This covers the steps needed to troubleshoot syslog alerting from AC-Hunter.

In this document *ac_hunter* is the ip address of the host system running the AC-Hunter docker containers and *syslog_server* refers to the ip address of the system waiting to accept logs from AC-Hunter. When running any command below with one of these, please substitute the correct IP address.

Please follow the steps until you reach one that fails. When you contact support (see the end for details on how to contact support), please mention the document date, which steps passed and which steps failed. Please also send along any error messages you find.

Many of the following steps require you to be logged in to one or both servers; we encourage you to leave open an ssh connection to both machines. You'll need to be logged into an account that can run commands under sudo (to test, run "`sudo whoami`"; if you do not get "`root`" when you enter your own password, please check with the system manager and get sudo privileges.

When doing these steps, please be careful about cutting and pasting any commands or text to go into a file. It's possible that quotes get turned into "smart quotes", spaces get turned into tabs, tabs get turned into spaces, etc. If you have any questions about what exact text should be used, please contact support.

Before editing any file, please make a backup of it. In that way, you can always return to a working state by restoring the old version and restarting AC-Hunter.

Finally, *please keep track of the changes you make*. Some of the files you edit may be overwritten during an AC-Hunter or system upgrade; we encourage you to note the needed changes and/or keep dated backups.

1. Upgrade AC-Hunter

If you're running AC-Hunter 5.1.0 or 5.2.0, please upgrade to 5.3.0 first. Both 5.1.0 and 5.2.0 contained a bug that blocked sending syslog messages. 5.3.0 has a fix for this bug.

2. Confirm that all AC-Hunter docker instances are running:

```
sudo docker ps | egrep 'STATUS|a[ic]hunter_'
```

```
CONTAINER ID        IMAGE                                      COMMAND                  CREATED
STATUS              PORTS                                                          NAMES

c29ef8032491        ai-hunter/web:latest                       "/usr/local/openrest…"   27 hours
ago         Up 27 hours         0.0.0.0:80->80/tcp, 0.0.0.0:443->443/tcp, 27017/tcp
aihunter_web

07889acbc091        ai-hunter/api:latest                       "/bin/bash /home/api…"   27 hours
ago         Up 27 hours         8080/tcp
aihunter_api
```

```
cfaf3d540c0d        ai-hunter/auth:latest                 "uwsgi /home/app/wsg…"   27 hours
ago         Up 27 hours         8000/tcp
aihunter_auth

d49c8a8b3afe        mongo:3.6.17-xenial                   "docker-entrypoint.s…"   27 hours
ago         Up 27 hours         27017/tcp
aihunter_db
```

a. Check that these 4 instances (aihunter_web, aihunter_api, aihunter_auth, aihunter_db) are running at all. If they aren't, run:

```
hunt down ; hunt up -d
```

b. Check the STATUS column (In the above output, these are all "Up 27 hours"). If these are below 5 minutes, the particular docker container may be crashing soon after restarting; please contact support.

3. **Can you ping the *syslog_server* from *ac_hunter*?** On *ac_hunter*, run:

```
ping -c 5 syslog_server
```

a. If you get no replies, make sure that syslog_server is reachable from ac_hunter.

4. **Do you have a running syslog software package on the *syslog_server* machine?** On that system run:

```
ps ax | grep -i log
```

a. You should see an entry for syslogd or rsyslogd. If you do not, please install, configure, and start the appropriate syslog server for your *syslog_server* machine. Centos and Ubuntu systems commonly use "rsyslogd"; potential blogs for setting this up:

https://www.howtoforge.com/how-to-setup-rsyslog-server-on-ubuntu-1804/
https://computingforgeeks.com/configure-rsyslog-centralized-log-server-on-ubuntu/
https://www.tecmint.com/create-centralized-log-server-with-rsyslog-in-centos-7/

Whenever you make changes to your syslog configuration, make sure you restart syslog with the commands in the appropriate blog.

