

Moloch 那些不得不说的

本文作者：Cherishao（信安之路作者团队成员 & 应急响应小组小组长）

成员招募：[信安之路应急响应小组寻找志同道合的朋友](#)

谈及 Moloch,想必大家都知道” moloch 是一个开源的、大规模的 IPv4 数据包捕获（PCAP），索引数据库系统。“它以标准 pcap 格式存储和索引网络流量提供快速的索引访问，从而减少可疑事件的分析时间。

优势：

- 1、moloch 公开了 API，允许 pcap 数据和 json 格式的会话数据直接下载和使用。
- 2、提供直观的 Web 界面，用于 PCAP 浏览、搜索、分析，Moloch 以标准 PCAP 格式存储和导出所有数据包。
- 3、可扩展性：Moloch 旨在部署在多个集群系统中，提供扩展可以处理多个千兆位/秒的流量。PCAP 保留基于可用的传感器磁盘空间，而元数据保留基于 Elasticsearch 集群的规模。两种保留大小都可以随时增加。
- 4、安全：通过使用具有摘要密码的 HTTPS 或使用提供 Web 服务器代理的身份验证来保护对 Moloch 的访问。PCAP 都存储在已安装的 Moloch 传感器上，只能通过 Moloch 接口或 API 访问。Moloch 支持在静止时加密 PCAP 文件。

简而言之：Moloch 可以保存所有原始数据流量，基于 elasticsearch 及 PCAP 的存储形式使它得以对通信数据流中的元数据进行快速检索。相对来说是一个比较好用的回溯分析系统。

Moloch 构成

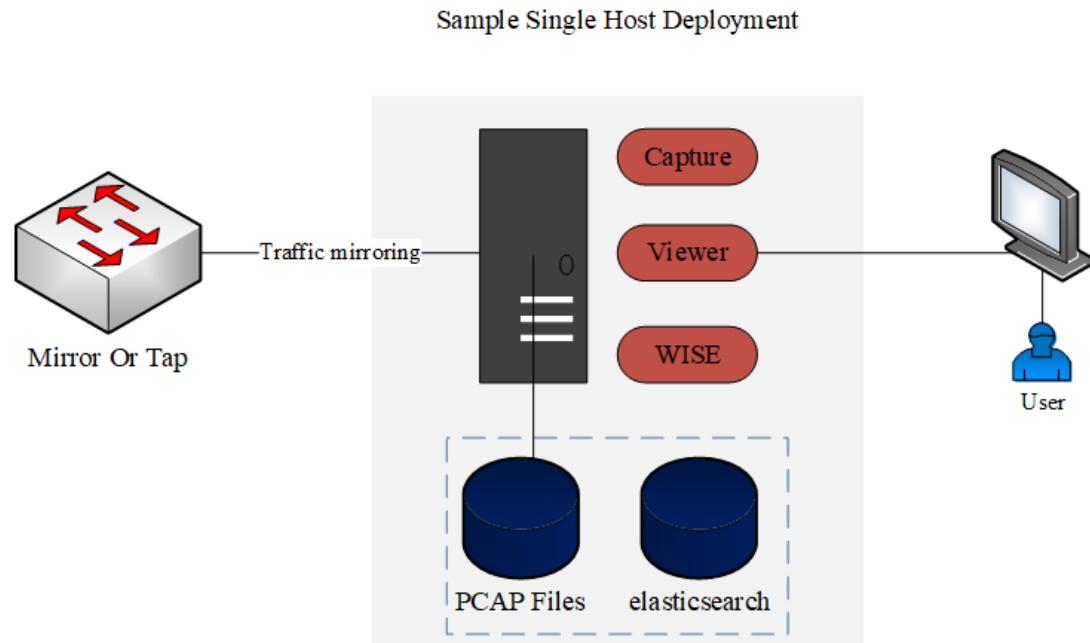
流量回溯系统通常都会面临这样几个问题：

- 1、数据包的存取和协议的分析；
- 2、数据量很大的时候检索的速度。

我们设想一下使用 tshark、Wireshark 对一个几十 GB 的数据包进行分析时，包的加载都会是一个很头疼的问题，更不用说过滤表达式的应用。而 Moloch 在这方面就具备了独特的优势，我们来看看它的构成。

