Antivirus Kaspersky : retour d'expérience

Capitoul
15 février 2018

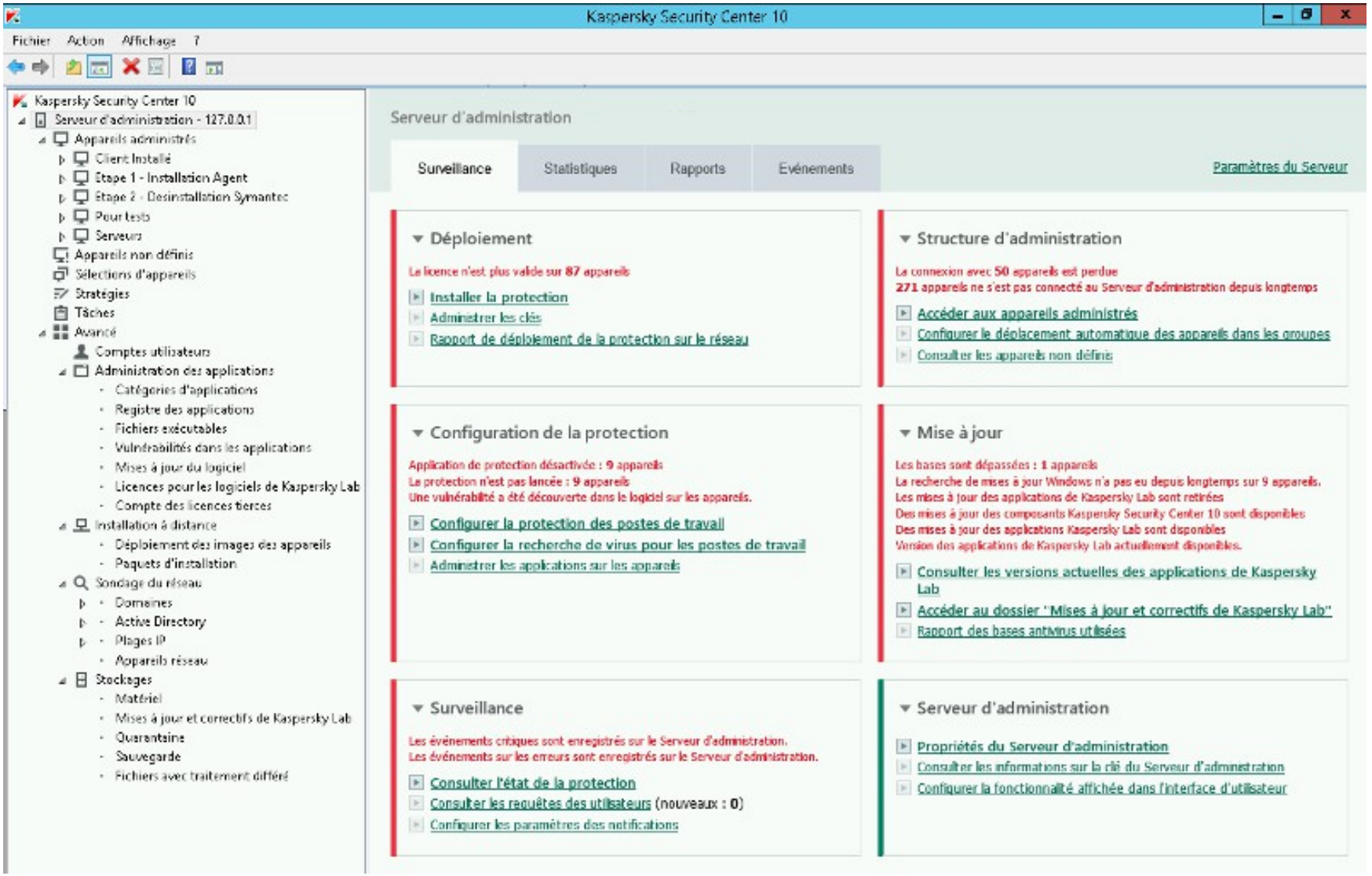
Arrivée

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

Premiers Contacts

- 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

Premiers Contacts

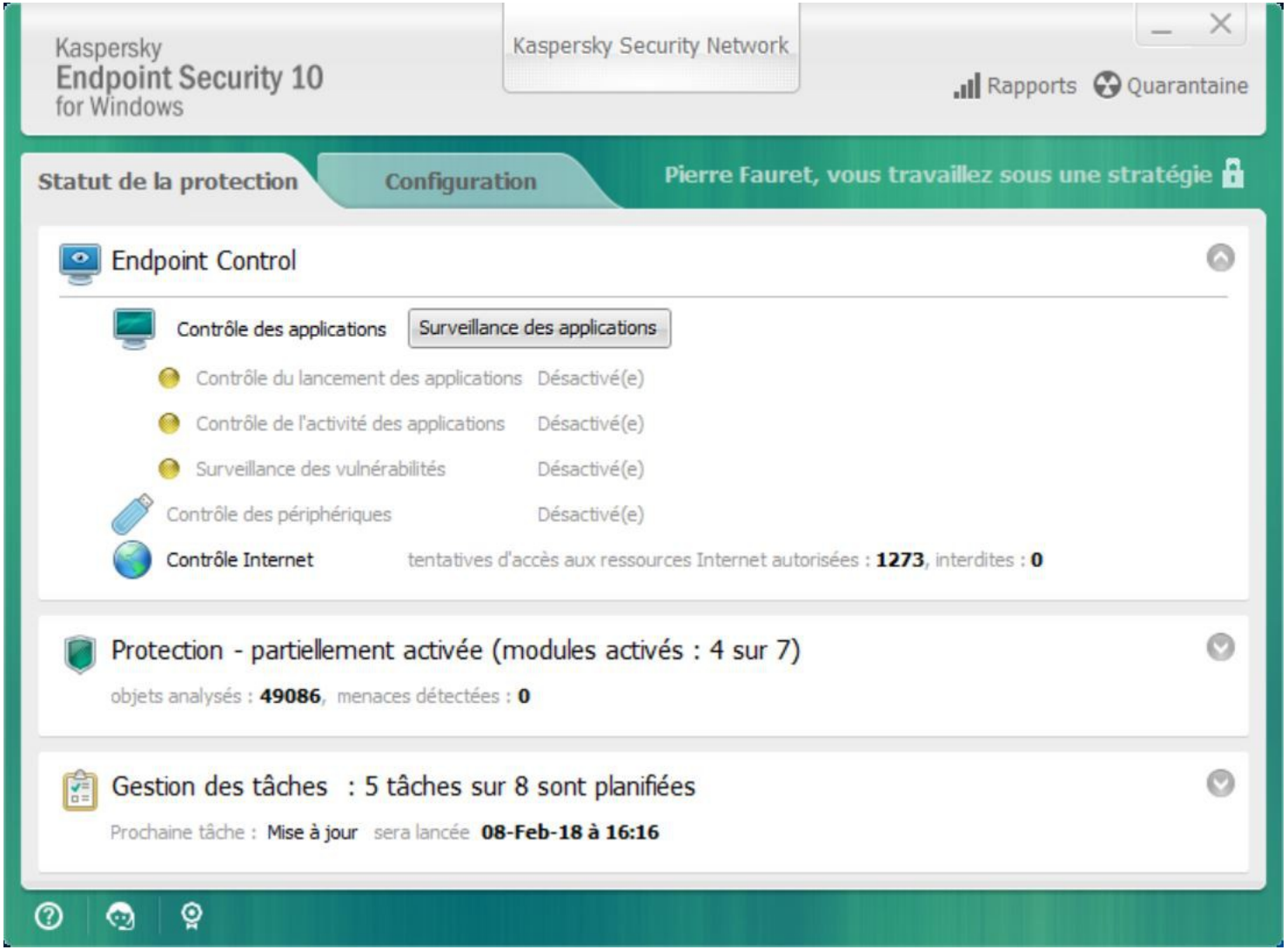


Premiers Contacts

- 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

Premiers Contacts



Déploiement

> 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 ⚠
  - Tâche de désinstallation de Symantec
- 3- Installation KES
- Groupe final + groupe serveur

Début 2018 => 168, 3, 680

Premiers Ecueils

> "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)

Premières Surprises

- Mise à jour SP2 -> ne recrée pas de stratégie
  - Obligation de re-créer 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)

Au quotidien

- 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)

Au quotidien

> Efficace ?

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

Au quotidien

> Efficace ?

Kaspersky	✔

Ad-Aware	Virtool.PHP.C99Shell.B	20180125
AegisLab	Backdoor.PHP.C99Shell.bt!c	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.bgzasf	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

Les X-Files

- Difficulté d'interpréter les évènements
- 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...)

Kestions ?