Qe-Log & Qe-LogRT

Qe-Machine de traitement de logs

Qe-Log est un module logiciel intégré à la solution Qualevent et dédié au traitement des logs. Il se présente sous la forme d'une ou plusieurs Qe-machines qui enrichissent l'hypervision grâce aux informations qu'elles produisent en analysant des logs. Deux versions sont disponibles ; Qe-Log pour le traitement des fichiers log d'état, et Qe-LogRT pour le traitement au fil de l'eau de flux de messages notamment en *syslog*. Les informations produites peuvent être croisées avec celles générées par d'autres Qe-machines d'une plateforme Qualevent. Qe-Log apporte aux équipes d'exploitation ou chargées du suivi des évènements une solution immédiatement opérationnelle alliant performance, capacité fonctionnelle et souplesse d'utilisation.

Fonctions essentielles

- Hypervision de l'état du SI par l'analyse des données de logs
- Collecte et traitement de logs d'état ou de flux de messages
- Présentation graphique du statut des objets du SI
- Extraction et valorisation de données
- Corrélation topologique
- Corrélation entre les données collectées
- Recherche multi-critères dans les logs
- Alarmes sur changement d'état des objets
- Présentation d'indicateurs techniques ou métier
- Stockage sur longue période
- Intégration immédiate à Qualevent

Analyse syntaxique et corrélation d'évènements

Qe-Log procède à la collecte de données de logs et à leur prétraitement puis les stocke suivant des paramètres de conservation configurables. Le prétraitement comprend des analyses syntaxiques en temps réel pour valoriser les données en produisant des indicateurs. Un premier niveau de corrélation de type topologique est réalisé sur les données collectées par Qe-Log, en croisement avec la modélisation présente dans la CMDB de Qualevent.

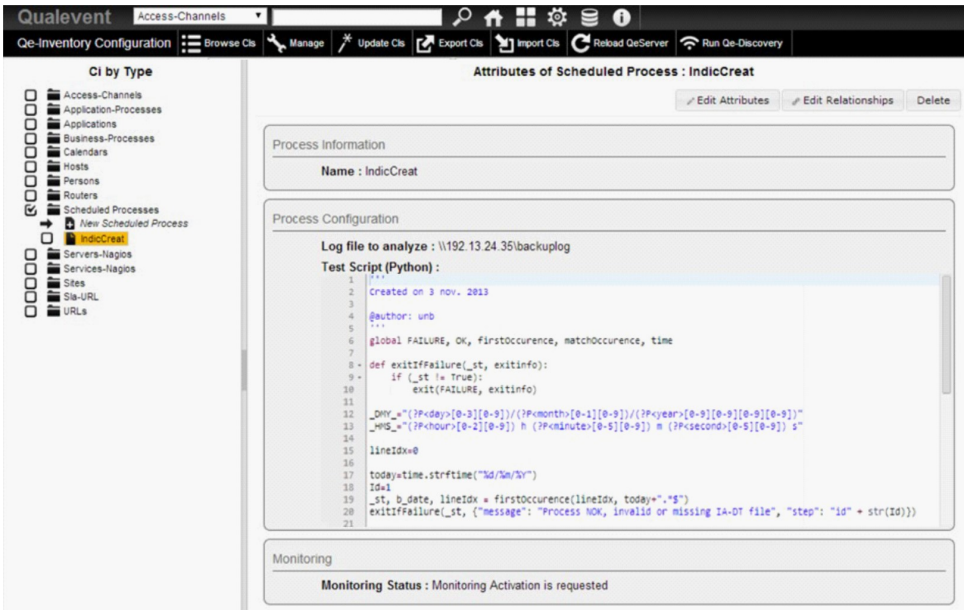

Illustration 1 : création d'un indicateur par recherche syntaxique dans des logs

Si des évènements anormaux sont identifiés lors du prétraitement des logs, Qe-Log gère la mise à jour de l'état des objets impactés. Des Qe-messages sont envoyés au dispositif central de Qualevent Qe-Server, qui procède à la présentation d'alarmes et à un second niveau de corrélation avec les données provenant d'autres Qe-machines. Qe-Log permet de corréler l'information émanant de l'infrastructure sous forme de logs avec d'autres informations produites par Qualevent telles que la performance et la disponibilité applicative, et de produire les évènements de haut niveau, les indicateurs et les statistiques qui en découlent. En procédant de la sorte on adresse tant les besoins d'information liés à l'exploitation que ceux relatifs à la connaissance de la disponibilité globale du SI et des applications.

