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

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Antwoord: \b[A-Za-z.-]{2,98}[A-Za-z0-9]@(shaw.com|shaw.net)\b

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).

**Monitor Master:**

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Service running op Master

Afbeelding met tekst, Lettertype, schermopname, zwart

Automatisch gegenereerde beschrijving

BOT-10.0.0.12 is toegevoegd als “client” in de config van Munin

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Syslogserver ingesteld op Master

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

**Monitor Bot (node)**

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Afbeelding met tekst, Lettertype, zwart, wit

Automatisch gegenereerde beschrijving

Master-Mol is toegevoegd als “Host/Server” in de config van Munin

**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.

**Antwoord:**

In deze screenshot kan je bewijs vinden uit de syslog logfile op de “Master” VM. Logs zijn gestuurd door BOT-404485 (verzamelbestand van alle logs)

Afbeelding met tekst, schermopname, zwart, zwart-wit

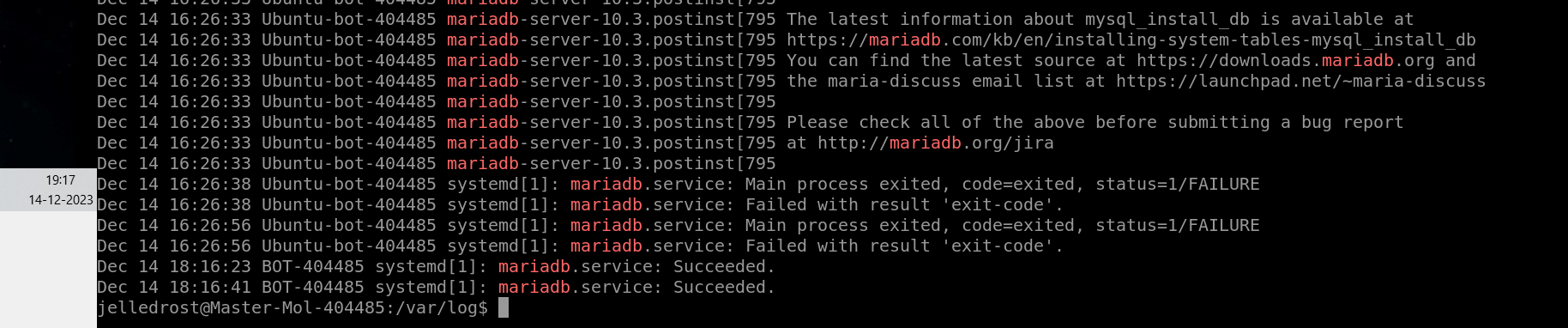
Automatisch gegenereerde beschrijving

Apache2

Afbeelding met tekst, schermopname

Automatisch gegenereerde beschrijving

MariaDB (zitten ook logs bij van vorige VM)



**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/>

#!/bin/bash

# Maak een back-up van de originele configuratiebestanden

cp /etc/apache2/apache2.conf /etc/apache2/apache2.conf.backup

cp /etc/apache2/conf-available/security.conf /etc/apache2/conf-available/security.conf.backup

# Zet ServerTokens en ServerSignature op minimaal

sed -i '/^ServerTokens/s/.\*/ServerTokens Prod/' /etc/apache2/apache2.conf

sed -i '/^ServerSignature/s/.\*/ServerSignature Off/' /etc/apache2/apache2.conf

# Activeer mod\_security en mod\_evasive

sudo a2enmod security2 evasive

# Configureer beveiligingsheaders

echo "Header always set X-Frame-Options DENY" >> /etc/apache2/apache2.conf

echo "Header always set X-XSS-Protection \"1; mode=block\"" >> /etc/apache2/apache2.conf

echo "Header always set X-Content-Type-Options nosniff" >> /etc/apache2/apache2.conf

echo "Header always set Referrer-Policy \"no-referrer-when-downgrade\"" >> /etc/apache2/apache2.conf

# Schakel directorylijsten uit

echo "Options -Indexes" > /var/www/html/.htaccess

# Beperk toegang tot gevoelige bestanden

echo "<FilesMatch \"(\\.htaccess|\\.htpasswd|config\\.php)\">" >> /etc/apache2/apache2.conf

echo " Require all denied" >> /etc/apache2/apache2.conf

echo "</FilesMatch>" >> /etc/apache2/apache2.conf

# Herstart Apache na het aanbrengen van wijzigingen

sudo systemctl restart apache2