INTEGRATION GUIDE

Deploying the vRealize Orchestrator Plug-in for F5 BIG-IP

April 2017 | Kent Munson

Contents

Introduction

Private cloud platforms are an essential tool enterprises use to deploy applications with the agility and efficiency of a public cloud. Enterprise customers have long realized the need to reduce their application deployment times from weeks down to minutes and have an infrastructure that rapidly adapts to these requirements. In order to realize these efficiencies a private cloud platform needs to address the following criteria:

1. **Virtualized** – the underlying platform is virtualized thereby using the full capacity of the underlying hardware
2. **Fully Orchestrated** - All components in the application. from server and storage, to networking, DNS and ADC can be combined into automated workflows using the respective vendors Application Programming Interfaces (APIs).
3. **Automated** – All the necessary components of the application deployment can be combined into a repeatable template or 'blueprint' that allows a push button deployment. However, automation does not remove the criticality of ensuring security. The necessary intelligence of security is incorporated into these blueprints.
4. **Monitoring and Performance:** A fully virtualized private cloud platform needs to have full insight into the performance of each layer of their infrastructure so operations staff can quickly identify and remediate potential performance and security bottlenecks.

This document provides clear guidance on deploying applications within the VMware vRealize Suite and the F5 BIG-IP. Customers have the ability to make full use of the full vRealize Suite in combination with BIG-IP.

Deploy the vRealize Orchestrator Plugin for BIG-IP

The *Blue Medora VMware vRealize Orchestrator (vRO) Plug-in for F5 BIG-IP Installation and Configuration Guide* describes how to install and run the workflows in Blue Medora's F5 BIG-IP Orchestrator Plug-in.

Installation and Configuration Requirements

Before installing and configuring the plug-in, ensure your system meets the following requirements:

	vRealize Orchestrator (vRO) Requirements	F5 BIG-IP Requirements
Version(s)	**vRealize Orchestrator 6 or 7**	**F5 BIG-IP v11.5.0+**
Credentials	vRO User Name/Password with **Administrative level access**	**F5 BIG-IP** User Name/Password with **Administrative level access**
Connection	vRO hostname or IP address	Hostname (Management IP or DNS name) of F5 BIG-IP system

NOTE: These instructions were written based on the Orchestrator 7 user interface. Some differences may exist between version 6 and 7 of vRO.

Licensing Requirements

A license key will be provided by Blue Medora when the plug-in is purchased, and must be added as a Registration key before the plug-in can be used. Licensing for the plug-in is per F5 BIG-IP instance.

Refer to Running the License BIG-IP Workflow for details about validating your plug-in license in vRealize Orchestrator.

Installing the Plug-in

Complete the following tasks to install the Plug-in in vRealize Orchestrator:

1. Uploading the Installation File
2. Re-starting Orchestrator (recommended)

Uploading the Installation File

The F5 BIG-IP plug-in is installed using a **.dar** file.

Before you begin

1. Obtain the F5 plug-in installation (**.dar**) file from: **http://www.bluemedora.com/products**
2. Ensure you have administrator privileges to access the vRealize Orchestrator portal.

To install the plug-in file

1. Save the plug-in **.dar** file in a temporary folder.
2. From a Web browser, navigate to the vRealize Orchestrator portal.
3. Click the **Orchestrator Control Center** link.
4. At the login prompt, type your Orchestrator admin credentials to log into the Control Center.
5. In the **Plug-ins** area, click the **Manage Plug-ins** icon.
6. In the Manage Plug-ins window, click ***Browse*** to navigate to the location where you saved the plug-in installation (.dar) file, and then click **Install**.
7. Click **Install** again when you see the preview of the plug-in.

