



Une plate-forme matérielle pensée pour la virtualisation des serveurs

Flexibilité renforcée, gains de performances et baisse du coût de revient grâce aux processeurs Intel® Xeon® série 5500



La virtualisation des serveurs est d'une aide précieuse à la direction des services d'information (DSI) de l'entreprise puisqu'elle lui permet d'améliorer le rendement de son datacenter sur plusieurs plans et, surtout, à la base. Elle favorise en effet le regroupement (« consolidation ») de plusieurs systèmes d'exploitation et leurs ensembles applicatifs sur un même serveur physique. Elle réduit ainsi le périmètre de l'infrastructure informatique tout en autorisant le déploiement de nouvelles applications en quelques minutes.

Elle admet aussi très facilement le basculement d'applications en cours d'exécution, d'un serveur sur un autre, sans indisponibilité, soit une gestion assouplie des charges applicatives et une forte continuité de service, tant à l'occasion des opérations de maintenance programmées que des incidents fortuits. C'est pourquoi investir dans des solutions de virtualisation représente une décision de gestion avisée, sachant que les avantages qu'elles dégageront en termes de rendement de l'infrastructure, d'économies d'énergie, d'administrabilité, de qualité de service et de structure de coûts peuvent être considérables.



Pour tirer le meilleur parti de la virtualisation, il faut cependant des serveurs prévus pour assumer les lourdes sollicitations, qui plus est fluctuantes, d'une infrastructure virtualisée et consolidée. Or c'est précisément pour aider l'entreprise à profiter au maximum de la virtualisation qu'Intel a conçu une plate-forme physique plus performante, dotée de fonctions d'assistance matérielle originales, qui rationalisent le fonctionnement du datacenter virtuel. Les processeurs Intel® Xeon® série 5500¹ sont les éléments précurseurs de cette nouvelle génération de plates-formes pour serveurs. Ils se caractérisent par une bande passante des E/S élargie, qui stimule les performances de virtualisation, ainsi que par la possibilité de migrer les machines virtuelles (VM) au sein d'un parc de serveurs de diverses générations, ce qui assure une flexibilité record aux environnements virtualisés.

La technologie Intel VT² de nouvelle génération renforce les performances de virtualisation natives d'un facteur allant jusqu'à 2,1³ et raccourcit jusque de 40 %⁴ le délai de basculement d'une charge applicative entre deux VM, grâce à des technologies d'assistance matérielle intégrées aux processeurs, aux chipsets et aux cartes réseau.

Processeurs : technologie de virtualisation Intel® VT

- Intel® VT FlexMigration
- Intel® VT FlexPriority
- Tables de pagination Intel® VT EPT (Extended Page Tables)

Chipset : technologie Intel® VT-d (directed I/Os) de virtualisation appliquée aux E/S

Réseau : technologie Intel® VT-c de virtualisation appliquée à la connectivité

- Files d'attente VMDq (Virtual Machine Device Queues)
- Connexion VMDC (Virtual Machine Direct Connect)

Si Intel intègre à tous les principaux composants d'un serveur des fonctions d'assistance matérielle à la virtualisation, c'est pour permettre aux DSI de consolider sur chaque machine un nombre plus important d'applications et des charges applicatives plus lourdes ainsi que pour renforcer la flexibilité et la fiabilité du datacenter et réduire son coût de revient.

« Le choix d'une plate-forme matérielle adaptée à la virtualisation des serveurs est tout aussi important que celui du logiciel de virtualisation lui-même. »⁵

Cabinet IDC

Une virtualisation hors pair grâce à un accompagnement matériel complet

Les serveurs sortis il y a quelques années étaient prévus pour n'accueillir qu'un seul système d'exploitation (OS), aussi leur virtualisation et sa rentabilité impose-t-elle la présence d'un logiciel capable d'émuler un environnement matériel complet pour chaque OS « invité ». Or l'intervention de ce dernier monopolise une importante capacité de traitement et pèse lourd sur les performances : les risques sont une baisse de réactivité des applications, une adaptabilité limitée des serveurs ainsi qu'une complexification nuisible à la fiabilité et à la sécurité de l'infrastructure. Au demeurant, les environnements mixtes ne sont guère mieux lotis : à l'arrivée de nouveaux serveurs, l'incapacité à translater les VM d'une machine à une autre, parce qu'elles sont de génération différente, entrave la souplesse du datacenter.

