2.12.6 Find File Content

Click one of the buttons to take you to that part of the video.

Find File Content 0:00-0:31

In this demonstration, we're going to talk about how to find specific information within files in the Linux file system. This is a very important skill for a Linux system administrator to have because when you're managing Linux system, you will commonly need to search through files, trying to find specific pieces of information, such as searching through a log file or searching through a configuration file. One option for doing this is to open that file up in a text editor and then try to manually find the information.

---

grep 0:32-4:19

A better way to do this is to use the grep utility. grep is extremely useful. It can be used to search through files to identify the lines of text that contain the specific information that you're looking for. For example, let's suppose we need to look through the boot log file for this system and search for any lines of text that contain the term 'udev'. udev is the Linux component that is used to manage kernel modules to support the hardware in the system. Maybe we're having some problems with the hardware. We want to see what happened during the boot process.

Let's, first of all, switch to our root user account. Let's switch to the /var/log directory. In this directory, we should see the boot.log file. This file contains entries that are created as the system boots up, telling you what's happening with the overall boot process. In order to search though that file for the term 'udev', we would enter 'grep' and then, in quotation marks, the text that we want to search for. The reason we use quotation marks is because it allows us to use text that contains spaces. In our case, we're just going to look for a single word, so we probably wouldn't need to use quotation marks, but it is a best practice.

We're going to search for '"udev"', and the file we want to search for that term within is the boot.log file. Press Enter, and it brings up every single line within this file. This is a very big file. It's got lots of lines in it. The grep utility just pulled out each line that had that term that we were searching for in it and writes it on the screen. Extremely useful. Instead of having to pore through the boot log file, trying to find every single line that has 'udev' in it, I run grep, and I have a nice condensed view of the information that I'm looking for without having to wade through a bunch of useless information.

grep has one other really fantastic feature that I absolutely love and I use on a daily basis. That is the fact that it can search across files for specific information. Instead of searching within a single file, it can look through a whole bunch of different files for the information you're looking for. For example, let's suppose that there is a configuration parameter that we need to find, but we're really not sure what file that parameter's saved in. In this situation, let's suppose that we need to configure the listen address parameter for the SSH daemon that's running on the system. We know that that parameter is probably saved in a configuration file somewhere in the /etc directory, so we'll start there. But from here, we're lost. In order to find this particular piece of information, we type 'grep', and then we use the '-r' parameter to cause grep to search recursively, meaning that it's going to look not only in the current directory, but it's going to look in all the subdirectories of /etc, as well, for the information we're looking for. It'll essentially go into each directory, open up each file, and look for the information we're looking for. If it finds a match, it'll put it on the screen; if not, it'll just move on to the next file, then will move on to the next subdirectory, and the next subdirectory, and so on.

We want to search for the term '"ListenAddress"'. Put it in quotation marks. We're going to enter a star (*) here to indicate we want to look in all files. The star is a wild card, which matches anything. So, by specifying just a star here, we're telling grep to look in every single file in every single subdirectory and look for the term 'ListenAddress'. Go ahead and run this. It takes a minute to run because it's got to go through a lot of different files. Here we go. There are two instances of ListenAddress. It looks like they're both in the same file. They're located in the SSH subdirectory of the /etc directory. The name of the file that contains these parameters is sshd_config.

You can also use a utility called egrep to accomplish the same task.

Create Regular Expressions with egrep 4:14-6:02

However, egrep provides some additional functionality. Using egrep allows you to use regular expressions to find information that matches these specific search criteria that you specify. Essentially, egrep allows you to create very complex searches. I do need to point out that if you were to run grep -e, it is exactly the same command as running egrep. You can use either option.

Let's suppose that we need to search through the user account file on this system, the /etc/password file, and locate each line that begins with the text 'rtracy'. In other words, I'm trying to search for my user account. In this situation, we know that the way the password file is formatted is such that the name of the user account always comes at the beginning of each line of text within the file. What we can do is use a regular expression to tell egrep to only look for the text we specify at the beginning of each line within the file. To do this, we use a caret character, and then we specify the text that we're looking for, rtracy. This is a regular expression. Then we have to tell it where to look. In this

case, we want to constrain the search to just the /etc/password file. We could search across all files if we wanted to. But, to make things faster, we're just going to constrain the search to one single file.

This command will search this file and will identify any lines that begin with 'rtracy'. Press Enter, and here's the single line of text that matches out of that file.

Notice that the line begins with the text that we specified in the command.

Where to Find Regular Expressions 6:02-6:25

There are hundreds of different regular expressions that you can create and use with the egrep command. We don't have time or space to go through all the options here. If you want to see some possibilities, you can go online and search for "grep regular expressions," and you'll see all kinds of different examples and tables containing regular expressions that can be used with the grep and egrep commands.

That's it for this demonstration.

Summary 6:24-6:33

In this demo, we talked about how to find information within files in the Linux file system. We first looked at using the grep command, and then we looked at creating regular expressions with the egrep command.