b. If you've not already done so, make sure your syslog server is listening on UDP and/or TCP port 514 for incoming connections. The above blogs show how to turn on this listener as it's not enabled by default. To check that your syslog software is listening on this port, run:

```
sudo netstat -anp | grep '^..p' | grep ':514'
```

If you get no lines of output, syslog is not ready to accept incoming syslog messages from the network. If you get a line starting with "tcp", you're ready to accept TCP port 514 messages. If you get a line starting with "udp", you're ready to accept UDP port 514 messages. You may wish to leave both enabled while you do the following troubleshooting, and when all is working shut off the one you don't use.

c. Is that syslog program configured to send "user.alert" messages to a specific file? On the syslog server run:

```
logger -p user.alert -n 127.0.0.1 --udp --tag ' localhost_logtest ' "udp
$RANDOM.$RANDOM"
```

You should see this log line show up in /var/log/syslog with:

```
sudo tail -n 200 syslog | grep localhost_logtest
```

Sample output; yours will differ:

```
Jun 22 15:48:59 demo.aihhosted.com [localhost_logtest] - [timeQuality
tzKnown="1" isSynced="1" syncAccuracy="355000"] udp 5055.28272
```

If it doesn't show up, perhaps it's being sent to a different file. Try:

```
sudo grep localhost_logtest /var/log/* 2>/dev/null | grep -v 'grep localhost_logtest'
```

On my system these show up in /var/log/syslog:

```
/var/log/syslog:Jun 22 15:48:59 demo.aihhosted.com
[localhost_logtest] - [timeQuality tzKnown="1" isSynced="1"
syncAccuracy="355000"] udp 5055.28272
```

Please use the filename you see in your output instead of /var/log/syslog or /var/log/messages in the following instructions.

d. .

e.

5. **Can you send syslog messages from *ac_hunter* to *syslog_server*?** On syslog_server, run:

```
tail -f /var/log/syslog /var/log/messages
```

(Note: if your syslog software is told to direct messages to a different file, please use that instead of /var/log/syslog and /var/log/messages.)

On *ac_hunter*, run:

```
logger -n syslog_server -P 514 --udp --tag ' hostlogger ' "udp $RANDOM"
```

If you're planning to send traffic over TCP instead of UDP, use

```
logger -n syslog_server -P 514 --tcp --tag ' hostlogger ' "tcp $RANDOM"
```

instead.

a. Does "udp *randomnumber*" or "tcp *randomnumber*" show up in the output of the "tail" command running on *syslog_server*? If not, retry the command. If you still get nothing, you may have a firewall, host firewall, or router that's blocking traffic from *ac_hunter* to *syslog_server*. Please check all of the devices, firewalls, and router ACL's to see if any traffic is being blocked.

b. For additional troubleshooting, you may want to use "tcpdump" to watch one or more network interfaces to see if the packets corresponding to the syslog messages are present. On the sending and receiving systems (and any routers in the middle where you have the ability to run commands), you can run:

```
sudo tcpdump -i eth0 -vtnpX 'port 514'
```

This will show any syslog messages, along with the hex and ascii decodes of the actual transmitted content. Note that the name of the network interface used to send or receive the syslog traffic may differ; to see the name of the interface associated with the default route, use:

```
route -n | grep '^0\.0\.0\.0' | awk '{print $8}'
eth0
```

c. Is IP forwarding enabled? To move packets from your docker container to your syslog server, you need to have forwarding enabled. Check with:

```
cat /proc/sys/net/ipv4/ip_forward
```

If this comes back with "0", forwarding is disabled. To enable it:

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

You also need to enable it for future boots; edit `/etc/sysctl.conf` and make sure it has the line:

```
net.ipv4.ip_forward=1
```

, uncommented with a value of 1 (and no line "`net.ipv4.ip_forward=0`").

d. Please also check SELinux. On both *ac_hunter* and *syslog_server*, run:

```
getenforce
```

If you get "Disabled", "Permissive", or any error message that getenforce is not installed, SELinux will not be blocking incoming or outgoing syslog traffic. If you get "Enforcing", that system may be blocking syslog messages. On that same system, run

```
sudo tail -f /var/log/audit/audit.log
```

and rerun the logger command with a new test string. If the audit log shows network traffic being blocked - especially UDP or TCP port 514 - you'll need to either disable SELinux or unblock that traffic. To disable SELinux, run:

```
sudo setenforce Permissive
```

and rerun:

```
sudo getenforce
```

to make sure the change persists. Please see your operating system documentation for how to make this change persist across reboots.

