

Dossier Solution

Protection des données – Points à prendre en considération pour les systèmes convergés et hyperconvergés. La solution Veritas.

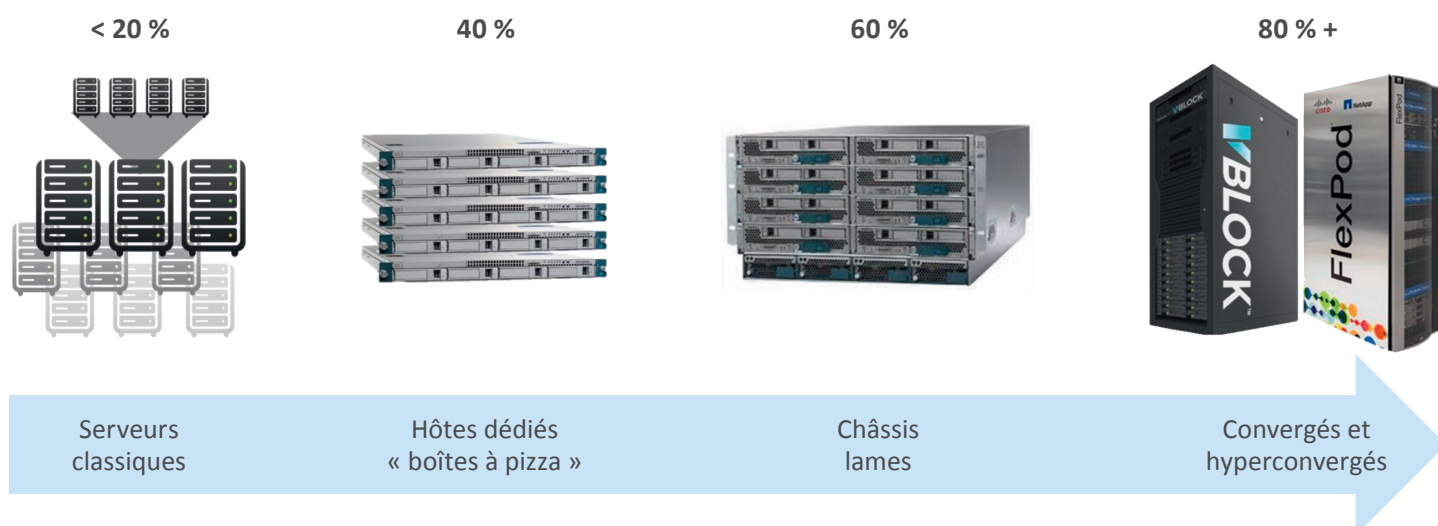
Date : février 2016 Auteur : Jason Buffington, analyste principal

Résumé : « Lorsqu'on modernise la production, on doit moderniser la protection ». Cela est vrai dans la plupart des discussions sur la transformation de l'IT. Mais ça l'est particulièrement quand on essaie de déterminer de quelle manière les stratégies et les méthodes de protection des données doivent évoluer lorsqu'on adopte des systèmes d'infrastructures convergées et hyperconvergées (CI/HC).

Introduction

Cela ne fait aucun doute : de tous les facteurs qui ont bouleversé l'informatique, aucun n'a été aussi décisif que la virtualisation des serveurs. Comme le montre la figure 1, l'informatique est passée de l'installation d'hyperviseurs sur des serveurs classiques via le déploiement de lames et de châssis à, tout dernièrement, ce que beaucoup considèrent comme la quintessence des fondements de l'infrastructure IT : l'appliance hyperconvergée et une architecture en racks de systèmes convergés.

