Consuming logs and statistics (debian 10)

Links ..

Fluentbit: https://fluentbit.io

Fluentd: https://fluentd.org

Fluentbit documentation: https://fluentbit.io/documentation/0.12/

Graylog: https://www.graylog.org/products/open-source

Grafana: https://grafana.com/oss

Create the Graylog server using debian 10. Replace 192.168.1.114 with your Graylog server IP below and pay attention to the echos:

```
# graylog server on deb10
apt-get update && apt-get upgrade -y
apt-get install apt-transport-https openjdk-11-jre-headless uuid-runtime pwgen dirmngr curl
apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv 4B7C549A058F8B6B
echo "deb http://repo.mongodb.org/apt/debian buster/mongodb-org/4.2 main" | tee /etc/apt/sources.list.d/mongodb-org-4.2.list
apt-get update && apt-get install mongodb-org -y
systemctl daemon-reload
systemctl enable mongod.service
systemctl restart mongod.service
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
echo "deb https://artifacts.elastic.co/packages/oss-6.x/apt stable main" | tee -a /etc/apt/sources.list.d/elastic-6.x.list
apt-get update && apt-get install elasticsearch-oss -y
echo "cluster.name: graylog" >> /etc/elasticsearch/elasticsearch.yml
echo "action.auto_create_index: false" >> /etc/elasticsearch/elasticsearch.yml
systemctl daemon-reload
systemctl enable elasticsearch.service
systemctl restart elasticsearch.service
wget https://packages.graylog2.org/repo/packages/graylog-3.1-repository_latest.deb
dpkg -i graylog-3.1-repository_latest.deb
apt-get update && apt-get install graylog-server -y
echo "for admin password as password and hash edit /etc/graylog/server/server.conf and set..."
echo "password_secret = naln41C22HRxw3hy9mJ8bipFWBo1aewKFgtXDXp22dNjNJNqEtid6uC0476zIfX5iQ3mZuRp9y7h3XcNY63inPo6vJy7FuLP"
echo "root_password_sha2 = 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8"
echo "http_bind_address = 192.168.1.114:9000"
echo "http_publish_uri = http://192.168.1.114:9000"
systemctl enable graylog-server.service
systemctl start graylog-server.service
```

graylog webui should be up on http://192.168.1.114:9000 now. create a GELF UDP input using the default port 12201.

```
# add fluentd on graylog server
apt-get install sudo ntp ntpdate ntpstat ruby-gelf
curl -L https://toolbelt.treasuredata.com/sh/install-debian-buster-td-agent3.sh
systemctl daemon-reload
systemctl enable td-agent
td-agent-gem install gelf
cd /etc/td-agent/plugin
wget https://raw.githubusercontent.com/emsearcy/fluent-plugin-gelf/master/lib/fluent/plugin/out_gelf.rb
cd ../
```

Append to /etc/td-agent/td-agent.conf ...

```
<source>
type syslog
tag hostname_goes_here
</source>
<match *.*>
type copy
<store>
type gelf
host 0.0.0.0
port 12201
flush_interval 5s
</store>
<store>
type stdout
</store>
</match>
```

```
systemctl restart td-agent
```

systemctl enable td-agent

Next steps to be executed on the sipXcom or Uniteme server(s). Replace 192.168.2.14 with your sipxcom or uniteme server IP, and replace 192.168.1.114 with your graylog server IP on the last output.

fluentbit on sipx/uniteme centos7
cd /etc/yum.repos.d/
nano fluentbit.repo

[fluentbit]
name = fluentbit
baseurl = http://packages.fluentbit.io/centos/7
gpgcheck=1
gpgkey=http://packages.fluentbit.io/fluentbit.key
enabled=1

yum update
yum install td-agent-bit -y
mv /etc/td-agent-bit/td-agent-bit.conf ~/td-agent-bit.conf.orig
nano /etc/td-agent-bit/td-agent-bit.conf

[SERVICE]
Flush 5
Parsers_File parsers.conf
Plugins_File plugins.conf

[INPUT]
Name cpu
Tag cpu.local
Interval_Sec 1

[INPUT]
Name mem
Tag memory

[INPUT]
Name disk
Tag disk.local
Interval_Sec 1

[INPUT]
Name netif
Tag netif.eth0
Interval_Sec 1
Interface eth0

[INPUT]
Name tail
Path /var/log/sipxpbx/proxy_stats.json
Refresh_Interval 1
Parser json

[INPUT]
Name tail
Path /var/log/sipxpbx/sipXproxy.log
Refresh_Interval 1
Skip_Long_Lines off
Multiline On
Multiline_Flush 25
Parser_Firstline syslog-rfc5424
Buffer_Chunk_Size 1M
Buffer_Max_Size 1G

