Fluentd voor elasticsearch op CentOS 7

Deze handleiding gaat er van uit dat Fluentd op een server wordt waarop ook Elasticsearch is geïnstalleerd volgens deze handleiding.

Prerequisites

File descriptors

Het maximum aantal open files per proces staat default op 1024 wat voor de meeste installaties prima is. echter fluentd moet er meer open kunnen hebben.

check de huidige settings met `ulimit -n`

pas de settings aan door:`vi /etc/security/limits.conf`

en toe te voegen voor `# End of file`:

```
root soft nofile 65536
root hard nofile 65536
* soft nofile 65536
* hard nofile 65536
```

Installatie van fluentd

installeer ruby:
`yum install ruby ruby-devel rubygems gcc`

En gebruik vervolgens de ruby installer om fluentd te installeren:
`gem install fluentd -v "~> 0.12.27" --no-ri --no-rdoc`

configuratie file

Maak de configuratie file aan:

```
mkdir /etc/td-agent
vi /etc/td-agent/td-agent.conf
```

en zet hier in:

systemd start stop configuratie

Omdat we niet uit een repository hebben geinstalleerd moeten we met de hand een systemd configuratie maken voor fluentd.

---

andere methode

Deze methode wordt op de fluentd website aanbevolen.

Het shell script installeert een repository en tegelijk `td-agent`:

```
curl -L https://toolbelt.treasuredata.com/sh/install-redhat-td-agent2.sh | sh
```

configuratie

```
vi /etc/td-agent/td-agent.conf
```

en zet hier in:

```
####
## Output descriptions:
###

## match tag=debug.** and dump to console
<match debug.**>
  type stdout
</match>

####
## Source descriptions:
##

## built-in TCP input
## @see http://docs.fluentd.org/articles/in_forward
<source>
  type forward
</source>

## built-in UNIX socket input
#<source>
#  type unix
#</source>

# HTTP input
# POST http://localhost:8888/<tag>?json=<json>
# POST http://localhost:8888/td.myapp.login?json={"user"%3A"me"}
# @see http://docs.fluentd.org/articles/in_http
<source>
  type http
```

```
  port 8888
</source>

## live debugging agent
<source>
  type debug_agent
  bind 127.0.0.1
  port 24230
</source>

####
## Examples:
##

## File input
## read apache logs continuously and tags td.apache.access
#<source>
#  type tail
#  format apache
#  path /var/log/httpd-access.log
#  tag td.apache.access
#</source>

## File output
## match tag=local.** and write to file
#<match local.**>
#  type file
#  path /var/log/td-agent/access
#</match>

## Forwarding
## match tag=system.** and forward to another td-agent server
#<match system.**>
#  type forward
#  host 192.168.0.11
#  # secondary host is optional
#  <secondary>
#    host 192.168.0.12
#  </secondary>
#</match>

## Multiple output
## match tag=td.*.* and output to Treasure Data AND file
#<match td.*.*>
#  type copy
#  <store>
#    type tdlog
#    apikey API_KEY
#    auto_create_table
#    buffer_type file
#    buffer_path /var/log/td-agent/buffer/td
```

```
#  </store>
#  <store>
#    type file
#    path /var/log/td-agent/td-%Y-%m-%d/%H.log
#  </store>
#</match>

###SNMP gedeelte
###

##SNMP waarden als input

# netwerk

<source>
  type snmp
  tag snmp.server3
  nodes name, value
  host "xxx.xxx.xxx.xxx {Router IP}"
  community public
  mib ifInOctets.7
  method_type get
  polling_time 5
  polling_type async_run
</source>

<source>
  type snmp
  tag snmp.server4
  nodes name, value
  host "xxx.xxx.xxx.xxx {Router IP}"
  community public
  mib ifOutOctets.7
  method_type get
  polling_time 5
  polling_type async_run
</source>


##output naar Elasticsearch

<match snmp.server*>
  type copy

  <store>
    type derive
    add_tag_prefix derive
    key2 value *8
  </store>

  <store>
```

```
    type stdout
  </store>

  <store>
    type elasticsearch
    host localhost
    port 9200
    type_name traffic
    logstash_format true
    logstash_prefix snmp
    logstash_dateformat %Y%m

    buffer_type memory
    buffer_chunk_limit 10m
    buffer_queue_limit 10
    flush_interval 1s
    retry_limit 16
    retry_wait 1s
  </store>
</match>
```

Bronnen

http://docs.fluentd.org/articles/install-by-gem

http://docs.fluentd.org/articles/install-by-rpm

https://translate.google.nl/translate?hl=nl&sl=ja&tl=en&u=http%3A%2F%2Fqiita.com%2Fapresia%2Fitems%2Fe46f7d72f14e570413d7

https://neverendingsecurity.wordpress.com/2015/04/13/open-source-log-visualization-with-elasticsearch-fluentd-and-kibana/

https://github.com/centos-opstools/opstools-doc/blob/master/centralised-logging.txt

https://translate.google.nl/translate?hl=nl&sl=ja&tl=en&u=http%3A%2F%2Fblog.nomadscafe.jp%2F2014%2F03%2Fdstat-fluentd-elasticsearch-kibana.html

http://www.elasticmining.com/post/2016-01-09/using-fluentd-to-collect-logs.html