Lab 3: File permissions and text filtering editors

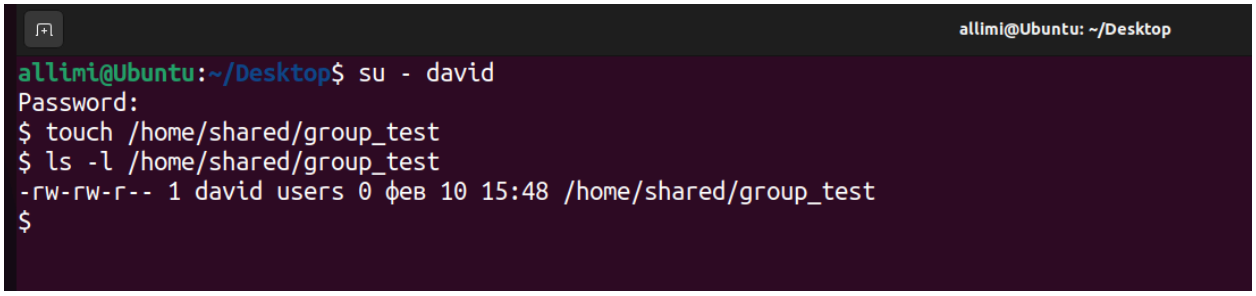
Ahmed Baha Eddine Alimi

Assignment Report

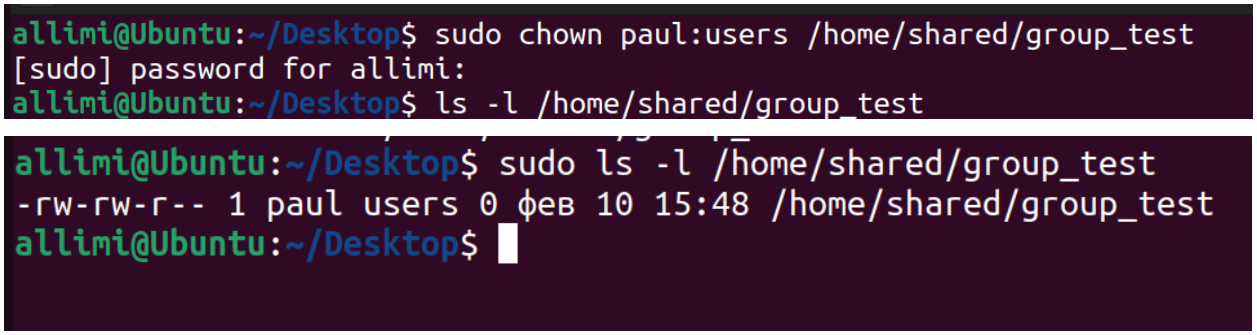
SD-01

I. File permissions:

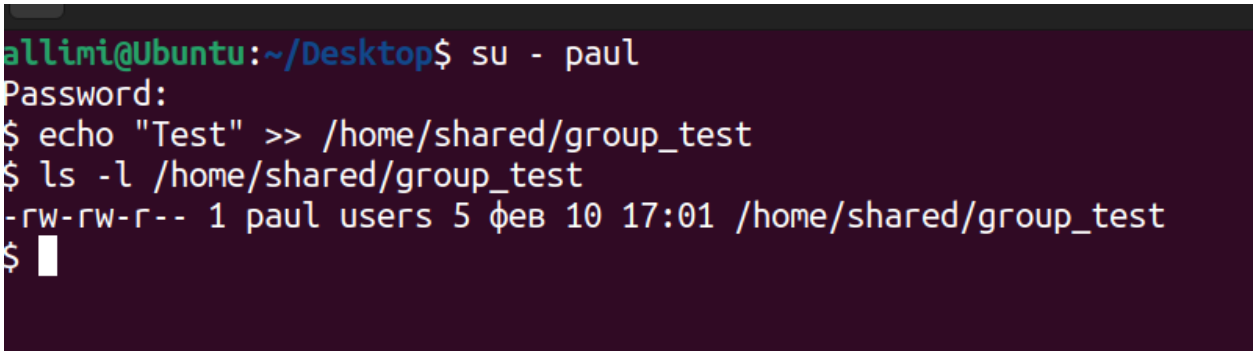
1. Create a file called `group_test` in `/home/shared` as a user `david`.



2. Change the owner of `group_test` to `paul` while keeping the group ownership as `users`.



3. Log in as `paul` and verify if he can modify `group_test`. Explain why.



The modification was successful, it means `paul` has write permission.
The reason `paul` can modify the file is that he is now the owner of `group_test`, and by default, the owner has read and write permissions `(rw-)`.

