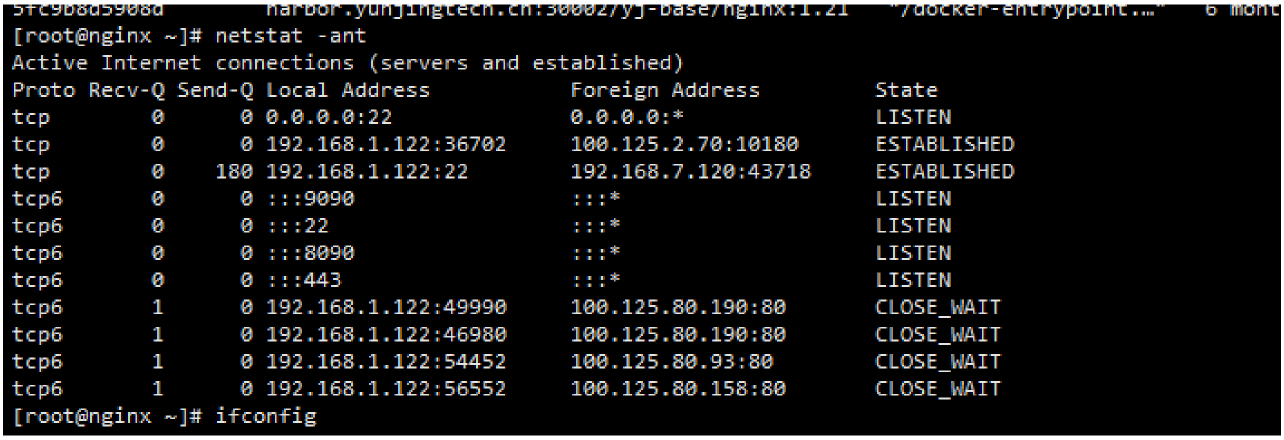
使用docker进行部署可实现快速的扩容部署，存在易用性，所以很多系统都是采用docker进行部署，但是利用docker部署的系统在发生攻击时，可能存在无法快速实现应急响应的问题。在宿主机上使用netstat -an是无法看到docker内的连接的，只能看到宿主机的连接