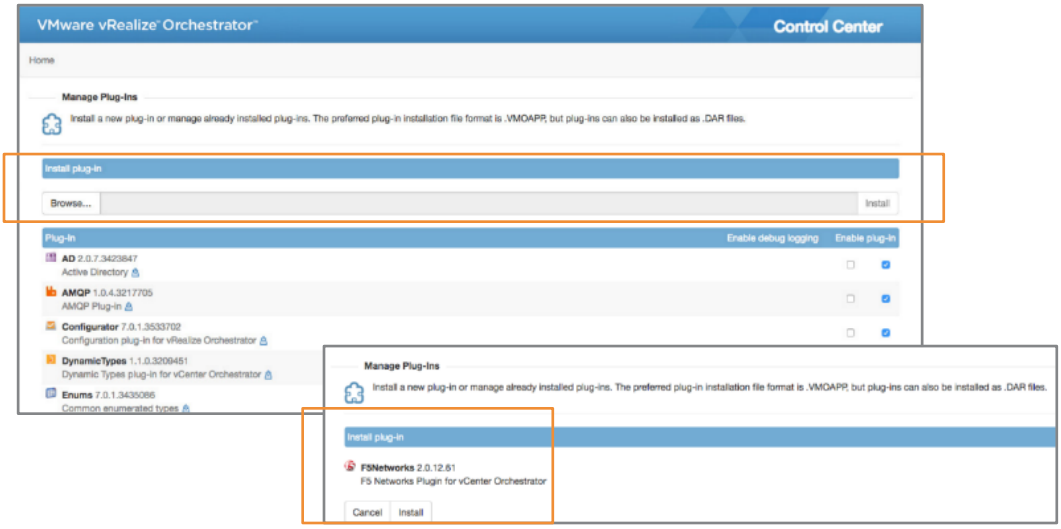

Figure 1: Manage Plug-ins Window

8. Once the F5 Plug-in has been installed, you see it in the Plug-in list.

Restarting the Orchestrator

After the plug-in is installed, we recommend you re-start the Orchestrator for the changes to take effect.

1. Click **Home** to return to the Control Center main page.
2. In the **Manage** area, click the **Startup Options** icon.
3. Under **Current Status**, click **Restart** to restart the Orchestrator service.

Running Workflows

Once you have installed the plug-in, you must run the *Attach BIG-IP* workflow (which configures the plug-in to an F5 BIG-IP instance) as well as the *License BIG-IP* workflow (which ensures the plug-in is licensed for use). After running these preliminary workflows, there are more than 50 additional workflows available in the plug-in to help automate your F5 administration tasks. Refer to Plug-in Workflows for the full list of workflows included with the plug-in.

Running the Attach BIG-IP Workflow

Before you can begin using the F5 plug-in, a BIG-IP system must be configured (attached) to pull in the necessary F5 objects.

Before you begin

1. Install the plug-in. Refer to Installing the Plug-in.
2. Ensure you have the appropriate F5 BIG-IP system hostname, admin level credentials, and plug-in license key.

To attach the BIG-IP workflow

1. Open the vRealize Orchestrator portal.
2. Click the **Start Orchestrator Client** link.
3. At the Orchestrator Login screen, enter your vRO admin credentials.

   *NOTE: If logging in to the Orchestrator for the first time, a notice to download a Java **client.jnlp** file appears. Follow the instructions to download and run the file to enable the Orchestrator client.*
4. Once you have logged in, click the **Workflows** tab.
5. Expand the **F5** folder. You see four high-level categories for F5 BIG-IP workflows: Basic, Ltm, Net, and Sys.
6. Expand the **Basic** category folder to view all the available basic workflows. The first workflow you need to run is the *Attach BIG-IP* workflow, which configures and licenses a BIG-IP instance for use.
7. Right-click the **Attach BIG-IP** workflow.
8. In the Attach BIG-IP workflow window, type the following information, and then click **Submit**:
   - The **Hostname** (or IP address) of the BIG-IP instance.
   - The **Username** of the BIG-IP instance.
   - The **Password** associated with the username of the BIG-IP instance.
9. After the workflw has finished running, a green checkmark appears next to the workflow indicating it was successful.

   NOTE: If a workflow fails, a red X appears next to the workflow, and errors are logged at the bottom of the screen.
10. Now that a BIG-IP instance has been configured for the plug-in, click the **Inventory** tab to ensure the F5 objects are visible in the F5 Networks Inventory Tree.