FIGURE 1. L'évolution de l'infrastructure de la virtualisation des serveurs



Source : Enterprise Strategy Group, 2016

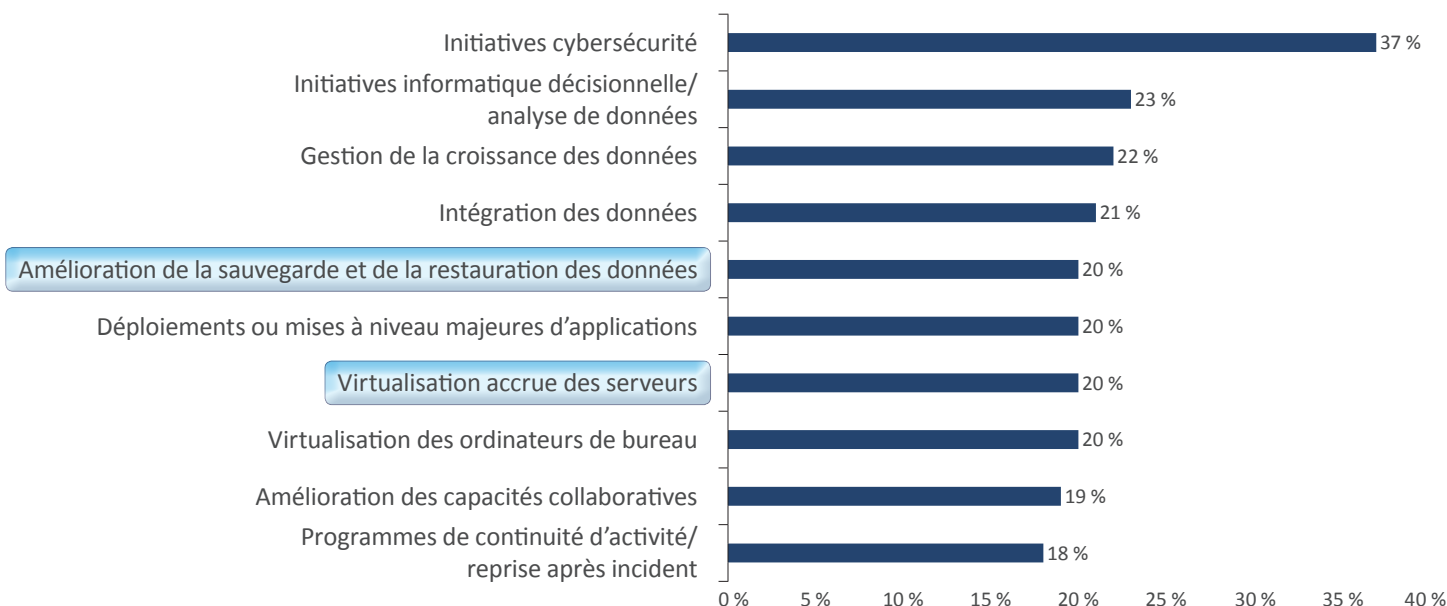
Mais la migration vers un état plus agile et plus virtualisé ne s'arrête pas là. Augmenter le recours à la virtualisation des serveurs demeure l'un des investissements IT qui revient le plus dans les priorités citées par les personnes interrogées dans le cadre de l'enquête ESG (voir la figure 2).¹

¹ Source : Rapport ESG, 2016 IT Spending Intentions Survey (Intentions d'investissements IT en 2016), publication prévue.

Comme le montre également la figure 2, une autre de ces priorités constamment évoquées est l'amélioration de la sauvegarde et récupération. Il ressort en effet des enquêtes menées par ESG en 2012, 2013, 2014 et 2015 sur les projets d'investissements IT qu'augmenter la virtualisation des serveurs et améliorer la sauvegarde figurent en permanence parmi les cinq priorités IT les plus mentionnées.

