

Linux - practicum week 3

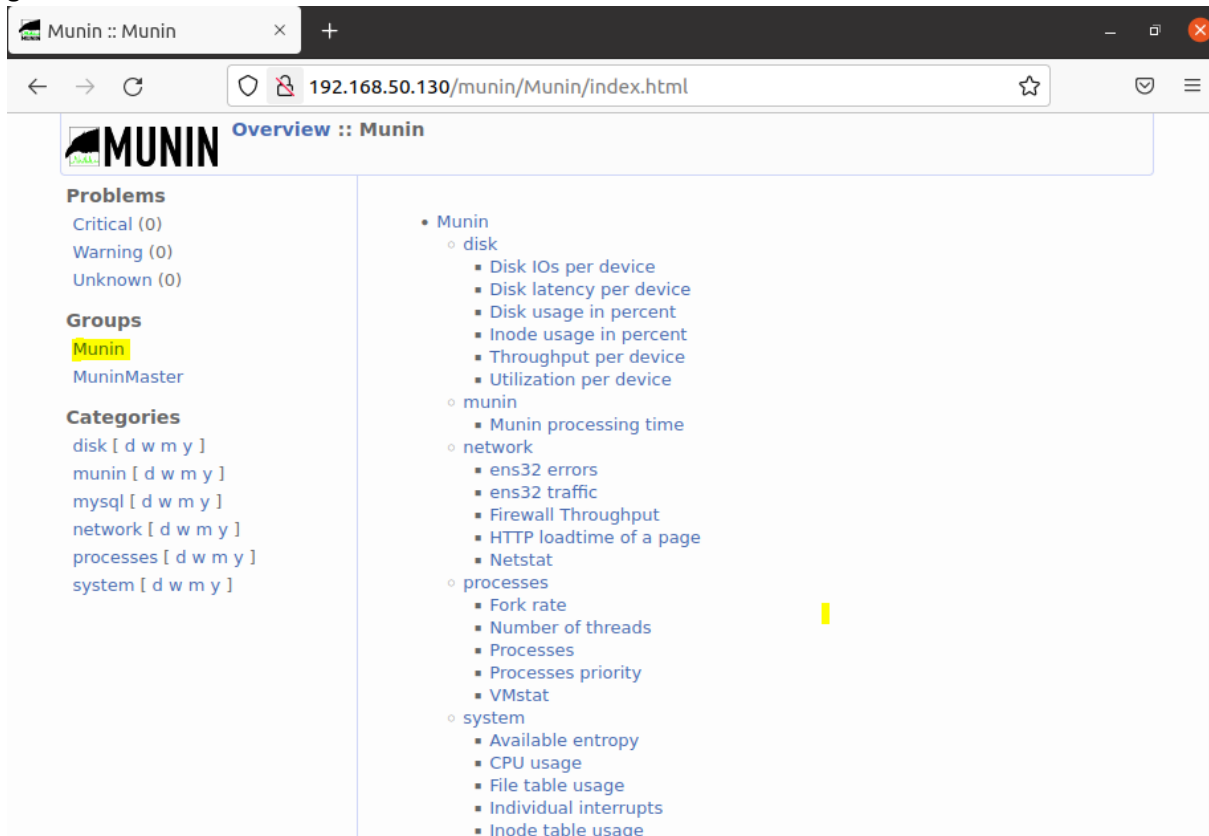
Opdracht 1: RegEx

grep -E -o "[a-zA-Z0-9+.-]{1,97}+[a-zA-Z0-9]{,1}+@shaw[.](com)(net)" acces log

Opdracht 2: monitoring en logging

A&B

gemonitord wordt.



The screenshot shows the Munin web interface at the URL 192.168.50.130/munin/Munin/index.html. The interface is titled "Overview :: Munin" and features a sidebar with navigation links for Problems, Groups, and Categories. The main content area displays a tree view of monitored metrics under the "Munin" group, including disk, munin, network, processes, and system categories. The disk category is expanded, showing sub-metrics like Disk I/Os per device, Disk latency per device, Disk usage in percent, Inode usage in percent, Throughput per device, and Utilization per device. The network category shows ens32 errors, ens32 traffic, Firewall Throughput, HTTP loadtime of a page, and Netstat. The processes category shows Fork rate, Number of threads, Processes, Processes priority, and VMstat. The system category shows Available entropy, CPU usage, File table usage, Individual interrupts, and Inode table usage.

