

Centrale log monitoring met Filebeat en ELK

Logstash kan op zich best als syslog server luisteren, maar logfiles van andere applicaties hebben vaak geen mechanisme om automatisch naar een logserver te sturen. Daarom gebruiken we filebeat om de files te versturen.

Begin met het installeren van de ELK stack door [Elasticsearch](#) en vervolgens [Logstash](#) en [Kibana](#) te installeren.

Logstash configureren voor filebeat

Logstash configuraties bestaan uit een input, een eventueel filter en een output.

input config

Aangezien sommige servers alleen over het internet te benaderen zijn zullen we uit security overwegingen, de verbindingen van filebeat over SSL laten lopen.

[maak een signed certificaat/key pair aan](#) voor de server.

Plaats de verkregen server certificaat en CA certificaat in `/etc/pki/tls/certs/` en plaats de verkregen server key in `/etc/pki/tls/private`

zet de permissies goed:

```
chmod 770 /etc/pki/tls/private
chmod 770 /etc/pki/tls/private/server.example.com.key
```

Maak een configuratie file voor de input van de Filebeats clients:

```
vi /etc/logstash/conf.d/02-input-filebeats.conf
```

```
input {
  beats {
    port => 5044
    ssl => true
    ssl_certificate => "/etc/pki/tls/certs/mnemosyne.example.nl.crt"
    ssl_key => "/etc/pki/tls/private/mnemosyne.example.nl.key"
  }
}
```

En zorg dat de firewall open staat:

```
firewall-cmd --permanent --add-port=5044/tcp
firewall-cmd --reload
```

filter config

Vervolgens stellen we een filter in voor syslog entries. Logfiles van andere applicaties hebben vaak andere formats en zullen een eigen filter moeten krijgen.

```
vi /etc/logstash/conf.d/10-filter-syslog.conf
```

en zet hier in:

```
filter {
  if [type] == "syslog" {
    grok {
      match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp}
%{SYSLOGHOST:syslog_hostname}
%{DATA:syslog_program}(?:\[ %{POSINT:syslog_pid} \])?:
%{GREEDYDATA:syslog_message}" }
      add_field => [ "received_at", "%{@timestamp}" ]
      add_field => [ "received_from", "%{host}" ]
    }
    date {
      match => [ "syslog_timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ]
    }
  }
}
```

output config

```
vi /etc/logstash/conf.d/30-output-filebeat.conf
```

```
output {
  elasticsearch {
    hosts => ["localhost:9200"]
    sniffing => true
    manage_template => false
    index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"
    document_type => "%{[@metadata][type]}"
  }
}
```

En herstart Logstash: `systemctl restart logstash`

Filebeat op de client

installeer Filebeat

Log in op de te monitoren machine.

Breng het ca certificaat over naar de client en [voeg de CA toe aan de trusted root CA store](#).

zet het certificaat van de ELK server in /etc/pki/tls/certs/ op de client.

Haal de gpg key van elasticsearch op en voeg die toe aan de yum keychain: `rpm --import http://packages.elastic.co/GPG-KEY-elasticsearch`

voeg de repository toe aan yum: `vi /etc/yum.repos.d/elastic-beats.repo`

en zet daarin:

```
[beats]
name=Elastic Beats Repository
baseurl=https://packages.elastic.co/beats/yum/el/$basearch
enabled=1
gpgkey=https://packages.elastic.co/GPG-KEY-elasticsearch
gpgcheck=1
```

en installeer: `yum -y install filebeat`

configureer Filebeat

`vi /etc/filebeat/filebeat.yml`

en zet hier de volgende opties:

```
paths:
  - /var/log/secure
  - /var/log/messages

document_type: syslog

# The Logstash hosts
hosts: ["ELK_server_private_IP:5044"]

bulk_max_size: 1024

# Optional TLS. By default is off.
tls:
  # List of root certificates for HTTPS server verifications
  certificate_authorities: ["/etc/pki/tls/certs/ca-bundle.crt"]
```

grafieken en dashboards in Kibana

Work in Progress

Bronnen

<https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-centos-7>

<https://www.elastic.co/guide/en/elasticsearch/reference/2.3/indices-delete-index.html>

From:
<https://wiki.auriel.nl/> -

Permanent link:
https://wiki.auriel.nl/doku.php?id=werkinstructies:centrale_log_monitoring_met_filebeat_en_elk&rev=1477379863 

Last update: **2016/10/25 09:17**