

Supervision sécurité et performances : une convergence nécessaire

Par Gilles LEHMANN

La supervision est un chaînon indispensable pour assurer la sûreté et la continuité de fonctionnement des systèmes d'information et de communication. Quelles que soient la robustesse du système, l'excellence de sa conception ou la compétence des équipes d'exploitation, un jour ou l'autre l'administration se complique. La supervision permet d'anticiper et de gérer les problèmes. Historiquement, ce sont les performances qui sont supervisées et ces techniques de supervision sont désormais matures. Aujourd'hui un nouvel enjeu apparaît, la gestion de la sécurité. Pour assurer son fonctionnement, il ne suffit plus de surveiller le système mais aussi de le protéger contre des attaques éventuelles... Les sujets de performances et de sécurité sont cependant traités par des intervenants différents au sein des équipes d'exploitation, et le premier réflexe est de construire deux systèmes distincts pour accomplir ces deux tâches de surveillance. A travers cet article, nous souhaitons démontrer que la distinction n'est pas aussi évidente et qu'il faut dès à présent réfléchir aux interactions et convergences entre les deux « mondes ».

Nous présenterons d'abord une introduction sur l'administration et la supervision de performances suivie d'une rapide présentation sur l'administration et la supervision de sécurité puis nous mettrons en évidence les rapprochements possibles entre ces deux métiers. En conclusion, nous présenterons une solution open-source pour construire une architecture globale.

L'administration et la supervision de performances

La supervision de performances permet de connaître à tout instant l'état du système d'information en termes de performances et précisément si chaque composant du système fonctionne correctement ou non. Pour cela, des indicateurs de performance sont relevés périodiquement et comparés à des seuils fixés au préalable. Si un seuil est dépassé, le système déclenche une alerte (un événement).

Les fonctions de la supervision de performances sont:

- La supervision des états : elle constitue le fondement de la supervision. Il s'agit

grâce à un ensemble de collecteurs (et parfois de sondes déployées sur les équipements) de remonter en un point central l'ensemble des événements sur le réseau. On peut représenter ces événements de plusieurs façons mais les plus classiques sont le « bac à événements » (un tableau dans lequel s'affiche tous les événements avec une identification de leur gravité) ou une cartographie (une représentation « visuelle » du parc géographique, fonctionnelle ou logique dans lequel l'exploitant peut naviguer). C'est l'outil principal des exploitants de premier niveau.

- La métrologie : elle consiste à étudier dans le temps l'évolution des valeurs des indicateurs remontée par la supervision. C'est un complément d'information en particulier pour la recherche de la cause fondamentale d'un événement. La métrologie est un des outils des exploitants de second niveau.
- Le reporting : il génère des synthèses périodiques sous forme de graphiques et de tableaux et permet de fournir à la direction ainsi qu'aux utilisateurs finaux et aux clients une vision de la qualité de service rendu par le système d'informa-

tion et son infrastructure. C'est l'outil de mesure des engagements.

L'administration et la supervision de sécurité

En résumé, ce métier plus récent permet de connaître à tout moment l'état du système d'information en termes de sécurité.

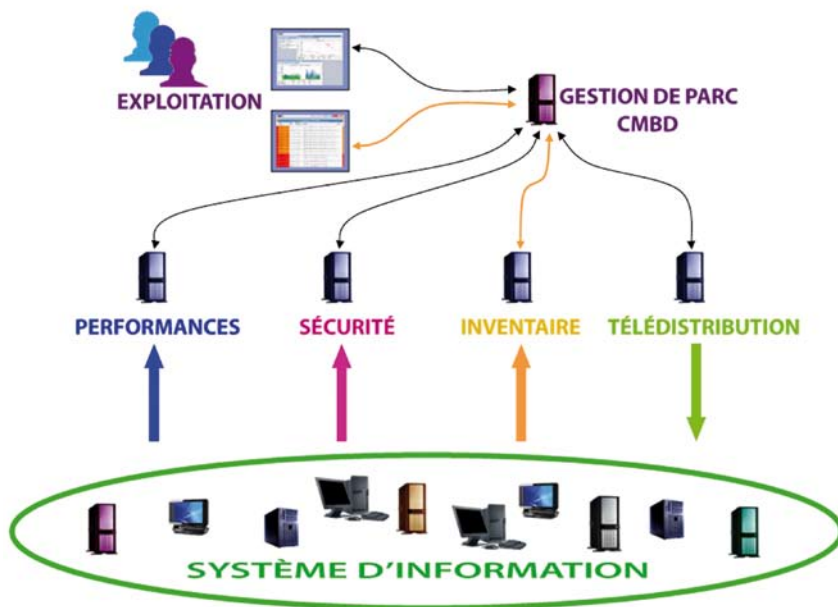
Cette définition, certes un peu simpliste, met en évidence les similitudes entre la supervision de performances et la supervision de sécurité. Les objectifs et les effets sont identiques mais les causes différentes. Par exemple, un serveur peut tomber en panne pour des raisons distinctes, liées soit à une défaillance matérielle (identifiable grâce à la supervision de performances) soit à une attaque réseau (identifiable grâce à la supervision de sécurité).