De l'analyse des logs à l'hypervision

Qe-Log permet donc de travailler sur deux niveaux de corrélation, le premier s'attachant à détecter les anomalies directement à partir des flux ou des fichiers de logs, et le second croisant les informations précédentes avec des données produites par d'autres Qe-machines. Cette approche autorise la corrélation des informations d'origines et de natures différentes. Elle met notamment en relation le domaine des logs avec celui de la mesure de performance ou encore celui de la supervision technique en temps réel pour une hypervision plus complète de l'ensemble des éléments du SI : analyse de temps de réponse, alarmes diverses indiquant des changements d'état de composants applicatifs système ou réseau, ou encore alarmes sur des codes erreur anormaux par exemple. Qe-Log permet de passer de l'analyse isolée de données de logs à l'hypervision du système d'information. Le post-traitement peut s'accompagner de la réalisation de statistiques suivant les différents éléments définis au niveau de l'inventaire du SI renseigné au niveau de Qe-Inventory.

Qe-Log et les métiers de la DSI

Qe-Log est une des briques de Qualevent permettant de consolider et valoriser les informations du système d'information et de bâtir une hypervision efficace. Les différents modes de présentation des résultats de Qualevent, graphiques temps réel, listes d'évènements, rapports, sont disponibles pour les informations produites par Qe-Log et s'adaptent aux métiers de la DSI. Les équipes d'exploitation en charge du diagnostic et de la gestion des incidents disposeront à la fois de la finesse d'analyse nécessaire à la compréhension des problèmes entre les différents environnements techniques, et de la simplicité d'utilisation garante d'efficacité. Pour les directions souhaitant disposer d'une vision simplifiée de tout ou partie de l'état du système d'information, des vues de synthèse sont disponibles à la demande.

Qe-Machines dans le modèle Qualevent et fonctionnement *stand-alone*

Suivant les besoins, les Qe-machines Qe-Log sont déployées en central dans un datacenter avec le module principal de Qualevent (Qe-Server), ou réparties de manière distante sur des environnements virtuels. Elles sont présentées ci-dessous dans l'architecture Qualevent.

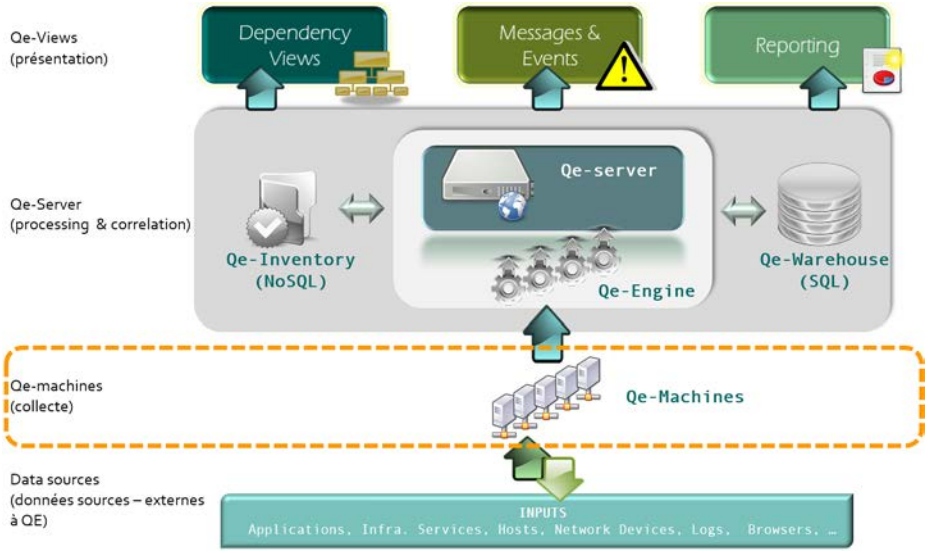

Illustration 2 : Qe-Machines dans l'architecture Qualevent

En fonctionnement *stand-alone*, elles sont embarquées sur tout environnement virtuel (VMWare, KVM ou autre) pour offrir des fonctionnalités d'analyse ou d'alerte gérées de manière centralisée au niveau de Qe-Server.

allentis
140bis, rue de Rennes
75006 Paris—France

Société par Actions Simplifiée au capital de 50.000 euros
RCS Paris B 533 336 848
Siret 533 336 848 000 15
NAF 5829C
TVA FR 18 533 336 848

Tél. : 01 70 38 25 45
Fax. : 01 70 38 23 00
info@allentis.eu
www.allentis.eu

allentis développe et commercialise des solutions et des services permettant l'hypervision des services IT, des processus, des applications et des infrastructures qui les sous-tendent.