Sécurité pour data centers

KASPERSKY SECURITY FOR VIRTUALIZATION 4.0

Nouvelles fonctions — pour une sécurité renforcée, une efficacité et une vitesse accrues

Les entreprises étant de plus en plus nombreuses à utiliser des SDDC (Software-defined data centers), il est plus que jamais essentiel d'assurer une protection puissante sans compromettre la productivité.

C'est précisément ce qu'offre Kaspersky Security for Virtualization : une protection puissante multiniveaux des infrastructures de bureau virtuel (ou VDI) et des structures de serveurs virtuels améliorées par l'intégration précise des plates-formes et des technologies de virtualisation les plus populaires, telles que VMware vSphere avec NSX, Microsoft Hyper-V, Citrix XenServer et KVM, ou encore VMware Horizon et Citrix XenDesktop.

Aujourd'hui, avec Kaspersky Security for Virtualization version 4.0, nous redéfinissons la façon dont votre SDDC et sa solution de sécurité interagissent, augmentant ainsi leur performance, leur vitesse et leur efficacité.

Découvrez quelques-unes des nouvelles fonctions de la version 4.0 :

Intégration native sans agent avec VMware NSX ***IMPORTANT***

RÉSEAU ANTI-MALWARE SANS AGENT

Bénéficiez, pour chacune de vos machines virtuelles (VM) gérées par VMware NSX, d'une protection instantanée contre les programmes malveillants basée sur notre moteur primé, sans avoir besoin d'installer un agent sur les machines.

PRÉVENTION DES INTRUSIONS

Protégez votre infrastructure virtuelle des menaces réseau et des vulnérabilités « zero-day » les plus avancées grâce aux performances des systèmes de détection et de prévention d'intrusion (IDS / IPS) proposées aux hôtes virtuels gérés par la plate-forme VMware NSX.

DÉPLOIEMENT AUTOMATISÉ

L'intégration de VMware NSX permet le déploiement entièrement automatisé d'appliances de sécurité (machine virtuelle de sécurité ou prévention des intrusions). Celles-ci apparaissent automatiquement sur l'hyperviseur en fonction des politiques de sécurité appliquées à chaque machine virtuelle.

POLITIQUES DE SÉCURITÉ

Cette intégration avec VMware NSX permet également à chaque machine virtuelle de disposer de fonctionnalités de sécurité individuelles précises et granulaires. Cette fonction prend également en charge la construction et l'évolution de SDDC parfaitement équilibrés.

TAGS DE SÉCURITÉ

Kaspersky Security for Virtualization et la plate-forme VMware NSX échangent désormais des balises de sécurité, pouvant varier selon des critères spécifiques (des programmes malveillants détectés dans une machine virtuelle, par exemple). L'interaction constante entre l'infrastructure et son système de sécurité permet au data center défini par logiciel de réagir instantanément à tout incident de sécurité, en démarrant automatiquement une reconfiguration de l'ensemble de l'infrastructure virtuelle, si nécessaire.

vmware PARTNER TECHNOLOGY ALLIANCE

vmware READY NETWORKING AND SECURITY

CITRIX READY

Analyse complète de l'infrastructure en mode sans agent ***IMPORTANT***

ANALYSE À LA DEMANDE DE MACHINES VIRTUELLES EN LIGNE ET HORS LIGNE

Les solutions « traditionnelles » ne permettent pas de réaliser une analyse anti-malware sans agent d'une machine virtuelle hors ligne. La nouvelle version de Kaspersky Security for Virtualization introduit une fonctionnalité avancée pour analyser l'ensemble des machines virtuelles, qu'elles soient en ligne ou hors ligne. Vous pourrez ainsi disposer d'une analyse à la demande plus efficace et d'une sécurité renforcée sur l'ensemble de votre infrastructure.

Light Agent sur serveurs Linux ***IMPORTANT***

PROTECTION DES SERVEURS WINDOWS ET LINUX AVEC LIGHT AGENT

Kaspersky Security for Virtualization Light Agent est la solution idéale pour les data centers hybrides, offrant des performances de sécurité avancées pour tous les serveurs, quel que soit leur système d'exploitation. Les plates-formes Linux comprennent :

- Red Hat Enterprise Linux Server 6.7, 7.2
- SUSE Linux Enterprise Server 12 SP1
- CentOS 6.8, 7.2
- Debian 8.5
- Ubuntu Server 14.04, 16.04 LTS

Light Agent pour une virtualisation basée sur RHEL

PRISE EN CHARGE POUR KVM BASÉE SUR L'OS RHEL

Nous continuons à allonger la liste de nos plates-formes de virtualisation prises en charge, avec l'ajout de KVM basée sur le système d'exploitation RHEL Server (Red Hat Enterprise Linux Server).

Prise en charge de solutions supplémentaires par Microsoft

WINDOWS SERVER 2016

Kaspersky Security for Virtualization Light Agent et Agentless offrent désormais les performances de sécurité les plus avancées sur Microsoft Windows Server 2016, pour une flexibilité accrue.

WINDOWS 10 RED STONE 1 (RS1)

Kaspersky Security for Virtualization Light Agent et Agentless prennent déjà en charge Windows 10, populaire dans les environnements de VDI. Nous offrons désormais une prise en charge supplémentaire pour Windows 10 Red Stone 1 (RS1).

