Log Analysis

1. General system messages

(/var/log/messages)

Display all "fail" or "error" messages:

```
# grep -Ei 'fail|error' /var/log/messages
```

---

2. Security and authentication messages

(/var/log/secure, potentially /var/log/auth.log)

Display all "fail" messages:

```
# grep -i "fail" /var/log/secure
```

Display failed console login attempts:

```
# grep 'FAILED LOGIN' /var/log/secure
```

Display successful console login attempts:

```
# grep 'LOGIN ON' /var/log/secure
```

Display the number of failed SSH login attempts:

```
# grep -E 'Failed (password|publickey)' /var/log/secure | wc -l
```

Display the number of successful SSH login attempts:

```
# grep -E 'Accepted (password|publickey)' /var/log/secure | wc -l
```

Display users with failed SSH login attempts in descending order:

```
# grep -E 'Failed (password|publickey)' /var/log/secure | awk '{print
$(NF-5)}' | sort | uniq -c | sort -r
```

Display users with successful SSH login attempts in descending order:

```
# grep -E 'Accepted (password|publickey)' /var/log/secure | awk '{print $9}'
| sort | uniq -c | sort -r
```

Display IP addresses with failed SSH login attempts in descending order:

```
# grep -E 'Failed (password|publickey)' /var/log/secure | awk '{print
$(NF-3)}' | sort | uniq -c | sort -r
```

Display IP addresses with successful SSH login attempts in descending order:

```
# grep -E 'Accepted (password|publickey)' /var/log/secure | awk '{print
$11}' | sort | uniq -c | sort -r
```

Extract data from the log for the last 24 hours and save them in the file <date>.report:

```
# lastday=$(LC_TIME="en_EN.UTF-8" date +"%b %d %T" -d "last day"); echo
$lastday | cat /var/log/secure - | sort | sed "1,/$lastday/d" > $(date +%d-
%m-%Y).report
```

---

3. Kernel messages

(/var/log/dmesg)

Display all "warning" messages:

```
# dmesg | grep -i "warn"
```

or

```
# grep -i "warn" /var/log/dmesg
```

---

4. System boot messages

(/var/log/boot.log)

Display all "KO" messages:

```
# grep "KO" /var/log/boot.log*
```

---

5. Cron daemon messages

(/var/log/cron)

Display all "error" messages:

```
# grep -i "error" /var/log/cron
```

---

6. Mail server messages

(/var/log/maillog)

Display all "reject" messages:

```
# grep "reject" /var/log/maillog
```

---

7. Systemd journal messages

(/run/log/journal, potentially /var/log/journal)

Display all messages since the last reboot:

```
# journalctl -b
```

Display all messages in the specified time range:

```
# journalctl -S "2020-01-01" -U "2020-01-03 06:00"
```

Display all messages with a priority of "error" or higher:

```
# journalctl -p err
```

Display all web server related messages:

```
# journalctl -u httpd
```

Display all messages related to the specified process:

```
# journalctl _PID=8088
```

Display all new incoming messages in real time:

```
# journalctl -f
```

---

8. Audit daemon messages

(/var/log/audit/audit.log)

Display failed login attempts:

```
# aureport -l --failed
```

Display successful login attempts:

```
# aureport -l --success
```

Display all login attempts:

```
# aureport -l
```

Search for failed login attempts during the specified period:

```
# ausearch -i -m USER_LOGIN -sv no -ts 10/20/2021 22:00 -te 10/21/2021 04:00
```

Search for the number of all authentication attempts of user "tester":

```
# ausearch -m USER_AUTH | grep "tester" | wc -l
```

Search for SELinux denials of the httpd service:

```
# ausearch -m AVC -c httpd
```

---

9. Apache web server messages

(/var/log/httpd/access_log and /var/log/httpd/error_log)

Display the 10 most requested URLs:

```
# awk '/GET/ {print $7}' /var/log/httpd/access_log | sort | uniq -c | sort -
rn | head -10
```

Display the top 10 visits by IP address:

```
# awk '{print $1}' /var/log/httpd/access_log | sort -n | uniq -c | sort -rn
| head -10
```

Display the total number of visits for each month sorted by month:

```
# awk '/[^(^$)]/ {print $4}' /var/log/httpd/access_log | cut -c 5-12 | awk -
F '/' '{print $1, $2}' | uniq -c | awk '{print $2, $3, "total visits: "$1}'
```

Display the number of unique visits for each month sorted by month:

```
# awk -F ":" '/[^(^$)]/ {print $1}' /var/log/httpd/access_log | sort -u |
awk -F "/" '{print $2, $3}' | LC_TIME="en_EN.UTF-8" sort -k2n -k1M | uniq -c
| awk '{print $2, $3, "unique visits: "$1}'
```

Display the top 10 visits for each month, including a bar chart, sorted by month:

```
# awk '/[^(^$)]/ {print $4}' /var/log/httpd/access_log | cut -c 5-12 | awk -
F '/' '{print $1, $2}' | sort -u | LC_TIME="en_EN.UTF-8" sort -k2 -k1M |
while read m y; do echo "$m $y"; awk -F ":" '/[^(^$)]/ {print $1}'
/var/log/httpd/access_log | grep $m/$y | awk '{print $1}' | sort -n | uniq -
c | sort -rn | awk -v c=$COLUMNS 'NR==1{t=$1} NR>1{r=int($1/t*c+.5);
b="\033[0m"; for (i=0; i<r; i++) b=b"#"; printf $1 " %s %s\n", $2, b}' |
head -10; echo; done
```

---

10. Command history

(~/.bash_history)

Display the command history of the logged in user:

```
$ history
```

or

```
$ cat $HISTFILE
```

Clear specific entries from the command history:

```
$ history -a
$ vi $HISTFILE
$ history -r
```

From:
https://prompt.cz/en/ - **Prompt.cz**

Permanent link:
https://prompt.cz/en/log-analysis

Last update: **2024/10/13 18:55**