La technologie Intel VT aborde cette problématique au niveau le plus fondamental du datacenter, à savoir celui des circuits électroniques, en intégrant aux puces des fonctions d'assistance matérielle très complètes qui dopent les performances des logiciels de virtualisation d'un facteur allant jusqu'à 2,1³ qui stimulent la réactivité applicative et qui assurent une fiabilité, une sécurité et une flexibilité

renforcées. Ces fonctions intégrées accélèrent ainsi les processus de base de la virtualisation sur l'ensemble de la plate-forme, y limitent les latences et préviennent les risques de congestion. Elles réduisent les sollicitations imposées aux logiciels de virtualisation afin de libérer des cycles d'horloge à consacrer aux applications métier et autorisent la migration des VM entre des serveurs d'architecture Intel de génération différente. On peut donc consolider sur chaque serveur davantage d'applications et des charges applicatives plus importantes, pour tirer un meilleur rendement de son investissement en matériel et en logiciels.

Intel travaille avec VMware, Microsoft, Citrix, Parallels et de nombreux autres grands noms des logiciels de virtualisation pour veiller à ce que les solutions d'aujourd'hui et de demain prennent largement en charge ses technologies en la matière et qu'elles conjuguent les plus importants bénéfices possibles à une transparence totale, tant pour la DSI que pour les utilisateurs : les fonctions des solutions de virtualisation restent les mêmes ; les serveurs virtualisés sont simplement plus réactifs, adaptables et fiables.



Processeurs : Intel® VT

Accompagnement à la virtualisation renforcé de la part des processeurs Intel

La technologie Intel VT contribue à renforcer dans leurs fondements la souplesse, la stabilité et les performances des solutions de virtualisation logicielles. Elle réduit en effet les interventions de l'hyperviseur en éliminant son obligation d'« écouter », de « piéger » et d'exécuter certaines instructions pour le compte de l'OS invité, que lui impose une virtualisation purement logicielle. Elle assure aussi un accompagnement matériel quand la maîtrise de la plate-forme se transmet entre l'hyperviseur et les OS invités, de sorte que, lorsque l'intervention de celui-ci est nécessaire, ces passations sont plus rapides, plus fiables et mieux sécurisées.

La technologie Intel VT dispose par ailleurs de fonctions de migration des machines virtuelles qui protègent l'investissement informatique et qui assouplissent les capacités de basculement sur VM analogue en cas d'indisponibilité, d'équilibrage des charges, de reprise sur sinistre ou de maintenance.

- **Intel® VT FlexPriority.** Lorsqu'un processeur exécute une tâche, il reçoit souvent des demandes (« interruptions ») de la part de ses périphériques ou d'autres applications, qui sollicitent ainsi son intervention. Pour en limiter l'incidence sur les performances, l'un de ses registres (registre TPR [Task Priority Register] de l'APIC) surveille la hiérarchie des tâches, pour que seules soient prises immédiatement en compte les interruptions dont la priorité est supérieure à celle des opérations en cours. La technologie Intel FlexPriority crée une copie virtuelle du registre TPR, lisible et, dans certains cas, modifiable par les OS invités, sans intervention de l'hyperviseur. Or cette particularité est susceptible d'offrir des gains de performances conséquents aux systèmes d'exploitation 32 bits qui exploitent fréquemment ce registre. (Elle peut ainsi stimuler jusque de 35 % les performances des applications gérées sous Windows Server* 2000.)⁷

- **Intel® VT FlexMigration.** L'un des avantages majeurs de la virtualisation est la capacité qu'elle assure à basculer d'un serveur physique à un autre les applications en cours d'exécution, sans interruption de service. Or la technologie Intel VT FlexMigration rend possible cette migration entre des serveurs d'architecture Intel actuels et futurs, même s'il arrivait que ces derniers exploitent un jeu d'instructions élargi. Grâce à cette technologie, les hyperviseurs établissent en effet un jeu d'instructions cohérent pour l'ensemble du pool de migration, d'où une capacité de basculement transparent des charges applicatives au sein de celui-ci. Il en résulte un pool de ressources serveur plus souple et unifié, qui fait fi des conflits de générations matérielles.