Munin is de server die gemonitord wordt, MuninMaster is de server waar munin op draait

```
[sudo] password for davidmeer2:
Jan 14 07:20:01 ubuntu CRON[107931]: pam_unix(cron:session): session opened for user munin by (uid=0)
Jan 14 07:20:10 ubuntu CRON[107931]: pam_unix(cron:session): session closed for user munin
Jan 14 07:25:01 ubuntu CRON[108602]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 14 07:25:01 ubuntu CRON[108603]: pam_unix(cron:session): session opened for user munin by (uid=0)
Jan 14 07:25:01 ubuntu CRON[108602]: pam_unix(cron:session): session closed for user root
Jan 14 07:25:11 ubuntu CRON[108603]: pam_unix(cron:session): session closed for user munin
Jan 14 07:28:42 ubuntu gdm-password[109277]: pam_unix(gdm-password:auth): Couldn't open /etc/securetty: No such file or directory
Jan 14 07:28:44 ubuntu gdm-password[109277]: pam_unix(gdm-password:auth): Couldn't open /etc/securetty: No such file or directory
Jan 14 07:28:44 ubuntu gdm-password[109277]: gkr-pam: unlocked login keyring
Jan 14 07:29:03 ubuntu sudo[109310]: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Jan 14 07:29:06 ubuntu sudo[109310]: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Jan 14 07:29:06 ubuntu sudo[109310]: davidmeer2 : TTY=pts/2 ; PWD=/home/davidmeer2/Documents ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
Jan 14 07:29:06 ubuntu sudo[109310]: pam_unix(sudo:session): session opened for user root by (uid=0)

root@ubuntu-server:~# ls /var/log/messages_192.168.50.130
/var/log/messages_192.168.50.130
root@ubuntu-server:~# cd /var/log/messages_192.168.50.130
bash: cd: /var/log/messages_192.168.50.130: Not a directory
root@ubuntu-server:~# sudo tail -f /var/log/messages_192.168.50.130
Jan 14 07:25:01 192.168.50.130 CRON[108603]: pam_unix(cron:session): session opened for user munin by (uid=0)
Jan 14 07:25:01 192.168.50.130 CRON[108602]: pam_unix(cron:session): session closed for user root
Jan 14 07:25:11 192.168.50.130 CRON[108603]: pam_unix(cron:session): session closed for user munin
Jan 14 07:28:42 192.168.50.130 gdm-password[109277]: pam_unix(gdm-password:auth): Couldn't open /etc/securetty: No such file or directory
Jan 14 07:28:44 192.168.50.130 gdm-password[109277]: pam_unix(gdm-password:auth): Couldn't open /etc/securetty: No such file or directory
Jan 14 07:28:44 192.168.50.130 gdm-password[109277]: gkr-pam: unlocked login keyring
Jan 14 07:29:03 192.168.50.130 sudo[109310]: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Jan 14 07:29:06 192.168.50.130 sudo[109310]: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Jan 14 07:29:06 192.168.50.130 sudo[109310]: davidmeer2 : TTY=pts/2 ; PWD=/home/davidmeer2/Documents ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
Jan 14 07:29:06 192.168.50.130 sudo[109310]: pam_unix(sudo:session): session opened for user root by (uid=0)
```

Syslog-ng op Server(rechts) en client(links) met dezelfde log-files

c) Installeer op de server, die bij opdracht b gecreëerd is, Apache en/of NGNIX samen met PHP en MySQL/MariaDB. De logs van de hiervoor genoemde applicaties worden op de log server verzameld.

d) Zorg voor hardening script die de Apache Server beter beveiligd dan de standaard instellingen, bijv. via deze handleiding:

<https://geekflare.com/apache-web-server-hardening-security/>

```
#ServerTokens Minimal
ServerTokens Prod_
#ServerTokens Full

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of: On | Off | EMail
#ServerSignature Off
ServerSignature Off
```