

Qe-Packets

Capture massive des paquets échangés sur les réseaux

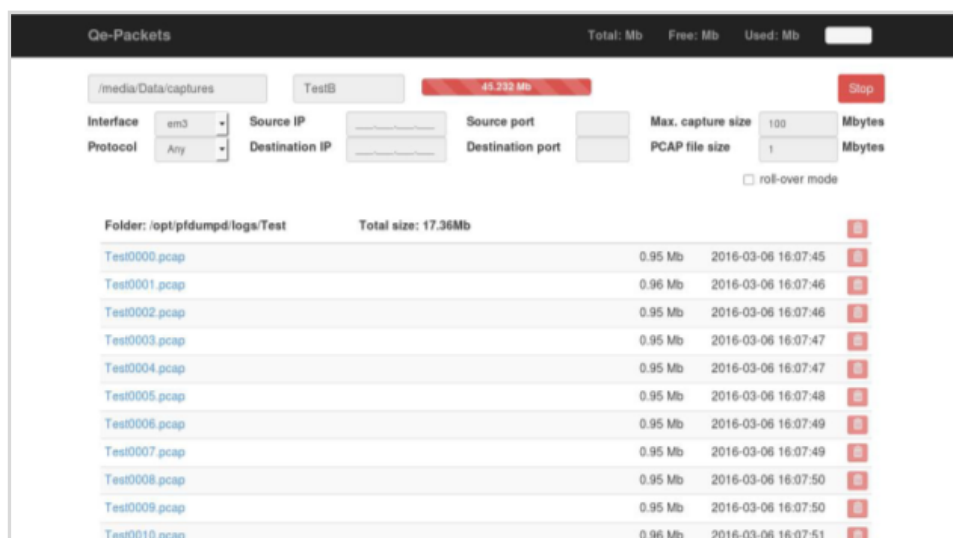
Fonctions essentielles

- Qe-Machine autonome sous forme d'appliance
- Stockage massif jusqu'à 40 To
- Construction de fichiers .pcap « à la volée »
- Corrélation des alertes avec les autres Qe-machines de la gamme
- Scripting à la demande pour prise en compte de problématiques spécifiques
- Indexation optionnelle du stockage en liaison avec Qualevent

Qe-Packets est un des modules de la solution Qualevent. C'est une appliance d'acquisition de flux et de tous les paquets échangés sur les liens sur lesquels elle est positionnée jusqu'à un débit de 20 Gbps (10 Gbps full duplex). Elle garantit une durée de rétention élevée par un stockage de 10, 20 ou 40 To en mode linéaire ou circulaire.

Solution autonome

Qe-Packets copie et stocke l'intégralité du trafic échangé sur les liens en surveillance. L'utilisateur décide du volume global de rétention des données. L'espace de stockage est configuré de manière circulaire ou linéaire afin de garantir une durée de rétention conforme aux contraintes de la production. Pour faciliter la relecture et l'accès aux données, le paramétrage de la taille des fichiers pcap est paramétrable. Par exemple, pour un stockage global de 1 To de données en mode circulaire, il peut être demandé la constitution de 1.000 fichiers de 1 Go. Cette approche garantit une extraction rapide des données. Des fonctions de filtrage sont disponibles afin de ne retenir que les données qui apparaissent les plus pertinentes. Les données produites peuvent être lues avec tous les produits du marché permettant la lecture de captures pcap.



Qe-Packets		Total: Mb	Free: Mb	Used: Mb
/media/Data/captures TestB 45.233 Mb [Stop]				
Interface	em3	Source IP	Source port	Max. capture size 100 Mbytes
Protocol	Any	Destination IP	Destination port	PCAP file size 1 Mbytes
☐ roll-over mode				
Folder: /opt/pfddump/logs/Test		Total size: 17.36Mb		
Test0000.pcap	0.95 Mb	2016-03-06 16:07:45		
Test0001.pcap	0.96 Mb	2016-03-06 16:07:46		
Test0002.pcap	0.95 Mb	2016-03-06 16:07:46		
Test0003.pcap	0.95 Mb	2016-03-06 16:07:47		
Test0004.pcap	0.95 Mb	2016-03-06 16:07:47		
Test0005.pcap	0.95 Mb	2016-03-06 16:07:48		
Test0006.pcap	0.95 Mb	2016-03-06 16:07:49		
Test0007.pcap	0.95 Mb	2016-03-06 16:07:49		
Test0008.pcap	0.95 Mb	2016-03-06 16:07:50		
Test0009.pcap	0.95 Mb	2016-03-06 16:07:50		
Test0010.pcap	0.96 Mb	2016-03-06 16:07:51		

