Bitdefender® ENTERPRISE

LIVRE BLANC

Comment tirer le meilleur parti du Cloud

Bitdefender®

SOMMAIRE

INTRODUCTION

Les entreprises subissent de plus en plus de pression pour réduire les coûts informatiques. Pour y parvenir, l'une des méthodes possibles consiste à transférer des applications dans le cloud. Le cloud computing permet aux entreprises de réaliser des économies sur la durée, alors que les datacenters traditionnels sont associés à des coûts initiaux. En passant d'un modèle CAPEX, basé sur les dépenses d'investissement, à un modèle OPEX, basé sur les coûts d'exploitation, les entreprises peuvent réduire les dépenses liées au matériel et au refroidissement des datacenters. Parmi les autres avantages on compte une productivité améliorée grâce à une charge administrative réduite, qui est la résultante de l'approche 'service à la demande' qui caractérise le cloud computing, et la capacité à fournir des ressources de façon évolutive et quasiment instantanée pour répondre au cahier des charges.

Lorsqu'on transfère une application dans le cloud, des considérations liées à la conception doivent être prises en compte. L'architecture du Cloud computing est assez différente de celle des environnements physiques ou virtuels. Par exemple, le stockage persistant d'Amazon Web Services (AWS) est dissocié de l'AMI (Amazon Machine Image) et les instances de machines virtuelles sont simplement supprimables.

Il est important de prendre en compte comment les applications fonctionnant dans le cloud ont besoin d'être sécurisées. Les machines virtuelles dans un environnement cloud, avec des données importantes de grande valeur, sont tout autant exposées à une exploitation malveillante que les machines physiques. Le même risque existe quelle que soit la plateforme sous-jacente (classique sous forme physique, virtualisée, ou sous forme de cloud privé ou public). **Bien que la sécurité classique puisse être utilisée dans le cloud, elle n'est ni conçue ni optimisée pour le cloud.** Ce document présente les éléments de conception à prendre en compte lors de la transition d'une application vers le cloud ; il évoque également l'impact des solutions antimalwares traditionnelles sur les performances du cloud, qui viennent grever le retour sur investissement (ROI) obtenu grâce au déplacement des besoins de ressources vers le cloud.

DÉPLACER VOTRE APPLICATION VERS LE CLOUD

Plusieurs aspects doivent être pris en compte lors du déplacement d'une application vers le cloud. Deux en particulier, qui sont étudiés dans ce document, sont la tolérance aux pannes et la sécurité des ressources machines. La panne d'Amazon[1] de l'an dernier, très médiatisée, a eu des répercussions sur la qualité de service de nombreuses organisations. Elle a entraîné des pertes de revenus, parfois importantes, dans les cas où la plus grosse partie ou l'intégralité de l'activité de certaines entreprises dépendait de leur connexion à Internet. Plus récemment, une panne d'Amazon provoquée par des orages et la seconde intercalaire[2] a encore provoqué des interruptions de services. Les deux pannes d'Amazon mentionnées ci-dessus ont affecté des zones de disponibilité spécifiques. Une zone de disponibilité peut être comparée à un datacenter. S'il y a une interruption de service dans une zone de disponibilité, les autres zones continuent à traiter les demandes si l'application concernée est conçue pour fonctionner de manière transverse sur plusieurs zones de disponibilité.

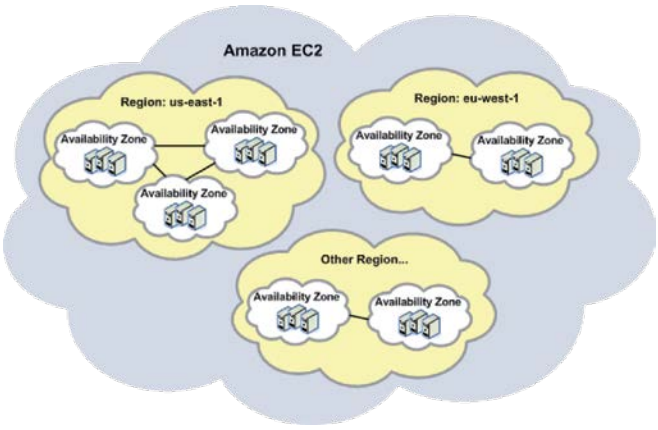

Figure 1 : Zones de disponibilité d'Amazon

[1] Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region – Source : http://aws.amazon.com/message/65648/

