Bitdefender® ENTERPRISE

LIVRE BLANC

L'impact de la sécurité de la virtualisation sur votre environnement VDI

vmware® PARTNER TECHNOLOGY ALLIANCE

CITRIX® ready

Bitdefender

INTRODUCTION

La virtualisation permet aux entreprises de réaliser d'importantes économies et leur apporte une grande flexibilité. L'infrastructure de poste virtuel (Virtual Desktop Infrastructure) est une technologie de virtualisation dont tirent profit de nombreuses entreprises. VDI fournit aux employés et aux employeurs de nombreux avantages, quelle que soit la taille de l'organisation. L'un des avantages de l'infrastructure VDI est sa capacité à fournir aux employés des environnements de bureau administrés de façon centralisée, disponibles sur tout type d'appareil. En procédant de cette façon, l'entreprise est assurée que les informations sont consultées et gérées de manière sécurisée, quel que soit l'endroit à partir duquel les utilisateurs y accèdent.

L'infrastructure VDI ne convient pas à toutes les configurations. Elle est utile dans des environnements de production tels que les centres d'appels ayant une concentration élevée d'employés effectuant un ensemble délimité de tâches, ou pour remplacer les déploiements de parcs d'ordinateurs de bureau à grande échelle. Cependant, quel que soit l'environnement, la sécurité devrait jouer un rôle clé et contribuer à améliorer l'activité de l'entreprise. C'est également le cas avec une infrastructure VDI ; la sécurité devrait être transparente, sans aucun impact sur l'expérience utilisateur. Conçue pour les environnements physiques, la sécurité traditionnelle peut constituer une gêne pour des déploiements VDI, allant même à l'encontre des objectifs premiers recherchés lors de l'adoption de la virtualisation ou d'une l'infrastructure VDI : l'efficacité, la souplesse et les économies de coûts.

Ce document fournit des informations sur les tests de performances réalisés en utilisant des outils standards du secteur tels que Login VSI. Les résultats du test comparent les quatre solutions de sécurité spécifiquement conçues pour les environnements virtualisés disponibles sur le marché actuellement. Ces résultats de tests visent également à aider les entreprises à mieux connaître les pré-requis nécessaires en matière de taille et de performances qu'elles peuvent attendre de leurs déploiements VDI en disposant d'une sécurité optimisée de la virtualisation.

QU'EST-CE QUE L'INFRASTRUCTURE VDI ?

L'infrastructure de poste virtuel (VDI) consiste à héberger le système d'exploitation d'un poste de travail dans une machine virtuelle. La machine virtuelle peut être hébergée dans le datacenter des entreprises ou dans le cloud. De cette manière, la VDI est accessible à partir d'appareils tels que des clients légers, des PC reconditionnés, des smartphones, des tablettes etc. Cela permet aux organisations de garantir une expérience utilisateur final de qualité, quel que soit l'appareil utilisé pour se connecter au réseau de l'entreprise.

Figure 1 : Infrastructure de poste virtuel

LES DÉFIS DE LA SÉCURITÉ DE LA VIRTUALISATION

Il est reconnu qu'une solution antivirus est indispensable de nos jours. Les applications fonctionnant dans des environnements physiques, virtuels ou cloud sont toutes exposées à une exploitation potentielle. Bien que la sécurité classique puisse être utilisée dans des environnements virtualisés, elle n'est ni conçue ni optimisée pour ces environnements.

Utiliser des solutions antivirus traditionnelles peut provoquer des conflits spécifiques dans un environnement VDI tels que :

- De faibles ratios de consolidation des machines virtuelles
- La latence au démarrage
- Des "AV storms" (conflits de ressources)
- Un antivirus non à jour sur les machines virtuelles inactives
- Des goulets d'étranglement pour leur administration

Les ratios de consolidation pâtissent de l'utilisation d'une sécurité traditionnelle dans des environnements virtuels. La sécurité traditionnelle traite chaque machine virtuelle séparément ; elle n'est pas conçue pour évaluer l'ensemble des instances de machines virtuelles d'un réseau ou d'un groupe spécifique. Toutes les actions des applications et des utilisateurs effectuées dans l'instance d'une machine virtuelle sont évaluées par l'agent de sécurité au sein du système d'exploitation. Cet effet de cloisonnement crée une importante duplication de l'utilisation des ressources allant des bases de données de signatures aux résultats d'analyse des mêmes fichiers, ce qui finit par entraîner un problème de performances, ainsi que la baisse des ratios de consolidation des machines virtuelles.

