BIG-IP Logging and Reporting Toolkit - part two

Colin Walker, 2010-10-03

In this second offering from Joe Malek's delve into some advanced configuration concepts, and more specifically the logging and reporting world, we take a look at the vendors that he investigated, what they offer, and how they integrate with F5 products. He discusses some of the capabilities of each, their strengths and weaknesses and some of the things you might use each for. If you've been wondering what your options are for more in-depth log analysis and reporting, take a look to see what his thoughts are on a couple of the leading solutions.

- Logging & Reporting Toolkit - Part 1
- Logging & Reporting Toolkit - Part 2
- Logging & Reporting Toolkit - Part 3
- Logging & Reporting Toolkit - Part 4

Vendor descriptions:

Splunk - http://www.splunk.com/

"IT Search" is Splunk's self identified core functionality. Splunk's software contains multiple ways to obtain data from IT systems, indexes the data and reports on the data using a web interface. Splunk has invested in creating a Splunk for F5 application containing dashboard style views into log data for F5 products. Currently included in the application are LTM, GTM, ASM, APM and FirePass. The application is able to consume log messages sent to Splunk servers via syslog – and by extension iRules using High Speed Logging. Splunk is deployed as software to be installed on a customer provided system. Windows, Mac OS, Linux, AIX, and BSD variants are all supported host operating systems. Splunk can receive messages via files, syslog, SNMP, SCP, SFTP, FTP, generic network ports, FIFO queues, directory crawling and scripting. Splunk has a very intuitive and "Google like" interface allowing users to easily navigate and report on data in the system. Users are able to define reports, indices, dashboards and applications to present data as an organization requires. Upon receipt of data, Splunk can process the data according to in-built training or according to a user constructed taxonomy.

Q1 Labs - http://www.q1labs.com/

Q1 Labs brings a product called QRadar to market. QRadar combines functionality commonly found in SIEM, log management and network behavior analysis products. Q1 products are able to consume event messages as well as record information on a network connection basis. QRadar is available as a pay-for appliance and a no-charge edition in a virtual machine. Differences between the two editions are the SIEM and advanced correlation functionality. The no-charge edition is a log management tool only.

QRadar can receive messages via syslog SNMP, JDBC connectors, SFTP, FTP, SCP, and SDEE. Additionally QRadar con obtain network flow information in a port mirror/span mode. Customizing data views and report building are based on regular expressions. Customers can create their own regular expressions and build upon pre-configured expressions for reporting. In the SIEM module, QRadar includes approximately 250 events that can be sequenced together into complex "Offenses" in a manner similar to building a rule in Microsoft Outlook. "Universal Device Support Modules" can be created and shared among Q1 Labs customers.

PresiNET – http://www.presinet.com/

Whereas tcpdump is like an x-ray for your network, Total View One is like an MRI. Total View One enables customers to maximize the use of infrastructure resources and network performance. Total View One sensors collect protocol state information by tracking connections through a network. This is commonly done out-of-line from traffic streams via port mirroring or network tap technologies. Currently PresiNET has implemented the NEDS specification which enables Total View One to receive messages from BIG-IP products to process them as if they'd come from a PresiNET sensor. This integration started with the NEDS iRule and specification and from this PresiNET created their own parser. PresiNET products are delivered as appliances in both a central unit and sensor unit mode. Optionally one may subscribe to PresiNET on a managed service basis. After you install a Total View One product in your network you get access to extensive views of available state information – with little or no additional work. If the included reporting capabilities aren't enough, you can export data from the system as a CSV file.

What's Next?

Now that you know who the players are and what they can do, be sure to check back next week to look at how the F5 products generate logs, how these technologies deal with them, and some testing results. To give you more of an idea of what's to come, I'll leave you with a look at the facts that will be delivered to the reporting systems from the F5 device(s) to see how they're handled:

Virtual server accessed, client IP address, client port, LB decision results, http host, http username, user-agent string, content encoding, requested URI, requested path, content type, content length, request time, server string, server port, status code, device identifier, referrer, host header, response time, VLAN id, IP protocol, IP type of service, connection end time, packets, bytes, anything sent to a dashboard, firewall messages, client source geography, extended application log data, health information for back end filers, audit logs, SNMP trap information, dedup efficacy, compression codec efficacy, wom error counters, link characteristics as known, system state

Logging and Reporting Toolkit Series: Part One | Part Three

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

F5 Networks, Inc.	F5 Networks	F5 Networks Ltd.	F5 Networks
Corporate Headquarters	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com