Running the License BIG-IP Workflow

Next, you must run the **License BIG-**IP workflow prior to general use of the plug-in. This workflow ensures a license key has been added in order to use the plug-in after purchase.

License BIG-IP workflow

1. Click the **Workflows** tab.
2. From the **Basic** category, right-click **License BIG-IP** and then click **Start workflow** to run the workflow.

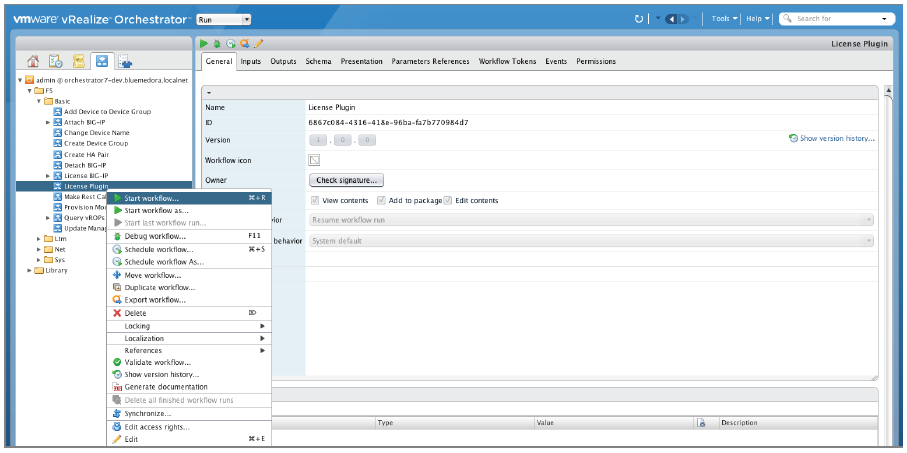

Figure 2: License BIG-IP Workflow

3. In the Start Workflow: License BIG-IP window, enter the license key from your plugin purchase.
4. Click **Submit** to run the workflow.

Additional workflows

Once you have successfully run both the **Attach BIG-IP** and **License BIG-IP** workflows, you can run any of the other workflows provided with the plug-in (refer to Plug-in Workflows).

The following section outlines a workflow that enables communication between the plug-in and the related vROps F5 management pack, also provided by Blue Medora. This example workflow process represents just one of the many options you have for automating your F5-related IT tasks.

Running the Query vROps Workflow

One of the unique workflows provided with the plug-in enables communication between the F5 vRO plug-in and the F5 vROps management pack.

Query vROps workflow

1. Click the **Workflows** tab.
2. From the **Basic** category, right-click **Query vROps** and then click **Start workflow** to run the workflow.
3. In the Start Workflow: Query vROps window, enter the BIG-IP instance that will query vROps, the appropriate vROps hostname and credentials, and the vROps resource ID to identify an object, and then click ***Submit*** to run the workflow.

Using API Explorer

To view all the available scripting objects, or search for a specific one, navigate to **Tools > API Explorer**. In the API Explorer window, you can search by specific F5 object names/keywords, or scroll through the list to browse. Select a scripting object to view related properties.

Plug-in Workflows

The vRO Plug-in for F5 BIG-IP contains the following out-of-box workflows.

Workflow Number	Workflow Name/Description
1	Create Virtual Server
2	Detach BIG-IP
3	Attach BIG-IP
4	Add Pool
5	Get Pools Members
6	Delete Pool
7	Delete Client SSL Profile
8	Delete Server SSL Profile
9	Remove Profile from Virtual Server
10	Delete VLAN
11	Delete Route Domain
12	Add VLAN
13	Add Profile to Virtual Server
14	Get member statistics and Get statistics for Pool Member
15	Create Route Domain
16	Add iRule to Virtual Server
17	Add Pool Member
18	Delete SSL Certificate
19	Delete SSL Key
20	Add SSL Certificate
21	Add SSL Key
22	Create SSL Client Profile with Certificate and Key
23	Create Server SSL Profile with Certificate and Key
24	Disable Pool Member
25	Enable Pool Member
26	Create HA Pair
27	License BIG-IP with conventional license
28	License BIG-IP with BIG-IQ pool license
29	Create Self IP
30	Create Route
31	Upload/install iApp
32	Upload/install certificates
33	Instantiate App Services iApp

