LTM 9.4.2+: Custom Syslog Configuration

Deb Allen, 2008-05-02

As of 9.4.2, LTM has begun implementing the Single Configuration File (SCF). One important aspect of that change is that you can no longer make permanent configuration changes by editing individual configuration files directly. If you do make direct changes to the running configuration files, the changes will (in most cases) be overwritten by the master configuration upon restart. The standard LTM configuration tools, such as the GUI, bigpipe commands, or the bigpipe shell (bpsh), provide the means to make most required configuration changes permanent.

This solution (SOL5527: Configuring BIG-IP to log to a remote syslog server) contains information about commonly requested syslog-ng modifications, but you can't edit the configuration file directly in LTM v9.4.2 or better. This solution (SOL8260: Configuring syslog settings using the bigpipe command) has some detail about the bigpipe commands you can use to make basic configuration changes, however they may not provide the granularity some customers require for extensive syslog customization. The "b syslog edit" command is intended to provide additional configuration options, and will be implemented in a future release (CR91841). In the meantime, this article will provide the details required to further customize syslog for version 9.4.2 and above

(Credit to Mr David Karakas on the F5 Support escalations team for the preliminary scoop, and to Mohamed Lrhazi for helping flesh out some of the final details.)

bigpipe syslog-ng include

Instead of editing the syslog-ng configuration file directly, you can use the "bigpipe syslog-ng include" command to pipe changes into the permanent configuration file (/config/bigip_sys.conf).
This approach uses an include file to add new object stanzas and modify existing ones. Each stanza must be properly formatted (standard syslog-ng format), however, you can not simply point to an existing syslog-ng.conf file and load it using 'include'.

If a duplicate object is defined in both the base configuration file and the include file, the version in the include file will be loaded last, overwriting the original definition. You'll see later that is the trick to re-defining the existing configuration to implement the most granular of modifications.

Adding to the default logging

If you just want to add to the default logging already configured for LTM, you can follow these steps to include additional configuration detail for syslog-ng. The first 2 examples in SOL5527 above ("Configuring BIG-IP to send all messages to a remote server" and "Configuring BIG-IP to send all messages to multiple remote servers") could be addressed this way:

1. Create and save a file containing the desired changes (remote server destination, catchall filter, and the log statement associating them):

```
syslog include "
 destination remote_server {
 udp(\"10.4.0.1\" port (514));
 udp(\"10.5.0.1\" port (514));
 };
 filter f_alllogs {
 level (notice...emerg);
 };
 log {
```

```
 source(local);
 filter(f_alllogs);
 destination(remote_server);
 };"
```

(For this example, the file will be named 'syslog.inc')

The double quotes before and after the syslog-ng.conf stanzas delimit the data that will be included in the configuration file. Any other double quotes (those embedded in the syslog-ng.conf stanzas themselves) must be escaped with a backslash '\,' as when defining destination IP addresses above.

2. At the LTM command line, direct the include file to the bigpipe shell (bpsh):

```
[root@bigip:Active] config # bpsh < syslog.inc
```

3. Verify your "include" statement has been included in the running configuration by running the following command:

```
b syslog include
```

The output should reflect the contents of the file you directed to bpsh:

```
[root@bigip] config # b syslog include
 SYSLOG - Include Data:
 destination remote_server {
 udp("10.4.0.1" port (514));
 udp("10.5.0.1" port (514));
 };
 filter f_alllogs {
 level (notice...emerg);
 };
 log {
 source(local);
 filter(f_alllogs);
 destination(remote_server);
 };
```

If no data has been included, the output will look like this instead:

```
[root@bigip] config # b syslog include
 SYSLOG - Include Data: none
```

4. Test your configuration before saving. To roll back changes, you can just reload the permanent configuration:

```
bigpipe load
```

5. Once you've confirmed them, save your changes to the permament configuration:

```
bigpipe save
```

(If you do not save, the configuration changes will be lost when the configuration is reloaded.)

Modifying the default logging

The third example in SOL5527 ("Configuring BIG-IP to send specific logs to remote servers") requires a slightly different approach, since a destination definition will be added, and an existing stanza must then refer to that new destination.

To change the existing syslog-ng configuration, you'll follow the same approach outlined above, but the include file will first define the remote server, then re-define the existing stanza in its entirety to include the original options plus the new destination. (Be sure to escape any double quotes.):

```
syslog include "
 destination remote_server {
 udp(\"10.4.0.1\" port (514));
 udp(\"10.5.0.1\" port (514));
 };

# local0.*               /var/log/ltm
filter f_local0 {
  facility(local0) and level(debug..emerg);
};
filter f_no_audit {
  not match(\"AUDIT\");
};
destination d_ltm {
  file(\"/var/log/ltm\" create_dirs(yes));
};
log {
  source(local);
  filter(f_local0);
  filter(f_no_audit);
  destination(d_ltm);
 destination(remote_server);
};"
```

The output should again reflect the contents of the file you directed to bpsh:

```
[root@bigip] config # b syslog include
SYSLOG - Include Data:
destination remote_server {
  udp("10.4.0.1" port (514));
  udp("10.5.0.1" port (514));
};
# local0.*               /var/log/ltm
filter f_local0 {
  facility(local0) and level(debug..emerg);
};
filter f_no_audit {
  not match("AUDIT");
};
destination d_ltm {
  file("/var/log/ltm" create_dirs(yes));
};
log {
  source(local);
```

```
  filter(f_local0);
  filter(f_no_audit);
  destination(d_ltm);
 destination(remote_server);
};
```

Including a new file replaces any previous includes, so existing entries from a previous include operation can be removed by including anything again.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com