heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud
http://www.heig-vd.ch

Travail de diplôme 2006

HEIG-VD
Route de Cheseaux 1
CH - 1401 Yverdon-les-Bains

Consolidation de logs chez Unicible

Les logs : pourquoi faire ?

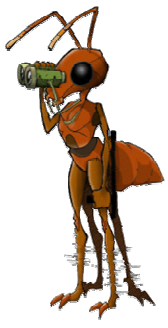
Les systèmes d'informatiques sont devenus un outil indispensable pour toutes organisations commerciales et administratives. La majorité, si ce n'est la totalité de leurs données, sont stockées sur des ordinateurs. La sécurité informatique est donc devenue un élément très important pour les entreprises.

D'un point de vue technique, l'analyse des logs permet de détecter toutes les défaillances d'un système. En les centralisant, puis de corrélant il est possible de détecter plus de défaillances.

D'un point de vue juridique, il permet de prouver l'intégrité de certaines données sensibles. Certaines lois, comme par exemple Sarbanes-Oxley (Etats-Unis), ou Bâle II (Europe), insistent sur la traçabilité des informations financière. Il faut pouvoir montrer qui a pu modifier ces informations. Ces dernières lois ont été l'un des principale moteur des gestions des logs ces dernières années.

But du travail

Le but de ce travail est de tester un centraliseur de logs, pour son utilisation dans un environnement complexe. Le centraliseur de logs choisi a été Prelude ses deux versions (OpenSource et commerciale) ont été testées et comparées.



Logo de Prelude

Le travail effectué

Les étapes suivantes ont été réalisées:

1. Compréhension du fonctionnement de Prelude, plus réalisation d'une architecture de tests, en développant quelques outils adéquats.
2. Réalisation des tests sur Prelude.
3. Analyse des résultats et proposition de différentes architectures possibles.

Le travail a donc été principalement la création d'un petit laboratoire pour pouvoir tester l'utilisation de Prelude.

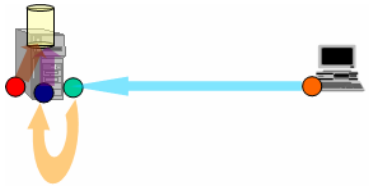
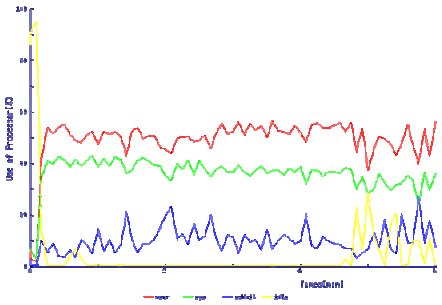


Schéma d'une mesure

Remarque : Les différents outils de tests ont été écrits en Perl.



Exemple de résultat

Conclusion

Une étude sur l'utilisation de Prelude a été menée. Il aurait été intéressant de pouvoir le comparer avec d'autres outils du marcher, dans des conditions similaire pour pouvoir avoir un avis plus complet sur son utilisation dans un environnement complexe.

Auteur: **Teboulbi Kerim**
Répondant externe: **M. Thierry Agassis**
Prof. responsable: **M. Stéphano Ventura**
Sujet proposé par: **Mme Minh Ricoz de Unicible**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale