Zeek Cluster Installation and Configuration

Zeek documentation is quite good. The best reference for information on Zeek components and configuration can be found at https://docs.zeek.org/en/stable/intro/index.html.

For further information and troubleshooting help, the Zeek mailing list has a large amount of information. http://mailman.icsi.berkeley.edu/pipermail/zeek/

Compiling Zeek

By default, Zeek will be installed to /usr/local/bro (or /usr/local/zeek) and you will place the configs in {bro/zeek}/etc.

Prerequisites: https://docs.zeek.org/en/stable/install/install.html#prerequisites

We compile Zeek with tcmalloc, GeoIP and PF_RING support.

- Installing gperftools will make Zeek automatically compile with tcmalloc support.
- GeoIP information can be found at https://docs.zeek.org/en/stable/frameworks/geoip.html#geolocation.
- PF_RING information can be found at https://docs.zeek.org/en/stable/configuration/index.html#pf-ring-cluster-configuration

Compiling Zeek

```
# First install some dependencies
yum install cmake make gcc gcc-c++ flex bison libpcap-devel openssl-devel
python-devel swig zlib-devel

# Install gperftools for tcmalloc support
yum install gperftools

# Download and compile PF_RING
PF_RING_VERSION=7.4.0
wget https://github.com/ntop/PF_RING/archive/$PF_RING_VERSION.tar.gz
tar -xzf $PF_RING_VERSION.tar.gz

cd PF_RING-$PF_RING_VERSION/userland/lib
./configure --prefix=/opt/pfring
make install

cd ../libpcap
./configure --prefix=/opt/pfring
make install

cd ../tcpdump
./configure --prefix=/opt/pfring
make install

cd ../../kernel
make
make install

# Install deps for GeoIP
yum install libmaxminddb-devel

# Grab the GeoIP databases
wget http://geolite.maxmind.com/download/geoip/database/GeoLite2-City.tar.
gz
tar xvf GeoLite2-City.tar.gz
mv GeoLite2-City_<date>/GeoLite2-City.mmdb /usr/share/GeoIP/

# Download and compile Zeek
BRO_VERSION=2.6.2
wget https://www.zeek.org/downloads/bro-$BRO_VERSION.tar.gz
tar xvfz bro-$BRO_VERSION.tar.gz
cd bro-$BRO_VERSION

# configure with PF_RING pcap location
./configure --with-pcap=/opt/pfring
make
make install
```

Verify Zeek Installation

Check to see if Zeek is linked to PF_RING libpcap and tcmalloc.

```
[bro@bro-a000 ~]$ ldd /usr/local/bro/bin/bro | egrep 'tcmalloc|libpcap'
    libpcap.so.1 => /opt/pfring/lib/libpcap.so.1 (0x00002b726499c000)
    libtcmalloc.so.4 => /usr/lib64/libtcmalloc.so.4 (0x00002b7265996000)
```

Check to see if GeoIP lookups are working.

```
# Interestingly, Purdue's subnets don't have region or city defined in the
databases
[bro@bro-a000 ~]$ bro -e "print lookup_location(128.211.X.Y);"
[country_code=US, region=<uninitialized>, city=<uninitialized>,
latitude=37.751, longitude=-97.822]

# CERN subnets are defined with region and city
[bro@bro-a000 ~]$ bro -e "print lookup_location(137.138.X.Y);"
[country_code=CH, region=GE, city=Geneva, latitude=46.2022, longitude=6.
1457]
```

Load PF_RING at Boot Time

Add pfring.conf to /etc/modules-load.d and pfring.conf to /etc/modprobe.d.

```
[bro@bro-a000 modules-load.d]$ pwd
/etc/modules-load.d
[bro@bro-a000 modules-load.d]$ cat pfring.conf
pf_ring

[bro@bro-a000 modprobe.d]$ pwd
/etc/modprobe.d
[bro@bro-a000 modprobe.d]$ cat pfring.conf
# Load PF_RING with the correct settings
options pf_ring enable_tx_capture=0 min_num_slots=32768
```

Pulsar Zeek Cluster Architecture

Documentation for cluster components and configuration can be found at https://docs.zeek.org/en/stable/configuration/index.html.

Manager, logger, and one proxy run on a Virtual Machine with 4 CPUs and 32 GB RAM. Typically, CPU utilization is 50% while used memory is ~6GB. This VM also runs Filebeat to send Zeek logs to Kafka.

Eight physical machines run Zeek worker processes. Each machine has:

- 2x Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz (24 cores total)
- 192 GB RAM (underutilized with typically ~36 GB used, ~5 GB cached)
- Dual port Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (i40e driver version 2.7.29)
- 11 Zeek workers are pinned to 11 cores on each CPU leaving 2 cores open on each machine
- Zeek compiled with tcmalloc, GeoIP and PF_RING support
- CentOS 7.6

Zeek Worker NIC Tweaks

The following tweaks should be applied to each NIC on Zeek workers.