[2] Storms, leap second trigger weekend of outages – Source : http://www.information-age.com/channels/the-cloud-andvirtualization/news/2110828/storms-leap-second-triggerweekend-of-outages.thtml

Les entreprises avec une architecture conçue pour supporter la tolérance aux pannes n'ont pas été affectées par les pannes d'AWS. En plus de concevoir plusieurs zones et régions de disponibilité, il faudrait envisager une architecture de fournisseur multicloud. Ainsi, une entreprise ne serait pas limitée à un fournisseur de cloud unique, mais répartirait le risque d'interruption de service entre plusieurs fournisseurs. Le coût de la bande passante avec deux fournisseurs de cloud peut être élevé et devrait être pris en compte, en plus des problèmes potentiels liés à la latence. Les applications mises en place dans des environnements cloud doivent être conçues pour supporter et tirer profit d'architectures, facilitant, par exemple, l'évolutivité horizontale.

Lorsqu'une application est déplacée vers le cloud, il n'est pas nécessaire de repartir de zéro. Ainsi, les courtiers en services de cloud proposent des solutions qui fournissent aux utilisateurs finaux des environnements et des modèles préconfigurés qui sont administrables à partir d'un point unique. Les courtiers en cloud sont également excellents pour gérer les déploiements multiclouds, réduisant ainsi le risque de défaillance de service.

Il existe également de nombreuses ressources en ligne et des intégrateurs de systèmes qui peuvent accompagner le déploiement d'une application dans le cloud. Concevoir une application fonctionnant dans une configuration hautement disponible est absolument essentiel dans le cloud, puisque la défaillance de service est inévitable. Un aspect clé de la conception est la sécurité, une sécurité insuffisante ou mal configurée ne causera pas seulement des pertes d'informations sensibles, mais peut également provoquer une mauvaise qualité de services. Bien que les fournisseurs de cloud disposent de multiples mesures de sécurité, c'est au possesseur de l'application qu'incombe la responsabilité de mettre en place des solutions de sécurité adaptées à l'application.

LA PROTECTION DE VOTRE APPLICATION DANS LE CLOUD

Lorsqu'on déplace une application vers le cloud, on doit prendre en compte tous les aspects de la sécurité mis en place dans les environnements physiques. Bien que les fournisseurs de cloud créent des séparations entre les utilisateurs du cloud, c'est à ces derniers qu'il revient de sécuriser les ressources machines contre les menaces potentielles. L'organisme Cloud Security Alliance fournit des conseils sur la sécurité des applications dans le cloud. La version 3.0[3] du guide de la CSA intitulé "Security Guidance for Critical Areas of Focus in Cloud Computing", comporte huit chapitres consacrés au fonctionnement du cloud qui constituent un guide de référence.

Le chapitre 13 du Guide de Sécurité CSA aborde la virtualisation, l'un des éléments clés du cloud computing. Cela nous conduit au second aspect à prendre en compte lorsqu'on déplace des applications dans le cloud : la protection des ressources machines. Quel que soit l'endroit où une tâche s'exécute, que ce soit un environnement physique, virtuel ou cloud, celui-ci doit être sécurisé. Comme l'explique le chapitre 13 du Guide de Sécurité CSA, **utiliser des logiciels de sécurité conçus pour des environnements physiques dans des environnements virtuels peut entraîner une importante dégradation des performances à la fois de l'hôte et de la machine virtuelle.**

Dans les environnements cloud, si les performances de l'hôte physique ne sont pas forcément la préoccupation de l'utilisateur, les performances de la machine virtuelle le sont assurément. Lorsque la solution de sécurité employée a un impact négatif sur les performances, il faut alors opter pour des instances de machines virtuelles plus grandes, ce qui constitue un coût supplémentaire, afin que l'application fonctionne de façon optimale. Cette différence de coût est de 8 à 32 centimes de dollar[4] supplémentaires par heure respectivement. Il serait donc judicieux d'évaluer les solutions de sécurité ayant été spécialement conçues et optimisées pour les environnements virtualisés.