Problématiques communes

Analysons maintenant les problématiques communes à ces deux mondes :

• Les sondes

La supervision de performances s'effectue généralement via SNMP sans « agents



locaux ». Néanmoins, il est parfois nécessaire d'installer une sonde sur les serveurs pour analyser des fichiers de logs par exemple ou lancer une commande. C'est aussi le cas des sondes de sécurité qui analysent les logs à la recherche d'expressions type. On peut ainsi, dans certains cas, installer deux sondes sur le même serveur dont une partie de l'activité est commune. Au-delà des problèmes d'administration (déploiement, mise à jours, etc.) et de consommation de ressources, il arrive que ces deux sondes ne puissent fonctionner simultanément leurs ressources étant identiques. Il est donc important dans une architecture commune de partager éventuellement ces sondes qui remonteront aux deux systèmes les informations nécessaires.

• La corrélation

En terme de corrélation on peut donner comme exemple la corrélation topologique qui consiste à corréler les événements avec la topologie du réseau. Par exemple, si un serveur est derrière un routeur « en panne », il est inutile de traiter les événements signalant que ce serveur est non joignable tant que le routeur n'est pas rétabli. Cette remarque est valable que l'on se place du point de vue des performances comme de la sécurité. Il est donc intéressant de partager ces informations de topologie et de ne les saisir qu'en un seul point. La corrélation des événements est

aussi nécessaire. Un serveur « tombé » à cause d'un disque défaillant (performances) peut provoquer des alarmes de sécurité car il n'est plus joignable. De la même façon si le serveur est attaqué par un DOS (Denial Of Service, problématique de sécurité) cela peut générer une alerte de performance sur sa consommation CPU. Dans les deux cas il est important que les événements de chaque système soient corrélés afin d'éviter des analyses inutiles de chaque côté à la recherche d'une cause qui est déjà connue.

• Gestion de parc et inventaire :

La première donnée nécessaire à la supervision est la connaissance aussi fine que possible du parc : quels sont les équipements, les serveurs, les logiciels, leurs versions, etc.

Ces informations ainsi que leurs évolutions sont nécessaires pour toute supervision. La fonction inventaire va permettre de suivre cette évolution. Il est important que la base inventaire soit partagée entre les différents mondes et qu'elle ne soit pas gérée en deux points distincts.

• Les processus

Un effort important est conduit actuellement pour améliorer les processus d'administration et de supervision « standard ». Des méthodes comme la méthode ITIL en particulier visent à modéliser l'ensemble des processus et à apporter une

meilleure cohérence. On y trouve la notion de gestion d'événements, de gestion d'incidents, la notion de CMDB (Configuration Management Data Base), etc. La gestion de la sécurité est en plusieurs points similaire à la gestion « standard », notamment les notions d'événement (alerte), d'incident (cause connue), de problème (cause inconnue). La gestion des interventions et de leurs documentations est similaire. La notion même de CMDB est aussi utile tant pour les informations d'inventaires que pour celles de services. Là encore la convergence est nécessaire.

• La télé-administration et le télé-déploiement

L'administration « standard » d'un grand parc nécessite de disposer d'un outil d'automatisation de nombreuses tâches : déploiement d'un logiciel, relance d'un service, changement d'une configuration, etc. Ce type d'outil est indispensable à l'administration de la sécurité (et en particulier au Maintien en Condition de Sécurité). En préventif, assurer la sécurité d'un système c'est, entre autres, déployer régulièrement les patches de sécurité. En réactif, la sécurité peut nécessiter le changement rapide et global de certaines configurations afin de se protéger : par exemple en isolant une partie du système. Il est donc intéressant de partager des outils de télé-administration.

Un exemple de solution complète open-source : Vigilo-Prelude-Pulse-GLPI

Pour conclure nous vous proposons un cas concret de rapprochement de différents outils des mondes de la performance et de la sécurité pour en faire une solution globale.

Cette solution est basée sur quatre logiciels phares open-source :

• **Vigilo** : Supervision de performances. Basé sur Nagios pour la collecte, Vigilo est une solution complète de supervision pour les grands parcs. Elle offre des interfaces de supervision, de métrologie et de reporting. Vigilo est développé sous licence GPL par la société CS .

