Damir Nabiullin - Lab 4

Answers:

1. Using `grep`:

```
dale@dale-nitro:~/Documents/SNA/Week 4$ grep -P "(ERROR|WARNING)" server-data.log
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
```

   Using `awk`:

```
dale@dale-nitro:~/Documents/SNA/Week 4$ awk '/(WARNING|ERROR)/{print $0}' server-data.log
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
```

2. `sed -n '/remoted: INFO/!p' server-data.log`

```
dale@dale-nitro:~/Documents/SNA/Week 4$ sed -n '/remoted: INFO/!p' server-data.log
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ACTION: none INFO: Remote syslog allowed from: '10.110.15.0/24'
```

3. `grep "ERROR" server-data.log | wc -l` or `awk "/ERROR/ {++i} END {print i}" server-data.log`

```
dale@dale-nitro:~/Documents/SNA/Week 4$ grep "ERROR" server-data.log | wc -l
2
dale@dale-nitro:~/Documents/SNA/Week 4$ awk "/ERROR/ {++i} END {print i}" server-data.log
2
```

4. `awk '{gsub(/INFO/, "NOTHING")}{print}' server-data.log > newlog.log`

```
dale@dale-nitro:~/Documents/SNA/Week 4$ cat newlog.log
2022/09/18 13:25:34 wazuh-remoted: NOTHING: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:34 wazuh-remoted: NOTHING: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
Log1 2022/09/18 13:25:35 wazuh-remoted: NOTHING: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:35 wazuh-remoted: NOTHING: Remote syslog allowed from: '10.110.15.0/24' END
2022/09/18 13:25:35 wazuh-remoted: ACTION: none NOTHING: Remote syslog allowed from: '10.110.15.0/24'
```

5. `grep -P "^(2022\/09\/18 13:25:3[45] wazuh-remoted)(: (\bINFO|WARNING|ERROR\b):).+('10\.110\.1[58]\.0\/24'$)" server-data.log`

```
dale@dale-nitro:~/Documents/SNA/Week 4$ grep -P "^(2022\/09\/18 13:25:3[45] wazuh-remoted)(: (\bINFO|WARNING|ERROR\b):).+('10\.110\.1[58]\.0\/24'$)" server-data.log
2022/09/18 13:25:34 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:34 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
2022/09/18 13:25:34 wazuh-remoted: INFO: Remote syslog allowed from: '10.110.15.0/24'
2022/09/18 13:25:35 wazuh-remoted: WARNING: Remote syslog not parsed from: '10.110.18.0/24'
2022/09/18 13:25:35 wazuh-remoted: ERROR: Remote syslog blocked from: '10.110.18.0/24'
```

6. I used such one line command: `sed -r 's/at/\nException occured inside method/; s/((\w*\.[\w\d\.]*\w*[\w\d\.\$]*)+)([\(])(\w*)([\.])(\w*)([\:])(.+\w)(.+)/`\1` from file `\4.\6` on line `\8`. The file was written in `\6`.\n\nCalled method \1 which calls line \8 of file \4.\6. The file is written in \6./'`.

   If you want to pass log file via my `sed` - you can used such form `cat <file> | sed …`

   (This bonus task was really hard :0)

```
dale@dale-nitro:~/Documents/SNA/Week 4$ sed -r 's/at/\nException occured inside method/; s/((\w*\.[\w
\d\.]*\w*[\w\d\.\$]*)+)([\(])(\w*)([\.])(\w*)([\:])(.+\w)(.+)/`\1` from file `\4.\6` on line `\8`. Th
e file was written in `\6`.\n\nCalled method \1 which calls line \8 of file \4.\6. The file is writte
n in \6./'
at org.apache.hadoop.fs.FileSystem$Cache.getInternal(FileSystem.java:2703)

Exception occured inside method `org.apache.hadoop.fs.FileSystem$Cache.getInternal` from file `FileSy
stem.java` on line `2703`. The file was written in `java`.

Called method org.apache.hadoop.fs.FileSystem$Cache.getInternal which calls line 2703 of file FileSys
tem.java. The file is written in java.
```

```
at com.databricks.backend.daemon.data.client.DatabricksFileSystemV2.recordOperation(DatabricksFileSys
temV2.scala:474)

Exception occured inside method `com.databricks.backend.daemon.data.client.DatabricksFileSystemV2.rec
ordOperation` from file `DatabricksFileSystemV2.scala` on line `474`. The file was written in `scala`
.

Called method com.databricks.backend.daemon.data.client.DatabricksFileSystemV2.recordOperation which
calls line 474 of file DatabricksFileSystemV2.scala. The file is written in scala.
```