

Installing Splunk for F5 Big-IP – Part 1

Preparing the Splunk server to receive data

The data from the F5 is in a Syslog format and configuring Splunk to receive it is trivial. Simple add a UDP port for Splunk to listen on (514 is default syslog port, but any port can be used) as shown:

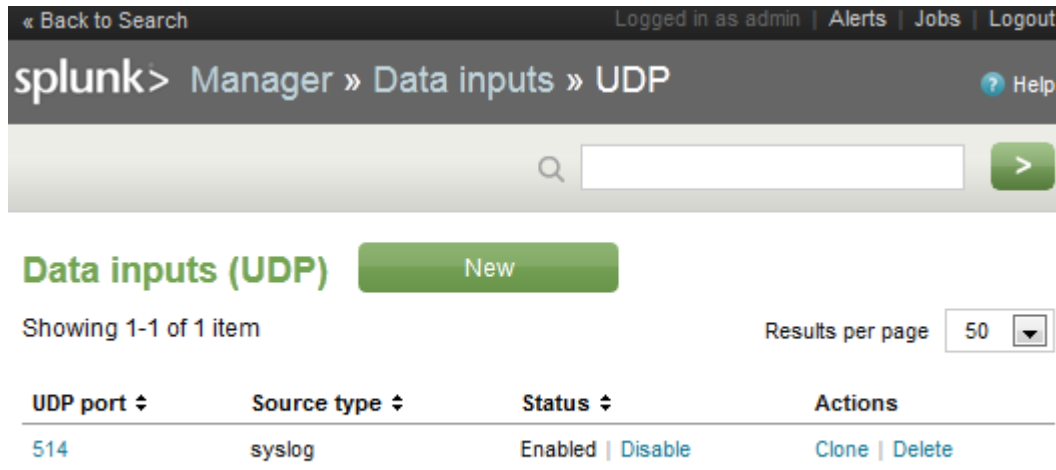


Fig 1-1

If a firewall is present on the system, it will need to be configured to allow traffic on the UDP port specified

Configuring the F5 Big-IP device to send the Data

Now that Splunk is listening for the data, the Big-IP will need to be configured to send it. To do this a pool will need to be created with the name 'pool_syslog', using the UDP health monitor and the Splunk server configured as a member of this pool. The service port will be the port configured on the Splunk server earlier.

See Figure 2-1 for an example.

Local Traffic » Pools : Pool List » New Pool...

Configuration: Basic

Name	pool_syslog	
Health Monitors	Active	Available
	udp << >>	https https_443 inband tcp tcp_half_open

Resources

Load Balancing Method	Round Robin
Priority Group Activation	Disabled
New Members	<input checked="" type="radio"/> New Address <input type="radio"/> Node List Address: 10.1.45.107 Service Port: 514 Select... Add R:1 P:0 C:0 10.1.45.107 :514 Edit Delete

Cancel Repeat Finished

Fig 2-1

Configuring the iRule on the BigIP

The Splunk for BigIP iRule will now need to be added to extract data from Web traffic.

Create a new iRule named splunk_http and copy the iRule data into the definition from the irule file accompanying the App. See figure 3-1 for configuration.