数据的来源是交换机的镜像端口，moloch 系统主要涉及三个组件 Capture，elasticsearch 和 Viewer


Capture（绑定 interface 运行的单线程 C 语言应用）用来抓取流量并以 pcap 的格式存储到硬盘上面，还会存一份对应关系到 elasticsearch（moloch 的数据检索驱动）中，Viewer（运行在 capture 主机上的 node.js web 应用）提供 web 界面，以下为 Moloch 的单个主机部署架构图。



Moloch 安装

由上图中的架构可知，部署 Moloch，我们需要安装 elasticsearch 及 Moloch（集成了 Capture 与 Viewer），存储数据包对机器的性能要求 moloch 提供了评估页面：

[Moloch Estimators](#)



HomeDemoEstimatorsDownloadsHelp

Average gigabits per second1

Capture Machines

More info in FAQ

Calculating the number of machines needed for capturing is relatively simple. It is based on the average traffic rate, the number of days of retention, how much space is available on each machine, and the avg amount of traffic each machine can handle. If more than one machine is required, we highly recommend getting a [NPB](#) to load balance the traffic across the cluster. We suggest RAID 5 or RAID 6 for capture disks.

Moloch makes it possible to not save encrypted packets, other than the session negotiation. If you plan on using this feature select the percentage of TLS/QUIC traffic on the network. Most networks will see 10-40% of TLS traffic, resulting in huge disk space savings.

PCAP RetentionDays3

Disk Size4 TB

Disks per machine20

TLS Percentage0%

Avg per machine3 Gbps

Space Required	All disks for data RAID 0	One disk extra RAID 5	Two disks extra RAID 6 or RAID 5 + Hot Spare
33 TB	1 host / 72 TB	1 host / 69 TB	1 host / 65 TB

Elasticsearch Machines

More info in FAQ

Calculating the number of machines needed for Elasticsearch is a fine art. It heavily depends on the type of traffic that Moloch will be seeing plus of course the traffic rate and number of days of retention. Each node requires 64GB - 128GB of memory, 30GB for ES, and 34-96GB for OS disk cache. For large machines plan on running multiple nodes per host. You may want to read more recommendations from Elastic's Reference and Blog.

Many scaling guides will recommend you do NOT use RAID 5, assuming you will use Elasticsearch replication. However by default Moloch does NOT enable replication, so it is strongly recommended that you **DO** use RAID 5 or RAID 6. If you decide to use Elasticsearch replication you will need more machines, but don't need RAID 5 in theory.

The calculated host counts are just estimates.