FIGURE 2. Les dix principales priorités d'investissements IT pour 2016

Les 10 priorités IT les plus importants au cours des 12 mois à venir.
(Pourcentage de personnes interrogées, N=633, dix réponses acceptées)



Source : Enterprise Strategy Group, 2016

Lorsqu'on modernise la production, on doit moderniser la protection

Si votre environnement n'est virtualisé qu'à 20 %, il y a toutes les chances qu'une approche médiocre de la sauvegarde vous suffise. Mais, si sa virtualisation atteint déjà les 50 %, ces approches anciennes risquent de vous freiner. Et, lorsque le taux de virtualisation atteindra ou dépassera les 70 %, ces approches de la sauvegarde seront un véritable boulet pour votre infrastructure de virtualisation. Pour le dire en d'autres termes, au fur et à mesure qu'augmentera la densité des machines virtuelles par hôte, de telles approches de la sauvegarde exerceront un impact négatif sur les VM à protéger et sur les hôtes et systèmes de stockage sous-jacents. Cette affirmation n'est pas purement théorique ; elle traduit une différence d'approche architecturale, dont le choix a une conséquence notoire pour les systèmes IT :

- **Les technologies traditionnelles, à base d'agents, qui s'exécutent au sein de chaque OS (physique ou virtuel)** et sont chargées de collecter et échanger des données avec le serveur de sauvegardes, *créent des pics importants dans le CPU et dans l'espace de stockage au sein de l'OS lorsque des opérations de sauvegarde sont en cours*. Les serveurs physiques sont souvent sous-utilisés et, de ce fait, tolèrent les pics sans ramifications. Les OS au sein des serveurs virtuels ne disposent pas de capacités inutilisées. Dans des environnements denses comme les systèmes convergés ou hyperconvergés (C/HC), le CPU, l'espace de stockage et la mémoire peuvent être sursollicités du fait de leur allocation et de leur partage dynamiques par les ressources sous-jacentes. Les pics qui mobilisent rapidement des ressources au sein d'une VM peuvent peser sur les autres ressources disponibles pour toutes les autres VM du même hôte ainsi que sur les ressources de cet hôte.
- **Les technologies modernes, basées sur les hôtes**, elles au contraire, protègent les VM du point de vue de l'hôte. Grâce à l'interaction avec des API matures au sein de l'hyperviseur – en l'occurrence, VMware vSphere API for Data Protection (VADP) ou Microsoft Hyper-V Volume Shadow Copy Services (VSS) – il est possible de protéger les VM de manière fiable sans créer de pics énormes nuisibles à l'environnement. Il peut quand même s'avérer nécessaire d'utiliser au sein de chaque VM un agent, un programme auxiliaire ou un module d'assistance pour s'assurer que les données présentes dans la VM sont prêtes à être sauvegardées (cela se fait souvent en invoquant, au sein de chaque VM, des appels VSS ou une autre application). Toute la différence réside en ceci : les données sont-elles transmises depuis l'OS virtualisé à l'aide d'une approche à base d'agent (« mauvais agent ») ou la VM est-elle protégée dans son ensemble des API de l'hôte (« bon agent »).

Pour être clairs, vous aurez à moderniser votre protection

Sauf à utiliser une version de solution unifiée de protection des données actuellement dans le commerce (c'est-à-dire, depuis 2014), votre adoption des systèmes C/HC vous amènera très vraisemblablement à mettre à jour votre solution de protection des données. La seule question alors est de savoir quand et de quelle manière.

Moderniser votre protection de manière proactive signifie que le choix et la modernisation de vos outils de protection des données ne sont pas indifférents pour votre stratégie IT générale de modernisation de votre infrastructure de production. Être proactifs permet aux administrateurs virtualisation, aux spécialistes sauvegarde et aux architectes IT de communiquer et de collaborer pour atteindre les objectifs des SLA et l'agilité en matière de récupération indispensable aux divers départements de l'entreprise. Une fois que ces spécifications ont été identifiées, un plan est développé et exécuté. Ce plan inclut le déploiement d'une ou plusieurs solutions de protection des données comme partie intégrante du déploiement de l'infrastructure de virtualisation.

