一　ELK

-logstash帮助文档

https://www.elastic.co/guide/en/logstash/current/index.html

[root@web fd]# echo jjjjjjjj > /dev/udp/192.168.3.20/8888

[root@web fd]# function sendtcp(){ exec 9<>/dev/tcp/192.168.3.20/8888; echo "$1" >&9; exec 9<&-;

> }

[root@web fd]# sendtcp 88888

[root@logstash ~]# cat /opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-patterns-core-2.0.5/patterns/grok-patterns

[root@web httpd]# yum -y install filebeat

[root@web httpd]# vim /etc/filebeat/filebeat.yml

filebeat:

prospectors:

-

paths:

- /var/log/httpd/access.log

input\_type: log

document\_type: apachelog

registry\_file: /var/lib/filebeat/registry

output:

logstash:

hosts: ["192.168.3.20:5044"]

shipper:

logging:

files:

rotateeverybytes: 10485760 # = 10MB