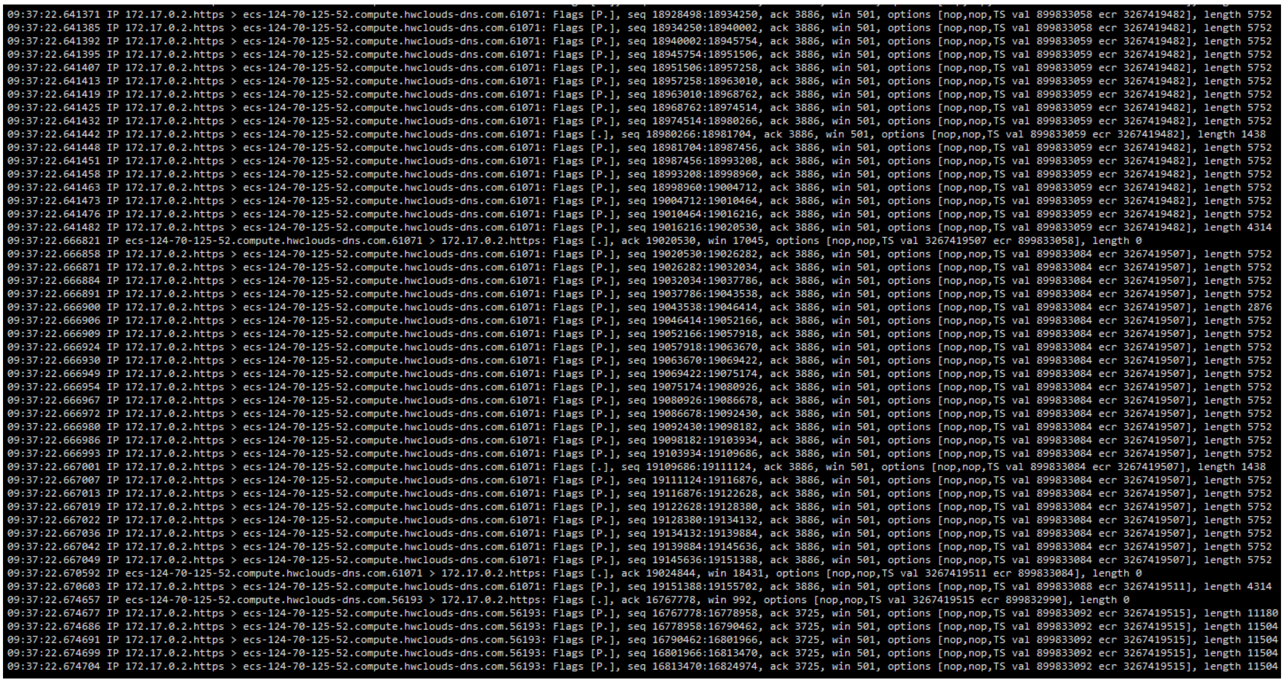
```
5fc9b8d5908d        harbor.yunjingtech.cn:30002/yj-base/nginx:1.21   "/docker-entrypoint.…"   6 mont
[root@nginx ~]# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.122:36702     100.125.2.70:10180      ESTABLISHED
tcp        0    180 192.168.1.122:22        192.168.7.120:43718     ESTABLISHED
tcp6       0      0 :::9090                 :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::8090                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
tcp6       1      0 192.168.1.122:49990     100.125.80.190:80       CLOSE_WAIT
tcp6       1      0 192.168.1.122:46980     100.125.80.190:80       CLOSE_WAIT
tcp6       1      0 192.168.1.122:54452     100.125.80.93:80        CLOSE_WAIT
tcp6       1      0 192.168.1.122:56552     100.125.80.158:80       CLOSE_WAIT
[root@nginx ~]# ifconfig
```