La modernisation de la protection est dite réactive lorsqu'une organisation essaie d'utiliser à toutes forces sa solution datée de sauvegarde pour son environnement virtualisé, ce qui n'est pas sans provoquer un impact important sur les E/S dans les VM et se solde par un mécontentement généralisé des administrateurs virtualisation, des architectes IT et des utilisateurs finaux. L'IT est alors forcée de pallier ce problème en procédant à la hâte à une mise à niveau de la sauvegarde, ce qui peut avoir un impact négatif sur les autres scénarios de protection des données tant que l'environnement dans son ensemble n'évolue pas vers une solution neuve. Au vu de l'urgence de la situation et compte tenu de l'anxiété régnant dans l'ensemble de l'équipe IT, une organisation peut se trouver confrontée à l'alternative drastique suivante :

- Option 1 : Mettre la solution datée de sauvegarde au niveau de sa dernière version, qui, très certainement, utilise les API VADP et VSS modernes permettant des sauvegardes fiables des VM à partir de leurs hôtes.
- Option 2 : Déployer un outil de protection des données virtualisées, qui vient compléter l'outil unifié de protection en existence.

Chacune de ces deux tactiques de réaction comporte son lot de soucis et d'avantages :

- L'option 1 (mettre à niveau la solution unifiée) permet à l'équipe IT de continuer à utiliser le framework et l'architecture de solution qui lui est familière, en exploitant les divers motifs (extensibilité, agilité, etc.) qui l'ont conduite à l'origine à adopter cette plateforme. Mais, selon les matériels et les logiciels utilisés, cela peut provoquer des modifications dans le contrôle ou d'autres effets collatéraux inattendus dans l'ensemble de l'environnement.
- L'option 2 (déployer une solution spécifique à la virtualisation) introduit des éléments distincts (IU, ensemble d'outils, plannings et scénarios de stockage), mais l'impact sur l'efficacité sera variable selon qui est en charge de gérer les sauvegardes des VM : *administrateurs virtualisation ou administrateur sauvegardes*, avec des performances variables en fonction du degré de virtualisation de l'environnement.

Pour un grand nombre d'organisations disposant actuellement de solutions unifiées vieillissantes, la meilleure option possible est l'option *proactive*.

Ce qui est à rechercher dans une protection moderne de la virtualisation

Selon une récente enquête ESG, cinq des six principaux soucis signalés dans la protection des environnements virtualisés ont rapport à la visibilité (voir la figure 3).² Cela touche au fait qu'un grand nombre d'outils de protection des données (la plupart utilisant des approches obsolètes) ne sont pas au fait de la virtualisation.