ES Retention Days3

Disk Size4 TB

Disks per machine4

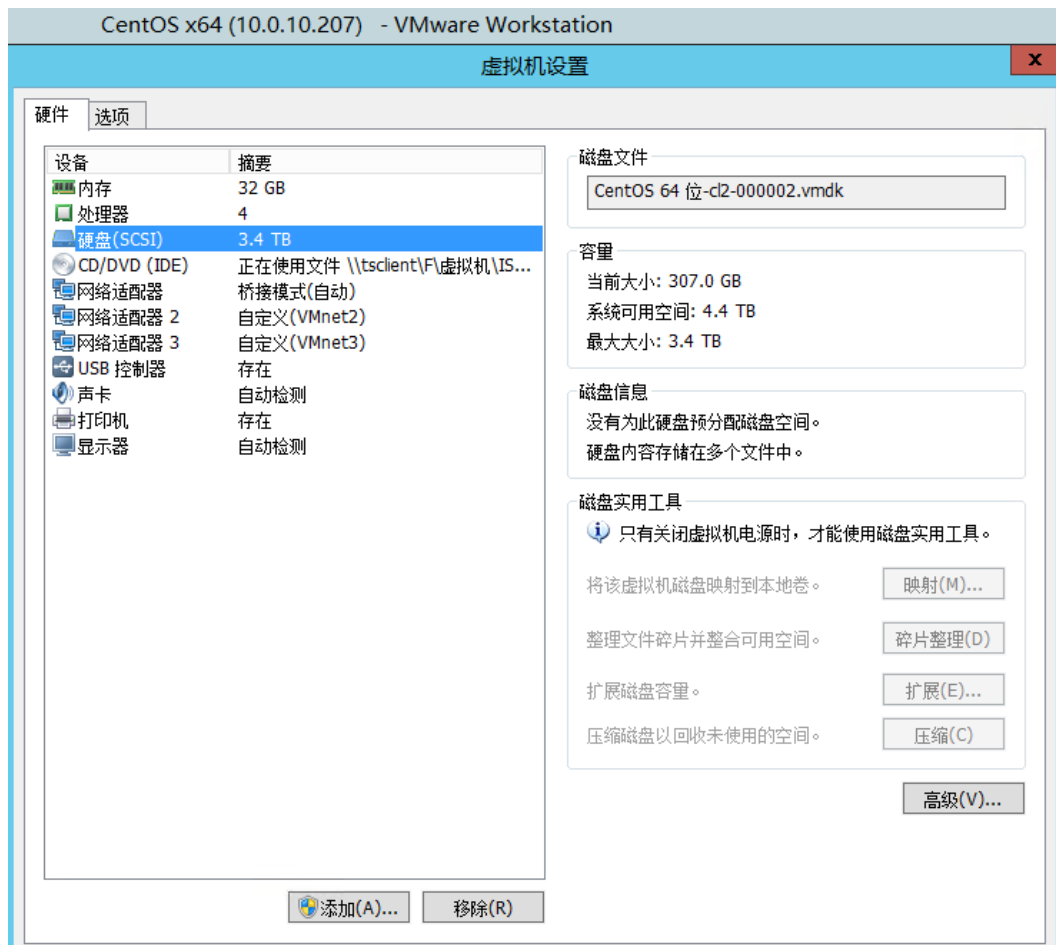
Nodes per machine1

Replication0 Replicas

	Total Space Required	All disks for data RAID 0	One disk extra RAID 5	Two disks extra RAID 6 or RAID 5 + Hot Spare
Average traffic mix	2 TB	1 host	1 host	1 host
High DNS/HTTP traffic	2 TB	1 host	1 host	1 host
Pathological traffic mix	3 TB	1 host	1 host	1 host

可根据 PCAP 包的存储天数、TLS (加密数据包保存的百分比)、每台机器的处理能力；ES 日志的存储天数、机器节点等选择适合自己的硬件资源。Moloch 的每个节点需要 64GB - 128GB 内存：ES 为 30GB，OS 磁盘缓存为 34-96GB。对于大型计算机，计划为每个主机运行多个节点。

笔者部署的硬件资源如下：



上图新增 2 张网卡，是将交换机镜像过来的流量镜像到虚拟机的网卡。

虚拟机情况：

```
# cat /etc/redhat-release
CentOS Linux release 7.5.1804 (Core)
# uname -r
3.10.0-862.11.6.el7.x86_64
```

elasticsearch 安装

在安装 Moloch 之前，我们需要先安装配置好 elasticsearch，由官网的 CHANGELOG 可知，elasticsearch 的版本应该大于等于 5.5.0，这里我们安装的版本为 elasticsearch-6.4.0。

```
← → ↺ 🔒 https://raw.githubusercontent.com/aol/moloch/master/CHANGELOG

NOTICE: Please see https://github.com/aol/moloch/wiki/FAQ#upgrading-moloch for upgrading info

ES Versions:
* Moloch >= 1.5.0 supports ES >= 5.5.0, 6.x, not 7.x or later
* Moloch >= 1.0.0 supports ES >= 5.5.0, 6.x (not prod tested, only for new installs), not 7.x or later
* Moloch >= 0.50.0 supports ES >= 5.5.0, not 6.x or later
* Moloch >= 0.18.1 supports ES 2.4.x, >= 5.3.1 not 6.x or later

Node Versions:
* Moloch >= 1.6.0 requires NodeJS 8.x or 8.12 or later
* Moloch >= 1.0.0 requires NodeJS 8.x
* Moloch >= 0.20.0 requires NodeJS 6.x
* Moloch >= 0.18.1 requires NodeJS 4.x

NOTICE: Restart wiseService before capture when upgrading
```

