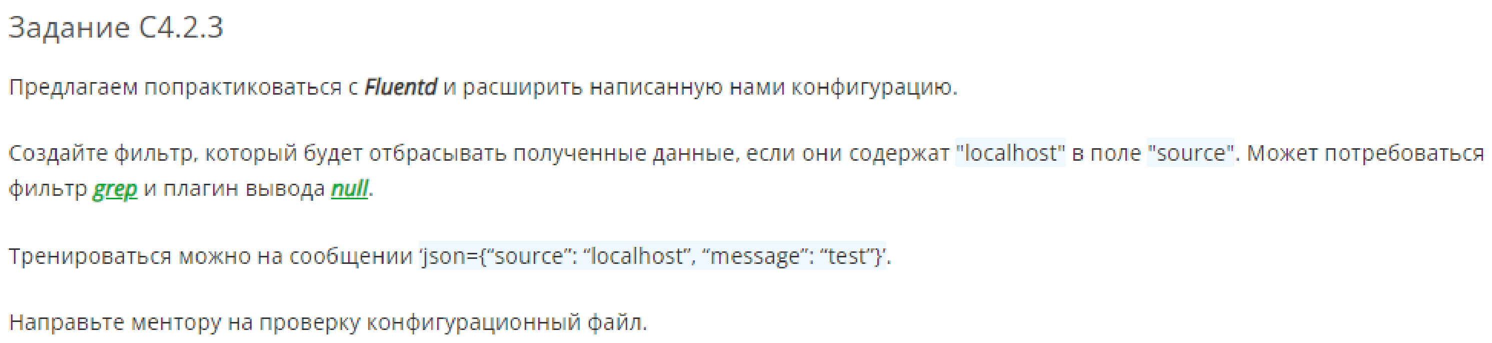
Module C4 Practical Work Report



Задание C4.2.3

Предлагаем попрактиковаться с ***Fluentd*** и расширить написанную нами конфигурацию.

Создайте фильтр, который будет отбрасывать полученные данные, если они содержат "localhost" в поле "source". Может потребоваться фильтр ***grep*** и плагин вывода ***null***.

Тренироваться можно на сообщении ‘json={“source”: “localhost”, “message”: “test”}’.

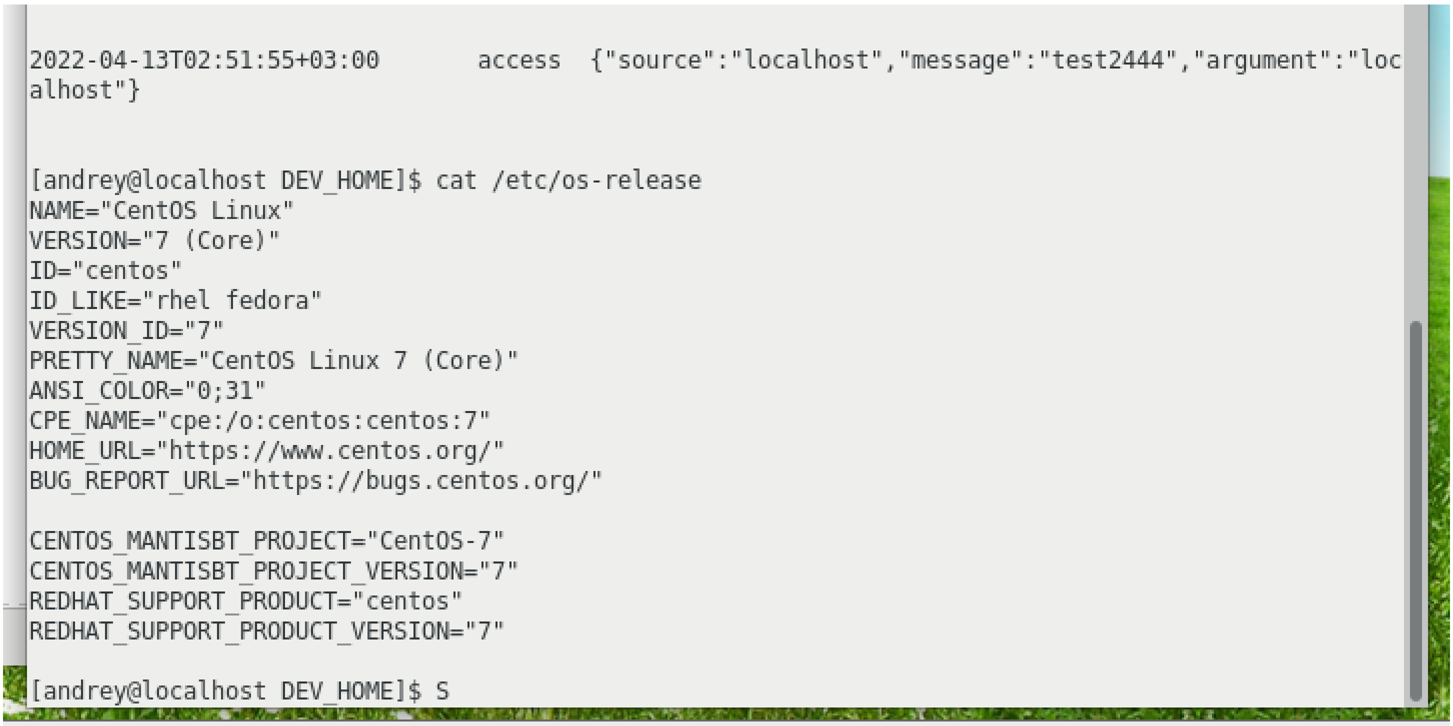
Направьте ментору на проверку конфигурационный файл.