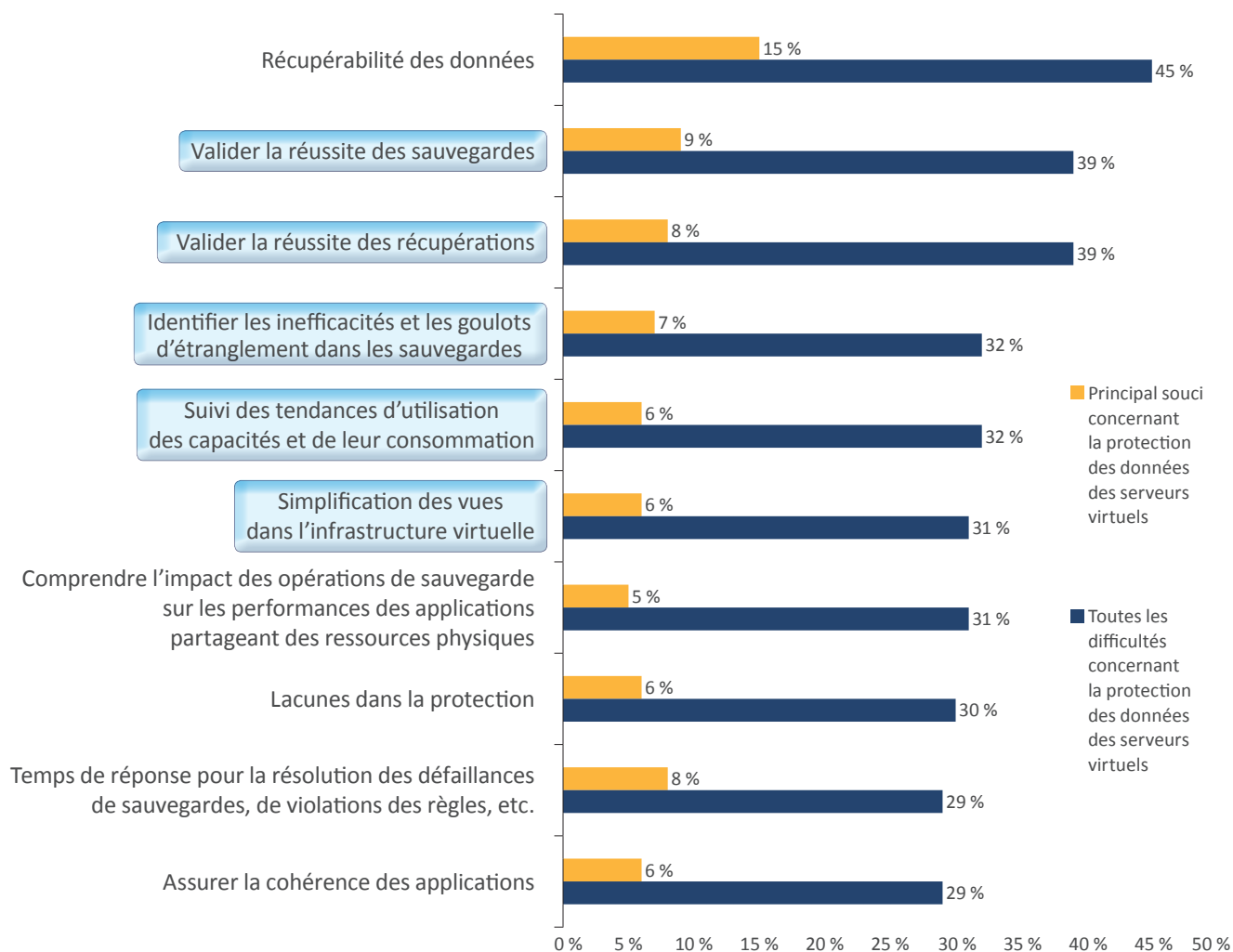
Outre le souci le plus fréquemment mentionné (la récupérabilité des données), les cinq autres préoccupations les plus citées tournent autour du fait que de nombreux outils de sauvegarde sont incapables de discerner si les sauvegardes et les récupérations ont réussi ou non. Ils sont incapables de voir où surviennent les problèmes. Ou bien ils ne peuvent décrire de quelle manière les sauvegardes affectent l'infrastructure virtuelle (et réciproquement).

En d'autres termes, même si la sauvegarde des VM a réussi, les informaticiens n'en sauront rien et resteront donc dans le doute à ce sujet. Ces doutes finiront par les amener à chercher une solution de remplacement qui n'améliorera rien en termes de performances et de communication de ses résultats.

² Source : Rapport ESG, [Trends in Protecting Virtualized Environments \(Tendances de la protection des environnements virtualisés\)](#), août 2015.

FIGURE 3. Les dix plus grands soucis dans la protection des environnements virtuels

Parmi les éléments suivants, lesquels désigneriez-vous comme des soucis concernant la protection de vos serveurs virtuels ?
 Lequel considérez-vous comme votre souci principal concernant la protection des données de vos serveurs virtuels ?
 (Pourcentage de personnes interrogées, N=375)



Source : Enterprise Strategy Group, 2016

Un élément différenciateur clé à rechercher est la compatibilité avec la virtualisation (VM/hôtes) des règles, du tableau de bord et du workflow de sauvegarde, quel que soit le cadre de travail d'administration des hyperviseurs et des systèmes utilisés ou envisagés.

L'enquête ESG (figure 4) met également en évidence les caractéristiques les plus recherchées par les organisations lorsqu'elles évaluent de nouvelles solutions de protection des données, qu'il s'agisse de solutions unifiées ou de solutions spécifiques à la virtualisation.³

³ ibid.