一、Java 环境安装

有两种安装方式：

1) yum 安装

```
$ yum install java-1.8.0-openjdk
$ java -version
```

2) 手动安装

从 oracle 官网下载 jdk-8u 的安装包进行安装，笔者采用的是手动安装的方式

<https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>

```
$ ls -lh jdk-8u191-linux-x64.tar.gz #查看文件大小
$ mv jdk-8u191-linux-x64.tar.gz /opt
$ cd /opt
$ tar -zxvf jdk-8u191-linux-x64.tar.gz
$ cd jdk1.8.0_191/
$ ln -s /opt/jdk1.8.0_191 /usr/local/jdk
$ vim /etc/profile # 新增如下变量
export JAVA_HOME=/usr/local/jdk
export PATH=$JAVA_HOME/bin:$PATH
$ source /etc/profile #让配置文件生效
$ java -version
java version "1.8.0_191"
Java(TM) SE Runtime Environment (build 1.8.0_191-b12)
Java HotSpot(TM) 64-Bit Server VM (build 25.191-b12, mixed mode)
```

二、elasticsearch 下载

下载 Linux 版 elasticsearch (下载地址
<https://www.elastic.co/downloads/elasticsearch>)

```
$ cd /opt
$ wget
https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-
6.4.0.tar.gz
$ tar -zxvf elasticsearch-6.4.0.tar.gz
$ cd elasticsearch-6.4.0/config
$ vim config/elasticsearch.yml
```

三、配置文件修改

1) elasticsearch.yml 修改以下三个部分, network.host 为指定的 IP 地址, 可以是多个。

```
# ----- Cluster -----
#
# Use a descriptive name for your cluster:
#
cluster.name: elasticsearch
#
# ----- Node -----
#
# Use a descriptive name for the node:
#
node.name: node-1
node.master: true
node.data: true
# ----- Network -----
#
# Set the bind address to a specific IP (IPv4 or IPv6):
#
network.host: 10.0.10.207
#
# Set a custom port for HTTP:
#
http.port: 9200
transport.tcp.port: 9300
http.cors.enabled: true
http.cors.allow-origin: "*"
# For more information, consult the network module documentation.
```

2) 为了预防文件描述符太低，在配置文件 `limits.conf` 中新增

```
$ vim /etc/security/limits.conf
```

```
* soft nofile 65526
* hard nofile 131072
* soft nproc 2048
* hard nproc 4096
```

3) 为了预防一个进程最多可用于的内存映射区太低，在配置文件 `sysctl.conf` 中新增

```
vim /etc/sysctl.conf
```

```
vm.max_map_count=655360
```

4) 重新加载系统参数使配置生效

```
sysctl -p
```

四、elasticsearch 启动

1) elasticsearch 不能使用 root 用户启动，创建组及用户

```
$ groupadd elasticsearch
$ useradd elasticsearch -g elasticsearch -p elasticsearch
$ chown -R elasticsearch /opt/elasticsearch-6.4.0
```

2) 切换用户启动 elasticsearch

```
$ su elasticsearch
$ ./elasticsearch -d # -d 参数代表后台启动
```

3) 关闭防火墙

```
$ systemctl stop firewalld
```

五、验证启动状态

访问: <http://10.0.10.207:9200> 或 `curl http://10.0.10.207:9200`

返回如下 json 信息，表示配置成功

```
{
  "name" : "node-1",
  "cluster_name" : "elasticsearch",
```

```
"cluster_uuid" : "9-dyTdtYTHmX7frIGWzIgw",
"version" : {
  "number" : "6.4.0",
  "build_flavor" : "default",
  "build_type" : "tar",
  "build_hash" : "595516e",
  "build_date" : "2018-08-17T23:18:47.308994Z",
  "build_snapshot" : false,
  "lucene_version" : "7.4.0",
  "minimum_wire_compatibility_version" : "5.6.0",
  "minimum_index_compatibility_version" : "5.0.0"
},
"tagline" : "You Know, for Search"
}
```

检查 ES 的健康状态


访问: http://10.0.10.207:9200/_cat/health 或 jcurl
http://10.0.10.207:9200/_cat/health 返回

```
1548230399 15:59:59 elasticsearch green 1 1 22 22 0 0 0 0 - 100.0%
```

表示健康

Moloch 下载

从官网下载适合自己的 Moloch 版本（下载地址：
<https://www.molo.ch/#downloads>），笔者这里为 Centos 7 的
Moloch.1.6.2, 更多支持的版本如下：


[Home](#)
[Demo](#)
[Estimators](#)
[Downloads](#)
[Help](#)

Downloads

BEFORE upgrading from **ES 5** to **ES 6** read the [How do I upgrade to ES 6](#) FAQ entry.
BEFORE upgrading to **Moloch 1.5** you must be on **Moloch 1.0 or 1.1** and finished any reindexing.
BEFORE upgrading to **Moloch 1.0 or 1.1** read the [How do I upgrade to Moloch 1.0](#) FAQ entry.
 Upgrading to 1.0 takes some time, work, and requires ES 5.x.
BEFORE upgrading from **ES 2** to **ES 5** read the [How do I upgrade to ES 5](#) FAQ entry.