6. **Can you send syslog messages from the specific AC-Hunter docker container?**

On *syslog_server*, open up the aihunter log file:

```
tail -f /var/log/syslog /var/log/messages
```

On *ac_hunter*, run:

```
sudo docker exec -it aihunter_api /bin/bash
```

to enter the API docker container. Your prompt will change; mine reads:

```
api@6446e0bcd107:~$
```

The `6446e0bcd107` is the hostname of the *container*, which is different from the AC-Hunter host. Inside this container, send a raw log entry over to the syslog server with:

```
/bin/logger --udp --server syslog.server.ip.address -P 514 test74
```

Do you see the new test string? If not, there may be some issue with the way packets are routed from Docker containers; please contact support.

To exit the Docker container and return to the host, type:

```
exit
```

7. **Have you instructed *ac_hunter* to log to *syslog_server*?** On *ac_hunter*, run:

```
less /etc/AI-Hunter/config.yaml    (*)
```

The entries in this file are nested: Look inside the "Alert:" section for another section called "Syslog:". In *that* section you need at least **Protocol:**, **Address:** and **Threshold:** lines, like so (there may be intermediate lines, which are fine):

```
Alert:
    Syslog:
        Threshold: 20
        Protocol: "udp"
        Address: "syslog_server:514"
```

Note that the spacing must match the spacing that's already there - for this file, singly indented lines have 4 spaces at the beginning, and doubly indented lines have 8 spaces, etc.

Edit this file with your favorite editor. If you don't have one, "nano" is reasonably beginner-friendly.

Once you've put in the right IP address for the *syslog_server* , also adjust the value following **Threshold:** ; we want a low value so that AC-Hunter will have something to report. 20 should be low enough to force some output.

Whenever you make changes to this file you'll need to restart AC-Hunter to pull the changes into the running system. On *ac_hunter*, run:

```
hunt up -d --force-recreate
```

8. **Now wait for 21-22 minutes past the hour.** AC-Hunter runs at around 20 minutes past each hour to import the new hourly logs from your sensors. As part of that import it updates the scores for each monitored system and reports on any whose scores are above the Threshold. You should see new entries when this import finishes; this could be a few minutes, or on heavily loaded networks, take most of the hour. Look at your log file on the *syslog_server* and see if you have new reports:

```
less -S /var/log/syslog
```

The log lines will look something like this:

```
2021-04-21T16:23:55-04:00 aabbccddeeff AI-Hunter[10]: Host:
10.1.96.40 Score: 57 PreviousScore: 0 Database: zeek02__1234-rolling
```

The up, down, left, and right arrows let you navigate this file. To go to the end, press and release the "Esc" key, then press and release ">". When you're done, "q" will exit less and return you to your command prompt.

a. If you see messages show up at your syslog server, you're all set. if nothing shows up, please check the other log files that syslog manages - is there a chance they're being redirected to a different log file?
b. If you do not see log lines coming across, bring up /etc/AI-Hunter/config.yaml (*) again. If you were using **"udp"** next to protocol, try switching to **"tcp"** (making sure that your syslog server will accept both before trying this. Similarly, if you were using **"tcp"** before, switch to **"udp"**. Whenever you make changes to this file you'll need to restart AC-Hunter to pull the changes into the running system. On *ac_hunter*, run:

```
hunt up -d --force-recreate
```

Come back after 20 minutes past the next hour and see if log lines show up now.

c. If you still do not get log lines, change the protocol to **""** , save the file, and restart AC-Hunter with:

```
hunt up -d --force-recreate
```

Please check back on the next hour to see if the logs flow now. If they start showing up with an empty protocol string, please let us know as this may be a bug.

