



L'équipe data communications:  
De g. à dr.: Laurent Patrigot,  
Pascal Brunat et François Bajas

## Gestion, corrélation et stockage des fichiers logs

*Toutes les entreprises qui cherchent une méthode rationnelle pour gérer et stocker leurs fichiers logs connaissent les mêmes problèmes: comment extraire valablement des informations à partir de dizaines de milliers de lignes de logs provenant de plusieurs sources différentes et en tirer les conclusions adéquates? Comment agréger et consolider les logs? Eviter la redondance des alertes? Etre informé clairement du niveau d'importance des alertes signalées? Disposer simplement d'une solution sur mesure, adaptable même à des applications ou des configurations internes particulières?*

Une société est confrontée à ce problème: l'Union Européenne de Radio-Télévision (UER). Fondée en 1950 par les pionniers de la radio et de la télévision, elle est la plus importante association professionnelle de radiodiffuseurs nationaux dans le monde et possède une position privilégiée en Europe. Depuis son siège de Genève, elle agit pour le compte de ses membres, négocie les droits de diffusion des grands événements sportifs et exploite les réseaux Eurovision et Euroradio.

Pascal Brunat est Head of Data Communications de l'UER, un département de trois personnes qu'il dirige depuis sa création en 1993. Laurent Patrigot est Ingénieur en transmission de données. Leur mission est d'assurer la bonne marche de la plate-forme de communication du siège et des cinq sites distants, ainsi que sa sécurité.

---

*"Comme nous ne sommes que trois, nous avons su dès le départ qu'un outil nous serait indispensable pour contrôler les logs."*

---

Pascal Brunat explique: " Nous assurons un service 24h/24 et sept jours sur sept. Nos installations comprennent deux accès internet à 50Mb/s et plusieurs serveurs web ainsi que les serveurs mail. Nos deux salles informatiques possèdent des infrastructures redondantes, deux niveaux de firewalls, et chacun des deux bâtiments de Genève est autonome. La plupart des informations que nous véhiculons sont publiques. Ce que nous voulons surtout éviter, c'est la corruption ou la manipulation des informations, qui pourraient avoir des conséquences catastrophiques."

Il était clair depuis le départ pour les intéressés qu'ils avaient besoin d'un

outil pour gérer et contrôler les fichiers logs. Leur problème: un premier produit installé à cet effet il y a quelques années ne s'est pas révélé entièrement satisfaisant à l'usage.

---

*"Le risque que nous prenions en choisissant cette nouvelle solution était calculé et mesuré, car nous connaissons les gens de Navixia et leur compétence depuis de nombreuses années."*

---

Pascal Brunat: "Pour le remplacer, Navixia nous a proposé un produit français plus convivial, ExaProtect. Le risque que nous prenions en choisissant cette nouvelle solution était limité, car nous connaissons les gens de Navixia et leur compétence depuis de nombreuses années."

Laurent Patrigot décrit l'architecture de cette solution: "Douze éléments sont connectés au corrélateur: les firewalls, les sondes de prévention et de détection d'intrusions, les serveur FTP, les serveurs web ainsi que les serveur mail. Ces éléments génèrent des millions de lignes de logs; il est clair qu'une machine analysera une telle quantité d'informations plus efficacement qu'un humain. Le système de corrélation nécessite deux serveurs. Le premier serveur récolte et récupère les lignes de logs directement depuis les systèmes connectés. Un agent donne à tous les logs un format identique, puis les envoie au corrélateur situé sur le deuxième serveur. C'est là que se fait leur agrégation et l'application des règles. L'outil rassemble les informations principales sur une console d'administration où elles sont condensées et présentées de manière conviviale. En cas d'attaque, une ligne de texte mise en évidence dans l'interface du corrélateur montre le cheminement des agresseurs. En cliquant sur ce texte, on peut remonter à tous les logs des différents systèmes. Pour notre petite équipe, l'administration est ainsi considérablement facilitée."

Une telle implantation demande un travail de préparation préalable. Laurent Patrigot: "Il faut définir quels sont les éléments qui envoient les logs, et quelles sont les règles d'analyse et de synthèse. Comme la gestion des serveurs web ne dépend pas de nous, nous recevons simplement les fichiers logs. Nos collègues nous aident à définir les règles appropriées à leurs besoins. Aujourd'hui, notre installation commence à être bien exploitable, sous réserve de quelques mises au point. Nous bénéficions d'un très bon support de Navixia. Nous disposons maintenant d'une belle architecture et d'un bon produit, qui demande juste encore quelques réglages."

ExaProtect reconnaît de nombreux formats d'équipement, mais des développements particuliers sur mesure sont toujours envisageables avec une grande souplesse. Pascal Brunat: "Nos nouvelles passerelles SMTP (CipherTrust/IronMail) génèrent des logs dans un format quasi propriétaire. Nous avons donc demandé à ExaProtect de développer un agent nous permettant d'exploiter ces logs, ce qui a été fait rapidement. Lorsque des e-mails sont expédiés à des centaines de destinataires, nous pouvons désormais savoir facilement à qui le message n'est pas parvenu."

Pascal Brunat a pu constater d'autres avantages à l'usage du corrélateur de logs ExaProtect: "Il nous permet d'être bien plus proactifs dans le domaine de la sécurité. Notre système de scan de vulnérabilités analyse régulièrement le réseau; son rapport est envoyé au corrélateur, qui nous informe en cas d'incident et nous permet de réagir immédiatement."



Salle de contrôle EVC en charge de la gestion du réseau Eurovision

---

*"En cas d'attaque, une ligne de texte mise en évidence dans l'interface du corrélateur montre le cheminement des agresseurs."*

---

Pascal Brunat et Laurent Patrigot sont donc satisfaits: la solution d'ExaProtect mise en place par Navixia leur permet d'avoir une démarche plus proactive et leur simplifie l'administration des éléments de sécurité. "Le projet a été opérationnel très rapidement. Nous avons tout de suite senti la convivialité du produit et avons déjà pu aller plus loin qu'avec la solution précédente." Cette architecture évolutive permet aussi de centraliser le monitoring des fonctions techniques et des services

---

*"Nous disposons maintenant d'une belle architecture et d'un bon produit, qui demande juste encore quelques réglages."*

---

De manière plus générale, une bonne gestion des logs répond à une vraie problématique d'entreprise. Un tel système peut représenter une solution intéressante pour toute société qui croule sous des logs disparates et souhaiterait exploiter efficacement et simplement ces informations importantes. Il s'adresse aussi à toutes celles qui cherchent à gérer et stocker ces informations sur la durée pour se mettre en conformité avec les contraintes légales et/ou imposées par des réglementations telles que Sarbanes-Oxley ou Bâle II.

**Navixia SA**

Route du Bois 1  
CH - 1024 Ecublens

**Tél.:**  
41 (0)21 324 32 00

**Fax:**  
41 (0)21 324 32 01

**E-mail:**  
info@navixia.com

**Web:**  
www.navixia.com