[NOTICE.txt](#)
[Changelog](#)
[Instructions](#)
[Open an Issue](#)

Moloch 1.7.0 2019-01-18	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	Ubuntu 18.04
Moloch 1.6.2 2018-12-08	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	Ubuntu 18.04
Moloch 1.6.1 2018-11-07	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	Ubuntu 18.04
hide more downloads					
Moloch 1.6.0 2018-10-30	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	Ubuntu 18.04
Moloch 1.5.3 2018-09-10	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	Ubuntu 18.04
Moloch 1.5.2 2018-07-26	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	Ubuntu 18.04
Moloch 1.5.1 2018-07-23	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	
Moloch 1.5.0 2018-07-17	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	
Moloch 1.1.1 2018-07-17	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	
Moloch 1.1.0 2018-04-30	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	
Moloch 1.0.0 2018-04-05	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	
Moloch 0.50.1 2018-03-30	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	
Moloch 0.50.0 2018-01-24	Centos 6	Centos 7	Ubuntu 14.04	Ubuntu 16.04	

Moloch 安装

```
$ yum install -y perl-JSON perl-libwww-perl libyaml-devel # 安装依赖
```

```
$ rpm -ivh moloch-1.6.2-1.x86_64.rpm #RPM 安装包
```

```
$ /data/moloch/bin/Configure #配置 Moloch 只需执行一次
```

ound interfaces: ens33;ens37;ens38;lo;virbr0

Semicolon ';' seperated list of interfaces to monitor [eth1] ens37 # 选择网卡, 我选 ens37

Install Elasticsearch server locally for demo, must have at least 3G of memory, NOT recommended for production use (yes or no) [no] no #选择 no

Elasticsearch server URL [http://localhost:9200]
http://10.0.10.207:9200 #数据库地址

Password to encrypt S2S and other things [no-default] elasticsearch # 设置个密码

Moloch - Creating configuration files

Installing systemd start files, use systemctl

Moloch - Installing /etc/logrotate.d/moloch to rotate files after 7 days

Moloch - Installing /etc/security/limits.d/99-moloch.conf to make core and memlock unlimited

Download GEO files? (yes or no) [yes] yes # 选择 yes, 下载相关地理位置文件

...

5) 初始化/升级 Elasticsearch Moloch 配置

第一次安装或者要清除数据可以运用如下命令

```
$ /data/moloch/db/db.pl http://ESHOST:9200 init
```

moloch 的包更新, 由 CHANGELOG 知 1.6.2 版本的包是需要更新的

@<https://raw.githubusercontent.com/aol/moloch/master/CHANGELOG>
1.6.2 2018/12/07

- 注意: 需要 db.pl 升级

```
$ /data/moloch/db/db.pl http://ESHOST:9200 upgrade
```

6) 新安装或 init 后添加管理员用户

```
$ /data/moloch/bin/moloch_add_user.sh admin "Admin User"
THEPASSWORD --admin
```

7) 启动 moloch

#如果使用 upstart (Centos 6 或有时 Ubuntu 14.04)

```
$ /sbin/start molochcapture
```

```
$ /sbin/start molochviewer
```

#如果使用 systemd (Centos 7 或 Ubuntu 16.04 或有时 Ubuntu 14.04)

