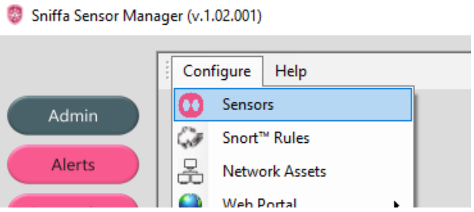
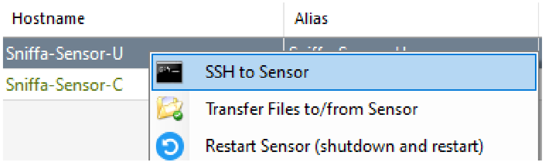
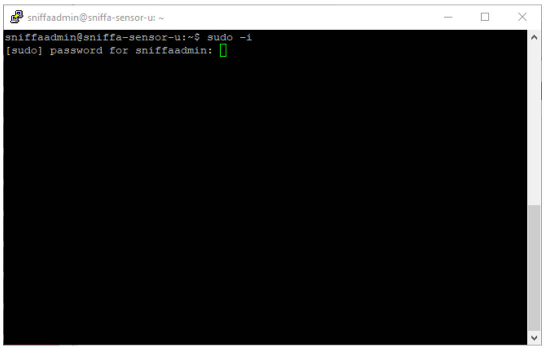
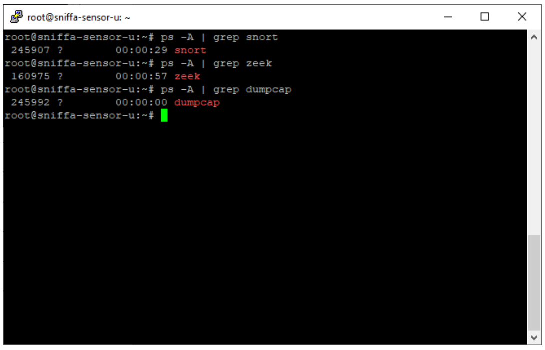
Sniffa Runbook
Troubleshooting the Sniffa NSS Sensor

Serial	Instruction	
	Overview This runbook includes the tasks needed to be completed, to troubleshoot a Sniffa NSS remote Sensor on the network and show it is operating as is expected.	
1.	**Open the Sensor Manager Application.** Go to the Admin Panel. Click on the ‘Configure’ menu item. Click on the ‘Sensors’ menu item.	 Sniffa Sensor Manager (v.1.02.001) Configure Help Admin Alerts Sensors Snort™ Rules Network Assets Web Portal
2.	Right click on the Sensor you want to troubleshoot. Click on the ‘SSH to Sensor’ menu item.	 Hostname Alias Sniffa-Sensor-U Sniffa-Sensor-C SSH to Sensor Transfer Files to/from Sensor Restart Sensor (shutdown and restart)

3.	Run commands:
	`sudo -i`
	Enter password
		
		`sniffaadmin@sniffa-sensor-u:~$ sudo -i`
		`[sudo] password for sniffaadmin:`

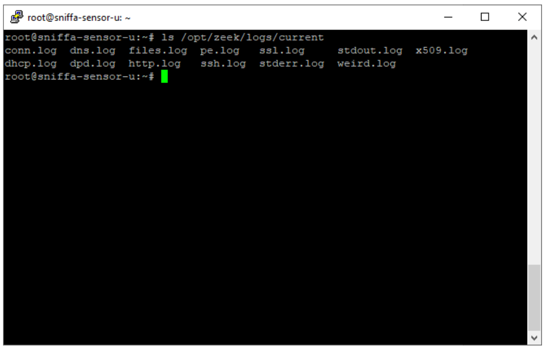
4.	Check the services are running.
	Run commands:
	`ps -A | grep snort`
	`ps -A | grep zeek`
	`ps -A | grep dumpcap`
		
		`root@sniffa-sensor-u:~# ps -A | grep snort`
		` 245907 ?        00:00:29 snort`
		`root@sniffa-sensor-u:~# ps -A | grep zeek`
		` 160975 ?        00:00:57 zeek`
		`root@sniffa-sensor-u:~# ps -A | grep dumpcap`
		` 245992 ?        00:00:00 dumpcap`
		`root@sniffa-sensor-u:~#`

6.

Check Zeek logs are being written to the correct directory.

