Extra, logiciel d'analyse du trafic réseau

Bernard Boutherin
Jérôme Fulachier
Jean Mirasolo
IN2P3 – LPSC Grenoble

Denis Pugnère
IN2P3 – IPNL Lyon

Laurent Caillat
IN2P3 – Centre de Calcul Lyon

Mots clefs

Trafic réseau, flux, traces, analyse, métrologie, surveillance, sécurité, top-ten

Résumé

Extra est un logiciel développé à l'IN2P3 pour la surveillance du trafic en entrée d'un site. Il offre une solution de métrologie adaptée à un réseau de laboratoire et permet la détection et le traçage d'évènements réseau en vue d'une analyse à des fins de sécurité. Extra est composé de plusieurs modules permettant : le recueil des flux en entrée de site, le stockage de ces flux dans une base de donnée, des prétraitements systématiques sur les flux, la mise à jour d'une interface Web graphique d'analyse.

La volumétrie réseau au cours du temps est visualisée sous forme de graphiques en histogramme empilé représentant des Top ten. (*Top ten* du trafic par machines internes ou externes, par services internes ou externes etc.).

Entièrement développé en Java, Extra met en œuvre un collecteur de flux, une base de donnée *mySQL*, un serveur de prétraitements, un serveur *Tomcat* pour l'interface web d'analyse. Il permet, à partir d'un navigateur web, de surveiller le trafic réseau au niveau des adresses IP, des ports, des protocoles et des volumes.

Extra est en cours de déploiement à l'IN2P3. Pour cela une distribution autonome sur Cdrom a été réalisée intégrant Linux, MySQL, Tomcat et Extra. De plus des outils ont été développés pour effectuer des requêtes systématiques ou à la demande sur l'ensemble des sites de l'IN2P3. Ces outils permettent le déclenchement d'alerte via des scripts et l'archivage centralisé des traces.

Il existe dans le domaine public un certain nombre de logiciels permettant la métrologie réseau tels que mrtg (rrdtool) et netmet. Extra se veut moins généraliste que ces logiciels et est adapté à la surveillance du trafic réseau en entrée d'un site simple. Extra apporte une interface graphique plus évoluée et interactive, ainsi que des fonctions d'archivage et d'analyse de haut niveau.