Chipset : Intel® VT-d

Accompagnement à la virtualisation renforcé de la part des chipsets Intel

Avec l'augmentation du nombre d'OS consolidés sur chaque serveur, les flux de données au sein du système et vers l'extérieur (trafic d'E/S) augmentent et se complexifient. Or, sans assistance matérielle, l'hyperviseur intervient directement dans chaque transaction d'E/S, ce qui a pour effet, non seulement de ralentir cette circulation, mais aussi d'alourdir la charge des processeurs centraux en raison de l'activité accrue de l'hyperviseur. C'est comme si tous les clients d'un centre commercial bondé devaient y entrer ou en sortir par une même porte et qu'ils ne pouvaient, de surcroît, s'orienter qu'avec l'aide du directeur : non seulement ils piétineraient, mais cette situation empêcherait également le pauvre homme de se consacrer à d'autres tâches pressantes.

Or la technologie Intel VT-d accélère la circulation des données et élimine une bonne partie des temps système en limitant l'intervention de l'hyperviseur pour la gestion du trafic d'E/S. Elle permet à ce dernier d'affecter de manière sécurisée des périphériques d'E/S donnés à tel ou tel OS invité. Chacun de ces périphériques se voit ainsi attribuer une zone réservée en mémoire vive, c'est-à-dire à laquelle il est le seul, avec l'OS concerné, à pouvoir accéder.

Lorsque ces affectations ont été définies, les données circulent alors librement entre un OS invité et les périphériques qui lui sont attribués. Le trafic des E/S est plus fluide et, l'hyperviseur étant moins sollicité, la charge des processeurs centraux s'en trouve diminuée elle aussi. La sécurité et la fiabilité se renforcent par ailleurs elles aussi, puisqu'aucun autre composant matériel ou logiciel invité ne peut accéder aux données d'E/S destinées à un périphérique ou à un OS invité précis.

Réseau : Intel® VT-c

Meilleure prise en charge de la virtualisation par les périphériques d'E/S Intel

Avec la multiplication des applications gérées en environnement virtualisé et la mise à profit de la migration en direct pour économiser l'énergie ou renforcer la continuité de service, les sollicitations imposées aux périphériques d'E/S virtualisés s'alourdissent considérablement. La technologie Intel VT-c optimise le réseau pour la virtualisation, en intégrant des fonctions d'assistance matérielle très complètes aux périphériques d'E/S qui relient les serveurs au réseau du datacenter, à son infrastructure de stockage et à des périphériques externes.

Ces fonctions sont comparables à celles d'un centre de tri postal chargé d'une multitude de lettres, paquets et autres plis pratiquement tous différents et à diriger vers leur destination respective : en effectuant cette opération sur des puces réseau dédiées, la technologie Intel VT-c accélère l'acheminement et en déleste l'hyperviseur ainsi que les processeurs centraux.

C'est parce qu'elle recouvre deux technologies particulières, désormais gérées par toutes les cartes 10 Gigabit Ethernet d'Intel pour serveurs et certaines de ses cartes Gigabit Ethernet :