1.获取异常连接ip

宿主机通过docker0和dockers容器进行通信，通过抓取docker0的数据包查看存在异常连接的docker，根据异常连接获取存在问题的docker：

抓取docker0的数据包：

```
tcpdump -i docker0
```

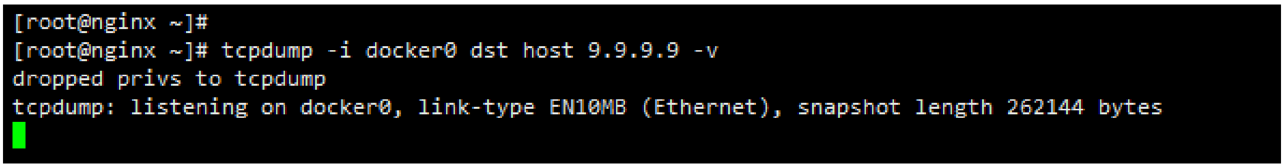


```
09:37:22.641371 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18928498:18934250, ack 3886, win 501, options [nop,nop,TS val 899833058 ecr 3267419482], length 5752
09:37:22.641385 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18934250:18940002, ack 3886, win 501, options [nop,nop,TS val 899833058 ecr 3267419482], length 5752
09:37:22.641392 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18940002:18945754, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641395 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18945754:18951506, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641407 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18951506:18957258, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641413 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18957258:18963010, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641419 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18963010:18968762, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641425 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18968762:18974514, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641432 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18974514:18980266, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641442 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [.], seq 18980266:18981704, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 1438
09:37:22.641448 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18981704:18987456, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641451 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18987456:18993208, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641458 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18993208:18998960, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641463 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 18998960:19004712, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641473 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19004712:19010464, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641476 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19010464:19016216, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 5752
09:37:22.641482 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19016216:19020530, ack 3886, win 501, options [nop,nop,TS val 899833059 ecr 3267419482], length 4314
09:37:22.666821 IP ecs-124-70-125-52.compute.hwclouds-dns.com.61071 > 172.17.0.2.https: Flags [.], ack 19020530, win 17045, options [nop,nop,TS val 3267419507 ecr 899833058], length 0
09:37:22.666858 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19020530:19026282, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666871 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19026282:19032034, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666884 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19032034:19037786, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666891 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19037786:19043538, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666900 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19043538:19046414, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 2876
09:37:22.666906 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19046414:19052166, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666909 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19052166:19057918, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666924 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19057918:19063670, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666930 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19063670:19069422, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666949 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19069422:19075174, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666954 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19075174:19080926, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666967 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19080926:19086678, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666972 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19086678:19092430, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666980 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19092430:19098182, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666986 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19098182:19103934, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.666993 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19103934:19109686, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.667001 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [.], seq 19109686:19111124, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 1438
09:37:22.667007 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19111124:19116876, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.667013 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19116876:19122628, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.667019 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19122628:19128380, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.667022 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19128380:19134132, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.667036 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19134132:19139884, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.667042 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19139884:19145636, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.667049 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19145636:19151388, ack 3886, win 501, options [nop,nop,TS val 899833084 ecr 3267419507], length 5752
09:37:22.670592 IP ecs-124-70-125-52.compute.hwclouds-dns.com.61071 > 172.17.0.2.https: Flags [.], ack 19024844, win 18431, options [nop,nop,TS val 3267419511 ecr 899833084], length 0
09:37:22.670603 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.61071: Flags [P.], seq 19151388:19155702, ack 3886, win 501, options [nop,nop,TS val 899833088 ecr 3267419511], length 4314
09:37:22.674657 IP ecs-124-70-125-52.compute.hwclouds-dns.com.56193 > 172.17.0.2.https: Flags [.], ack 16767778, win 992, options [nop,nop,TS val 3267419515 ecr 899832990], length 0
09:37:22.674677 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.56193: Flags [P.], seq 16767778:16778958, ack 3725, win 501, options [nop,nop,TS val 899833092 ecr 3267419515], length 11180
09:37:22.674686 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.56193: Flags [P.], seq 16778958:16790462, ack 3725, win 501, options [nop,nop,TS val 899833092 ecr 3267419515], length 11504
09:37:22.674691 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.56193: Flags [P.], seq 16790462:16801966, ack 3725, win 501, options [nop,nop,TS val 899833092 ecr 3267419515], length 11504
09:37:22.674699 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.56193: Flags [P.], seq 16801966:16813470, ack 3725, win 501, options [nop,nop,TS val 899833092 ecr 3267419515], length 11504
09:37:22.674704 IP 172.17.0.2.https > ecs-124-70-125-52.compute.hwclouds-dns.com.56193: Flags [P.], seq 16813470:16824974, ack 3725, win 501, options [nop,nop,TS val 899833092 ecr 3267419515], length 11504
```

可获取docker的ip地址：172.17.0.2

在已经获取异常外联ip的情况下，可根据实际的地址进行过滤，如已知道异常外联ip地址为9.9.9.9：

```
tcpdump -i docker0 dst host 9.9.9.9 -v
```

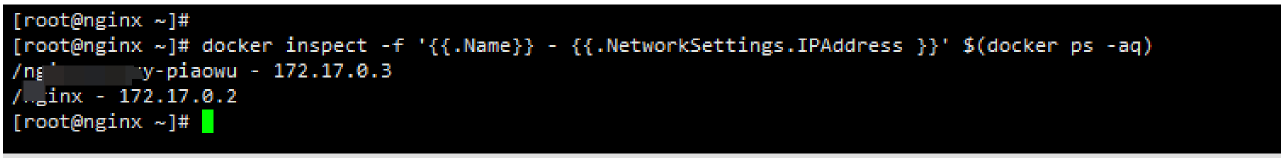


```
[root@nginx ~]#
[root@nginx ~]# tcpdump -i docker0 dst host 9.9.9.9 -v
dropped privs to tcpdump
tcpdump: listening on docker0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

可通过该命令获取docker ip地址

根据docker 的ip地址获取容器id，获取所有的coker 容器ip

