F5 BIP-IP Log Insight Content Pack

- **Overview:**
  The vRealize Log Insight Content Pack for F5 BIG-IP enables a simple and intuitive way of collecting, analyzing and structuring various aspects of F5 BIG-IP system such system logs, network traffic data, performance logs etc. and graphically displaying them on the Log Insight console in an easy to understand manner. The information is collected using syslog, making REST API calls, iRules and high speed logging (HSL). These logs are analyzed in real time and plotted under various dashboards to give an overview on F5 systems and send out alerts in case of critical events.

- **Description:**
  The vRealize Log Insight Content Pack for F5 BIG-IP includes 8 predefined dashboards, and around 53 widgets and 10 alerts for offering a more customized user experience to F5 BIG-IP administrators.
  The content pack includes:
  Events from LTM - Local Traffic Manager Logs (Pool/Node Status Info, Hardware Issues): These 2 dashboards talk of various events derived from LTM logs identified by specific error codes. It covers incidents related to node and pool status and hardware related issues like temperature, fan speed, slot id etc.
  GTM - Global Traffic Manager and DNS Statistics: This dashboard group covers DNS related events such as DNS lookup failure, various events related to DNS request and response, wide IP and virtual server IP. The DNS Statistics dashboard also gives you DNS AVR and DNS global statistics of the BIG-IP system to help you manage and report on the DNS traffic on your network.
  Web Access Info: Widgets in these dashboard groups provide details on the LTM traffic. The widgets are logically clubbed into 2 dashboards under this based on traffic being categorized on basis of request and response time.
  AVR Statistics: This group makes use of Application Visibility and Reporting (AVR) module to render various widgets using the analytics profile that is set up.

- **Tech Specs:**

  - **Compatibility:**
    F5 BIG-IP 11.4, 12.x, 13.x. Licensed LTM, GTM modules.

  - **Pre requisites:**

    - You need to enable **AVR** (*Application Visibility and Reporting*) module on the BIG-IP system. This should be configured to send the logs remotely to LI instance.
      Follow the link: https://support.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/avr-implementations-11-2-0/1.html

Important:
Currently there are issue with AVR log "ServerLatencyMax" field in F5 BIG IP v13.x. The field gets ”N/A" value like ServerLatencyMax="N/A".

The following workaround suggested to fix value for the ServerLatencyMax field:
Please navigate to "Local Traffic" ›› Profiles : Analytics : HTTP Analytics >> MNIT-VRLI-http and unchecked checkbox for the "HTTP Timing (RTT, TTFB, Duration)" field in the "Collected Metrics" section. (Need to be wait for 5min for new logs)

- **Set up and view DNS statistics:** To view DNS AVR and DNS global statistics you need to configure this. This will also have external logging enabled which will send the logs remotely to your LI server.
  Follow the link:
  v11 https://support.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/avr-implementations-11-2-0/1.html
  v12 https://support.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/analytics-implementations-12-1-0/1.html
  v13 https://support.f5.com/kb/en-us/products/big-ip_analytics/manuals/product/analytics-implementations-13-1-0/1.html

- **Requirement:**
  This content pack uses syslog mechanism to send remote syslog data from an F5 device to Log Insight Server. Steps to configure it are mentioned in the section “**Configure F5 for syslog**” below.

- **Installation**
  - Navigate to the "Content Pack" menu in Log Insight. Select the "Import Content Pack" button. In the "Import Content Pack" menu, do the following:
  -Select the "Browse..." button and select the content pack you are trying to import
  -Select the "Install as content pack" radio button
  -Select the "Import" button

  Alternately, you can also install the content pack from the marketplace available on Log Insight UI
  -On Log Insight UI, browse to Content Pack ->Marketplace
  -Click on the content pack and then click ‘Install’

- **Configuration:**

- ***Configure F5 for syslog***

Add the Log Insight server IP to the remote syslog server list in the F5 BIG-IP system to send remote syslog data from an F5 device to Log Insight Server. To do this follow the instructions at:

https://support.f5.com/kb/en-us/solutions/public/13000/000/sol13080.html

- ***iRule for LTM***

In order to collect additional data from F5 LTM, iRules need to be configured in F5 which will send traffic data as HSL through the F5 device to Log Insight server.