- **Les files d'attente VMDq (Virtual Machine Device Queues) maximisent le débit des E/S.** En environnement serveur habituel, l'hyperviseur doit trier et acheminer chaque paquet de données vers sa VM de destination, ce qui monopolise souvent toute une série de cycles d'horloge. Avec les files VMDq, cette fonction de tri est déléguée à des composants matériels dédiés des cartes réseau Intel pour serveur. L'hyperviseur n'a ainsi plus qu'à acheminer les groupes de paquets pré-triés aux OS concernés. La latence des E/S s'en trouve réduite, et le processeur peut consacrer une plus grande partie de ses capacités de traitement aux applications métier. La technologie Intel VT-c va ainsi jusqu'à

doubler le débit des E/S dans certains cas et fournit une bande passante quasiment native aux applications virtualisées, de sorte que l'on peut en consolider un plus grand nombre par serveur, avec moins de congestions.⁹

- **La connexion VMDc (Virtual Machine Direct Connect) stimule les performances en virtualisation.** Elle autorise en effet les VM à accéder directement aux équipements d'E/S réseau en exploitant le standard SR-IOV (Single Root I/O Virtualization) du groupement PCI-SIG (PCI Special Interest Group), ce qui dope les performances en virtualisation. Comme indiqué plus haut, la technologie Intel VT-d instaure une communication directe entre un OS invité et un port d'E/S du périphérique concerné. Le standard SR-IOV vient ainsi la prolonger, en autorisant l'établissement de plusieurs canaux de communication directe pour chaque port d'E/S du périphérique en question. Dès lors, dans le cas de dix OS invités, on peut affecter à chacun un lien protégé et dédié à 1 Go/s vers le réseau, sur un seul port d'une carte 10 Gigabit Ethernet Intel. Cette communication directe contourne le commutateur de l'hyperviseur et accélère les E/S tout en délestant les processeurs centraux.

Une plate-forme mieux adaptée à la virtualisation

Dotés de fonctions d'assistance matérielle originales qui rationalisent l'exploitation du datacenter et qui contribuent à juguler la multiplication incontrôlée des serveurs, les processeurs Intel Xeon série 5500 sont parfaitement adaptés à la virtualisation. Grâce à la microarchitecture nouvelle génération d'Intel, dont le nom de code est Nehalem, ils confortent les avantages de ce mode de fonctionnement au travers d'innovations qui dopent les performances, renforcent les ratios de consolidation et permettent d'associer des machines de générations différentes au sein d'un même pool de serveurs virtualisées. Ils renforcent aussi les capacités de basculement sur une VM symétrique en cas d'indisponibilité, d'équilibrage des charges et de reprise sur sinistre.

De plus, ces technologies sont totalement intégrées, ont été scrupuleusement testées et sont exploitées par les principales solutions de virtualisation logicielles. Elles constituent donc pour les DSI un tremplin confirmé et privilégié pour rentabiliser au maximum leurs investissements en serveurs et dans la virtualisation.

Actualité des technologies de virtualisation Intel :

www.intel.com/technology/virtualization/server (en anglais)

Renseignements détaillés sur les technologies Intel VT-c et VT-d : www.intel.com/go/vtc (en anglais)

¹ La numérotation des processeurs Intel® ne constitue pas une indication quantitative de leurs performances. Elle permet de différencier des modèles appartenant à une même série de processeurs, mais non pas à des séquences différentes. Voir http://www.intel.com/products/processor_number/fra à ce sujet.

² Le bénéfice de la technologie de virtualisation Intel® VT (Virtualization Technology) suppose que l'ordinateur concerné soit équipé d'un processeur Intel®, d'un jeu de composants, d'un BIOS, d'un hyperviseur et, pour certains usages, de logiciels de niveau plate-forme particuliers, qui tous ont été optimisés pour elle. Les fonctionnalités, les performances et autres avantages varient selon la configuration matérielle et logicielle et peuvent nécessiter la mise à jour du BIOS. Les hyperviseurs sont susceptibles de ne pas être compatibles avec tous les systèmes d'exploitation. Pour plus d'informations sur un hyperviseur précis, consultez son éditeur.

