Q-Log®

The **Q-Log**® is an extremely small form factor, low-power-consumption server providing full log collection and automated visual analysis for all devices and services on a network. It works with all SNMP-available logs. The **Q-Log** uses the ELK Stack (Elasticsearch, Logstash, and Kibana) to aggregate and analyze logs, as well as provide alerts. Logstash aggregates and normalizes all log data, using over 160 different connectors and transformation tools. Elasticsearch provides near real-time search and analysis. Kibana is the visualization and navigation tool for log analysis.

This ultra compact design allows exceptionally flexible and creative deployment options as well as significant electricity and space savings.

- **Q-Log *Hardware Specifications*:**
- 108mm x 64mm x 26mm – 170 grams
  (4.25" x 2.50" x 1.125" – 6 oz)
- Power consumption under full load:
  8 watts, 120v-240v
- No fan or any moving parts. Must be installed in a well-ventilated space.
- Operates 0°C–70°C (32°F–158°F)

LED indicators:

- Power
- Link (physical connection to network)
- Activity (network traffic)
- 1000 mbps (gigabit) NIC connection
- Dual Band WiFi. (2.4 GHz & 5 GHz)

The **Q-Log** includes:

- **Logstash**® **– Logstash**® is the leading open source, enterprise-class, log aggregation and log data normalization tool. **Logstash** has more than 160 different log connectors and data transformation tools so that logs from all kinds of hardware and services can be aggregated for subsequent unified analysis.

- **Elasticsearch**® **– Elasticsearch**® is the leading open source, enterprise-class, RESTful search and analysis tool. **Elasticsearch** makes it possible to run inquiries against the logs normalized and aggregated by **Logstash**. It uses standard RESTful APIs as well as JSON. There are also clients in other languages such as Java available.

- **Kibana**® **– Kirbana**® is the leading open source, enterprise-class, log data visualization package, opening up log analysis to non-experts. **Kibana** provides graphical analysis, which opens up log analysis to non-experts in the field of log analysis. **Kibana** includes the ability to do geo-analysis of log data.

Contact: Richard Avery
646-449-7810
Q-Log@quantalytics.com

Quantalytics. In-depth network defenses.

- **ModSecurity® – ModSecurity®** (**ModSec**) is the leading open source Web Application Firewall (WAF) for cross-scripting attack protection. We have hardened the **Q-Log**'s built-in Apache web server to prevent conceivable attacks.

- **ClamAV® – ClamAv®** is the leading open source anti-virus software package.

- **Tiny Honeypot (THP) - THP** fools attackers by making it appear that the attack is working, while meanwhile logging the attack info. **THP** wastes an attacker's time, and creates an opportunity to detect the network intrusion by offering to the attacker what appears to be thousands of services.

- **Webmin – Webmin** is the leading open source Web GUI package for server configuration and maintenance. **Webmin** also allows for the linkage of multiple **Q-Log** appliances for simplified administration.

- **HA Proxy – HA Proxy** is the leading open source package for automatic failover and load balancing. Up to 32 **Q-Log** appliances may be linked for automatic failover or load balancing for coverage of extremely large networks. Administration is done through a Web GUI.

The **Q-Log** is completely administered through a Web GUI. This makes all features easily available even to novice network administrators. No Command Line Interface (CLI) or Linux skill is required.

The **Q-Log** has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.)

The **Q-Log** is also available as a Virtual Machine (VM).

Using the provided **Webmin** module, two-factor authentication can be added using **Google Authenticator** or **Authy**, a commercial service with its own app. **Google Authenticator** runs on Android, IOS, and Blackberry devices, and uses the standard TOTP protocol.

Notifications are provided by e-mail using **SendMail**, which is configured with a module in **Webmin**, and syslog entries. The **Q-Log** can be integrated with **Nagios®** in the **Q-Box®** as a notification route. SMS notification is available as an option. The **Q-Log** can also be integrated with any other Syslog or SIEM (Security Information and Event Management) solution.

Contact: Richard Avery
646-449-7810
Q-Log@quantalytics.com