K13223: Configuring the BIG-IP system to log TCP RST packets

Non-Diagnostic

Original Publication Date: May 5, 2016
Update Date: Dec 30, 2017

Topic

You should consider using this procedure under the following conditions:

- Your BIG-IP system sends TCP reset (RST) packets.
- You want to find the cause of the TCP RST packets.

Prerequisites

You must meet the following prerequisite to use this procedure:

- You can access the BIG-IP command line.

Description

Starting in BIG-IP 10.2.3, you can configure the BIG-IP system to log the reasons for generating the TCP RST packets to the `var/log/ltm` log file. To configure this functionality, you can enable the `TM.RstCause.Log` database variable, which is disabled by default. The accompanying `TM.RstCause.Pkt` database variable, when enabled, allows the BIG-IP system to include the RST cause information in the TCP RST packet payload; the `TM.RstCause.Pkt` database variable is also disabled by default.

Note: In BIG-IP 11.2.0 and later, you can view the TCP RST cause by capturing internal Traffic Management Microkernel (TMM) information using the `tcpdump` utility. The TCP RST cause is included in the medium level details, regardless of the `TM.RstCause.Pkt` variable setting.

Important: Including the RST cause information in the TCP RST packet payload by enabling the `TM.RstCause.Pkt` database variable can be a potential security risk by advertising information about your environment that an attacker would not otherwise have. Enabling logging of TCP RST packets with the `TM.RstCause.Log` database variable has the potential to cause higher system resource consumption and a possible system performance degradation in the event of a denial-of-service (DoS) attack. For these reasons, F5 recommends that you enable these database variables for troubleshooting purposes only, and that you disable the respective database variables after you have completed any troubleshooting steps.

- Configuring the BIG-IP system to log the TCP RST packets
- Viewing the statistics for TCP RST packets
- Interpreting the log entries for TCP RST packets
- Resetting the statistics for TCP RST packets
- Configuring the BIG-IP system to disable the logging of the TCP RST packets
Configuring the BIG-IP system to log the TCP RST packets

**Impact of procedure:** An overloaded BIG-IP system may experience performance degradation if the BIG-IP system processes a huge amount of TCP RST packets and logs them to the `/var/log/ltm` file.

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

   tmsh

2. To configure the BIG-IP system to log the TCP RST cause in the `/var/log/ltm` file, you must enable the `TM.RstCause.Log` database variable by typing the following command:

   ```
   modify /sys db tm.rstcause.log value enable
   ```

3. Optional: To configure the BIG-IP system to include the RST cause information in the TCP RST packet payload, you must enable the `TM.RstCause.Pkt` database variable by typing the following command:

   ```
   modify /sys db tm.rstcause.pkt value enable
   ```

Viewing the statistics for TCP RST packets

**Impact of procedure:** Performing the following procedure should not have a negative impact on your system.

1. Log in to the `tmsh` utility by typing the following command:

   tmsh

2. To view the statistics for TCP RST packets, type the following command:

   ```
   show /net rst-cause
   ```

   The system displays output that appears similar to the following example:

   ```
   -----------------------------
   TCP/IP Reset Cause
   RST Cause: Count
   -----------------------------
   Access denied 2
   Flow expired (sweeper) 2
   TCP 3WHS rejected 2
   ```

Interpreting the log entries for TCP RST packets

You can view the log entries for the TCP RST packets in the `/var/log/ltm` log file. The BIG-IP system logs an entry for a TCP RST packet in the following format:

```
01230140:3: RST sent from <source IP:port> to <destination IP:port>, [<F5 internal code>] <{peer} if RST is from others> <reason for TCP reset>
```
For example, the BIG-IP system logs the following message in the `/var/log/ltm` log file when the virtual server `10.10.100.100:80` sends a TCP RST to the client `10.10.10.124` upon receiving a TCP RST from one of its pool members:

```
01230140:3: RST sent from 10.10.100.100:80 to 10.10.10.124:39272, [0x112d82a:1721] {peer} TCP RST from remote system
```

The following table provides a list of common TCP RST log messages:

**Important**: The following list is not exhaustive and does not cover all TCP RST causes.

<table>
<thead>
<tr>
<th>Log message</th>
<th>Cause for the TCP RST packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client side detached due to reselect</td>
<td>When an existing client-side connection has been detached from the server-side connection and reselects a new server, the BIG-IP system sends a TCP RST to the server to close the existing server-side connection. This behavior typically comes from using iRule commands such as <code>LB::reselect</code>.</td>
</tr>
</tbody>
</table>
| Flow expired (sweeper)              | The BIG-IP system will reap a connection from the connection table and send a TCP RST packet to the client when one of the following two conditions is met:  
  - An idle timeout for the connection expired. This may be impacted by the Idle Timeout setting in the assigned TCP profile of the affected virtual server.  
  - Memory usage on the BIG-IP system increased beyond the reaper high-water mark and triggered adaptive reaping. |
<p>| HTTP Chunk parse error              | The HTTP request/response from the client contains incorrectly formatted chunked data that the BIG-IP system cannot process. |
| HTTP header size exceeded by client | The HTTP request/response from the client contains a header that is larger than the value configured for the <strong>Maximum Header Size</strong> setting in the assigned HTTP profile of the affected virtual server. |
| HTTP header size exceeded by server | The HTTP request/response from the server contains a header that is larger than the value configured for the <strong>Maximum Header Size</strong> setting in the assigned HTTP profile of the affected virtual server. |
| HTTP internal error (bad state transition) | The HTTP response from the server contains HTTP data that is not RFC2616 compliant. |
| HTTP Unexpected server data past end of response | The BIG-IP system receives unexpected HTTP data from the server. A typical case occurs when a server sends an HTTP response with a Content-Length header value that is smaller than the actual size of the content. |
| iRule execution error               | An error has occurred when executing an iRule.                                                   |
| No route to host                    | The BIG-IP system is unable to find the path to the destination host.                          |</p>
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 3WHS rejected</td>
<td>The BIG-IP system failed to establish a TCP connection with the host (client or server) due to a failure during the TCP 3-way handshake process.</td>
</tr>
<tr>
<td>TCP 3WHS rejected (bad ACK)</td>
<td></td>
</tr>
<tr>
<td>TCP 3WHS rejected (bad SEQ)</td>
<td></td>
</tr>
<tr>
<td>TCP 3WHS rejected (bad flags)</td>
<td></td>
</tr>
<tr>
<td>TCP early FIN</td>
<td>The BIG-IP system received a TCP packet from a host (client or server) with only the FIN bit set and no data.</td>
</tr>
<tr>
<td>TCP keep-alive timeout</td>
<td>The BIG-IP system received no response for three consecutive TCP Keep-Alive probes. This is the default behavior, and is not configurable.</td>
</tr>
<tr>
<td>TCP retransmit timeout</td>
<td>The BIG-IP system has resent the data segment to the affected TCP connection the maximum number of times. (The default value for the Maximum Segment Retransmissions setting is eight.)</td>
</tr>
<tr>
<td>TCP bad flags</td>
<td>The BIG-IP system received a TCP packet that contained corrupted flags from the client.</td>
</tr>
<tr>
<td>TCP zero window timeout</td>
<td>The affected TCP connection has exceeded the value configured for the Zero Window Timeout setting in the assigned TCP profile of the affected virtual server.</td>
</tr>
<tr>
<td>TCP RST from remote system</td>
<td>When a host (client or server) sends a TCP RST for an existing TCP connection, the BIG-IP system in turns sends a TCP RST to the host at the other end of the TCP connection.</td>
</tr>
<tr>
<td>RST from BIG-IP internal Linux host</td>
<td>When the BIG-IP system receives a RST acknowledgement (ACK) in response to terminating a service check.</td>
</tr>
<tr>
<td>Access denied</td>
<td>The BIG-IP system receives a SYN for either one of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>- A virtual server of type reject</td>
</tr>
<tr>
<td></td>
<td>- A port that is protected by the Port Lockdown settings on a self IP address</td>
</tr>
<tr>
<td>No Local Listener</td>
<td>The BIG-IP system receives a SYN for a non-existent port on a virtual address.</td>
</tr>
<tr>
<td>No return route to client</td>
<td>The BIG-IP system is unable to find the return path to the source client</td>
</tr>
<tr>
<td>Packet filter (reject)</td>
<td>An active packet filter has blocked a host from an attempt to establish a connection with the BIG-IP system.</td>
</tr>
<tr>
<td>SIP error [error_code]</td>
<td>SIP message processing, for example, either execution of TCL events, error sending the message, parsing of the message, internal error when processing of the message.</td>
</tr>
<tr>
<td>assoc alloc</td>
<td>Failed to allocate memory to process the message.</td>
</tr>
<tr>
<td>assoc init</td>
<td>Failed to initialize internal data structure.</td>
</tr>
<tr>
<td>msg alloc</td>
<td>Failed to allocate memory to process the message.</td>
</tr>
</tbody>
</table>
Resetting the statistics for TCP RST packets

**Impact of procedure:** Performing the following procedure should not have a negative impact on your system.

1. Log in to the Traffic Management Shell (**tmsh**) by typing the following command:

   tmsh

2. To reset the statistics for TCP RST packets, type the following command:

   reset-stats /net rst-cause

   **Note:** The **reset-stats /net rst-cause** command exists only in BIG-IP 11.0.0 and later versions. There is no equivalent command in BIG-IP 10.2.3 and 10.2.4.

Configuring the BIG-IP system to disable the logging of the TCP RST packets

**Impact of procedure:** Performing the following procedure should not have a negative impact on your system.

1. Log in to the Traffic Management Shell (**tmsh**) by typing the following command:

   tmsh

2. To configure the BIG-IP system to stop logging the TCP RST packets to the `/var/log/ltm` file, you must disable the **TM.RstCause.Log** database variable by typing the following command:

   modify /sys db tm.rstcause.log value disable

3. Optional: To configure the BIG-IP system to stop sending the TCP RST cause as payload in the TCP RST packets, you must disable the **TM.RstCause.Pkt** database variable by typing the following command:

   modify /sys db tm.rstcause.pkt value disable

**Supplemental Information**

- [K9812: Overview of BIG-IP TCP RST behavior](#)
- [K13189: The BIG-IP system now writes TCP RST causes to the log files](#)
- [K13637: Capturing internal TMM information with tcpdump](#)

**Applies to:**

**Product:** BIG-IP, BIG-IP AAM, BIG-IP AFM, BIG-IP APM, BIG-IP ASM, BIG-IP DNS, BIG-IP Edge Gateway, BIG-IP GTM, BIG-IP Link Controller, BIG-IP LTM, BIG-IP PEM, BIG-IP PSM, BIG-IP WebAccelerator, BIG-
IP WOM
13.0.0, 12.1.2, 12.1.1, 12.1.0, 12.0.0, 11.6.1, 11.6.0, 11.5.4, 11.5.3, 11.5.2, 11.5.1, 11.5.0, 11.4.1, 11.4.0,
11.3.0, 11.2.1, 11.2.0, 11.1.0, 11.0.0, 10.2.4, 10.2.3