openSUSE Conference : surveiller ses serveurs Linux avec SystemTap

L'intégration des SUSE Labs dans l'openSUSE Conference 2011 de Nuremberg permet de disposer de présentations d'un très haut niveau technique, comme celle portant sur SystemTap. Cette dernière se propose de répondre à une question cruciale pour les développeurs et les administrateurs système : que se passe-t-il à l'intérieur du noyau Linux de mon serveur ?

Cette session a été réalisée par **Daniel Gollub** (notre photo), assisté de **Stefan Seyfried** (qui a animé cette autre présentation). Tous deux travaillent chez B1 Systems GmbH, un des partenaires de cet événement.

SystemTap : de la surveillance et bien plus encore

SystemTap est à ce jour uniquement dédié au noyau Linux. Il permet d'insérer des dérivations pointant vers votre code, à n'importe quel endroit du *kernel* (et de ses modules). Ainsi, lorsqu'une fonction sera utilisée, le système appellera à un script SystemTap développé par vos soins.

Premier exemple d'utilisation : quand une demande d'accès au système de fichiers est effectuée, il est possible d'afficher le nom du processus qui est à l'origine de cette demande. Un script qui ne nécessite que quelques courtes lignes de code. Plus complexe, lorsqu'une application souhaite créer un fichier au nom indésirable sur votre disque, il est possible de court-circuiter l'appel au noyau et de renvoyer une fin de non-recevoir. SystemTap permet donc d'aller au-delà de la simple surveillance, ses possibilités étant très étendues. Un outil de bidouilleurs par excellence.

Un langage de script peu gourmand en ressources

Votre code se présente sous la forme de scripts utilisant un langage de programmation proche du C. De très nombreux exemples sont d'ores et déjà disponibles. Au besoin, ils pourront être aisément adaptés à vos besoins. Cette technologie sera donc parfaitement à la portée des administrateurs système ne disposant pas de connaissances avancées en programmation.

Simple, le langage de script utilisé ici se veut très optimisé et peu gourmand en ressources. SystemTap dispose également de mécanismes lui permettant d'éviter qu'un script ne s'accapare tout le temps processeur. S'il est trop lent, son exécution sera ainsi arrêtée. Pratique, mais potentiellement ennuyeux. Dans ces conditions, rien ne vous garantit en effet que vos scripts seront bien lancés lorsqu'une sonde sera placée au cœur du noyau.

Ce problème, nous avons pu le constater de visu lors de la démonstration de Daniel Gollub : une sonde posée à un endroit un peu trop passager du noyau Linux menait invariablement à la non-exécution du script associé, sans signes avant-coureurs. L'adage *« trop d'information tue l'information »* n'a jamais été aussi vrai ! Il faudra donc vous montrer à la fois imaginatif et astucieux pour profiter au mieux de cette technologie.