La latence au démarrage est le résultat de l'utilisation d'un antimalware classique dans des environnements virtuels. Lorsqu'une machine virtuelle est lancée, la solution de sécurité doit télécharger les dernières signatures des moteurs antivirus, ainsi que les dernières mises à jour logicielles. Ce processus de mise à jour peut prendre à lui-seul entre 5 et 12 secondes, ce qui crée potentiellement une opportunité pour des attaques malveillantes.

Les "AV storms" ou conflits de ressources se produisent lorsque les agents de la solution de sécurité traditionnelle installés sur chaque machine virtuelle tentent au même moment d'effectuer une mise à jour ou une analyse planifiée. En procédant ainsi, le processeur, la mémoire et l'IOP de l'hôte sont surchargés, ce qui entraîne de mauvaises performances de la machine virtuelle et dans certains cas, la défaillance totale de l'hôte.

Un antivirus non à jour sur des machines virtuelles inactives entraine des problèmes cycliques de gestion des solutions de sécurité antimalwares traditionnelles. Les agents antimalwares installés sur les machines virtuelles inactives peuvent uniquement être mis à jour lorsque les machines virtuelles sont lancées, ce qui crée des problèmes de latence au démarrage et éventuellement des "AV storms", ce qui ne permet pas à la machine virtuelle mal protégée de disposer des fichiers de signatures les plus récents.

L'administration des solutions de sécurité traditionnelles peut devenir délicate, en particulier lors des déploiements les plus importants. À chaque fois qu'un nouvel agent classique est installé, il est enregistré auprès de la console d'administration. Lorsqu'une machine virtuelle est supprimée ou inactive, l'agent classique demeure indexé auprès de la console de sécurité et cette entrée ne peut être supprimée que manuellement. Cela peut devenir une tâche fastidieuse, notamment pour les grandes organisations dans lesquelles les machines virtuelles sont constamment en mouvement.

CHOISIR LA SOLUTION DE SÉCURITÉ DE VIRTUALISATION ADAPTÉE

Bitdefender a utilisé Login Virtual Session Indexer (Login VSI) pour tester l'impact sur un environnement VDI des quatre solutions de sécurité de la virtualisation disponibles actuellement sur le marché. Ces résultats peuvent être utilisés pour déterminer les pré-requis de taille nécessaire à un environnement VDI, lors du déploiement de la sécurisation d'un environnement virtualisé.

Login VSI est l'outil de benchmark VDI de référence qui simule le comportement d'un utilisateur type dans les environnements VDI. L'outil mesure le temps de réponse total de plusieurs opérations effectuées par l'utilisateur avec un poste de travail dans une boucle scriptée. Trois valeurs sont particulièrement importantes à comparer : la valeur de référence, VSIMax #VDI et VSIMax Dynamique.

1. La valeur de référence est la mesure du temps de réponse de certaines opérations effectuées au sein du poste de travail, en millisecondes (ms).
2. Le VSIMax #VDI correspond au nombre maximal de sessions VDI pouvant être obtenues sur l'hôte avant d'observer une dégradation des performances de l'hôte et de VDI.
3. Le VSIMax Dynamique est calculé en fonction de temps de réponse étant systématiquement supérieurs à un seuil donné. Ces seuils sont calculés de façon dynamique en fonction du temps de réponse de la valeur de référence du test.

Une valeur de référence faible correspond à une meilleure expérience utilisateur, et à des réponses plus rapides des applications dans l'environnement VDI.

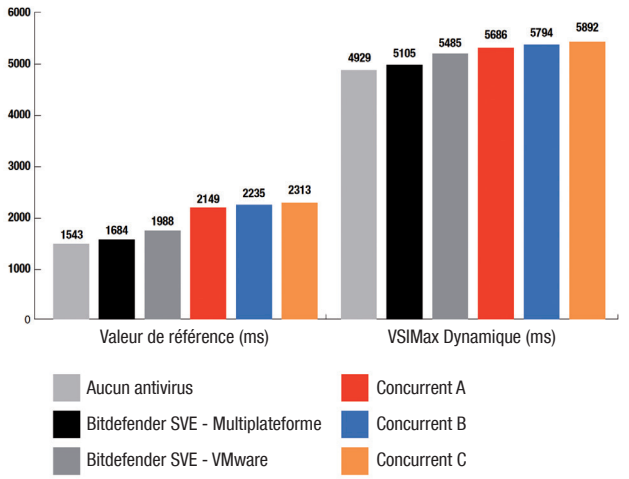

Figure 2 : Login VSI – temps de réponse

La figure 2 représente les résultats des tests de Security for Virtualized Environments (SVE) by Bitdefender comparés à ceux de trois produits de sécurité de virtualisation du marché. Il est important de noter que :

1. Les trois autres solutions de sécurité de la virtualisation utilisent l'intégration à VMware vShield Endpoint. Bien que SVE supporte cette intégration à vShield Endpoint, elle ne se limite pas aux environnements avec VMware vShield Endpoint. Bitdefender SVE a été conçue et optimisée pour tout environnement virtualisé. Sur la figure 2 se trouvent les versions SVE for VMware vShield Endpoint et SVE Multiplateforme.
2. Security for Virtualized Environments (SVE) a les temps de réponse Login VSI les plus bas en comparaison avec ses concurrents, ce qui permet d'obtenir de meilleures performances sur les postes de travail et de profiter d'une meilleure expérience utilisateur.
3. SVE ayant les meilleurs temps de réponse, les entreprises utilisant SVE sont également capables d'atteindre un nombre de sessions plus élevé par rapport aux solutions de sécurité concurrentes.
4. Avec SVE, on peut obtenir au moins 20 sessions supplémentaires par rapport au concurrent le plus proche. Les coûts VDI sont donc inférieurs puisqu'on utilise moins de matériel pour héberger le même nombre de sessions VDI.

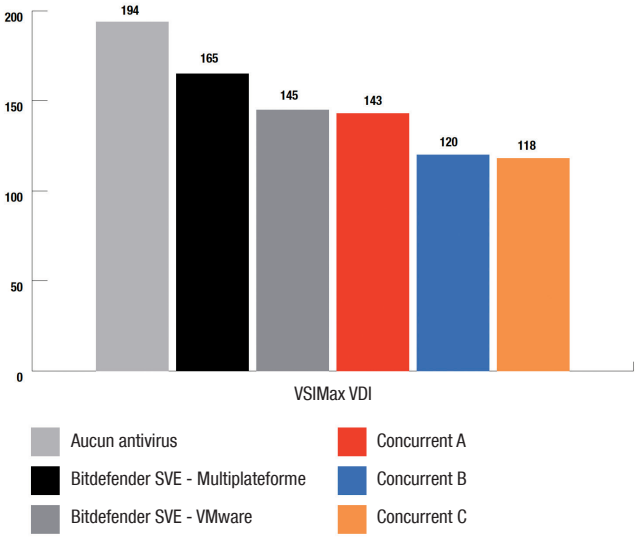

Figure 3 : Login VSI –Nombre maximal de sessions VDI

CONCLUSION

Il n'est plus à démontrer que la sécurité est essentielle pour protéger les applications et les données des entreprises. Cependant, la sécurité ne doit pas entraver le bon fonctionnement des activités de l'entreprise de quelque manière que ce soit. Choisir une solution de sécurité adaptée permet d'éviter des dépenses supplémentaires en matériel, une frustration de la part des utilisateurs et une baisse de leur productivité. Il est donc essentiel de faire le bon choix. Dans un environnement VDI, la solution de sécurité mise en place doit avoir l'impact le plus faible possible sur les ressources disponibles – une vitesse d'ouverture plus rapide des applications, améliorer la productivité des employés et contribuer à faire baisser le nombre d'appels au service d'assistance.

Security for Virtualized Environments est une solution de sécurité complète, spécifiquement conçue pour tout type d'infrastructure virtualisée. Lorsque SVE est déployée dans un environnement VDI, elle permet de gérer le nombre de sessions VDI le plus élevé possible en comparaison avec toutes les autres solutions de sécurité de virtualisation disponibles sur le marché.