```
docker inspect -f '{{.Name}} - {{.NetworkSettings.IPAddress }}' $(docker ps -aq)
```



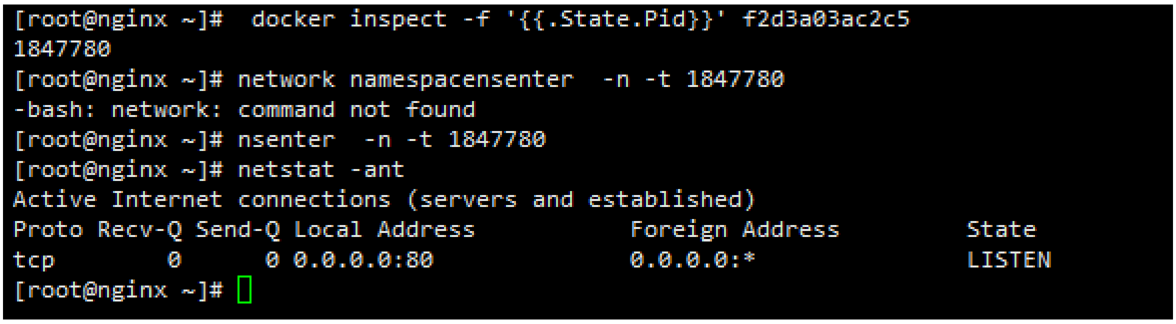
```
[root@nginx ~]#
[root@nginx ~]# docker inspect -f '{{.Name}} - {{.NetworkSettings.IPAddress }}' $(docker ps -aq)
/ng[redacted]y-piaowu - 172.17.0.3
/[redacted]inx - 172.17.0.2
[root@nginx ~]#
```

可利用grep命令进行过滤，获取相关docker容器的名称

```
docker inspect -f '{{.Name}} - {{.NetworkSettings.IPAddress }}' $(docker ps -aq) |
grep 172.17.0.2
```

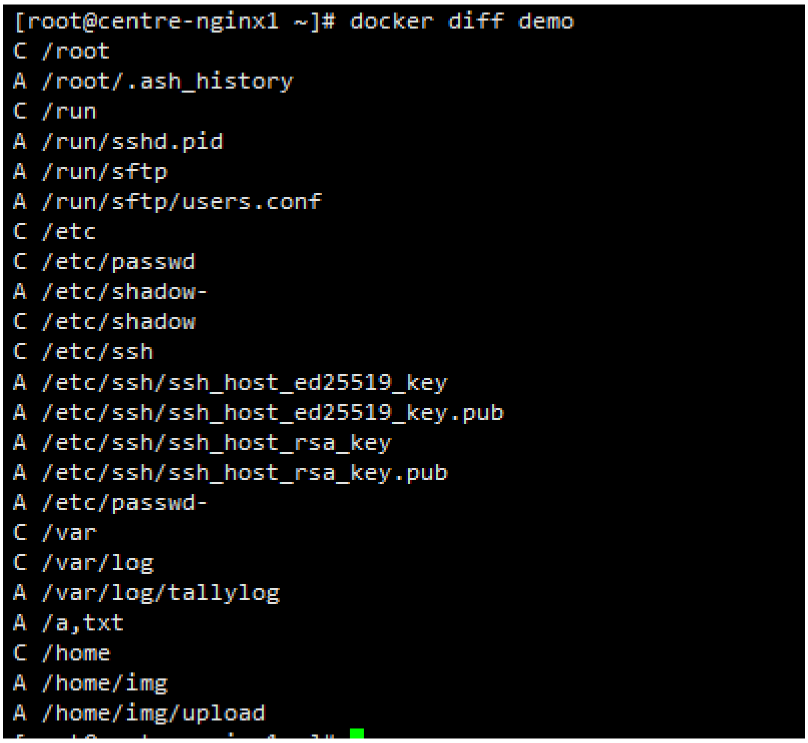
假如不知道异常的外联ip地址，可在network namespace进行确认，