andreys_fluentd.sh

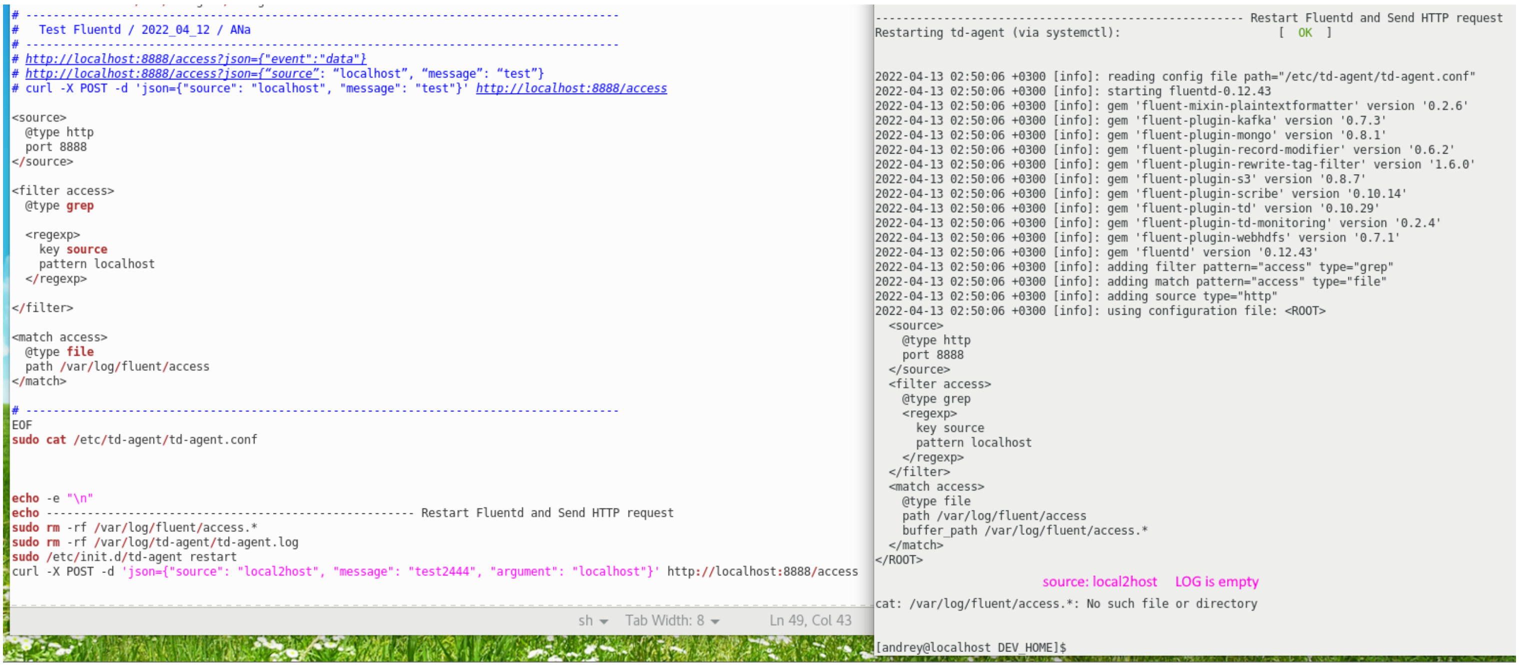
```
#!/bin/sh
# ---------------------------------------------------------------------------------------
#   Test Fluentd Image with Docker / 2022_04_12 / ANa
# ---------------------------------------------------------------------------------------

echo -e "\n"
echo ------------------------------------------------------ Updating /etc/td-agent/td-agent.conf
echo -e "\n"
sudo rm -rf /etc/td-agent/td-agent.conf
sudo touch /etc/td-agent/td-agent.conf
sudo chmod 777 /etc/td-agent/td-agent.conf
sudo cat << EOF > /etc/td-agent/td-agent.conf
# ---------------------------------------------------------------------------------------
#   Test Fluentd / 2022_04_12 / ANa
# ---------------------------------------------------------------------------------------
# http://localhost:8888/access?json={"event":"data"}
# http://localhost:8888/access?json={“source”: “localhost”, “message”: “test”}
# curl -X POST -d 'json={"source": "localhost", "message": "test"}' http://localhost:8888/access

<source>
  @type http
  port 8888
</source>

<filter access>
  @type grep

  <regexp>
    key source
    pattern localhost
  </regexp>

</filter>

<match access>
  @type file
  path /var/log/fluent/access
</match>

# ---------------------------------------------------------------------------------------
EOF
sudo cat /etc/td-agent/td-agent.conf
```

```
echo -e "\n"
echo ------------------------------------------------------ Restart Fluentd and Send HTTP request
sudo rm -rf /var/log/fluent/access.*
sudo rm -rf /var/log/td-agent/td-agent.log
sudo /etc/init.d/td-agent restart
curl -X POST -d 'json={"source": "local2host", "message": "test2444", "argument": "localhost"}' http://localhost:8888/access


echo -e "\n"
sudo cat /var/log/td-agent/td-agent.log
echo -e "\n"
sudo cat /var/log/fluent/access.*
echo -e "\n"
```

