Homework_Lesson 12

Описание задачи:
У вас есть лог-файл, имитирующий логи сервера.
Необходимо извлечь все IP-адреса, с которых произошел успешный вход (код ответа 200). Также извлечь все уникальные пользователи (usernames), которые пытались авторизоваться, но получили ошибку (код ответа 403).

2024-11-26 12:30:15 [INFO] user=johndoe ip=192.168.1.10 status=200
2024-11-26 12:31:03 [INFO] user=alice ip=10.0.0.5 status=403
2024-11-26 12:35:42 [INFO] user=bob ip=172.16.0.1 status=200
2024-11-26 12:36:00 [INFO] user=johndoe ip=192.168.1.10 status=403
2024-11-26 12:40:22 [INFO] user=charlie ip=10.0.0.8 status=403
2024-11-26 12:42:10 [INFO] user=alice ip=10.0.0.5 status=200

Инструкция к выполнению:
Скачайте лог-файл (или создайте его на основе примера выше).

Напишите Bash-скрипт, который:
Находит все IP-адреса с кодом статуса 200.
Находит всех уникальных пользователей, у которых был статус 403.
Пример вывода Bash-скрипта:

Successful logins (IP addresses):
192.168.1.10
172.16.0.1
10.0.0.5

Users with failed logins:
johndoe
alice
charlie

Код генерации логов:

```
#!/bin/bash
# Генерация лог-файла
LOGFILE="server.log"
echo "2024-11-26 12:30:15 [INFO] user=johndoe ip=192.168.1.10 status=200" > $LOGFILE
echo "2024-11-26 12:31:03 [INFO] user=alice ip=10.0.0.5 status=403" >> $LOGFILE
echo "2024-11-26 12:35:42 [INFO] user=bob ip=172.16.0.1 status=200" >> $LOGFILE
echo "2024-11-26 12:36:00 [INFO] user=johndoe ip=192.168.1.10 status=403" >> $LOGFILE
echo "2024-11-26 12:40:22 [INFO] user=charlie ip=10.0.0.8 status=403" >> $LOGFILE
echo "2024-11-26 12:42:10 [INFO] user=alice ip=10.0.0.5 status=200" >> $LOGFILE
```

Создадим директорию и скрипт с данными из примера

```
14:58:00  227  ~  mkdir hw12
mkdir: created directory 'hw12'
14:58:52  228  ~  cd hw12
/home/sttewie/hw12
14:58:56  229  hw12  nano generate_log.sh
```

```
#!/bin/bash
# Генерация лог-файла
LOGFILE="server.log"
echo "2024-11-26 12:30:15 [INFO] user=johndoe ip=192.168.1.10 status=200" > $LOGFILE
echo "2024-11-26 12:31:03 [INFO] user=alice ip=10.0.0.5 status=403" >> $LOGFILE
echo "2024-11-26 12:35:42 [INFO] user=bob ip=172.16.0.1 status=200" >> $LOGFILE
echo "2024-11-26 12:36:00 [INFO] user=johndoe ip=192.168.1.10 status=403" >> $LOGFILE
echo "2024-11-26 12:40:22 [INFO] user=charlie ip=10.0.0.8 status=403" >> $LOGFILE
echo "2024-11-26 12:42:10 [INFO] user=alice ip=10.0.0.5 status=200" >> $LOGFILE
```

Запустим скрипт для генерации лог-файла, это создаст файл server.log с содержимым:

```
15:38:55  232  hw12  ls -l
total 8
-rwxrwxr-x 1 sttewie sttewie 565 Dec  6 14:59 generate_log.sh
-rw-rw-r-- 1 sttewie sttewie 380 Dec  6 15:38 server.log
15:41:13  217  hw12  cat server.log
2024-11-26 12:30:15 [INFO] user=johndoe ip=192.168.1.10 status=200
2024-11-26 12:31:03 [INFO] user=alice ip=10.0.0.5 status=403
2024-11-26 12:35:42 [INFO] user=bob ip=172.16.0.1 status=200
2024-11-26 12:36:00 [INFO] user=johndoe ip=192.168.1.10 status=403
2024-11-26 12:40:22 [INFO] user=charlie ip=10.0.0.8 status=403
2024-11-26 12:42:10 [INFO] user=alice ip=10.0.0.5 status=200
```

Теперь, когда у нас есть лог-файл, мы напишем скрипт, который извлечет нужную информацию.

nano analyze_logs.sh

```
#!/bin/bash

# Указываем путь к лог-файлу
LOGFILE="server.log"

# Извлекаем все IP-адреса с кодом ответа 200
echo "Successful logins (IP addresses):"
grep "status=200" $LOGFILE | awk -F "ip=" '{print $2}' | awk -F " status" '{print $1}' | sort | uniq

# Извлекаем всех уникальных пользователей с кодом ответа 403
echo
echo "Users with failed logins:"
grep "status=403" $LOGFILE | awk -F "user=" '{print $2}' | awk -F " ip=" '{print $1}' | sort | uniq
```

- grep "status=200" $LOGFILE: Этот командой мы находим все строки в логах, где статус равен 200 (успешный вход).
- awk -F "ip=" '{print $2}': Используется для извлечения IP-адреса после ip=.
- awk -F " status" '{print $1}': Разделяет строку до статуса, чтобы получить только IP-адрес.
- sort | uniq: Сортирует и удаляет дублирующиеся значения, оставляя только уникальные IP-адреса.

Для обработки неудачных логинов (статус 403), мы используем аналогичный подход:

- grep "status=403" $LOGFILE: Находит строки с ошибкой 403.
- awk -F "user=" '{print $2}': Извлекает имя пользователя после user=.
- awk -F " ip=" '{print $1}': Разделяет строку на имя пользователя, получая только имя.
- sort | uniq: Сортирует и удаляет дубли, оставляя уникальные имена пользователей.

Запускаем скрипт ./analyze_logs.sh

Результат

```
15:54:29  221  hw12  ./analyze_logs.sh
Successful logins (IP addresses):
10.0.0.5
172.16.0.1
192.168.1.10

Users with failed logins:
alice
charlie
johndoe
```