LES PIÈGES DE LA SÉCURITÉ TRADITIONNELLE

Au sein d'AWS, les modèles de machines virtuelles intitulés Amazon Machine Images (AMI) sont utilisés pour créer plusieurs copies d'instances de machines virtuelles à partir d'une seule Image Machine Amazon (AMI). Techniquement, il est possible d'utiliser la sécurité traditionnelle dans un environnement cloud, mais à quel coût ? Lorsqu'on prend une décision concernant la sécurité, plusieurs aspects doivent être pris en compte.

Les failles de sécurité

Dans les infrastructures cloud telles qu'AWS, les solutions antimalwares avec des agents ne seront potentiellement plus à jour à un moment ou à un autre en raison de l'inactivité d'une machine virtuelle restée non connectée – l'AMI. Lorsqu'une instance de machine virtuelle de l'AMI est démarrée, 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.

La duplication

En raison de la nature des applications fonctionnant dans le cloud, les machines virtuelles sont instanciées et arrêtées selon la demande. Dans de nombreux cas, de multiples instances de machines virtuelles sont générées à partir d'une image de base et des applications sont installées sur l'image via des scripts de démarrage, qui permettent la personnalisation de l'environnement des applications. Ces instances de machines virtuelles ont besoin d'être protégées contre les malwares. Avec les antivirus traditionnels, un agent contenant les signatures du moteur de l'antivirus s'exécute sur chaque instance de machine virtuelle afin de fournir la protection adéquate. Cela déduplique l'effort lié à l'installation de l'agent classique sur chaque instance de machine virtuelle à chaque fois que l'une d'entre elle est créée et génère une importante charge d'administration.

L'administration

À chaque fois qu'un nouvel agent classique est installé, il est enregistré auprès de la console d'administration de sécurité. Lorsque l'instance d'une machine virtuelle est arrêtée, l'agent demeure indexé auprès de la console de sécurité et cette entrée ne peut être supprimée que manuellement. Cela peut devenir une tâche fastidieuse, notamment si l'organisation arrête et crée des instances de machines virtuelles quotidiennement pour répondre aux fluctuations de la demande.

Le mode de licence

Les licences de sécurité traditionnelle sont généralement octroyées par utilisateur ou par machine. Pourtant, dans le cloud, le nombre d'instances de machines et d'utilisateurs fluctue en fonction de la demande. Les entreprises doivent donc estimer leur nombre maximal de machines virtuelles ou d'utilisateurs, et acheter des licences en conséquence. Pourquoi payer pour ce qu'on n'utilise pas ? Les licences antivirus classiques ne proposent pas le modèle basé sur la consommation horaire.

Les performances

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'une zone de disponibilité spécifique en tant que groupe. Toutes les actions des applications et des utilisateurs effectuées dans l'instance d'une machine virtuelle sont évaluées par l'agent de sécurité de cette instance. Cet effet de cloisonnement crée une importante duplication, allant des bases de données de signatures aux résultats d'analyse des mêmes fichiers, ce qui finit par entrainer un problème de performances. Cet impact sur les performances doit être estimé en fonction de la nature de l'application s'exécutant dans le cloud et de la taille de l'instance de la machine virtuelle utilisée pour répondre aux besoins de services.

[3] Security Guidance for Critical Areas of Focus in Cloud Computing – source : https://cloudsecurityalliance.org/research/security-guidance/

[4] http://aws.amazon.com/ec2/pricing/

LA SÉCURITÉ CLOUD SPÉCIALEMENT CONÇUE POUR LA VIRTUALISATION ET LE CLOUD

Une alternative aux solutions antimalwares traditionnelles consiste à utiliser les solutions de sécurité spécialement conçues pour les architectures de virtualisation et de cloud. Ces solutions aident à limiter les problèmes présentés dans ce document. Security for Virtualized environments (SVE) by Bitdefender permet aux clients d'obtenir des ratios de consolidation plus élevés et de meilleures performances de leurs machines virtuelles dans des clouds privés ou publics. Cela est possible grâce aux technologies d'optimisation de Bitdefender dont les brevets sont en cours d'homologation, qui simplifient les processus antimalwares et limitent l'utilisation de ressources sur chaque instance de machine virtuelle.

Bitdefender exécute une analyse centralisée en transférant une grande partie de la fonctionnalité antimalware de chaque instance de machine virtuelle vers des appliances de sécurité virtuelles dédiées sécurisées (SVA). Cette approche optimise à la fois les processus d'analyse à l'accès et à la demande tout en dédupliquant les ressources informatiques critiques. Pour cela, un agent silencieux optimisé spécifiquement pour les environnements virtuels est installé sur chaque instance de machine virtuelle. L'agent silencieux élimine les pièges de sécurité mentionnés précédemment, comme nous l'expliquerons plus en détail ci-dessous.