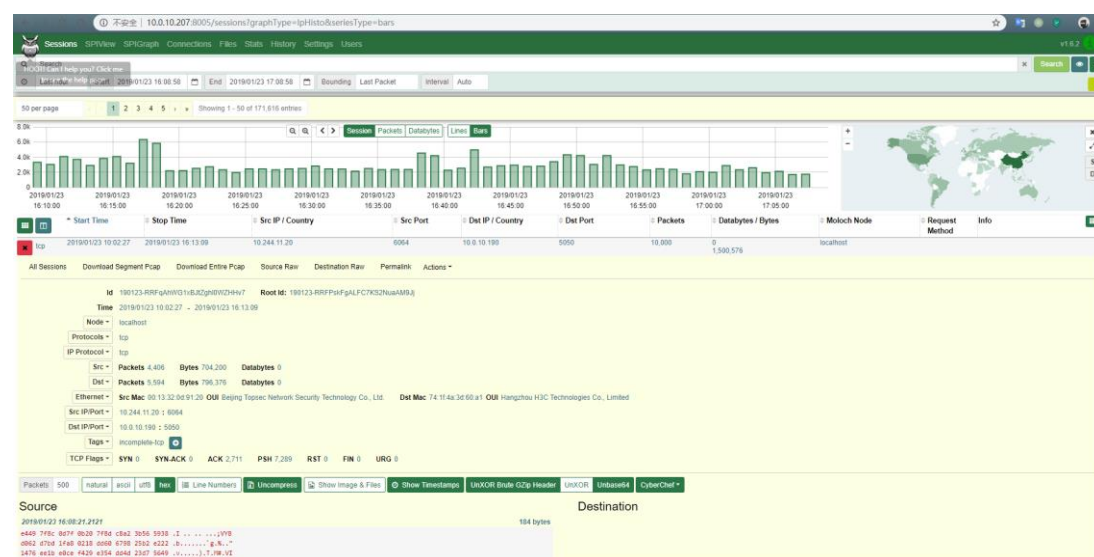
```
$ systemctl start molochcapture.service
```

```
$ systemctl start molochviewer.service
```