9. **Please check the logs from the Docker instance.** On *ac_hunter* please run:

```
hunt logs api | tee /tmp/hunt-logs-api
```

a. Does the output from this include "...Successfully ran SendSyslog…", or does it include error messages related to syslog? Does it include any errors at all? If it scrolls by too quickly you can view the log file with:

```
less -S /tmp/hunt-logs-api
```

10. **Tag your messages.** (optional) Once you've confirmed that the log messages are coming across, you can add an (optional) Tag - a short string that's included in the syslog output:

```
Alert:
    Syslog:
        Threshold: 20
        Protocol: "udp"
        Address: "syslog_server:514"
        Tag: " AC-Hunter "
```

You can pick any tag you'd like; this is only for your benefit, and allows other tools to locate these log lines quickly. We strongly encourage leaving a space character after your tag and before the final quote on that line so that the Tag does not run up against the text that follows it.

Whenever you make changes to this file you'll need to restart AC-Hunter to pull the changes into the running system. On *ac_hunter*, run:

```
hunt up -d --force-recreate
```

Closing notes:

11. There's an alternate approach where your AC-Hunter docker container doesn't log directly to the syslog_server, but instead hands the logs down to the syslog server running on the AC-Hunter host operating system. To do this, leave the Address: value empty (follow it with two double quotes) and restart AC-Hunter with `hunt up -d --force-recreate`. Make sure you have a syslog server running on the *ac_hunter* system, though it does not need to be listening on either a UDP or TCP port (the logs are passed in a different way; for those interested in the gory details, AC-Hunter sends the alerts to /dev/log inside the docker container and docker relays these to /dev/log on the AC-Hunter host system, where rsyslog accepts them).

12. If you'd like to send log entries to multiple destinations, do the steps in the previous item to log to the AC-Hunter host syslog server (instead of sending tcp or udp packets directly from AC-Hunter). In the host's rsyslog configuration, direct it to log to multiple destinations (see https://www.rsyslog.com/doc/v8-stable/tutorials/reliable_forwarding.html for details).

13. If you prefer a different hostname to show up in the logs than the random hex string assigned by docker, you'll need to edit /opt/AI-Hunter/docker/api.yml (*) and add the "hostname: achunterapi" line. Here's a sample of the resulting file (just the top lines) from my test system:

```
grep -A 3 -B 10 hostname /opt/AI-Hunter/docker/api.yml    (*)
version: '3.2'
services:
  api:
    image: ai-hunter/api:latest
    container_name: aihunter_api
    hostname: achunterapi
    build: ../middleware
    restart: unless-stopped
```

As with all yaml files, the spacing is important - there must be exactly 4 spaces in front of hostname:... . Note that this file will be replaced on the next upgrade, so you'll have to make this change by hand after each upgrade. Once the change is done, please run:

```
hunt up -d --force-recreate
```

The next logs to go over will have the "achunterapi" hostname.

14. To contact support, please email support@activecountermeasures.com . Please include the following:

- For each of the items above "Closing notes", what did you find?
- Did you get any errors running the above?
- Please send back the file /tmp/hunt-logs-api .
- Please run:

```
TF=$(mktemp -q /tmp/aihstat.$(date +%Y%m%d%H%M%S).XXXXXX)
/opt/AI-Hunter/scripts/troubleshooting/aih_status.sh >"$TF" 2>&1
gzip -9 "$TF"
echo "Please email ${TF}.gz to support@activecountermeasures.com"
zless -S $TF.gz
```

and send back the /tmp/aihstat…. file whose name is printed above in the above commands.

* We encourage you to back up any yaml files you edit so you can quickly restore them after an upgrade. To confirm that the file is formatted correctly, transfer the yaml/yml file over to your laptop, go to http://www.yamllint.com , and upload the file to the form there. It will report back if any issues with your yaml file are found.

Document date: 2021/08/12 10:46