Des failles de sécurité réduites

L'agent silencieux ne comprend pas de moteur d'analyse ni de fichiers de signatures, contrairement à la sécurité classique basée sur des agents. Puisqu'il n'est pas nécessaire de mettre à jour les signatures du moteur antivirus ou du moteur d'analyse sur chaque machine virtuelle, la faille de sécurité est réduite. Cela est possible car l'ensemble de l'analyse est transféré vers la SVA.

Deux options de déploiement de l'agent silencieux dans un environnement AWS EC2 sont disponibles.

Le déploiement flexible

Lorsqu'on crée une image AMI, Bitdefender Silent Agent peut être installé avec d'autres applications dans l'image AMI. Lorsque plusieurs instances sont générées à partir d'une image AMI sur laquelle Bitdefender Silent Agent est installé chacune de ces instances est protégée et figure dans la Console de Sécurité SVE avec les politiques ayant été configurées pour l'image AMI parente.

Le déploiement automatique

Lorsqu'on gère des déploiements cloud avec des outils fournis par RightScale par exemple, les instances utilisées seront dérivées des images AMI de base avec des applications installées au démarrage selon les besoins. En procédant ainsi, on peut automatiser la création de serveur de façon contrôlée et reproductible. Bitdefender offre la possibilité d'ajouter des tags de déploiement automatique lorsqu'on crée une instance afin que l'agent silencieux soit installé au démarrage.

L'administration intuitive intégrée

SVE s'intègre à de nombreuses API AWS. Les informations sur l'état de l'instance de cette machine virtuelle sont donc disponibles sur la console d'administration AWS et répliquées dans la console d'administration SVE. Si une instance est terminée, elle est retirée de la console SVE. Cependant, tous les événements associés à l'instance terminée sont conservés à des fins de journalisation et de reporting.

La baisse du coût de la sécurité cloud

Les utilisateurs du cloud computing sont habitués aux licences basées sur l'utilisation, avec tarifs évolutifs (pay-as-you grow). Les antivirus traditionnels ne proposent pas ce mode de licence, ce qui empêche de bénéficier des économies associées normalement au cloud computing. Le coût des licences est un élément important à prendre en compte lorsqu'on choisit la solution de sécurité à déployer, en fonction du modèle de licence le plus adapté aux besoins des entreprises. Bitdefender SVE offre cette flexibilité. Les clients peuvent choisir d'utiliser SVE en mode SaaS avec le modèle basé sur la consommation horaire ou, pour un abonnement mensuel fixe à un tarif inférieur, peuvent déployer SVE dans AWS pour protéger un nombre donné de machines virtuelles.

Dans le récent livre blanc de Citrix "Scalability and economics of XenApp on Amazon Cloud"[5] se trouve un exemple de coût horaire par utilisateur, sans sécurité, pour XenApp hébergé dans AWS. À titre de test, Bitdefender a pris l'exemple de 65 sessions utilisateurs XenApp dans une petite entreprise hébergeant XenApp sur AWS. Le test comprend l'impact de l'ajout de la sécurité tout en fournissant au moins 65 sessions utilisateurs. Nos résultats figurent dans ce livre blanc.

Instance type	Compute units	RAM (GB)	vCPUs	East Coast Cost per hr	User Sessions	Cost per hr per user
Standard small	1	1.7	1	$0.115	0	N/A
Standard medium	2	3.7	2	$0.230	5	$0.0460
Standard large	4	7.5	2	$0.460	9	$0.0511
Standard extra large	8	15	4	$0.920	18	$0.0511
Micro 32-bit or 64-bit	1	0.613	1	$0.030	0	N/A
High-memory extra large	6.5	17.1	2	$0.570	17	$0.0335
High-memory double extra large	13	34.2	4	$1.140	33	$0.0345
High-memory quadruple extra large	26	68.4	8	$2.280	65	$0.0351
High-CPU medium	5	1.7	2	$0.285	2	$0.1425
High-CPU extra large	20	7	8	$1.140	23	$0.0495
Cluster compute quadruple extra large	33.5	23	16	$1.610	85	$0.0189
Cluster compute eight extra large	88	60.5	32	$2.970	150	$0.0198
Cluster GPU quadruple extra large	33.5	22	16	$2.600	85	$0.0306