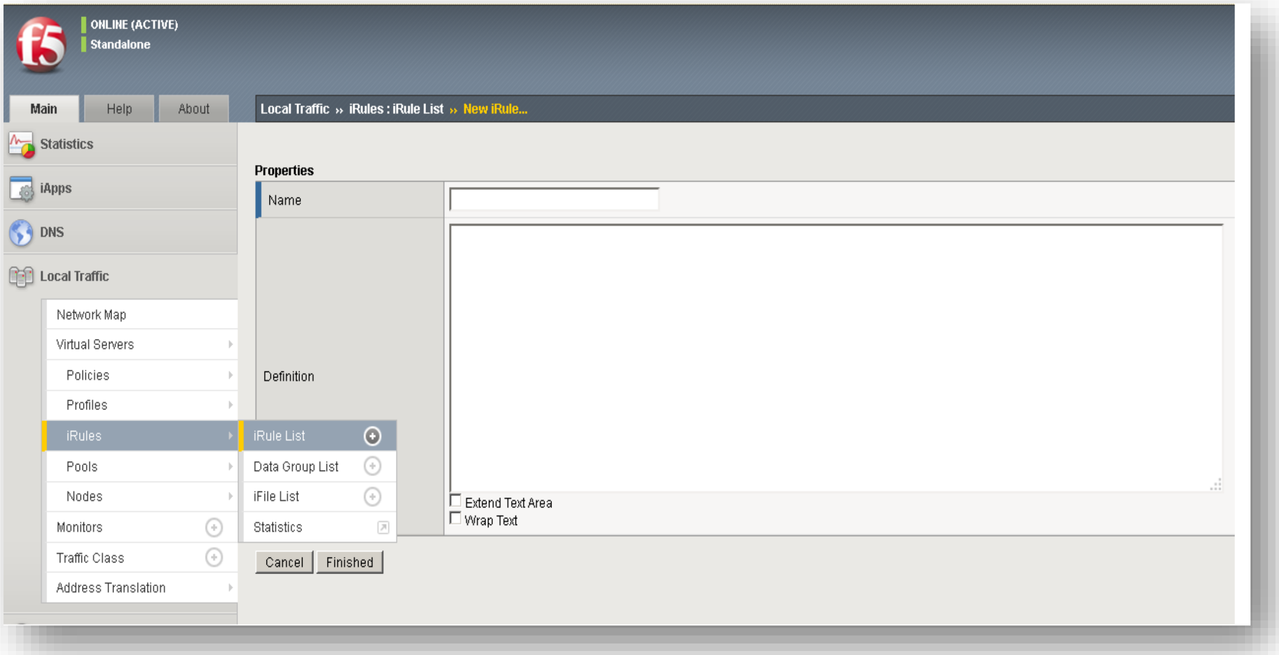
Pre-requisite:

Using the F5 BIG-IP User Interface (UI) /configuration utility, create a Pool for HSL with pool name **logInsight_pool_syslog**. Add this pool to the Local Traffic Pool List in the F5 BIG-IP system. Add a pool member with IP address of your Log Insight server specifying Node Name as **logInsight_node**.

Configure iRules for LTM:

Follow the steps mentioned below to add iRule for LTM:

- Login to the F5 BIG-IP User Interface (UI) /configuration utility.
- Click on **Local Traffic → iRules → iRule List**
- Click on **Create**
- Enter Name as “**logInsight_iRule_http**”, copy and paste the code below and click Finished.



```
# =============================
# iRule: logInsight_iRule_http START
# ==============================

when CLIENT_ACCEPTED {
    set client [IP::client_addr]
    set client_req_start_time [clock clicks -milliseconds]
}

when SERVER_CONNECTED
{
     set server_req_start_time [clock clicks -milliseconds]
}

when HTTP_REQUEST_SEND
{
    set http_req_send_start_time [clock clicks -milliseconds]
    set node_elapsed_time [expr {$http_req_send_start_time - $server_req_start_time}]

}

when HTTP_REQUEST {

    set client_latency [expr {[clock clicks -milliseconds] -  $client_req_start_time} ]
    set vhost [HTTP::host]:[TCP::local_port]
```

```
   set url [HTTP::uri]
   set method [HTTP::method]
   set http_version [HTTP::version]
   set user_agent [HTTP::header "User-Agent"]
   set tcp_start_time [clock clicks -milliseconds]
   set req_start_time [clock format [clock seconds] -format "%Y/%m/%d %H:%M:%S"]
   set req_elapsed_time 0
   set virtual_server [LB::server]

   if { [HTTP::header Content-Length] > 0 } then {
      set req_length [HTTP::header "Content-Length"]
      if {$req_length > 4000000} then {
         set req_length 4000000
      }
      HTTP::collect $req_length
   } else {
      set req_length 0
   }

   if { [HTTP::header "Referer"] ne "" } then {
      set referer [HTTP::header "Referer"]
   } else {
      set referer -
   }
}


when HTTP_RESPONSE {

   set hsl [HSL::open -proto TCP -pool logInsight_pool_syslog]
   set resp_start_time [clock format [clock seconds] -format "%Y/%m/%d %H:%M:%S"]
   set node [IP::server_addr]:[TCP::server_port]
   set status [HTTP::status]
  set req_elapsed_time [expr {[clock clicks -milliseconds] - $tcp_start_time}]
   set server_latency [expr {[clock clicks -milliseconds] -  $server_req_start_time} ]

   if { [HTTP::header Content-Length] > 0 } then {
      set response_length [HTTP::header "Content-Length"]
   } else {
      set response_length 0
   }

  HSL::send $hsl
"<190>f5_web_access_info|$vhost|$virtual_server|$client|$method|\"$url\"|HTTP/$http
```

```
_version|$req_start_time|$req_length|$req_elapsed_time|$node|$status|$resp_start_ti
me|$response_length|$user_agent|$client_latency|$server_latency|\"$referer\"\r\n"
}

# =============================
# iRule: logInsight_iRule_http END
# ==============================
```