FIGURE 4. Les principales capacités spécifiques à la virtualisation pour le choix d'un nouveau produit de protection des données

Parmi les capacités de protection spécifiques aux machines virtuelles, lesquelles sont des facteurs primordiaux pour le choix de nouveaux produits de protection des données ? (Pourcentage de personnes interrogées, N=375, trois réponses acceptées)



Source : Enterprise Strategy Group, 2016

Ce qui est intéressant, c'est que le souci majeur concernant la protection des environnements virtualisés (figure 3) et la fonctionnalité mentionnée comme la plus recherchée pour le choix d'un produit de protection des données (figure 4) sont tous deux en rapport avec la récupération des données.

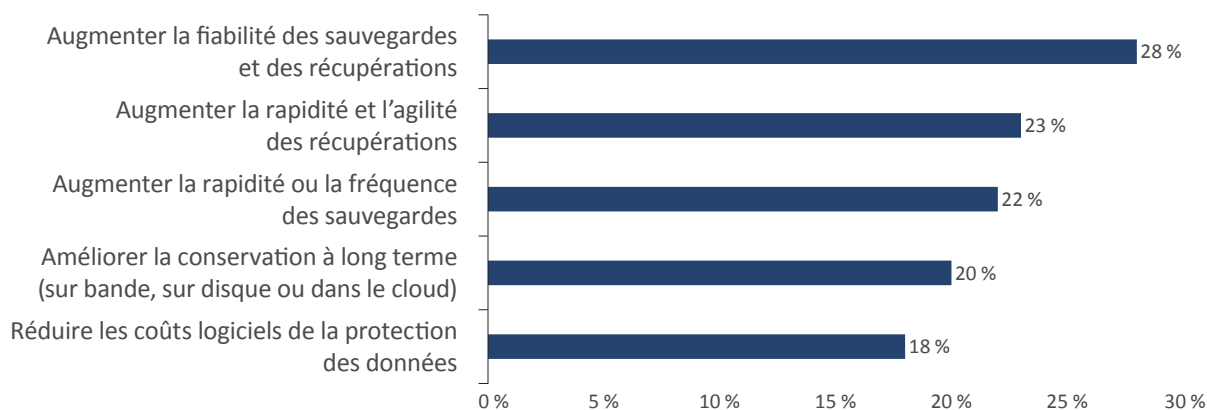
Au contraire viennent ensuite, comme cinq *soucis* les plus mentionnés les problèmes en rapport à l'administration et à la surveillance, susceptibles de provoquer du mécontentement. Mais les cinq *caractéristiques recherchées* les plus mentionnées ensuite ont toutes rapports à des fonctionnalités (intégration au cloud, réplication, déduplication et efficacité générale). D'un point de vue pratique, la figure 4 indique les caractéristiques clés à rechercher :

- **Immédiateté ou rapidité des récupérations de VM** – l'époque est révolue qui voyait les chefs d'entreprise attendre après les restaurations pour que l'activité de l'entreprise puisse reprendre.
- **Capacité à utiliser des services cloud** – pour la survivabilité des données dans des secteurs non soumis à réglementations, le degré de préparation à la continuité de l'activité et à la reprise après incident, etc.
- **Plus grande continuité de la protection** – afin de réduire les pertes de données entre les fenêtres de sauvegardes. Cela s'obtient souvent par une combinaison des clichés, de la réplication et des règles de sauvegarde dans un même cadre de travail d'administration.

Ces caractéristiques sont en phase avec les impératifs en matière de protection des données, définis par les directions IT en 2015 et signalés lors de l'enquête ESG (figure 5).⁴

FIGURE 5. Les cinq principaux impératifs en matière de protection des données imposés par les directions IT en 2015

Quelles sont les principales obligations imposées par la direction IT de votre organisation pour la protection des données ?
(Pourcentage de personnes interrogées, N=375, trois réponses acceptées)