Run commands:

```
ls /opt/zeek/logs/current
```



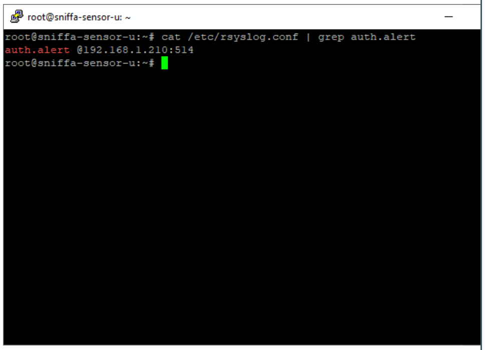
```
root@sniffa-sensor-u:~# ls /opt/zeek/logs/current
conn.log  dns.log  files.log  pe.log   ssl.log     stdout.log  x509.log
dhcp.log  dpd.log  http.log   ssh.log  stderr.log  weird.log
root@sniffa-sensor-u:~#
```

7.

Check that rsyslogd is configured to send alert log messages to the correct IP address.

Run commands:

```
cat /etc/rsyslog.conf | grep auth.alert
```



```
root@sniffa-sensor-u:~# cat /etc/rsyslog.conf | grep auth.alert
auth.alert @192.168.1.210:514
root@sniffa-sensor-u:~#
```

8.

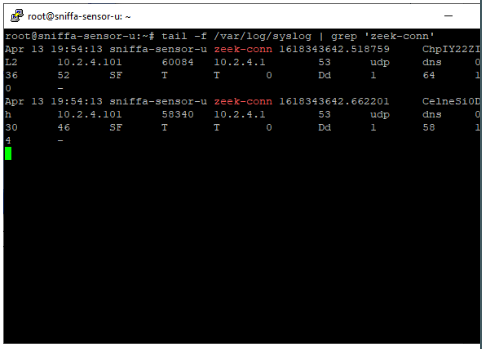
Check that rsyslogd is sending alert log messages to syslog.

Run commands:

```
tail -f /var/log/syslog | grep ‘zeek-conn’
```

Note:

Hit Ctl + C to stop.



```
root@sniffa-sensor-u:~# tail -f /var/log/syslog | grep 'zeek-conn'
Apr 13 19:54:13 sniffa-sensor-u zeek-conn 1618343642.518759     ChpIY22ZI
L2      10.2.4.101      60084   10.2.4.1        53      udp     dns     0
36      52      SF      T       T       0       Dd      1       64      1
0       -
Apr 13 19:54:13 sniffa-sensor-u zeek-conn 1618343642.662201     CelneSi0D
h       10.2.4.101      58340   10.2.4.1        53      udp     dns     0
30      46      SF      T       T       0       Dd      1       58      1
4       -
```

9.

Check Snort™ rules files are present.

Run commands:

```
ls /etc/snort/rules
```

Check that sniffa.rules is not empty.

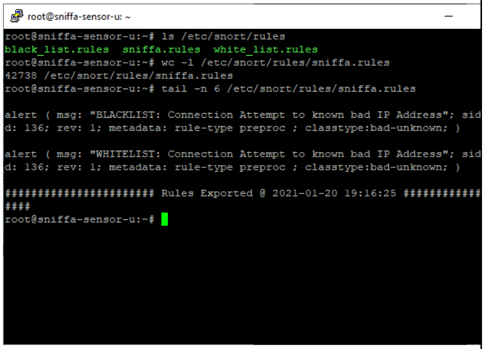
Run commands:

```
wc -l /etc/snort/rules/sniffa.rules
```

Check date of last rules update.

Run commands:

```
tail -n 6 /etc/snort/rules/sniffa.rules
```



```
root@sniffa-sensor-u:~# ls /etc/snort/rules
black_list.rules  sniffa.rules  white_list.rules
root@sniffa-sensor-u:~# wc -l /etc/snort/rules/sniffa.rules
42738 /etc/snort/rules/sniffa.rules
root@sniffa-sensor-u:~# tail -n 6 /etc/snort/rules/sniffa.rules

alert ( msg: "BLACKLIST: Connection Attempt to known bad IP Address"; sid
d: 136; rev: 1; metadata: rule-type preproc ; classtype:bad-unknown; )

alert ( msg: "WHITELIST: Connection Attempt to known bad IP Address"; sid
d: 136; rev: 1; metadata: rule-type preproc ; classtype:bad-unknown; )

###################### Rules Exported @ 2021-01-20 19:16:25 ###########
####
root@sniffa-sensor-u:~#
```

Sniffa Runbook
Troubleshooting the Sniffa NSS Sensor

10. Send a Sniffa Heartbeat Message to Syslog.

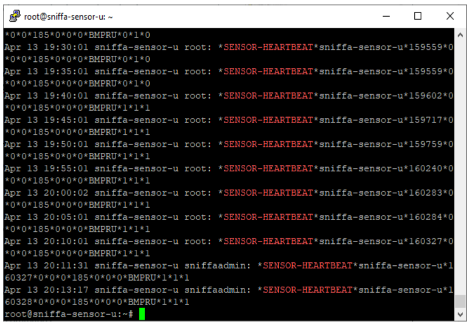
Run commands:

```
bash /usr/local/sniffa/heartbeat/heartbeat
```

Check heartbeat message was logged by syslog.