[OUTPUT]
Name forward
Match *
Host 192.168.1.12
Port 24224

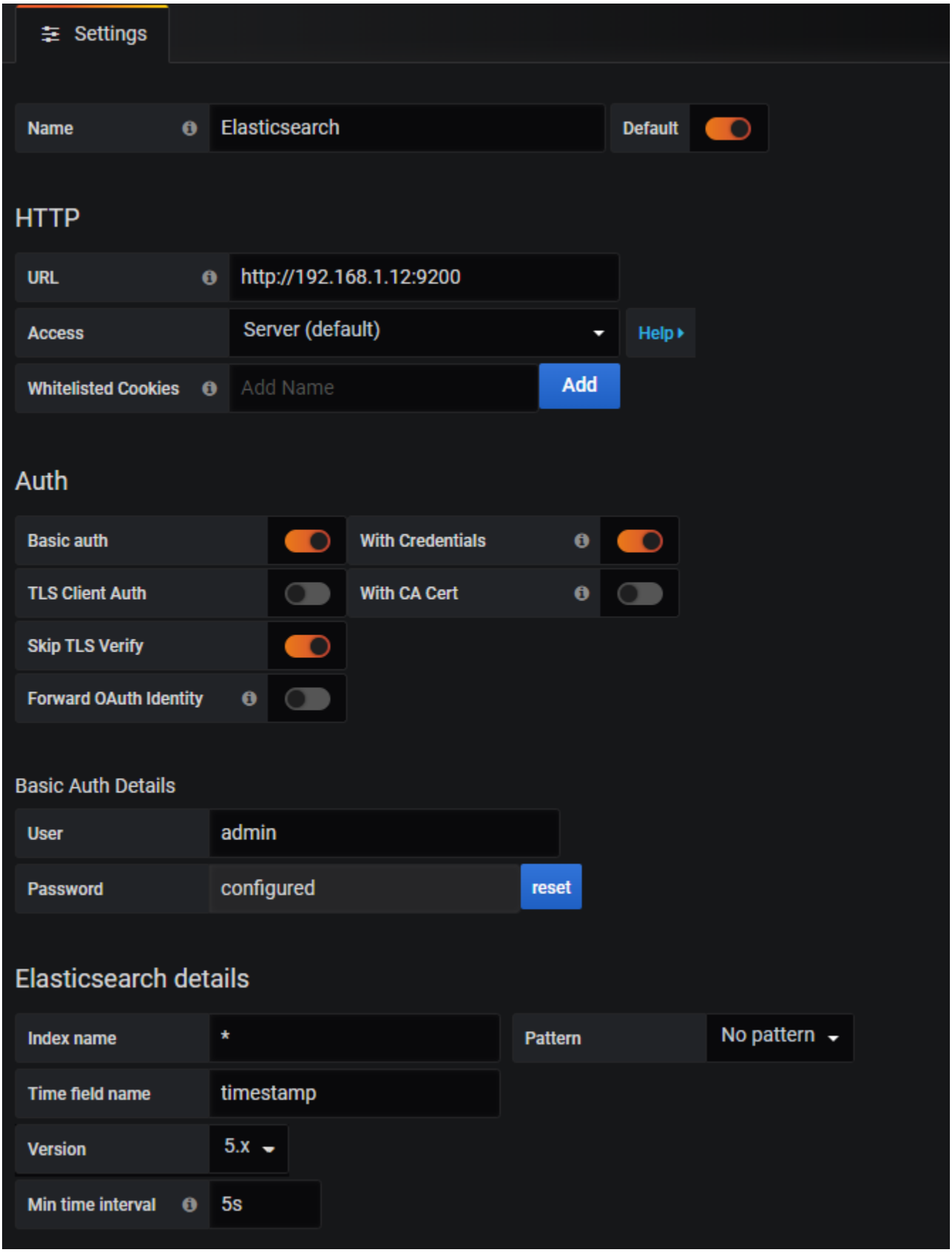
service td-agent-bit restart

systemctl enable td-agent-bit

Grafana on deb10

```
echo "deb https://packages.grafana.com/oss/deb stable main" > /etc/apt/sources.list.d/grafana.list
apt-get install apt-transport-https gnupg2 -y
wget -q -O - https://packages.grafana.com/gpg.key | apt-key add -
apt-get update
apt-get install grafana
```

You may need to edit /etc/grafana/grafana.ini to set the address to bind to. Grafana can use the Elasticsearch input to connect to the Graylog server.



The graylog /etc/elasticsearch/elasticsearch.yml will need to be adjusted to listen to the ip and port 9200 and restarted before this will work.

root@graylog2:/etc/elasticsearch# grep -v "#" elasticsearch.yml
path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch
network.host: 192.168.1.12
http.port: 9200
discovery.zen.ping.unicast.hosts: ["192.168.1.12", "127.0.0.1"]

cluster.name: graylog
action.auto_create_index: false

Also edit /etc/graylog/server/server.conf and point to the elasticsearch ip instead of the localhost ip, then restart graylog

root@graylog2:/etc/graylog/server# grep "192.168.1.12:9200" server.conf
elasticsearch_hosts = http://192.168.1.12:9200