Workflow Number	Workflow Name/Description
34	Query vROPs F5 Management pack
35	Add Persistence profile to virtual server
36	Adhoc REST Request
37	Duplicate Virtual Server
38	Get Pool member by name and port
39	Get Pools
40	Remove Pool Member
41	Add Node Workflow
42	Delete Node Workflow
43	Search for F5 Object
44	Route Domain Add Members
45	VLAN Add Interface
46	Upload iRule
47	Create Client SSL profile
48	Create Server SSL profile
49	Get FQDN from IP
50	Get IP from FQDN
51	Remove Virtual Server
52	Delete Route

Install vRealize Operations Manager Management Pack

Installation and Configuration Requirements

Before installing and configuring the Management Pack for F5 BIG-IP, ensure your system meets the following requirements:

	vRealize Operations Requirements	F5 BIG-IP Requirements
Version(s)	**vRealize Operations v6.2+** (Advanced & Enterprise editions)	**F5 BIG-IP v11.6.0+**
Credentials	N/A	F5 BIG-IP username/password with a **minimum of Auditor user role with iControl REST API access**. **NOTE**: To create a user with permissions to read REST, you must first create an Auditor user, then give the user REST permissions as described in the "About iControl and RBAC for user accounts" section of the iControl® REST User Guide, version 11.6. **NOTE**: An F5 Administrator user role is required to collect the following metrics: **System**: CPU Idle Ticks CPU Usage Ticks: System CPU Usage Ticks: User Chassis Serial Number Memory Total Memory Used Platform Product **Device**: syncState **Device Group**: All metrics and resources (device groups will not exist with Auditor role)
Connection	vROps hostname or IP address	F5 BIG-IP **hostname** (for example Management IP or DNS name of F5 BIG-IP System)

Licensing Requirements

When purchased individually, the Management Pack for F5 BIG-IP is licensed **per F5 BIG-IP instance (physical** or **virtual**).

Alternatively, customers who have purchased Blue Medora's True Visibility Suite (Standard, Advanced, or Enterprise) can access all management packs within that suite (and the edition below it, if applicable). The Management Pack for F5 BIG-IP is part of Blue Medora's **Advanced** True Visibility Suite (TVS), which means a TVS **Advanced** license or higher is required to use it. For more information, visit http://www.bluemedora.com/true-visibility-suite-for-vmware/.

A license key is provided by Blue Medora when the Management Pack or True Visibility Suite is purchased and must be added as an F5 BIG-IP Adapter License within vRealize Operations before the Management Pack can be configured and used. Refer to Adding a License Key for details.

Upgrading the Management Pack

Before upgrading to a newer version of the Management Pack (uploading a new **.pak** file), we recommend the following clean-up tasks:

1. Delete existing F5 BIG-IP dashboards.
2. Delete existing F5 BIG-IP adapter instance(s) and objects.

Deleting existing F5 BIG-IP dashboards

If you do not remove the dashboards from a previous version of the Management Pack before upgrading, you see duplicate F5 BIG-IP dashboards in the Dashboard List drop-down menu after installation.

To remove existing Management Pack dashboards:

1. Navigate to **Content > Dashboards**.
2. Multi-select all F5 BIG-IP dashboards.
3. Click **Delete Dashboard**.
4. Click **Yes** when the confirmation dialog box appears to delete the selected dashboards.

Deleting existing F5 BIG-IP adapter instance(s) and objects

You must also remove previous adapter instance(s) and their related objects, as the old instance(s) do not collect data and creating new instances makes new related objects instead of using existing objects.

After deleting existing dashboards and installing the new version of the Management Pack, remove the previous adapter instance(s) and their related objects, and then configure the new adapter instance(s).

To remove existing Management Pack adapter instance(s) and objects:

1. Log in to vRealize Operations as an administrator.
2. Click the Administration navigation shortcut. The **Solutions** view should automatically open.
3. From the **Solutions** list, click **F5 BIG-IP Adapter**.

