Analýza logů

1. Obecné systémové zprávy

(/var/log/messages)

Zobrazte všechny zprávy s výsledkem „fail“ nebo „error“:

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

---

2. Zprávy týkající se bezpečnosti a ověřování identity

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

Zobrazte všechny zprávy s výsledkem „fail“:

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

Zobrazte neúspěšné pokusy o přihlášení z konzole:

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

Zobrazte úspěšné pokusy o přihlášení z konzole:

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

Zobrazte počet neúspěšných pokusů o přihlášení přes SSH:

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

Zobrazte počet úspěšných pokusů o přihlášení přes SSH:

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

Zobrazte uživatele s neúspěšnými pokusy o přihlášení přes SSH v sestupném pořadí:

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

Zobrazte uživatele s úspěšnými pokusy o přihlášení přes SSH v sestupném pořadí:

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

Zobrazte IP adresy s neúspěšnými pokusy o přihlášení přes SSH v sestupném pořadí:

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

Zobrazte IP adresy s úspěšnými pokusy o přihlášení přes SSH v sestupném pořadí:

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

Vyberte z logu data za posledních 24 hodin a uložte je do souboru <datum>.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. Zprávy jádra

(/var/log/dmesg)

Zobrazte všechny zprávy s výsledkem „warning“:

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

nebo

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

---

4. Zprávy během spouštění systému

(/var/log/boot.log)

Zobrazte všechny zprávy s výsledkem „KO“:

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

---

5. Zprávy cron démona

(/var/log/cron)

Zobrazte všechny zprávy s výsledkem „error“:

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

---

6. Zprávy poštovního serveru

(/var/log/maillog)

Zobrazte všechny zprávy s výsledkem „reject“:

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

---

7. Zprávy systemd žurnálu

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

Zobrazte všechny zprávy od posledního rebootu:

```
# journalctl -b
```

Zobrazte všechny zprávy v daném časovém rozmezí:

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

Zobrazte všechny zprávy s prioritou „error“ nebo vyšší:

```
# journalctl -p err
```

Zobrazte všechny zprávy týkající se webového serveru:

```
# journalctl -u httpd
```

Zobrazte všechny zprávy týkající se daného procesu:

```
# journalctl _PID=8088
```

Zobrazte všechny nově příchozí zprávy v reálném čase:

```
# journalctl -f
```

---

8. Zprávy audit démona

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

Zobrazte neúspěšné pokusy o přihlášení:

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

Zobrazte úspěšné pokusy o přihlášení:

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

Zobrazte všechny pokusy o přihlášení:

```
# aureport -l
```

Vyhledejte neúspěšné pokusy o přihlášení během daného období:

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

Vyhledejte počet všech pokusů o ověření identity uživatele „tester“:

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

Vyhledejte informace o blokaci služby httpd SELinuxem:

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

---

9. Zprávy webového serveru Apache

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

Zobrazte 10 nejvíce požadovaných URL adres:

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

Zobrazte 10 nejčastějších návštěv podle IP adres:

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

Zobrazte celkový počet návštěv za každý měsíc seřazený podle měsíců:

```
# 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}'
```

Zobrazte počet unikátních návštěv za každý měsíc seřazený podle měsíců:

```
# 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}'
```

Zobrazte 10 nejčastějších návštěv za každý měsíc, včetně sloupcového grafu, seřazených podle měsíců:

```
# 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. Historie příkazů

(~/.bash_history)

Zobrazte historii příkazů přihlášeného uživatele:

```
$ history
```

nebo

```
$ cat $HISTFILE
```

Vymažte konkrétní záznamy z historie příkazů:

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