数据库审计linux无法安装agent

数据库审计 **李云龙的意大利炮** 2020-09-11 发表

组网及说明

数据库服务器无法通过镜像流量来审计，需要安装agent客户端。

问题描述

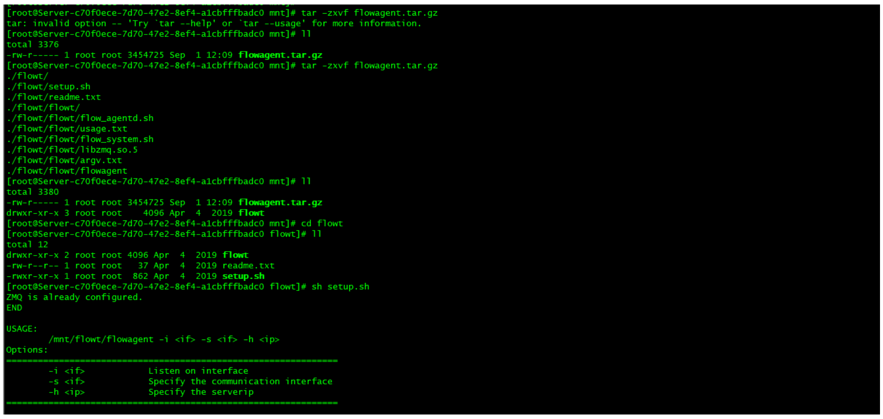
按照agent安装方法在linux上安装agent失败

过程分析

看报错内容，缺少什么就通过yum去安装什么，遇到错误上网查询

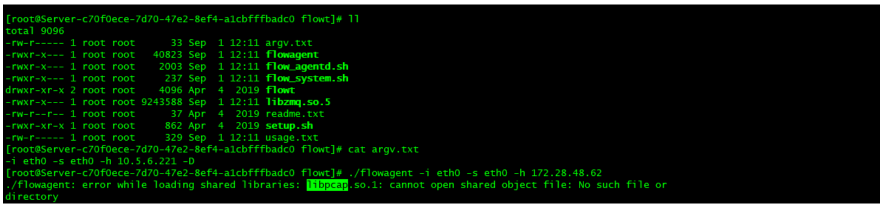
解决方法

首先将agent客户端通过ftp软件上传到服务器上，解压该文件



```
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 mnt]# tar -zxvf flowagent.tar.gz
tar: invalid option -- 'Try `tar --help' or `tar --usage' for more information.
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 mnt]# ll
total 3376
-rw-r----- 1 root root 3454725 Sep  1 12:09 flowagent.tar.gz
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 mnt]# tar -zxvf flowagent.tar.gz
./flowt/
./flowt/setup.sh
./flowt/readme.txt
./flowt/flowt/
./flowt/flowt/flow_agentd.sh
./flowt/flowt/usage.txt
./flowt/flowt/flow_system.sh
./flowt/flowt/libzmq.so.5
./flowt/flowt/argv.txt
./flowt/flowt/flowagent
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 mnt]# ll
total 3380
-rw-r----- 1 root root 3454725 Sep  1 12:09 flowagent.tar.gz
drwxr-xr-x 3 root root    4096 Apr  4  2019 flowt
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 mnt]# cd flowt
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# ll
total 12
drwxr-xr-x 2 root root 4096 Apr  4  2019 flowt
-rw-r--r-- 1 root root   37 Apr  4  2019 readme.txt
-rwxr-xr-x 1 root root  862 Apr  4  2019 setup.sh
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# sh setup.sh
ZMQ is already configured.
END

USAGE:
        /mnt/flowt/flowagent -i <if> -s <if> -h <ip>
Options:
================================================================
        -i <if>            Listen on interface
        -s <if>            Specify the communication interface
        -h <ip>            Specify the serverip
================================================================
```