Run commands:

```
cat /var/log/syslog | grep HEARTBEAT
```

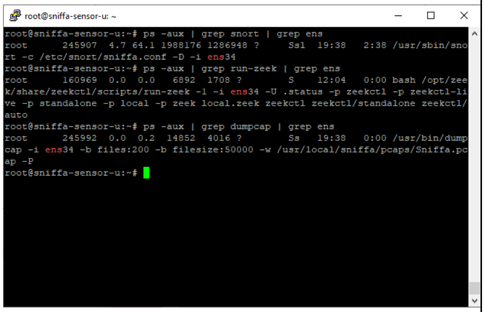


```
root@sniffa-sensor-u: ~
*0*0*185*0*0*0*BMPRU*0*1*0
Apr 13 19:30:01 sniffa-sensor-u root: *SENSOR-HEARTBEAT*sniffa-sensor-u*159559*0
*0*0*185*0*0*0*BMPRU*0*1*0
Apr 13 19:35:01 sniffa-sensor-u root: *SENSOR-HEARTBEAT*sniffa-sensor-u*159559*0
*0*0*185*0*0*0*BMPRU*0*1*0
Apr 13 19:40:01 sniffa-sensor-u root: *SENSOR-HEARTBEAT*sniffa-sensor-u*159602*0
*0*0*185*0*0*0*BMPRU*1*1*1
Apr 13 19:45:01 sniffa-sensor-u root: *SENSOR-HEARTBEAT*sniffa-sensor-u*159717*0
*0*0*185*0*0*0*BMPRU*1*1*1
Apr 13 19:50:01 sniffa-sensor-u root: *SENSOR-HEARTBEAT*sniffa-sensor-u*159759*0
*0*0*185*0*0*0*BMPRU*1*1*1
Apr 13 19:55:01 sniffa-sensor-u root: *SENSOR-HEARTBEAT*sniffa-sensor-u*160240*0
*0*0*185*0*0*0*BMPRU*1*1*1
Apr 13 20:00:02 sniffa-sensor-u root: *SENSOR-HEARTBEAT*sniffa-sensor-u*160283*0
*0*0*185*0*0*0*BMPRU*1*1*1
Apr 13 20:05:01 sniffa-sensor-u root: *SENSOR-HEARTBEAT*sniffa-sensor-u*160284*0
*0*0*185*0*0*0*BMPRU*1*1*1
Apr 13 20:10:01 sniffa-sensor-u root: *SENSOR-HEARTBEAT*sniffa-sensor-u*160327*0
*0*0*185*0*0*0*BMPRU*1*1*1
Apr 13 20:11:31 sniffa-sensor-u sniffaadmin: *SENSOR-HEARTBEAT*sniffa-sensor-u*1
60327*0*0*0*185*0*0*0*BMPRU*1*1*1
Apr 13 20:13:17 sniffa-sensor-u sniffaadmin: *SENSOR-HEARTBEAT*sniffa-sensor-u*1
60328*0*0*0*185*0*0*0*BMPRU*1*1*1
root@sniffa-sensor-u:~#
```

11. Check services are using the correct interface to listen on.

Run commands:

```
ps -aux | grep snort | grep ens
ps -aux | grep run-zeek | grep ens
ps -aux | grep dumpcap | grep ens
```



```
root@sniffa-sensor-u: ~
root@sniffa-sensor-u:~# ps -aux | grep snort | grep ens
root      245907  4.7 64.1 1988176 1286948 ?     Ssl  19:38   2:38 /usr/sbin/sno
rt -c /etc/snort/sniffa.conf -D -i ens34
root@sniffa-sensor-u:~# ps -aux | grep run-zeek | grep ens
root      160969  0.0  0.0   6892  1708 ?        S    12:04   0:00 bash /opt/zee
k/share/zeekctl/scripts/run-zeek -1 -i ens34 -U .status -p zeekctl -p zeekctl-li
ve -p standalone -p local -p zeek local.zeek zeekctl zeekctl/standalone zeekctl/
auto
root@sniffa-sensor-u:~# ps -aux | grep dumpcap | grep ens
root      245992  0.0  0.2  14852  4016 ?        Ss   19:38   0:00 /usr/bin/dump
cap -i ens34 -b files:200 -b filesize:50000 -w /usr/local/sniffa/pcaps/Sniffa.pc
ap -P
root@sniffa-sensor-u:~#
```

12. End of Runbook.