4. Click the **Configure** icon. The **Manage Solution** window appears.
5. Select an instance from the list on the left and then click the **Delete** icon.
6. In the dialog box that appears, click **Remove related objects**, and then click **Yes**.

Installing the Management Pack

Installing the Management Pack in vRealize Operations involves completing the following tasks:

1. Uploading the Installation File
2. Adding a License Key

Uploading the Installation File

The Management Pack for F5 BIG-IP is installed using a .**pak** file.

Prerequisites

1. Obtain the Management Pack installation file from http://www.bluemedora.com/true-visibility-suite- for-vmware/.
2. Read the release notes included with the file.

To upload the file

1. Save the **.pak** file in a temporary location.
2. Log in to vRealize Operations as an admin user.
3. Click the **Home** icon, and then from the panel on the left, click the **Administration** navigation shortcut. In the right panel, the **Solutions** tab displays.
4. Click the ***Add*** icon to upload the **.pak** file to the vRealize Operations server.
5. In the dialog that appears, browse to the location of the saved .pak file, then click **Upload**.

   NOTE: The .pak file upload may take several minutes to complete. Status information appears in the Installation Details text box throughout the installation process.
6. When the upload has finished, click **Next**.
7. Read the *End User License Agreement (EULA)*, click to accept the terms, and then click ***Next***.
8. When the installation process is complete, click the **Finish** button.

   *NOTE: The installation utility creates the **bm_f5_big_ip** folder and **bm_f5_big_ip.jar** file in the **$VCOPS_BASE/user/plugins/inbound** folder. Refer to section* 7. Appendix I: Management Pack Folders and Files *for more information.*

Adding a License Key

The Management Pack requires a valid license for full operation. Complete the following steps to license the Management Pack.

To install the License

1. In vRealize Operations Manager, navigate to **Administration > Licensing > License Keys**.
2. Click the **Add** icon. In the dialog that appears, select **F5 BIG-IP**.
3. Enter your Blue Medora license key, then click **Validate**. If successful, you see a **License key validated successfully** message.
4. Click **Save**.

Configuring the Management Pack

Configuring the Management Pack for F5 BIG-IP includes the following tasks:

1. Creating an Adapter Instance and Credential
2. Manually Discovering Resources (if necessary)
3. Validating Management Pack Data Collection

Creating an Adapter Instance and Credentials

You must create an adapter instance and credential for the Management Pack to define the adapter type and identify the device(s) from which the adapter instance retrieves data.

Prerequisites

Install the Management Pack for F5 BIG-IP. Refer to section *5. Installing the Management Pack*.

To create the adapter instance and credentials

1. Log in to vRealize Operations as an administrator.
2. Click the **Administration** navigation shortcut. The **Solutions** view should automatically open.
3. From the **Solutions** list, click **F5 BIG-IP**.
4. Click the **Configure** icon. The **Manage Solution** window appears.

   *NOTE: If creating multiple adapter instances, click the **Add** icon above the list of **Instance Names** on the left.*

5. In the **Manage Solution** window, enter the following information:

   Adapter Settings:

   - **Display Name:** A name for this particular instance of the Management Pack.
   - **Description:** Optional; helps in differentiating multiple adapter instances of the Management Pack.

   Basic Settings:

   - **Host:** Management IP or DNS name of F5 BIG-IP System to be monitored.

   NOTE: To ensure the Management Pack is always receiving active metrics, you must set the host to a self

IP that follows the active load balancing when configuring against a failover cluster.

- **License Type:** Select Physical or Virtual, depending on your license type (either selection will work for TVS licensing).
- **Port:** Default port is 443; can be overridden (this is the port to access the iControl/Configuration interface).
- **Exclude Nodes and Pool Members:** Default value is **False** to avoid slowing down vROps for extremely large environments; set to **True** to include monitoring data for nodes and pool members.
- **Exclude Relationships:** Default value is **False** to avoid slowing down vROps for extremely large environments; set to **True** to include relationships.
- **Credential:** Click the **Add** icon, then select the credential type.