解压完成以后执行命令安装，发现报错，报错为缺少libpcap.so.1

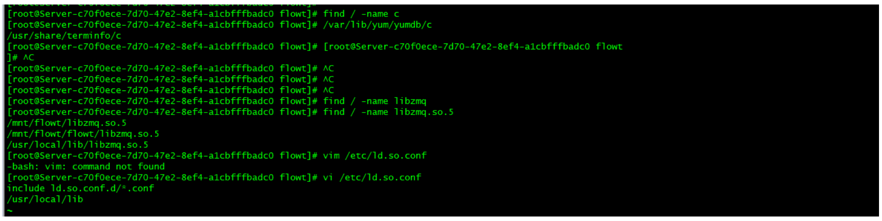


```
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# ll
total 9096
-rw-r----- 1 root root      33 Sep  1 12:11 argv.txt
-rwxr-x--- 1 root root   40823 Sep  1 12:11 flowagent
-rwxr-x--- 1 root root    2003 Sep  1 12:11 flow_agentd.sh
-rwxr-x--- 1 root root     237 Sep  1 12:11 flow_system.sh
drwxr-xr-x 2 root root    4096 Apr  4  2019 flowt
-rwxr-x--- 1 root root 9243588 Sep  1 12:11 libzmq.so.5
-rw-r--r-- 1 root root      37 Apr  4  2019 readme.txt
-rwxr-xr-x 1 root root     862 Apr  4  2019 setup.sh
-rw-r----- 1 root root     329 Sep  1 12:11 usage.txt
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# cat argv.txt
-i eth0 -s eth0 -h 10.5.6.221 -D
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# ./flowagent -i eth0 -s eth0 -h 172.28.48.62
./flowagent: error while loading shared libraries: libpcap.so.1: cannot open shared object file: No such file or
directory
```

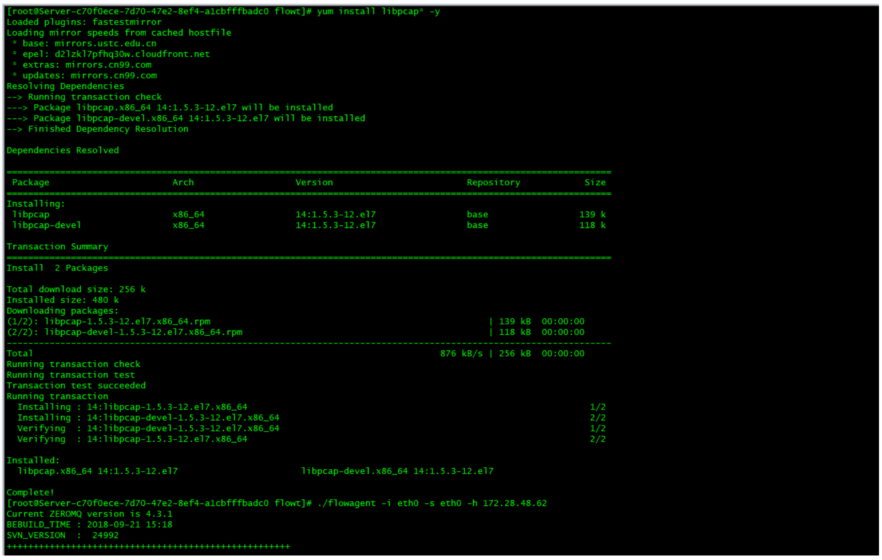
上网查询，某个网站是这样解决的https://blog.csdn.net/Sunny_Future/article/details/105410625

于是按照该方法添加以后，还需要yun安装一下libpcap,

*libpcap*是unix/linux平台下的网络数据包捕获函数包，大多数网络监控软件都以它为基础.

