logstash-client

1.- copia de la clau ssl

Nota:

*sauron* és el *server* logstash

*hestia* és el *client* que volem configurar

|  |
| --- |
| [root@sauron ~]# scp /etc/pki/tls/certs/logstash-forwarder.crt root@hestia.prib.upf.edu:/tmp  The authenticity of host 'hestia.prib.upf.edu (172.20.16.107)' can't be established.  RSA key fingerprint is 15:56:cf:ef:95:7b:48:94:2b:f5:24:69:d2:e9:42:8f.  Are you sure you want to continue connecting (yes/no)? yes  Warning: Permanently added 'hestia.prib.upf.edu,172.20.16.107' (RSA) to the list of known hosts.  root@hestia.prib.upf.edu's password:  logstash-forwarder.crt 100% 1123 1.1KB/s 00:00  [root@sauron ~]# |

|  |
| --- |
| [root@hestia ~]# cp /tmp/logstash-forwarder.crt /etc/pki/tls/certs/ |

2.- instalacio del filebeat

|  |
| --- |
| [root@hestia ~]# vi /etc/yum.repos.d/elastic-beats.repo  [root@hestia ~]# cat /etc/yum.repos.d/elastic-beats.repo  [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  [root@hestia ~]# yum install filebeat -y |

3- Configuracio del filebeat:

EL fitxer /etc/filebeat/filebeat.yml el copiem com filebeat.bkup i creem un de nou:

|  |
| --- |
| [root@hestia ~]# cat /etc/filebeat/filebeat.yml  filebeat:  prospectors:  -  paths:  - /root/info-per-logstash.log  # - /var/log/\*.log    input\_type: log    document\_type: log  registry\_file: /var/lib/filebeat/registry  output:  logstash:  hosts: ["sauron.prib.upf.edu:5044"]  bulk\_max\_size: 1024  tls:  certificate\_authorities: ["/etc/pki/tls/certs/logstash-forwarder.crt"]  shipper:  logging:  files:  rotateeverybytes: 10485760 # = 10MB  [root@hestia ~]# |

4.- engeguem el servei

|  |
| --- |
| [root@hestia ~]# service filebeat start  Starting filebeat: [ OK ]  [root@hestia ~]# chkconfig filebeat on |

Ja podem anar al kibana i veure les dades.