Figure 1 : Coût d'Amazon Elastic Compute Cloud par heure - "Scalability and economics of XenApp on Amazon Cloud"

D'après le test de performances de Login VSI, effectué avant que toute application ou antivirus ne soit installé, pour supporter au moins 65 sessions utilisateurs XenApp, une instance de machine virtuelle AWS quadruple, extra large à mémoire élevée, est nécessaire. À l'aide des mêmes outils de référence Login SVI, utilisés pour évaluer l'impact de la sécurité dans un environnement VDI, Bitdefender, après avoir installé un antivirus traditionnel sur l'instance quadruple extra large à mémoire élevée, a constaté que seules 55 sessions XenApp étaient obtenues.

[5] Scalability and economics of XenApp on Amazon Cloud – Source: http://community.citrix.com/download/attachments/173117739/Citrix_XenApp_on_AWS_Sizing_Economics_Whitepaper_050912.pdf

En raison de la capacité de transfert de l'analyse antimalware utilisée par Security for Virtualized Environments (SVE), le support de 65 sessions utilisateurs XenApp ne nécessite pas d'augmentation de la taille de l'instance de la machine virtuelle AWS hébergeant XenApp dans AWS. Cela signifie que le coût mensuel d'AWS est inférieur à celui associé à l'utilisation de solutions antivirus traditionnelles.

Le graphique ci-dessous illustre les résultats du test effectué avec une instance de machine virtuelle AWS quadruple, extra large à mémoire élevée, hébergeant XenApp. Il présente la différence entre le coût horaire associé à l'utilisation de SVE et celui associé à un antivirus traditionnel. Le graphique présente également les différents modèles de tarification de Bitdefender pour répondre aux besoins des clients.

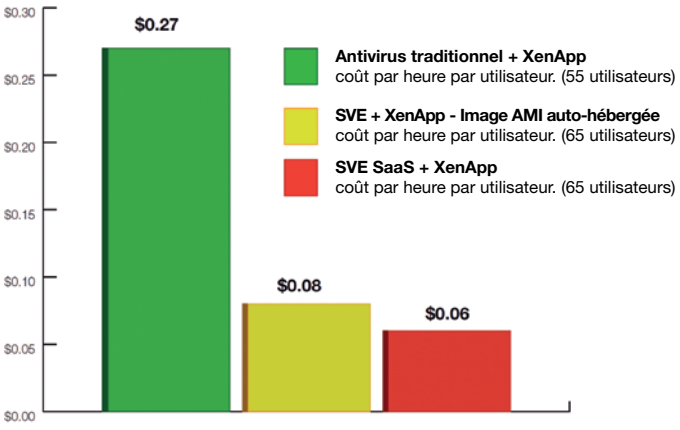

Figure 2 : Coût d'une session XenApp par utilisateur avec un Antivirus

Sur le graphique 1, deux informations essentielles requièrent votre attention :

- L'antivirus traditionnel réduit les performances de l'application – le nombre maximal de sessions utilisateurs est passé de 65 à 55.
- Le coût de l'antivirus traditionnel comparé à SVE est supérieur d'au moins 22% par utilisateur et par heure.

Les coûts par utilisateur comprennent le coût de l'hébergement de la console d'administration de l'antivirus traditionnel sur une petite instance sur AWS. Les coûts de l'image AMI auto-hébergée de SVE comprennent les coûts de l'hébergement de l'appliance d'analyse SVE et de la console d'administration sur AWS.

Ce qui n'est pas inclus, et doit être ajouté au coût de l'antivirus traditionnel, est le coût de la bande passante pour mettre à jour tous les agents traditionnels s'exécutant sur l'instance de la machine virtuelle. De plus, les licences des antivirus traditionnels sont généralement basées sur des montants mensuels ou annuels fixes, correspondant à un nombre fixe de postes de travail. SVE apporte à ces modèles de licences la souplesse à laquelle les utilisateurs du cloud sont habitués.

L'antivirus est assurément indispensable aux systèmes actuellement. Le test réalisé par Login VSI dans le livre blanc de Citrix "Scalability and economics of XenApp on Amazon Cloud" montre que l'antivirus traditionnel et la virtualisation des applications ont un impact sur le temps de réponse de XenApp.