Comparée à d'autres solutions de sécurité de virtualisation, SVE dans un environnement VDI permet :

- De réaliser des économies plus importantes.
- De bénéficier d'un meilleur temps de réponse des applications.
- D'obtenir un nombre plus élevé de sessions VDI.
- D'utiliser tout type d'hyperviseur.

ANNEXE

Méthodologie utilisée pour les tests

L'exemple suivant illustre la méthode de calcul de la valeur de référence (en ms) :

Activité	Résultat (ms)	Poids (%)	Résultat pondéré (ms)
Actualiser un document (ACTUALISER)	160	100%	160
Lancer Word avec un nouveau document (CHARGER)	1400	33,3%	467
Boîte de dialogue d'ouverture de fichier (OUVRIR)	350	100%	350
Lancer Notepad (NOTEPAD)	50	300%	150
Boîte de dialogue d'impression (IMPRIMER)	220	200%	440
Boîte de dialogue Remplacer (RECHERCHER)	10	400%	40
Document Zip (ZIP)	130	200%	230
Valeur de référence			**1837**

1. **VSIMax Dynamique (ms) –** La formule de calcul du seuil dynamique est la suivante : Temps de réponse de la valeur de référence moyenne x 125% + 3000. Ainsi, lorsque le temps de réponse de la valeur de référence est de 1800 ms, le seuil VSIMax est de 1800 x 125% + 3000 = 5250 ms.
2. **VSIMax # VDI –** Lorsque la réponse (ms) de toutes les sessions est supérieure à VSIMax Dynamique (ms), le "Nombre maximal de sessions ouvertes" (VSIMax VDI) est atteint.
3. **Nombre de machines -** Avant de commencer les véritables tests, un certain nombre de VDI sont lancées et attendent VSI Login pour se connecter à l'environnement. 220 machines virtuelles sont lancées au début de chaque test. L'objectif est de mieux imiter les environnements de production dans lesquels la connexion peut échouer. Ainsi, le nombre de "VDI en attente" est plus important que celui des "VDI connectées" et sa valeur doit être constante pour que le nombre de VDI soit le même pour tous les tests.
4. **Durée du test :** L'outil de test (Login Vsi Tool) lance des sessions, il doit y avoir un intervalle entre le lancement des sessions. Cette valeur est définie avant le test pour calibrer LoginVSI pour l'environnement. La valeur "Durée" est le temps total alloué au lancement des 220 sessions. L'outil de test connecte un utilisateur toutes les 16 secondes. Cela signifie qu'il doit terminer de connecter tous les utilisateurs en 3 600 secondes.
5. **Charges de travail importantes :** Une charge de travail importante consomme plus de mémoire et de processeur car un plus grand nombre d'applications s'exécutent en arrière-plan. Cette charge de travail simule un utilisateur avancé. Une fois une session démarrée, la charge de travail importante se répète toutes les 12 minutes. Lors de chaque boucle, le temps de réponse est mesuré toutes les 2 minutes.
   - La charge de travail importante ouvre jusqu'à 8 applications à la fois.
   - La vitesse de frappe est de 130 ms par caractère.
   - 40 secondes d'inactivité pour simuler les utilisateurs du monde réel.

   Chaque boucle ouvre et utilise :
   - Outlook 2007/2010, consultation de 10 messages.
   - Internet Explorer, une instance est laissée ouverte (BBC.co.uk), une instance se rend sur Wired.com, Lonelyplanet.com et la lourde application flash gettheglass.com.
   - Word 2007/2010, une instance pour mesurer le temps de réponse, une instance pour consulter et éditer un document.
   - Bullzip PDF Printer & Acrobat Reader, le document Word est imprimé et converti en PDF.
   - Excel 2007/2010, une très grande feuille est ouverte au hasard.
   - PowerPoint 2007/2010, une présentation est consultée et modifiée.
   - 7-zip : les données de la session sont zippées à l'aide de la version en ligne de commande.
6. **Description du système d'exploitation :**
   - Windows 7 X86 SP1, à jour
   - Défragmenteur désactivé
   - Indexeur de recherche désactivé
   - Windows Update désactivé
   - Tâches planifiées désactivées
   - Pare-feu désactivé
   - Windows Defender désactivé
   - Découverte automatique de proxy Web désactivée
   - Thèmes désactivés
   - Superfetch désactivé
   - Service Expérience d'application désactivé
   - Fonctionnalité Fichiers hors connexion désactivée
   - Centre de sécurité désactivé
   - Service Machine Debug Manager désactivé
   - Fonctionnalité Rapport d'erreurs désactivée
   - Mémoire RAM allouée de 1172, sans réserve
   - 1 VCPU alloué sans réserve
   - Fichier d'échange défini sur statique pour 2xRAM