stockage de l'intégralité du trafic par Qe-Packets

Qe-machine à part entière

Dans le modèle de supervision Qualevent, les Qe-machines sont destinées à collecter les informations susceptibles de qualifier l'état des services aux métiers. Dans certains cas c'est dans les paquets eux-mêmes qu'il peut être nécessaire d'aller



identifier une information indisponible par ailleurs. Pour répondre à ce besoin la Qe-machine Qe-Packets peut fonctionner en mode autonome ou en liaison avec Qualevent. Positionnée en des points de concentration stratégiques, l'appliance autorise l'analyse de champs spécifiques lorsqu'elle est intégrée à la solution globale Qualevent. Ce fonctionnement permet de rendre compte de l'état d'un élément qu'il n'a pas été possible de qualifier par ailleurs. Cet état ainsi remonté par Qe-Packets au Qe-Server central va de cette manière permettre de fournir l'information manquante pour qualifier l'état des services métier dans le modèle de corrélation défini. De plus, toujours dans le cas de l'implémentation de Qe-Packets avec l'ensemble de Qualevent et afin de garantir un accès rapide à l'information, les données peuvent être indexées. Cette indexation est alors paramétrée à la demande sur un ensemble défini de champs disponibles au niveau des trames capturées. Ces informations deviennent alors accessibles en extraction rapide afin de répondre à des problématiques d'analyse allant au-delà de ce qui a été prévu au départ. Dans ce cas de figure, Qe-Packets peut être utilisé à des fins d'investigation ou de reporting statistique.

Qe-Packets dans le modèle Qualevent

Si Qe-Packets répond à des problématiques de capture massive, la solution participe à l'objectif global de Qualevent dans l'hypervision de performance des applications métier du système d'information. Les indicateurs fournis peuvent donc être corrélés avec l'ensemble des informations traitées par les différentes Qe-machines de la gamme. En liaison avec Qe-Inventory, ces indicateurs analysés et interprétés par Qe-Packets sont intégrés au modèle de dépendances défini pour comprendre l'état global de fonctionnement des applications en fonction des éléments qui participent à les délivrer. Ainsi, des événements identifiés dans les trames elles-mêmes peuvent être intégrés pour comprendre l'état de services délivrés par la direction des systèmes d'information. La *météo* de l'état des applications aux métiers n'en est que plus réaliste.

Adaptations pour besoins spécifiques

Comme l'ensemble des Qe-machines de la gamme, Qe-Packets peut faire l'objet d'adaptations pour répondre à des besoins spécifiques dans l'analyse « à la volée » des données échangées sur les réseaux. La méthode agile retenue par les équipes de développement de allentis permet de répondre rapidement sur la faisabilité de prise en compte des demandes. Le cas échéant, ces évolutions sont réalisées rapidement pour délivrer des *packages* de mises à jour spécifiques. Dans tous les cas, ces évolutions sont supportées dans le cadre des contrats de support et de maintenance standard. Cette approche représente une garantie supplémentaire pour les clients dans le cycle de vie de leurs projets.

Déploiement en environnement virtuel ou sous forme d'appliances

Comme toutes les Qe-machines, Qe-Packets peut être livrée sous forme d'une OVA à installer sur un environnement virtuel (VMWare ou KVM). Toutefois Dans des environnements où sont attendues des systèmes de type *all in box*, et surtout quand il s'agit de capturer du trafic sur des liens à hauts débits, allentis propose une gamme de matériels adaptés pour livrer ses solutions sous forme d'appliances embarquant les modules nécessaires. Dans les deux cas, les services de maintenance et support proposés garantissent à tous les clients le maintien en conditions opérationnelles de ces solutions tout en délivrant les évolutions mineures et majeures mises à disposition dans les nouvelles versions.

allentis

140bis, rue de Rennes
75006 Paris—France

Société par Actions Simplifiée
au capital de 80.150 euros
RCS Paris B 533 336 848
Siret 533 336 848 000 15
NAF 5829C
TVA FR18 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 allentis, Qualevent, le logo allentis et tous les noms des produits allentis sont des marques déposées. Ce document est fourni uniquement à titre d'information et ne constitue en aucun cas un engagement contractuel de la part de allentis, de ses partenaires ou de ses soustraitants. Notamment les spécifications techniques contenues présentées sont susceptibles d'être modifiées à tout moment sans préavis. Les photographies présentées peuvent montrer des maquettes. Les équipes commerciales de allentis sont accessibles à info@allentis.eu afin de répondre à toute demande de renseignement sur les données contenues dans la présente publication.