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`

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`

Bronnen

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%2F

items%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