³ Résultats obtenus au banc d'essai VMmark*. Les chiffres s'appuient sur des résultats publics pour le processeur Xeon® X5470 et sur des mesures effectuées en interne par Intel (février 2009) pour le processeur Xeon® X5570. Résultats et configurations : 1) score de 9,15 pour 7 « mosaïques » (ensembles de six machines virtuelles chacune) sur plate-forme serveur HP ProLiant® ML370 G5 dotée de processeurs Intel® Xeon® X5470 (3,33 GHz, 2 x 6 Mo de cache L2, bus principal à 1 333 MHz), de 48 Go de mémoire vive et de VMware ESX 3.5.0 Update 3 ; 2) score de 19,51 pour 13 mosaïques sur plate-forme équipée de processeurs Intel® Xeon® X5570 (2,93 GHz, 8 Mo de cache L3, bus QPI à 6,4 GT/s), de 72 Go (18 x 4 Go) de mémoire vive DDR3-800 et de VMware ESX Build 140815.

⁴ Source : relevés effectués en interne par Intel. Comparaison entre processeurs Intel® Xeon® séries 5500 (Nehalem) et 5400.

⁵ Source : « Choosing the Right Hardware for Server Virtualization », dossier IDC établi en partenariat avec Intel, réf. 211622, avril 2008 (<http://www.intel.com/business/technologies/IDCchoosingthehardware.pdf>).

⁶ La technologie Intel® VT est compatible avec les solutions articulées aussi bien sur des processeurs Intel® Xeon® d'architecture 32 bits que 64 bits (Intel® 64 et IA-32).

⁷ Les tests d'Intel mettent en évidence des gains de performances de 35 % pour Windows Server® 2000 et 2003 avec SP1 gérés en systèmes d'exploitation invités.

⁸ La technologie Intel® VT FlexMigration gère le déplacement des machines virtuelles (VM) sur l'ensemble des serveurs de microarchitecture Intel® Core™, y compris dans sa dernière génération (nom de code Nehalem). Intégrée aux nouveaux processeurs Intel® Xeon® série 5500, elle assure la compatibilité des transferts de VM sur processeurs actuels de microarchitecture Intel Core ainsi que sur les futurs processeurs multicœurs d'Intel. Pour connaître les conditions de prise en charge, contactez l'éditeur de votre hyperviseur.

⁹ Résultats obtenus à partir de tests réalisés en interne par Intel et VMware. Complément d'information : dossier « Intelligent Queueing Technologies for Virtualization, An Intel-VMware perspective: Enhanced Performance in Virtualized Servers » (http://download.intel.com/network/connectivity/products/whitepapers/Intel-VMware_VMDq_wp_May08.pdf).

Les tests et les indices de performances portent sur des configurations spécifiques, leurs éléments ou les deux. Ils rendent compte approximativement des performances des produits Intel mesurées par ces tests. Une différence dans la configuration matérielle ou logicielle est ainsi susceptible d'avoir une incidence sur les performances effectives. Il est donc conseillé aux acheteurs de consulter d'autres sources d'informations pour évaluer les performances des configurations ou des éléments de configuration dont ils envisagent l'acquisition. Pour plus d'informations sur les tests de performances des produits Intel, consulter la page www.intel.com/performance/resources/ (en anglais).

Les résultats en performances sont établis en attribuant la valeur indiciaire 1,0 au résultat d'un banc d'essai, puis en divisant le résultat effectif à chaque banc d'essai de la plate-forme de référence par celui des autres plates-formes et en leur attribuant un coefficient de performances relatif qui est en corrélation avec le différentiel de performances constaté.

Les produits Intel ne sont pas conçus pour une utilisation dans des applications médicales, de sécurisation ou de maintien de la vie, dans des systèmes de commande ou de sûreté essentiels ou dans le nucléaire. Les dates et produits mentionnés ne le sont qu'à des fins de planification et sont sujets à modification sans préavis.

© 2009 Intel Corporation. Tous droits réservés. Intel, le logo Intel, Xeon et le logo Xeon Inside ainsi que Intel Core sont des marques déposées ou enregistrées d'Intel Corporation ou de ses filiales, aux États-Unis et dans d'autres pays.

* Les autres noms et dénominations peuvent être revendiqués comme marques par des tiers.