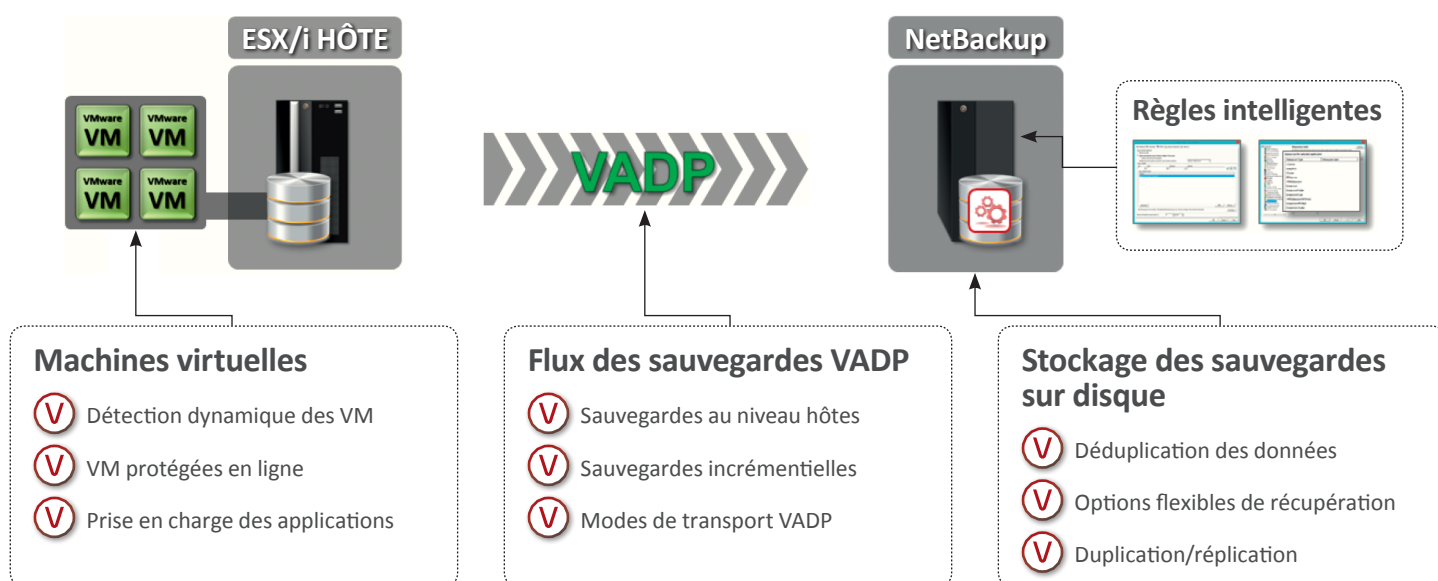


Source : Enterprise Strategy Group, 2016

En quoi Veritas NetBackup répond aux besoins de protection et de récupération des environnements CI/HC

Veritas, leader de longue date dans la protection des données, continue de répondre aux besoins des organisations en attente d'une protection et d'une récupération hétérogènes au niveau de toute l'entreprise. En exploitant pleinement les API VMware VADP (VMware APIs for Data Protection), Microsoft VSS (Volume Shadow Copy Services) et le Microsoft System Center Virtual Machine Manager (SCVMM), NetBackup 7.7 est fidèle à l'engagement de Veritas : garantir à toutes les plateformes IT une rigueur identique de protection pour la conservation et la récupérabilité des données. En outre, NetBackup continue d'offrir aux administrateurs virtualisation et aux spécialistes de la protection des données une expérience optimisée de leur plateforme (VMware), leur garantissant une protection correcte et une récupérabilité fiable de leurs VM comme du reste de l'entreprise (figure 6).⁵

FIGURE 6. Vue d'ensemble des mécanismes de sauvegarde par Veritas NetBackup 7.7 exploitant les VADP VMware



Source : Veritas, 2016

⁴ Source : Rapport de recherches ESG, [Trends in Protecting Virtualized Environments \(Tendances de la protection des environnements virtualisés\)](#), août 2015.

⁵ ibid.