Login VSI a mesuré le temps de réponse pour illustrer le nombre maximal de sessions utilisateurs pouvant être obtenu sur un système spécifique hébergeant XenApp. Dans le test Login VSI, l'antivirus traditionnel a un impact sur le nombre de sessions utilisateurs, qui entraîne une baisse de 15% du nombre de sessions utilisateurs (55 au lieu de 65) par rapport au nombre de sessions utilisateurs permis par SVE.

Security for Virtualized Environments (SVE) by Bitdefender est conçu spécialement pour les environnements virtualisés. Il a été pensé pour fournir les meilleures performances possibles avec le moins d'impact, tout en assurant une sécurité de qualité.

Une intelligence intégrée

Security for Virtualized Environments de Bitdefender utillise un mécanisme de mise en cache intelligent unique, dont le brevet est en cours d'homologation, qui crée une liste blanche d' applications et de fichiers courants du système d'exploitation . Ce processus améliore de façon significative les performances d'analyse des machines virtuelles, et est mis à jour en continu. Cela est possible grâce aux deux niveaux de cache utilisés par la solution. L'un d'entre eux est un cache d'auto-apprentissage, intégré à la SVA. Silent Agent utilise un cache local pré-rempli en fonction des variables de son environnement. Il peut donc transférer l'analyse des objets requis uniquement, tout en excluant les objets qui sont répertoriés comme étant sûrs.

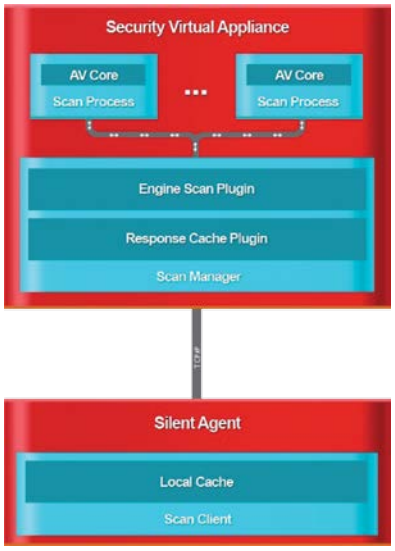

Figure 3: Aperçu de l'architecture d'analyse

CONCLUSION

Lorsqu'on déplace une application vers le cloud, l'utilisation d'une forme de sécurité traditionnelle aura des effets nocifs ayant au final un impact négatif sur l'activité des entreprises. Il est indispensable d'utiliser des solutions de sécurité spécialement conçues dès le départ pour les environnements virtualisés. Utiliser des solutions antivirus classiques dans le cloud entraine une diminution des performances système tout en augmentant les coûts. Peu d'économies sont réalisées, voire aucune, ce qui limite l'intérêt du transfert d'applications vers le cloud.

Security for Virtualized Environments est une solution conçue spécifiquement pour les clouds privés et publics. Elle isole le service d'analyse des instances de machines virtuelles qui sont protégées, relevant un nombre important des défis présentés précédemment. De plus, d'importants gains de performances sont obtenus grâce aux mécanismes de mise en cache intelligents employés par SVE qui sont mis à jour en permanence. Cela permet de réaliser de plus grandes économies en raison de l'impact très réduit de SVE sur chacune des instances de machines virtuelles en comparaison avec la sécurité classique.

ANNEXE

À propos de Login VSI

VDI et HVD étant des technologies d'infrastructures pour utilisateurs finaux de plus en plus utilisées, 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 bureaux 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'infrastructure, 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 D'AMAZON WEB SERVICES

Amazon Web Services (AWS) est un éditeur mondial de services d'infrastructure cloud. Amazon Web Services est une plate-forme informatique à haute fiabilité, redimensionnable et à bas coût dans le nuage qui alimente des centaines de milliers d'entreprises dans 190 pays. Avec des centres de données situés aux États-Unis, en Europe, à Singapour et au Japon, les clients de tous les secteurs bénéficient d'un coût réduit, d'une agilité, d'une élasticité instantanée et d'une sécurité multiniveau dans le cloud.

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 400 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 la société PROFIL TECHNOLOGY S.A., spécialiste de la sécurité des systèmes d'information et du filtrage de contenus numériques.