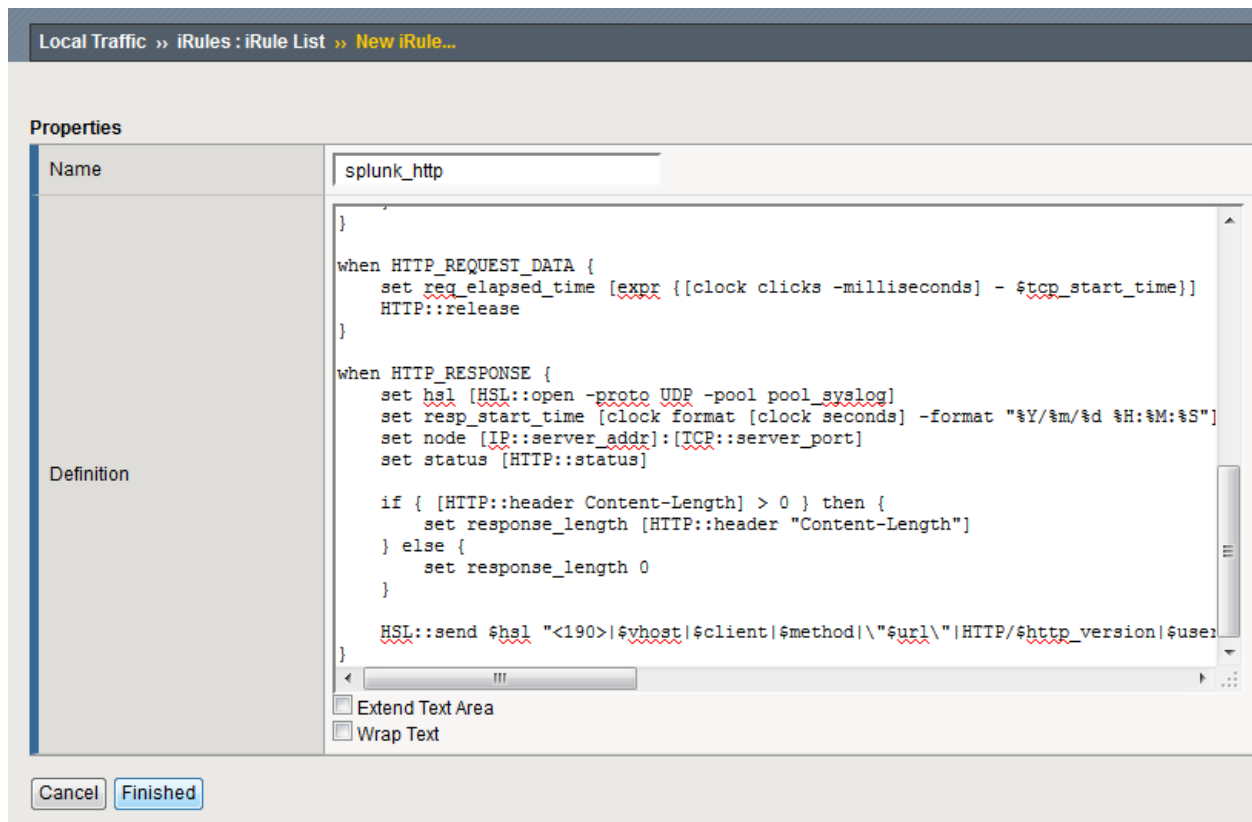


Fig 3-1

Adding the iRule to Virtual Servers

The iRule will need to be added to any Virtual Servers that you wish to extract the Web Data from. An HTTP profile will need to be enabled on the Virtual Server before the iRule will function properly. See figure 4-1 for example.


Local Traffic >> Virtual Servers : Virtual Server List >> vs_bd-labs.splunk.com_http

Properties

Resources

Statistics

General Properties

Name	vs_bd-labs.splunk.com_http
Partition	Common
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.1.232.221
Service Port	80 HTTP
Availability	
State	Enabled

Configuration: Basic

Type	Standard
Protocol	TCP
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	http
FTP Profile	None
SSL Profile (Client)	None
SSL Profile (Server)	None
Diameter Profile	None
SIP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels

Update
Delete

Fig 4-1

And now the iRule can be added. Go to the Resources tab on the Virtual Server and click on the manage button just above the iRule list.

Local Traffic » Virtual Servers : Virtual Server List » vs_bd-labs.splunk.com_http

Properties Resources Statistics

Load Balancing

Default Pool	pl_bd-labs.splunk.com_http
Default Persistence Profile	None
Fallback Persistence Profile	None

Update

iRules Manage...

Name
log_http

Enable the splunk_http iRule. This iRule can be added in any order and will not affect other iRules.