La plateforme Veritas NetBackup est conçue pour tirer parti des mêmes mécanismes VADP que ceux utilisés par des solutions exclusivement VM, tout en fournissant le cadre de travail NetBackup de règles et d'administration, les options diversifiées de supports de sauvegarde, un catalogue à l'échelle de l'entreprise, la déduplication et les avantages de surveillance auxquels sont habitués les utilisateurs de NetBackup. Cela dit, NetBackup 7.7 offre plusieurs capacités de virtualisation :

- protection dynamique des VM Windows (à l'aide de VSS) et Linux (à l'aide de SYMCquiesce)
- récupération granulaire des données depuis les disques virtuels des VM VMware
- déduplication au niveau de l'hôte des sauvegardes et au sein de NetBackup Media Server afin de réduire considérablement les besoins en stockage lors de la protection d'un grand nombre de machines virtuelles similaires
- utilisation intégrée de VMware Change Block Tracking afin de réduire considérablement la durée des sauvegardes, tout en assurant une récupération flexible via des sauvegardes complètes synthétiques, grâce à NetBackup Accelerator
- reprise rapide du fonctionnement à l'aide de Veritas Instant Recovery for VMware (IRV) permettant de monter des VM depuis l'espace de stockage NetBackup, pour utiliser ensuite VMware Storage vMotion afin de déplacer la VM restaurée vers un hôte de production une fois que les utilisateurs ont pu reprendre leur activité

Autres avantages de la plateforme Veritas NetBackup : ses offres d'appliances, solutions clé en mains pour une protection des données efficace et optimisée pour le stockage au sein des datacenters, des bureaux distants et des environnements virtuels. La plateforme et les appliances NetBackup apportent aux organisations la certitude de bénéficier d'une protection des données moderne pour leur infrastructure convergée ou leur environnement hyperconvergé.

La vérité

Améliorer la protection des données continue d'être l'une des priorités d'investissements IT les plus mentionnées par les décideurs IT. Revenant d'une année sur l'autre, cette priorité est souvent motivée par le déploiement de nouvelles charges de travail IT qui exigent la modernisation de la protection et de la récupération. La virtualisation des serveurs est l'un des facteurs clés incitant à un nouveau niveau de protection des données. La virtualisation (du stockage, des calculs et des réseaux) est souvent réalisée par la convergence ou l'hyperconvergence des plateformes en raison de la pré-intégration de ces dernières, de la facilité et de la cohérence de leur déploiement, et de leur capacité à intensifier la densité des VM, pour un surcroît d'efficacité et d'agilité.

Il est impossible de sous-estimer l'impact transformateur de la virtualisation sur l'IT. Mais les mêmes mécanismes de virtualisation qui dopent l'agilité des environnements IT de production peuvent créer des problèmes de non-fiabilité ou entraver les efforts de sauvegarde et récupération. La réponse à ce problème est de planifier, **de manière proactive**, la modernisation des mécanismes et des stratégies de protection dans le cadre d'une modernisation de l'infrastructure de production.

Toutes les marques commerciales sont la propriété de leurs détenteurs respectifs. Les informations contenues dans cette publication ont été obtenues par des sources que The Enterprise Strategy Group (ESG) considère comme fiables mais qu'il ne garantit pas. Cette publication peut contenir des opinions d'ESG, qui sont susceptibles d'évoluer. Cette publication est soumise à copyright par The Enterprise Strategy Group, Inc. Toute reproduction ou redistribution de cette publication, en tout ou partie, que ce soit au format papier ou sous forme électronique ou autre, pour des personnes non autorisées à la recevoir, sans le consentement exprès de The Enterprise Strategy Group, Inc., constitue une violation de la loi des États-Unis sur le copyright et pourra donner lieu à des actions en justice et le cas échéant à des poursuites pénales. En cas de question, veuillez contacter le service de Relations clientèle ESG au 508.482.0188.



Enterprise Strategy Group est un cabinet d'analyses, de recherches, de validation et de stratégie, qui alimente la communauté IT mondiale en renseignements commerciaux et en analyses exploitables.

© 2016 par The Enterprise Strategy Group, Inc. Tous droits réservés.

