K86480148: Troubleshooting issues sending logs to a remote syslog server

Diagnostic

Original Publication Date: Nov 1, 2016
Update Date: Jun 9, 2018

Issue

You should consider using this procedure under the following conditions:

- You have configured your BIG-IP system to send logs to a remote syslog server.
- Log messages from your BIG-IP system do not appear on the remote syslog server.

Symptoms

As a result of issues with sending logs to a remote syslog server, you may encounter the following symptom:

- Log messages from your BIG-IP system are not visible on the remote syslog server.

Recommended Actions

When you add a remote server to the BIG-IP syslog configuration, the syslog-ng service creates the server as a separate destination for log messages, so in addition to logging locally, the BIG-IP system will also log to the remote device. After you have configured the BIG-IP system to log to a remote syslog server, if the logs do not appear on the remote device, F5 recommends that you perform the following procedures to confirm that the BIG-IP system is behaving as expected.

Procedures

When you experience issues sending logs to a remote syslog server, you can use the following troubleshooting steps to confirm or rule out the BIG-IP system as the cause:

- Verifying the syslog settings on the BIG-IP system
- Verifying name resolution of the remote syslog server hostname
- Determining the interface that the BIG-IP system uses to reach the remote syslog server
- Performing connectivity tests
- Using the tcpdump utility to verify that syslog traffic is sent by the BIG-IP system

Verifying the syslog settings on the BIG-IP system

You should verify the syslog settings to confirm that they are configured correctly for your environment.

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

1. Log in to the BIG-IP command line.
2. Display the BIG-IP **syslog** configuration by typing the following command:

   tmsh list sys syslog

For example:

```
# tmsh list sys syslog
sys syslog {
    remote-servers {
        remotesyslog1 {
            host 172.16.1.110
            local-ip 172.18.1.1
        }
    }
}
```

**Note:** The remote port will not be displayed in the `remote-servers` section if port 514 is configured.

Alternatively, a remote server may appear within the `include` setting. A filter can be implemented using this method, which is important to keep in mind when troubleshooting. For example, a filter could be in place to send only `local0` log messages remotely, as opposed to sending all logs. The following example shows a remote `syslog` configuration with a filter deployed using the `include` setting:

```
# tmsh list sys syslog
sys syslog {
    include "destination d_loghost { udp(172.16.1.110 port(514) localip(172.18.1.1));}; log {source (s_syslog_pipe); filter(f_local0); destination(d_loghost);};"
}
```

3. Review the configuration settings and correct any errors.

4. Take note of the remote server IP address and port as well as the local IP address (if set), as they will be used in the following procedures.

Verifying name resolution of the remote syslog server hostname

You can skip this procedure if you have defined the remote `syslog` server with its IP address. When a remote server is added to the BIG-IP `syslog` configuration using its hostname, the BIG-IP system will resolve the name using the DNS servers that are defined in the system configuration. If the BIG-IP system is unable to resolve the hostname, no log messages will be sent remotely. The following example shows the BIG-IP `syslog` configuration containing a remote `syslog` server defined with a hostname.

```
# tmsh list sys syslog
sys syslog {
    remote-servers {
        remotesyslog1 {
            host host1.example.com
```
You should verify the DNS server configuration and manually resolve the remote `syslog` server hostname to verify name resolution.

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

1. Log in to the BIG-IP command line.
2. Display the DNS configuration by typing the following command:

   ```
   tmsh list sys dns
   ``

   For example:

   ```
   # tmsh list sys dns
   sys dns {
       name-servers { 172.24.1.1 }
   }
   ```

3. Check that the name servers have been configured and correct any errors with the settings.
4. If no name servers exist, then you will need to add them or define the remote `syslog` server using its IP address in the BIG-IP `syslog` configuration. For more information refer to [K13205: Configuring the BIG-IP system to resolve DNS hostnames (11.x and later)](https://example.com). If name servers exist and any errors have been corrected, manually resolve the `syslog` server hostname using the `dig` utility. To do so, use the following syntax:

   ```
   dig host1.example.com
   ```

   For example, the following output shows a successful answer to a query for `host1.example.com`:

   ```
   # dig host1.example.com
   ; <<>> DiG 9.9.8-P3 <<>> host1.example.com
   ;; global options: +cmd
   ;; Got answer:
   ;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 55064
   ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
   
   ;; OPT PSEUDOSECTION:
   ; EDNS: version: 0, flags:; udp: 4000
   ;; QUESTION SECTION:
   ;host1.example.com. IN A

   ;; ANSWER SECTION:
   host1.example.com. 1109 IN A 172.16.1.110
   ```
If you do not get an answer to the query, contact the DNS administrator for your site. Otherwise, move on to the next procedure.

Determining the interface that the BIG-IP system uses to reach the remote syslog server

The BIG-IP system can use the management interface (assigned with the management IP) or a Traffic Management Microkernel (TMM) interface (assigned with a Virtual Local Area Network (VLAN) and self IP) to transmit log messages to a remote syslog server. You should determine which of the two options the BIG-IP system uses to reach your remote syslog server to confirm that the BIG-IP system is using the expected interface, and so you know where to run a packet capture in the final procedure.

**Note:** If only a default gateway is defined as a management route, the system will prefer the TMM default gateway. For more information, refer to [K13284: Overview of management interface routing (11.x - 12.x)](https://support.arenadata.com/knowledgebase/article/K13284)

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

1. Log in to the BIG-IP command line.
2. If the local IP setting has not been configured, skip to step 3. If the local IP setting has an IP address configured, the BIG-IP system will only send log messages from the interface to which the IP address is assigned and ignore routes that use other interfaces, even if a destination is a closer match. To determine the interface that the local IP address belongs to, search a list of the management IP and all self IP addresses and their associated VLANs using the following command syntax:

   ```bash
   (tmsh list sys management-ip;echo " ";tmsh list net self { address vlan }) | grep -C 1
   <IP_address_used_for_local-ip>
   ```

   For example, the following output reveals that the local IP is a self IP that is configured on the VLAN example, which is assigned to a TMM interface:

   ```bash
   # (tmsh list sys management-ip;echo " ";tmsh list net self { address vlan }) | grep -C 1 172.18.1.1
   net self example_self {
       address 172.18.1.1/24
       vlan example
   }
   ```

   If you have completed this step, you can skip to the next procedure.

3. You can use either the `ip route get` command or the `route` command to determine the interface that the BIG-IP system uses to reach the remote syslog server.

   **Note:** The interface reported in the output of either command can be the management interface or the name of a VLAN configured with a TMM interface.

   - To use the `ip route get` command to determine the interface used to reach the remote syslog server, use the following command syntax:
ip route get <IP_address_of_syslog_server>

For example, the output shows that the BIG-IP system uses the interface named example, which is a VLAN reported as the value of dev and the source address of 172.16.1.1, which is a self IP reported as the value of src to reach 172.16.1.110:

```
# ip route get 172.16.1.110
172.16.1.110 dev example src 172.16.1.1
    cache mtu 1500 advmss 1460 hoplimit 64
```

- Alternatively, to determine the interface used to reach the remote syslog server with route, type the following command:

```
route -n
```

For example, the following output shows that the BIG-IP system uses the interface named example, which is a VLAN listed under the iface column to reach the host 172.16.1.110, which most closely matches 172.16.1.0 under the Destination column:

```
# route -n
Kernel IP routing table
Destination    Gateway     Genmask     Flags Metric Ref    Use Iface
127.1.1.0      0.0.0.0     255.255.255.0 U      0      0      0 tmm
172.24.22.0     0.0.0.0     255.255.255.0 U      0      0      0 eth0
172.16.1.0     0.0.0.0     255.255.255.0 U      0      0      0 example
127.2.0.0      127.1.1.253 255.255.0.0   UG     0      0      0 tmm
127.20.0.0     0.0.0.0     255.255.0.0   U      0      0      0 tmm_bp
0.0.0.0        172.24.22.254 0.0.0.0     UG     9      0      0 eth0
```

Performing connectivity tests

Once you have performed the previous procedures and you have not resolved the issue, you should perform connectivity tests to confirm that the remote syslog server is reachable. Since the BIG-IP system transmits log messages over User Datagram Protocol (UDP), the remote device will not reply when testing on the Transport Layer. Therefore, you can use Network Layer utilities such as ping or traceroute. Additionally, you can manually send a log message to the remote syslog server using the netcat utility.

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

1. Log in to the BIG-IP command line.
2. Test the server with the ping utility by using the following syntax:

```
ping -c 4 <IP_address_of_syslog_server>
```

For example:
# ping -c 4 172.16.1.110
PING 172.16.1.110 (172.16.1.110) 56(84) bytes of data.
64 bytes from 172.16.1.110: icmp_seq=1 ttl=64 time=2.03 ms
64 bytes from 172.16.1.110: icmp_seq=2 ttl=64 time=0.609 ms
64 bytes from 172.16.1.110: icmp_seq=3 ttl=64 time=0.680 ms
64 bytes from 172.16.1.110: icmp_seq=4 ttl=64 time=0.724 ms

If the connectivity test with ping fails, it does not necessarily mean that the server is unable to accept syslog traffic on a UDP port; the following step will help you further verify this.

3. Manually send a log message using the netcat utility by using the following syntax:

   echo '<0>Testing LTM for connectivity' | nc -w 1 -u <IP_address_of_syslog_server> <port_of_syslog_server>

   For example:

   # echo '<0>Testing LTM for connectivity' | nc -w 1 -u 172.16.1.110 514

   Log messages on the remote syslog server will appear similar to the following example when the IP address is the system that transmitted the log message:

   Nov 14 12:15:09 172.16.1.101 Testing LTM for connectivity

4. If both tests failed, you should troubleshoot the remote syslog server and the network between the BIG-IP system and the syslog server. If possible, you should perform a packet capture on the remote syslog server to confirm if the traffic transmitted by the ping utility or the netcat utility on the BIG-IP system have traversed the network and arrived. If the traffic has not arrived, you should examine the network between for potential routing or firewall issues, otherwise investigate the server to determine why it is unable to respond to ICMP echo requests or accept syslog messages over the network. If either of the connectivity tests succeed, move on to the next procedure.

Using the tcpdump utility to verify that syslog traffic is sent by the BIG-IP system

The tcpdump utility captures the communication between network devices. This procedure sets up the tcpdump utility to filter the network traffic so it captures only syslog traffic to a remote syslog server. You should perform this procedure to confirm that the BIG-IP system is sending log messages to the remote syslog server.

Note: For more information on packet tracing with tcpdump, refer to K411: Overview of packet tracing with the tcpdump utility.

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

1. Log in to the BIG-IP command line
2. To capture traffic sent to the remote syslog server, use the following command syntax:

   tcpdump -s0 -A -nni <interface> host <remote_syslog_IP> and port <remote_syslog_port>
In the previous syntax, note the following:

- `-A` will decode the packet data to print ASCII strings so you can view the log messages.
- `<interface>` is the interface you determined in the third procedure, which can be either a management interface or TMM interface.
- `<remote_syslog_IP>` is the IP address of the remote syslog server that you gathered in the first procedure.
- `<remote_syslog_port>` is the port of the remote syslog server that you gathered in the first procedure.

For example, the following `tcpdump` output shows log messages sent to the remote server `172.16.1.110` on port `514`:

```
# tcpdump -A -nni example host 172.16.1.110 and port 514
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on example, link-type EN10MB (Ethernet), capture size 65535 bytes
13:18:21.481515 IP 172.16.1.1.56090 > 172.16.1.110.514: SYSLOG local0.notice, length: 118 out slot1/tmm0 lis=
E...O.@.@........n......n..<133>Sep 16 13:18:21 bigip1 notice tmm[18901]: 013e0001:5: Tcpdump
starting bcast on 127.1.1.1:2 from 127.1.1.254:35727
....... 
13:18:21.482061 IP 172.16.1.1.56090 > 172.16.1.110.514: SYSLOG local0.notice, length: 119 out slot1/tmm0 lis=
E...O.@.@........n......n..<133>Sep 16 13:18:21 bigip1 notice tmm1[18901]: 013e0001:5: Tcpdump
starting bcast on 127.1.1.2:2 from 127.1.1.254:35727
....... 
13:18:37.929191 IP 172.16.1.1.56090 > 172.16.1.110.514: SYSLOG local0.notice, length: 153 out slot1/tmm0 lis=
E...O.@.@........n......n..<133>Sep 16 13:18:37 bigip1 notice bigd[14096]: 01060144:5: Pool /Common
/http_pool member /Common/my_node_110 session status enabled by monitor
....... 
13:18:38.731925 IP 172.16.1.1.56090 > 172.16.1.110.514: SYSLOG local0.notice, length: 199 out slot1/tmm0 lis=
E...O ..@..u.......n......n..<133>Sep 16 13:18:38 bigip1 notice mcpd[5480]: 01070727:5: Pool
/Common/http_pool member /Common/my_node_110:80 monitor status up. [/Common/http: up ] [ was unchecked for 0hr:0min:38sec ]
....... 
```

*Note:* You may need to leave the `tcpdump` running for several minutes to capture syslog traffic.

3. After capturing syslog traffic or leaving `tcpdump` running for a period of time with no packets seen, stop `tcpdump` by pressing `Ctrl+C`.
4. Take one of the following actions based on the outcome of a packet capture:

- If log messages appear in a capture, then the BIG-IP system is behaving correctly, and you should proceed with troubleshooting the remote syslog server and the network between the BIG-IP system and the syslog server. If possible, you should capture on the remote syslog.
server that is receiving the log messages from BIG-IP system, to confirm if the messages sent have traversed the network and arrived. If messages have arrived, check that the syslog server is configured to listen for log messages arriving from the network over UDP, and that system policies are not blocking the listening port. If messages have not arrived, the network between should be examined for potential routing or firewall issues.

- If no log messages appear in the capture, you can use the logger command to generate a log message manually. Run the tcpdump utility again using the same syntax from step 2. While tcpdump is running, open another command line session to the BIG-IP system, log in and use the following command syntax to generate a log message:

  logger -p <facility>.<level> "<descriptive message>"

  For example:

  logger -p local0.notice "Test message for tcpdump"

  If after you have manually generated log messages concurrently with a capture, and logs did not appear to be transmitted by the BIG-IP system, then contact F5 Technical Support for further troubleshooting steps. Otherwise, go back to the first bullet point in this list.

**Supplemental Information**

- K7342: Overview of the syslog-ng.conf file
- K7227: Considerations when using the tcpdump utility with tagged VLAN traffic
- K13080: Configuring the BIG-IP system to log to a remote syslog server (10.x - 12.x)
- K13083: Configuring syslog settings from the command line (11.x - 12.x)
- K13317: Configuring the level of information that syslog-ng sends to log files (11.x - 12.x)
- K13333: Filtering log messages sent to remote syslog servers (11.x - 12.x)

**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
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, 11.2.1