Logstash server

Instal.lació

|  |
| --- |
| [root@sauron ~]# cat /etc/yum.repos.d/logstash.repo  [logstash-5.x]  name=Elastic repository for 5.x packages  baseurl=https://artifacts.elastic.co/packages/5.x/yum  gpgcheck=1  gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch  enabled=1  autorefresh=1  type=rpm-md  [root@sauron ~]# |

|  |
| --- |
| [root@sauron ~]# yum install logstash -y |

el logstash el configurem de manera per a que treballi amb filebeat com client:

Cal generar el certificat

|  |
| --- |
| [root@sauron ~]# cd /etc/pki/tls  [root@sauron tls]# openssl req -subj '/CN=sauron.prib.upf.edu/' -x509 -days  3650 -batch -nodes -newkey rsa:2048 -keyout private/logstash-forwarder.key  -out certs/logstash-forwarder.crt  Generating a 2048 bit RSA private key  ................+++  ........+++  writing new private key to 'private/logstash-forwarder.key'  -----  [root@sauron tls]# |

Al client: veure la doc logstash-client, bàsicament cal copiar el certificat, instal.lar filebeat i configurar-lo per dir-li de quins fitxers ha d’enviar info al logstash server.

La idea és que tindrem aquest circuit:

**filebeat → filtre → elasticsearch**

Exemple

|  |
| --- |
| [root@sauron ~]# ls /etc/logstash/conf.d/  02-beats-input.conf 10-rsynclog-filter.conf 30-elasticsearch-output.conf  [root@sauron ~]# |

Input:

|  |
| --- |
| [root@sauron conf.d]# cat 02-beats-input.conf  input {  beats {  port => 5044  ssl => true  ssl\_certificate => "/etc/pki/tls/certs/logstash-forwarder.crt"  ssl\_key => "/etc/pki/tls/private/logstash-forwarder.key"  }  }  [root@sauron conf.d]# |

Filtre:

|  |
| --- |
| [root@sauron conf.d]# cat 10-rsynclog-filter.conf  filter {  if [type] == "log" {  grok {  match => [ "message", "total size is %{NUMBER:bytes\_copied}" ]  add\_field => [ "received\_at", "%{@timestamp}" ]  add\_field => [ "received\_from", "%{host}" ]  add\_field => [ "copiats", "%{bytes\_copied}" ]  }  }  }  [root@sauron conf.d]# |

Output:

|  |
| --- |
| [root@sauron conf.d]# cat 30-elasticsearch-output.conf  output {  elasticsearch {  hosts => ["172.20.16.195:9200", "172.20.16.194:9200", "172.20.16.198:9200", "localhost:9200"]  }  stdout { codec => rubydebug }  }  [root@sauron conf.d]# |

Ara testegem si hi ha errors de sintaxi a la configuracio:

|  |
| --- |
| [root@sauron ~]# service logstash configtest  Configuration OK  [root@sauron ~]# |

Ara engeguem el servei i el configurem per a que arranqui al boot

|  |
| --- |
| [root@sauron ~]# systemctl restart logstash  [root@sauron ~]# systemctl enable logstash  logstash.service is not a native service, redirecting to /sbin/chkconfig.  Executing /sbin/chkconfig logstash on  [root@sauron ~]# |