Advanced Settings:

- **Collectors/Groups:** Automatically selected.
- Support Autodiscovery: True/False.

  NOTE: For the Support Autodiscovery option, the default setting is True, which enables the adapter instance to create resources for you. If you select False, you must manually discover your F5 BIG-IP resources. Refer to the section Manually Discovering Resources *on this page for instructions.*
- **Timeout (Seconds):** A timeout interval (in seconds) for API calls; the recommended default value is 30 seconds.
- **Credential Name:** A name for this set of Management Pack credentials.
- **User Name:** User Name for your F5 BIG-IP user account.
- **Password:** Password for your F5 BIG-IP user account.

NOTE: The following vRealize user name/password fields are shown only when the deprecated credential kind is selected. These fields are maintained for backward compatibility purposes only and are not necessary for proper operation of the Management Pack.

- **vRealize User Name:** User Name for your vRealize Operations user account
- **vRealize Password:** Password for your vRealize Operations user account

6. Click **OK** to save your credential.
7. Click **Test Connection** to ensure vRealize Operations can connect properly to the system.
8. Click **Save Settings** to save your adapter instance configuration.

Manually Discovering Resources

With manual discovery, the adapter sends a request to F5 BIG-IP to return resources, which you then manually select to import into vRealize Operations.

Prerequisites

Create an F5 BIG-IP adapter instance and credential. Refer to the previous section, Creating an Adapter Instance

and Credential for details.

6.2.2 Manual Resource Discovery

1. Log in to vRealize Operations as an administrator.
2. Click the ***Administration*** navigation shortcut.
3. In the Navigation pane, click **Inventory Explorer**.
4. Under **Adapter Instances**, select the F5 BIG-IP Adapter Instance.
5. Click the **Discover Resources** icon to open the Discover Objects window.
6. In the **Discover Objects** window, complete the following information:
   - The Collector you want to use.

     NOTE: Unless you added additional collectors, the only available collector is your vROps server
   - Adapter Type = F5 BIG-IP Adapter.
   - Select the applicable **Adapter Instance**.
   - Discovery Info = F5 BIG-IP Discovery.
   - Choose whether ***Only New Objects*** (select or de-select checkbox) should be collected
7. Click **OK** to start the discovery process.
   The discovery process can take several seconds to several minutes. When it has finished, the ***Discovery Results*** window lists your resources.
8. Double-click each resource kind that contains resources to add.
9. Select options for each kind of resource. Refer to the following table.

OPTION	DESCRIPTION
Import	Import the resources but do not start collecting data. Resources appear in the resource list as Not Collecting; data is not stored; analysis is not performed.
Collect	Import the resources and start collecting data. When you select the Collect check box, the Import check box is also selected.

10. Click ***OK***. The ***Discovery Results*** window closes and the new resources appear.

What To Do Next

If you did not select the option to start metric collection when you defined a resource, you can start metric collection after the resource is defined. To start collecting metrics for a resource, choose the resources, and then click the **Start Collecting** icon.

Validating Data Collection

After you add an F5 BIG-IP adapter instance, the next task is to validate the data that it collects in vROps.

Prerequisites

Add an F5 BIG-IP adapter instance. Refer to Creating an Adapter Instance and Credentials.

To validate data collection

1. Select the ***Environment*** shortcut.

   NOTE: If you enabled Autodiscovery for the adapter instance, it will create resources as soon as it begins collecting metrics. If you disabled Autodiscovery for the adapter instance, you must go back and discover resources manually before you can validate data collection. Refer to section 6.2 Manually Discovering Resources.

2. Under Inventory Trees, select ***All Objects***, then expand the ***F5 BIG-IP Adapter*** objects list.

3. Select a resource from the list, then click the ***Troubleshooting*** tab and ***All Metrics*** view to validate values against the data source.