• **Prelude** : Prelude est le pendant de Vigilo dans la détection d'intrusion. Prelude est un "Security Information Management"

(SIM) Universel. Prelude collecte, normalise, catégorise, agrège, corrèle et présente tous les événements sécurité indépendamment de la marque ou de la licence du produit dont ces événements sont issus : il est "Agentless". Prelude est développé sous licence GPL par la société Prelude IDS Technologie.

- **Pulse** : Pulse est un outil de télé-déploiement, d'inventaire et de gestion technique de parc. Il est développé par la société Mandriva.
- **GLPI (Gestion Libre de Parc Informatique)** : GLPI est un outil de gestion fonctionnelle de parc informatique. Il offre des possibilités d'inventaire, de gestion des matériels mais aussi de gestion de ticket d'incident. Il est développé par l'association Indepnet.

Les travaux en cours actuellement sur ces logiciels sont les suivants :

- Uniformisation de la base de données (CMDB) : proposer une base commune contenant l'ensemble des informations sur le parc. Vigilo et Prelude en extraient les informations pour construire leurs configurations. Pulse s'appuie sur cette base pour les actions de push (mises à jour des patches par exemple) mais maintient aussi la conformité de la base grâce à ses fonctions d'inventaire. Enfin, la gestion fonctionnelle des processus (GLPI) s'appuie sur cette base et la complète.
- Rapprochement des interfaces : Vigilo et Prelude proposent des interfaces de type Bac à événements légèrement similaires. Les réflexions en cours sur les interfaces sont multiples : uniformisation des ergonomies, partage d'information (pouvoir identifier facilement à partir de l'interface de sécurité l'état de « performance » d'un équipement ainsi que son historique), etc.
- Globalisation des processus : gérer la sécurité au même titre que le reste avec un suivi par gestion de tickets (et d'historique), des systèmes de workflow, un rapprochement des événements annexes, etc. grâce à GLPI.
- Corrélation : Vigilo et Prelude disposent aujourd'hui chacun de leur moteur de corrélation. Nous menons une réflexion

pour « corrélér » ces deux corrélateurs. Ainsi un serveur attaqué pour Prelude ne généra pas inutilement des alertes multiples de baisses de performances pour les équipes d'exploitation mais par exemple une alerte globale.

Pour illustrer comment ces rapprochements permettent d'adresser les problématiques communes présentées plus haut nous vous proposons deux scénarios courants dans la vie d'un système d'information.

Déploiement d'un serveur :

- Un nouveau serveur Linux est installé sur le parc.
- Cela fait l'objet d'un ticket de gestion de changement dans GLPI et renseignement de la base.
- Pulse lit dans la base qu'il y a un nouveau serveur Linux, il déploie son agent d'inventaire et télé-déploie et procède au premier inventaire.
- Vigilo et Prelude lisent dans la base qu'il y a un nouveau serveur Linux ainsi que son inventaire. Ils se configurent pour le superviser et poussent la demande à Pulse de déployer l'agent nécessaire.
- L'agent est déployé automatiquement et renvoie les informations collectées vers Vigilo et Prelude.

Maintien en condition de sécurité :

- Un nouveau patch pour Apache est publié, il est téléchargé et stocké sur les serveurs de patches.
- La base GLPI est renseignée sur l'existence de ce patch.
- Grâce à la base inventaire, les serveurs qui hébergent Apache sont identifiés.
- Pulse déploie automatiquement sur cette liste de serveurs les patches en question. Il procède si nécessaire à l'arrêt/relance des serveurs Apache.
- L'inventaire est relancé pour vérifier que les patches sont correctement installés.
- Vigilo lance périodiquement ses requêtes

HTTP qui valident que les serveurs continuent à bien fonctionner.

- Nota : cette opération est identique si un serveur Apache est attaqué et qu'un patch pour protéger le serveur est disponible. Mais il est bien plus efficace grâce à l'anticipation d'une attaque.

En conclusion,

l'administration et la supervision de sécurité sont des nouveaux aspects incontournables pour la sûreté des systèmes d'information. Il est important de les intégrer dans les processus et les outils existants aujourd'hui pour la gestion « standard » des systèmes et éviter le risque d'introduire des redondances, des incohérences qui au final en affaibliraient la sûreté. ■



Gilles LEHMANN est architecte de systèmes d'information. Il conçoit des systèmes sécurisés d'envergure pour le civil ainsi que dans le monde de la Défense. Il est aujourd'hui responsable de l'offre open-source à CS.

Références :

- Vigilo : supervision performances**
<http://www.projet-vigilo.org>
- Prelude : supervision sécurité**
<http://www.prelude-ids.com>
- Pulse : télé-déploiement/inventaire**
<http://pulse.mandriva.org>
- GLPI : Gestion de Parc**
<http://www.glpi-project.org>