Filebeat Data overdracht herstarten vanaf een eerder moment

Er zijn situaties waar een misconfiguratie in logstash, het per ongeluk uitstaan van logstash of een corruptie in de elasticsearch data het nodig maken om log data, vanaf een bepaalde dag, opnieuw naar de ELK server te krijgen.

Voorbereiding

stop filebeat op de betreffende clients. log in alle betreffende nodes en doe:
`service filebeat stop`

stop logstash op de ELK server. log in op de ELK server en doe:
`service logstash stop`

Elasticsearch cleanup

Als er een parsefout is opgetreden of als er partial data is moeten de betreffende indices verwijderd worden in Elasticsearch.

log in op de Elasticsearch node en vindt de index , list all indices: `curl 'localhost:9200/_cat/indices?v`

verwijder de index door: `curl -XDELETE 'localhost:9200/indexnaam'`

filebeat cliënt datum reset

De filebeat cliënt houdt in een registry bij welke files er al ge-parced zijn. Door de entry van de laatste dagen weg te gooien laat je filebeat geloven dat die nog niet verwerkt zijn.

`vi /var/lib/filebeat/registry`

Helaas zitten er geen line returns in deze file dus is de file wat lastig leesbaar:

```
(https://www.dokuwiki.org/plugin:wrap nog toevoegen aan dociwiki)
{"/opt/think/log/TA/node01/jboss/localhost_access_log.2016-12-11.log":{"sour
ce":"/opt/think/log/TA/node01/jboss/localhost_access_log.2016-12-11.log","of
fset":3192204,"FileStateOS":{"inode":5376524,"device":64
771}},"/opt/think/log/TA/node01/jboss/localhost_access_log.2016-12-12.log":{
"source":"/opt/think/log/TA/node01/jboss/localhost_access_log.2016-12-12.log
","offset":2440847,"FileStateOS":{"inode":5376525,"devic
e":64771}},"/opt/think/log/TA/node01/jboss/localhost_access_log.2016-12-13.l
og":{"source":"/opt/think/log/TA/node01/jboss/localhost_access_log.2016-12-1
```

```
3.log","offset":2687084,"FileStateOS":{"inode":5376357,"
device":64771}},"/opt/think/log/TA/node01/jboss/localhost_access_log.2016-12
-14.log":{"source":"/opt/think/log/TA/node01/jboss/localhost_access_log.2016
-12-14.log","offset":2430752,"FileStateOS":{"inode":5376
376,"device":64771}},"/opt/think/log/TA/node01/jboss/localhost_access_log.20
16-12-15.log":{"source":"/opt/think/log/TA/node01/jboss/localhost_access_log
.2016-12-15.log","offset":2474377,"FileStateOS":{"inode"
:5376400,"device":64771}},"/opt/think/log/TA/node01/jboss/localhost_access_l
og.2016-12-16.log":{"source":"/opt/think/log/TA/node01/jboss/localhost_acces
s_log.2016-12-16.log","offset":2417372,"FileStateOS":{"i
node":5376407,"device":64771}},"/opt/think/log/TA/node01/jboss/localhost_acc
ess_log.2016-12-17.log":{"source":"/opt/think/log/TA/node01/jboss/localhost_
access_log.2016-12-17.log","offset":2722408,"FileStateOS
":{"inode":5376392,"device":64771}},"/opt/think/log/TA/node01/jboss/localhos
t_access_log.2016-12-18.log":{"source":"/opt/think/log/TA/node01/jboss/local
host_access_log.2016-12-18.log","offset":3141147,"FileSt
ateOS":{"inode":5376428,"device":64771}},"/opt/think/log/TA/node01/jboss/loc
alhost_access_log.2016-12-19.log":{"source":"/opt/think/log/TA/node01/jboss/
localhost_access_log.2016-12-19.log","offset":2823749,"F
ileStateOS":{"inode":5376361,"device":64771}},"/opt/think/log/TA/node01/jbos
s/localhost_access_log.2016-12-20.log":{"source":"/opt/think/log/TA/node01/j
boss/localhost_access_log.2016-12-20.log","offset":35391
79,"FileStateOS":{"inode":5376430,"device":64771}},"/opt/think/log/TA/node01
/jboss/localhost_access_log.2016-12-21.log":{"source":"/opt/think/log/TA/nod
e01/jboss/localhost_access_log.2016-12-21.log","offset":
2982598,"FileStateOS":{"inode":5376462,"device":64771}},"/opt/think/log/TA/n
ode01/jboss/localhost_access_log.2016-12-22.log":{"source":"/opt/think/log/T
A/node01/jboss/localhost_access_log.2016-12-22.log","off
set":2624898,"FileStateOS":{"inode":5376528,"device":64771}},"/opt/think/log
/TA/node01/jboss/localhost_access_log.2016-12-23.log":{"source":"/opt/think/
log/TA/node01/jboss/localhost_access_log.2016-12-23.log"
,"offset":3028418,"FileStateOS":{"inode":5376492,"device":64771}}}
```


Maar de basis opmaak is dus:

```
{   "/var/log/localhost_access_log.2016-10-14.log":
{"source":"/var/log/localhost_access_log.2016-10-14.log","offset":2750260,"F
ileStateOS":
          {"inode":3410337,"device":64771}}
    ,
    "/var/log/localhost_access_log.2016-10-15.log":
{"source":"/var/log/localhost_access_log.2016-10-15.log","offset":2960699,"F
ileStateOS":
          {"inode":3410511,"device":64771}}
    ,
    "/var/log/localhost_access_log.2017-02-10.log":
{"source":"/var/log/localhost_access_log.2017-02-10.log","offset":308034,"Fi
leStateOS":
          {"inode":3410407,"device":64771}}
```

```
}
```

Dus de laatste accolade laten staan en de voorgaande comma ook verwijderen.

Vervolgens is het belangrijk om te checken in de file `/etc/filebeat/filebeat.yml` of de waarden voor `ignore_older: 51h` en `close_older: 50h` wijd genoeg staan om de files opnieuw in te lezen. Overigens moet ignore_older groter zijn dan close_older.

afronden

Start logstash op de ELK server: `service logstash start`

en start filebeat op de betreffende clients: `service filebeat start`