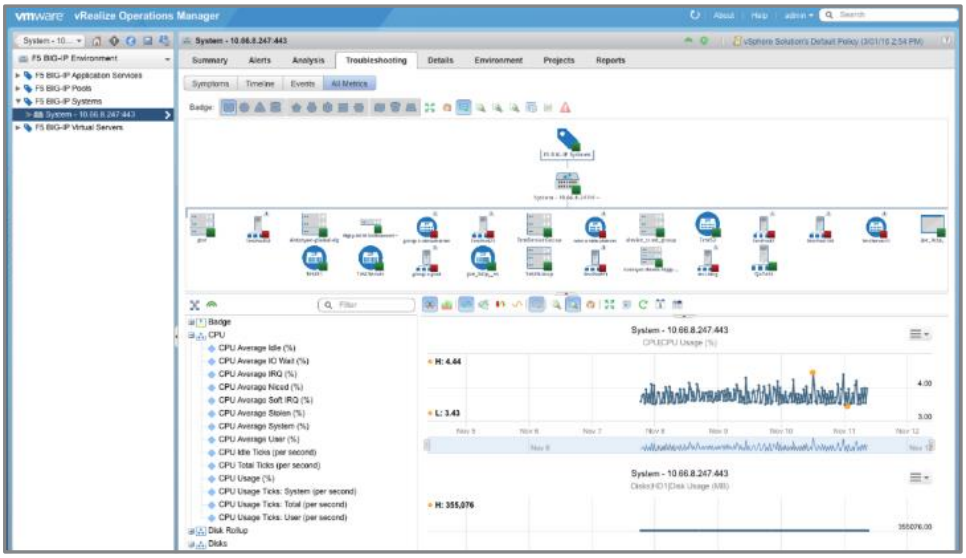

Figure 3: F5 BIG-IP Adapter Objects Troubleshooting

Installing the F5 BIG-IP Log Insight Content Pack

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 as system logs, network traffic data, and performance logs 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 two dashboards include various events derived from LTM logs identified by specific error codes. They cover incidents related to node and pool status and hardware related issues like temperature, fan speed, slot id, and so on.
- **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 Application Visibility and Reporting (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 two dashboards under this based on traffic being categorized on basis of request and response time.
- **AVR Statistics**
  This group makes use of the AVR module to render various widgets using the analytics profile that is set up.

Technical Specifications

Compatibility

F5 BIG-IP 11.4 and later. Licensed LTM, GTM modules.

Prerequisites:

1. 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-11-1-0/1.html
2. ***Set up and view DNS statistics:*** To view DNS AVR and DNS global statistics you need to configure this. It also has external logging enabled which will send the logs remotely to your LI server. Follow the link: https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-dns-services-implementations-11-3-0/11.html

Requirements:

This content pack uses a syslog mechanism to send remote syslog data from an F5 device to Log Insight Server. See the Configure F5 for syslog in the Configuration section for details.

Installation:

1. Navigate to the **Content Pack** menu in Log Insight.
2. Click the **Import Content Pack** button.
   From the **Import Content Pack** menu, do the following:
   - Click the **Browse** button and select the content pack you are trying to import.
   - Click the **Install as content pack** radio button.
   - Click the **Import** button

Alternately, you can also install the content pack from the marketplace available on Log Insight interface

1. From the Log Insight UI, browse to **Content Pack ->Marketplace**
3. Click 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

To collect additional data from F5 LTM, iRules need to be configured on the BIG-IP which send traffic data as HSL (High Speed Logging) through the F5 device to Log Insight server.

Prerequisites:

Using the F5 BIG-IP web-based Configuration utility, create a Pool for HSL with pool the 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, naming the node **logInsight_node**.

Configure iRules for LTM:

Follow the steps mentioned below to add iRule for LTM:

1. Login to the F5 BIG-IP Configuration utility.
2. Click **Local Traffic > Rules > iRule List**.
3. Click **Create**.
4. In the **Name** field, type **logInsight_iRule_http**
5. In the **Definition** section, copy and paste the following code.

```
# ============================
# 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|$resp_start_time|$response_length|$user_ag
ent|$client_latency|$server_latency|\"$referer\"\r\n"
}

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

6. Click **Finished**.

After creating the iRule, add it to the virtual server.

1. Click **Local Traffic > Virtual Servers > Virtual Server List.**
2. Click the appropriate virtual server, and then click **Resources** on the menu bar.
3. Under **iRules**, click **Manage**.
4. From the **Available** list, add the iRule you created and click the Add button (<<) to move it to the **Enabled** list.
5. 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:

1. Login to the F5 BIG-IP Configuration utility.
2. Click **DNS > GSLB > iRules**.
3. Click **Create**.
4. In the **Name** field, type **logInsight_dns_request**.
5. In the **Definition** section, copy and paste the following code.