```
#获取容器PID  docker inspect -f '{{.State.Pid}}' <containerId>
#进入容器的network namespace    nsenter  -n -t pid
# 验证是否进入容器的network namespace     netstat -an|grep xx.xx.xx.xx
```



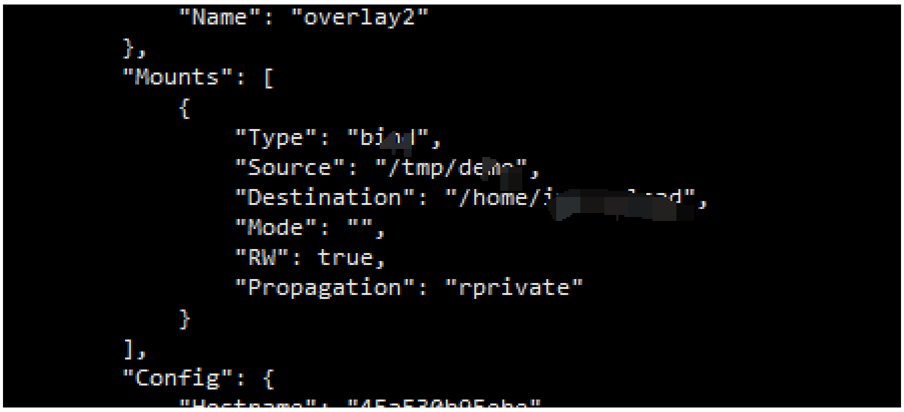
```
[root@nginx ~]#  docker inspect -f '{{.State.Pid}}' f2d3a03ac2c5
1847780
[root@nginx ~]# network namespacensenter  -n -t 1847780
-bash: network: command not found
[root@nginx ~]# nsenter  -n -t 1847780
[root@nginx ~]# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
[root@nginx ~]#
```

查看容器内文件状态变化：docker diff demo



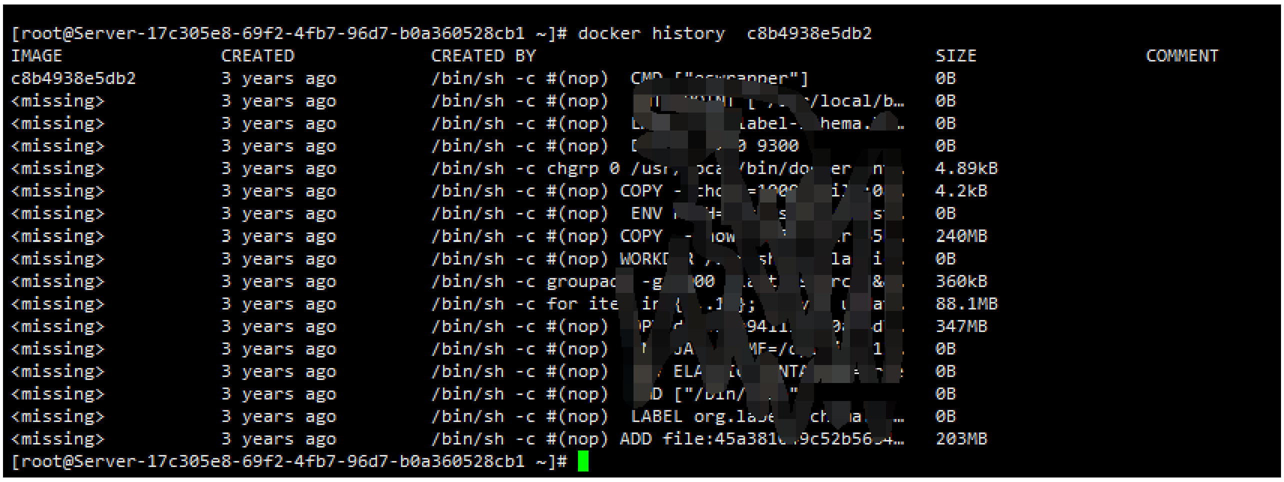
```
[root@centre-nginx1 ~]# docker diff demo
C /root
A /root/.ash_history
C /run
A /run/sshd.pid
A /run/sftp
A /run/sftp/users.conf
C /etc
C /etc/passwd
A /etc/shadow-
C /etc/shadow
C /etc/ssh
A /etc/ssh/ssh_host_ed25519_key
A /etc/ssh/ssh_host_ed25519_key.pub
A /etc/ssh/ssh_host_rsa_key
A /etc/ssh/ssh_host_rsa_key.pub
A /etc/passwd-
C /var
C /var/log
A /var/log/tallylog
A /a,txt
C /home
A /home/img
A /home/img/upload
```

docker定位宿主机目录：docker inspect demo