4. Now change the group ownership to a new group called shared_group (which you need to create) and verify access control.

```
allimi@Ubuntu:~/Desktop$ sudo groupadd shared_group
allimi@Ubuntu:~/Desktop$ sudo chown paul:shared_group /home/shared/group_test
```

```
allimi@Ubuntu:~/Desktop$ sudo ls -l /home/shared/group_test
-rw-rw-r-- 1 paul shared_group 5 фев 10 17:01 /home/shared/group_test
```

I added `david` to the `shared_group` and tested the permission:

```
allimi@Ubuntu:~/Desktop$ sudo usermod -aG shared_group david
allimi@Ubuntu:~/Desktop$ su - david
Password:
$ echo "Some Text" >> /home/shared/group_test
$
```

II. Text filtering editors:

1. View only error and warning messages in `server-data.log`. Show how you can do this with `grep` and `awk`.

Using `grep`:

```
allimi@Ubuntu:~/Desktop$ grep -E "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`:

```
allimi@Ubuntu:~/Desktop$ awk '/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'
```

2. View every line except lines with informational messages.

Using `grep`:

```
allimi@Ubuntu:~/Desktop$ grep -v "INFO" 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`:

```
allimi@Ubuntu:~/Desktop$ awk '!/INFO/' 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'
```

3. Count how many error messages are in the log.

Using `grep`:

```
allimi@Ubuntu:~/Desktop$ grep -c "ERROR" server-data.log
2
```

Using `awk`:

```
allimi@Ubuntu:~/Desktop$ awk '/ERROR/ {count++} END {print count}' server-data.log
2
```

4.Hide the IP addresses. Replace all IP addresses with `xxx.xxx.xxx.xxx•/xx` and save the output to a file `newlog.log`. Show the output..

Using `sed`:

```
allimi@Ubuntu:~/Desktop$ sed -E "s/[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+\/[0-9]+/xxx.xxx.xxx.xxx\/xx/g" server-data.log > newlog.log
```

output:

5. Write a single regular expression to match the following lines in server-data.log. Show the full command and regex used.

```
allimi@Ubuntu:~/Desktop$ grep -E '^20[0-9]{2}/(0[1-9]|1[0-2])/(0[1-9]|[12][0-9]|3[01]) [0-9]{2}:[0-9]{2}:[0-9]{2} wazuh-remoted: (INFO|ERROR|WARNING): Remote syslog (allowed|blocked|not parsed) from: '\''[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/[0-9]{1,2}'\''$' server-data.log
```

```
2022/09/18 13:25:34 wazuh-remoted: INFO: Remote syslog allowed from: '10.410.15.0/24'
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'
```

Regex Explanation:

Date format:

- `^20[0-9]{2}` **Matches the year (2020–2099).**
- `/(0[1-9]|1[0-2])` **Matches the month (01–12).**
- `/(0[1-9]|[12][0-9]|3[01])` **Matches the day (01–31).**

Time format:

- `[0-9]{2}:[0-9]{2}:[0-9]{2}` **Matches the time in HH:MM:SS format.**

Static text:

- `wazuh-remoted:` **Matches the literal text** `"wazuh-remoted:"`**.**
- `(INFO|ERROR|WARNING):` **Matches the log level (INFO, ERROR, or WARNING).**
- `Remote syslog (allowed|blocked|not parsed) from:` **Matches the specific log message patterns.**

IP Address Matching:

- `'\''[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/[0-9]{1,2}'\''`
  - **Matches an IP address in** `xxx.xxx.xxx.xxx/xx` **format.**
  - `[0-9]{1,3}` **ensures valid octets.**
  - `/[0-9]{1,2}` **captures the subnet mask.**

End of Line:

- `$` **ensures the match only extends to the end of the line.**

III. Bonus Questions:

1.Answer:

```
allimi@Ubuntu:~/Desktop$ sed -E 's/at ([^()]+)\(([^:]+):([0-9]+)\)/Exception occurred inside method `\1` from file `\2` on line `\3`. The file was written in java./' logfile.txt
Exception occurred inside method `com.databricks.backend.daemon.data.client.DatabricksFileSystemV2.recordOperation` from file `DatabricksFileSystemV2.scala` on line `474`. The file was written in java.
Exception occurred inside method `com.databricks.backend.daemon.data.client.DBFSV2.initialize` from file `DatabricksFileSystemV2.scala` on line `64`. The file was written in java.
Exception occurred inside method `com.databricks.backend.daemon.data.client.DatabricksFileSystem.initialize` from file `DatabricksFileSystem.scala` on line `222`. The file was written in java.
Exception occurred inside method `org.apache.hadoop.fs.FileSystem.createFileSystem` from file `FileSystem.java` on line `2669`. The file was written in java.
Exception occurred inside method `org.apache.hadoop.fs.FileSystem.access$200` from file `FileSystem.java` on line `94`. The file was written in java.
Exception occurred inside method `org.apache.hadoop.fs.FileSystem$Cache.getInternal` from file `FileSystem.java` on line `2703`. The file was written in java.
allimi@Ubuntu:~/Desktop$
```

Used Command:

```
sed -E 's/at ([^()]+)\(([^:]+):([0-9]+)\)/Exception occurred inside method `\1` from file `\2` on line `\3`. The file was written in java./' logfile.log
```

Explanation:

- `-E`: Enables extended regular expressions.
- `s/.../.../`: This is the substitution command in sed.
- `at ([^()]+)\(([^:]+):([0-9]+)\)`: This is the regex pattern that matches the stack trace lines:
- `at` : Matches the literal "at " at the beginning of the line.
- `([^()]+)`: Captures the method name
- `\(`: Matches the literal opening parenthesis
- `(. ([^:]+)`: Captures the file name. `[^:]+` matches any characters except a colon. `:([0-9]+):` Captures the line number (e.g., 2703). `[0-9]+` matches one or more digits. `\):` Matches the literal closing parenthesis).
- `Exception occurred inside method \1from file\2on line\3. The file was written in java.`: This is the replacement string: \1, \2, and \3 are back-references to the captured groups (method name, file name, and line number, respectively).