

# Avis d'expert : comment bien surveiller une infrastructure virtualisée

Il y a quelques années seulement, le cabinet Gartner avait prédit que la virtualisation des serveurs serait la tendance majeure de 2012. L'année 2012 est maintenant révolue et nous avons le recul nécessaire pour constater la justesse de ces prévisions. Notre ère est celle des infrastructures informatiques extrêmement souples. Cette souplesse est désormais une exigence courante et **la virtualisation est devenue l'un des piliers essentiels des infrastructures informatiques** dans le monde entier. Et comme nous utilisons cette virtualisation au quotidien, nous connaissons désormais plus précisément les problèmes liés aux machines virtuelles.

## Infrastructure distribuée

Les applications des entreprises se trouvent probablement à différents endroits (serveurs, réseaux...), voire dans le Cloud. Il se peut même que les calculs soient effectués dans des datacenters disséminés à travers le monde. Dans ces conditions, si les connexions aux réseaux venaient à échouer, des centaines d'applications seraient indisponibles, ce qui représenterait un risque majeur pour l'activité de la société !

Ces aspects critiques de la virtualisation représentent un défi de taille pour les dernières technologies de l'information. À l'ère des environnements virtuels, **la surveillance de la structure devient une obligation** qu'il revient de traiter comme une priorité absolue en tant qu'administrateur. La superposition d'une couche de virtualisation sur les équipements matériels nécessite un traitement rapproché de l'infrastructure logique. C'est pour cela qu'une solution de surveillance permet de réagir en cas de difficulté, avant que le système soit impacté, et de limiter les problèmes liés aux environnements informatiques dynamiques.

Outre qu'ils surveillent la santé des composants physiques du réseau, ainsi que les performances et la sécurité de ce dernier, les outils de surveillance offrent plusieurs capteurs natifs adaptés aux machines virtuelles. Grâce à ceux-ci, l'administrateur peut suivre de près **les performances de son serveur hôte**, VMware par exemple, **l'utilisation de l'unité centrale et de la mémoire** par une machine virtuelle, ainsi que **l'utilisation du réseau par des conteneurs**, Parallels Virtuozzo Containers par exemple. Il peut également voir l'état d'une machine XenServer, l'espace disque disponible sur ses volumes partagés de cluster Microsoft Hyper-V, le nombre de machines virtuelles exécutées sur un hôte Citrix Xen, ou encore la vitesse de lecture et d'écriture sur disque des services Amazon Cloud, pour ne citer que quelques-unes des nombreuses options à disposition. Tout est possible avec un outil de surveillance de qualité.

## Souplesse

Pour être utile, un outil de surveillance doit faire preuve d'une **extrême adaptabilité dans les tâches d'administration**, se mettant ainsi au diapason des besoins dans des infrastructures informatiques évoluant très rapidement. L'administrateur doit ajouter un nouvel équipement dans

son datacenter ? Il peut utiliser simplement l'option de création de modèle d'équipement. Ensuite, il ne lui reste plus qu'à exécuter le mécanisme de reconnaissance automatique conjointement avec le fichier modèle pour inclure son nouvel équipement dans la surveillance, sans lancer une quelconque recherche potentiellement chronophage.

Qu'il s'agisse de manager le datacenter ou les applications, l'administrateur apprécie cette adaptabilité. En effet, s'il gère les composants physiques de son système, il s'attachera à la fiabilité des connexions hautes performances partagées, par exemple, tandis que son collègue chargé des ressources partagées choisira probablement de surveiller la qualité du service entre les connexions réseau, ainsi que l'utilisation globale des serveurs, dans la mesure où les applications sont distribuées sur différents serveurs. De fait, certaines applications requièrent un surplus de ressources à certains moments. Un bon outil de surveillance du réseau permettra d'effectuer l'ensemble de ces tâches grâce à des capteurs chargés de surveiller le trafic de sorte que la bande passante soit toujours suffisante. Il est également possible d'utiliser des capteurs pour assurer la qualité de service des connexions réseau ou bien pour surveiller l'utilisation de l'unité centrale, de la mémoire et des disques sur les systèmes hôtes et les machines (virtuelles) en les équipant de capteurs dédiés.

## Changement de point de vue

Chaque administrateur veut disposer d'une vue d'ensemble qui l'informe sur l'infrastructure en fonction de ses besoins. L'outil de surveillance peut présenter l'état des équipements physiques sous forme d'arborescence. Toutefois, tout logiciel de surveillance doit au moins pouvoir refléter la structure logique des environnements informatiques dans lesquels les applications sont également largement distribuées. L'outil nécessaire doit donc répondre à cette exigence et proposer des fonctionnalités de création de bibliothèques et des tableaux de bord indépendants de la structure physique du réseau.

En conclusion, l'assistant de surveillance de réseau doit **informer à la fois sur les machines physiques et virtuelles**, ainsi que sur le **réseau local et global**. Il doit être simple et intuitif. Grâce à lui, l'administrateur peut prendre rapidement les décisions qui s'imposent pour que les connexions au réseau fonctionnent en continu. Enfin, l'outil de surveillance doit être fiable et sûr, indépendamment de la taille et de l'infrastructure du réseau, car celles-ci peuvent évoluer rapidement.

---

### Voir aussi

[Silicon.fr étend son site dédié à l'emploi IT](#)

[Silicon.fr en direct sur les smartphones et tablettes](#)