The Tyranny of the Clock
Linux.conf.au 2020: Sysadmin Miniconf
Jan 13th

Craig Miskell - SRE, GitLab

about.gitlab.com
The problem

ssh_exchange_identification: connection closed by remote host
fatal: Could not read from remote repository
Hypotheses

- DNS
- Firewall/proxy
- DNS, it’s always DNS
- Problem at *The Other End*
Capturing some data

SRE team, inspecting ~26 million connections/day

https://unsplash.com/photos/2Huoyf8DDDe - @matthew_t_rader
### Packet Captures

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>21:53:52</td>
<td>205.123.145.22</td>
<td>35.198.188.187</td>
<td>TCP</td>
<td>76</td>
<td>35962</td>
</tr>
<tr>
<td>2</td>
<td>21:53:52</td>
<td>205.123.145.22</td>
<td>35.198.188.187</td>
<td>TCP</td>
<td>76</td>
<td>35962</td>
</tr>
<tr>
<td>3</td>
<td>21:53:52</td>
<td>205.123.145.22</td>
<td>35.198.188.187</td>
<td>TCP</td>
<td>76</td>
<td>35962</td>
</tr>
<tr>
<td>4</td>
<td>21:53:52</td>
<td>205.123.145.22</td>
<td>35.198.188.187</td>
<td>TCP</td>
<td>76</td>
<td>35962</td>
</tr>
</tbody>
</table>

### Wireshark - Follow TCP Stream (tcp.stream eq 48) - 1-1.pcap

- **SSH-2.0-OpenSSH_7.7**
- **Find:**
  - Find:
  - Filter Out This Stream
  - Print
  - Save as...
  - Back
  - Close
Updated hypotheses

- DNS
- Firewall/proxy
- DNS, it’s always DNS
- Problem at The Other End
Lesson #1:
Wireshark has lots of analysis tools
You should know:
  1. They exist
  2. Vaguely what they might be able to do
## Conversations

### Wireshark: Conversations - 1-1.pcap

<table>
<thead>
<tr>
<th>Address A</th>
<th>Port A</th>
<th>Address B</th>
<th>Port B</th>
<th>Packets</th>
<th>Bytes</th>
<th>Packets A → B</th>
<th>Bytes A → B</th>
<th>Packets B → A</th>
<th>Bytes B → A</th>
<th>Rel Start</th>
<th>Duration</th>
<th>Bits/s A → B</th>
<th>Bits/s B → A</th>
</tr>
</thead>
<tbody>
<tr>
<td>165.227.164.44</td>
<td>35052</td>
<td>35.180.168.187</td>
<td>443</td>
<td>8</td>
<td>581</td>
<td>4</td>
<td>301</td>
<td>4</td>
<td>280</td>
<td>835.264513</td>
<td>1072</td>
<td>12k</td>
<td>11k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>51812</td>
<td>35.180.168.187</td>
<td>443</td>
<td>8</td>
<td>581</td>
<td>4</td>
<td>301</td>
<td>4</td>
<td>280</td>
<td>1676.526316</td>
<td>1793</td>
<td>12k</td>
<td>11k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>50524</td>
<td>35.180.168.187</td>
<td>443</td>
<td>8</td>
<td>581</td>
<td>4</td>
<td>301</td>
<td>4</td>
<td>280</td>
<td>2156.500751</td>
<td>1993</td>
<td>12k</td>
<td>11k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>45492</td>
<td>35.180.168.187</td>
<td>443</td>
<td>8</td>
<td>581</td>
<td>4</td>
<td>301</td>
<td>4</td>
<td>280</td>
<td>2577.330465</td>
<td>1969</td>
<td>12k</td>
<td>11k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>40574</td>
<td>35.180.168.187</td>
<td>443</td>
<td>8</td>
<td>581</td>
<td>4</td>
<td>301</td>
<td>4</td>
<td>280</td>
<td>2695.559340</td>
<td>1980</td>
<td>12k</td>
<td>11k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>42090</td>
<td>35.180.168.187</td>
<td>443</td>
<td>8</td>
<td>581</td>
<td>4</td>
<td>301</td>
<td>4</td>
<td>280</td>
<td>3535.547099</td>
<td>1970</td>
<td>12k</td>
<td>11k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>48286</td>
<td>35.180.168.187</td>
<td>443</td>
<td>8</td>
<td>581</td>
<td>4</td>
<td>301</td>
<td>4</td>
<td>280</td>
<td>3905.558162</td>
<td>1972</td>
<td>12k</td>
<td>11k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>57782</td>
<td>35.180.168.187</td>
<td>443</td>
<td>8</td>
<td>581</td>
<td>4</td>
<td>301</td>
<td>4</td>
<td>280</td>
<td>7077.94880</td>
<td>2061</td>
<td>11k</td>
<td>10k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>35240</td>
<td>35.180.168.187</td>
<td>443</td>
<td>8</td>
<td>581</td>
<td>4</td>
<td>301</td>
<td>4</td>
<td>280</td>
<td>7135.422444</td>
<td>1969</td>
<td>12k</td>
<td>11k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>53934</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5441</td>
<td>29785366</td>
<td>14654</td>
<td>25k</td>
<td>29k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>54634</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5441</td>
<td>91808260</td>
<td>14643</td>
<td>25k</td>
<td>29k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>34298</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5441</td>
<td>18666264</td>
<td>15414</td>
<td>23k</td>
<td>28k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>38570</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5441</td>
<td>285415039</td>
<td>14911</td>
<td>24k</td>
<td>29k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>58172</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5441</td>
<td>402006511</td>
<td>14854</td>
<td>24k</td>
<td>29k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>40086</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5441</td>
<td>471626509</td>
<td>14664</td>
<td>25k</td>
<td>29k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>37824</td>
<td>25.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5373</td>
<td>49698269</td>
<td>15788</td>
<td>23k</td>
<td>27k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>40662</td>
<td>25.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5441</td>
<td>683197344</td>
<td>16651</td>
<td>25k</td>
<td>29k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>40798</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5441</td>
<td>745243296</td>
<td>14707</td>
<td>24k</td>
<td>29k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>41538</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5485</td>
<td>80763141</td>
<td>15462</td>
<td>23k</td>
<td>28k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>39620</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5441</td>
<td>115082860</td>
<td>15046</td>
<td>24k</td>
<td>28k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>39930</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5441</td>
<td>121250203</td>
<td>15110</td>
<td>24k</td>
<td>28k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>40770</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5441</td>
<td>1336182252</td>
<td>15037</td>
<td>24k</td>
<td>28k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>50874</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5373</td>
<td>1342224522</td>
<td>15173</td>
<td>24k</td>
<td>28k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>48134</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5485</td>
<td>136661359</td>
<td>14626</td>
<td>25k</td>
<td>30k</td>
</tr>
<tr>
<td>165.227.164.44</td>
<td>41504</td>
<td>35.180.168.187</td>
<td>443</td>
<td>45</td>
<td>10k</td>
<td>22</td>
<td>4589</td>
<td>23</td>
<td>5453</td>
<td>1398242332</td>
<td>15035</td>
<td>24k</td>
<td>29k</td>
</tr>
</tbody>
</table>
Logs logs and more logs - BigQuery to the rescue