- After this add the iRule under Resources tab of virtual server.
- Go to **Local Traffic →Virtual Servers → Virtual Server List**
- Click on the **desired virtual server name from the list → Click on Resources tab**
- Under **iRules →Click Manage**
- From the **Available** list on the right add the iRule created above to the **Enabled** List and click **Finished.**

- ***iRules for GTM***

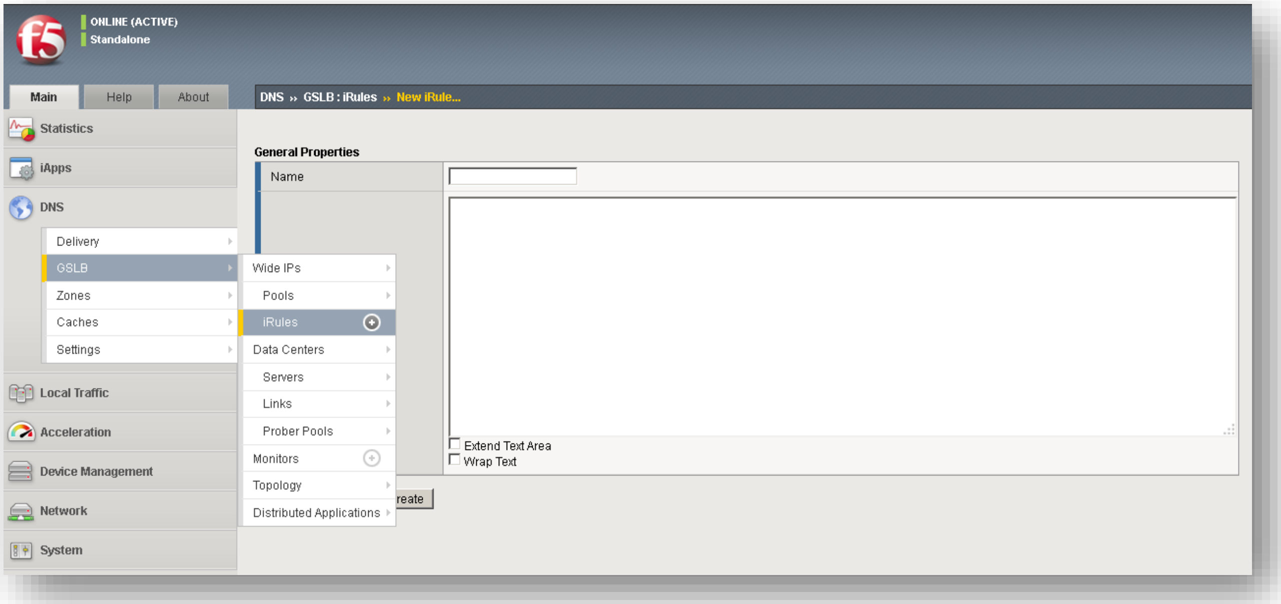
Global Traffic data can be directed to Log Insight server instance by creating an iRule. Check this link for more info: https://support.f5.com/kb/en-us/products/big-ip_gtm/manuals/product/gtm_config_guide_10_1.html.

Configure iRules for GTM

For logInsight_dns_request:

Follow the steps mentioned below to add iRule for GTM:

- Login to the F5 BIG-IP User Interface (UI) /configuration utility.
- Click on **DNS → GSLB → iRules → Create**
- Enter the name as "**logInsight_dns_request**", copy and paste the code below and click on Create.