Result



```
2022-04-13T02:51:55+03:00       access  {"source":"localhost","message":"test2444","argument":"loc
alhost"}


[andrey@localhost DEV_HOME]$ cat /etc/os-release
NAME="CentOS Linux"
VERSION="7 (Core)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="7"
PRETTY_NAME="CentOS Linux 7 (Core)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:centos:centos:7"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"

CENTOS_MANTISBT_PROJECT="CentOS-7"
CENTOS_MANTISBT_PROJECT_VERSION="7"
REDHAT_SUPPORT_PRODUCT="centos"
REDHAT_SUPPORT_PRODUCT_VERSION="7"

[andrey@localhost DEV_HOME]$ S
```

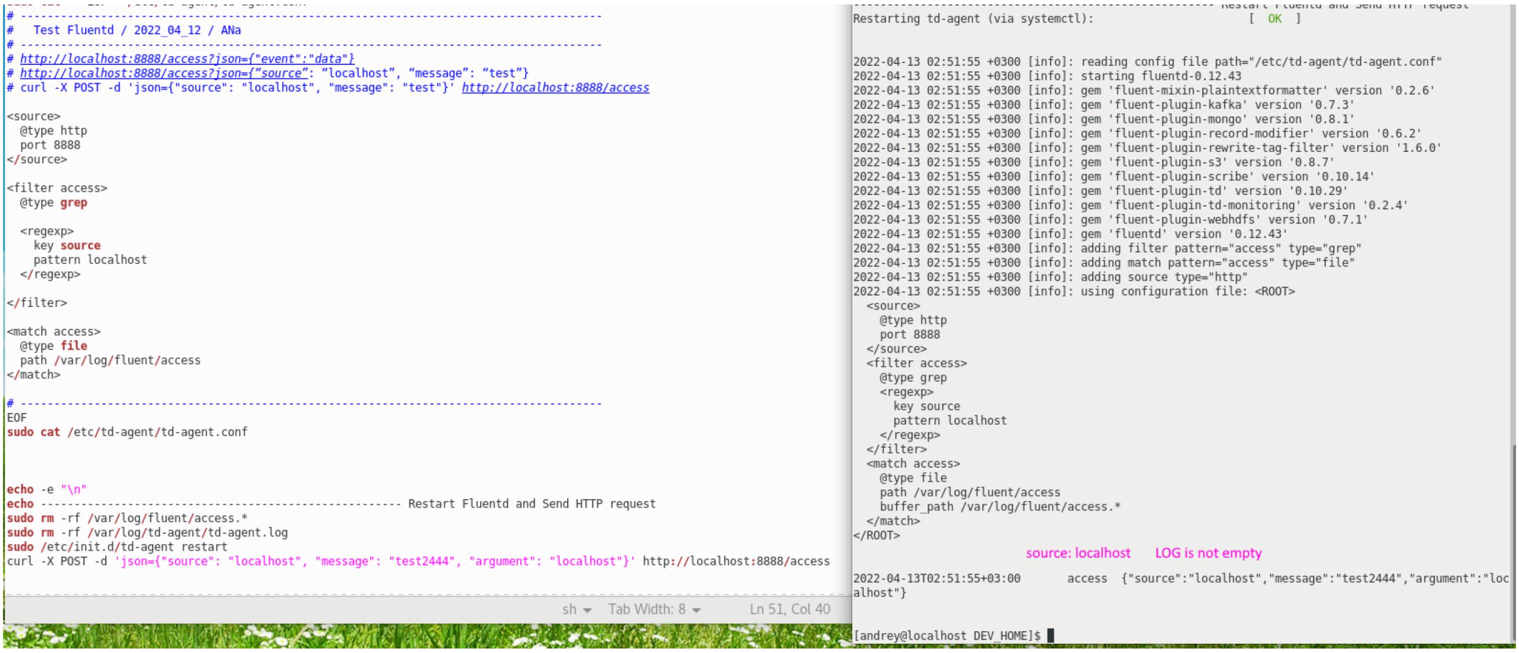


```
# ------------------------------------------------------------------------------------
#   Test Fluentd / 2022_04_12 / ANa
# ------------------------------------------------------------------------------------
# http://localhost:8888/access?json={"event":"data"}
# http://localhost:8888/access?json={“source”: “localhost”, “message”: “test”}
# curl -X POST -d 'json={"source": "localhost", "message": "test"}' http://localhost:8888/access

<source>
  @type http
  port 8888
</source>

<filter access>
  @type grep

  <regexp>
    key source
    pattern localhost
  </regexp>

</filter>

<match access>
  @type file
  path /var/log/fluent/access
</match>

# ------------------------------------------------------------------------------------
EOF
sudo cat /etc/td-agent/td-agent.conf



echo -e "\n"
echo --------------------------------------------------------- Restart Fluentd and Send HTTP request
sudo rm -rf /var/log/fluent/access.*
sudo rm -rf /var/log/td-agent/td-agent.log
sudo /etc/init.d/td-agent restart
curl -X POST -d 'json={"source": "local2host", "message": "test2444", "argument": "localhost"}' http://localhost:8888/access