访问 <http://MOLOCHHOST:8005>

user: admin

password: THEPASSWORD from step #6



Moloch 使用

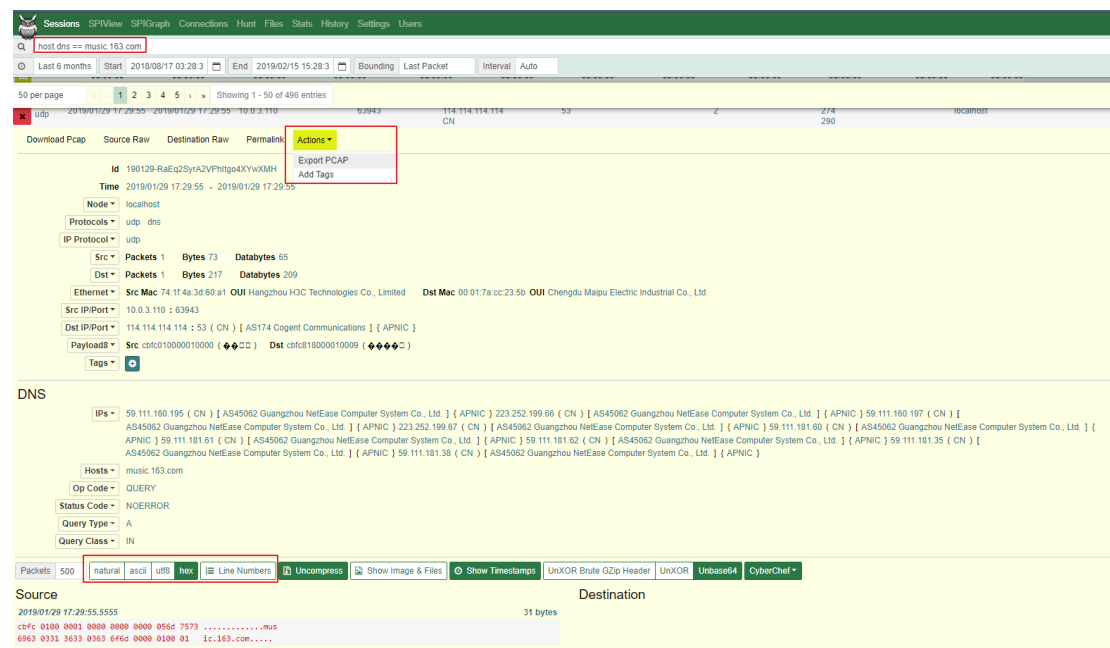
1) 回溯分析

检索局域内的指定源 IP `ip.src== host` 目的 IP `ip.dst == host`

`ip.src == 10.0.3.36`

检索局域网内的指定 dns `host.dns== dns`

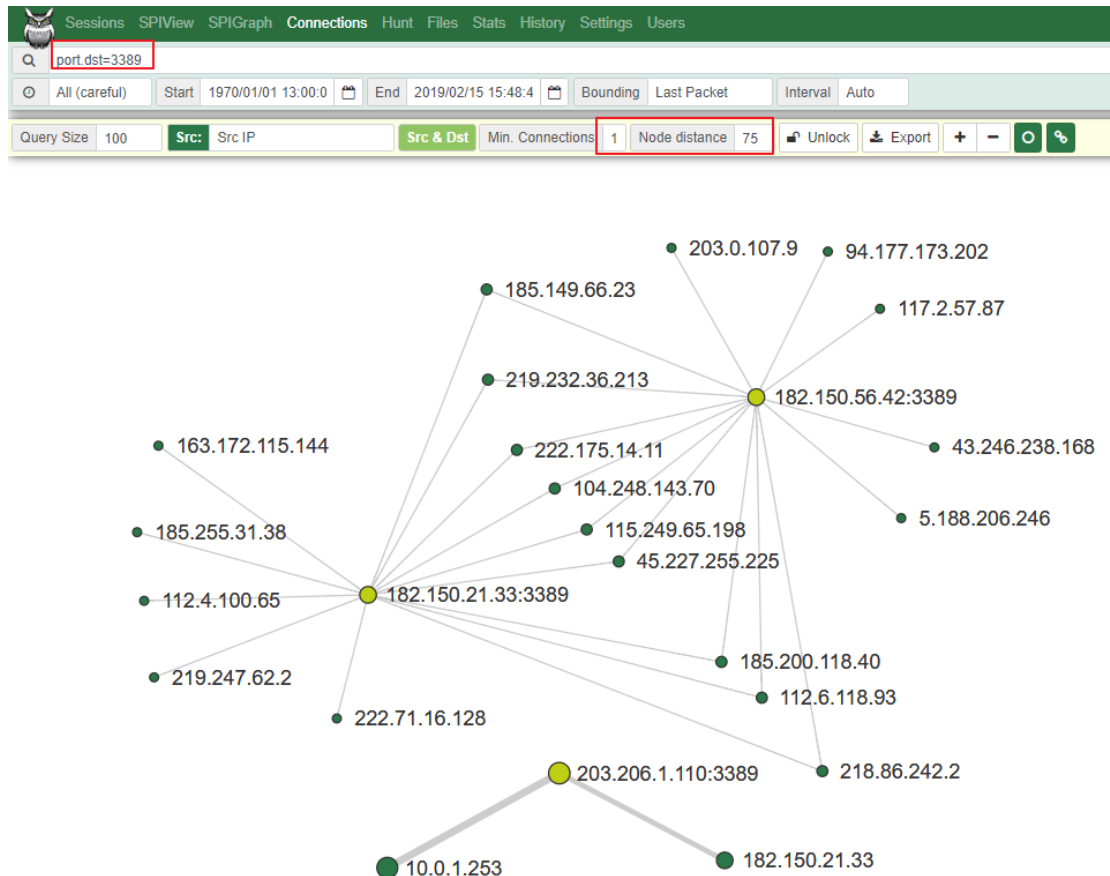
`host.dns== music.163.com`



上图中的 **Action** 支持将检索到的数据流以 PCAP 形式导出及 打上标签；对于数据流可以 `natural`、`asci`、`utf8` 等多种编码形式展示，流可以以 `image` 格式保存，对于简单的 `Xor` 及 `base64` 能进行解码。

检索局域网内利用 3389 端口进行通信的连接： `port.dst == port`

`port.dst == 3389`



利用表达式进行过滤后，在 Connections 中，可以看到与之节点的相关连接统计信息（一个华而不实的功能 :)..

更多 Search Expression 的运用，这里就不介绍了，Know it then do it.

Moloch 优化

1) 修改 moloch 的 config.ini 配置文件,在 High Performance settings 进行如下修改，降低丢包现象。

```
### High Performance settings
magicMode=basic
pcapReadMethod=tpacketv3
tpacketv3BlockSize=8388608
tpacketv3NumThreads=4
# tpacketv3NumThreads=2
pcapWriteMethod=simple
pcapWriteSize = 2560000
packetThreads=5
dbBulkSize=4000000
compressES=true
```

```
maxPacketsInQueue = 300000
```