```
            "Name": "overlay2"
        },
        "Mounts": [
            {
                "Type": "[redacted]",
                "Source": "/tmp/de[redacted]",
                "Destination": "/home/[redacted]",
                "Mode": "",
                "RW": true,
                "Propagation": "rprivate"
            }
        ],
        "Config": {
            "Hostname": "45a530b05aba",
```

查看镜像历史情况：docker history c8b4938e5db2



```
[root@Server-17c305e8-69f2-4fb7-96d7-b0a360528cb1 ~]# docker history  c8b4938e5db2
IMAGE               CREATED             CREATED BY                                      SIZE                COMMENT
c8b4938e5db2        3 years ago         /bin/sh -c #(nop)  CMD [redacted]               0B
<missing>           3 years ago         /bin/sh -c #(nop)  [redacted]                   0B
<missing>           3 years ago         /bin/sh -c #(nop)  [redacted]                   0B
<missing>           3 years ago         /bin/sh -c #(nop)  [redacted]                   0B
<missing>           3 years ago         /bin/sh -c chgrp 0 /us[redacted]                4.89kB
<missing>           3 years ago         /bin/sh -c #(nop) COPY [redacted]               4.2kB
<missing>           3 years ago         /bin/sh -c #(nop)  ENV [redacted]               0B
<missing>           3 years ago         /bin/sh -c #(nop) COPY [redacted]               240MB
<missing>           3 years ago         /bin/sh -c #(nop) WORKD[redacted]               0B
<missing>           3 years ago         /bin/sh -c groupad[redacted]                    360kB
<missing>           3 years ago         /bin/sh -c for ite[redacted]                    88.1MB
<missing>           3 years ago         /bin/sh -c #(nop)  [redacted]                   347MB
<missing>           3 years ago         /bin/sh -c #(nop)  [redacted]                   0B
<missing>           3 years ago         /bin/sh -c #(nop)  [redacted]                   0B
<missing>           3 years ago         /bin/sh -c #(nop)  [redacted]                   0B
<missing>           3 years ago         /bin/sh -c #(nop)  LABEL org.la[redacted]       0B
<missing>           3 years ago         /bin/sh -c #(nop) ADD file:45a381[redacted]     203MB
[root@Server-17c305e8-69f2-4fb7-96d7-b0a360528cb1 ~]#
```

查找镜像相关的容器：

docker ps -a | grep <IMAGE_NAME>

进入docker容器：

docker exec -it 531b2fdcad3c bash

查看日志：

docker log names

查看docker容器运行状态：

docker stats es

攻击容器处理：

删除相关容器和镜像：

```
docker rm -f  <containerId>
docker rmi <IMAGE_NAME>
```

docker pause 暂停容器中所有的进程

断开docker 容器的网络：

```
docker network disconnect bridge <container-name>
```

保留入侵痕迹，使用docker commit保存为镜像，可作为demo

将容器打包成镜像：

```
docker commit 135a0d19f757 jenkins:1.0
```

打包镜像为my_jenkins.tar：

```
docker save -o my_jenkins.tar jenkins:1.0
```

新服务器载入镜像：

```
docker load --input my_jenkins.tar
```

执行docker run：

```
docker run centos:7 /usr/local/bash -c ls /
```