```

```
------------------------------------------------------ Restart Fluentd and Send HTTP request
Restarting td-agent (via systemctl):                       [  OK  ]


2022-04-13 02:50:06 +0300 [info]: reading config file path="/etc/td-agent/td-agent.conf"
2022-04-13 02:50:06 +0300 [info]: starting fluentd-0.12.43
2022-04-13 02:50:06 +0300 [info]: gem 'fluent-mixin-plaintextformatter' version '0.2.6'
2022-04-13 02:50:06 +0300 [info]: gem 'fluent-plugin-kafka' version '0.7.3'
2022-04-13 02:50:06 +0300 [info]: gem 'fluent-plugin-mongo' version '0.8.1'
2022-04-13 02:50:06 +0300 [info]: gem 'fluent-plugin-record-modifier' version '0.6.2'
2022-04-13 02:50:06 +0300 [info]: gem 'fluent-plugin-rewrite-tag-filter' version '1.6.0'
2022-04-13 02:50:06 +0300 [info]: gem 'fluent-plugin-s3' version '0.8.7'
2022-04-13 02:50:06 +0300 [info]: gem 'fluent-plugin-scribe' version '0.10.14'
2022-04-13 02:50:06 +0300 [info]: gem 'fluent-plugin-td' version '0.10.29'
2022-04-13 02:50:06 +0300 [info]: gem 'fluent-plugin-td-monitoring' version '0.2.4'
2022-04-13 02:50:06 +0300 [info]: gem 'fluent-plugin-webhdfs' version '0.7.1'
2022-04-13 02:50:06 +0300 [info]: gem 'fluentd' version '0.12.43'
2022-04-13 02:50:06 +0300 [info]: adding filter pattern="access" type="grep"
2022-04-13 02:50:06 +0300 [info]: adding match pattern="access" type="file"
2022-04-13 02:50:06 +0300 [info]: adding source type="http"
2022-04-13 02:50:06 +0300 [info]: using configuration file: <ROOT>
  <source>
    @type http
    port 8888
  </source>
  <filter access>
    @type grep
    <regexp>
      key source
      pattern localhost
    </regexp>
  </filter>
  <match access>
    @type file
    path /var/log/fluent/access
    buffer_path /var/log/fluent/access.*
  </match>
</ROOT>
```

