

Antivirus Kaspersky : retour d'expérience

Capitoul
15 février 2018

- > Au LAAS en avril 2016 (moi)
- > Au marché CNRS en mai 2016 (Kaspersky)
- > Début du déploiement en juin 2016

> Kaspersky Security Center

- Windows Server
- Console mmc
- SQL intégré ou autre si +10.000 appareils
- Site web (apache/php sous linux ou sous windows...)
- VM 4 vcpus, 8 Go RAM, 60 Go disque

The screenshot displays the Kaspersky Security Center 10 administration console. The interface is divided into a left-hand navigation pane and a main content area. The main area is titled 'Serveur d'administration' and features several tabs: 'Surveillance', 'Statistiques', 'Rapports', and 'Evénements'. A 'Paramètres du Serveur' link is visible in the top right of the main area.

The left-hand navigation pane includes the following categories:

- Appareils administrés
 - Client Installé
 - Étape 1 - Installation Agent
 - Étape 2 - Désinstallation Symantec
 - Pour tests
 - Serveurs
- Appareils non définis
- Sélections d'appareils
- Stratégies
- Tâches
- Avancé
 - Comptes utilisateurs
 - Administration des applications
 - Catégories d'applications
 - Registre des applications
 - Fichiers exécutables
 - Vulnérabilités dans les applications
 - Mises à jour du logiciel
 - Licences pour les logiciels de Kaspersky Lab
 - Compte des licences tierces
 - Installation à distance
 - Déploiement des images des appareils
 - Paquets d'installation
 - Sondage du réseau
 - Domaines
 - Active Directory
 - Plages IP
 - Appareils réseau
 - Stockages
 - Matériel
 - Mises à jour et correctifs de Kaspersky Lab
 - Quarantaine
 - Sauvegarde
 - Fichiers avec traitement différé

The main content area displays several key alerts and actions:

- Déploiement:** 'Le licence n'est plus valide sur 87 appareils'. Actions include 'Installer la protection', 'Administrer les clés', and 'Rapport de déploiement de la protection sur le réseau'.
- Structure d'administration:** 'La connexion avec 50 appareils est perdue' and '271 appareils ne s'est pas connecté au Serveur d'administration depuis longtemps'. Actions include 'Accéder aux appareils administrés', 'Configurer le déplacement automatique des appareils dans les groupes', and 'Consulter les appareils non définis'.
- Configuration de la protection:** 'Application de protection désactivée : 9 appareils', 'La protection n'est pas lancée : 9 appareils', and 'Une vulnérabilité a été découverte dans le logiciel sur les appareils'. Actions include 'Configurer la protection des postes de travail', 'Configurer la recherche de virus pour les postes de travail', and 'Administrer les applications sur les appareils'.
- Mise à jour:** 'Les bases sont dépassées : 1 appareils', 'La recherche de mises à jour Windows n'a pas eu depuis longtemps sur 9 appareils', 'Les mises à jour des applications de Kaspersky Lab sont retirées', 'Des mises à jour des composants Kaspersky Security Center 10 sont disponibles', 'Des mises à jour des applications Kaspersky Lab sont disponibles', and 'Version des applications de Kaspersky Lab actuellement disponibles'. Actions include 'Consulter les versions actuelles des applications de Kaspersky Lab', 'Accéder au dossier "Mises à jour et correctifs de Kaspersky Lab"', and 'Rapport des bases antivirus utilisées'.
- Surveillance:** 'Les événements critiques sont enregistrés sur le Serveur d'administration.' and 'Les événements sur les erreurs sont enregistrés sur le Serveur d'administration.'. Actions include 'Consulter l'état de la protection', 'Consulter les requêtes des utilisateurs (nouveaux : 0)', and 'Configurer les paramètres des notifications'.
- Serveur d'administration:** Actions include 'Propriétés du Serveur d'administration', 'Consulter les informations sur la clé du Serveur d'administration', and 'Configurer la fonctionnalité affichée dans l'interface d'utilisateur'.

- > Kaspersky Endpoint Security
 - Client proprement dit
 - Windows / Mac / Linux / Android

- > Agent d'administration Kaspersky
 - Livré avec le KSC
 - Sert à lier le serveur aux clients

Kaspersky Endpoint Security 10 for Windows

Kaspersky Security Network

Rapports Quarantaine

Statut de la protection Configuration Pierre Fauret, vous travaillez sous une stratégie

Endpoint Control

- Contrôle des applications** Surveillance des applications
 - Contrôle du lancement des applications Désactivé(e)
 - Contrôle de l'activité des applications Désactivé(e)
 - Surveillance des vulnérabilités Désactivé(e)
- Contrôle des périphériques** Désactivé(e)
- Contrôle Internet** tentatives d'accès aux ressources Internet autorisées : **1273**, interdites : **0**

Protection - partiellement activée (modules activés : 4 sur 7)
objets analysés : **49086**, menaces détectées : **0**

