Elasticsearch Heap Adjustment

1. From the `Manager Node`, navigate to the directory listed below and open the file `<managername>.sls`.
   `/opt/so/saltstack/local/pillar/minions/`

2. Adjust the `<esheap: '####m'>` setting to half of the available ram allocated to the manager node and not to exceed 32GB (see documentation).
   https://www.elastic.co/guide/en/elasticsearch/reference/7.17/advanced-configuration.html#set-jvm-heap-size

```
manager:
  mainip: '172.16.1.8'
  mainint: 'ens224'
  esheap: '4066m'
  esclustername: {{ grains.host }}
  freq: 0
  domainstats: 0
  mtu:
  elastalert: 1
  es_port: 9200
  log_size_limit: 262
  cur_close_days: 30
  grafana: 1
  osquery: 1
  thehive: 1
  playbook: 1

elasticsearch:
  mainip: '172.16.1.8'
  mainint: 'ens224'
  esheap: '4066m'
  esclustername: {{ grains.host }}
  node_type: ''
  es_port: 9200
  log_size_limit: 262
  node_route_type: 'hot'
```

3. Save the file and restart **Elasticsearch** with `so-restart elasticsearch`

4. Verify the changes took effect by running `GET _cat/nodes?h=heap*` from Dev Tools in Kibana.

Zeek and Suricata CPU Adjustment

One reason a user may submit a ticket for an increase in vCPUs on a sensor is a large amount of dropped packets by **Suricata** or **Zeek**. Suricata and Zeek are CPU-intensive and when starved for resources, these tools drop packets. Either of these tools dropping packets is a sign there are insufficient processor cores available to handle the volume of traffic ingestion within the range. This behavior is rare within PCTE deployments. If increasing vCPUs alone does not resolve the issue, perform the following steps to adjust the number of cores each tool will utilize for processing.

1. From the `Manager Node`, navigate to the directory listed below and open the file `<sensorname>.sls`. `/opt/so/saltstack/local/pillar/minions/`
2. Adjust `zeek_lbprocs: #` and/or `suriprocs: #` as necessary, ensuring you do not exceed the number of available cores.

```
sensor:
  interface: 'bond0'
  mainip: '192.168.1.100'
  mainint: 'ens33'
  zeek_lbprocs: 2
  suriprocs: 2
  manager: ''
  mtu: 1500
  uniqueid: 1646451543
  hnsensor:
```

4. Write and save the file.
5. Perform **Step 2** for each sensor minion where a vCPU change was made.
6. Update `Salt` from the manager by running `sudo salt-call state.highstate`
7. Restart **Suricata** and/or **Zeek** `sudo salt $SENSORNAME_$ROLE state.apply suricata` | `sudo salt $SENSORNAME_$ROLE state.apply zeek`

Extending NSM Volume After New Disk Allocation

```
sudo pvcreate /dev/sdb
sudo lvmdiskscan -l
sudo vgextend system /dev/sdb
sudo lvextend -l +100%FREE /dev/system/nsm
sudo xfs_growfs /dev/system/nsm
df -h
```