À PROPOS DE LOGIN VSI

VDI et HVD étant des technologies d'infrastructures pour utilisateurs finaux de plus en plus employées, la performance apparaît comme l'un des problèmes clés de ces environnements centralisés. Les organisations qui s'intéressent à ces nouvelles infrastructures ou les implémentent veulent prendre les bonnes décisions concernant les éditeurs, les produits et leur capacité. Elles recherchent de nouveaux moyens de prédire l'effet que ces modifications de l'infrastructure peuvent avoir sur les performances globales après l'implémentation.

Login Virtual Session Indexer (Login VSI) est un outil de benchmark indépendant permettant de tester et de mesurer de façon objective les performances et l'extensibilité des environnements de bureau Windows centralisés tels que Server Based Computing (SBC) et Virtual Desktop Infrastructure (VDI). Les analystes et éditeurs informatiques leaders reconnaissent Login VSI comme l'outil de benchmark de référence pour SBC et VDI, et le recommandent.

Login VSI peut être utilisé pour tester les environnements de bureau virtuels tels que Citrix XenDesktop et XenApp, Microsoft VDI et RDS (Terminal Server), VMware View, Quest vWorkspace et d'autres solutions VDI/SBC.

L'outil Login VSI est utilisé pour :

- **Le benchmark,** afin de prendre les bonnes décisions concernant différentes options d'infrastructures, en fonction de tests.
- **Les tests de montée en charge,** afin d'obtenir des informations sur la capacité maximale de votre environnement hardware actuel (ou futur).
- **La gestion de la capacité,** afin de décider quelle infrastructure permet aux utilisateurs de bénéficier d'un poste de travail optimal.
- **L'analyse de l'impact d'un changement,** afin de tester et prévoir l'impact sur les performances de chaque modification souhaitée avant son implémentation.

Les éditeurs d'infrastructures qui s'engagent à améliorer continuellement les performances et l'extensibilité utilisent Login VSI comme outil de benchmark objectif pour tester, comparer et améliorer les performances et l'extensibilité de leurs solutions. Ils publient leurs résultats dans des livres blancs techniques (vous pouvez les consulter sur www.loginvsi.com) et présentent leurs résultats lors de conférences. Login VSI est également utilisé par des organisations d'utilisateurs finaux, des intégrateurs de systèmes, des fournisseurs d'hébergement et des organismes de tests.

Login VSI est l'outil de référence utilisé dans tous les tests réalisés par le projet de renommée internationale Virtual Reality Check (pour plus d'informations, consultez www.projectvrc.com).

À PROPOS DE BITDEFENDER

Bitdefender est une entreprise internationale qui développe, édite et commercialise des solutions de sécurité dans plus de 200 pays. Sa technologie proactive, en évolution permanente, protège aujourd'hui plus de 500 millions d'utilisateurs dans le monde et est reconnue et certifiée par les organismes de tests indépendants comme l'une des plus efficaces et rapides du marché. Grâce aux équipes de R&D, d'alliances et de partenariats, Bitdefender a atteint l'excellence à la fois dans sa technologie classée n°1 et ses alliances stratégiques avec certains des fournisseurs de virtualisation et de technologie cloud leaders dans le monde. Depuis 2001, Bitdefender confie, pour la France et les pays francophones, l'édition et la commercialisation de ses solutions à la société Editions Profil.

PROFIL TECHNOLOGY

Plus de **500 millions d'utilisateurs**
sont protégés par les technologies Bitdefender.

Bitdefender

Bitdefender est édité en France et dans les pays francophones par PROFIL TECHNOLOGY S.A., éditeur et distributeur de logiciels pour les particuliers et les entreprises.