Gestion des tâches : 5 tâches sur 8 sont planifiées
Prochaine tâche : Mise à jour sera lancée **08-Feb-18 à 16:16**

> Notion de groupe ~ OU AD

> Définition de "stratégie de groupe"

- Pour l'agent d'administration
- Pour le client
- Appliqué au groupe final

> Notion de tâches

- Nombreuses par défaut

> Récupération des machines

- AD
- Scan réseau windows (netbios)
- Scan réseau ip

> Ancien AV à désinstaller (Symantec)

- Echec via GPO
- Via Kaspersky, grâce au support pour modifier les applications incompatibles
- <https://companyaccount.kaspersky.com/>

> 3 groupes

- 1- A faire -> machines en situation d'origine
 - Tâche d'installation de l'agent d'administration
- 2- Désinstallation Antivirus Δ
 - Tâche de désinstallation de Symantec
- 3- Installation KES
- Groupe final + groupe serveur

Début 2018 => 168, 3, 680

> "Ça redémarre tout seul"

- Désactivation du reboot automatique en fin d'install

> "C'est lent"

- Désactivation de la surveillance des vulnérabilités
- Désactivation de la surveillance de l'activité des applications et system watcher
- Planification plus précise des tâches
 - Mises à jour (dès le téléchargement sur le serveur)
 - Scan rapide (tout les 3 jours, 13h30)
 - Inventaire (tout le 2 du mois à 13h00)

> "Ça marche pû"

- Désactivation du contrôle de l'activité des applications
- Désactivation surveillance mail (application précise)

- > Mise à jour SP2 -> ne recrée pas de stratégie
 - Obligation de re-crée une deuxième stratégie pour les clients passés en SP2
 - Réparé avec le KSC 10.4.343

- > Incompatibilité avec le shell ubuntu intégré dans W10
 - Pas de réponse du support

- > Remarque sur le versioning à la русский
 - KES 10 SP1 MR2 (10.2.4.674 et 10.2.5.3201)
 - KES 10 SP2 (10.3.0.6294)
 - KES 10 SP2 MR1 (idem)

> Rapports

- Customisables
- Par mail ou upload dossier smb
- pdf, html, xml

> Mises à jour automatiques du logiciel, agents de mises à jour

> Restauration de fichiers en quarantaine

> Désactivation temporaire (temps, action, reboot)

> Efficace ?

- pas de cryptolocker depuis 2016 :)
- Mais pas parfait (ex: c99 php webshell)

> Efficace ?

Kaspersky 

Ad-Aware	Virtool.PHP.C99Shell.B	20180125
AegisLab	Backdoor.PHP.C99Shell.btfc	20180125
AhnLab-V3	PHP/C99Shell	20180125
ALYac	Backdoor.PHP.C99Shell.A	20180125
Arcabit	Virtool.PHP.C99Shell.B	20180125
Avast	JS:Agent-BMD [Trj]	20180125
AVG	JS:Agent-BMD [Trj]	20180125
Avira (no cloud)	PHP/C99Shell.B	20180124
Baidu	PHP.Backdoor.C99Shell.d	20180124
BitDefender	Virtool.PHP.C99Shell.B	20180125
Bkav	VEX490D.Webshell	20180124
CAT-QuickHeal	HTML.Agent.AD	20180124
ClamAV	Php.Trojan.C99Shell-2	20180125
Cyren	PHP/C99Shell.A	20180125
DrWeb	PHP.Shell.99	20180125
Emsisoft	Virtool.PHP.C99Shell.B (B)	20180125
ESET-NOD32	PHP/C99Shell.A	20180125
F-Prot	PHP/C99Shell.A	20180125
GData	Virtool.PHP.C99Shell.B	20180125
Ikarus	PHP.C99Shell.B	20180124
Jiangmin	Trojan/Script.Gen	20180125
MAX	malware (ai score=89)	20180125
Microsoft	Backdoor:PHP/C99shell.U	20180125
eScan	Virtool.PHP.C99Shell.B	20180125
NANO-Antivirus	Trojan.Script.C99Shell.bgzsf	20180125
Panda	PHP/C99Shell.A	20180124
Qihoo-360	php.script.c99shell.10	20180125
Rising	Backdoor.C99Shell!8.366 (TOPIS:ixyrDQAioEK)	20180125
Sophos AV	Mal/C99-A	20180125

- > Difficulté d'interpréter les événements
- > Difficulté de suivre l'activité virale
 - Auto-traitement (suppression/quarantaine)
 - RAZ virus manuel :(
- > Charge sur les machines clientes reste importante
- > Comportement avec les VMs windows
 - Visibles...
 - Mais certaines se dupliquent sur le KSC...
 - On ne peut pas les administrer...
 - Problème du NAT Virtualbox ?
- > Souvent suspect car agit a de nombreux niveaux (réseau, protocoles, usb...)