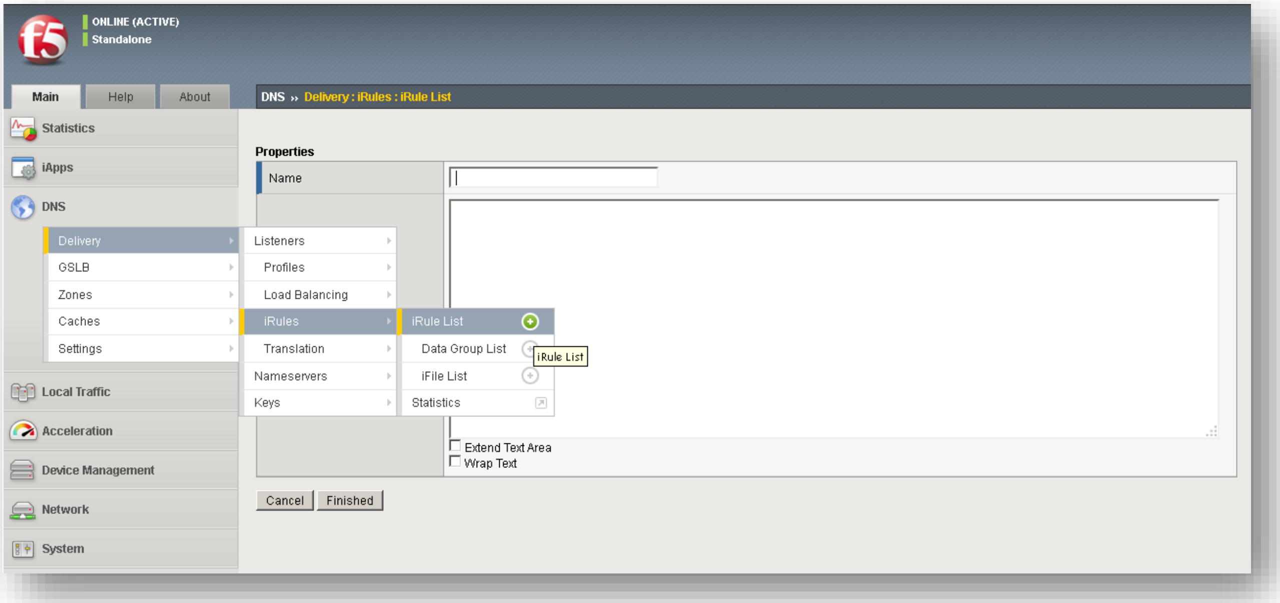
```
# ===============================
# iRule: logInsight_dns_request START
# ================================
    when DNS_REQUEST {
      set client_addr [IP::client_addr]
      set dns_server_addr [IP::local_addr]
      set question_name [DNS::question name]
      set question_class [DNS::question class]
      set question_type [DNS::question type]
      set data_center [whereami]
      set geo_information [join [whereis $client_addr] ;]
      set gtm_server [whoami]
      set wideip [wideip name]
      set dns_len [DNS::len]

      set hsl [HSL::open -proto UDP -pool logInsight_pool_syslog]
      HSL::send $hsl
    "<190>f5_irule=web_access_DNS_REQUEST,src_ip=$client_addr,dns_server_ip=$dns_server_addr,src_geo_info=$geo_information,question_name=$question_name,question_class=$question_class,question_type=$question_type,data_center=$data_center,gtm_server=$gtm_server,wideip=$wideip,dns_len=$dns_len\r\n"
    }

# ===============================
# iRule: logInsight_dns_request END
# ================================
```

- Go to **GSLB→Wide IPs → Wide IP List**
- Click on the desired **Wide IP name** from the list → **Click on iRule tab**
- Under **iRules →Click Manage**
- From the **drop down** list select the iRule created above and click **Add** and then click **Finished.**

For logInsight_dns_response:

Follow the steps mentioned below to add iRule for GTM:

- Login to the F5 BIG-IP User Interface (UI) /configuration utility.
- Click on **DNS → Delivery → iRules → iRuleList → Create**
- Enter the name as "**logInsight_dns_response**", copy and paste the code below and click on Finished.



```
# ================================
# iRule: logInsight_dns_response START
# =================================
when DNS_RESPONSE {
   set client_addr [IP::client_addr]
   set dns_server_addr [IP::local_addr]
   set question_name [DNS::question name]
   set is_wideip [DNS::is_wideip [DNS::question name]]
   set answer [join [DNS::answer] ;]
   set hsl [HSL::open -proto UDP -pool logInsight_pool_syslog]
   HSL::send $hsl "<190>f5_irule=web_access_DNS_RESPONSE,src_ip=$client_addr,dns_server_ip=$dns_server_addr,question_name=$question_name,is_wideip=$is_wideip,answer=\"$answer\"\r\n"
}
# ===============================
# iRule: logInsight_dns_response END
# ================================
```

- Go to **DNS→Delivery → Listeners List**
- Click on the desired **listener name** from the list → **Click on iRule tab**
- Under **iRules →Click Manage**
- From the **Available** list on the right add the iRule created above to the **Enabled** List and click **Finished.**