs are stored in the **/var/log** directory. There are lots of log files in this directory, and you can view them with this command:

```
ls /var/log
```

Copied!

content_copy

```
alternatives.log  auth.log  dpkg.log  faillog  messages  user.log

apt               btmp      exim4     lastlog  syslog    wtmp
```

We're interested in syslog for the moment. The logs on Linux can be viewed like any text file; you can use the command below to view the contents of syslog:

```
sudo cat /var/log/syslog
```

Copied!

content_copy

The log contents are super long, so you'll have to scroll through the logs to look for the five entries that are relevant to this lab. The logs are entered chronologically, and the logs that you'll need to fix should be timestamped around the time that the lab started. For convenience, all of the log entries you need to fix contain the phrase "Qwiklab Error". Knowing this, you could also filter out the relevant labs using the grep command.

We'll walk through addressing one of the log's issues, then the other four will be up to you!

Low disk space!

Here's the log entry we will be dealing with first:

```
Aug 11 12:33:21 75b72110ff5a root: Qwiklab Error: Disk space is super low, fix it!
```

This error indicates that your computer is running out of memory due to a super large file. Unfortunately, it doesn't indicate which file is causing the problem, so you'll need to find it. Luckily, Linux has an easy way to find the largest files on your file system. The **du** command can be used to list all files in a directory (recursively through subdirectories, too), which you can sort by size to find the largest files. By piping the output of du (using the "|" symbol) to the **sort** command, you can sort the output by file size. The "-n" and "-r" flags tell sort to treat the string output on each line as a number (the file size), and to sort in reverse order so that the largest files are listed first. By piping the output of this into the **head** command, you can print out only the top few results (you can specify how many to output by adding "-n [NUMBER]" to the end of the command).

The command below uses **du**, **sort**, and **head** to show the top five largest files, starting from your /home directory:

```
sudo du -a /home | sort -n -r | head -n 5
```

Copied!

content_copy

```
3147112 /home

3147076 /home/lab

3145736 /home/lab/storage

3145732 /home/lab/storage/ultra_mega_large.txt

1328    /home/lab/downloads
```

You can see that the largest file in your home directory is /home/lab/storage/ultra_mega_large.txt, at about 5GB. This isn't an important file, but it's taking up a lot of space, so you can delete it to fix the disk space error:

```
sudo rm /home/lab/storage/ultra_mega_large.txt
```

Copied!

content_copy

Now that the large file is gone, this log's issue has been dealt with. You can see that the log entry is still present in the log file; logs aren't deleted once the errors that caused them are resolved.

Fix low disk space

Check my progress

The remaining log entries

The rest of the logs involve issues that you have already successfully fixed in earlier labs in this course. Refer back to those lessons and labs to refresh yourself on the required steps, if you’re stuck:

- Finding and deleting files (Week 1 Labs)
-

  Remove corrupted file
- Check my progress
-
- Updating software that's out-of-date (Week 3 Labs)
-

  Update VLC
- Check my progress

-
- Finding and terminating specific processes (Week 5 Labs)
-

  End malicious processes
- Check my progress
-
- Modifying file permissions (Week 2 Labs)
-

  Change permission of secret file to public (777)
- Check my progress
- If you’d like to check your steps along the way, refer to your score in the top right of the lab. Click the score and run each step to check individually as you go. Good luck!

Note: Please make sure that you are running the commands using **sudo**. The purpose of sudo is to execute the command given to it with root privileges.

Conclusion

Excellent job! You've successfully used logs to track down and fix issues on a Linux machine.