Proposed new Lua commands for DNSDIST
June 7, 2017
Seth Ornstein
Global Cyber Alliance
sornstein@globalcyberalliance.org

To obtain a copy of the source for the modified DNSDIST version:

    git clone -b dnsdist-mod2 https://github.com/GlobalCyberAlliance/pdns.git

Example scripts and configuration file are located in: pdns/zzz-gca-examples

Lua additional functions that act on the DNSQuestion parameter dq.

They are expected to be used inside of a Lua function that is setup for use in the dnsdist configuration file by the addLuaAction function.   They are used to store text label and value pairs in the DNSQuestion dq and accessed by the DNSResponse Lua functions below.

    To store a text label and value pair in the DNSQuestion:

        dq:setTag("LabelText", "ValueText")

    To store values as a table in the DNSQuestion structure:

        dq:setTagArray(exampleTable)

Lua additional functions that act on the DNSResponse parameter dr.

These are expected to be located inside of a Lua function that is setup for use in the dnsdist configuration file by the RemoteLogAction function as the "alterFunction". They are used to obtain the text label and value pairs that were stored in the DNSQuestion Lua functions above.

    To read matching value from DNSQuestion structure:

        dr:getTagMatch("LabelText")

    To read text values as an array from DNSQuestion structure:

        dr:getTagArray()

Lua additional functions that act on the DNSDistProtoBufMessage parameter pbMsg.

These are expected to be located inside of a Lua function that is setup for use in the dnsdist configuration file by the RemoteLogAction function as the "alterFunction". They are used to modify the protobuf message that is being sent to the protobuf server.

To store text values in the protobuf "tags" field:

pbMsg:setTag("LabelText", "ValueText")

To store text values as a table in protobuf tag fields

pbMsg:setTagArray(exampleTable)

To change the protobuf message from a 'query' to a 'response'.
The variable is the dns name the client requested to be looked up.
A zero is inserted in the 'query time' protobuf field.

pbMsg:setProtobufResponseType("example.com")

To change the protobuf message from a 'query' to a 'response' and set 'query time'.
The variable is the dns name the client requested to be looked up.
The second variable is the query time in seconds.
The third variable is the fractional micro-seconds.

pbMsg:setProtobufResponseTypeQT("example.com", os.time(), 123456)

Building the modified dnsdist with the new Lua functions:

1. Open a console in pdns/zzz-gca-examples and run ./build-dnsdist2.sh
   This builds dnsdist with libsodium enabled for cache testing.

Running the test scripts:

1. Open a console in pdns/zzz-gca-examples and run ./protobuf-server2.sh

2. Open a console in pdns/zzz-gca-examples and run ./dnsdist2.sh

3. Open a console in pdns/zzz-gca-examples and run ./dig-test-rpz.sh

4. Verify that the protobuf server console shows a response with tags indicating RPZ.

5. Open a console in pdns/zzz-gca-examples and run ./dig-test-nocookie.sh

6. Verify that the protobuf server console shows a response with tags indicating FWD.

7. Run ./dig-test-nocookie.sh a second time.

8. Verify that the protobuf server console shows a response with tags indicating CACHE.

Protobuf server sample output:

Note that the unused "Tags" protobuf field now has the entries passed by the pbMsg:setTag and pbMsg:setTagArray functions. The tag data is separated by commas and the order is label followed by value for each 'Tag' in the protobuf 'Tags' field. The values in the protobuf 'Tags' field were set by the pbMsg:setTagArray function in luaLogBL in dnsdist.conf

Typical response from the protobuf server from a RPZ 'hit' :

Note that since this protobuf was originally a 'query' and not a 'response' due to dnsdist's treatment of returning a NXDOMAIN response to the client without having examined the cache or forwarded the request to a DNS server. Also since the function pbMsg:setProtobufResponseType was used the 'Query time' field has the zero time.

[2017-06-07 12:11:45.745800] Response of size 56: 127.0.0.1 -> 127.0.0.1 (UDP), id: 15891, uuid: dc7c809436b74bc48b7dc07b49f3831d
- Question: 1, 1, 1jw2mr4fmky.net.
- Query time: 1969-12-31 19:00:00.0
- Response Code: 3, RRs: 1, Tags: lua-time,12:11:45-06/07/17,Test1,One Two Three,lua-ver,Lua 5.1,Test2,Four Five Six,Trans,RPZ,RPZ-Info,reject-example,From,127.0.0.1:56144,TCP,false
        - 1, 1, 1jw2mr4fmky.net., 123, 127.0.0.1

Typical response from the protobuf server from a forwarded message:

Note that the protobuf 'Tags' field has the label 'Trans' and the value 'FWD', which was set using the pbMsg:setTagArray function in luaLogForward in dnsdist.conf.

[2017-06-07 12:12:50.409444] Response of size 87: 127.0.0.1 -> 127.0.0.1 (UDP), id: 52616, uuid: 3ec48935be3846609cc175136693608f
- Question: 1, 1, google.com.
- Query time: 2017-06-07 12:12:50.390094
- Response Code: 0, RRs: 3, Tags: Trans,FWD
        - 1, 1, google.com., 299, 216.58.217.78
        - 1, 1, google.com., 299, 216.58.217.78
        - 1, 1, google.com., 299, 216.58.217.78

Typical response from the protobuf server from a cache message:

Note that the protobuf 'Tags' field has the label 'Trans' and the value 'CACHE', which was set using the pbMsg:setTagArray function in luaLogForward in dnsdist.conf.

[2017-06-07 12:12:55.598121] Response of size 87: 127.0.0.1 -> 127.0.0.1 (UDP), id: 29215, uuid: d16852328b394d49ac0519fd7a2b6a25
- Question: 1, 1, google.com.
- Query time: 2017-06-07 12:12:55.598087
- Response Code: 0, RRs: 3, Tags: Trans,CACHE
        - 1, 1, google.com., 294, 216.58.217.78
        - 1, 1, google.com., 294, 216.58.217.78
        - 1, 1, google.com., 294, 216.58.217.78

Additional scripts:

make-dnsdist.sh - make script for dnsdist

dnsdist-check-config.sh - quick checking of dnsdist.conf configuration file.

dnsdist2-debug.sh - run dnsdist with configuration file with debugging statements.

dnsdist-debug.conf - configuration file for use with dnsdist2-debug.sh
        Note that you need to set lines 20 to 25 to true to enable the text debugging.

Source code files modified in DNSDIST:

dnsdist-lua.cc

dnsdist-lua2.cc

dnsdist.hh

protobuf.cc

protobuf.hh

To locate the modified source code search for the words Seth or GCA

ie. grep -i Seth *   or grep -i GCA *