source: local2host   LOG is empty

```
cat: /var/log/fluent/access.*: No such file or directory

[andrey@localhost DEV_HOME]$
```



```
# ------------------------------------------------------------------------------------
#   Test Fluentd / 2022_04_12 / ANa
# ------------------------------------------------------------------------------------
# http://localhost:8888/access?json={"event":"data"}
# http://localhost:8888/access?json={“source”: “localhost”, “message”: “test”}
# curl -X POST -d 'json={"source": "localhost", "message": "test"}' http://localhost:8888/access

<source>
  @type http
  port 8888
</source>

<filter access>
  @type grep

  <regexp>
    key source
    pattern localhost
  </regexp>

</filter>

<match access>
  @type file
  path /var/log/fluent/access
</match>

# ------------------------------------------------------------------------------------
EOF
sudo cat /etc/td-agent/td-agent.conf



echo -e "\n"
echo --------------------------------------------------------- Restart Fluentd and Send HTTP request
sudo rm -rf /var/log/fluent/access.*
sudo rm -rf /var/log/td-agent/td-agent.log
sudo /etc/init.d/td-agent restart
curl -X POST -d 'json={"source": "localhost", "message": "test2444", "argument": "localhost"}' http://localhost:8888/access
```

```
Restarting td-agent (via systemctl):                       [  OK  ]


2022-04-13 02:51:55 +0300 [info]: reading config file path="/etc/td-agent/td-agent.conf"
2022-04-13 02:51:55 +0300 [info]: starting fluentd-0.12.43
2022-04-13 02:51:55 +0300 [info]: gem 'fluent-mixin-plaintextformatter' version '0.2.6'
2022-04-13 02:51:55 +0300 [info]: gem 'fluent-plugin-kafka' version '0.7.3'
2022-04-13 02:51:55 +0300 [info]: gem 'fluent-plugin-mongo' version '0.8.1'
2022-04-13 02:51:55 +0300 [info]: gem 'fluent-plugin-record-modifier' version '0.6.2'
2022-04-13 02:51:55 +0300 [info]: gem 'fluent-plugin-rewrite-tag-filter' version '1.6.0'
2022-04-13 02:51:55 +0300 [info]: gem 'fluent-plugin-s3' version '0.8.7'
2022-04-13 02:51:55 +0300 [info]: gem 'fluent-plugin-scribe' version '0.10.14'
2022-04-13 02:51:55 +0300 [info]: gem 'fluent-plugin-td' version '0.10.29'
2022-04-13 02:51:55 +0300 [info]: gem 'fluent-plugin-td-monitoring' version '0.2.4'
2022-04-13 02:51:55 +0300 [info]: gem 'fluent-plugin-webhdfs' version '0.7.1'
2022-04-13 02:51:55 +0300 [info]: gem 'fluentd' version '0.12.43'
2022-04-13 02:51:55 +0300 [info]: adding filter pattern="access" type="grep"
2022-04-13 02:51:55 +0300 [info]: adding match pattern="access" type="file"
2022-04-13 02:51:55 +0300 [info]: adding source type="http"
2022-04-13 02:51:55 +0300 [info]: using configuration file: <ROOT>
  <source>
    @type http
    port 8888
  </source>
  <filter access>
    @type grep
    <regexp>
      key source
      pattern localhost
    </regexp>
  </filter>
  <match access>
    @type file
    path /var/log/fluent/access
    buffer_path /var/log/fluent/access.*
  </match>
</ROOT>
```

source: localhost   LOG is not empty

```
2022-04-13T02:51:55+03:00       access  {"source":"localhost","message":"test2444","argument":"loc
alhost"}

[andrey@localhost DEV_HOME]$
```