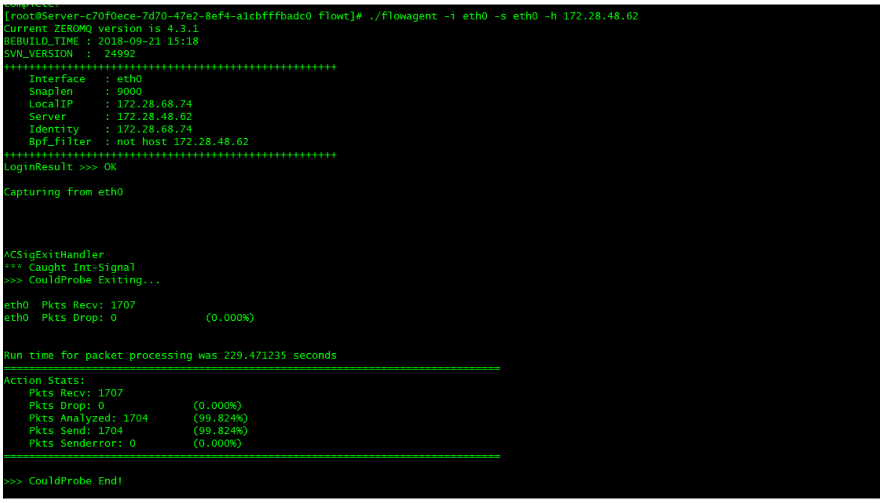


```
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# find / -name c
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# /var/lib/yum/yumdb/c
/usr/share/terminfo/c
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# [root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt
]# ^C
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# ^C
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# ^C
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# ^C
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# find / -name libzmq
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# find / -name libzmq.so.5
/mnt/flowt/libzmq.so.5
/mnt/flowt/flowt/libzmq.so.5
/usr/local/lib/libzmq.so.5
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# vim /etc/ld.so.conf
-bash: vim: command not found
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# vi /etc/ld.so.conf
include ld.so.conf.d/*.conf
/usr/local/lib
~
```



```
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# yum install libpcap* -y
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.ustc.edu.cn
 * epel: d2lzkl7pfhq30w.cloudfront.net
 * extras: mirrors.cn99.com
 * updates: mirrors.cn99.com
Resolving Dependencies
--> Running transaction check
---> Package libpcap.x86_64 14:1.5.3-12.el7 will be installed
---> Package libpcap-devel.x86_64 14:1.5.3-12.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

==========================================================================================================
 Package                      Arch                    Version                         Repository     Size
==========================================================================================================
Installing:
 libpcap                      x86_64                  14:1.5.3-12.el7                 base          139 k
 libpcap-devel                x86_64                  14:1.5.3-12.el7                 base          118 k

Transaction Summary
==========================================================================================================
Install  2 Packages

Total download size: 256 k
Installed size: 480 k
Downloading packages:
(1/2): libpcap-1.5.3-12.el7.x86_64.rpm                                              | 139 kB  00:00:00
(2/2): libpcap-devel-1.5.3-12.el7.x86_64.rpm                                        | 118 kB  00:00:00
----------------------------------------------------------------------------------------------------------
Total                                                                     876 kB/s | 256 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 14:libpcap-1.5.3-12.el7.x86_64                                                         1/2
  Installing : 14:libpcap-devel-1.5.3-12.el7.x86_64                                                   2/2
  Verifying  : 14:libpcap-devel-1.5.3-12.el7.x86_64                                                   1/2
  Verifying  : 14:libpcap-1.5.3-12.el7.x86_64                                                         2/2

Installed:
  libpcap.x86_64 14:1.5.3-12.el7                       libpcap-devel.x86_64 14:1.5.3-12.el7

Complete!
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# ./flowagent -i eth0 -s eth0 -h 172.28.48.62
Current ZEROMQ version is 4.3.1
BEBUILD_TIME : 2018-09-21 15:18
SVN_VERSION  :  24992
+++++++++++++++++++++++++++++++++++++++++++++++++++++
```

yum安装完以后，执行命令，安装成功



```
[root@Server-c70f0ece-7d70-47e2-8ef4-a1cbfffbadc0 flowt]# ./flowagent -i eth0 -s eth0 -h 172.28.48.62
Current ZEROMQ version is 4.3.1
BEBUILD_TIME : 2018-09-21 15:18
SVN_VERSION  :  24992
+++++++++++++++++++++++++++++++++++++++++++++++++++++
    Interface   : eth0
    Snaplen     : 9000
    LocalIP     : 172.28.68.74
    Server      : 172.28.48.62
    Identity    : 172.28.68.74
    Bpf_filter  : not host 172.28.48.62
+++++++++++++++++++++++++++++++++++++++++++++++++++++
LoginResult >>> OK

Capturing from eth0




^CSigExitHandler
*** Caught Int-Signal
>>> CouldProbe Exiting...

eth0  Pkts Recv: 1707
eth0  Pkts Drop: 0               (0.000%)


Run time for packet processing was 229.471235 seconds
===============================================================================
Action Stats:
    Pkts Recv: 1707
    Pkts Drop: 0                (0.000%)
    Pkts Analyzed: 1704         (99.824%)
    Pkts Send: 1704             (99.824%)
    Pkts Senderror: 0           (0.000%)
===============================================================================

>>> CouldProbe End!
```

然后数据库探针添加服务器地址，正常审计数据库。