1： 修改/etc/sudoers

@1: 更改权限

```
[root@localhost opt]# chmod u+w /etc/sudoers
[root@localhost opt]# vim /etc/sudoers
```

@2：注释方框那行

```
#         You have to run "ssh -t hostname sudo <cmd>".
#
#Defaults    requiretty

#
```

@3：增加最后一行 deamon ALL=(ALL) NOPASSWD:ALL

```
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
elk     ALL=(ALL)       ALL
deamon  ALL=(ALL)       NOPASSWD:ALL
## Allows members of the 'sys' group to run networking, software,
```

@4： 把权限改回来

```
[root@localhost opt]# chmod u-w /etc/sudoers
[root@localhost opt]#
```

2： 更改 change_ip_port 文件，前半部分改成如下样式

```
[root@localhost elk]# cd ..
[root@localhost opt]# cd elk/
[root@localhost elk]# cat change_ip_port
NEW_IP=$1
NEW_PORT=$2

sed -ri "/host =>/,+1c host => \"$NEW_IP\"\nport => $NEW_PORT" /opt/elk/filter/l
ogstash/etc/logstash_rsyslog.conf

#restart logstash
```

3：编辑 change_filter_ip_restart 文件

```
[root@localhost filter]# cd ..
[root@localhost elk]# cd filter/
[root@localhost filter]# vim change_filter_ip_restart
```

然后按下 esc 键，输入:set fileformat=unix 再 :wq 保存退出

```
}\n
}\n
\n
filter {\n
json { source => \"message\"  }\n
$NEW_FILTER \n
}\n
\n
output{\n

udp {\n
host => \"$NEW_IP\"\n
port => $NEW_PORT \n
:set fileformat=unix
```

```
}\n
\n
output{\n

udp {\n
host => \"$NEW_IP\"\n
port => $NEW_PORT \n
:wq
Ready                    ssh2: AES-256-CTR    24,  4
```

4： 更改 **PHP** 源代码

```
[root@localhost opt]#
[root@localhost opt]# cd lampp/htdocs/
[root@localhost htdocs]# vim changefilter.php
```

```
// add filter;
$message=shell_exec("sudo -iu root /opt/elk/f
terstring $oldip $oldport");
```

改成以下

```
// add filter;
$message=shell_exec("sudo /opt/elk/filter/c
 $oldip $oldport");
```

5： 更改 **changeipport.php** 文件

```
changefilter.php" [dos] 78L, 1957C written
[root@localhost htdocs]# vim changeipport.php
<?php
```

```
// add change ip and port program;
$message=shell_exec("sudo -iu root /opt/elk/change_ip_p
//sleep(10);
```

改成以下

```
// add change ip and port program;
$message=shell_exec("sudo /opt/elk/change_ip_port $ipaddr $port");
//sleep(10);
```

附录： 注意哪些文件默认需要你改

```
[root@localhost htdocs]#
[root@localhost htdocs]# cd /opt/elk/kibana/config/
[root@localhost config]# vim kibana.yml
```

改成你自己的 ip

```
# The Elasticsearch instance to use for all your queries.
elasticsearch_url: "http://192.168.1.107:9200"
```

改成你自己的 ip

```
[root@localhost kibana]# vim /opt/elk/kibana/src/public/elk/layout/global.js
var GlobalIP = "192.168.1.107";
var GlobalURL ="http://"+GlobalIP+":9200";
var GlobalApiURL = "http://"+GlobalIP+":8099";
var PageSize = 8000000;
~
~
~
~
~
~
~
~
~
```

Lamp 的配置文件

```
[root@localhost opt]#
[root@localhost opt]#
[root@localhost opt]#
[root@localhost opt]# vim lampp/etc/httpd.conf
#
# This is the main Apache HTTP server configuration file.  It conta
```

```
# prevent Apache from glomming o
#
#Listen 12.34.56.78:80
Listen 80

#
```

改成以下

```
#
#Listen 12.34.56.78:80
Listen 8099

#
```