Linux - practicum week 3

Zorg ervoor dat alle voortgang wordt bijgehouden in de Git repository.

Opdracht 1: RegEx

In de file apache-access-log.txt vind je een access-log.
Schrijf een regex die mailadressen herkent van het bedrijf “shaw”. Het bedrijf staat zowel onder de tld com en .net geregistreerd.

In de basis volgt het bedrijf Shaw de conventies van email-naamgeving van RFC 822.

Daarboven op hebben ze de volgende naamgevingssystemetiek.

- Generieke opbouw van een mailadres bij Shaw is: <mailnaam>@shaw.com of <mailnaam>@shaw.net
- Voor de <mailnaam> geldt:
    - Minimaal 2 karakters (karakter= cijfer, letter en speciale tekens), maximaal 99
    - Op laatste positie staat of een letter (“a” t/m “z” , “A” t/m “Z”), of een cijfer(“0” t/m “9”)
    - Op andere posities geen cijfers toegestaan, wel letters of de speciale tekens “.”, “_” en “-“
    - Andere speciale tekens geheel niet toegestaan

De regex kun je als volgt controleren:
grep -E -o "<YOUR_REGEX>" access_log

```
"^[a-zA-Z0-9._-]{2,99}@shaw\.(com|net)$"
```

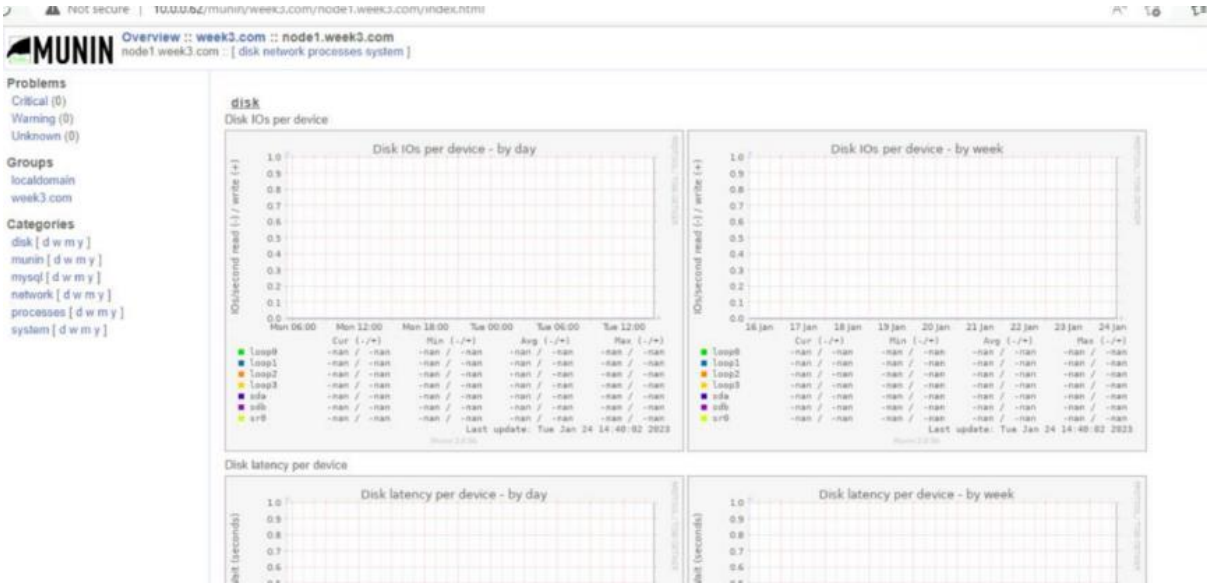
Opdracht 2: monitoring en logging

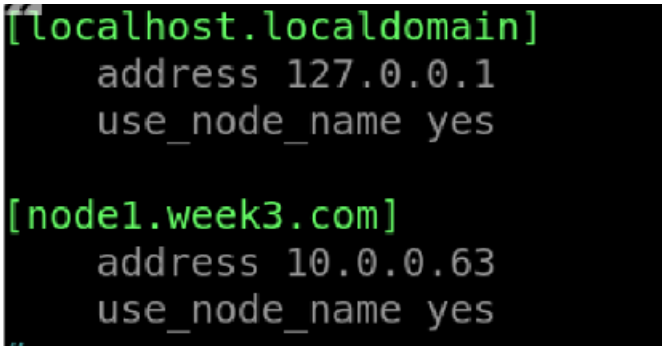
a) Zet een Linux (Ubuntu)server op die als monitor/log server kan dienen.

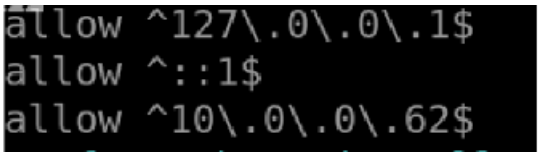
Als monitor tool kun je de volgende tools gebruiken:
Munin
Nagios
Prometheus
(andere mogen ook na overleg met docent).

Voor het opzetten van een centrale syslog server:
Syslog
Syslog NG
Elastic Stack
(andere mogen ook na overleg met docent).

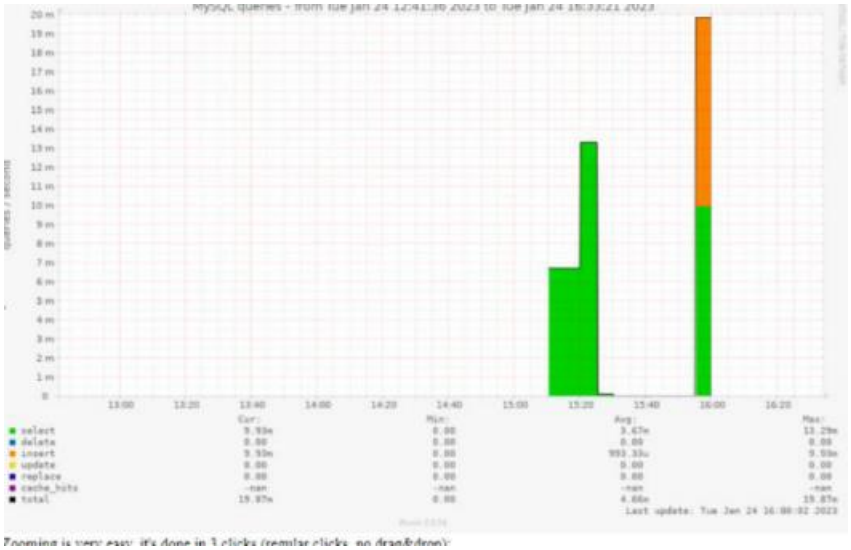
b) Zet zelf een Ubuntu Linux server op die door de vorige server (in opdracht a) gemonitord wordt.







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/

#Sayid Abd-Elaziz, ITV2G, 439378

#Schakelt slapende apache2 modules uit

sudo a2dismod status

sudo a2dismod autoindex

#Enable mod_headers

sudo a2enmod headers

Enable mod_security

sudo a2enmod security

#Set ServerSignature to Off

sudo sed -i "s/ServerSignature On/ServerSignature Off/" /etc/apache2/conf-available/security.conf

#Set ServerTokens to Prod

sudo sed -i "s/ServerTokens OS/ServerTokens Prod/" /etc/apache2/conf-available/security.con

#Disable register_globals in PHP

sudo sed -i "s/register_globals = On/register_globals = Off/" /etc/php/7.4/apache2/php.ini

#Disable expose_php in PHP

```
sudo sed -i "s/expose_php = On/expose_php = Off/" /etc/php/7.4/apache2/php.ini

sudo systemctl restart apache2
```