Query editor

```
SELECT * FROM `gitlab-production.haproxy_logs.haproxy_20191208`
WHERE jsonPayload前端_name like 'altssh'
AND jsonPayload.ç_port = '49898'
AND jsonPayload.ç_ip = 'null'
order by jsonPayload.t
```

Query results

<table>
<thead>
<tr>
<th>nginx.hostname</th>
<th>jsonPayload.environment</th>
<th>jsonPayload.verb</th>
<th>jsonPayload.t</th>
<th>jsonPayload.ssl_version</th>
<th>jsonPayload.tw</th>
<th>jsonPayload.status</th>
</tr>
</thead>
<tbody>
<tr>
<td>02-lb-gprd</td>
<td>gprd</td>
<td>null</td>
<td>08/Dec/2019:18:25:09.507</td>
<td>-</td>
<td>1</td>
<td>null</td>
</tr>
</tbody>
</table>
Torn down connections

S: aborted by the server, or the server explicitly refused it
D: the session was in the DATA phase.
An illuminating graph
Lesson #2: Apparently a lot of people have time synchronization set up properly.
MaxStartups

Specifies the maximum number of concurrent unauthenticated connections to the SSH daemon. Additional connections will be dropped until authentication succeeds or the LoginGraceTime expires for a connection. The default is 10:30:100.

Alternatively, random early drop can be enabled by specifying the three colon separated values start:rate:full (e.g. "10:30:60"). sshd(8) will refuse connection attempts with a probability of rate/100 (30%) if there are currently start (10) unauthenticated connections. The probability increases linearly and all connection attempts are refused if the number of unauthenticated connections reaches full (60).
Updated hypotheses/Proven point

- DNS
- Firewall/proxy
- DNS, it’s always DNS
- Problem at The Other End

SSH Configuration Issue
Lesson #3:

It is polite to log interesting information at default levels

Deliberately dropping a connection for any reason is definitely interesting to system administrators.
sum(rate(haproxy_server_response_errors_total{server=~"\*\*\*[1m]"})[1m])
How high could we go?
Some extremely dodgy math

\[ \text{ratelimit} = \frac{B \times S}{F \times T} \]

F => Front-end (haproxy) server count (18)
B => Back-end server count (27)
S => Session allowed in startup (first value in MaxStartups)
T => How long a session spends in unauthenticated state (in seconds)
Surprising data
Lesson #4: When you choose specific non-default settings, leave a comment or link to documentation/issues as to why, future people will thank you.
A delightful graph

sum(rate(haproxy_server_response_errors_total{server="git.*"}[1m]))
Lesson #5: As scary as it looks, MaxStartups appears to have very little performance impact even if it's raised much higher than the default.
A bit of ret-con math

\[
\text{ratelimit} = \frac{B \times S}{F \times T}
\]

\[
T = \frac{B \times S}{F \times \text{ratelimit}}
\]

\[
\frac{27 \times 200}{18 \times 110} = 2.72
\]

\[
\frac{27 \times 250}{18 \times 110} = 3.409
\]
1.5%
Lesson #6: Measure early, measure often
Followup: Why u no alert?

rate(haproxy_server_response_errors_total[1m]) > .5 for: 2m

1. Arbitrary limit (0.5), not a ratio
2. Per front-end (18) and back-end (27) server combo
3. Average over 1 minute
4. Had to be elevated for 2 minutes

Also not everything is HTTP (yet)...

Y U NO ALERT!?
$termination_cause == "S" && $termination_state == "D" && $bytes_read == 0 {
    haproxy_ssh_max_startups_breachedException_total[$server_name]++
}
Visualize the Tyranny

2019-12-11: grouped by minute/second
X * * * * sleep $((RANDOM/653 + 5)) && /path/to/script.sh
   I love you.

Or, in a systemd.timer:
RandomizedDelaySec=50
AccuracySec=0
OnCalendar=*-*-* *:X:05
Final thoughts

1. The little details matter
2. Assumptions and estimates can be risky
3. Stampeding herds bound by the clock can ruin all your best laid plans