

La sécurisation des postes de travail virtuels — Dernier obstacle levé pour une adoption généralisée

Simon Crosby, Directeur des Technologies, division Datacenter & Cloud, Citrix Systems, Inc.

En mai 2010, McAfee et Citrix ont conclu un partenariat stratégique et un accord de collaboration visant à offrir une sécurité des postes de travail virtuels plus simple et plus évolutive pour les déploiements d'entreprise de grande taille. Cette collaboration entre les deux leaders de la sécurité et de la virtualisation permet aux clients Citrix XenDesktop d'étendre la gestion de la sécurité des postes clients aux environnements virtuels à l'aide de la plate-forme McAfee® ePolicy Orchestrator®. Ce partenariat a vu le jour face à la demande croissante des clients d'une gestion de la sécurité intégrée dans les grands déploiements VDI d'entreprise.

Citrix peut se vanter d'en savoir long dans le domaine de la virtualisation. La société a notamment développé le produit phare de virtualisation des postes de travail Citrix XenDesktop. Nous n'avons par contre aucune prétention en ce qui concerne la sécurité informatique. Bien sûr, nous avons pleinement conscience de l'importance de la sécurisation dans le cadre de la virtualisation des postes de travail et des serveurs. Toutefois, il nous semble plus judicieux de travailler avec des partenaires experts dans le domaine de la sécurité informatique plutôt que d'essayer d'intégrer ces fonctionnalités dans notre offre de solutions. Le partenariat conclu entre Citrix et McAfee présente un intérêt considérable pour nos clients, en ce sens qu'il leur permet de tirer pleinement parti des avantages attendus de la virtualisation.

Cet aspect est important car, malgré les bénéfices évidents de la virtualisation, les entreprises sont plus frileuses à l'adopter que prévu, particulièrement en ce qui concerne l'infrastructure des postes de travail. Selon les estimations, seulement 40 % des entreprises susceptibles de tirer des avantages de la virtualisation des postes de travail ont franchi le pas. Les analystes, dont Gartner, expliquent cette lenteur par la crainte d'un impact négatif de la sécurisation sur les performances dans un environnement virtualisé. Et il faut admettre que ces préoccupations étaient tout à fait justifiées, jusqu'à présent.

Pourquoi ? Sans solution de sécurité optimisée pour la virtualisation, les services informatiques ont appliqué aux machines et aux postes de travail virtuels le modèle de sécurisation des postes clients, à savoir : un poste client égale un agent de sécurité. En d'autres termes, ils ont déployé un agent de sécurité sur chaque machine ou poste de travail virtuel à protéger, comme s'il s'agissait d'un poste de travail.

Ce modèle adapté aux postes clients traditionnels pose de graves problèmes dans un environnement virtualisé. Etant donné qu'une même machine physique peut héberger un grand nombre de machines ou de postes de travail virtuels — disposant chacun de leur propre agent —, le serveur physique est inondé par une multitude de copies d'agents de sécurité, de fichiers de signatures et de bases de données sur les menaces, entre autres. Cette approche gaspille les capacités de stockage et les ressources du processeur et de la mémoire.

Mais le véritable défi est celui des performances. Si ces systèmes de protection des postes clients sont mis à jour simultanément, on assiste à un « bombardement antivirus » qui amoindrit les performances. Ce modèle finit par solliciter trop lourdement le processeur et la mémoire, saturer le réseau et provoquer des goulots d'étranglement au niveau des E/S. Imaginez 120 systèmes de sécurité qui s'exécutent en parallèle sur le même serveur — il n'est pas étonnant que les administrateurs informatiques s'inquiètent des performances.

Certains fournisseurs de virtualisation ont voulu alléger l'impact de la sécurisation sur les performances en essayant de renforcer les fonctionnalités de sécurisation de leurs propres produits. Si nous saluons leurs efforts, nous n'en pensons pas moins qu'ils se fourvoient. Comme je l'ai déjà mentionné, Citrix estime qu'une approche intégrée, basée sur une technologie de pointe, vaut bien mieux pour nos clients. Nous l'avouons sans honte : « chasser les intrus » n'est pas notre cœur de métier. De notre point de vue, un partenariat avec McAfee constitue l'alliance idéale entre une vaste gamme de solutions de sécurisation et une offre non moins vaste de technologies et de services.

C'est dans cet esprit que Citrix et McAfee ont adopté une approche qui déplace la fonction de sécurisation de la machine virtuelle vers l'infrastructure virtuelle, de sorte que cette dernière est désormais responsable de la protection des machines virtuelles invitées qu'elle héberge. Cette approche présente également l'avantage de protéger l'infrastructure virtuelle elle-même. Mais l'avancée la plus notable concerne les performances.

La plate-forme McAfee Management for Optimized Virtual Environments (McAfee MOVE), qui prend en charge Citrix XenDesktop, offre une gestion de la sécurité spécialement conçue pour les environnements virtualisés. Au lieu d'exécuter un agent de sécurité sur chaque machine virtuelle, la solution McAfee MOVE AntiVirus for Virtual Desktops propose une appliance virtuelle qui consolide les processus d'analyse et les mises à jour de signatures afin de protéger efficacement tous les postes de travail virtualisés, tout en améliorant considérablement l'évolutivité.

Le fait de déplacer la fonction de sécurisation hors de la machine virtuelle permet également aux administrateurs informatiques de planifier des analyses intelligentes au moment le plus opportun, en fonction de la charge de l'hyperviseur ou lorsque les images sont hors ligne. Cette approche permet également de décharger les machines virtuelles des tâches de traitement intensif. Elle simplifie aussi le travail des services informatiques dans la mesure où elle centralise la gestion de la sécurité pour permettre de gérer en toute facilité les analyses antivirus et les mises à jour des fichiers de signatures à partir d'une console unique, telle que McAfee ePolicy Orchestrator. La réduction des besoins d'utilisation du processeur, de la mémoire et du stockage, alliée à la simplification de la protection des postes de travail, nous a permis d'améliorer la sécurisation et l'évolutivité des déploiements de postes de travail virtuels.

Les résultats dépassent toutes les espérances. Lors de tests menés par McAfee et Citrix, l'utilisation de McAfee MOVE AntiVirus for Virtual Desktops a permis aux serveurs de prendre en charge trois fois plus de machines virtuelles que lorsque la solution de sécurité était installée sur ces dernières. Une telle efficacité est un argument majeur auprès des entreprises en faveur de la virtualisation des postes de travail. Ce niveau de performances lève le principal obstacle à une adoption généralisée de la virtualisation.

Pour plus d'informations sur la manière dont le partenariat conclu entre McAfee et Citrix peut vous aider à profiter des avantages de la virtualisation des postes de travail, consultez le site www.mcafee.com/fr/partners/global-alliances/citrix-systems.aspx ou www.mcafee.com/fr/solutions/virtualization/virtualization.aspx.



Simon Crosby occupe le poste de Directeur des Technologies de la division Datacenter & Cloud de Citrix. Il a fondé XenSource, dont il était le Directeur des Technologies avant l'acquisition de la société par Citrix. Avant cela, M. Crosby était ingénieur principal chez Intel et avait également fondé l'éditeur de logiciels d'optimisation des réseaux CPlane, Inc.