2) pfring 安装

moloch 的 Capture 默认使用 libpcap 后面我们会用 pfring 提升抓包性能

```
# 官方建议 先去尝试 tpacketv3 我们上面用的就是, 如需更改可以如下:  
pfring We suggest you try tpacketv3 first if available on the host  
[root@moloch ~]# vim /data/moloch/etc/config.ini #修改  
rootPlugins=reader-pfring.so  
pcapReadMethod=pfring
```

3) 指定一个 PCAP 包目录

```
$ mkdir /data/moloch/pcap  
$ vim /data/moloch/etc/config.ini #进行如下配置  
# The directory to save raw pcap files to  
pcapDir = /data/moloch/pcap
```

4) 考虑数据的删除保留问题

```
$ vim /data/moloch/etc/config.ini  
freeSpaceG = 10% #
```

Moloch 日常维护技巧

查看 ES 启动情况

```
$ ps -ef | grep elasticsearch  
root      4045   3562  0 09:59 pts/1    00:00:00 su elasticsearch  
elastic+  4153       1 92 10:00 pts/1    00:00:09  
/usr/local/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -  
XX:CMSInitiatingOccupancyFraction=75 -  
XX:+UseCMSInitiatingOccupancyOnly -XX:+AlwaysPreTouch -Xss1m -  
Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djna.nosys=true -XX:-  
OmitStackTraceInFastThrow -Dio.netty.noUnsafe=true -  
Dio.netty.noKeySetOptimization=true -  
Dio.netty.recycler.maxCapacityPerThread=0 -  
Dlog4j.shutdownHookEnabled=false -Dlog4j2.disable.jmx=true -  
Djava.io.tmpdir=/tmp/elasticsearch.Ck5c9TqC -  
XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=data -  
XX:ErrorFile=logs/hs_err_pid%p.log -XX:+PrintGCDetails -  
XX:+PrintGCDateStamps -XX:+PrintTenuringDistribution -  
XX:+PrintGCApplicationStoppedTime -Xloggc:logs/gc.log -
```

```
XX:+UseGCLogFileRotation -XX:NumberOfGCLogFiles=32 -
XX:GCLogFileSize=64m -Des.path.home=/opt/ES6/elasticsearch-6.4.0 -
Des.path.conf=/opt/ES6/elasticsearch-6.4.0/config -
Des.distribution.flavor=default -Des.distribution.type=tar -cp
/opt/ES6/elasticsearch-6.4.0/lib/*
org.elasticsearch.bootstrap.Elasticsearch -d
elastic+ 4161 4046 0 10:00 pts/1 00:00:00 grep --color=auto
elasticsearch
```

如没有正常启动，需切换到用户 elasticsearch 启动

```
$ cd /opt/ES6/elasticsearch-6.4.0/bin
$ ./elasticsearch -d #-d 后台启动
$ kill -9 4153
```

常规检查与数据清除

这里也提供一些检查的清单：

Elasticsearch 健康状态检查

http://localhost:9200/_cat/health

数据库初始化检查

<http://localhost:9200>

可访问性检查

<http://viewerhostname:8005>

ES 节点检查

<http://viewerhostname:8005/stats?statsTab=2>

elasticsearch 中存储的 SPI 数据删除

`/data/moloch/db/db.pl ESHOST:ESPORT wipe` *#相对于 init 不会删除用户*

PCAP 包删除

`rm -rf /data/moloch/pcap` *#pcap 存储目录根据 config.ini 来确定，我这里是自己新建的 pcap*

重启 molochcapture

```
$ systemctl restart molochcapture.service
$ systemctl stop molochcapture.service
$ systemctl start molochcapture.service
$ systemctl status molochcapture.service
```

重启 molochviewer

```
$ systemctl restart molochviewer.service
$ systemctl stop molochviewer.service
```

```
$ systemctl start molochviewer.service
```

关闭 firewalld

```
$ systemctl stop firewalld
```

查看日志文件是否有错误

```
$ echo "" > capture.log #清除日志内容  
$ cat /data/moloch/logs/viewer.log  
$ cat /data/moloch/logs/capture.log
```

网卡配置

```
ethtool -G ens38 rx 4096 tx 4096 #设置环形缓冲区大小  
ethtool -K ens38 rx off tx off gs off tso off gso off #关闭功能, 查看  
ens38 的可用功能
```

参考链接

- <https://github.com/aol/moloch/wiki/FAQ>
- <https://github.com/aol/moloch/wiki/Settings>