- Set NIC to promiscuous mode
- Set MTU to 9000
- Disable NIC offloading features, see https://blog.securityonion.net/2011/10/when-is-full-packet-capture-not-full.html
  - If high capture loss is present, it might be due to the NIC combining frames before passing them up the stack. The larger frames cannot be analyzed by Zeek when pcapsnaplen is set to 9216.
  - This issue was present on our workers and confirmed via packet analysis of pcaps in Wireshark, single frames were observed to be > 16000 bytes
  - After running the suggested commands to disable those features, all frames were < 9216 bytes and capture loss significantly decreased
- Increase RX/TX buffer size (the impact of this change was not quantified)

These changes are applied to both NICs on system startup in rc.local

NIC tweaks in rc.local

```
# Update NICs with necessary changes
for nic in enp59s0f0 enp59s0f1
  do

  # Set Promiscuous mode on
  ip link set $nic promisc on

  # Setting MTU to 9000
  ifconfig $nic mtu 9000 up

  # Disable NIC features that interfere with Zeek
  for i in rx tx sg tso ufo gso gro lro
    do ethtool -K $nic $i off
  done

  # Increase RX/TX buffers
  ethtool -G $nic rx 4096 tx 4096
done
```

Zeek Configuration

There are three main config files that are needed to run Zeek: node.cfg, networks.cfg and broctl.cfg.

networks.cfg

Defines what networks are considered "local" to your institution. Defining these networks will make the Zeek logs more informative as connections will be marked as originating from local or remote addresses. This information can be used to modify alerting based on location, i.e. only alert via email if a port scan comes from a local address.

```
# List of local networks in CIDR notation, optionally followed by a
# descriptive tag.
# For example, "10.0.0.0/8" or "fe80::/64" are valid prefixes.

10.0.0.0/8          Private IP space
172.16.0.0/12       Private IP space
192.168.0.0/16      Private IP space
X.X.0.0/16          Local network #1
Y.Y.0.0/16          Local network #2
```

node.cfg

Defines the architecture of the Zeek cluster.

We use a more descriptive name for Zeek workers than the typical [worker-1]. The name follows the convention [<hostname>-<nic port #>]. The worker name is a column in the connection log and using a meaningful name makes it easier to identify problems with either a worker or a specific NIC.

```
[manager]
type=manager
host=<manager host IP>

[proxy-0]
type=proxy
host=<manager host IP>

[logger-0]
type=logger
host=<manager host IP>

[bro-a000-0]
type=worker
host=172.18.X.Y
interface=enp59s0f0
lb_method=pf_ring
lb_procs=11
pin_cpus=0,2,4,6,8,10,12,14,16,18,20

[bro-a000-1]
type=worker
host=172.18.X.Y
interface=enp59s0f1
lb_method=pf_ring
lb_procs=11
pin_cpus=1,3,5,7,9,11,13,15,17,19,21

[bro-a001-0]
type=worker
host=172.18.X.Z
interface=enp59s0f0
lb_method=pf_ring
lb_procs=11
pin_cpus=0,2,4,6,8,10,12,14,16,18,20

[bro-a001-1]
type=worker
host=172.18.X.Z
interface=enp59s0f1
lb_method=pf_ring
lb_procs=11
pin_cpus=1,3,5,7,9,11,13,15,17,19,21
```

broctl.cfg

The most important changes to broctl.cfg are listed below. The cluster ID and snaplen changes were found when originally deploying Bro 2.5. Defining the pfring cluster ID is a critical step. If this ID is not defined, all Zeek workers on a host will receive copies **all** packets sent to the host. If 100% CPU utilization is seen across all Zeek workers on a host and duplicate traffic is seen in the connection log or via "bro doctor" you might have this problem. Increasing the snaplen is required for Jumbo Ethernet Frame support in versions below Zeek 2.6.

A complete configuration reference can be found at https://github.com/zeek/zeekctl.

broctl.cfg

```
################################################
# Mail Options

# Recipient address for all emails sent out by Bro and BroControl.
MailTo = email@somewhere.com

...
<snip>
...

# Set the pfring cluster ID
pfringclusterid=21

# Change snaplen to support jumbo frames
pcapsnaplen=9216
```

Broctl cron configuration

The broctl cron command checks the status of the cluster and will restart any failed components. The command should run every few minutes on the manager host to ensure the cluster is operating properly. Adding the following **broctl-cron** crontab will make it run every 5 minutes.

```
*/5 * * * * root /usr/local/bro/bin/broctl cron
```

Managing the Zeek Cluster

Running `broctl deploy` on the manager node will start the cluster. The manager uses ssh to configure all the worker nodes. Some type of password-less SSH authentication (either public key or host based) must be configured

Note: Before running `broctl deploy` for the first time one must first ssh into all child nodes from the master and accept their host keys.

Check the status of the cluster with the `broctl status` command.

```
root@pulsar-master:~ $ broctl status
Name         Type    Host             Status    Pid    Started
logger-1     logger  172.18.X.A      running   32596  12 Jul 16:18:40
manager      manager 172.18.X.A      running   32637  12 Jul 16:18:42
proxy-1      proxy   172.18.X.A      running   4131   13 Jul 01:55:04
bro-a000-0-1 worker  172.18.X.B      running   10324  12 Jul 16:18:45
bro-a000-0-2 worker  172.18.X.B      running   10348  12 Jul 16:18:45
<snip>
bro-a007-1-10 worker  172.18.X.C      running   10316  12 Jul 16:18:45
bro-a007-1-11 worker  172.18.X.C      running   10317  12 Jul 16:18:45
```