```
# ================================
# 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=$question_class,quest
ion_type=$question_type,data_center=$data_center,gtm_server=$gtm_server,wideip=$wideip,dns_l
en=$dns_len\r\n"
}
# ================================
# iRule: logInsight_dns_request END
# ================================
```

6. Click **Finished**.
7. Click **GSLB > Wide IPs > Wide IP List**.
8. Click the appropriate Wide IP, and then click the **iRule** tab.
9. Under **iRules**, click **Manage**.
10. From the list, add the iRule you created and click the **Add** button.
11. Click **Finished**.

For logInsight_dns_response:

1. Login to the F5 BIG-IP Configuration utility.
2. Click **DNS > Delivery > iRules**.
3. Click **Create**.
4. In the **Name** field, type **logInsight_dns_response**.
5. In the **Definition** section, copy and paste the following code.

```
# ================================
# 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=$dns_server_addr,questio
n_name=$question_name,is_wideip=$is_wideip,answer=\"$answer\"\r\n"
}
# ================================
# iRule: logInsight_dns_response END
# ================================
```

6. Click **Finished**.
7. Click **DNS > Delivery > Listerner List**.
8. Click the appropriate Listener, and then click the **iRule** tab.
9. Under **iRules**, click **Manage**.
10. From the **Available** list, add the iRule you created and click the Add button (<<) to move it to the **Enabled** list.

For more information about F5 and VMware solutions, visit http://www.vmware.com/partners/global-alliances/f5.html or https://f5.com/solutions/technology-alliances/vmware.

Appendix I: Management Pack Folders and Files

The installer places the Management Pack (adapter) files in the **$VCOPS_BASE/user/plugins/inbound/bm_f5_big_ip** folder as shown below

Folder/File(s)	Folder/File(s)	Description
conf	dashboards (folder)	Contains JSON files for Management Pack Dashboards
	describe.xml	Describes the Management Pack
	describe.dtd	Used to validate describe XML
	images (folder)	Contains .png files for AdapterKind, ResourceKinds, and TraversalSpec
	oss_attribution.txt	Open source license file
	reports (folder)	Contains .xml files for Management Pack Reports
	reskndmetrics (folder)	Contains .xml files for Dashboard Metric configuration
	resources (folder)	Contains resources.properties file
	scripts (folder)	Contains .sdm files consumed by the adapter
	version.txt	Contains version information
	views (folder)	Contains .xml files for Management Pack Views
lib	Refer to lib folder for entire list	JAR files that contain the classes and resources used to implement the Management Pack
work	lastcollect.properties	Tracks when the last collection for each adapter instance was performed (used when historic mode is enabled)

Appendix II: Revision Notes

This guide is updated with each release of the product, or when necessary. The following table provides its revision history.

REVISION	DATE	DESCRIPTION
REV-03	25-NOV-2016	• Added *Upgrading the Management Pack* • Added new settings to configuration screen: *Exclude Pool Members and Nodes*, *Exclude Relationships*, and *Timeout (Seconds).* • Removed vRealize credential requirement and deprecated that credential screen. • Added support for F5 Auditor user role; documented additional metrics available for Administrator user role in the *System Requirements* table.
REV-02	27-SEP-2016	Added information to section *3. Licensing Requirements* about Blue Medora's True Visibility Suite
REV-01	30-SEP-2015	Initial release

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

Americas info@f5.com
Asia-Pacific apacinfo@f5.com
Europe/Middle-East/Africa emeainfo@f5.com
Japan f5j-info@f5.com