MODE COMPLET ET MODE SERVER CORE

Kaspersky Security for Virtualization version 4.0 Light Agent et Agentless prennent en charge les systèmes d'exploitation Windows Server à la fois en mode complet et en mode Server Core. Cet élément est particulièrement essentiel au moment où les entreprises développent de plus en plus de serveurs d'infrastructures stratégiques sans interface utilisateur en mode Server Core (contrôleurs de domaine, DHCP, DNS, par exemple).

WINDOWS HYPER-V 2016

Kaspersky Security for Virtualization Light Agent prend également en charge la toute dernière plate-forme de virtualisation Microsoft, permettant aux entreprises de sécuriser leurs data centers définis par logiciel sous Hyper-V 2016, grâce à nos solutions contre les programmes malveillants et à nos performances en termes de protection réseau.

DÉPLOIEMENT DE SCVMM (SYSTEM CENTER VIRTUAL MACHINE MANAGER)

Kaspersky Security for Virtualization Light Agent peut désormais être déployé simultanément sur plusieurs hôtes Microsoft Windows Hyper-V via le SCVMM.

Light Agent en mode silencieux

DÉSACTIVATION DE L'INTERFACE UTILISATEUR LIGHT AGENT

Le système Kaspersky Security for Virtualization Light Agent UI (Interface Utilisateur) peut désormais être désactivé sur toute machine virtuelle du SDDC. Cela peut par exemple s'avérer utile dans le cas de virtualisation de bureau sur les systèmes d'exploitation Windows Server, lorsque les fonctionnalités Remote Desktop ou Terminal Services sont activées, ou dans le cas de virtualisation d'application basée sur Citrix XenApp.

Serveur d'intégration amélioré

PLUSIEURS SERVEURS VMWARE VCENTER SUR UN SEUL SERVEUR D'INTÉGRATION

Les serveurs d'intégration dédiés de Kaspersky Security for Virtualization peuvent être connectés à plusieurs serveurs VMware vCenter, obtenant ainsi des informations supplémentaires à partir de votre infrastructure virtuelle basée sur VMware.

Auto-surveillance machine virtuelle de sécurité (SVM)

AGENT SNMP AVANCÉ SUR SVM

Kaspersky Security for Virtualization peut être installé avec un agent SNMP. Celui-ci permet de gérer et d'envoyer de nombreuses informations concernant « l'état de santé » de la SVM à des outils de contrôle SNMP tiers, tels que Zabbix et Nagios. Les protocoles SNMP comprennent des indicateurs généraux de SVM (CPU, RAM, etc.) et d'autres indicateurs spécifiques.

Autres améliorations

EXCEPTIONS OU GESTION DE LA MISE À EXÉCUTION

Kaspersky Security for Virtualization Light Agent propose désormais une liste plus étendue d'applications logicielles tierces à utiliser quand vous précisez les exceptions ou configurez la politique d'analyse à respecter.

INSTALLATION UNIFIÉE DU PLUG-IN ET DU SERVEUR D'INTÉGRATION

Vous pouvez à présent installer le plug-in d'administration et le serveur d'intégration de Kaspersky Security for Virtualization de façon unique et unifiée. Le plug-in et le centre d'administration du serveur d'intégration sont installés et configurés à l'aide de l'assistant d'installation des volets de gestion de Kaspersky Security. Vous pouvez également démarrer l'installation depuis la ligne de commande.

API VSHIELD ENDPOINT TOUJOURS PRISE EN CHARGE

De nombreuses entreprises migrent, ou prévoient de migrer, vers VMware NSX. Elles sont pourtant encore nombreuses à utiliser l'ancienne technologie, vShield Endpoint. Security for Virtualization Agentless version 4 assure une prise en charge totale de vShield Endpoint, et nous nous engageons à prendre en charge cette technologie aussi longtemps que nos clients le souhaiteront. En termes de sécurité, vous pourrez donc effectuer une transition en douceur et à votre rythme.

Kaspersky Security for Virtualization version 4.0 — une sécurité renforcée, une efficacité et une vitesse accrues.

Plates-formes prises en charge :

HYPERVISEURS :

vCenter Server
NSX 6.2.4*
vSphere 6.5**
vSphere 6.0
vSphere 5.5
vSphere 5.1**

MS SCVMM 2016**
MS SCVMM 2012 R2**
Hyper-V 2016** (mode complet + server core)
Hyper-V 2012 R2** (mode complet + server core)

XenServer 6.5 SP1**
XenServer 7.0**

CentOS 7.2**
Ubuntu Server 14.04 LTS**
RHEL Server 7u1**

SERVEUR OS :

Windows Server 2016 (mode complet + server core)
Windows Server 2012 R2 (mode complet + server core)
Windows Server 2012 (mode complet + server core)
Windows Server 2008 R2 (mode complet + server core)
Windows Server 2008** (mode complet + server core)
Windows Server 2003 R2*
Debian 8.5
Ubuntu Server 14.04, 16.04 LTS**
CentOS 6.8, 7.2**
RHEL Server 6.7, 7.2**
SUSE LES 12 SP1**

BUREAU OS :

Windows 10 (RS1 compris)
Windows 8.1
Windows 8*
Windows 7
Windows XP SP3 (32 bits)*

PLATE-FORMES VDI :

Citrix XenDesktop 7.9, 7.11**
Citrix Provisioning Services 7.9, 7.11**
VMware Horizon View 7**

* Pris en charge par la solution KSV Agentless uniquement

** Pris en charge par la solution KSV Light Agent uniquement

EN SAVOIR PLUS :
http://www.kaspersky.fr/enterprise-security

© 2016 Kaspersky Lab. Tous droits réservés. Les marques déposées et marques de service sont la propriété de leurs détenteurs respectifs.