Quantalytics

Q-Log®

Le **Q-Log**® est un serveur de faible consommation de faible consommation, offrant une collecte complète des journaux et une analyse visuelle automatisée pour tous les appareils et services sur un réseau. Il fonctionne avec tous les journaux disponibles sur SNMP. Le **Q-Log** utilise l'ELK Stack (**Elasticsearch**, **Logstash** et **Kibana**) pour agréger et analyser les journaux, ainsi que pour fournir des alertes. **Logstash** agrège et normalise toutes les données de journal, en utilisant plus de 160 connecteurs différents et des outils de transformation. **Elasticsearch** fournit des recherches et des analyses en temps quasi réel. **Kibana** est l'outil de visualisation et de navigation pour l'analyse du journal.

Ce design ultra compact permet des options de déploiement exceptionnellement flexibles et créatives, ainsi que d'importantes économies d'électricité et d'espace.

- **Q-Log *Spécifications matérielles*:**
- 108 mm x 64 mm x 26 mm – 170 grammes (4.25” x 2.50” x 1.125” – 6 oz)
- Consommation électrique à pleine charge: 8 watts, 120v-240v
- Pas de ventilateur ou de pièces mobiles. Doit être installé dans un espace bien ventilé.
- Fonctionne 0°C–70°C (32°F–158°F)

Indicateurs LED:

- Pouvoir électrique
- Lien (connexion physique au réseau)
- Activité (trafic réseau)
- 1000 mbps (gigabit) NIC connexion
- 100 (10/100 mbps connexion)

Le **Q-Log** comprend:

- **Logstash**® – **Logstash** est l'outil principal de gestion des classes, de la classe entreprise, de l'agrégation des journaux et de la normalisation des journaux. **Logstash** possède plus de 160 connecteurs de log et outils de transformation de données différents, de sorte que les enregistrements de tous types de matériel et de services peuvent être agrégés pour une analyse unifiée ultérieure.
- **Elasticsearch**® – **Elasticsearch** est l'outil de recherche et d'analyse open source open source, de classe entreprise, RESTful. **Elasticsearch** permet d'effectuer des recherches sur les journaux normalisés et agrégés par **Logstash**. Il utilise les API RESTful standard ainsi que JSON. Il existe également des clients dans d'autres langues telles que Java disponibles.
- **Kibana**® – **Kibana** est le premier programme de visualisation de données log, open-source, classe d'entreprise, ouvrant une analyse de journal à des experts non-experts. **Kibana** fournit une analyse graphique, qui ouvre une analyse de journal à des non-experts dans le domaine de l'analyse de journal. **Kibana** inclut la possibilité de faire une analyse géométrique des données du journal.
- **ModSecurity**® – **ModSecurity** (**ModSec**) est le premier paquet de protection contre les attaques croisées en code source open source afin de durcir le serveur web Apache intégré du **Q-Log** et d'éviter les attaques imaginables.

Contact: Richard Avery
+1 646-449-7810
Q-Log@quantalytics.com

Quantalytics. Défenses de réseau en profondeur.

- **ClamAV®** – **ClamAv** est le premier logiciel antivirus open source.
- **Tiny Honeypot (THP) - THP** trompe les attaquants en faisant apparaître que l'attaque fonctionne, tout en enregistrant les informations d'attaque. **THP** gaspille le temps d'un attaquant et crée l'opportunité de détecter l'intrusion du réseau en offrant à l'attaquant ce qui semble être des milliers de services.
- **Webmin** – **Webmin** est le paquet GUI Web open source leader pour la configuration et la maintenance du serveur. Webmin permet également la liaison de plusieurs appareils **Q-Log** pour une administration simplifiée.
- **HA Proxy** – **HA Proxy** est le premier fournisseur open source pour le basculement automatique et l'équilibrage de charge. Jusqu'à 32 appareils **Q-Log** peuvent être liés pour le basculement automatique ou l'équilibrage de charge pour la couverture de réseaux extrêmement grands. L'administration se fait via une interface graphique Web.

Le **Q-Log** est complètement administré via une interface graphique Web. Cela rend toutes les fonctionnalités facilement accessibles même pour les administrateurs réseau novateurs. Aucune interface de ligne de commande (CLI) ou Linux n'est requise.

Le **Q-Log** possède à la fois un NIC Gigabit (1000 mbps) et un WiFi Dual Band 802.11. (2.4 GHz et 5 GHz.)

Le **Q-Log** est également disponible en tant que Machine Virtuelle («VM»).

Le **Q-Log** est entièrement administré via une interface graphique Web. L'utilisation de tous les packages se fait via des interfaces Web. Aucune interface de ligne de commande (CLI) ou Linux n'est requise.

En utilisant le module **Webmin** fourni, l'authentification à deux facteurs peut être ajoutée à l'aide de **Google Authenticator** ou **Authy**, un service commercial avec sa propre application. **Google Authenticator** s'exécute sur les appareils Android, IOS et Blackberry, et utilise le protocole standard de TOTP.

Les notifications sont fournies par e-mail à l'aide de **SendMail**, qui est configuré avec un module dans **Webmin** et les entrées syslog. Le **Q-Log** peut être intégré avec **Nagios®** dans le **Q-Box®** comme voie de notification. La notification par SMS est disponible en option. Le **Q-Log** peut également être intégré à toute autre solution Syslog ou SIEM.

Contact: Richard Avery
+1 646-449-7810
Q-Log@quantalytics.com